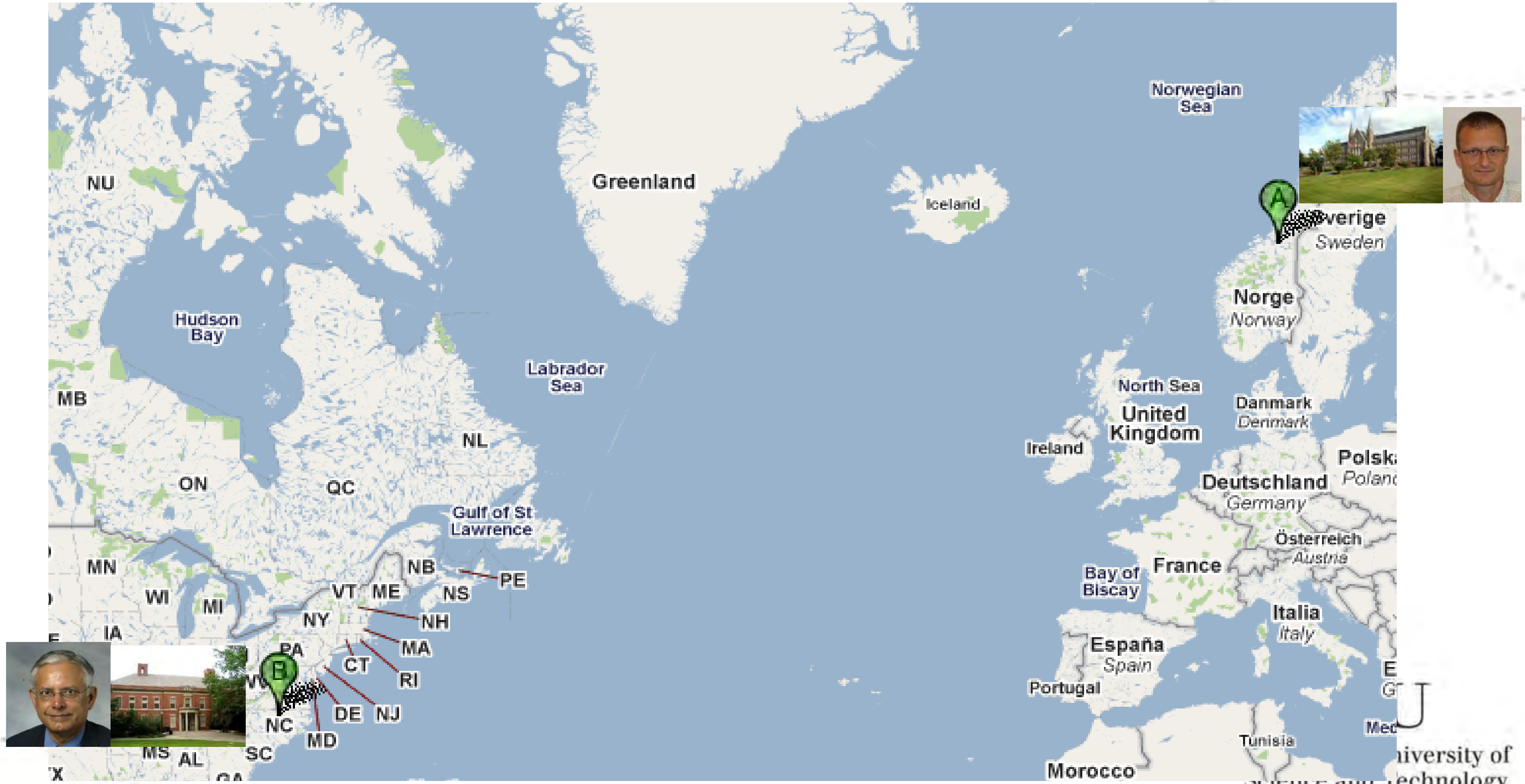
Network Survivability Modeling and Quantification

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
Norwegian University of Science and Technology

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 in are in reliability, availability, performance, performability, security and survivability evaluation of computer and communication systems. He works closely with industry in carrying our 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.

NTNU
Norwegian University of Science and Technology

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.

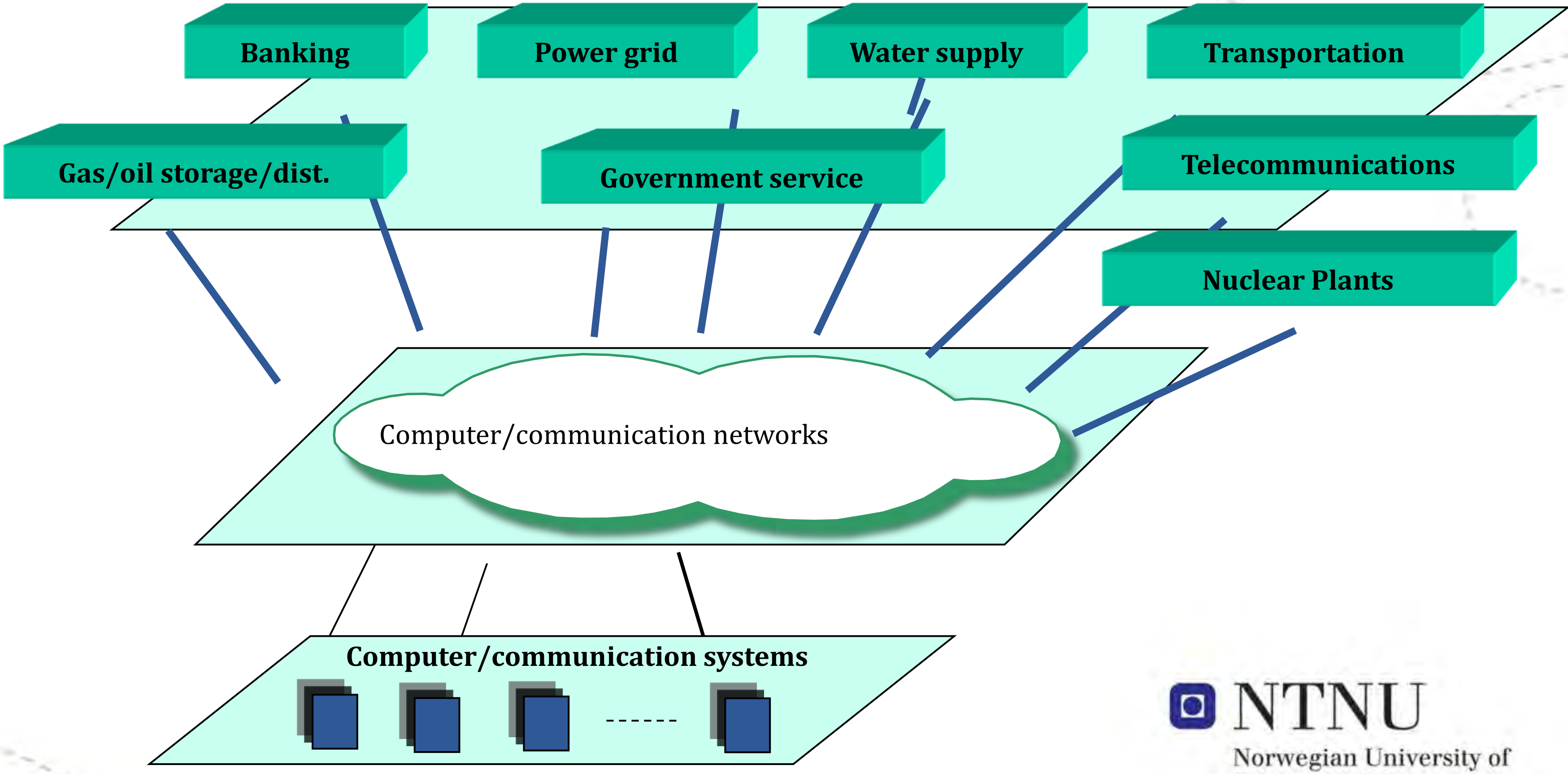
Tutorial outline

I. Survivability concepts and definition

II. Network survivability modeling and quantification

III. Case studies

What needs to be survivable?



Why survivability?

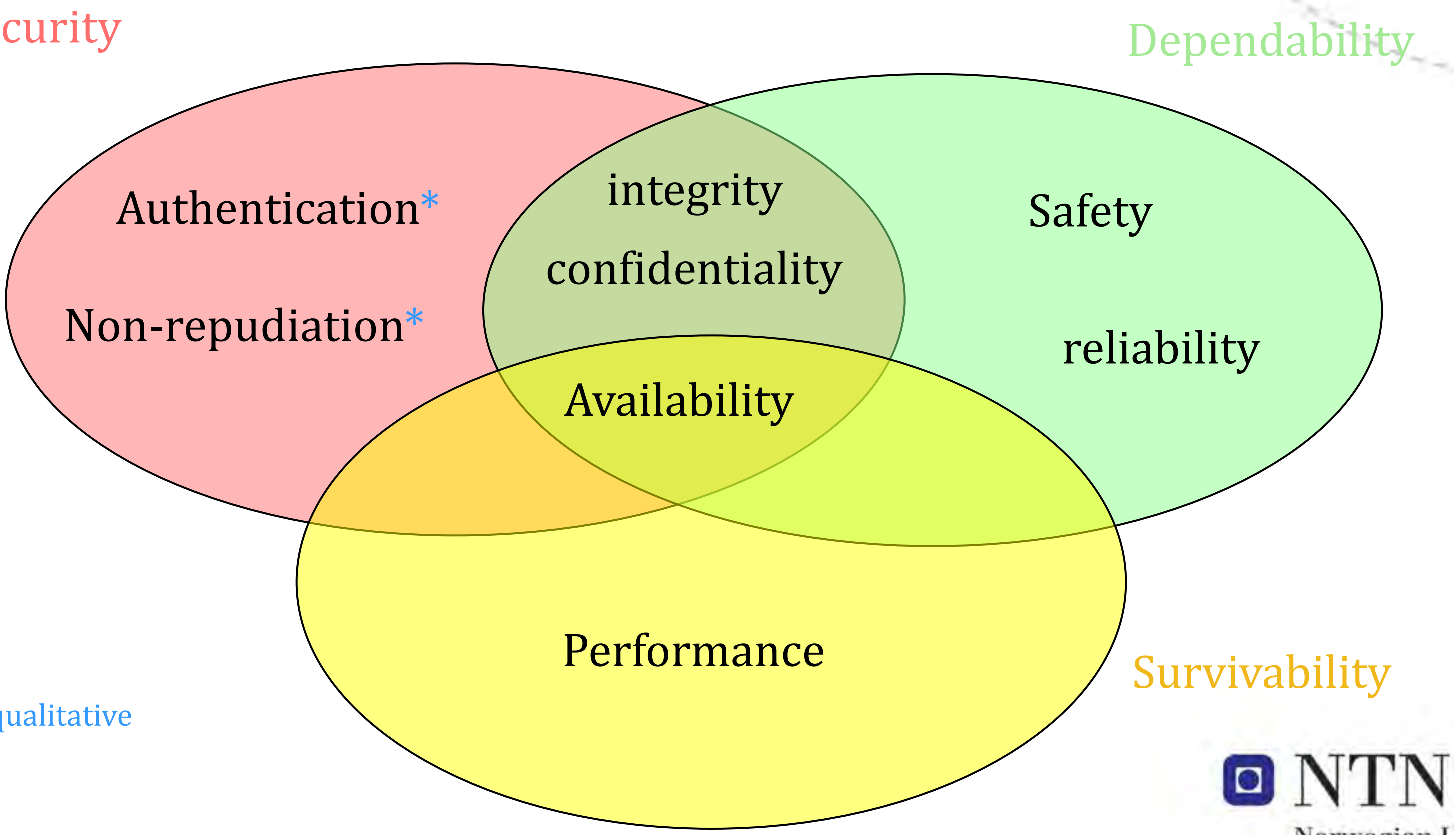
- Society heavily depends on telecommunication services
- Critical services must be available even under
  - Technical network failures
  - Malicious attack
  - Accidents and natural disasters
- Security, dependability, survivability, availability, reliability…
  - All concerned with trusted services 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

NTNU

Norwegian University of Science and Technology

Our View on Survivability, Performance, Dependability and Security

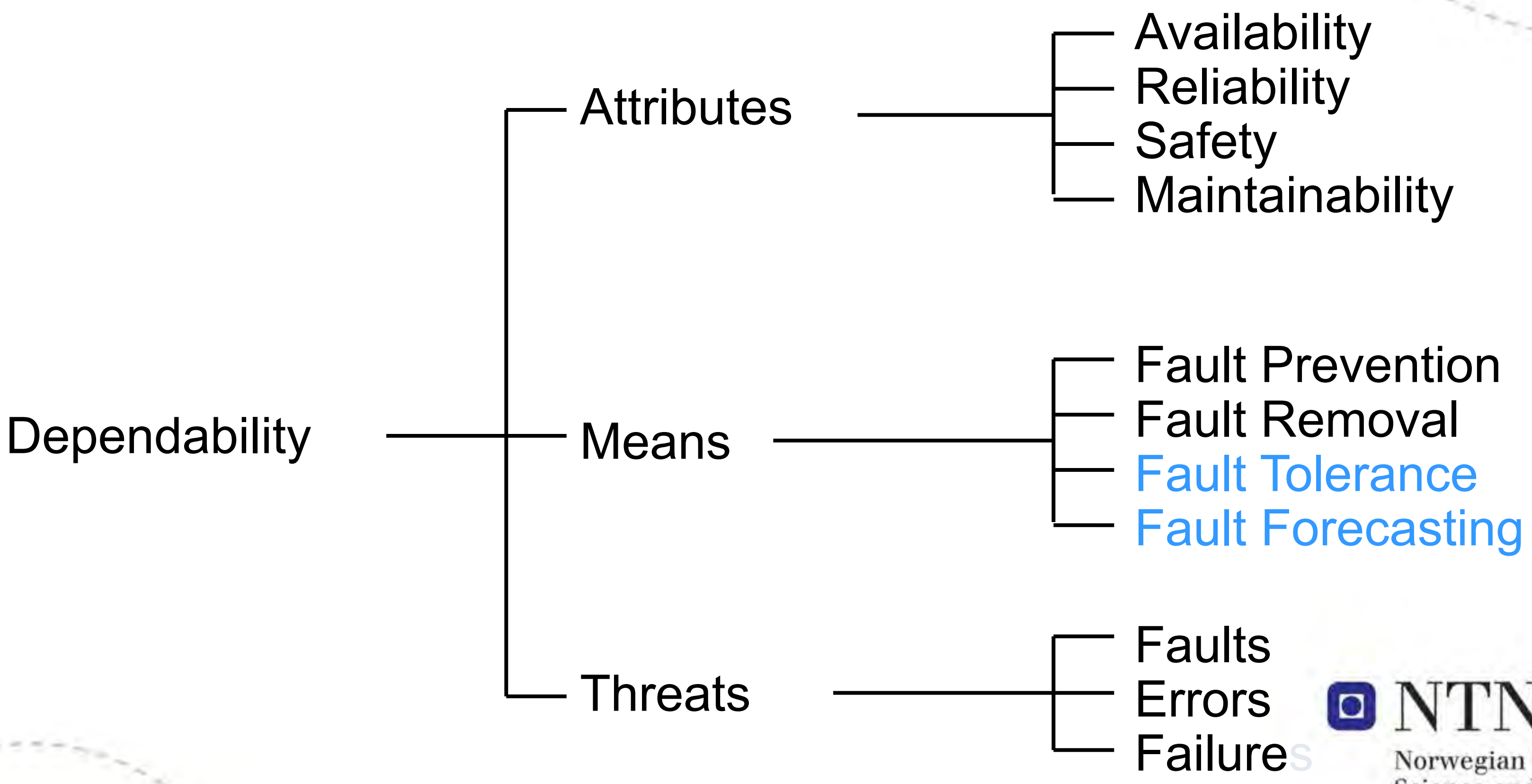


*: qualitative

Performance + Availability/Reliability = Performability

Dependability– An umbrella term

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



NTNU
Norwegian University of Science and Technology

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?"

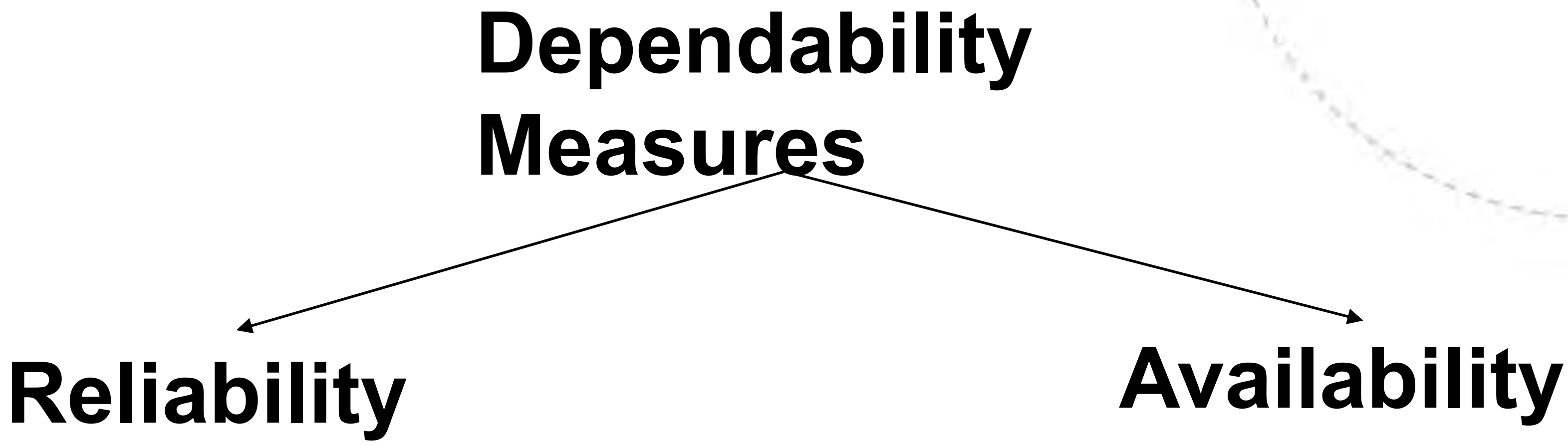
NTNU
Norwegian University of Science and Technology

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

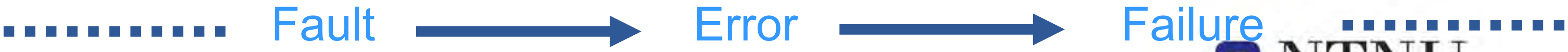
Availability

- **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.*“

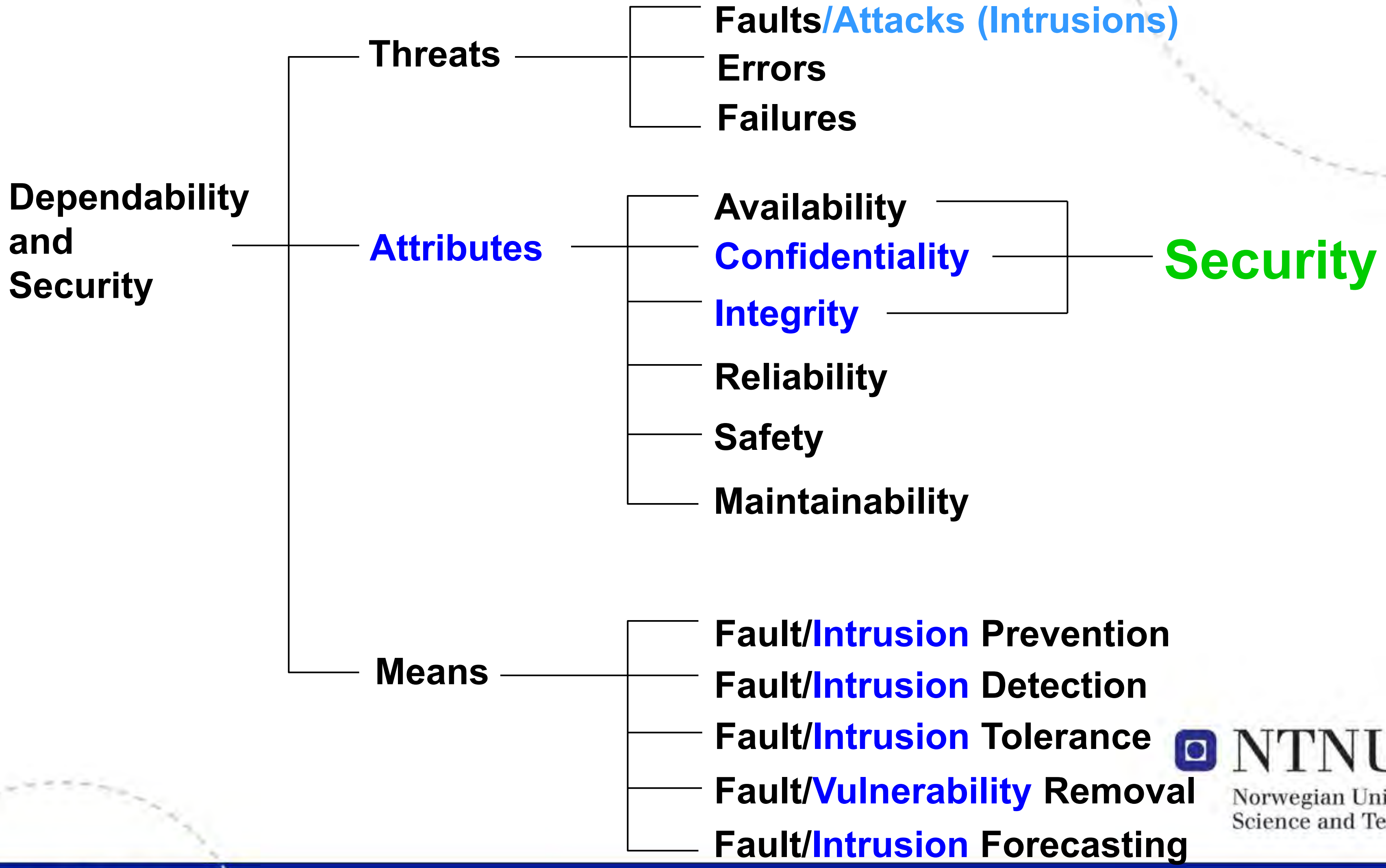
IFIP WG10.4

- **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
  - Attributes
    - Availability
    - Confidentiality
    - Integrity
    - Reliability
    - Safety
    - Maintainability
  - Means
    - Fault/Intrusion Prevention
    - Fault/Intrusion Detection
    - Fault/Intrusion Tolerance
    - Fault/Vulnerability Removal
    - Fault/Intrusion Forecasting

