An Approach to Quantifying Resilience in Mobile Ad hoc Networks

Abdul Jabbar, Hemanth Narra, James P.G. Sterbenz
Information and Telecommunication Technology Center
The University of Kansas
Lawrence, KS 66045
Email: {jabbar, hemanth, jpgs}@ittc.ku.edu

***Abstract*—Resilience is the ability of a network to provide acceptable service in the presence of challenges to normal operations. With increasing significance of resilience in modern communications infrastructure and services, there is a need for rigorous quantitative evaluation of resilience. In this paper, we present a framework to quantify resilience between any two layers in the network stack. Resilience is quantified as a function of state transitions wherein states are defined as aggregation of points in the two orthogonal dimensions of operational and service state. This approach is applied to the case of mobile ad hoc networks in order to determine the resilience of various levels to the perturbations in the normal operations of the network. Simulation results show that this framework provides a tractable approach and abstraction to quantify multilevel resilience.**

I. Introduction

The significance of resilient communication networks in modern society is well established, wherein resilience is defined as *the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation* [1] and includes survivability, dependability, and performability[1]. Resilience and survivability [2], [3] mechanisms in current networks are limited and domain specific. Subsequently, the evaluation methods are either qualitative assessments or context-specific metrics. Due to this lack of consistency in evaluating network resilience, it is difficult to guarantee that the networks being designed and developed would satisfy the requirements of both the end users and their applications [4]. Without standard metrics to measure the relative effectiveness of resilience mechanisms, it is difficult to identify potential solutions that lead to resilient networks. While it is clear that a number of new and innovative solutions are needed to provide network resilience, a key problem is *how to measure and specify resilience*. We need a methodology to *measure* the resilience (or lack thereof) of current and proposed networks and *evaluate the benefit* of particular architectures, designs, and mechanisms. This methodology needs to be both rigorous in capturing service parameters and operational metrics, as well as tractable so that it is useful in practice. The challenge is to bring order to a fundamentally complex problem; we do not underestimate the difficulty in this task and note that the QoS (quality of service) community has struggled with a related problem for some years. An important aspect is to produce abstractions that provide useful insight even if not completely representing the problem. The development of resilience measures is further complicated by the heterogeneity of communication networks. In other words, a resilience scheme that applies well to a specific network scenario may not work as well on a different network scenario. A recent survey on resilience differentiation frameworks [5] specifically points to this lack of unified strategy to deal with resilience issues at different level of the Internet - from core to the access networks.

Furthermore, the resilience strategy must be *multilevel* because it is necessary to improve the resilience of a communication network at each layer in the protocol stack. Hence, in this paper we propose a *new multilevel framework to measure and analyze network resilience* at a given layer boundary. Resilience is effectively quantified as robustness, which measures service degradation in the presence of challenges (perturbations) to the operational state of the network. In order to demonstrate the applicability of the proposed framework, we analyze the resilience of typical MANETs (wireless mobile ad hoc networks). MANETs present an interesting case for resilience analysis. MANETs are inherently challenged due their mobile wireless environment and are therefore prone to service failures. They are the target of several mechanisms whose objective is to enhance the survivability. In this paper, we apply the framework to simulation-based studies of MANETs to evaluate their resilience in the presence of various challenges to normal operations.

The rest of the paper is organised as follows: Section II discusses related work followed by an overview of our approach in Section III. The mathematical formulation of the metrics state space in presented in Section IV. Section VI describes the MANET simulation setup. The resilience of MANET at three boundaries: topology–routing, routing–transport, and transport–application is presented in Section VII, Section VIII, and Section IX respectively. Lastly, the conclusions of the paper are in Section X.

II. Related Work

Traditionally, both resilience mechanisms and measures have been domain specific as well as challenge specific. For example, existing research on fault tolerance measures

[1]Please refer to [1] for formal definitions and relationship between resilience and survivability, dependability, and performability omitted here due to space constraints.

978-1-61284-125-0/11/$26.00 ©2011 IEEE

such as reliability and availability targets single instances of random faults, such as topology based survivability analysis, considering node and link failures [6], [7]. More recently, generic survivability frameworks consider network dynamics in addition to infrastructure failures [8]–[11]. Survivability can be quantified based on availability and network performance models [12], [13] using the T1A1.2 working group definition of survivability [4], [14]. Resilience can be quantified as the transient performance and availability measure of the network when subjected to challenges outside of the design envelope [15]. Service oriented network measures include *user lost erlangs* (measuring the traffic capacity lost during an outage) and *unservability* [16], [17]. Based on the common distinction in the industry between equipment vendor, service provider, and end user, specific metrics have been developed for each domain. In the field of network security, the common approach is to perform a vulnerability analysis [18]–[20] in order to determine how a network responds to security risks. Resilience evaluation is more difficult than evaluating networks in terms of traditional security metrics, due to the need to evaluate the ability of the network to continue providing an acceptable level of service, while withstanding challenges [19], [21]. In this paper, we quantify network resilience as a measure of service degradation in the presence of challenges (perturbations) to the operational state of the network.

III. Overview

In this section, we present a overview of our approach to quantify resilience at the application layer introduced in [21] and further described in [22]. A more detailed analysis of resilience at multiple layers will be presented in Section V. Our approach is a three step process. First, we represent the operational condition of the network using metrics derived from the fundamental characteristics of the network. These are termed as *operational metrics* since they define the operational state of network parameters such as link utilization. Secondly, the level of service being provided by the network is quantified using representative functions based on application requirements such as goodput and delay; these are termed as *service parameters*. Hence, the network can be viewed (at any layer) as consisting of two orthogonal dimensions as shown in Figure 1: one is the operational state of the network, which consists of its physical infrastructure and their protocols; the second dimension is the service being provided by the network and its requirements.

