Network Survivability Modeling and Quantification

Prof. Poul E. Heegaard, 
poul.heegaard@item.ntnu.no 
Department of Telematics 
Norwegian University of Science and Technology (NTNU)

Prof. Kishor S. Trivedi 
kst@ee.duke.edu 
Elect. & Comp. Eng. Dept., 
Pratt School of Engineering 
Duke University
NTNU, Trondheim, Norway (A), Duke University, Durham, NC (B)
Kishor S. Trivedi  
Pratt School of Engineering, Duke University

Kishor S. Trivedi holds the Hudson Chair in the Department of Electrical and Computer Engineering at Duke University, Durham, NC. He has been on the Duke faculty since 1975. He is the author of a well known text entitled, Probability and Statistics with Reliability, Queuing and Computer Science Applications, published by Prentice-Hall; a thoroughly revised second edition (including its Indian edition) of this book has been published by John Wiley. He has also published two other books entitled, Performance and Reliability Analysis of Computer Systems, published by Kluwer Academic Publishers and Queueing Networks and Markov Chains, John Wiley. He is a Fellow of the Institute of Electrical and Electronics Engineers. He is a Golden Core Member of IEEE Computer Society. He has published over 420 articles and has supervised 42 Ph.D. dissertations. He is the recipient of IEEE Computer Society Technical Achievement Award for his research on Software Aging and Rejuvenation. His research interests are in reliability, availability, performance, performability, security and survivability evaluation of computer and communication systems. He works closely with industry in carrying out reliability/availability analysis, providing short courses on reliability, availability, performability modeling and in the development and dissemination of software packages such as SHARPE and SPNP.
Poul E. Heegaard, Norwegian University of Science and Technology

Poul E. Heegaard is Associate Professor and Head of Department at Department of Telematics, Norwegian University of Science and Technology (NTNU). Heegaard has since 2006 been on the faculty at NTNU. From 1999 - 2009 he was a Senior Research Scientist at Telenor R&I. He has previously been a Research Scientist and Senior Scientist at SINTEF Telecom and Informatics (1989-1999). His research interests cover performance, dependability and survivability evaluation and management of communication systems. Special interest is in rare event simulation techniques, and monitoring, routing and management in dynamic networks. He has developed a Java-based traffic generator called GenSyn. His current research focus is on distributed, autonomous and adaptive management and routing in communication networks and services. Heegaard has been active in several EU-IST collaborations.

Heegaard is the author/co-author of a number of research papers, reports and lecture notes. He has given numerous talks in national and international meetings and conferences. He serves in various international organization committees such as General Chair for RESIM 2012, and program committees, such as Dependable Systems and Networks (DSN) 2011. He is frequently an expert reviewer for different journals and PhD committees.
Summary of tutorial

Critical services in a telecommunication network should be continuously provided even when undesirable events like sabotage, natural disasters, or network failures happen. It is essential to provide virtual connections between peering nodes with certain performance guarantees such as minimum throughput, maximum delay or loss. The design, construction and management of virtual connections, network infrastructures and service platforms aim at meeting such requirements.

In this tutorial we consider the network's ability to survive major and minor failures in network infrastructure and service platforms that are caused by undesired events that might be external or internal. Survive means that the services provided comply with the requirement also in presence of failures. The network survivability is quantified as defined by the ANSI T1A1.2 committee -- that is, the transient performance from the instant an undesirable event occurs until steady state with an acceptable performance level is attained.

The goal of this tutorial is to provide an introduction to the concept and definition of survivability and to demonstrate approaches to model and quantify the survivability in networks. Examples are taken from the survivability of virtual connection over an IP network.
Tutorial outline

I. Survivability concepts and definition
II. Network survivability modeling and quantification
III. Case studies
What needs to be survivable?

Critical national infrastructure

- Banking
- Power grid
- Water supply
- Transportation
- Gas/oil storage/dist.
- Government service
- Telecommunications
- Nuclear Plants

Computer/communication networks

Computer/communication systems
Why survivability?

- Society heavily depends on telecommunication services
- Critical services must be available even under
  - Technical network failures
  - Malicious attack
  - Accidents and natural disasters
- Security, dependability, survivability, availability, reliability...
  - All concerned with trusted services according its requirements
- Differ in their main focus on threats
  - Dependability: physical, design, and interactions
  - Security: recognition and resistance to attacks
  - Survivability: attack, accidents, and failures
I. Survivability concepts and definitions
Our View on Survivability, Performance, Dependability and Security

Security
- Authentication*
- Non-repudiation*

Dependability
- integrity
- confidentiality

Safety
- reliability

Availability
- Performance

Survivability

Performance + Availability/Reliability = Performability

*: qualitative
Dependability—An umbrella term

- Trustworthiness of a computer system such that reliance can justifiably be placed on the service it delivers
MEASURES TO BE EVALUATED

- Dependability
  - Reliability: $R(t)$, System MTTF
  - Availability: Steady-state, Transient, Interval
  - Downtime
  - Security, safety

“Does it work, and for how long?"

- Pure (Failure Free) Performance
  - Throughput, Blocking Probability, Response Time
    (mean, distribution)

“Given that it works, how well does it work?”
MEASURES TO BE EVALUATED

• Composite Performance and Dependability

“How much work will be done(lost) in a given interval including the effects of failure/repair/contention?”
Dependability Attributes or Measures

Dependability Measures

Reliability

Availability

• **Reliability**: “The ability of a system to perform a required function under given conditions for a given time interval.” No recovery is assumed after system fails (there can be recovery after a component failure)

• **Availability**: “The ability of a system to be in a state to perform a required function at a given instant of time or at any instant of time within a given time interval.”
IFIP WG10.4

• **Failure** occurs when the delivered service no longer complies with the desired output.
• **Error** is that part of the system state which is liable to lead to subsequent failure.
• **Fault** is adjudged or hypothesized cause of an error.

Faults are the cause of errors that may lead to failures
Extended Dependability and Security tree

Dependability and Security

- Threats
  - Faults/Attacks (Intrusions)
    - Errors
    - Failures
  - Availability
  - Confidentiality
  - Integrity
  - Reliability
  - Safety
  - Maintainability

- Attributes
  - Fault/Intrusion Prevention
  - Fault/Intrusion Detection
  - Fault/Intrusion Tolerance
  - Fault/Vulnerability Removal
  - Fault/Intrusion Forecasting

- Security

Fault/Intrusion Removal

Fault/Intrusion Forecasting
Survive What?