Availability, Confidentiality, Integrity → Security

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

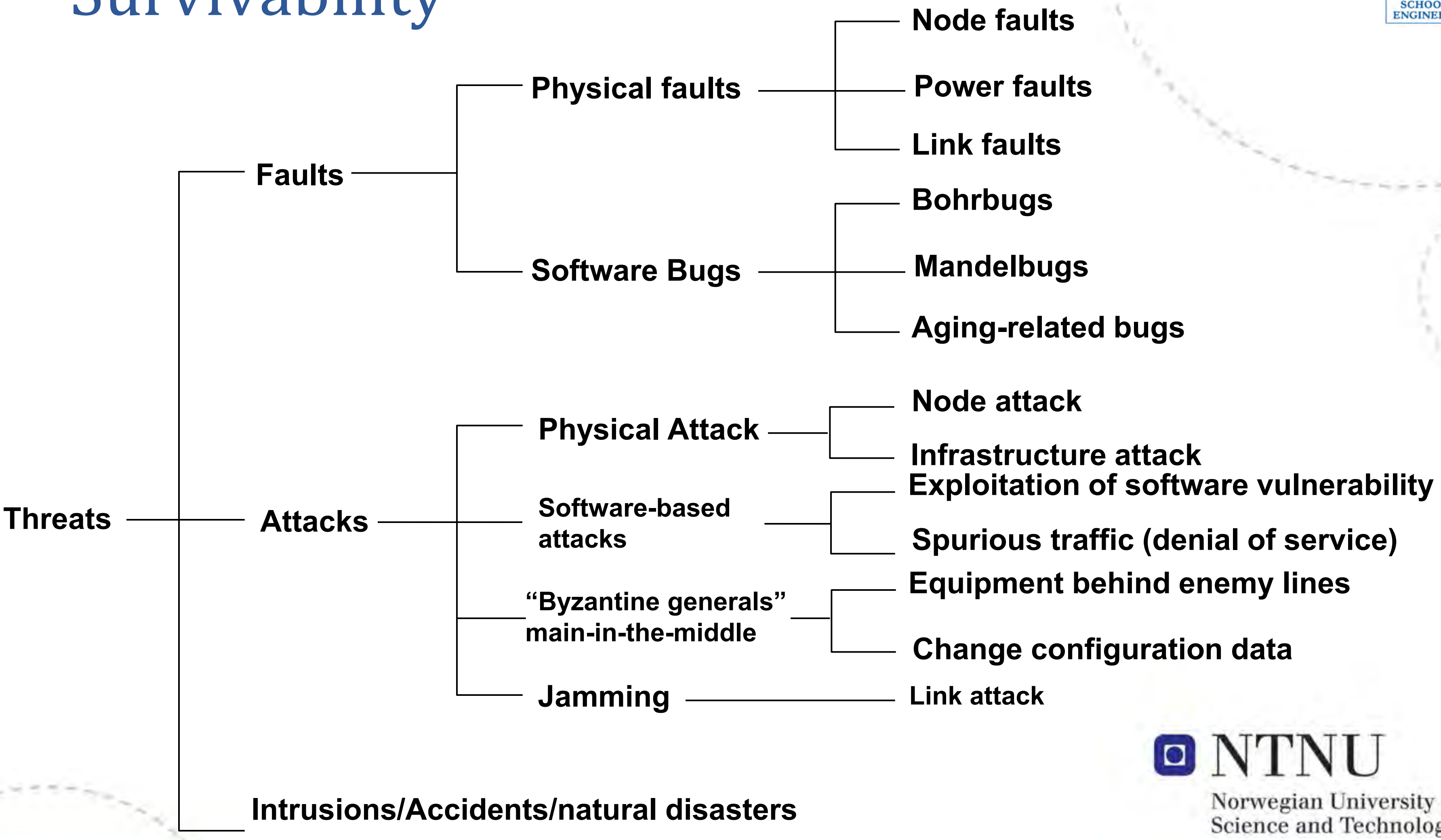
Survivability Principles

- **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



- Threats
  - Faults
    - Physical faults
      - Node faults
      - Power faults
      - Link faults
    - Software Bugs
      - Bohrbugs
      - Mandelbugs
      - Aging-related bugs
  - Attacks
    - Physical Attack
      - Node attack
      - Infrastructure attack
    - Software-based attacks
      - Exploitation of software vulnerability
      - Spurious traffic (denial of service)
    - "Byzantine generals" main-in-the-middle
      - Equipment behind enemy lines
      - Change configuration data
    - Jamming
      - Link attack
  - Intrusions/Accidents/natural disasters

NTNU
Norwegian University of
Science and Technology

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

[3] R.J. Ellison, D.A. Fischer, R.C. Linger, H.F. Lipson, T. Longstaff, and N.R.Mead. Survivable network systems: an emerging discipline. Technical report, Technical Report CMU/SEI-97-TR-013, November 1997, revised May 1999.

Laprie's View on Dependability and Survivability

Concept	Dependability	Survivability
Goal	1) Ability to deliver service that can justifiably be trusted 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)	Capability of a system to fulfill its mission in a timely manner
Threats present	1) design faults (e.g., software flaws, hardware errata, malicious logics) 2) physical faults (e.g., production defects, physical deterioration) 3) interaction faults (e.g., physical interference, input mistakes, attacks, including viruses, worms, intrusions)	1) failures (internally generated events due to, e.g., software design errors, hardware degradation, human errors, corrupted data) 2) attacks (e.g., intrusions, probes, denials of service) 3) accidents (externally generated events such as natural disasters)

[A. Avizienis, J. Laprie and B. Randell, Fundamental Concepts of Computer System Dependability, IARP/IEEE-RAS Workshop on Robot Dependability, Seoul, Korea, May 2001.

Software Engineering Institute, Carnegie Mellon

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

[3] R.J. Ellison, D.A. Fischer, R.C. Linger, H.F. Lipson, T. Longstaff, and N.R.Mead. Survivable network systems: an emerging discipline. Technical report, Technical Report CMU/SEI-97-TR-013, November 1997, revised May 1999.

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

[1] J. Knight and K. Sullivan, On the definition of survivability, TR-CS-00-33, University of Virginia, Dec., 2000.

[2] J. Knight, E. Strunk and K. Sullivan, Towards a Rigorous Definition of Information System Survivability, DISCEX 2003.

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.*

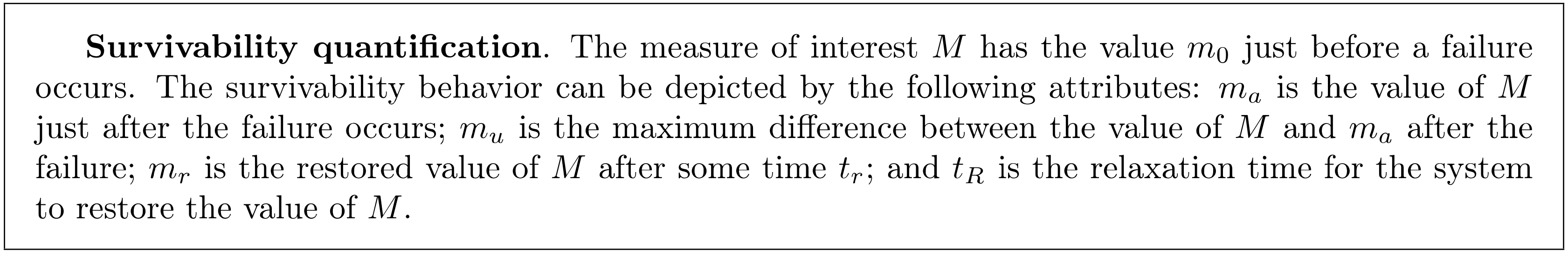
[1] Federal standard 1037C, Telecommunications: Glossary of telecommunication terms, 1996

[2] P. G. Neumann, Practical Architectures for Survivable Systems and Networks, SRI International, CA, 2000.

[3] R. J. Ellison et al, Survivable network systems: an emerging discipline, TR CMU/SEI-97-TR-013, Nov., 1997, revised May 1999.

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.

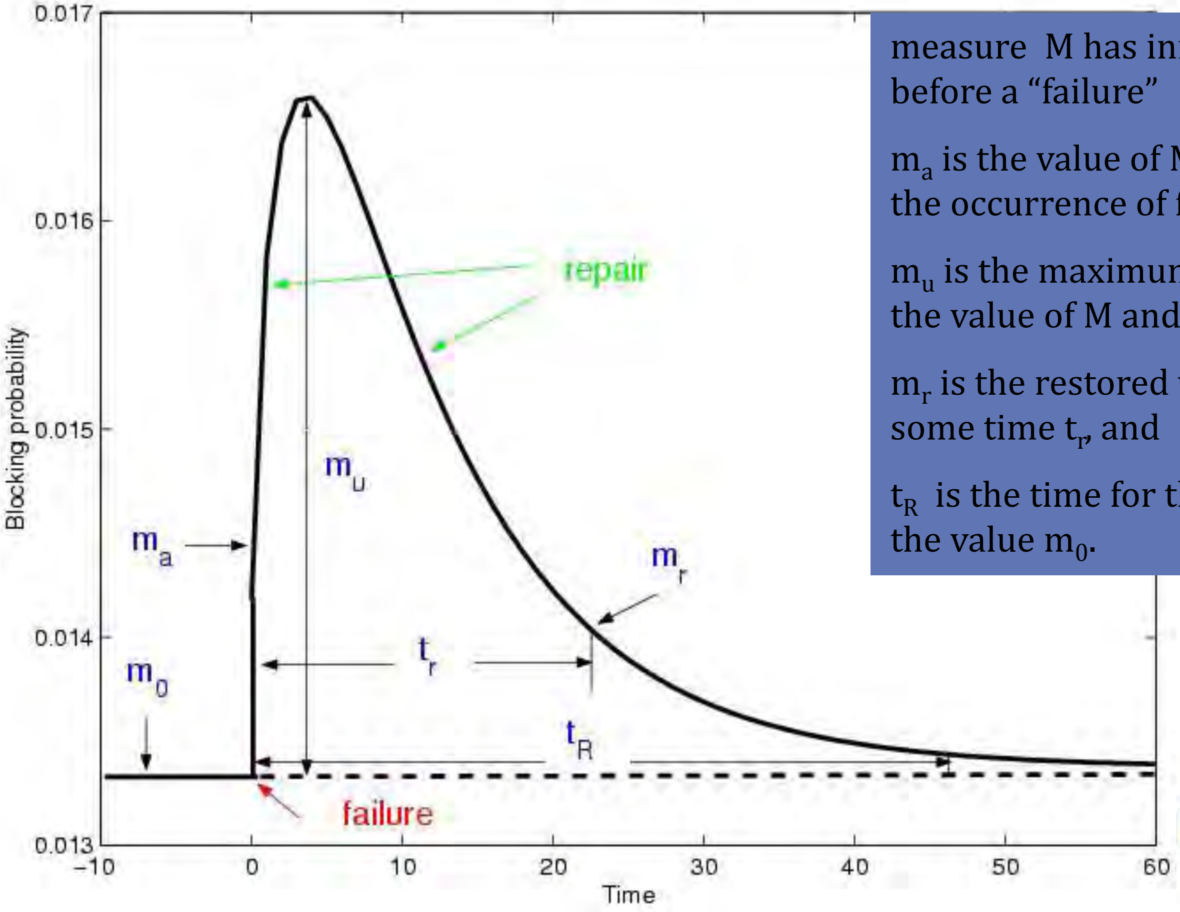


Survivability quantification. The measure of interest M has the value m_0 just before a failure occurs. The survivability behavior can be depicted by the following attributes: m_a is the value of M just after the failure occurs; m_u is the maximum difference between the value of M and m_a after the failure; 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.

[8] T1A1.2 Working Group on Network Survivability Performance, Technical report on enhanced network survivability performance, Feb., 2001.

Quantitative Definition of Survivability



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

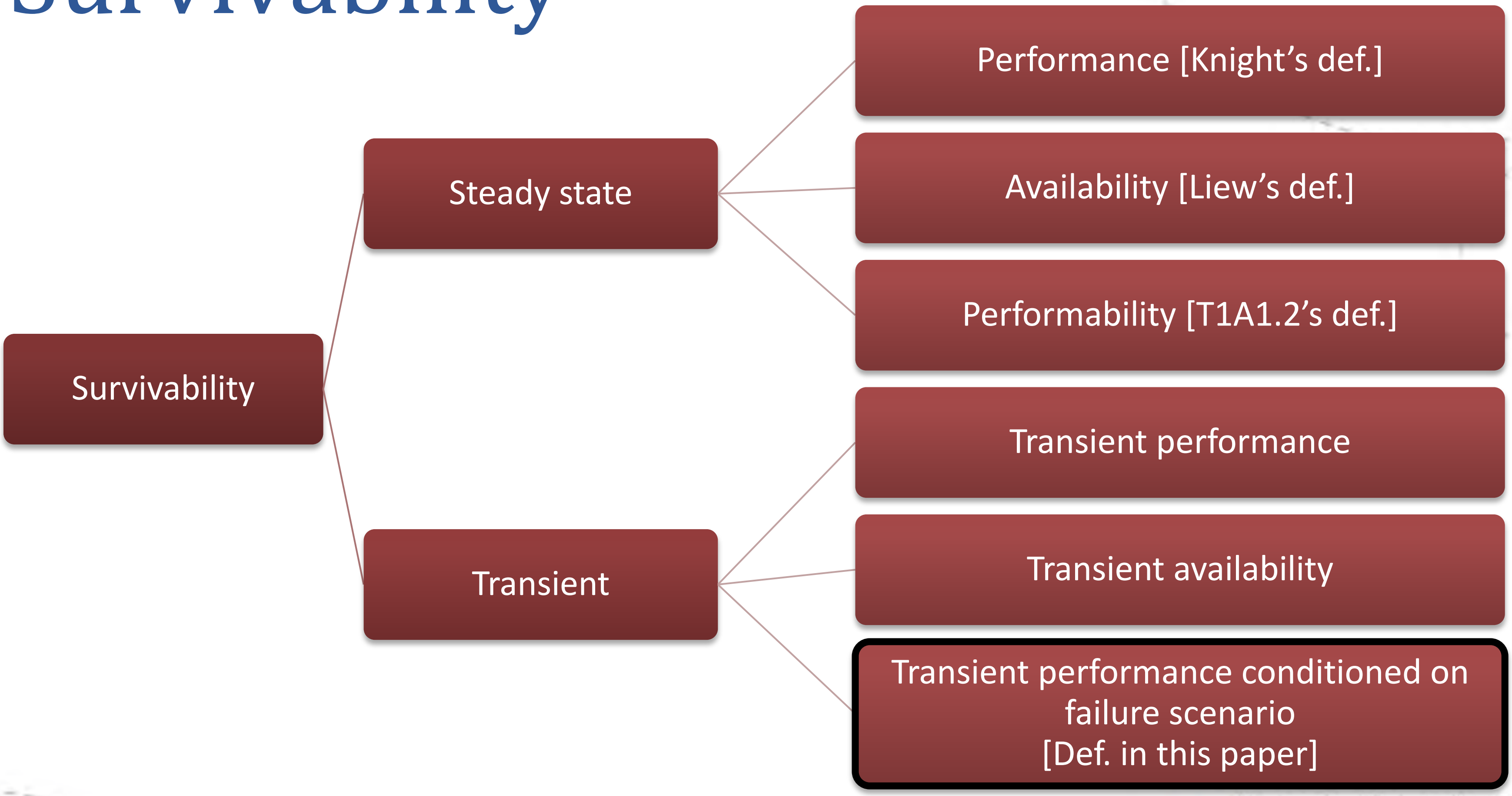
m_a is the value of M immediately after the occurrence of failure,

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



Survivability

Steady state

Transient

Performance [Knight’s def.]

Availability [Liew’s def.]

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

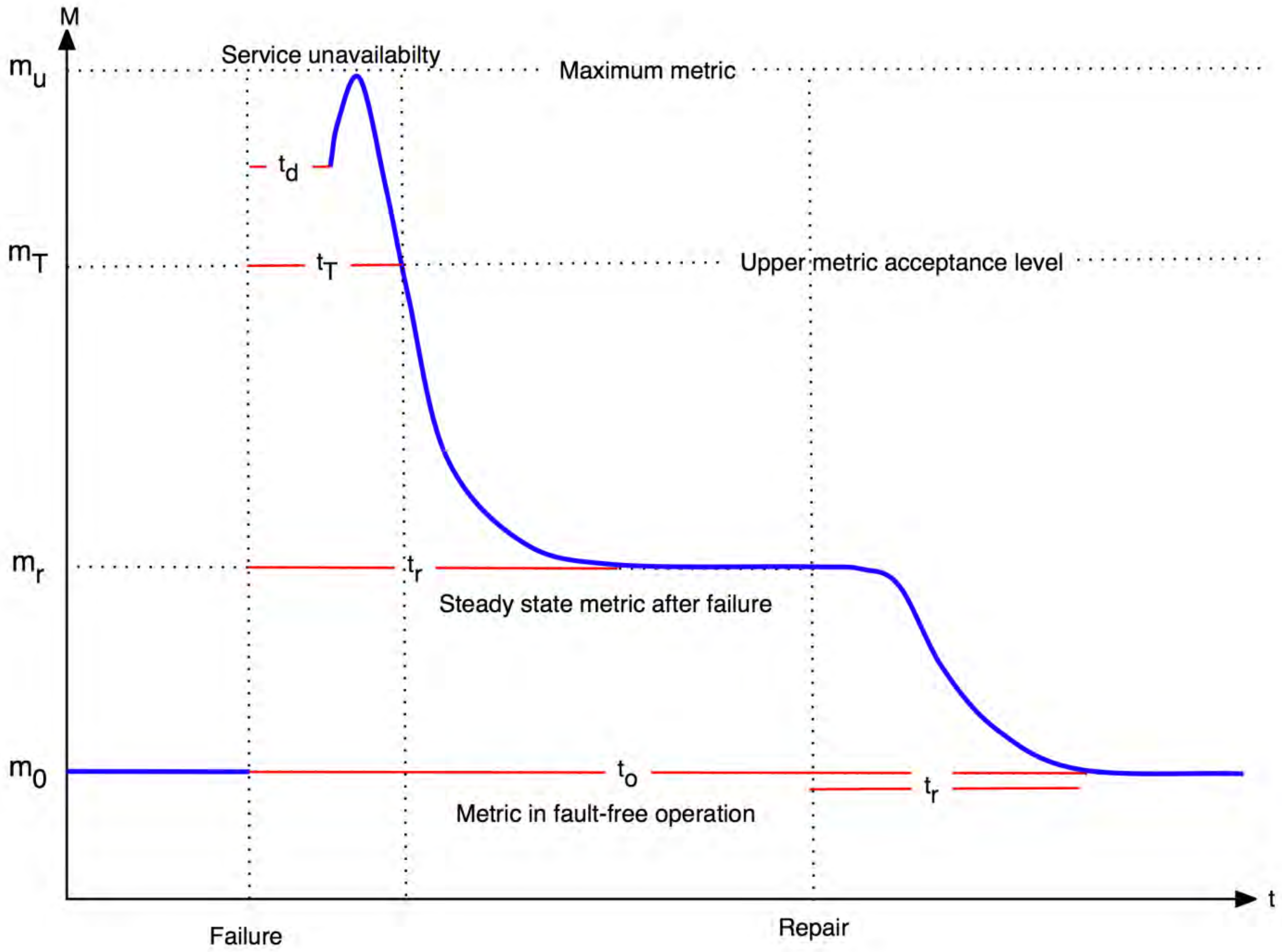
Survivability Research at Duke University and NTNU

- Publications
  - **Poul E. Heegaard and Kishor Trivedi. "Network Survivability Modeling". Computer Networks, Volume 53, Issue 8 (2009), pp. 1215-1234. Elsevier.**
  - Poul E. Heegaard and Kishor Trivedi. "Survivability Quantification of Communication Services". In proceedings from The 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2008). June 24-27, 2008, Anchorage, AK, USA, pp 462-471.
  - Transient behavior of ATM networks under overloads IEEE INFOCOM' 96, pages 978–985, San Francisco, CA, March 1996.
  - Network survivability performance evaluation: a quantitative approach with applications in wireless ad-hoc networks ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM' 02), Atlanta, GA, September 2002.
  - A general framework of survivability quantification Proc. of l2th GI/ITG. Conf. On Measuring, Modelling and Evaluation of Computer and Communication Systems (MMB'04)
  - Survivability analysis of telephone access network Proc. of 15th IEEE International Symposium on Software Engineering (ISSRE'04)

NTNU
Norwegian University of Science and Technology

II. Network survivability modeling and quantification

Network survivability quantification



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

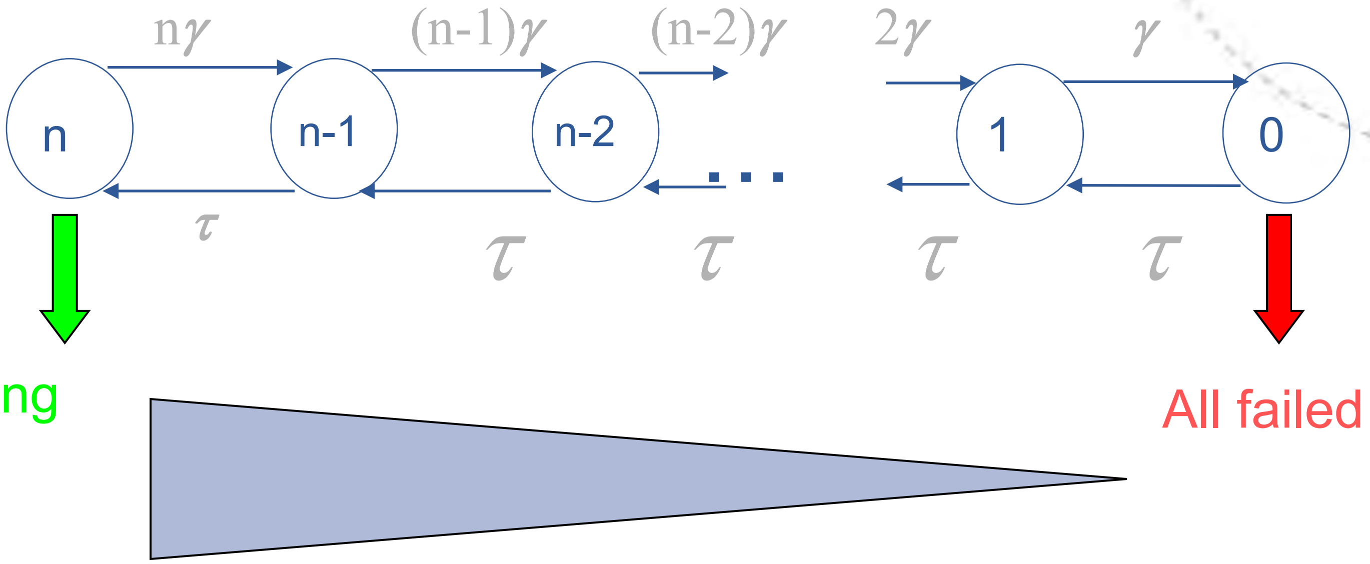
A General Quantification Procedure

- 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 $Exp(\lambda)$
  - Call holding time $Exp(\mu)$
  - Time to failure $Exp(\gamma)$
  - Time to repair $Exp(\tau)$
  - Single repair facility