The full representation of the network state thus requires a knowledge of both the operational metrics and service parameters at any given instant of time. Therefore, the third step involves aggregating operational metrics and their corresponding service parameters into discrete states that we call *network state* represented by the circles in Figure 1. Due to the time-varying nature of these metrics, especially in dynamic networks, a continuous representation gets increasingly complex with the number of such metrics. Hence, we choose a discrete representation that scales well with the number of metrics and service parameters.

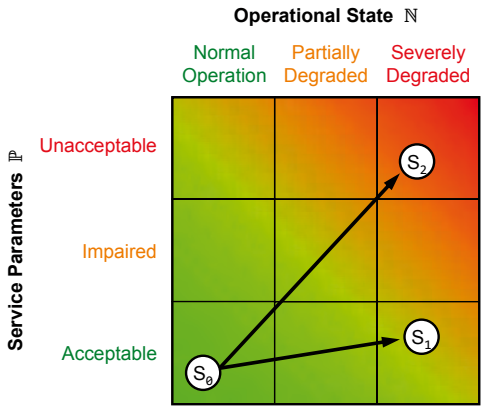

Fig. 1. Resilience state space

In order to quantify the resilience of the system, we formulate that challenges in the form of adverse events transform 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 a given network infrastructure (e.g. technology and topology) and their transitions under the presence of challenges. Evaluating network resilience in this way effectively quantifies it as a measure of service degradation in the presence of challenges (perturbations) to the operational state of the network. Therefore, a comprehensive view of resilience requires the knowledge of quantitative performance of the network in all the states that it may visit under normal or adverse conditions.

In order to provide a second level of granularity, the operational and service space of the network may be divided into three regions each as shown in Figure 1. This purpose of this set of coarse grained regions in which the states reside is to simplify the resilience analysis. The network operational space is divided into *normal*, *partially degraded*, and *severely degraded* regions. Similarly, the service space is divided into *acceptable*, *impaired*, and *unacceptable* regions. While an arbitrary number of such regions is possible, one of the primary goals of this work is to achieve tractable yet useful solutions, and this set of nine (3×3) regions provides the necessary abstraction while limiting the number total regions. Each region may contain multiple states if the service demands such a fine granularity. In the limiting case, each region represents just one state.

When an adverse event degrades the operational state of the network, the level of service being provided degrades as well resulting in *state transitions*. For example, Figure 1 shows the sample trajectory $S_0 \rightarrow S_1$ that an arbitrary application may take through the network if a malicious attack were to occur. Resilience is then evaluated as the transition of the network through this state space, measured as the area under the curve obtained by plotting operational metrics versus service parameters on a multivariate piecewise axis. For example, when comparing two services over a given network, the service with a smaller slope $(S_0 \rightarrow S_1)$ is considered more resilient than one with a steeper slope as $(S_0 \rightarrow S_2)$.

IV. METRICS STATE SPACE

In this sections, we present the formulation of operational and service state spaces as well as overall network state (a refinement of [21]). Then, we discuss the impact of challenges on network states in terms of state transitions.

A. Operational State Space

Operational metrics capture the operational state of the network at any arbitrary service boundary. Let the system $\mathcal{S}$ (network at an arbitrary level) be represented by ℓ operational metrics, $N_{\mathcal{S}} = \{N_1, \ldots, N_\ell\}$. Each operational metric $N_i, 1 \leq i \leq \ell$, is in itself a set of m values, representing all possible settings of the particular operational metric, $N_i = \{n_{i,1}, \ldots, n_{i,m}\}$. For example, at the physical layer of an ISP network, the number of link failures and link capacities could be two operational metrics. The *operational state space* of $\mathcal{S}$ is $\mathcal{N}_{\mathcal{S}} = \times_i N_i$ where $\times$ represents the cross product operator. Therefore, the operational state space consists of all possible combinations of the operational metrics.

We now define an *operational state*, $\mathbb{N}$ as a subset of the complete state space $\mathcal{N}_{\mathcal{S}}$. Therefore, $\mathbb{N}$ is an operational state if $\mathbb{N} \subseteq \mathcal{N}_{\mathcal{S}}$. Let $\mathbb{N}_{\mathcal{S}}$ be a set of operational states, $\mathbb{N}_{\mathcal{S}} = \{\mathbb{N}_1, \ldots, \mathbb{N}_k\}$. $\mathbb{N}_{\mathcal{S}}$ is valid if $\mathbb{N}_{\mathcal{S}}$ is a partition of $\mathcal{N}_{\mathcal{S}}$. That is $\mathbb{N}_i \cap \mathbb{N}_j = \varnothing, \mathbb{N}_i, \mathbb{N}_j \in \mathbb{N}_{\mathcal{S}}$ and $i \neq j$ and $\cup_i \mathbb{N}_i = \mathbb{N}_{\mathcal{S}}$ where $\cup$ represents the union operator. Hence, in the generic case, an operational state is defined as a subset of $\mathcal{N}_{\mathcal{S}}$.

Special Case : If N_i is numeric, ordered, and continuous then it is a set of all real values bounded by $[\underline{n}_i, \overline{n}_i]$, where $\underline{n}_i$ and $\overline{n}_i$ represent the lower and upper limit of the i^{th} operational metric, respectively. Furthermore, the k^{th} operational state $\mathbb{N}_k$ can be defined using the same notation used to define the complete state space instead of specifying it as a subset of $N_{\mathcal{S}}$. Therefore, $\mathbb{N}_k = \{N_{1k}, \ldots, N_{ik}, \ldots, N_{\ell k}\}$. 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 $N_{ik} \equiv \{\underline{n}_{ik}, \ldots, \overline{n}_{ik}\}$. Thus N_{ik} represents the set of i^{th} operational metric values that correspond to the operational state $\mathbb{N}_k$. However, note that irrespective of the way in which the individual states are defined, an operational state $\mathbb{N}_k$ is always a partition of the state space $\mathcal{N}_{\mathcal{S}}$.