- Hardware/software faults
  - Programming bugs, hardware failure
- Man-made accidents
  - Cable cuts, operator errors
- Malicious cyber attacks
  - Denial of service, virus/spyware/rogueware
- Natural disasters
  - Fire, flood, earthquake, hurricane
- Terrorist attacks
Survivability Principles

- **Decentralization**
  - Provide service without reliance on a common reference node in the architecture

- **Redundancy**
  - Provide service by switching (failing) over workload of the affected node(s) or link(s) to standby (backup) node(s) or link(s)

- **Geographic Separation** (Diversity)
  - Placement of standby nodes or links outside of the expected radius of damage of related nodes or links
What Is Survivability?

- **Reliability**
  - Continuity of service, how long will the system work w/o system failure (component failures are allowed)
- **Availability**
  - Readiness of service, how frequently it fails and how quickly can it be repaired
- **Performability**
  - Performance in the presence of failure
- **Safety**
  - Avoiding catastrophic consequences (human life)
- **Confidentiality**
  - Preventing unauthorized disclosure
- **Integrity**
  - Preventing improper alteration
- **Survivability**
  - ?
Threats in Dependability, Security and Survivability

**Faults**
- Physical faults
  - Node faults
  - Power faults
  - Link faults
  - Bohrbugs
  - Mandelbugs
  - Aging-related bugs

**Software Bugs**
- Bohrbugs
- Mandelbugs
- Aging-related bugs

**Physical Attack**
- Node attack
- Infrastructure attack
- Exploitation of software vulnerability
- Spurious traffic (denial of service)
- Equipment behind enemy lines
- Change configuration data
- Link attack

**Software-based attacks**
- "Byzantine generals" main-in-the-middle

**Intrusions/Accidents/natural disasters**
- Node attack
- Infrastructure attack
- Exploitation of software vulnerability
- Spurious traffic (denial of service)
- Equipment behind enemy lines
- Change configuration data
- Link attack
Survivability, Security, and Fault Tolerance

- Survivability vs. Security
  - Security
    - Availability, confidentiality and integrity
    - Recognition of attacks, resistance to attacks
  - Survivability
    - Broader than security
    - Maintain essential service and recover under attacks and natural disasters

- Survivability vs. Fault Tolerance
  - Fault tolerance does not (normally) consider malicious attacks (Intrusion Tolerance does) and natural disasters
  - Geographic diversity in survivable systems needed to avoid vulnerabilities to massive attacks or disasters

Laprie’s View on Dependability and Survivability

<table>
<thead>
<tr>
<th>Concept</th>
<th>Dependability</th>
<th>Survivability</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Goal</strong></td>
<td>1) Ability to deliver service that can justifiably be trusted</td>
<td>Capability of a system to fulfill its mission in a timely manner</td>
</tr>
<tr>
<td></td>
<td>2) ability of a system to avoid failures that are more frequent or more severe, and outage durations that are longer, than is acceptable to the user(s)</td>
<td></td>
</tr>
<tr>
<td><strong>Threats present</strong></td>
<td>1) design faults (e.g., software flaws, hardware errata, malicious logics)</td>
<td>1) failures (internally generated events due to, e.g., software design errors, hardware degradation, human errors, corrupted data)</td>
</tr>
<tr>
<td></td>
<td>2) physical faults (e.g., production defects, physical deterioration)</td>
<td>2) attacks (e.g., intrusions, probes, denials of service)</td>
</tr>
<tr>
<td></td>
<td>3) interaction faults (e.g., physical interference, input mistakes, attacks, including viruses, worms, intrusions)</td>
<td>3) accidents (externally generated events such as natural disasters)</td>
</tr>
</tbody>
</table>

SEI’s View on Survivability, Security, and Fault Tolerance

- Survivability vs. Security
  - Security
    - Availability, confidentiality and integrity (non-repudiation and authentication)
    - Recognition of attacks, resistance to attacks
  - Survivability
    - Broader than security
    - Maintain essential service and recover under attacks and natural disasters
    - Adaptation and evolution to attacks

- Survivability vs. Fault Tolerance
  - Fault tolerance does not (normally) consider malicious attacks (Intrusion Tolerance does)
  - Geographic diversity in survivable systems needed to avoid vulnerabilities to massive attacks or disasters

Knight’s View on
Survivability, Dependability,
Security, and Fault Tolerance

• Survivability vs. security
  – In critical information systems security attacks are not a major cause of 
    service failures so far
  – Security faults can be included in survivability requirements as a 
    comprehensive approach

• Survivability vs. dependability
  – Survivability is a property of dependability (an attribute of dependability 
    in Laprie terminology)
  – Other properties (attributes a la Laprie) include reliability, availability, 
    safety, etc.

• Survivability vs. fault tolerance
  – Fault tolerance is a design mechanism (means a la Laprie) to achieve 
    certain dependability properties
  – Other mechanisms (means a la Laprie) include fault avoidance, fault 
    elimination, fault forecasting

Qualitative Definitions of Survivability

- National Communication System Technology & Standards [1]
  - The ability of a system, subsystem, equipment, process, or procedure to continue to function during and after a natural or man-made disturbance.

- Peter G. Neumann [2]
  - Survivability is the ability of a system to satisfy and to continue to satisfy critical requirements in the face of adverse conditions.

- CMU/SEI [3]
  - Survivability is the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.

- All of them point to the transient behavior of system after a failure, attack or a natural disaster.

**Survivability** is the system’s ability to continuously deliver services in compliance with the given requirements in the presence of failures and other undesired events.

---

Quantitative Definition of Survivability

• Quantitative Definition [8]. Suppose a measure of interest $M$ has the value $m_0$ just before a “failure” happens. The survivability behavior can be depicted by the following attributes:
  - $m_a$ is the value of $M$ immediately after the occurrence of failure,
  - $m_u$ is the maximum difference between the value of $M$ and $m_a$ after the failure,
  - $m_r$ is the restored value of $M$ after some time $t_r$, and
  - $t_R$ is the time for the system to restore the value $m_0$.

**Survivability quantification.** The measure of interest $M$ has the value $m_0$ just before a failure occurs. The survivability behavior can be depicted by the following attributes: $m_a$ is the value of $M$ just after the failure occurs; $m_u$ is the maximum difference between the value of $M$ and $m_a$ after the failure; $m_r$ is the restored value of $M$ after some time $t_r$; and $t_R$ is the relaxation time for the system to restore the value of $M$.

• This definition is proposed by the T1A1.2 network “Survivability performance working group”. By this definition, survivability depicts the time-varying performance (measure $M$) of the system after a failure, attack or a natural disaster occurs.