Pure Availability Model



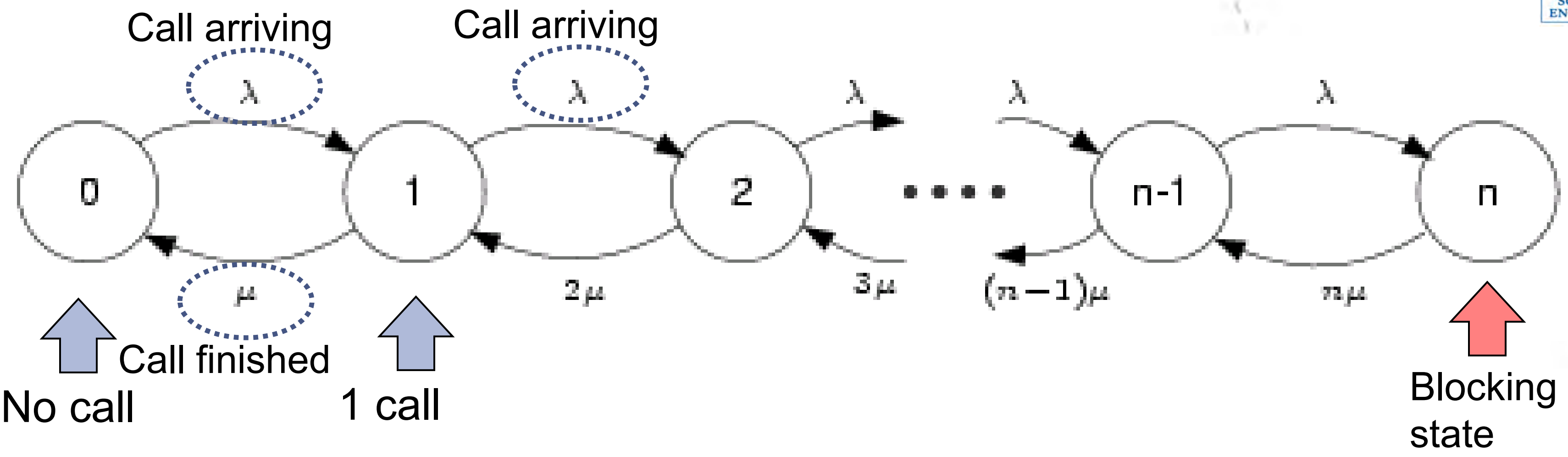
Resource degradation

$$\pi_i^A = \frac{\left(\frac{\tau}{\gamma}\right)^i / i!}{\sum_{k=0}^{n} \left(\frac{\tau}{\gamma}\right)^k / k!}$$

n=25, γ=0.002 s^{-1}, τ=0.1 s^{-1}

NTNU
Norwegian University of Science and Technology

Pure Performance Model



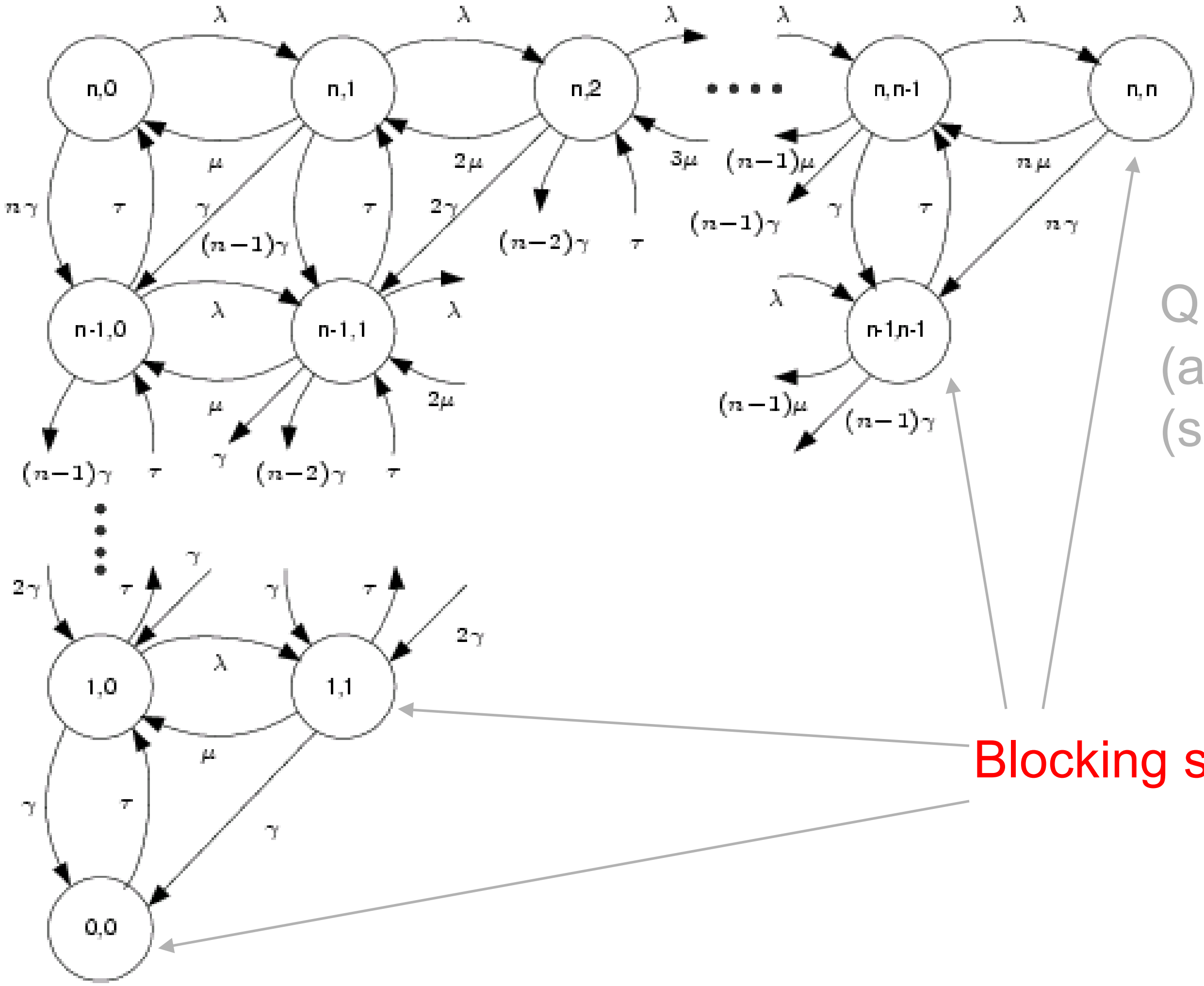
Steady state closed-form solution:
Erlang B Formula

$$\pi_j^P = \frac{\left(\frac{\lambda}{\mu}\right)^j / j!}{\sum_{k=0}^{n} \left(\frac{\lambda}{\mu}\right)^k / k!}$$

Blocking probability: $P_{bk} = \pi_n^P$

n=25, λ=5 s^{-1}, μ=0.3 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
  - $P_{bk}' = \sum_{k=0}^{n} \pi_{k,k}^C = 0.020178$

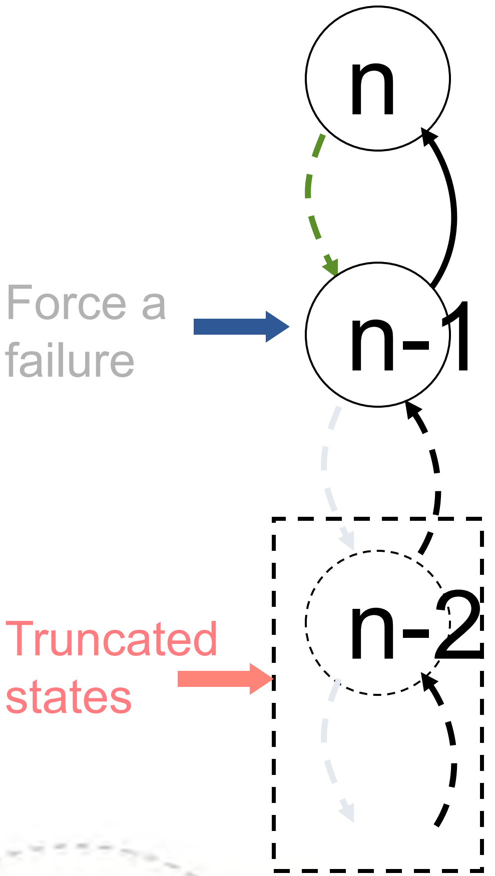
NTNU

Norwegian University of Science and Technology

Survivability Quantification Approach

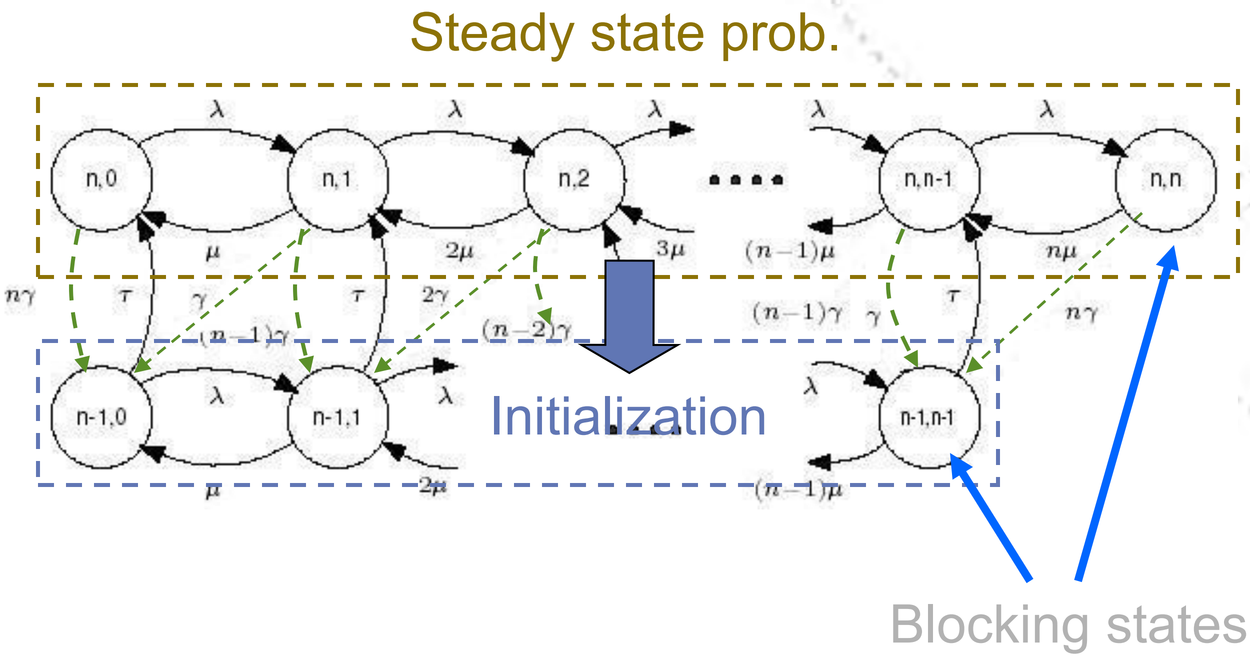
- System operating in steady state
- Force a failure:
  - Initial state probabilities for the degraded mode states
  - Transient solution of the truncated performability model

Truncated Performability Model



Force a failure

Truncated states



Steady state prob.

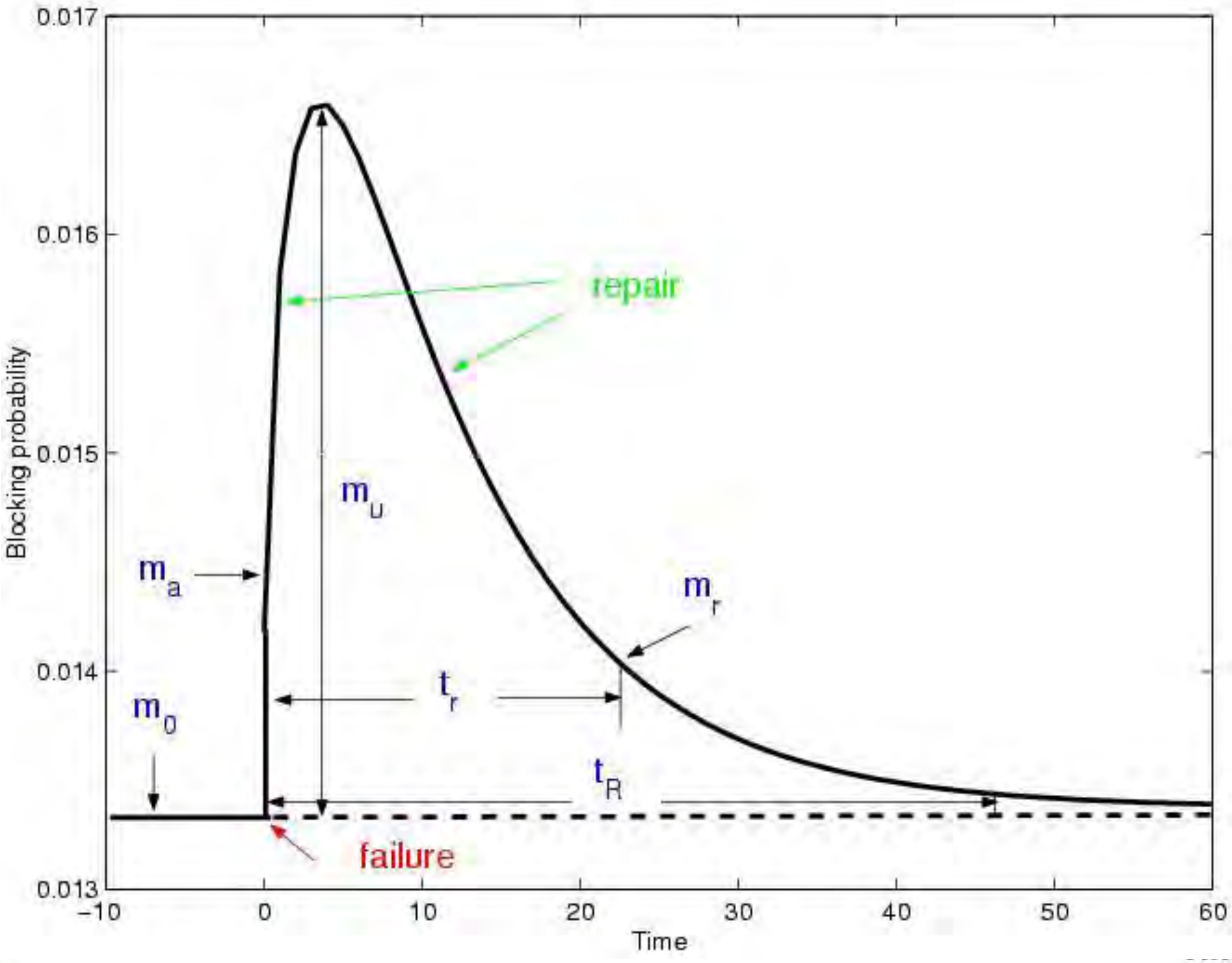
Initialization

Blocking states

(forced) Failure transitions

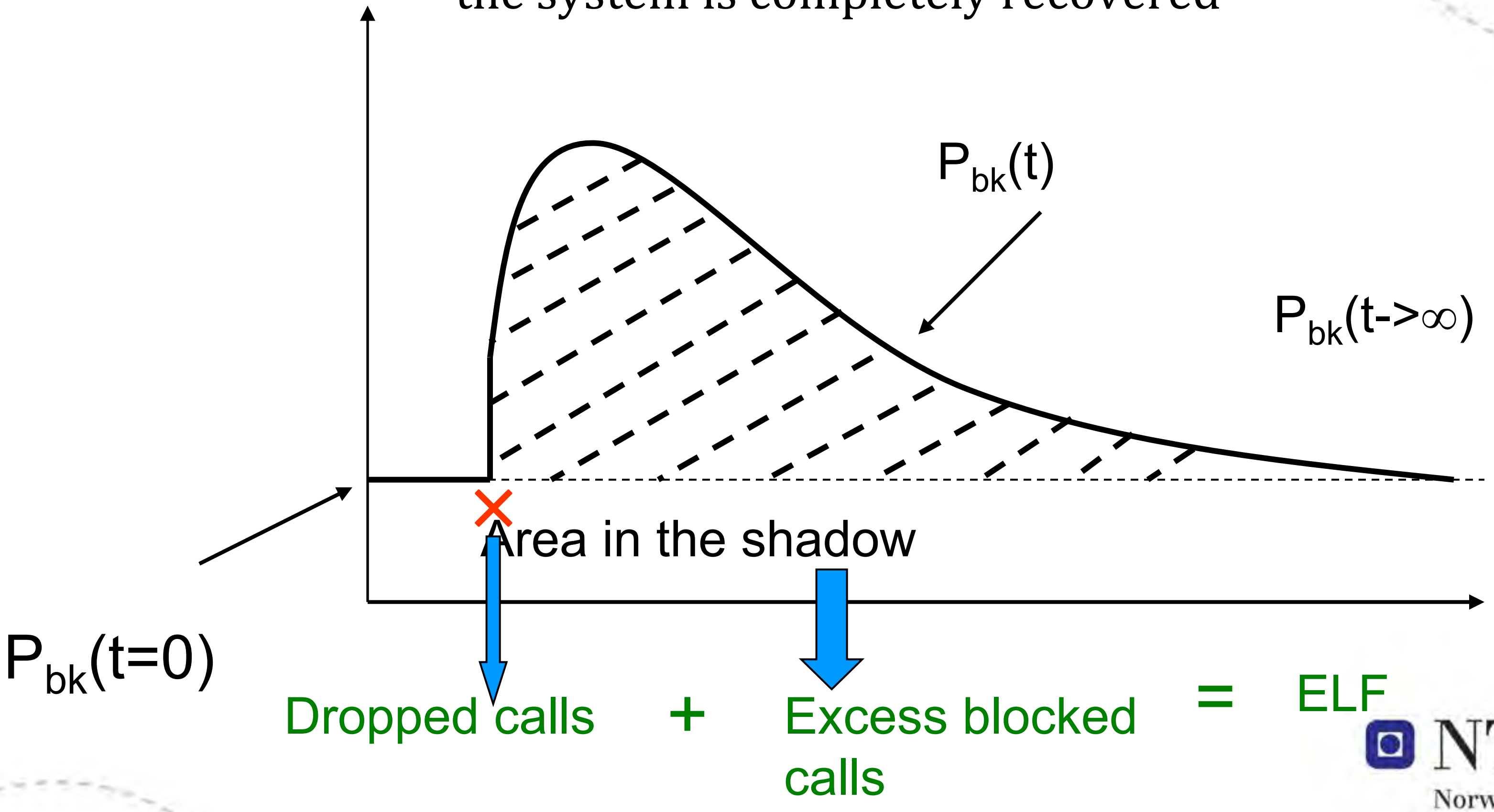
NTNU
Norwegian University of Science and Technology

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



ELF results

Relaxation time*	Call loss due to the 1st failure N_d	Extra call loss due to blocking N_b	ELF
39s	0.6557	0.2457	0.9014

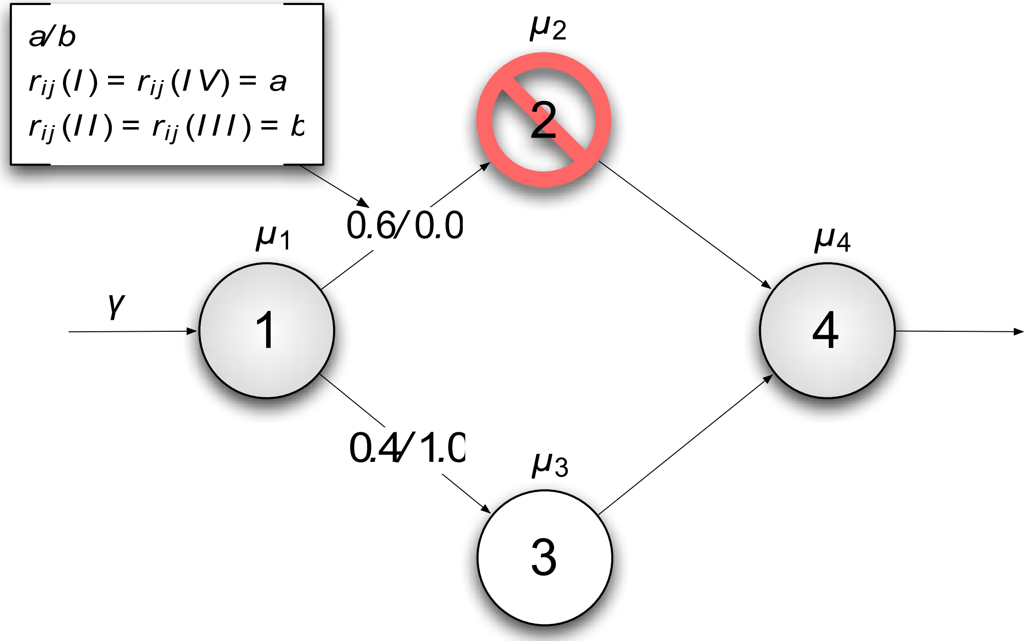
$$N_d = \frac{j}{n}\pi_j^P .$$

$$N_b = \int_0^{t_R} \left(P_{bk}(t) - P_{bk}(t \to \infty)\right)\lambda \, dt$$