The network properties that are used in deriving operational metrics depend upon the type of network and the specific layer at which resilience is being categorized. Later in this paper we will present an example of how operational metrics are obtained for a mobile wireless ad hoc network.

B. Service State Space

We now present the service state space which is orthogonal to the operational state space. The service parameters capture the requirement of the service that is being provided across the service interface. For example, the service from the transport layer to the application layer can be quantified using end-to-end delay in case of a voice application (in which latency affects the quality of service of the voice chat). Let the the system $\mathcal{S}$ (network at an arbitrary level) be represented by ℓ service parameters, $P_{\mathcal{S}} = \{P_1, \ldots, P_\ell\}$. Each service parameter $P_i, 1 \leq i \leq \ell$, is in itself a set of m values (representing all possible values of the particular service parameter), $P_i = \{p_{i,1}, \ldots, p_{i,m}\}$. For example, service parameters metrics such as largest connected component and clustering coefficient may be used to characterize the topology service. The *service state space* of $\mathcal{S}$ is $\mathcal{P}_{\mathcal{S}} = \times_i P_i$. Therefore, the service state space consists of all possible combinations of the service parameters.

We now define a *service state*, $\mathbb{P}$, as a subset of the complete state space $\mathcal{P}_{\mathcal{S}}$. Therefore, $\mathbb{P}$ is a service state if $\mathbb{P} \subseteq \mathcal{P}_{\mathcal{S}}$. Let $\mathbb{P}_{\mathcal{S}}$ be a set of service states, $\mathbb{P}_{\mathcal{S}} = \{\mathbb{P}_1, \ldots, \mathbb{P}_k\}$. $\mathbb{P}_{\mathcal{S}}$ is valid if $\mathbb{P}_{\mathcal{S}}$ is a partition of $\mathcal{P}_{\mathcal{S}}$. That is, $\mathbb{P}_i \cap \mathbb{P}_j = \varnothing, \mathbb{P}_i, \mathbb{P}_j \in \mathbb{P}_{\mathcal{S}}$ and $i \neq j$ and $\cup_i \mathbb{P}_i = \mathbb{P}_{\mathcal{S}}$. In a generic case, service states are specified as partitions of the complete service state space.

Special Case : If P_i is numeric, ordered, and continuous then it is a set of all real values bounded by $[\underline{p}_i, \overline{p}_i]$, where $\underline{p}_i$ and $\overline{p}_i$ represent the lower and upper limit of the i^{th} service parameter, respectively. Furthermore, the k^{th} service state can be represented as $\mathbb{P}_k = \{P_{1k}, \ldots, P_{ik}, \ldots, P_{\ell k}\}$. A member P_{ik} in the set $\mathbb{P}_k$ is in itself a set of values bounded by $[\underline{p}_{ik}, \overline{p}_{ik}]$, representing the lower and upper limit of the i^{th} service metric. We can define $P_{ik} \equiv \left\{\underline{p}_{ik}, \ldots, \overline{p}_{ik}\right\}$. Thus, P_{ik} represents the set i^{th} service parameter values that correspond to the service state $\mathbb{P}_k$.

The service parameters invariably depend upon the service and application being supported. Hence the resilience of the network must be evaluated in terms of the particular service metric that is critical for the application. Given this framework, it is also possible for new and emerging application to define new metrics.

C. Network State

As discussed earlier, in order to characterize a network at a service boundary we need to define both operational state and service state of the network. Hence, we define the overall *state* $S_{\mathcal{S}}$ of the system $\mathcal{S}$, (also termed as *network state*) as a tuple of operational state and service state: $(\mathbb{N}, \mathbb{P})$. Therefore the k^{th} network state $S_k = (\mathbb{N}_k, \mathbb{P}_k)$

This overall state of the system $S_{\mathcal{S}}$ represents a mapping between the operational state space $\mathcal{N}_{\mathcal{S}}$ and service state space $\mathcal{P}_{\mathcal{S}}$. Furthermore, this mapping is an onto mapping, meaning that for every service state there is an operational state. There are no service states without a corresponding operational state. In other words, all service states are derived from the system.

In a deterministic system, the mapping of $\mathcal{N}_{\mathcal{S}}$ to $\mathcal{P}_{\mathcal{S}}$ is functional, meaning that for each operational state there is one and only one service state. However, if the system is stochastic then this mapping is also stochastic in which one operational state maps to multiple service states based on the randomness in the execution of the system. In order to eliminate the stochastic nature of the $\mathcal{N}_{\mathcal{S}}$ to $\mathcal{P}_{\mathcal{S}}$ mapping, in our analysis, we present the $\mathbb{N}_{\mathcal{S}}$ to $\mathbb{P}_{\mathcal{S}}$ mapping, thereby focussing on the mapping of *aggregates* rather than individual operational or service states. In other words, instead of looking at the mapping of a instantaneous value of transmit range

(operational metric) to the largest component size (service parameter), we focus on the mapping of normal operating range of the transmit range (operational state) to acceptable region of the largest connected component size (service state).

D. Projected State Space

The operational state space $\mathcal{N}_S$ and the service state space $\mathcal{P}_S$ are both multivariate. Each element of the operational state space is a set with ℓ elements. Similarly, each element of the service state space is also a set with ℓ elements. In order to visualize this state space on a two dimensional state space, we project both the operational state space and service state space on to one dimension. This projection is achieved via an objective function that is applied in the both the state spaces. This is only possible if all operational metrics N_i and service parameters P_i are numeric and ordered.

Let $\mathcal{N}_S^*$ be the projected operational state space of the original state space $\mathcal{N}_S$. This is achieved via an objective function f such that ${\mathcal{N}_S}^* = f(\times_i N_i)$. Meaning that for each set in the $\mathcal{N}_S$, we apply a objective function on its ℓ member elements. This objective function may be a linear combination with normalized weights or logical functions (e.g. AND, OR).