Quantitative Definition of Survivability

measure \( M \) has initial value \( m_0 \) just before a “failure”

\( m_a \) is the value of \( M \) immediately after the occurrence of failure,

\( m_u \) is the maximum difference between the value of \( M \) and \( m_a \)

\( m_r \) is the restored value of \( M \) after some time \( t_r \), and

\( t_R \) is the time for the system to restore the value \( m_0 \).
Qualitative Definitions of Survivability

- **Steady state**
  - Performance [Knight’s def.]
  - Availability [Liew’s def.]
- **Transient**
  - Performability [T1A1.2’s def.]
  - Transient performance
  - Transient availability
  - Transient performance conditioned on failure scenario [Def. in this paper]

From Yun Liu’s thesis
Survivability Research at Duke University and NTNU

• Analysis approach
  - Develop, parameterize, and solve Markov and non-Markov models including failure modes, traffic patterns, and resource contention.
  - T1A1.2 based survivability measures do NOT depend on the disaster rate; this may be considered good as the disaster rate is hard to quantify in practice
Survivability Research at Duke University and NTNU

- **Publications**
  - Survivability analysis of telephone access network Proc. of 15th IEEE International Symposium on Software Engineering (ISSRE’04)
II. Network survivability modeling and quantification
Network survivability quantification

- Service unavailability
- Maximum metric
- Upper metric acceptance level
- Steady state metric after failure
- Metric in fault-free operation

failure
repair
Implications of T1A1.2 Definition

- System is initially assumed to be in steady state (pure performance model) with all components functioning
- Force a failure in the system and study the transient behavior until it reaches the original steady state upon completion of repair
A General Quantification Procedure

• Step 1
  – Develop the pure availability model in which the resources (hardware and/or software) fail and get repaired (or rebooted).

• Step 2
  – Develop a pure performance model and obtain the steady state results of the pure performance model, which reflects the resource usage and other system state information before a failure happens. The performance model could have arrival and service of tasks reflected.

• Step 3
  – Combine the availability and performance models obtained in the first two steps into a composite model.

• Step 4
  – Choose a survivability measure of interest. Force a specific failure in the system and construct a truncated model. In order to reflect the system resource usage before the failure happens, initial probability must be appropriately assigned for the truncated model.

• Step 5
  – Perform the transient analysis of the truncated composite model.
An illustrative example 1: A telecom switching system

- Assumptions
  - A telecom switching system with \( n \) trunks
  - Call inter-arrival time \( \text{Exp}(\lambda) \)
  - Call holding time \( \text{Exp}(\mu) \)
  - Time to failure \( \text{Exp}(\gamma) \)
  - Time to repair \( \text{Exp}(\tau) \)
  - Single repair facility
Pure Availability Model

$n=25, \gamma=0.002 \text{ s}^{-1}, \tau=0.1 \text{ s}^{-1}$
Pure Performance Model

Steady state closed-form solution:
Erlang B Formula

Blocking probability:

\[ P_{bk} = \pi_n^p \]

\[ n=25, \lambda=5 \text{ s}^{-1}, \mu=0.3 \text{ s}^{-1} \]
Composite Performability Model

Q: What state(s) is (are) blocking state (s)?

Blocking states
Performance, Availability, and Performability Measure of Interest : $P_{bk}$

- **Performance**
  - From pure performance model
  - Steady state blocking probability $P_{bk}$
  - $P_{bk} = \pi_n^P = 0.013376$

- **Availability**
  - From pure availability model
  - $P_A = 1 - \pi_n^A = 1 - 2.6935 \times 10^{-18}$

- **Performability (PA type)**
  - From composite model
  - $P_{bk} = \sum_{k=0}^{n} \pi_{k,k}^C = 0.020178$
Survivability Quantification Approach

- System operating in steady state
- Force a failure:
  - Initial state probabilities for the degraded mode states
  - Transient solution of the truncated performability model
Truncated Performability Model

Steady state prob.

Initialization

Blocking states

(forced) Failure transitions

Force a failure

Truncated states
Survivability Results
Another Survivability Measure: Excess Loss Due to Failure (ELF)

ELF: a survivability measure reflecting the total loss before the system is completely recovered

\[ \text{ELF} = P_{bk}(t) + P_{bk}(t \rightarrow \infty) \]

\[ P_{bk}(t) \]

\[ P_{bk}(t \rightarrow \infty) \]

Dropped calls + Excess blocked calls = ELF
## ELF results

<table>
<thead>
<tr>
<th>Relaxation time*</th>
<th>Call loss due to the $1^{st}$ failure $N_d$</th>
<th>Extra call loss due to blocking $N_b$</th>
<th>ELF</th>
</tr>
</thead>
<tbody>
<tr>
<td>39s</td>
<td>0.6557</td>
<td>0.2457</td>
<td>0.9014</td>
</tr>
</tbody>
</table>

$$N_d = \frac{j}{n} \pi j^p.$$  
$$N_b = \int_0^{t_R} (P_{bk}(t) - P_{bk}(t \to \infty)) \lambda dt$$

*: based on a relative error of 0.1%, i.e., 100.1% of the original blocking prob. restored
Illustrative example 2: Network with 4 nodes

- Simulation model (Simula/DEMOS)
- Stochastic Reward Net (Generalized PetriNets) model
- CTMC model of each node
- Closed form solution
- Comparisons

\[
\frac{a}{b} \\
\begin{aligned}
   r_{ij}(I) &= r_{ij}(IV) = a \\
   r_{ij}(II) &= r_{ij}(III) = b \\
\end{aligned}
\]
Network with 4 nodes: Approaches

- Simulation
  - DEMOS/Simula
  - Discrete event, process-oriented simulation model
- Analytical
  - SRN: Stochastic Reward Networks
    - Full CTMC, same as simulation model
    - Solved by SPNP and SHARPE
  - CTMC: (Decomposed) Markov models
    - Combined performance and dependability model
    - Product-form approximation
    - Solved by SHARPE
Objective

- Performance in networks with virtual connections
- Transience from occurrence of an undesired event until steady state operation is restored
- Routing in acyclic, directed graph
- Directed from SRC->DST nodes
- Goal: Survivability model of performance after network failure(s)
Modeling approach

Performance model

Phased recovery model

Composite performability model

Survivability model
Network with 4 nodes: Simulation model
Network with 4 nodes: Stochastic Reward Net model