*: 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



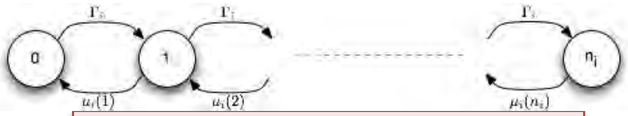
Network with 4 nodes: Approaches

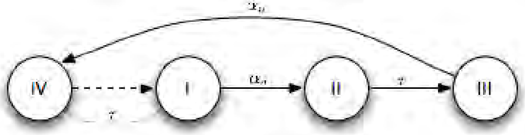
- Simulation
  - DEMOS/Simula
  - Discrete event, process-oriented simulation model
- Analytical
  - SRN: Stochastic Reward Networks
    - Full CTMC, same as simulation model
    - Solved by SPNP and SHARPE
  - CTMC: (Decomposed) Markov models
    - Combined performance and dependability model
    -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



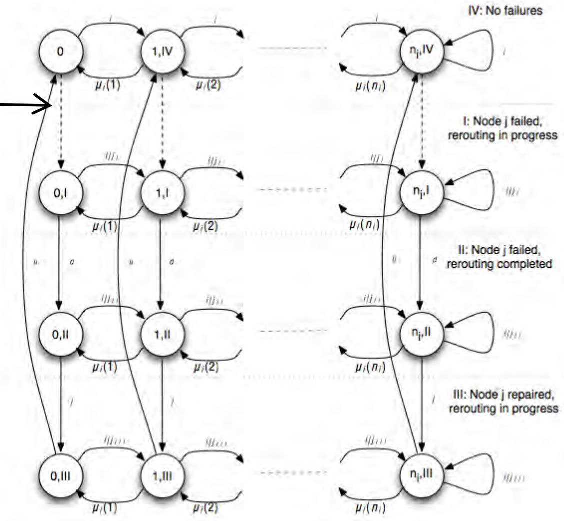


Performance model

Phased recovery model

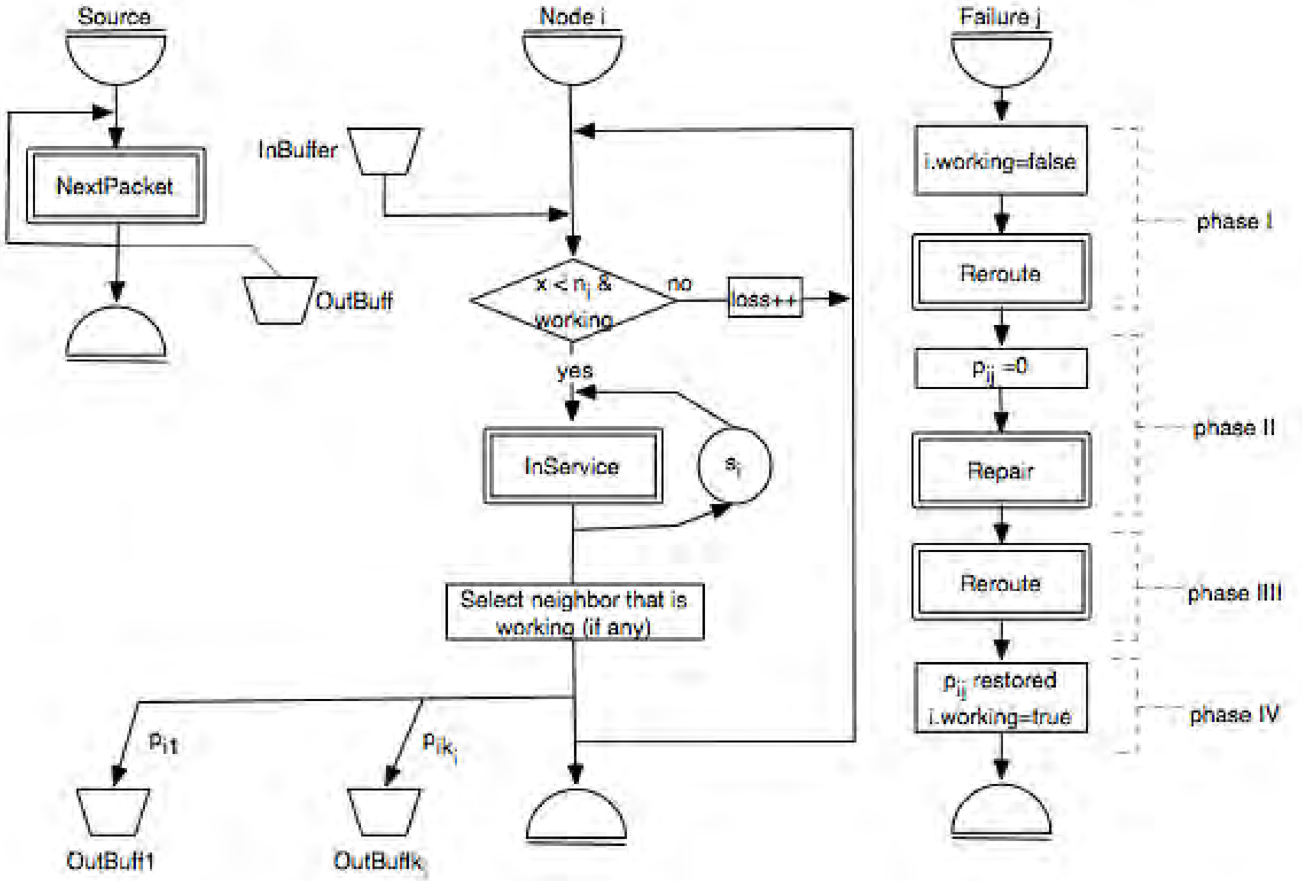
*

Composite performability model


0
1,IV
n_j,IV
0,I
1,I
n_j,I
0,II
1,II
n_j,II
0,III
1,III
n_j,III
μ_j(1)
μ_j(2)
μ_j(n_j)
IV: No failures
I: Node j failed, rerouting in progress
II: Node j failed, rerouting completed
III: Node j repaired, rerouting in progress

Survivability model

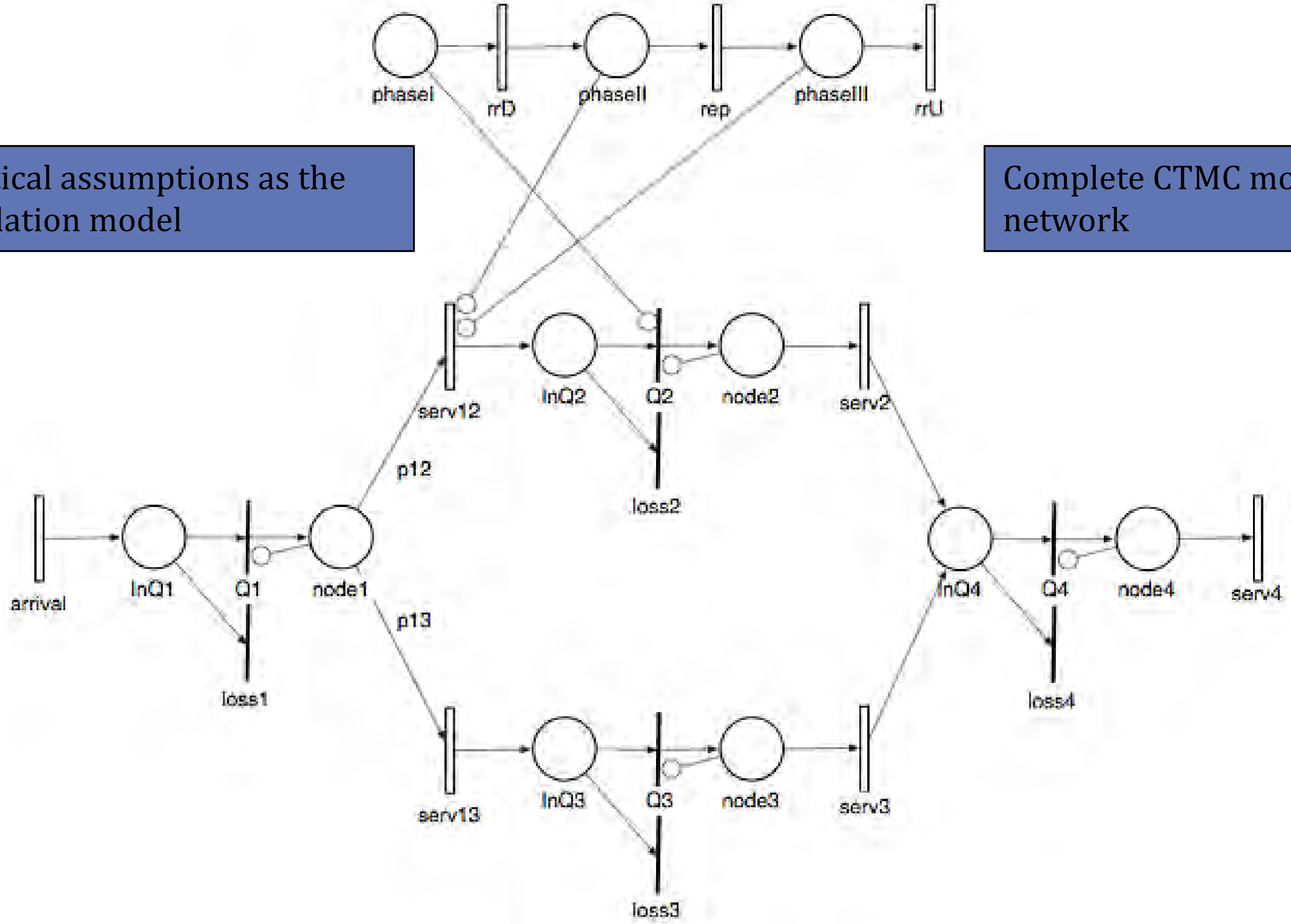
Network with 4 nodes: Simulation model



Network with 4 nodes: Stochastic Reward Net model

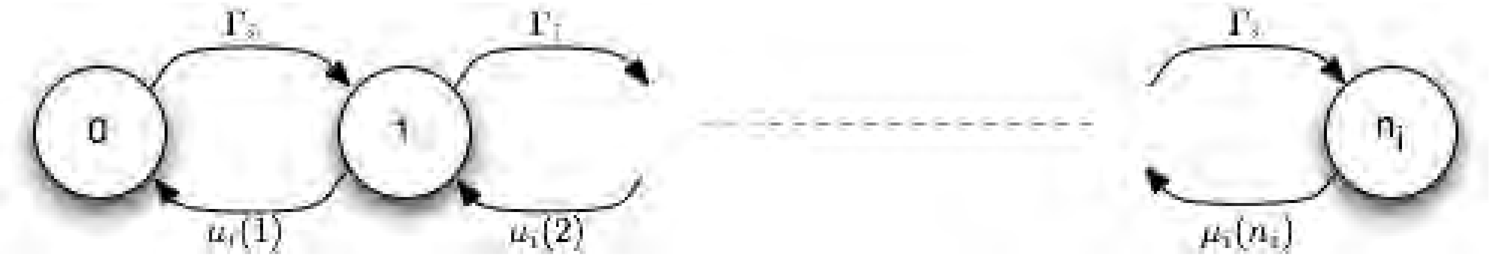
Identical assumptions as the simulation model

Complete CTMC model of network



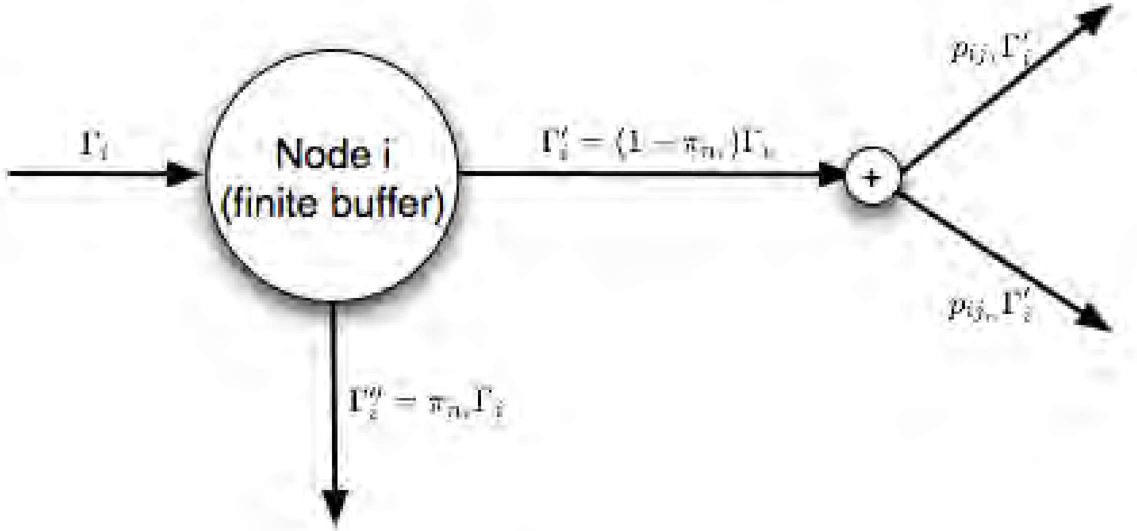
Network with 4 nodes: CTMC Performance model

- 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

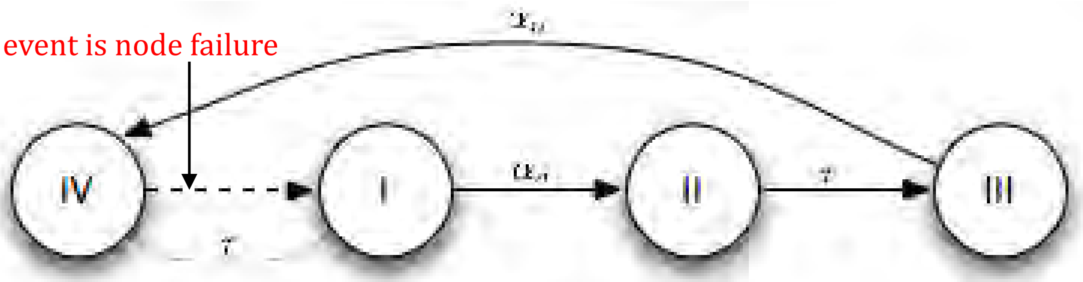
- Assume acyclic graph from SRC to DST



NTNU
Norwegian University of Science and Technology

Network failure and rerouting

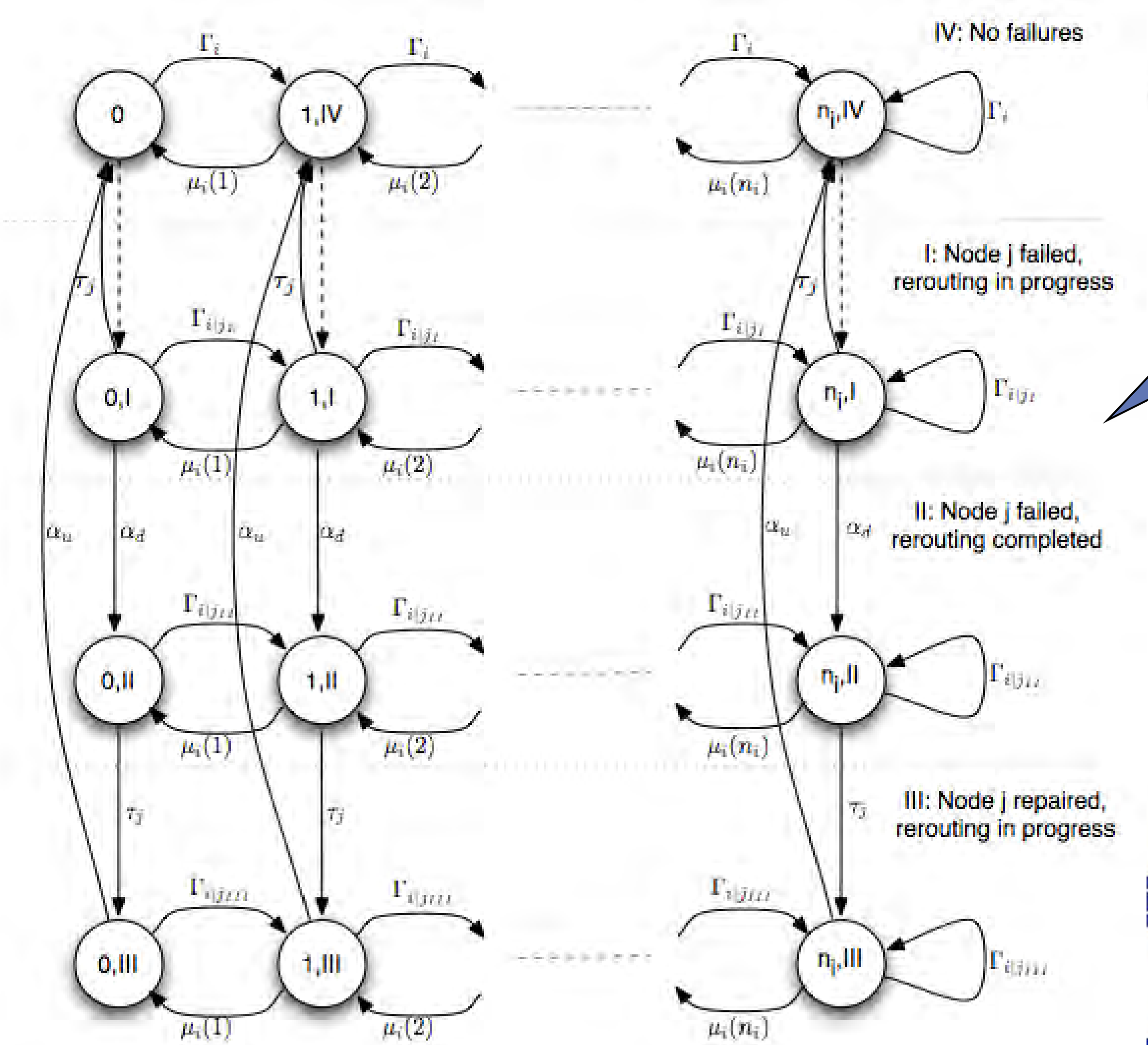
- Phase I:
  - Rerouting after failure is $T_D \sim \exp(\alpha_D)$
- Phase II:
  - Restoration time is $T_R \sim \exp(\tau)$
- Phase III
  - Rerouting after failure is $T_U \sim \exp(\alpha_U)$



Undesired event is node failure

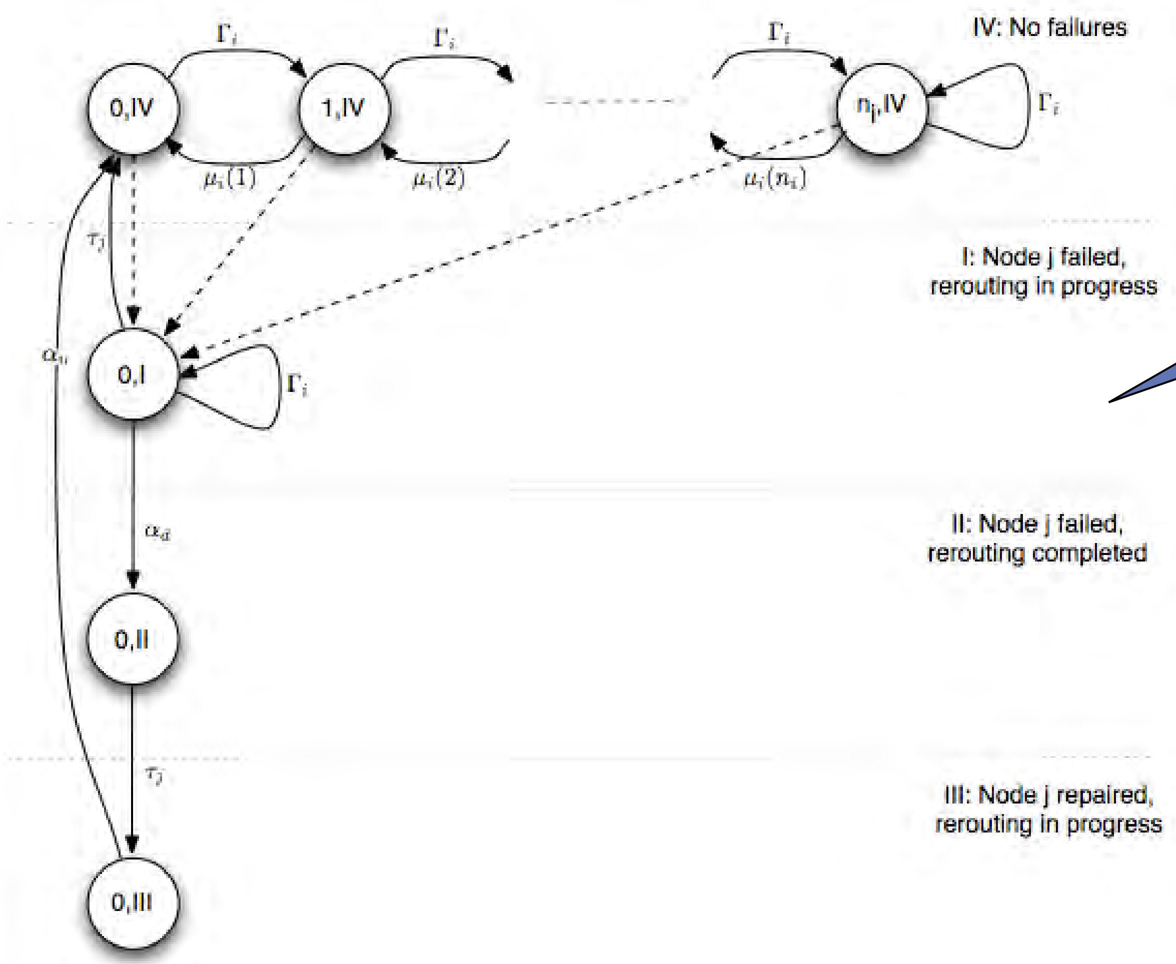
NTNU
Norwegian University of Science and Technology