Similarly let ${\mathcal{P}_S}^*$ be the projected service state space of the original service state space $\mathcal{P}_S$. This is achieved via an objective function f such that ${\mathcal{P}_S}^* = f(\times_i P_i)$. Therefore, for each set in the $\mathcal{P}_S$, we apply a objective function on its ℓ member elements. This objective function could be a linear combination with normalized weights or logical functions.

In the case of numeric, ordered, and continuous operational metrics and service parameters, the individual operational $\mathbb{N}_i$ and service $\mathbb{P}_i$ states with the range of their respective members. When these are projected over two dimension, we represent them as $\mathbb{N}_i^* = f(\mathbb{N}_i)$ and $\mathbb{P}_i^* = f(\mathbb{P}_i)$. When states are defined over the projected operational and service states, we can represent these states on a piece-wise linear axis.

E. State Transitions

There are two types of network transitions: sub-state transitions and state transitions. The stimuli that triggers these transitions include normal operational conditions such as traffic dynamics as well as various challenges and attacks. The sub-state transitions reflect the instantaneous changes (of lesser magnitude) in the operational metrics with time due to dynamic nature of the network and traffic.

Sub-state transitions aside, as long as the operational metrics and service parameters do not violate the state boundaries, the network remains in its current state and only sub-state transitions are possible. However, events of large magnitude (often due to an external challenge or attack) result in state transitions. The range of operational metrics and service parameters for a given state is determined by the specific scenario. For example, a voice application may require two states based on the service metric – end-to-end delay: one state in which the delay is less than 200 msec and the other state for delays greater than 200 msec. On the other hand, data applications may require more states to differentiate the service requirements of HTTP, P2P, and FTP traffic. Lastly, states are not be confused with regions which are coarse grained divisions of the state-space that allows a second layer of granularity in the analysis. In summary, the entire state-space is divided in to regions, each region may contain one or more states and a state is composed of infinitely large instantaneous sub-states. Since the sub-state transitions do not impact the resilience evaluations directly. Hence in the remainder of this paper we focus only on state transitions across different regions.

V. Multilevel Resilience Evaluation

In this section, we discuss the multilevel aspect of the metrics framework. Furthermore, we use a mobile ad hoc network (MANET) example to demonstrate how resilience propagates across layer boundaries.

In order to optimize resilience, it should be addressed at all levels, in the sense that each layer does the best it can, given practical constraints. These constraints are often based on the cost of resilience. *Therefore, resilience must be analyzed at each layer individually as well as for the network as a whole*. For this purpose, the metrics framework supports multilevel resilience evaluation. Formally, resilience $\mathbb{R}_{ij}$ is defined at the boundary B_{ij} between any two adjacent layers L_i, L_j. Based on the formulation of Section IV, let there be a set of k *operational metrics* $\mathbb{N} = \{N_1, N_2, \ldots, N_k\}$ that characterize the state of the network below the boundary B_{ij}. Similarly, let there be a set of l *service parameters* $\mathbb{P} = \{P_1, P_2, \ldots, P_l\}$ that characterize the service from layer i to layer j. Resilience $\mathbb{R}_{ij}$ at the boundary B_{ij} is then evaluated as the transition of the network through this state space. The goal is to derive the $\mathbb{R}_{ij}$ as a function of $\mathbb{N}$ and $\mathbb{P}$. In the simplest case $\mathbb{R}_{ij}$ is the area under the curve obtained by plotting $\mathbb{P}$ vs. $\mathbb{N}$ on a multivariate piecewise axis.

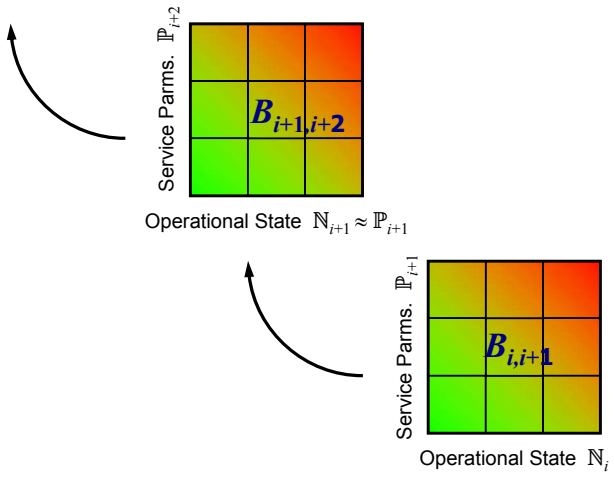

Fig. 2. Resilience across multiple levels

In the multilevel analysis, as shown in Figure 2, the service parameters at the boundary B_{ij} become the operation metrics at boundary $B_{i+1,j+1}$. In other words, the service provided by

a given layer becomes the operational state of the layer above, which has a new set of service parameters characterizing its service to the layer above.

VI. Simulation Setup

We used the ns-3 simulator [23] for conducting the simulations presented in this paper. While considering all the factors that affect the simulations, we choose parameters such that they cover a wide operational range from normal to severely degraded operations in order to evaluate the resilience of different layers in the presence of challenges. The simulation setup consists of 25 nodes in a 1000 $\times$ 1000 meter region. The random waypoint mobility model with zero pause times was used. The wireless simulation uses the 802.11 PHY module in infrastructure mode; the physical channel uses Friis propagation model. The simulation parameters that are varied over the course of the simulation runs include node speed, transmission power (and hence range), and the network load. A detailed list of simulation parameters is given in Table I. All simulations are averaged over 10 runs and 95% confidence intervals are shown as appropriate.

