

I. Introduction and Motivation

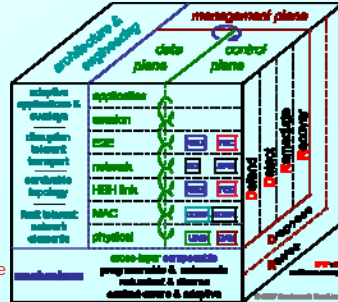
Objective

- Develop a taxonomy to characterize networks using operational metrics and service parameters
- Quantify network resilience towards a number of challenges and attacks using two-dimensional state space analysis
- Understand how to design and engineer networks with a higher resilience

Resilient Network

Ability to operate and maintain an acceptable level of service under the presence of adverse conditions such as:

- natural faults and misconfiguration of network components
- failures due to operational errors
- large-scale natural disasters
- attacks against hardware, software, protocol infrastructure
- unpredictably-long-delay paths
- weak, asymmetric, episodic connectivity of wireless channels
- high-mobility of nodes and sub-networks
- unusual but legitimate traffic load (e.g. flash crowds)



Multilevel Resilience

- Optimal operation at every layer and in all planes
- Bottom-up with cross-layer knobs and dials
- Inside-out from individual components to entire network
- D²R² + DR strategy: defend, detect, remediate, recover, diagnose, refine

Research Problem

- Resilience and survivability important for all networks including challenged networks
- Lack of rigorous and efficient representation methods using standard metrics
- Use operational metrics and service parameters to represent network states
- Evaluate the resilience of the network as it moves through various states

II. Network Characterization

Network Characterization

- Define challenged networks using fundamental properties formulated in concise metrics
- Enables clear representation of different types of networks
- Facilitates network transformation from one state to another
- Cannot guarantee unique representation of all the possible network scenarios
- Need a solution that can capture the inherent complexity, yet be tractable for efficient use

Approach

- Characterization based on specific applications and scenarios cannot represent networks in general way
- Network characterization should be based on the factors that are fundamental to every network
 - physical characteristics of the network
 - traffic to be serviced by the network
 - service/performance expected out of the network
- Application and scenario independent
- Identify comprehensive set of properties
 - represent the dynamic network structure and traffic
- Ongoing research is focused on deriving a small set of metrics
 - independent of one another
 - sufficient for understanding and engineering
 - simple enough for tractability

- Network state is defined by
 - physical metrics
 - data traffic
 - expected service

Density	number of nodes, area of spread, distribution pattern, rate of topology change
Mobility	node velocity, mobility model, predictability
Channel	capacity distribution, propagation model, bit error rate, error model
Node Resources	electrical power, computing power, memory, transmit/receive power, location awareness
Network Traffic	rate, delay, jitter, distribution, packet size, source/sink placement
Derived Properties	degree of connectivity, propagation delay, queuing delay, node willingness

III. Mathematical Formulation

Operational Metrics

- Function of one or more network properties that efficiently represents physical characteristics
- Characteristics of the k^{th} state are represented as $\mathbf{N}_k = \{N_{1k}, N_{2k}, \dots, N_{ik}, \dots, N_{sk}\}$.
- The i^{th} operational metric N_{ik} is bounded by the limits $[l_{ik}, \bar{n}_{ik}]$
- Network boundaries of N_{ik} for each state are determined by the desired performance of the state

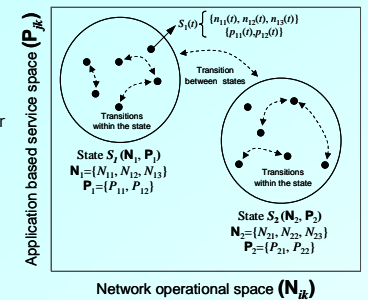
Service Parameters

- Quantifies the acceptable level of service of a network using representative functions
- Based on application requirements
- Service of the network in k^{th} state is represented as $\mathbf{P}_k = \{P_{1k}, P_{2k}, \dots, P_{jk}, \dots, P_{sk}\}$
- The j^{th} service parameter P_{jk} is a set of values bounded by $[l_{jk}, \bar{p}_{jk}]$

Network State

- A network state S_k is defined by the tuple $(\mathbf{N}_k, \mathbf{P}_k)$
- Network transitions with in a state and between states
- External or internal stimulus drives the network from one state to another
- For a given application under the given suite of protocols

- i^{th} operational metric at an instant t is $n_i(t)$
- j^{th} service parameter is $p_j(t)$,
- network is said to be in a state S_k iff:
 1. $\forall \{i : N_{ik} \in \mathbf{N}_k\}, n_i(t) \in N_{ik}$ and
 2. $\forall \{j : P_{jk} \in \mathbf{P}_k\}, p_j(t) \in P_{jk}$



IV. Network Resilience

Resilience State Space

- Network operational space is divided in three regions
 - normal, partially degraded, severely degraded
- Application service space is also divided in three regions
 - acceptable, impaired, unacceptable
- Stimuli that cause state transitions are various adverse conditions
- May be more than one state in each region

State Transitions: Following the occurrence of an adverse event

1. Remains in the same state or moves to another state in the same region
 - operational metrics and service parameters remain in the limits
 - adverse events of smaller magnitude
 - network defense prevents active faults or service failures
 - network is engineered such that multiple states fall in the same region
2. Moves to a state in a different (inferior) region
 - operational metrics and service parameters exceed their limits
 - adverse events of higher magnitudes
 - challenges cause active faults leading to service failures
3. Moves to state in a different (superior) region
 - network remediation compensates for service failures
 - network recovery corrects the fault that led to service degradation

Resilience Measure

- Ability to remain in the acceptable region in the presence of challenges and attacks
- Graceful degradation, quick remediation, restoration of the state