CTMC: Combine models



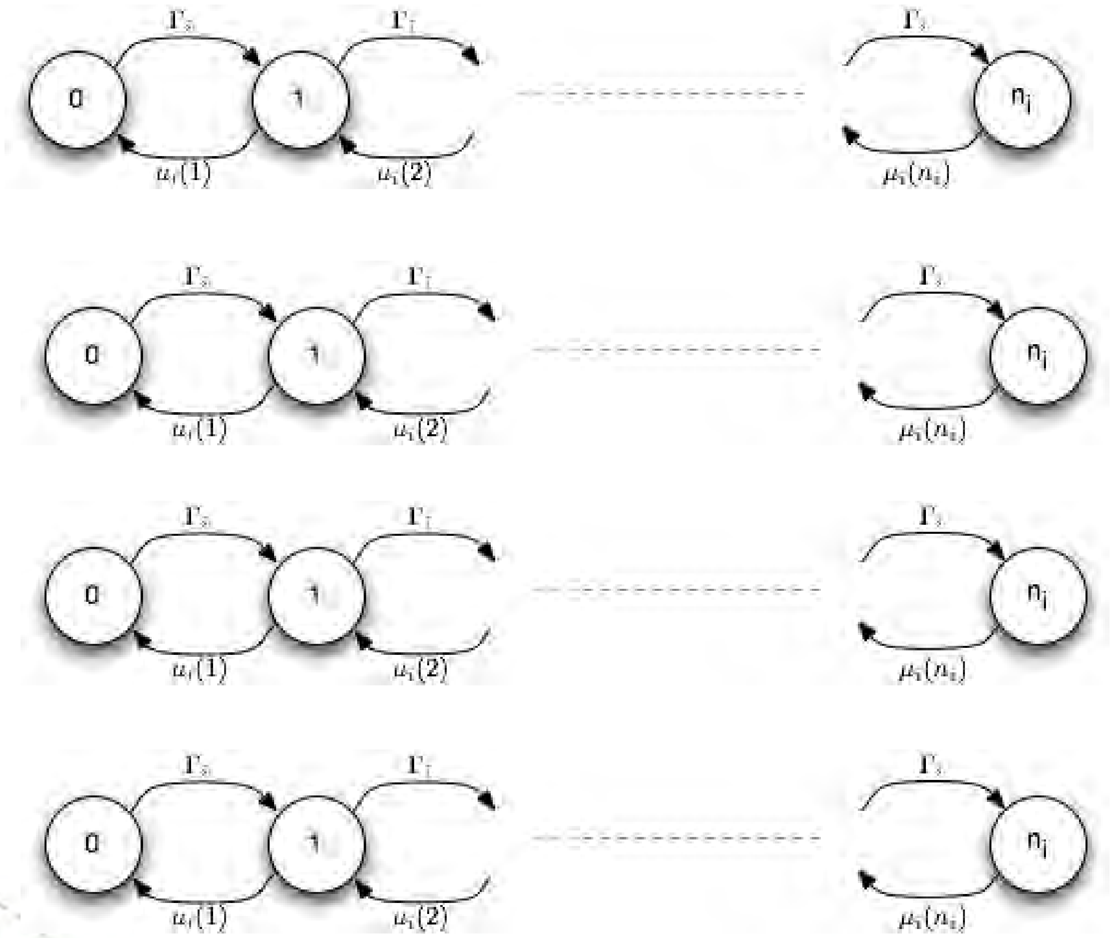
Non-failed node

CTMC: Combine models

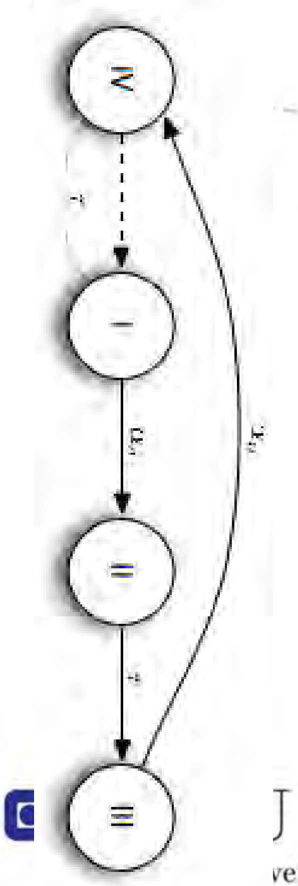


Failed node

CTMC: Combine models



*



versity of
Science and Technology

CTMC: Combine models

- Number of states in combined model
  - Transient solution of N_{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_{res} states and one with N_{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
  - $P_k(t;x,i) = \pi_k(x)*p(t,i)$,

  where state $x=1,\ldots n_k$, phase $i=I,\ldots,IV$

Performance metrics

- Packet loss,

$$l_k(t) = \sum_{i=I}^{IV} \pi_k(n)\mathrm{RL}_k(n,i)p(t,i)$$

- Throughput,

$$l(t) = \sum_{k=1}^{N_{node}} l_k(t)/\Gamma_s$$

$$\rho(t) = 1 - l(t)$$

Performance metrics

- Delay,

$$\mathrm{EN}_k(t) = \sum_{i=1}^{IV} \mathrm{RD}_k(x,i)\pi_k(x)p_k(t,i)$$

$$d(t) = \sum_{k=1}^{N_{node}} \mathrm{EN}_k(t)/\Gamma_s$$

Rewards in Markov model

- Reward

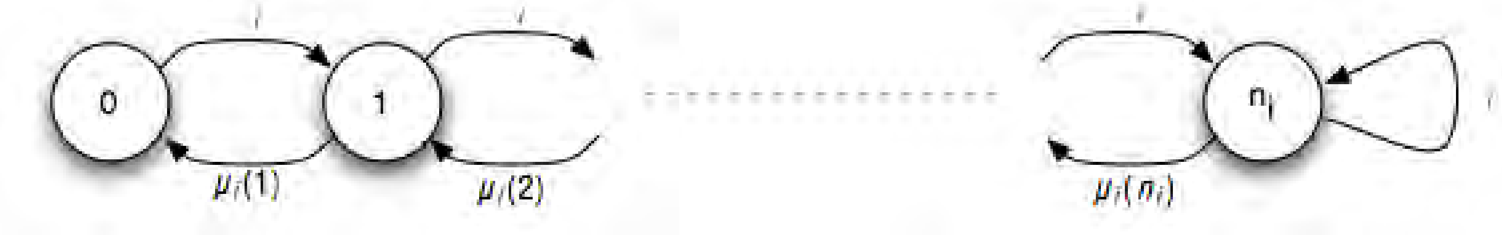
  $R_k(x,i); k=1,\cdots,N_{\text{node}}, x=0,\cdots N_{\text{res}}, i=I,\cdots,IV$

- Reward packet loss
  - $\text{RL}_k(x,i)=0$ for all states and phases except
    - for each node and all phases i: $\text{RL}_k(N_{\text{res}},i)=\Gamma_k$
    - for all states in phase I of the failed node $\text{RL}_k(x,I)=\Gamma_k$
- Reward delay: (Number in system+Little)
  - $\text{RD}_k(x,i)=x$ for all states and phases except

    for the failed node $\text{RD}_k(x,i)=0; i=I,II,III$

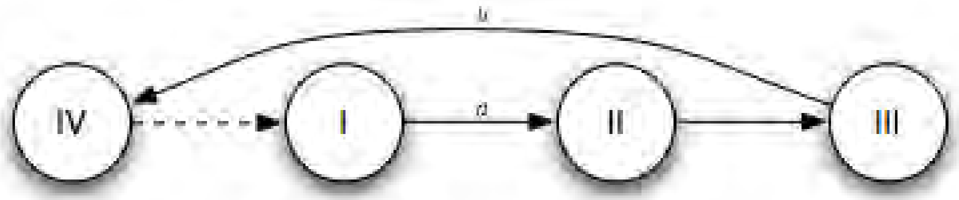
NTNU
Norwegian University of Science and Technology

CTMC model of each node



Performance model

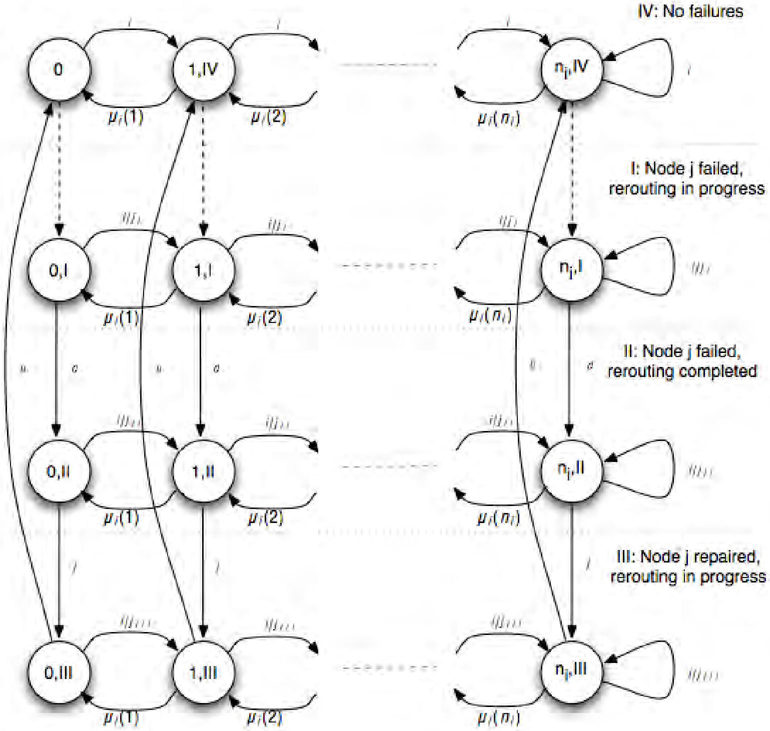
Assume product form solution (Jackson)



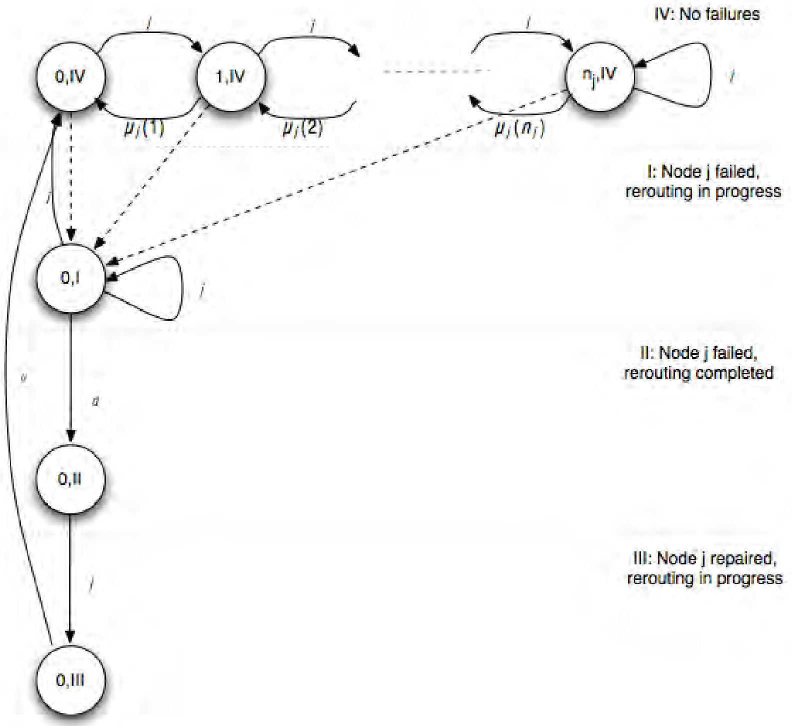
Availability model

CTMC model of each node

Survivability models



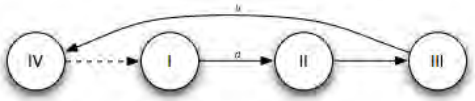
Non-failed node


IV: No failures
0,IV
1,IV
n_j,IV
$\mu_j(1)$
$\mu_j(2)$
$\mu_j(n_j)$
I: Node j failed, rerouting in progress
0,I
II: Node j failed, rerouting completed
0,II
III: Node j repaired, rerouting in progress
0,III

Failed node

Closed form solution

- Assume product form solution (Jackson Network)
- Determine steady state performance of each phase, $p_{j,i}$
  - I. Immediately after a failure
  - II. Rerouting completed after failure
  - III. Restoration/repair done
  - IV. 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



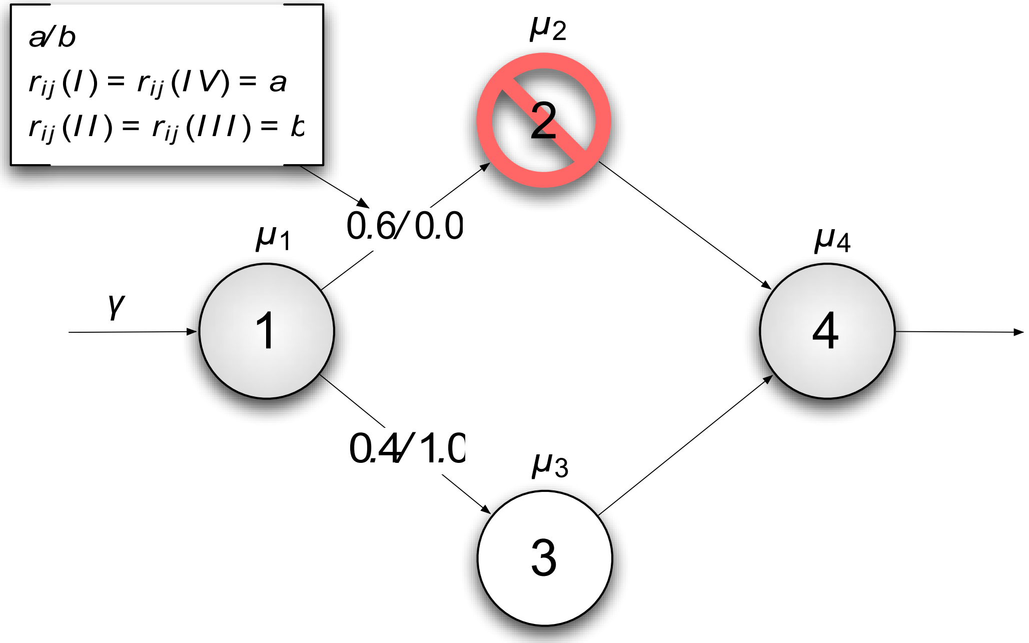
Transient reward: $R(t)=\Sigma_j \Sigma_i \; p_{j,i} \; r_{j,i} p_i \; (t)$

Solving the models

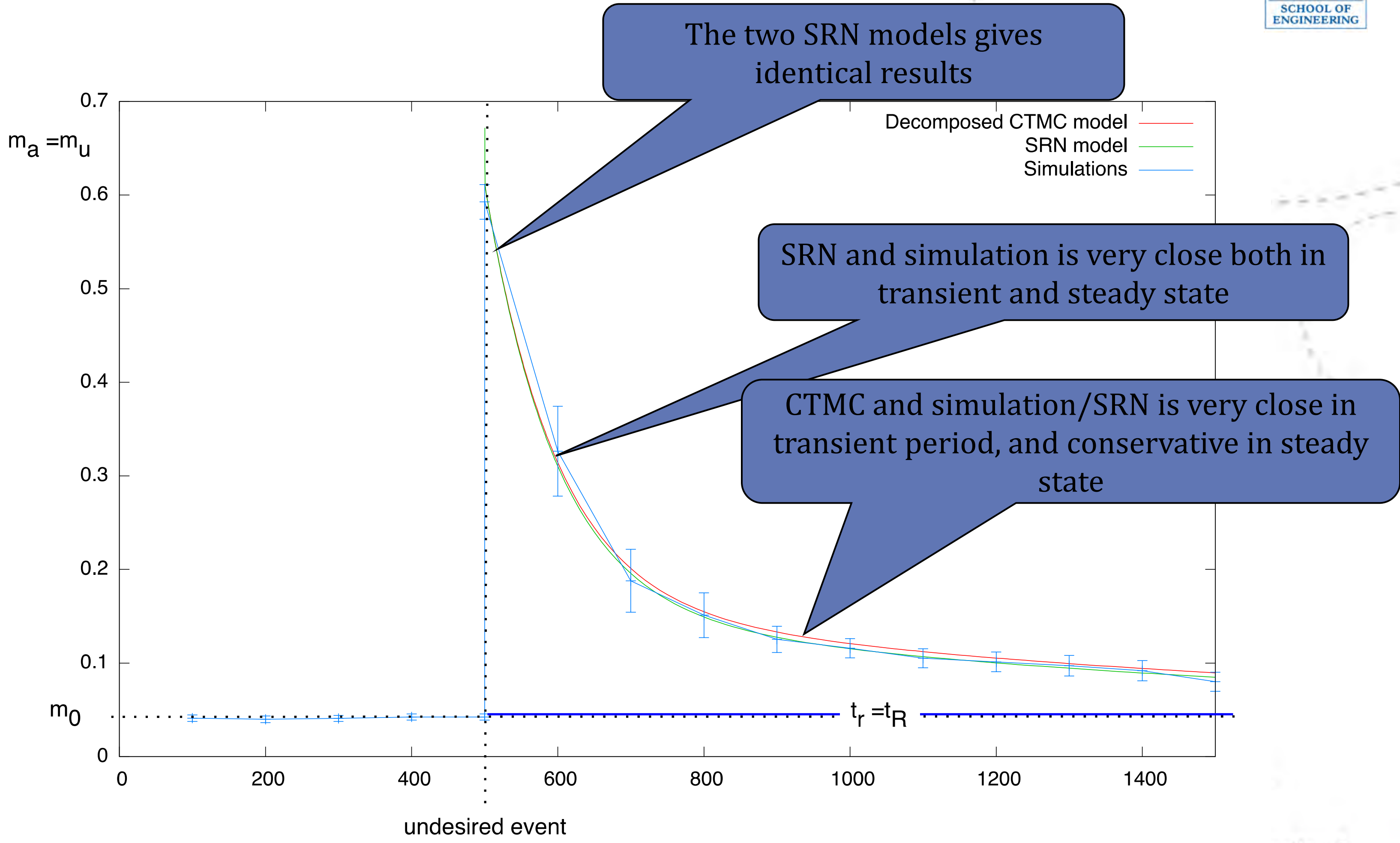
- SRN
  - Transient solution of model with $N_{\text{node}} \times N_{\text{res}} \times N_{\text{phase}}$ states
- Depomposed CTMC
  - Transient solution of N_{node} models with $N_{\text{res}} \times N_{\text{phase}}$ states
- Depomposed CTMC
  - Steady state solution of $N_{\text{node}} \times N_{\text{phase}}$ models with N_{res} states
  - Transient solution of one model with N_{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