Identical assumptions as the simulation model

Complete CTMC model of network
Network with 4 nodes: CTMC Performance model

- Decomposed CTMC to reduce number of states
- Nodes modeled separately
- The arrival intensities change when node or link fails
- The resource utilization model below is solved for each set of intensities
CTCM: Arrival intensities to a node

- Assume acyclic graph from SRC to DST
Network failure and rerouting

- Phase I:
  - Rerouting after failure is $T_D \sim \exp(\alpha_D)$
- Phase II:
  - Restoration time is $T_R \sim \exp(\tau)$
- Phase III
  - Rerouting after failure is $T_U \sim \exp(\alpha_U)$

Undesired event is node failure
CTMC: Combine models

Non-failed node
CTMC: Combine models

Failed node
CTMC: Combine models
CTMC: Combine models

- Number of states in combined model
  - Transient solution of $N_{\text{node}}$ models with $N_{\text{res}} \times N_{\text{phase}}$ states
- Product-form approximation
  - When arrival and service rates are “significantly” higher than rerouting and failure rates
  - This means when the state of the performance model at state changes in the dependability model does not have a significant impact of the transient behavior
  - Solve $N_{\text{node}} \times N_{\text{phase}}$ models with $N_{\text{res}}$ states and one with $N_{\text{phase}}$
CTMC: Combine models

- Arrival & service rates are much larger than rerouting & restoration rates
  - Product form solution can be assumed
  - Do not need to consider initial states in failure and rerouting model
- State probability at time $t$ of node $k$ is
  - $P_k(t;x,i) = \pi_k(x)\cdot p(t,i)$,
  where state $x=1,...,n_k$, phase $i=I,...,IV$
Performance metrics

- Packet loss,

\[ l_k(t) = \sum_{i=I}^{IV} \pi_k(n) R L_k(n, i) p(t, i) \]

- Throughput,

\[ l(t) = \sum_{k=1}^{N_{node}} \frac{l_k(t)}{\Gamma_s} \]

\[ \rho(t) = 1 - l(t) \]
Performance metrics

- Delay,

\[
EN_k(t) = \sum_{i=1}^{IV} RD_k(x, i) \pi_k(x) p_k(t, i)
\]

\[
d(t) = \sum_{k=1}^{N_{node}} EN_k(t)/\Gamma_s
\]
Rewards in Markov model

- Reward
  \[ R_k(x, i); k = 1, \ldots, N_{\text{node}}, x = 0, \ldots, N_{\text{res}}, i = I, \ldots, IV \]

- Reward packet loss
  - \( RL_k(x, i) = 0 \) for all states and phases except
    - for each node and all phases \( i: RL_k(N_{\text{res}}, i) = \Gamma_k \)
    - for all states in phase I of the failed node \( RL_k(x, I) = \Gamma_k \)

- Reward delay: (Number in system+Little)
  - \( RD_k(x, i) = x \) for all states and phases except
    for the failed node \( RD_k(x, i) = 0; i = I, II, III \)
CTMC model of each node

Performance model

Availability model

Assume product form solution (Jackson)
CTMC model of each node

Survivability models

Non-failed node

Failed node
Closed form solution

- Assume product form solution (Jackson Network)
- Determine steady state performance of each phase, $p_{j,i}$
  1. Immediately after a failure
  2. Rerouting completed after failure
  3. Restoration/repair done
  4. Rerouting completed after repair (normal operation)
- Assign rewards, $r_{j,i}$, and determine expected rewards
- Determine transient probabilities of each phase, $p_i(t)$
- Assumptions
  - Event rate in performance models high
  - Event rate in availability model low
  - At phase changes: Immediate change between steady state solutions

Transient reward: $R(t) = \sum_j \sum_i p_{j,i} r_{j,i} p_i(t)$
Solving the models

- **SRN**
  - Transient solution of model with $N_{\text{node}} \times N_{\text{res}} \times N_{\text{phase}}$ states

- **Decomposed CTMC**
  - Transient solution of $N_{\text{node}}$ models with $N_{\text{res}} \times N_{\text{phase}}$ states

- **Decomposed CTMC**
  - Steady state solution of $N_{\text{node}} \times N_{\text{phase}}$ models with $N_{\text{res}}$ states
  - Transient solution of one model with $N_{\text{phase}}$ states
Illustrative example 1: Network with 4 nodes

- Simulation model (Simula/DEMOS)
- Stochastic Reward Net (Generalized PetriNets) model
- CTMC model of each node
- Closed form solution
- Comparisons

\[ a/b \]
\[ r_{ij}(I) = r_{ij}(IV) = a \]
\[ r_{ij}(II) = r_{ij}(III) = b \]
Network with 4 nodes: loss ratio

The two SRN models gives identical results.

SRN and simulation is very close both in transient and steady state.

CTMC and simulation/SRN is very close in transient period, and conservative in steady state.
Network with 4 nodes: average number in system

![Graph showing average number in system with excellent performance indicated]
III. Case studies
Application in Real sized network

- **System**
  - packet switched, telecommunication network

- **Service**
  - virtual connection between specific peering nodes in the network

- **Requirement**
  - maximum packet loss probability and end-to-end delay of non-lost packets in the virtual connections

- **Undesired events**
  - link and node failures caused by attacks, accidents, and software and hardware failures
Why does the voice network need to be survivable

- Telecommunications network
  - Voice network
  - Data network
- The voice network is a part of the critical infrastructure.
- Other critical infrastructure depends on the voice network for effective functioning; for example
  - emergency services
  - government services
  - banking and finance
- There are several examples of the failure of the voice network as a result of catastrophic events.
- Many architectures concentrate high density trunks and lines at switch nodes, which exacerbates the extent of communication loss after a catastrophic event.
Telecommunications system failures

• Externally caused events (North American examples)
  – Hinsdale, Illinois central office switch fire, May 1988
  – San Francisco Bay Area earthquake, October 1989
  – Oakland fire storm, October 1991
  – Judge Thomas senate vote, October 1991
  – Events of September 11, 2001
  – North America power outage, August 14, 2003

• Internally caused events (North American examples)
  – Signaling System 7 (SS7) outage, January 1990
  – Newark fiber cut, January 1991
  – New York power outage, September 1991
Classical PSTN network hierarchy of switches

Class 1
Regional

Physical Realization

Class 2
Sectional

highly survivable
• Diverse switch locations

Class 3
Primary

• SDH/SONET facility protection
• Alternate routes between offices

Class 4
Toll

Class 5
Local

Big impact after loss of a class 5 switch due to no redundancy
Class 5: more problematic