TABLE I
Simulation Parameters

Parameter	Category	Value
number of nodes	fixed	25
simulation region	fixed	1000 $\times$ 1000 metes
transmit range	variable	100 – 800 meters
node speed	variable	5, 10, 20 , 50, 100
propagation mode	fixed	Friis propagation
PHY	fixed	YANS wifi Phy
MAC	fixed	802.11 b
routing protocol	variable	DSDV, OLSR
transport protocol	fixed	UDP
data rate	variable	0.25, 0.5, 1, 2, 4, 8, 16 Kbps
packet size	fixed	1000 Bytes
application	fixed	CBR
traffic model	fixed	$n(n-1)$ flows = 600 flows

Figure 3 shows the metrics in the multilevel resilience analysis of a MANET. Next, we evaluate the resilience of the network at various level boundaries.

VII. Resilience at Topology – Routing

At this boundary $B_{3t,3r}$ (Figure 3), we evaluate the resilience of the the MANET topology under the presence of challenges to its normal operations. The operational metrics to represent the operational state of the network at this layer are node speed and the transmission range. Secondly, the service parameters that are relevant at this boundary are the relative size of the largest connected component and the average link duration.

A. Variation in parameters

First, we show the variation of the first operational metric using standard two dimensional plots. Figure 4 shows the variation of the average link durations with transmit range and speed. The plot shows that the average link duration is significantly affected by both the parameters and varies over a wide range. Since the ability of the routing protocol to find

Level	Layer Boundary	Operational Metrics	Service Parameters	Protocol or Mechanism
User				
Application (7)	$B_{7,user}$	data transfer (throughput, end-to-end delay)	*performance* (goodput, completed flows)	application (HTTP, FTP, CBR)
Transport (4)	$B_{4,7}$	path metrics (reachable pairs, latency, pathFER)	*data transfer* (throughput, end-to-end delay)	transport protocol (TCP, UDP)
Path Routing (3r)	$B_{3r,4}$	topology metrics (partitions, link lifetime, link cost)	*paths* (reachable pairs, latency, pathFER)	routing protocol (OLSR, DSDV)
Topology (3t)	$B_{3t,3r}$	link metrics, mobility (speed)	*topology* (partitions, link lifetime, link cost)	policy,topology discovery
Link+MAC (2)	$B_{2,3t}$	channel metrics, node density, flow rate	*links* (capacity, FER)	MAC protocol (802.11)
Physical (1)	$B_{1,2}$	radio, tx-power, distance, propagation loss	*channel* (baud rate, BER, transmit range)	modulation, encoding

Fig. 3. Multilevel resilience evaluation of a MANET

paths depends on the churn in topology, this is a crucial metric to characterize the topology service.

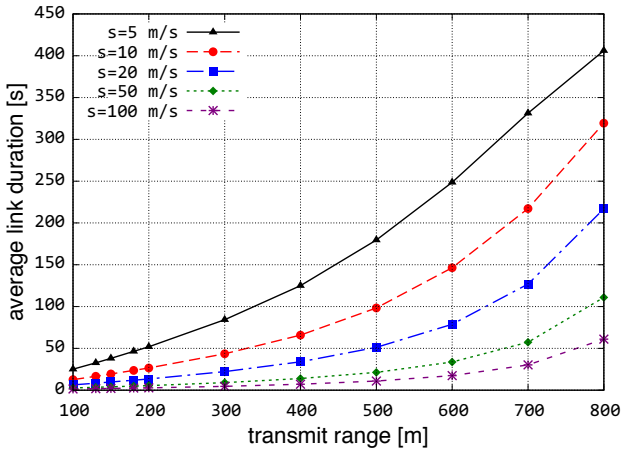

Fig. 4. Variation of link durations

Figure 5 shows the variation of the relative size of the largest connected component (LC size). As can be seen from the plot, the LC size depends primarily on the transmit range and does not vary much with node speed. This is because the connectivity of the network is heavily dominated by the transmit range especially at the higher end of the transmit range. The 95% confidence intervals showed high confidence in the averaged results.

B. State Space Computations

We now generate the state space representation (described in Section IV) at this boundary. For all values of the the operational metrics and service parameters, we need to calculate the corresponding projected values, N^* and P^* of the state space region. In order to get a single N^* or P^* value from a set of operational metrics and service parameters, we define

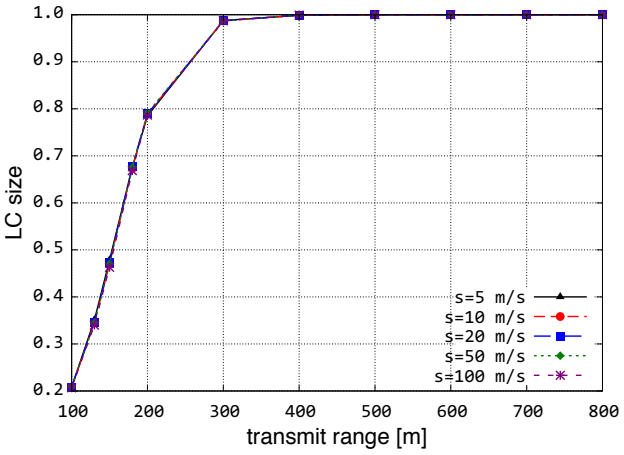

Fig. 5. Variation of LC size

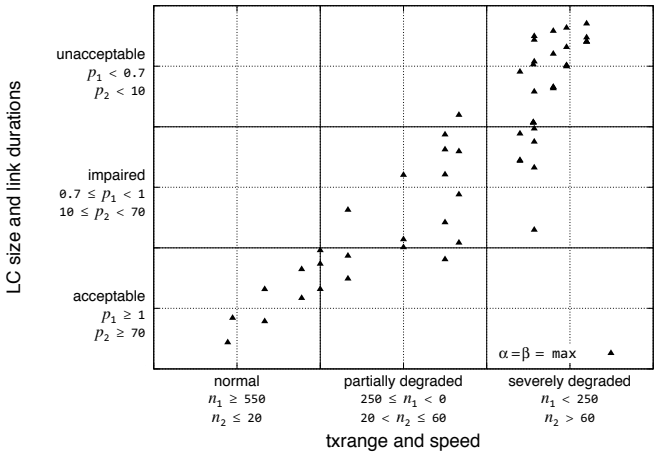

Fig. 6. Resilience state space at $B_{3t,3r}$ when α =max and β =max

an objective function. The methodology used to perform these calculations is as follows:

When operational state and service space is represented by more than one non-independent metrics, we need to apply an objective function to obtain the operational metrics and service parameters. Lets say there are two operational state of the network $N_{\mathcal{S}}$ be represented by two metrics $N_{\mathcal{S}} = \{N_1, N_2\}$. In order to project these metrics on to a two dimensional state space, we calculate the projected state $N^*_{\mathcal{S}} = f(N_1, N_2)$ Secondly, we define the boundaries for the normal, partially degraded and severely degraded regions. When the regions are defined this way, they are simply three states $\mathbb{N}_1, \mathbb{N}_2, \mathbb{N}_3$ with their respective ranges in the projected space $N^*_{\mathcal{S}}$.

In order to calculate the x-axis value (say, n^*) for pair of instantaneous values of the operational metrics n_1, n_2, we calculate the n_1^* corresponding to n_1 and n_2^* corresponding to n_2 on a piecewise linear scale. So if n_1 lies in the range of the range of the i_{th} regions, then $n_1^* = \frac{n_1}{\overline{n}_{1i} - \underline{n}_{1i}}$. Once we calculate n_1^* and n_2^* independently, we apply an objective function such that $n^* = \alpha n_1^* + (1-\alpha) n_2^*$. The value of α is determined by the service specification from the layer above. Furthermore, the framework also supports logical objective functions of AND and OR. These are treated as the special cases and the program written to compute states supports this mode via special flags. The same procedure is repeated for deriving the p^* value from a set of selected service parameters and the region boundaries. The objective function used is either logical (AND, OR) or a linear function: $p^* = \beta p_1^* + (1-\beta) p_2^*$

Figures 6 and 7 shows the state space transitions for varying values of α and β. In these figures, the keyword *max* is used to indicate the logical AND condition. These plots show that the MANET provides an acceptable topology as long as the operational metrics at the level, transmit range and node speed remain normal. However, as the operations degrade, the service degrades in a near linear fashion. The slope of this resilience curve depends on the objective function chosen. In the next section, we evaluate the impact of this objective function and if an upper and lower limit on the resilience can be found.

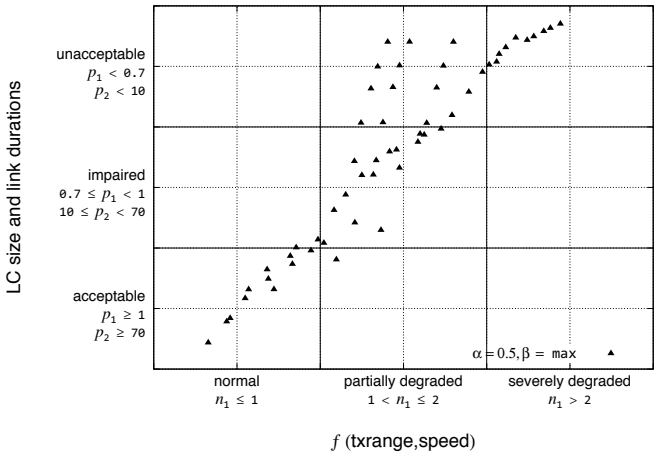

Fig. 7. Resilience state space at $B_{3t,3r}$ when $\alpha = 0.5$ and β =max

VIII. Resilience at Routing – Transport

Next, we move one level up from the topology-routing boundary $B_{3t,3r}$ to the routing-transport boundary $B_{3r,4}$ as illustrated in Figure 3. Here we evaluate the resilience of routing protocols (e.g. OLSR, DSDV). We define the service at this boundary as the ability to provide reachable paths to the transport layer in the presence of disruptions or perturbations to the underlying topology. Therefore, we characterize this service using one parameter: *path availability*, which is defined as percentage of time the network is able to find valid path between a pair of nodes, averaged over all node pairs. Therefore, $\mathbb{P} = \{P_1\} = \{\text{path reliability}\}$. Secondly, the operational metrics at this level are nothing but the service parameters from the layer below. Therefore, $\mathbb{N} = \{N_1, N_2\} = \{\text{LC size, link durations}\}$.

Based on the simulation states we compute the state transitions using the 3×3 regions modeled as three states each in the operational space and service space. We conducted simulations using two different routing protocols: OLSR and DSDV. Figure 8 shows the state space for the OLSR and

DSDV routing protocols when using $\alpha = \beta = \max$, meaning that logical AND is being used to derive x values from the two operational metrics. Comparing these two protocols, we see that OLSR is more resilient to perturbations in the normal operating conditions compared to DSDV. While the absolute location of points varies with different values of α, β as shown in Figure 9, in generally OLSR has a better resilience profile than DSDV.