Network with 4 nodes: loss ratio

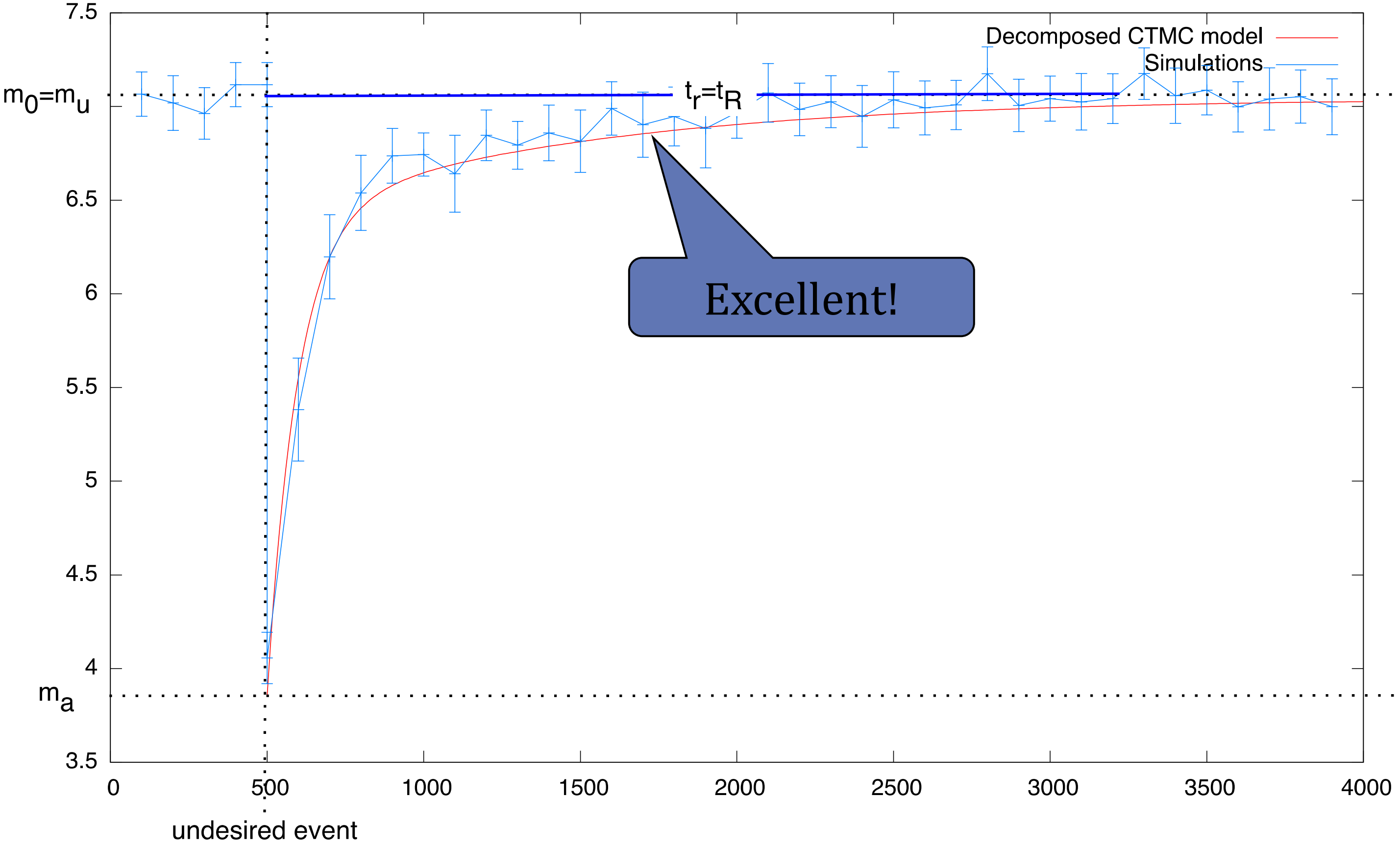


The two SRN models gives identical results

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



III. Case studies

COURTESY: DURHAM CONVENTION AND VISITORS BUREAU

© 1998 Vadim Makarov www.vadi.com

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

Class 2
Sectional

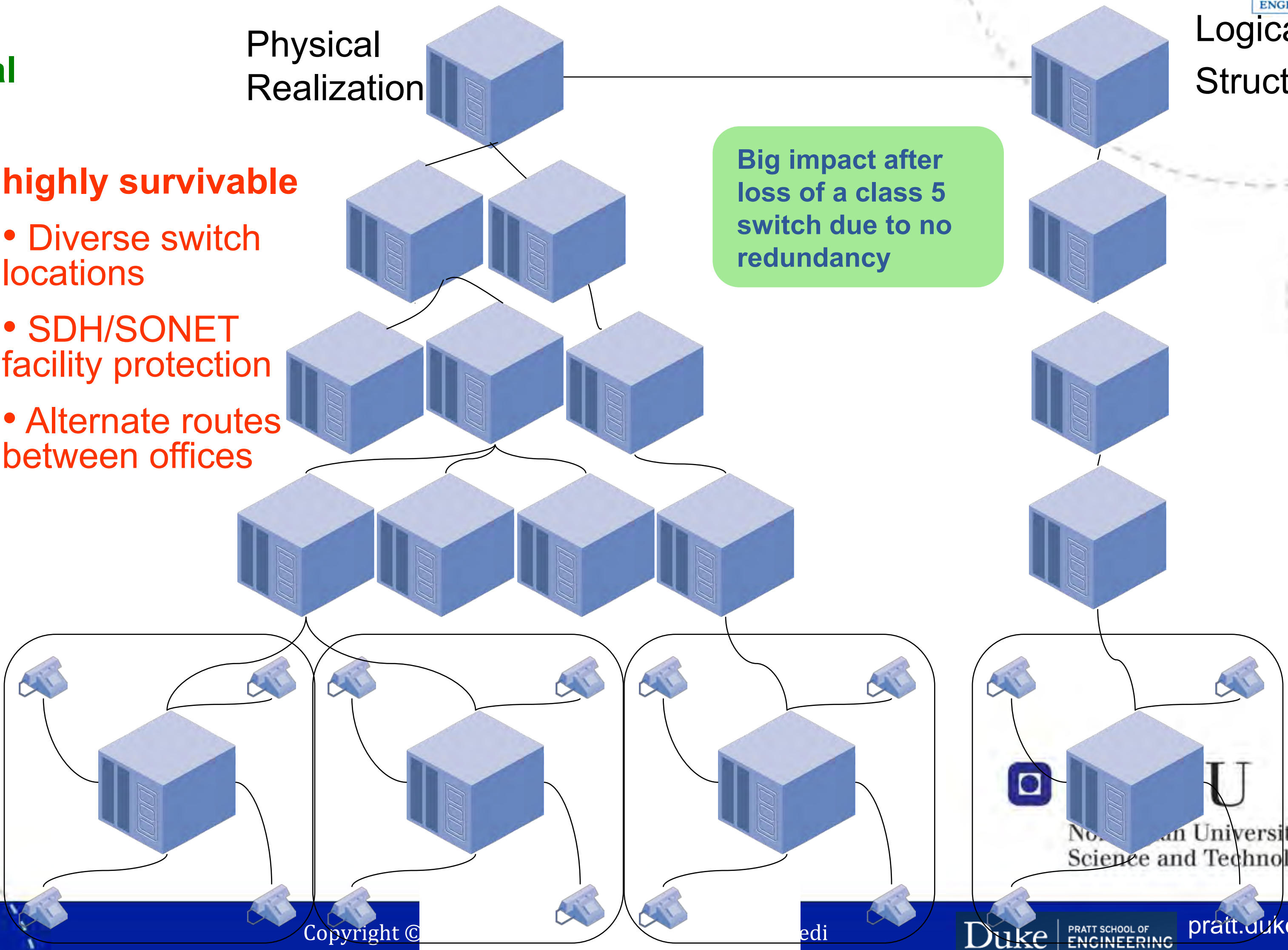
Class 3
Primary

Class 4 Toll

Class 5
Local

highly survivable

- Diverse switch locations
- SDH/SONET facility protection
- Alternate routes between offices



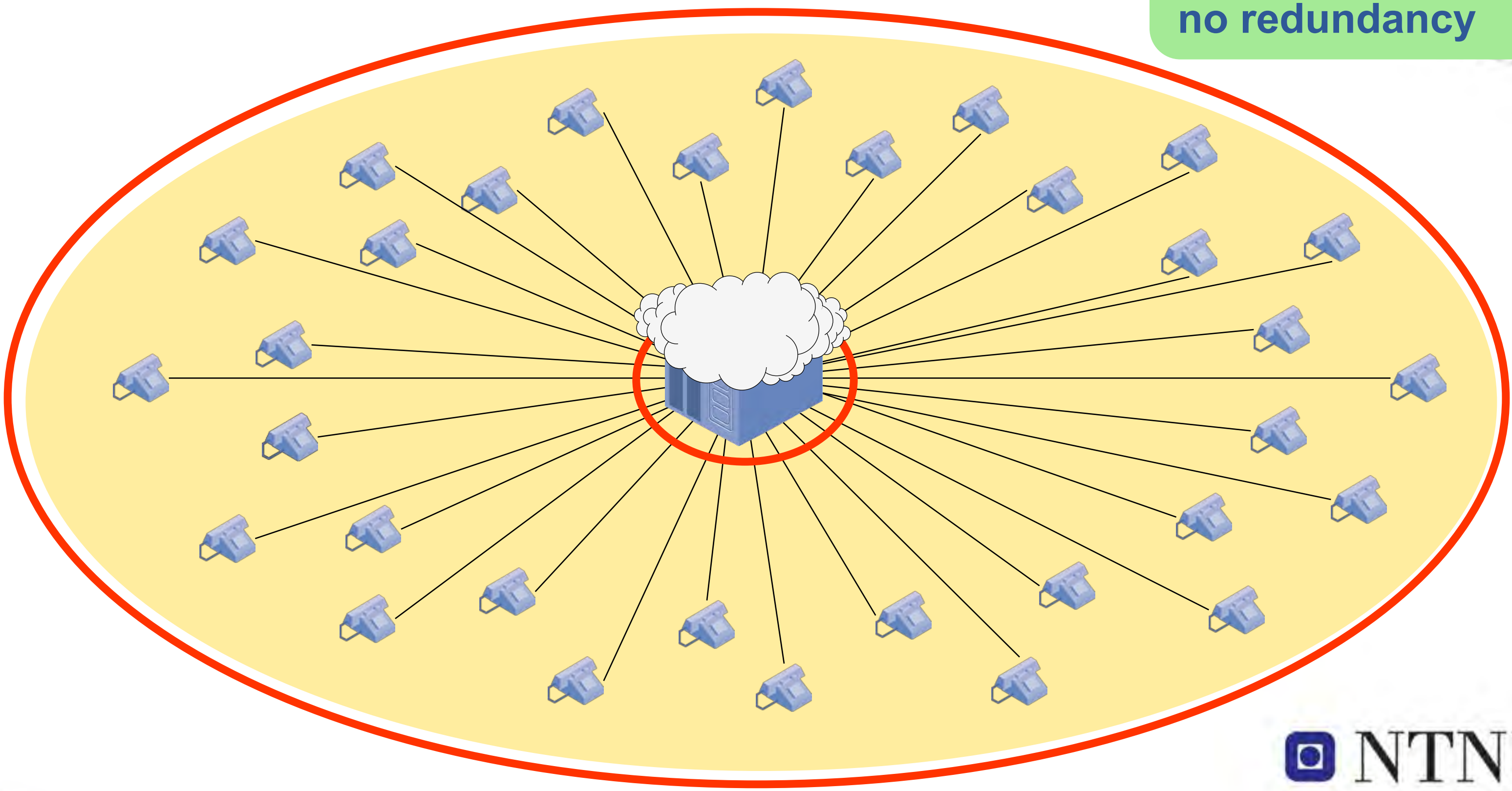
Physical Realization

Logical Structure

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

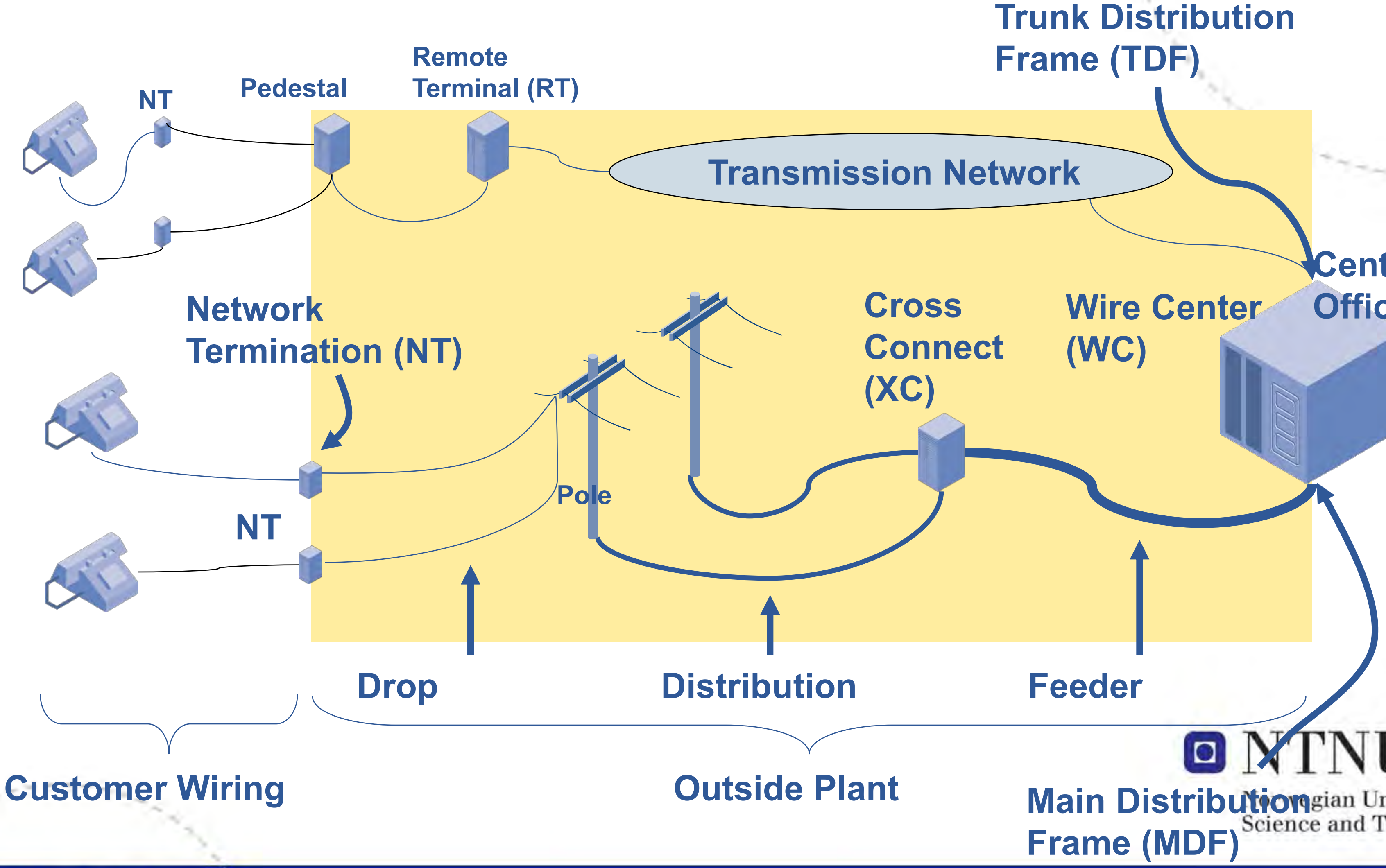


10,000 or more pair of wires meet at a single point

NTNU
Norwegian University of Science and Technology

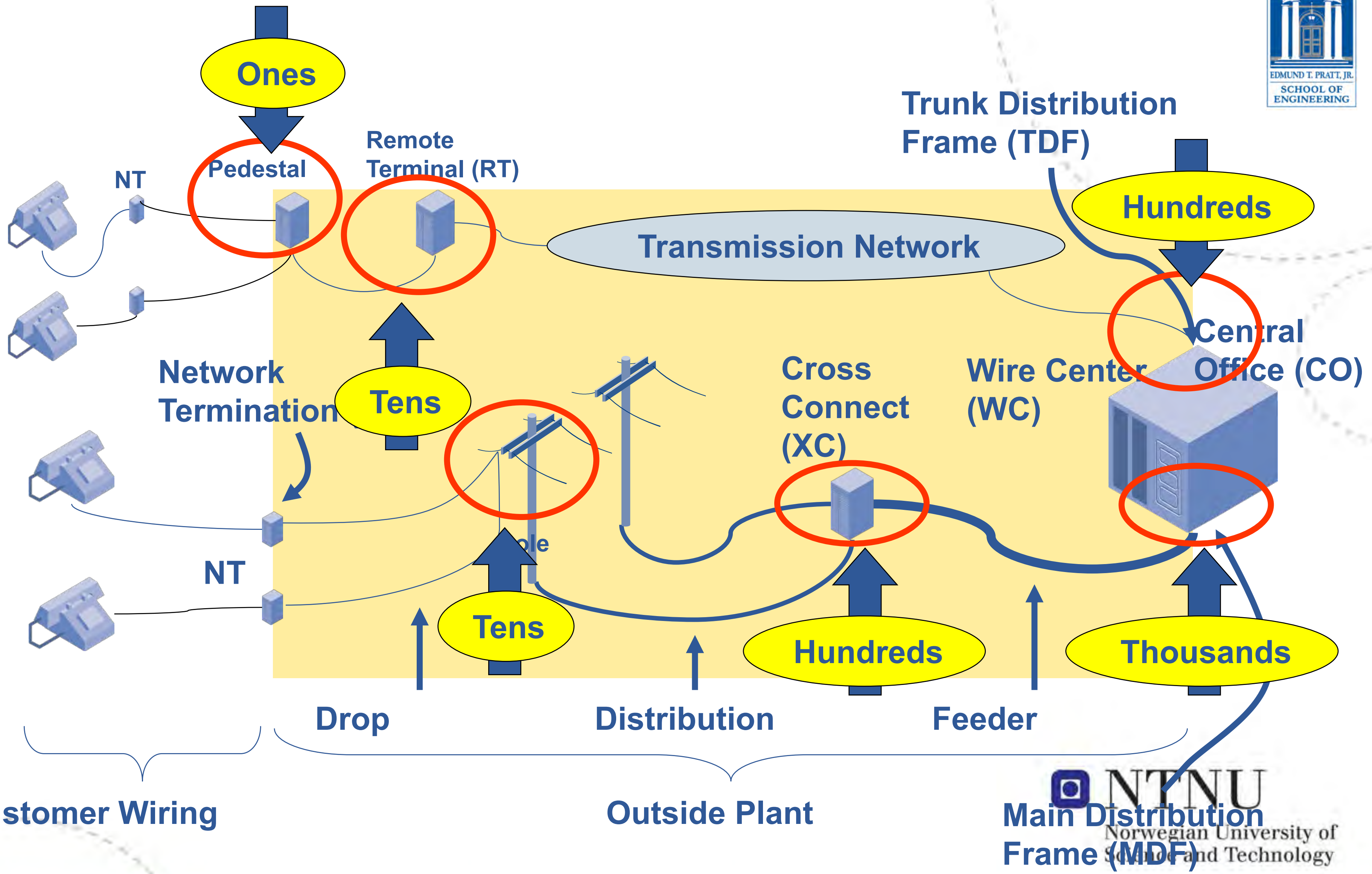
Telephony terms

LAU	Line Access Unit
CSU	Call Processing Unit
HPU	Central Host Unit



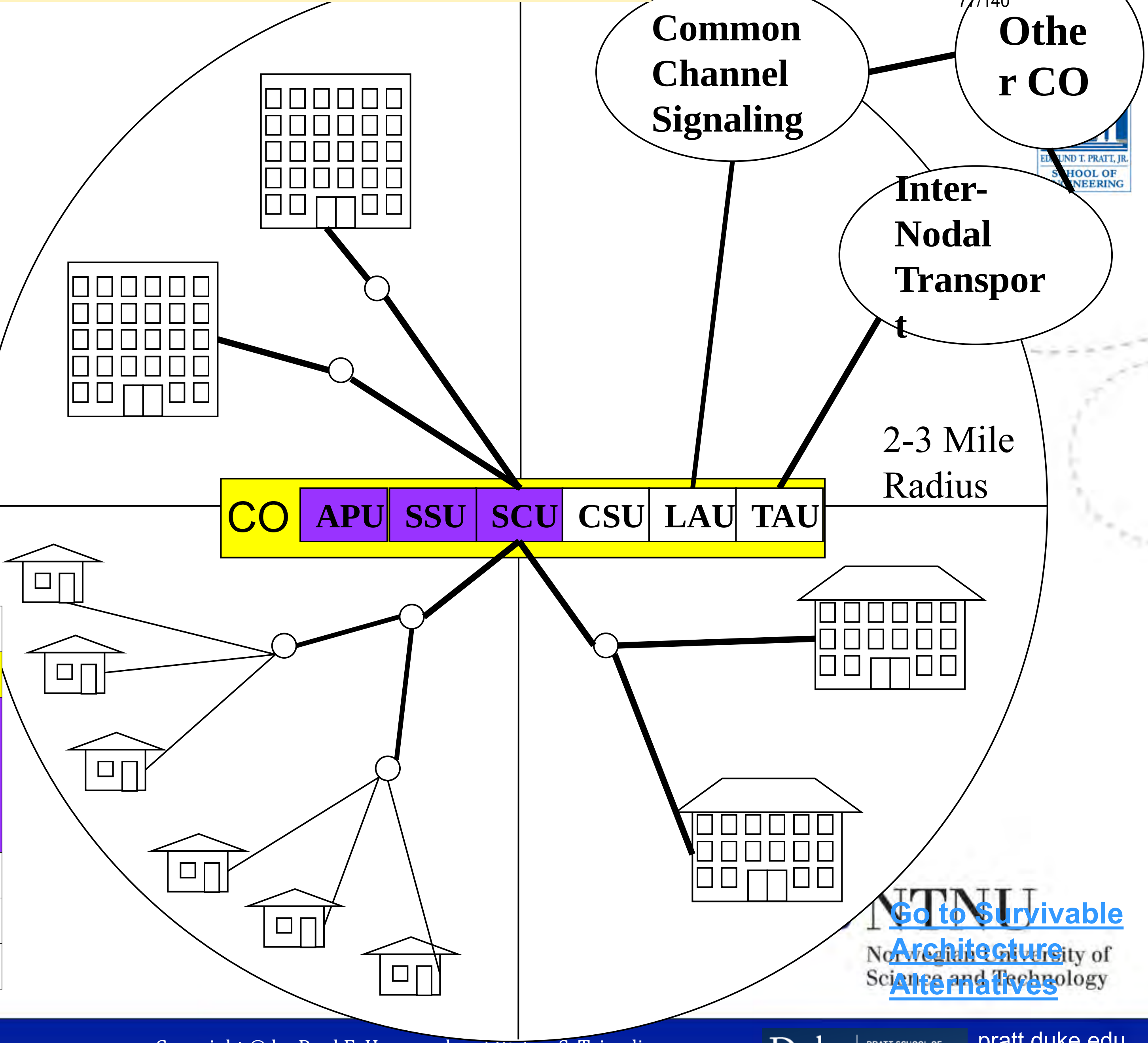
APU
SCU
LAU
CSU
SSU
TAU
HPU

Increasing wire concentration approaching central office



Classical Architecture

Symbol	Meaning
○	Wiring Cross-Point
━	Multi-Pair Cable
═	Drop Cable
🏠	Single Family Residence
🏢	Business
🏬	Multi-Family Dwelling



Unit	Type
CO	Central Office
HPU APU SSU SCU	Host Administrative Signaling Communications
CSU	Call Service
LAU	Line Access
TAU	Trunk Access

Go to Survivable Architecture Alternatives

Layered architecture

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

[16] V. B. Mendiratta and C. A. Witschorik. Telephone service survivability. In IEEE workshop on the design of reliable communication networks (DRCN2003), October 2003.