Big impact after loss of a class 5 switch due to no redundancy

10,000 or more pair of wires meet at a single point
Telephony terms

- Drop Distribution Feeder
- Cross Connect (XC)
- Remote Terminal (RT)
- NT
- Transmission Network
- Central Office (CO)

Terms:
- LAU: Line Access Unit
- CSU: Call Processing Unit
- HPU: Central Host Unit
- Main Distribution Frame (MDF)
- Wire Center (WC)
- Pedestal
- Pole
- Network Termination (NT)
- Trunk Distribution Frame (TDF)
- Customer Wiring
- Outside Plant

Diagram components:
- LAU
- SCU
- CSU
- SSU
- TAU
- HPU
- APU
- NTNU
Increasing wire concentration approaching central office

- Remote Terminal (RT)
- Transmission Network
- Trunk Distribution Frame (TDF)
- Central Office (CO)
- Cross Connect (XC)
- Wire Center (WC)
- Main Distribution Frame (MDF)
- Network Termination (NT)
- Pedestal
- Ones
- Tens
- Hundreds
- Thousands
- Customer Wiring
- Outside Plant
- Feeders (Tens, Hundreds, Thousands)

Diagram showing the flow of wires from customer wiring through to the central office, with various network terminations and distribution frames.
Classical Architecture

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>○</td>
<td>Wiring Cross-Point</td>
</tr>
<tr>
<td></td>
<td>Multi-Pair Cable</td>
</tr>
<tr>
<td></td>
<td>Drop Cable</td>
</tr>
<tr>
<td>🏠</td>
<td>Single Family Residence</td>
</tr>
<tr>
<td>🏡</td>
<td>Multi-Family Dwelling</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unit</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO</td>
<td>Central Office</td>
</tr>
<tr>
<td>HPU</td>
<td>Host</td>
</tr>
<tr>
<td>APU</td>
<td>Administrative</td>
</tr>
<tr>
<td>SSU</td>
<td>Signaling</td>
</tr>
<tr>
<td>SCU</td>
<td>Communications</td>
</tr>
<tr>
<td>CSU</td>
<td>Call Service</td>
</tr>
<tr>
<td>LAU</td>
<td>Line Access</td>
</tr>
<tr>
<td>TAU</td>
<td>Trunk Access</td>
</tr>
</tbody>
</table>

Go to Survivable Architecture Alternatives
## Layered architecture

<table>
<thead>
<tr>
<th>Layer</th>
<th>Nodal Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Customer premise equipment and access network</td>
<td>Elements owned by the subscriber and the copper wire network between the subscriber and a telephone company LAU</td>
</tr>
<tr>
<td>2 Line cards</td>
<td>Nodal elements providing signal conversion and transport between the subscriber and other layers</td>
</tr>
<tr>
<td>3 Call processing</td>
<td>Nodal elements providing call management</td>
</tr>
<tr>
<td>4 Transport</td>
<td>Transport equipment such as ADMs, Digital Cross-Connect systems and transmission cables that interconnect nodal elements</td>
</tr>
<tr>
<td>5 Central elements</td>
<td>Elements of the digital switch that must remain centralized</td>
</tr>
<tr>
<td>6 Trunks</td>
<td>Inter-switch trunks that provide routes between PSTN offices</td>
</tr>
<tr>
<td>7 Application</td>
<td>Auxiliary elements that provide services, i.e., voice mail, conference bridges, E9-1-1</td>
</tr>
</tbody>
</table>

## New options for different layers

<table>
<thead>
<tr>
<th>Layer</th>
<th>Option 1</th>
<th>Option 2</th>
<th>Option 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. CPE and Access Network</td>
<td>Direct wire to CO</td>
<td>Shortened loop LAU at or near site</td>
<td></td>
</tr>
<tr>
<td>2. Line Cards (LAU)</td>
<td>RT at or near site</td>
<td>Multiple small LAUs at or near site</td>
<td></td>
</tr>
<tr>
<td>3. Call Processing</td>
<td>Distributed CSU (single switch)</td>
<td>Multi-switch CSU architecture</td>
<td>Emergency CSU/LAU combination</td>
</tr>
<tr>
<td>4. Transport</td>
<td></td>
<td>General diversity and redundancy principles apply</td>
<td></td>
</tr>
<tr>
<td>5. Central Elements</td>
<td>Active/Active HPU</td>
<td>Active/Standby HPU</td>
<td></td>
</tr>
<tr>
<td>6. Trunks</td>
<td></td>
<td>General diversity and redundancy principles apply</td>
<td></td>
</tr>
<tr>
<td>7. Application</td>
<td></td>
<td>General diversity and redundancy principles apply</td>
<td></td>
</tr>
</tbody>
</table>
HPU Synchronization

- HPU functions include:
  - Management of global resources: intra-switch fabric, trunks, and signaling links
  - Administrative activities: billing, operations support system (OSS) links, and human/machine interaction
- Databases on the standby HPU are kept synchronized with the active HPU through periodic updates and tape backups
  - Line additions/deletions
  - New hardware
  - Dialing plans
  - Subscriber features
  - Outside facilities
- Frequency and integrity of updates determines the time required (syn rate) and the success rate (syn coverage) of restoring the system to a working state after loss of an HPU
- HPU synchronization
  - Near instantaneous with some coverage (A/S I)
  - Delay before service is restored with perfect coverage + all subscribers (A/S II), 50% subscribers (A/A)
### Survivable architecture alternatives

<table>
<thead>
<tr>
<th>Layer</th>
<th>Classical Architecture</th>
<th>Survivable Architectures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>A/S I</td>
</tr>
<tr>
<td>2. Line Cards</td>
<td>All LAUs at CO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Multiple LAU at or near site</td>
<td></td>
</tr>
<tr>
<td>3. Call Processing</td>
<td>All CSUs at CO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Distributed CSU, Single Switch</td>
<td></td>
</tr>
<tr>
<td>5. Central Elements</td>
<td>All at CO</td>
<td>HPU active/standby</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HPU active/active</td>
</tr>
<tr>
<td>Syn.</td>
<td>-</td>
<td>w/.prob. c</td>
</tr>
<tr>
<td></td>
<td></td>
<td>w/.prob. 1</td>
</tr>
</tbody>
</table>

Active/standby: the standby HPU takes over all the customers and trunks when the active HPU is destroyed in a disaster.
Active/active: load sharing, each HPU serves half customers with half trunks.
Architecture A/S I, A/S II: Reduce Length of Copper Loops +
Distribute Call Processing + Active/Standby Host

Customer Wiring
Outside Plant

Pedestal
Remote Terminal (RT)
Network Termination (NT)
Pole
Drop Distribution

Transmission Network

Remote Terminal (LAU)