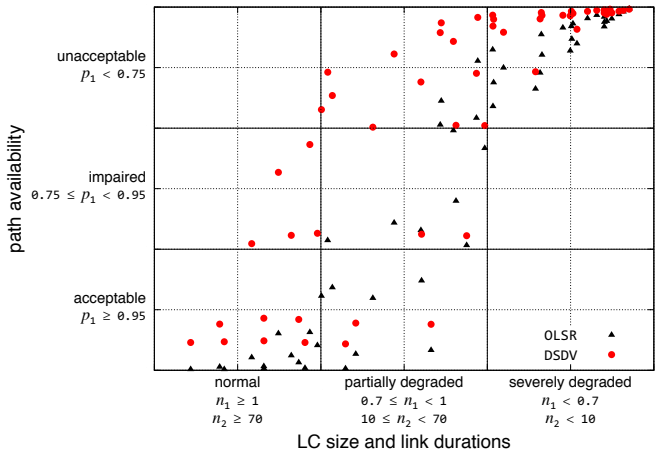

Fig. 8. Comparing the resilience of OLSR and DSDV with α =max

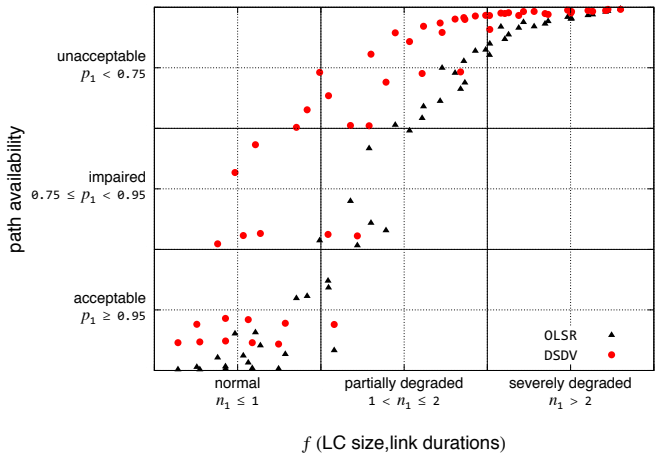

Fig. 9. Comparing the resilience of OLSR and DSDV with $\alpha = 0.35$

A. Impact of Objective Function Parameters

In order to determine the impact of the objective function in the analysis of the resilience, we explore the full range of α and β in this section. Figure 10 shows the state space plot when the value if α is varied from 0 to 1 in increments of 0.01 both for DSDV and OLSR. Note that since there is only one service metric, $\beta = 1$ for all runs.

From this plot, we observe that if we probe the entire space of the objective function, we get an *envelope of the resilience*. In other words, we get an empirical bound on the resilience for all values of α and β. Comparing DSDV and OLSR, we see that the envelope of the DSDV tends to lean more towards the impaired and unacceptable service region when compared to OLSR.

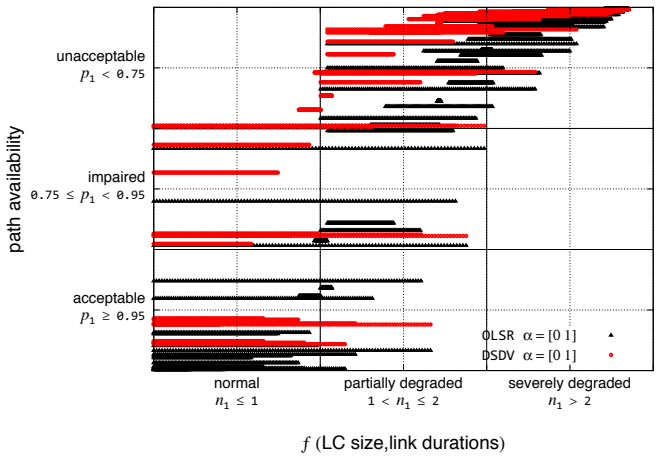

Fig. 10. Impact of α on routing state space

IX. Resilience at Transport – Application

Lastly, we evaluate the resilience of the MANET at the transport-application boundary $B_{4,7}$. At this boundary, we evaluate the resilience of the transport protocol under the presence of challenges. The service provided by the transport protocol to the application is end-to-end data transfer in the presence of perturbation in the paths provided by the underlying transport layer. The service parameters at this level are the packet delivery ratio (PDR) and end-to-end delay. Therefore, $\mathbb{P} = \{P_1, P_2\} = \{\text{PDR, delay}\}$. In addition to the the service parameters from the layer below, the operational metrics at this level include the relative traffic load that is dependent on the rate of the transport protocol. Relative load in this example is arbitrarily calculated as 1 for a sending rate of 0.54 Mb/s. Therefore, $\mathbb{N} = \{N_1, N_2\} = \{\text{path availability, relative load}\}$.

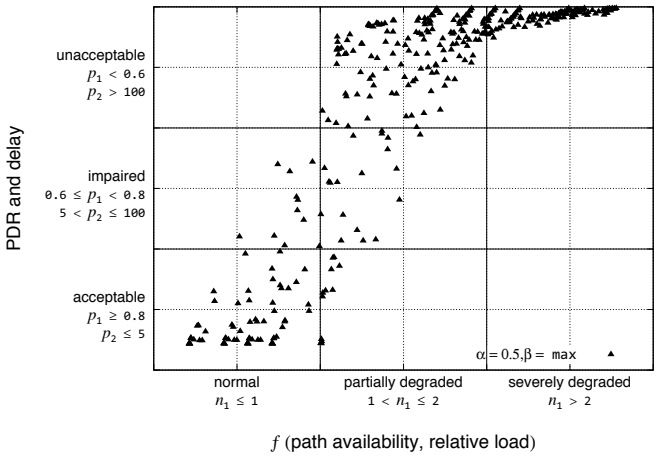

Fig. 11. Transport state space: UDP resilience, run 1

Using the state computation procedure detailed in Section VII-B, we plot the state transitions of the UDP protocol on a 3 × 3 region for two different data sets in Figure 11.

Looking at all the state instances, we clearly observe a specific pattern, an envelope that characterizes the resilience of the protocol. We observe that the service degrades almost linearly with respect to degradations in the operational state. Furthermore, the service sharply declines as the operations become severely degraded. In summary, we illustrated how the proposed resilience framework can be applied recursively at different resilience boundaries in the protocol stack in order to ascertain multi-level resilience. The assumption here is that if we are able to quantify the resilience at any arbitrary service boundary, we can then evaluate the impact of a potential enhancement (e.g. additional fiber paths to improve topology in a wireline broadband access network) at the respective level as well as evaluating the impact at the application boundary, which is often considered to be *overall resilience*.