New options for different layers

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

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)

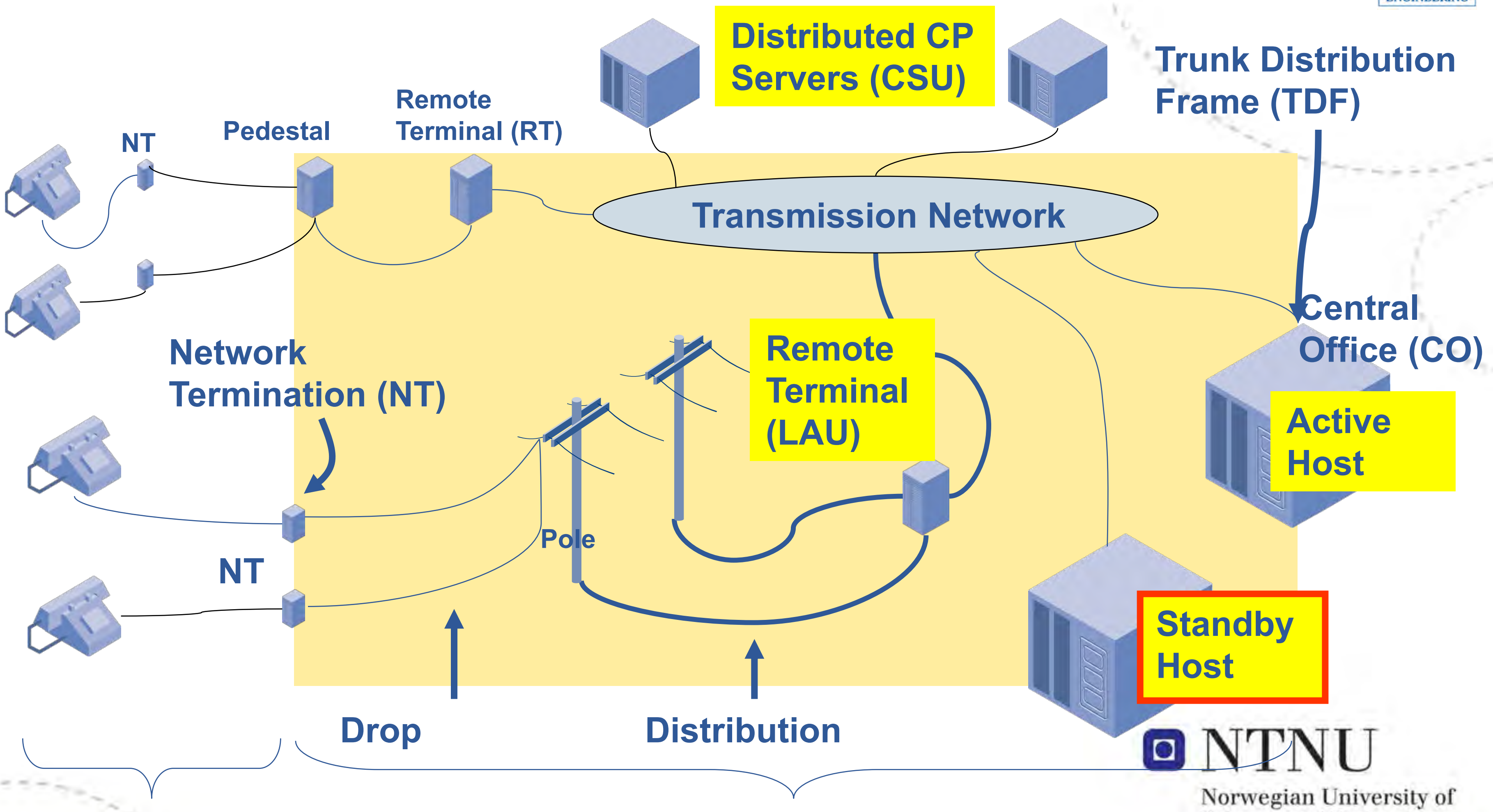
Survivable architecture alternatives

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

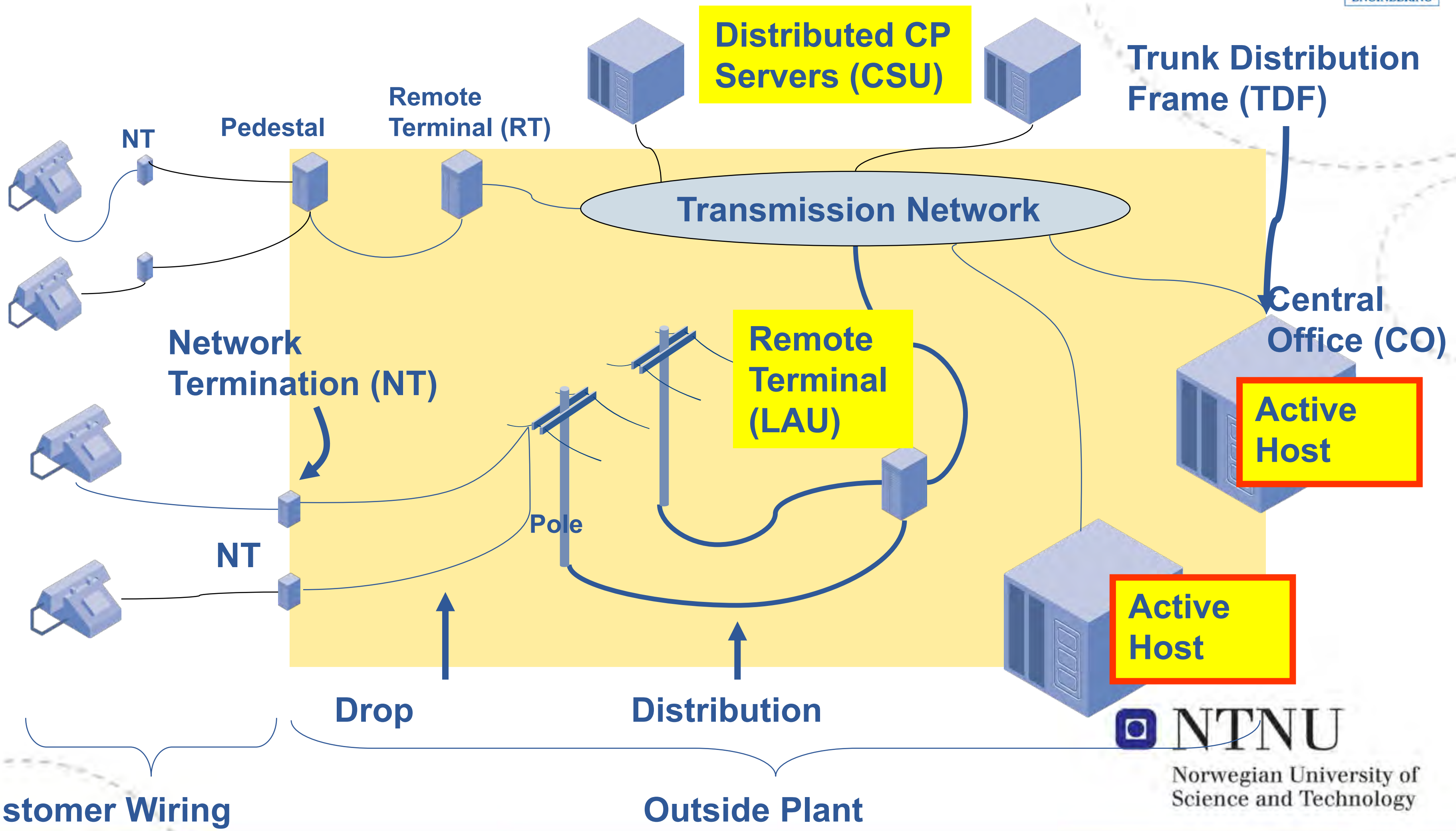
Active/standby: the standby HPU takes over all the customers and trunks when the active HPU is destroyed in a disaster

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

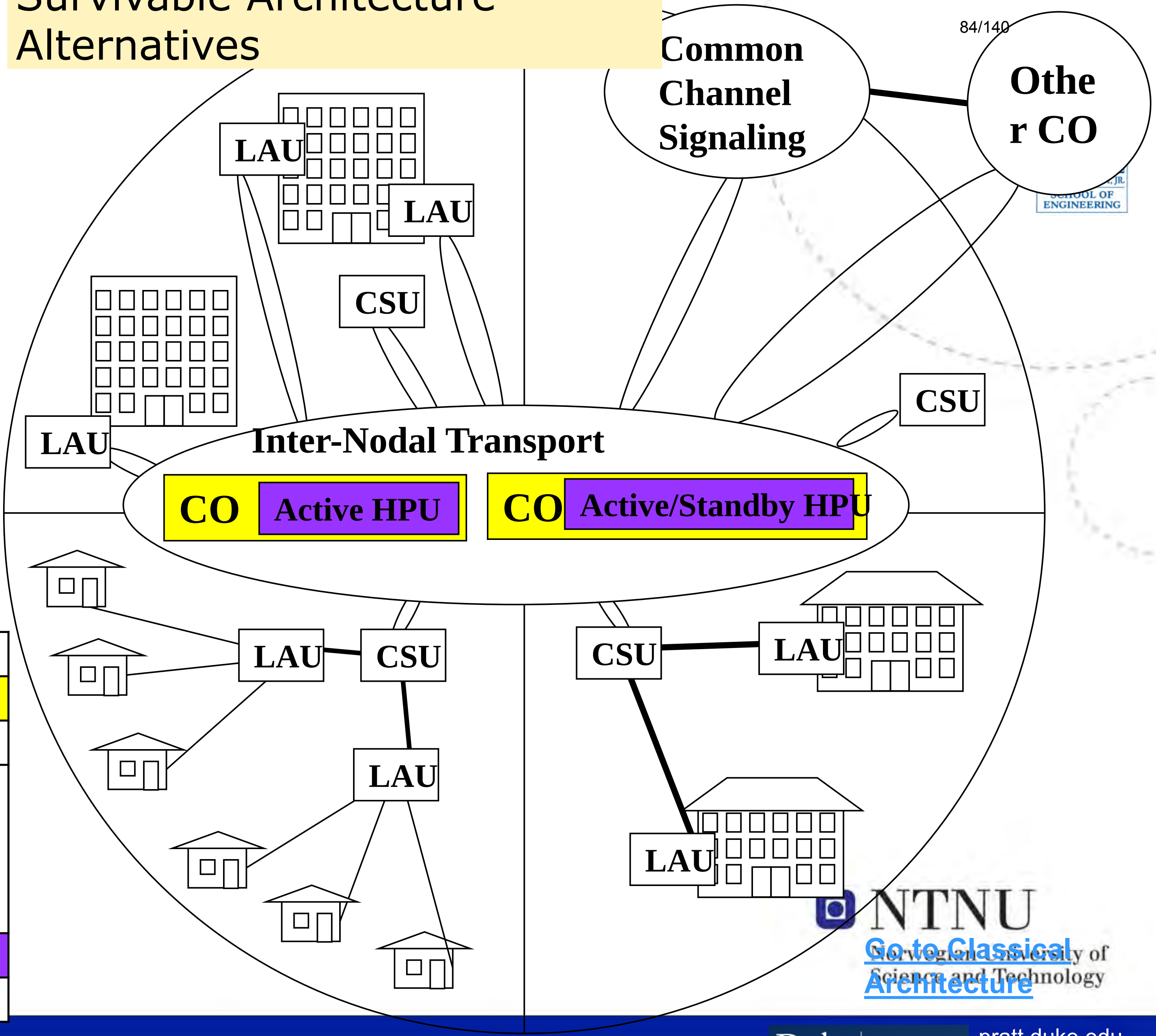


Architecture A/A: Reduce Length of Copper Loops + Distribute Call Processing + Active/Active Host



Survivable Architecture Alternatives

Symbol	Meaning
━	Multi-Pair Cable
═	Drop Cable
⬭	Protected Cable
🏠	Single Family Residence
🏢	Business
🏬	Multi-Family Dwelling



Unit	Type
CO	Central Office
APU	Administrative
CSU	Call Service Communication s Signaling Trunk Access
HPU	Host Processing
LAU	Line Access

Go to Classical Architecture

Architectures A/S I, A/S II, A/A

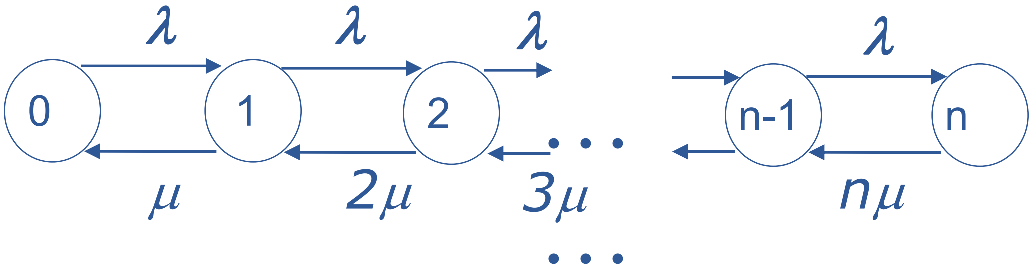
- Distributed CSU
  - Maintain basic service ($r_b \times 100\%$ of total traffic) when HPU fails
  - Reduced capacity ($r_r \times 100\%$ of total trunks) for basic service
- Redundant HPU
  - Active/standby A/S I
    - Switchover coverage
    - Synchronization probability
  - Active/standby A/S II
    - Switchover coverage
    - Synchronization delay ($r_p \times 100\%$ of customers get service before synchronization)
  - Active/active A/A
    - Load sharing, each serves half subscribers
    - Switchover coverage
    - Synchronization delay ($r_p \times 100\%$ of customers get service before synchronization)
- Failure scenario
  - Loss of one active HPU

System parameters

- Total capacity n: 10000 trunks
- Call arrival rate $\boldsymbol{\lambda}$: 100 / sec^{-1}
- Mean call holding time μ^{-1}: 100 seconds
- Disaster rate λ_f: 1 / year^{-1}
- Mean detection time δ_d^{-1}: 1 second
- Mean switchover time δ_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 δ_s^{-1}: 10 minutes
- Mean manual recovery time μ_r^{-1}: 2 hours
- Mean manual repair time μ_R^{-1} : 10 days
- Mean reconfiguration time β^{-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

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

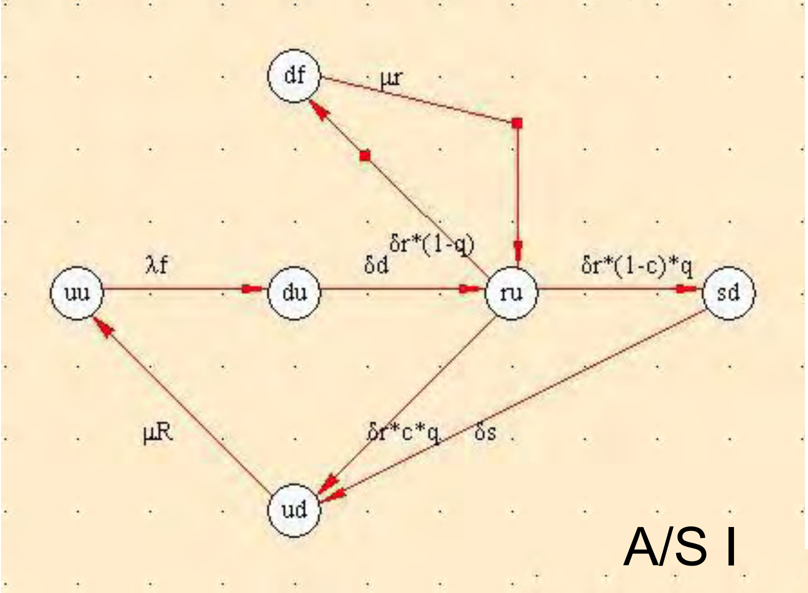
Blocking probability:

$$P_{bk} = \pi_n$$

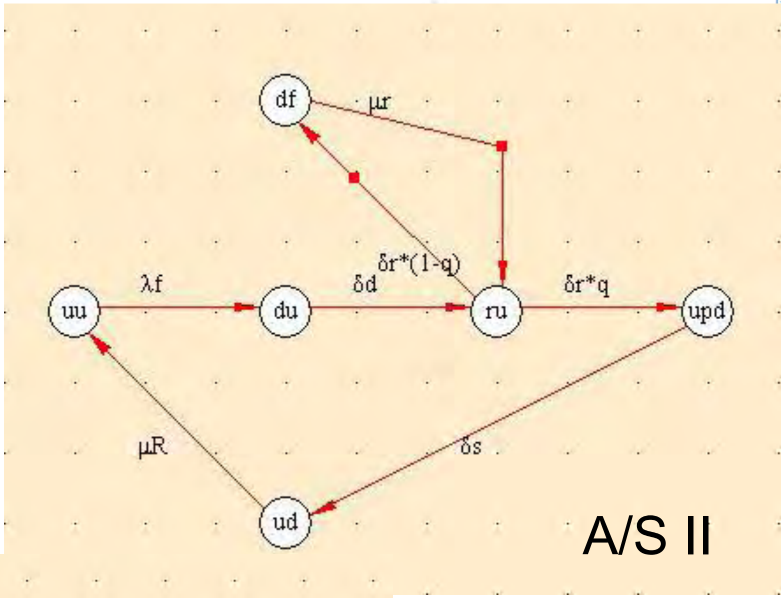
Expected number of calls in the system:

$$\sum_{k=0}^{n} k\, \pi_k$$

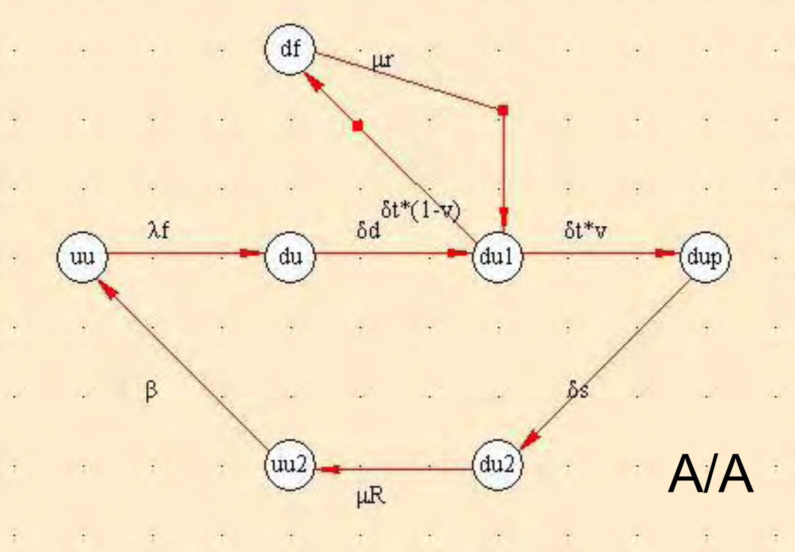
Pure availability models: A/S I, A/S II, A/A



A/S I



A/S II



A/A

Pure performance analysis:

blocking probability P_{bk}

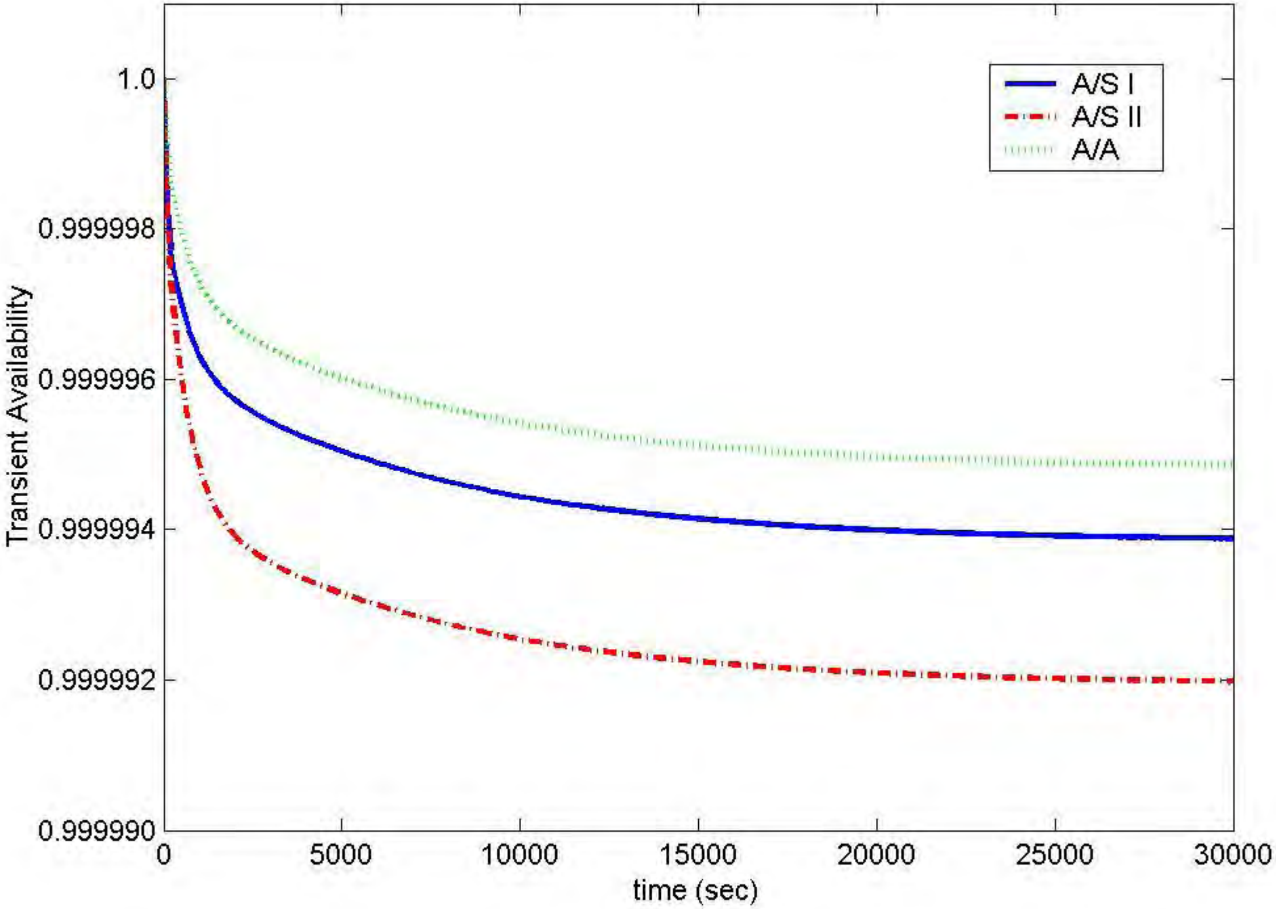
State	A/S I	A/S II	A/A
(u,u)	0.0079366	0.0079366	0.01120
(u,d)	0.0079366	0.0079366	-
(d,u)	0.6050	0.6050	0.3056
(r,u)	0.6050	0.6050	-
(d,f)	0.6050	0.6050	0.6050
(s,d)	0.6050	-	-
(u_p,d)	-	0.08829	-
$(d,u_2),(u,u_2)$	-	-	0.007937
(d,u_1)	-	-	0.3
(d,u_p)	-	-	0.008045