Distributed CP Servers (CSU)

Trunk Distribution Frame (TDF)

Central Office (CO)
Active Host
Standby Host

NTNU
Norwegian University of Science and Technology
Architecture A/A: Reduce Length of Copper Loops + Distribute Call Processing + Active/Active Host
Survivable Architecture Alternatives

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Pair Cable</td>
<td>4-wire trunk cable with four independent pairs</td>
</tr>
<tr>
<td>Drop Cable</td>
<td>4-wire trunk cable with different cable types or services</td>
</tr>
<tr>
<td>Protected Cable</td>
<td>4-wire trunk cable with additional protective measures</td>
</tr>
<tr>
<td>Single Family Residence</td>
<td>2-wire trunk cable for single-family residences</td>
</tr>
<tr>
<td>Business</td>
<td>4-wire trunk cable for business applications</td>
</tr>
<tr>
<td>Multi-Family Dwelling</td>
<td>2-wire trunk cable for multifamily dwellings</td>
</tr>
</tbody>
</table>

Unit Type

<table>
<thead>
<tr>
<th>Unit</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO</td>
<td>Central Office</td>
</tr>
<tr>
<td>APU</td>
<td>Administrative</td>
</tr>
<tr>
<td>CSU</td>
<td>Call Service</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td>Trunk Access</td>
</tr>
<tr>
<td>HPU</td>
<td>Host Processing</td>
</tr>
<tr>
<td>LAU</td>
<td>Line Access</td>
</tr>
</tbody>
</table>

Inter-Nodal Transport

Common Channel Signaling

Other CO

Survivable Architecture Alternatives

NTNU

Go to Classical Architecture

Duke

Norwegian University of Science and Technology

pratt.duke.edu
Architectures A/S I, A/S II, A/A

- Distributed CSU
  - Maintain basic service \( (r_b \times 100\% \text{ of total traffic}) \) when HPU fails
  - Reduced capacity \( (r_r \times 100\% \text{ of total trunks}) \) for basic service

- Redundant HPU
  - Active/standby A/S I
    - Switchover coverage
    - Synchronization probability
  - Active/standby A/S II
    - Switchover coverage
    - Synchronization delay \( (r_p \times 100\% \text{ of customers get service before synchronization}) \)
  - Active/active A/A
    - Load sharing, each serves half subscribers
    - Switchover coverage
    - Synchronization delay \( (r_p \times 100\% \text{ of customers get service before synchronization}) \)

- Failure scenario
  - Loss of one active HPU
System parameters

- Total capacity $n$: 10000 trunks
- Call arrival rate $\lambda$: 100 / sec$^{-1}$
- Mean call holding time $\mu^1$: 100 seconds
- Disaster rate $\lambda_f$: 1 / year$^{-1}$
- Mean detection time $\delta_d^{-1}$: 1 second
- Mean switchover time $\delta_r^{-1}$: 60 seconds
- Switchover coverage of architecture A/S I, A/S IIq: 0.9
- Switchover coverage of architecture A/A v: 0.9
- Syn. probability $c$: 0.99
- Mean syn. time $\delta_s^{-1}$: 10 minutes
- Mean manual recovery time $\mu_r^{-1}$: 2 hours
- Mean manual repair time $\mu_r^{-1}$: 10 days
- Mean reconfiguration time $\beta^1$: 10 minutes
- Partial service probability $r_p$: 0.99
- Basic traffic percentage $r_b$: 0.4
- Local trunk facility percentage $r_r$: 0.4
Pure performance model

What happens before the occurrence of failure?

Steady state closed-form solution: Erlang B Formula

\[ \pi_j = \frac{(\lambda/\mu)^j / j!}{\sum_{k=0}^{n} (\lambda/\mu)^k / k!} \]

Blocking probability:

\[ P_{bk} = \pi_n \]

Expected number of calls in the system:

\[ \sum_{k=0}^{n} k \pi_k \]
Pure availability models: A/S I, A/S II, A/A
Pure performance analysis: blocking probability $P_{bk}$

<table>
<thead>
<tr>
<th>State</th>
<th>A/S I</th>
<th>A/S II</th>
<th>A/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>(u,u)</td>
<td>0.0079366</td>
<td>0.0079366</td>
<td>0.01120</td>
</tr>
<tr>
<td>(u,d)</td>
<td>0.0079366</td>
<td>0.0079366</td>
<td>-</td>
</tr>
<tr>
<td>(d,u)</td>
<td>0.6050</td>
<td>0.6050</td>
<td>0.3056</td>
</tr>
<tr>
<td>(r,u)</td>
<td>0.6050</td>
<td>0.6050</td>
<td>-</td>
</tr>
<tr>
<td>(d,f)</td>
<td>0.6050</td>
<td>0.6050</td>
<td>0.6050</td>
</tr>
<tr>
<td>(s,d)</td>
<td>0.6050</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>(u_p,d)</td>
<td>-</td>
<td>0.08829</td>
<td>-</td>
</tr>
<tr>
<td>(d,u_2),(u,u_2)</td>
<td>-</td>
<td>-</td>
<td>0.007937</td>
</tr>
<tr>
<td>(d,u_1)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>(d,u_p)</td>
<td>-</td>
<td>-</td>
<td>0.008045</td>
</tr>
</tbody>
</table>
Pure availability analysis: steady state

- Steady state availability
  - A/S I
    - Up states: uu, ud
    - Down states: du, df, ru, sd
    - $P_{\text{coA}} = P(uu) + P(ud) = 0.999994$
  - A/S II
    - Up states: uu, ud
    - Partial up state: upd
    - Down states: du, df, ru
    - $P_{\text{coA}} = P(uu) + P(ud) + P(u_d)d_{\text{p}}r_{\text{p}} = 0.999992$
  - A/A
    - Up states: uu, uu2, du2
    - Partial Up State: du, du1, dup
    - Down states: df
    - $P_{\text{coA}} = P(uu) + P(uu2) + P(du2) + P(du)*0.5 + P(du1)*0.5 + P(dup)*(0.5 + r_{\text{p}}/2) = 0.999995$

- Expected Downtime
  - A/S I: 3.15 minutes per year
  - A/S II: 4.20 minutes per year
  - A/A: 2.63 minutes per year

Availability hereinafter means capacity-oriented availability (COA), $P_{\text{COA}} = 1$ means full capacity.
Pure availability analysis: transient

![Graph showing transient availability over time with different curves labeled A/S I, A/S II, and A/V/A.](graph.png)
Performability results