X. Conclusion

This paper defines resilience at a given service boundary between two successive or arbitrary layers. We defined network state as an aggregation of the operational and service state. The resilience of the system is quantified as a function of state transitions in the network state-space. At any given boundary, the network is said to be resilient if it prevents degradation in the operational condition from leading to degradations in service. We presented a rigorous mathematical framework and a tractable methodology to easily evaluate resilience. To that end, we applied this metrics framework to MANETs in order to evaluate the resilience to challenges at various levels. We presented how state space computation can be performed with the help of an objective function. The impact of the parameters of the objective function was also explored. The resilience analysis was conducted for 4 successive levels or 3 level boundaries: topology $\rightarrow$ routing $\rightarrow$ transport $\rightarrow$ application. We quantified the resilience of the topology and compared the OLSR and DSDV in terms of their ability to survive perturbations in the topology. While this is a rigorous framework, it is an abstraction whose goal is to permit quantitative comparison of resilience without fully expressing all the instantaneous states of the system.

Acknowledgments

We would like to acknowledge Gary J. Minden, David Hutchison, Justin P. Rohrer, and Egemen K. Çetinkaya for their comments and discussion in support of this work. This research was partly supported by the National Science Foundation FIND Grant No. CNS-0626918 (Postmodern Internet Architecture) and European Commission under grant FP7-224619 (ResumeNet).

References

[1] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer Networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[2] J. P. 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.

[3] 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.

[4] T1A1.2 Working Group, "Enhanced network survivability performance," Alliance for Telecommunications Industry Solutions (ATIS), Technical Report T1.TR.68-2001, February 2001.

[5] P. Cholda, A. Mykkeltveit, B. Helvik, O. Wittner, and A. Jajszczyk, "A survey of resilience differentiation frameworks in communication networks," *IEEE Communications Surveys Tutorials*, vol. 9, no. 4, pp. 32–55, 2007.

[6] S. Liew and K. Lu, "A framework for network survivability characterization," in *SUPERCOMM/ICC'92: Proceedings of IEEE International Conference on Communications, 1992. ICC 92, Conference record, /, Discovering a New World of Communications.*, 1992, pp. 405–410.

[7] A. Antonopoulos, "Metrication and performance analysis on resilience of ring-based transport network solutions," in *GLOBECOM'99: Global Telecommunications Conference*, vol. 2, 1999, pp. 1551–1555.

[8] E. K. Çetinkaya, D. Broyles, A. Dandekar, S. Srinivasan, and J. P. Sterbenz, "A Comprehensive Framework to Simulate Network Attacks and Challenges," in *IEEE/IFIP 2nd International Workshop on Reliable Networks Design and Modeling (RNDM)*, Moscow, Oct. 2010, pp. 538–544.

[9] 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.

[10] Q. Gan and B. Helvik, "Dependability modelling and analysis of networks as taking routing and traffic into account," in *NGI '06: Proceedings of the Conference on Next Generation Internet Design and Engineering*, April 2006.

[11] W. Molisz, "Survivability function-a measure of disaster-based routing performance," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 9, pp. 1876–1883, 2004.

[12] P. E. Heegaard and K. S. Trivedi, "Network survivability modeling," *Computer Networks*, vol. 53, no. 8, pp. 1215–1234, 2009, performance Modeling of Computer Networks: Special Issue in Memory of Dr. Gunter Bolch.

[13] K. Trivedi, D. Kim, A. Roy, and D. Medhi, "Dependability and security models," in *Proceedings of the International Workshop of Design of Reliable Communication Networks (DRCN)*. IEEE, 2009, pp. 11–20.

[14] T1A1.2 Working Group, "Reliability-related metrics and terminology for network elements in evolving communications networks," Alliance for Telecommunications Industry Solutions (ATIS), American National Standard for Telecommunications T1.TR.524-2004, June 2004.

[15] K. Trivedi, D. Kim, and R. Ghosh, "Resilience in computer systems and networks," in *Proceedings of the 2009 International Conference on Computer-Aided Design (ICCAD)*. IEEE, 2009.

[16] A. Zolfaghari and F. J. Kaudel, "Framework for network survivability performance," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 12, no. 1, pp. 46–51, January 1994.

[17] W. D. Grover, *Mesh-Based Survivable Networks*. Upper Saddle River, New Jersey: Prentice Hall PTR Pearson, 2004.

[18] G. Qu, R. Jayaprakash, S. Hariri, and C. Raghavendra, "A framework for network vulnerability analysis," in *CT '02: Proceedings of the 1st IASTED International Conference on Communications, Internet, Information Technology*, St. Thomas, Virgin Islands, USA, Sep-Oct 2002, pp. 289–298.

[19] S. Hariri, G. Qu, T. Dharmagadda, M. Ramkishore, and C. S. Raghavendra, "Impact analysis of faults and attacks in large-scale networks," *IEEE Security and Privacy*, vol. 01, no. 5, pp. 49–54, 2003.

[20] D. M. Nicol, W. H. Sanders, and K. S. Trivedi, "Model-based evaluation: From dependability to security," *IEEE Transactions on Dependable and Secure Computing*, vol. 01, no. 1, pp. 48–65, 2004.

[21] A. J. Mohammad, D. Hutchison, and J. P. Sterbenz, "Towards quantifying metrics for resilient and survivable networks," in *Proceedings of the 14th IEEE International Conference on Network Protocols (ICNP)*, November 2006, pp. 17–18.

[22] J. P. Sterbenz, E. K. Çetinkaya, M. A. Hameed, A. Jabbar, and J. P. Rohrer, "Modelling and Analysis of Network Resilience (invited paper)," in *The Third IEEE International Conference on Communication Systems and Networks (COMSNETS)*, Bangalore, Jan. 2011, pp. 1–10.

[23] (2009, July) The ns-3 network simulator. http://www.nsnam.org.