Steady state:
A/S I: 0.0079404
A/S II: 0.0079393
A/A: 0.01115
Model modification for survivability definition: A/S I

Force a failure in the system

Normally operating in this state

Make this the initial state

similar modification for A/S II and A/A

\[ P_{bk} = 0.0079366 \]

\[ P_{bk} = 1 \]
Implication of the modification

- What does it mean when transition ($\lambda_f$) is removed?
  - A failure is injected into the system
  - All the system survivability measures do **not** depend on the value of $\lambda_f$
  - All previous performance/availability/performability measures and the first two survivability measures do depend on the value of $\lambda_f$
  - It is usually difficult to have agreement on the value of $\lambda_f$ in practice. Therefore, those measures depending on $\lambda_f$ are controversial.
  - This is the reason why only the T1A1.2 definition gives an important, useful and novel survivability measure.
Survivability results: A/S I

- **0 sec**
  \[ P_{bk} = 0.6050 = 76.2 \times P_{bk}(uu) \]

- **10 sec**
  \[ P_{bk} = 0.5309 = 66.9 \times P_{bk}(uu) \]

- **10 min**
  \[ P_{bk} = 0.0378 = 4.76 \times P_{bk}(uu) \]

- **1 hr**
  \[ P_{bk} = 0.01183 = 1.49 \times P_{bk}(uu) \]

- **10 hr**
  \[ P_{bk} = 0.00798 = 1.005 \times P_{bk}(uu) \]
Survivability results

![Graph showing survivability results with different curves for A/S I, A/S II, A/A, and steady state over time in seconds.](image-url)
## Survivability results

<table>
<thead>
<tr>
<th></th>
<th>A/S I</th>
<th>A/S II</th>
<th>A/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0$</td>
<td>0.007937</td>
<td>0.007937</td>
<td>0.01120</td>
</tr>
<tr>
<td>$m_a$</td>
<td>0.6050</td>
<td>0.6050</td>
<td>0.3056</td>
</tr>
<tr>
<td>$m_u$</td>
<td>0.5971</td>
<td>0.5971</td>
<td>0.2944</td>
</tr>
<tr>
<td>$m_r$ (t_r=10 sec)</td>
<td>0.5309</td>
<td>0.5229</td>
<td>0.2602</td>
</tr>
<tr>
<td>$m_r$ (t_r=10 min)</td>
<td>0.03778</td>
<td>0.01391</td>
<td>0.01356</td>
</tr>
<tr>
<td>$m_r$ (t_r=10 hr)</td>
<td>0.01183</td>
<td>0.01164</td>
<td>0.01163</td>
</tr>
<tr>
<td>$t_R^*$</td>
<td>31610 sec</td>
<td>31550 sec</td>
<td>4300 sec</td>
</tr>
</tbody>
</table>

*A relative error 1% is assumed for calculating $t_R$*
## Comparison – ELF

<table>
<thead>
<tr>
<th></th>
<th>Call loss due to failure</th>
<th>Extra call loss due to blocking</th>
<th>ELF</th>
</tr>
</thead>
<tbody>
<tr>
<td>A/S I</td>
<td>9920</td>
<td>11874</td>
<td>21794</td>
</tr>
<tr>
<td>A/S II</td>
<td>9920</td>
<td>8436</td>
<td>18266</td>
</tr>
<tr>
<td>A/A</td>
<td>4944</td>
<td>2465</td>
<td>7409</td>
</tr>
</tbody>
</table>
## Survivability ranking

<table>
<thead>
<tr>
<th></th>
<th>A/S I</th>
<th>A/S II</th>
<th>A/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_{\text{full}}$</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>$E[N]$</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>$N_{0%}$</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>$m_a^*$</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>$m_r^* t=10 \text{ min}$</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>$m_r^* t=1 \text{ hour}$</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>$t_R$</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>ELF</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

$P_{\text{full}}$ is the steady state prob. of providing full service

$m_a^*$, $m_r^*$ are relative values with respect to $p_{bk}(uu)$
Interpretation of results

- Active/active A/A offers the best survivability in most cases
  - however, it is most complex and costly in terms of development and operation
  - also requires changes to the signaling network
- Active/standby A/S II offers better survivability than active/standby A/S I
  - this is due to the synchronization delay associated with A/S I
  - A/S II is a more realistic scenario
- Architecture can be chosen by different criteria
- There are tradeoffs between survivability, cost, and operations complexity
- Architecture choice also depends on subscriber type
  - Residential
    - desirable to have basic service in shortest time for all customers after a disaster event
  - Business or government
    - desirable to have full service to a certain group of customers immediately after a disaster event
  - Precedence and preemption schemes can be implemented to give priority of service to govt and service personnel
    - gives priority subscribers better probability of call completion after a disaster event
- Finally, the choice of architecture depends on the loss scenarios that are important
Objectives and target system

- Transient performance in networks with virtual connections
- From occurrence of an undesired event until steady state operation is restored
- Goal: Survivability model of performance after network failure(s)
Network survivability models

- Phased recovery model
- Modeling approach
- Complete composite model
- Space-decomposed model
- Time-decomposed model
Undesired event is node failure
Phased recovery model

- **Phase I:**
  - Rerouting after failure is $T_D \sim \exp(\langle D \rangle)$

- **Phase II:**
  - Restoration time is $T_R \sim \exp(\mid)$

- **Phase III:**
  - Rerouting after failure is $T_U \sim \exp(\langle U \rangle)$

- **Phase IV:**
  - Fault free network with default routing

Undesired event is node failure
Modeling approach

- Performance model
- Phased recovery model
- Composite performability model
- Survivability model
Complete composite model

- **Simulation**
  - DEMOS/Simula
  - Discrete event, process-oriented simulation model

- **Analytical**
  - SRN: Stochastic Reward Nets
  - Full CTMC
  - Solved by SPNP and SHARPE
Complete composite model
Complete composite model

Identical assumptions as the simulation model

Complete composite CTMC model of 4 node network

SRN model
Numerical example: packet loss probability

The two SRN models give identical results.

SRN and simulation is very close both in transient and steady state.
Space-decomposed model

- Decomposed CTMC to reduce number of states
- Nodes modeled separately
- The arrival intensities change when node or link fails
- The resource utilization model below is solved for each set of intensities
Time-decomposed model

- When arrival and service rates are “significantly” higher than rerouting and failure rates (recall John Meyer’s Performability models)
- This means when the state of the performance model at state changes in the dependability model does not have a significant impact on the transient behavior
Numerical example: average number in system

Number drops packets are lost

Compares decomposed models and simulations
Modeling assumptions

- External packet arrivals are Poisson
- Packet service time distribution is assumed to be exponential
- Space decomposition assumes independent network nodes
- Each recovery phase has steady-state performance
- Phase time distribution in the recovery model is (for simplicity) assumed to be exponential
Modeling scalability

• Complete composite model - SRN
  – Transient solution of model with $N_{node} \times N_{res} \times N_{phase}$ states

• Space decomposed CTMC
  – Transient solution of $N_{node}$ models with $N_{res} \times N_{phase}$ states

• Time decomposed CTMC
  – Steady state solution of $N_{node} \times N_{phase}$ models with $N_{res}$ states
  – Transient solution of one model with $N_{phase}$ states
Summary of real sized network application

- Complete composite CTMC
  - Identical assumptions as in the simulation model
  - State space explosion and transient solution is slow
- Space decomposed CTMC
  - Models of nodes are independent
  - High accuracy when performance is dominated by failed node and its neighborhood
  - Reduced state space but transient solution is still rather slow
- Time composed CTMC
  - Approximation is very good with orders of magnitude different rates
  - Significantly reduces computation time because transient model is reduced
Illustrative example 2: Network with 10 nodes

- Simulation model
- Closed form solution
- Comparisons

\[
ad/b
\]

\[r_{ij}(I) = r_{ij}(IV) = a\]

\[r_{ij}(II) = r_{ij}(III) = b\]

\[
N = 50
\]

Source: Poisson arrivals

Exponential service time
Network 10 nodes: loss delay

Rerouting model is $F(t) = p \times \exp(-t \alpha_D)$

(Almost) all loss is due to delayed rerouting
Network 10 nodes: average number in system

Phase I  Phase II+III

Delay of dropped packets is decreased
Summary of observations

- **SRN with complete CTMC**
  - Identical to simulation model
  - State space explosion and transient solution is slow
- **Node independent CTMC**
  - Breaks dependence between nodes
  - Close to complete model when performance is dominated by failed node and its neighborhood
  - Reduced state space but transient solution is still rather slow
- **Node independent and product form approximation CTMC**
  - Approximation is very good with orders of magnitude different rates
  - Significantly reduces computation because transient model is reduced
Network with 58 nodes

Uninett IP backbone
20 virtual connections
Severe link and node failures

Routing schemes from CEAS
Five phases from link failure

(i) single link failure
(ii) hurricane
Network with 58 nodes

- Each phase has a routing scheme
- Determine (steady state) performance for each phase
  - Jackson Network
  - Determine loss: only on failure before rerouting
  - Determine delay: approximate model
- Assume change from phase to phase will instantaneously change performance model
- Transient model for phase changes
- Combine transient phase and steady state performance solutions
- Compare analytic vs. simulation
Network with 58 nodes

- Assumptions
  - Infinite buffers
  - (Semi) Markov properties
  - Significant difference between activities in performance and availability models allows immediate shift in performance
  - Product form solution enables much more details in the availability model, such as multiple failure modes and failure types
Network with 58 nodes: loss ratio

$L(t)$

$\mu_m$ 0.25

$\mu_r$ 0.05

$t_r$

90 replications

Very good fit
Network with 58 nodes: delay distribution

- T=0.1: 90 replications
- T=5.0: Fair, but not perfect match
Objectives and target system

- Transient performance in networks with virtual connections
- From occurrence of an undesired event until steady state operation is restored
- **Goal**: Survivability model of performance after network failure(s)
Modeling approach

- Response time blocks for delay distributions
- Space-time decomposition to reduce models
- Time samples to model routing protocol behavior

\[
\begin{align*}
\mu_1 - \Gamma_1 \mu_2 - \Gamma_2 \left( \mu_3 - \Gamma_3 \right) r (2) \\
\mu_{10} - \Gamma_{10} \mu_{11} - \Gamma_{11} \left( \mu_5 - \Gamma_5 \right) r (2) \\
\mu_4 - \Gamma_4 \mu_7 - \Gamma_7 \mu_8 - \Gamma_8 \left( \text{best path routing} \right) & \quad \left( \text{stochastic routing} \right)
\end{align*}
\]
\( P_{S_f}(t) = \text{probability of delay less or equal to } t \)

\( \Gamma_s \) are determined by traffic equations

Routing probability from node 3 to 5 of VC2

CTMC for VC1
(best path routing)

CTMC for VC2
(stochastic routing)
Response time blocks – link down

All traffic lost until rerouting takes effect, $P_{sf}(t) = 0$
Response time blocks – rerouting

![Diagram showing response time blocks with rerouting via 6]

- Source node: src1
- Destination node: dst1
- Intermediate nodes: S1, S2, S6, S10, S11, Sf
- VC1

Mathematical expression: $\mu_1 - \Gamma_1 \mu_2 - \Gamma_2 \mu_6 - \Gamma_6 \mu_{10} - \Gamma_{10} \mu_{11} - \Gamma_{11}$
Space-time decomposition

State space explosion!

Each phase (routing time sample) reaches stable state

Traffic to each node treated independently
Phased recovery model

- Sample routing probabilities at different phases
  - Simulations in ns-2 (this paper)
  - Routing table dumps from routers
- Routing probability matrix, \( R(t) = \{r_{ij}^{(vc)}(t)\} \)

<at failure> \[ t_0 \]

<after rerouting> \[ t_1 \]
Numerical example: packet loss probability

ns2 simulations and decomposed analytic model coincide well
Numerical example: delay distribution

All exponential

Pareto service times

Pareto arrival times
Numerical example: packet loss probability
Numerical example: delay distribution

\[ D(0.0, u) \]

\[ D(0.1, u) \]

\[ D(0.2, u) \]

\[ D(50.0, u) \]
Closing remarks

- Choose an appropriate definition of survivability
- Established a general analytical modeling approach for survivability quantification
- Extended the work to wireless cellular networks
- For complex systems
  - Rough assumption provide significant simplifications, or
  - Simulative (rather than analytic) solution
- Network models
  - State space explosion
  - Significant simplifications in analytic models
  - Realistic simulation models
- Compare survivability quantifications
Closing remarks

• In summary
  – Survivability in networks under failures
  – Time-decomposed model approach for large networks
  – Delay distribution of virtual connections
  – Very good correspondence with simulation results

• Current and planned work
  – Large scale networks exposed to extensive failures
  – Semi-Markov approach for non-Exponential distributions
  – Validate and relax assumptions
References

Reference

Reference