Pure availability analysis: steady state

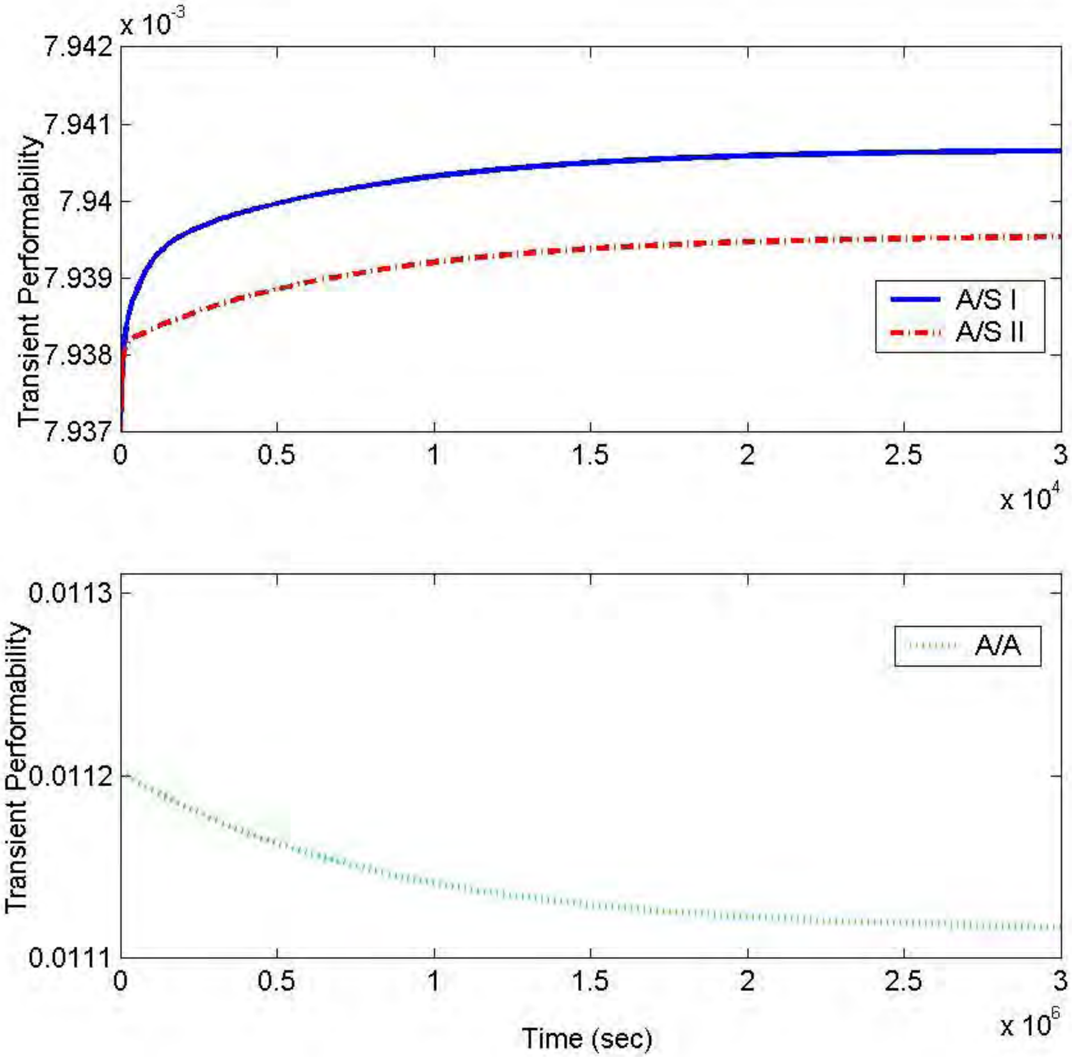
- Steady state availability
  - A/S I
    - Up states: uu, ud
    - Down states: du, df, ru, sd
    - P_{coA} = P(uu)+P(ud) = 0.999994
  - A/S II
    - Up states: uu, ud   Partial up state: upd
    - Down states: du, df, ru
    - P_{coA} = P(uu)+P(ud)+P(u_pd)*r_p= 0.999992
  - A/A
    - Up states: uu, uu2, du2   Partial Up State: du, du1, dup
    - Down states: df
    - P_{coA} = P(uu)+P(uu2)+P(du2)+P(du)*0.5+P(du1)*0.5+ P(dup)*(0.5+r_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_{COA}=1 means full capacity

Pure availability analysis:
transient



Performability results



Steady state:

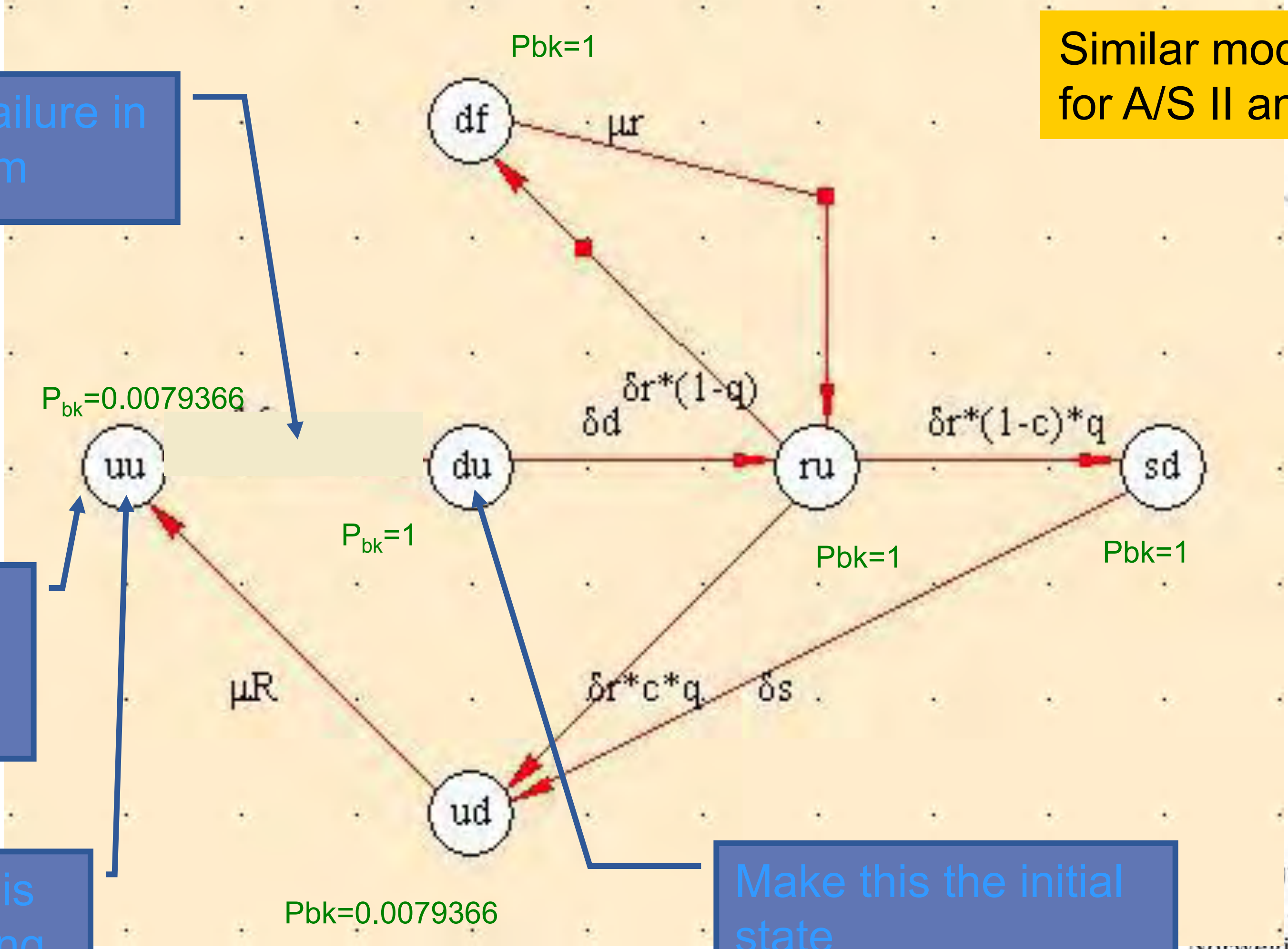
A/S I: 0.0079404

A/S II: 0.0079393

A/A: 0.01115

Model modification for survivability definition: A/S I

Similar modification for A/S II and A/A



Force a failure in the system

Normally operating in this state

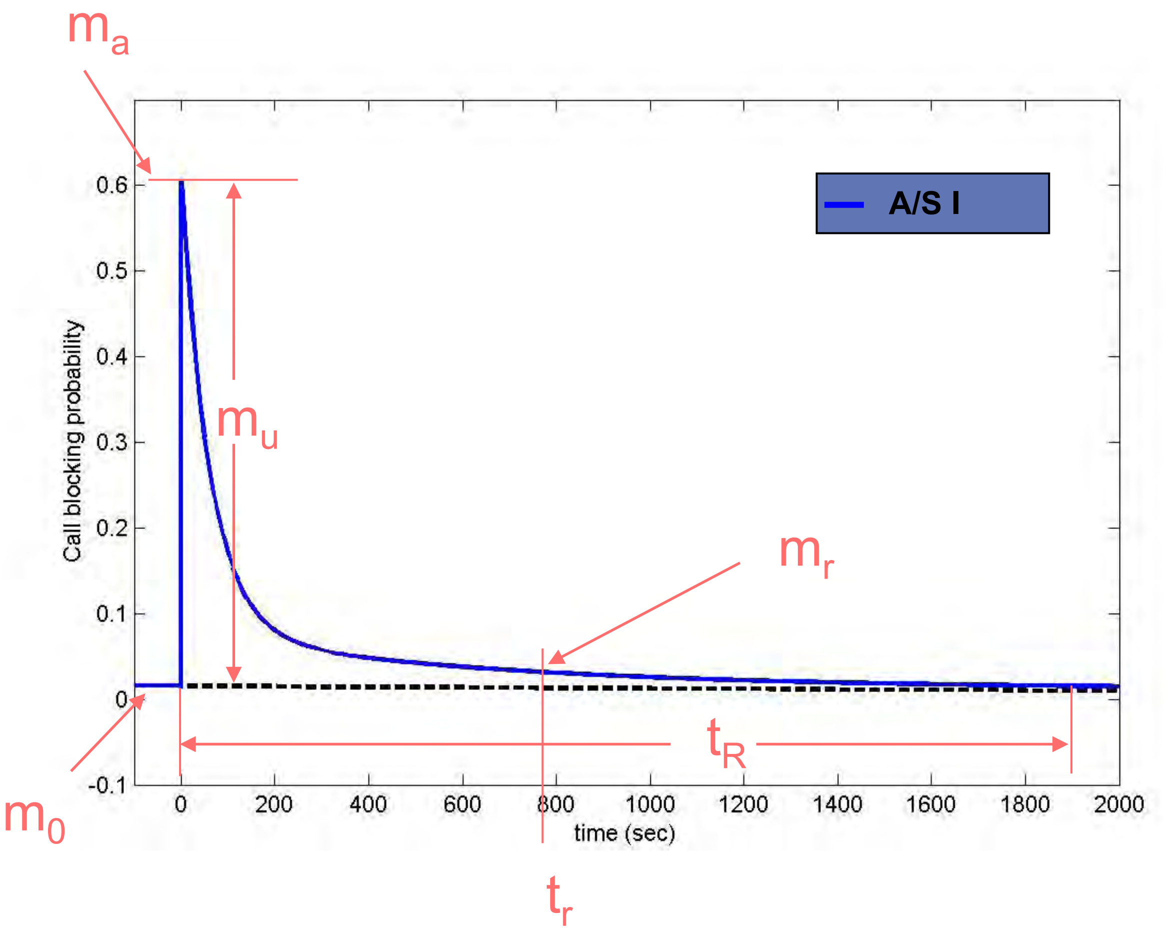
Make this Absorbing state

Make this the initial state

Implication of the modification

- What does it mean when transition (λ_f) is removed?
  - A failure is injected into the system
  - All the system survivability measures do **not** depend on the value of λ_f
  - All previous performance/availability/performability measures and the first two survivability measures do depend on the value of λ_f
  - It is usually difficult to have agreement on the value of λ_f in practice. Therefore, those measures depending on λ_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

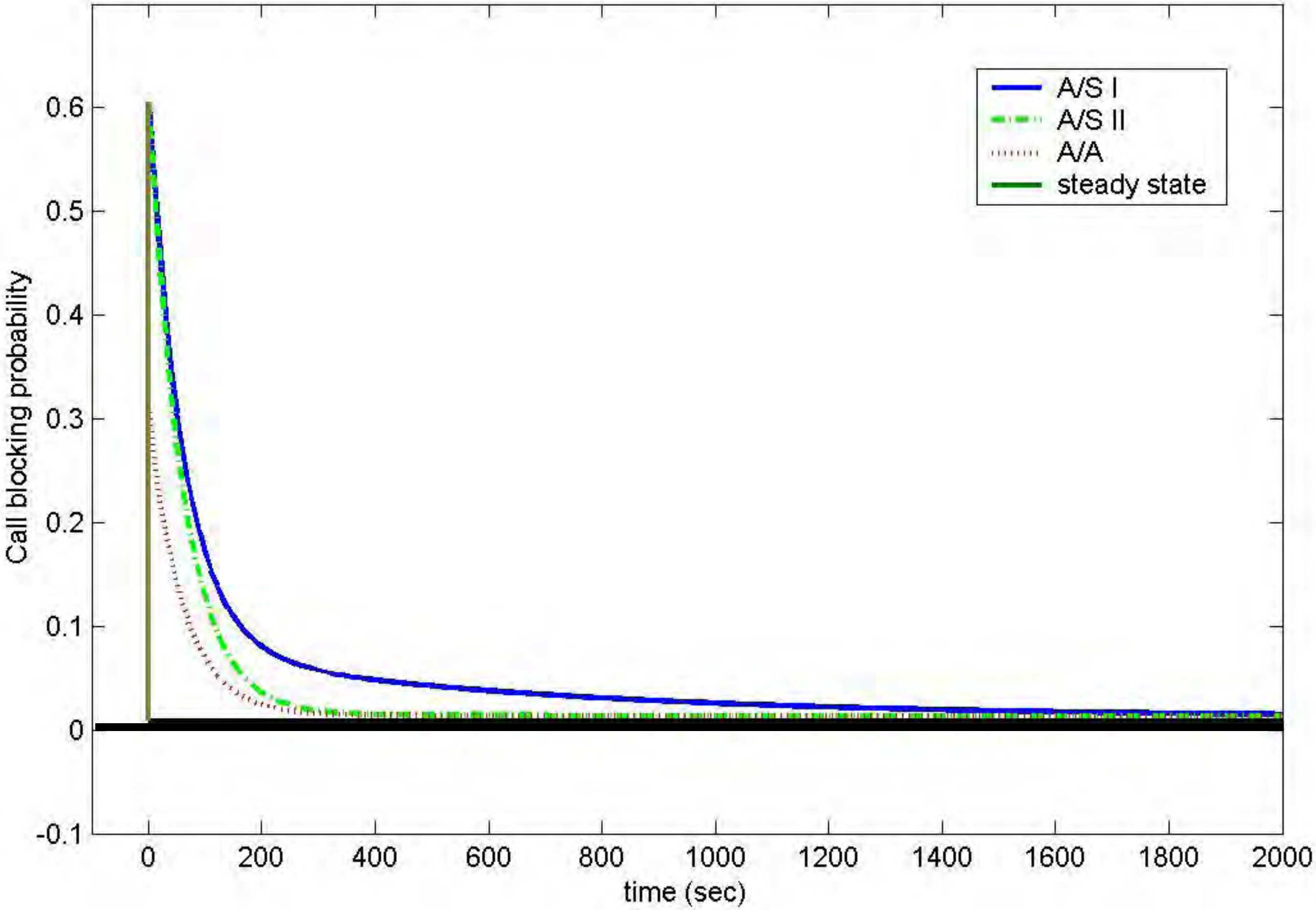
  $P_{bk} = 0.5309 = 66.9 \times P_{bk}(uu)$
- 10 min

  $P_{bk} = 0.0378 = 4.76 \times P_{bk}(uu)$
- 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



Norwegian University of Science and Technology

Survivability results

	A/S I	A/S II	A/A
m_0	0.007937	0.007937	0.01120
m_a	0.6050	0.6050	0.3056
m_u	0.5971	0.5971	0.2944
m_r, (t_r=10 sec)	0.5309	0.5229	0.2602
m_r, (t_r=10 min)	0.03778	0.01391	0.01356
m_r, (t_r=10 hr)	0.01183	0.01164	0.01163
t_R*	31610 sec	31550 sec	4300 sec

*A relative error 1% is assumed for calculating t_R

Comparison – ELF

	Call loss due to failure	Extra call loss due to blocking	ELF
A/S I	9920	11874	21794
A/S II	9920	8436	18266
A/A	4944	2465	7409

Survivability ranking

	A/S I	A/S II	A/A
P_{full}^*	3	2	1
E[N]	3	2	1
$N_{0\%}$	3	2	1
m_a*	3	2	1
m_r* t=10 min	3	2	1
m_r* t=1 hour	3	2	1
t_R	3	2	1
ELF	3	2	1

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

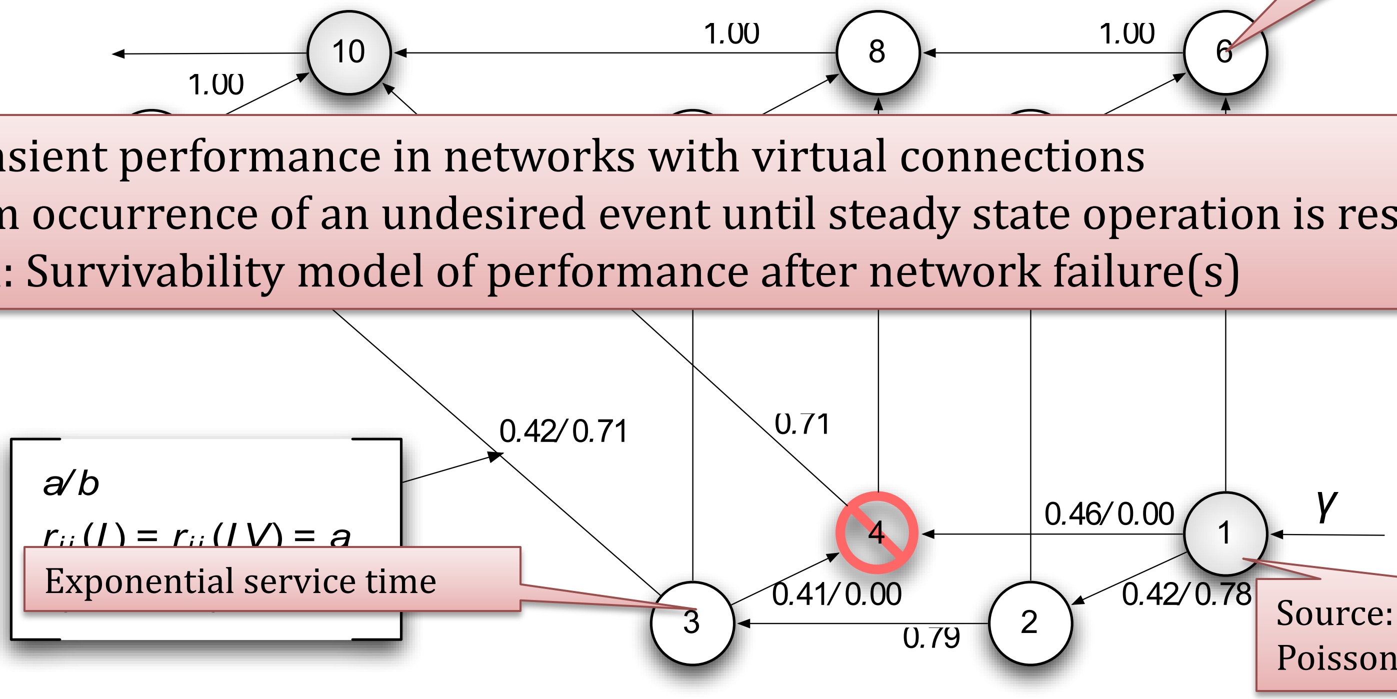
m_a*, m_r* are relative values with respect to p_{bk}(uu)

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

NTNU
Norwegian University of Science and Technology

Objectives and target system



N=50

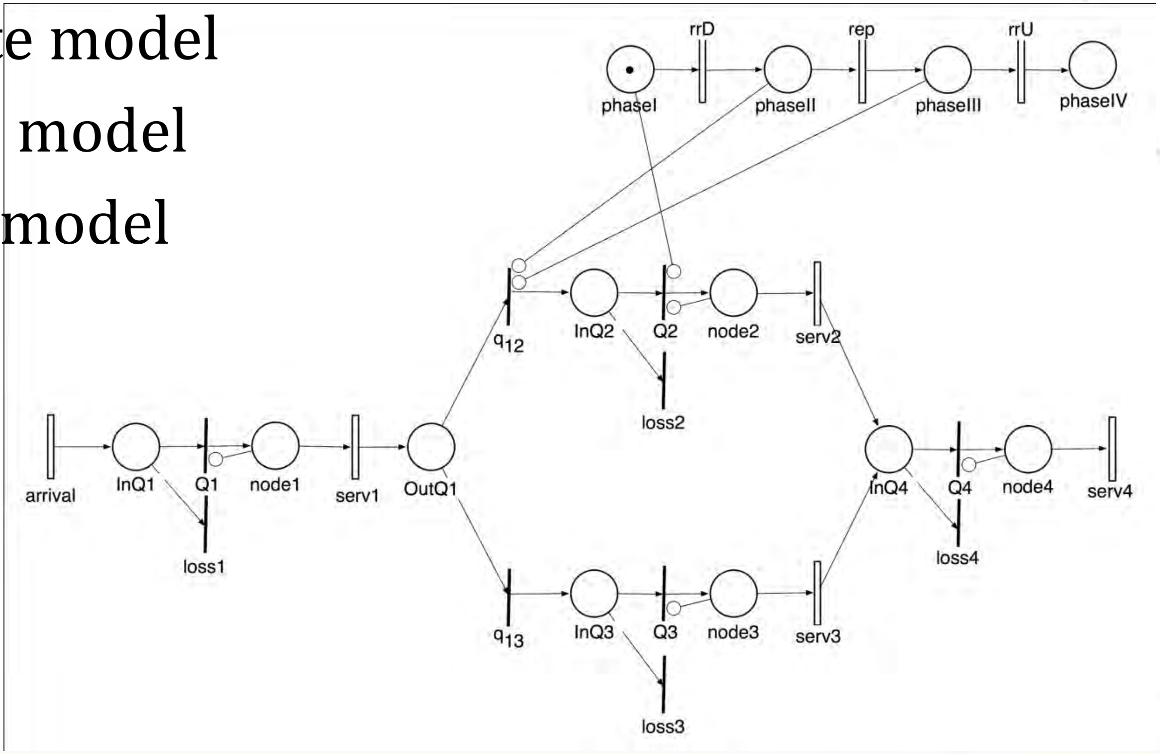
- Transient performance in networks with virtual connections
- From occurrence of an undesired event until steady state operation is restored
- Goal: Survivability model of performance after network failure(s)

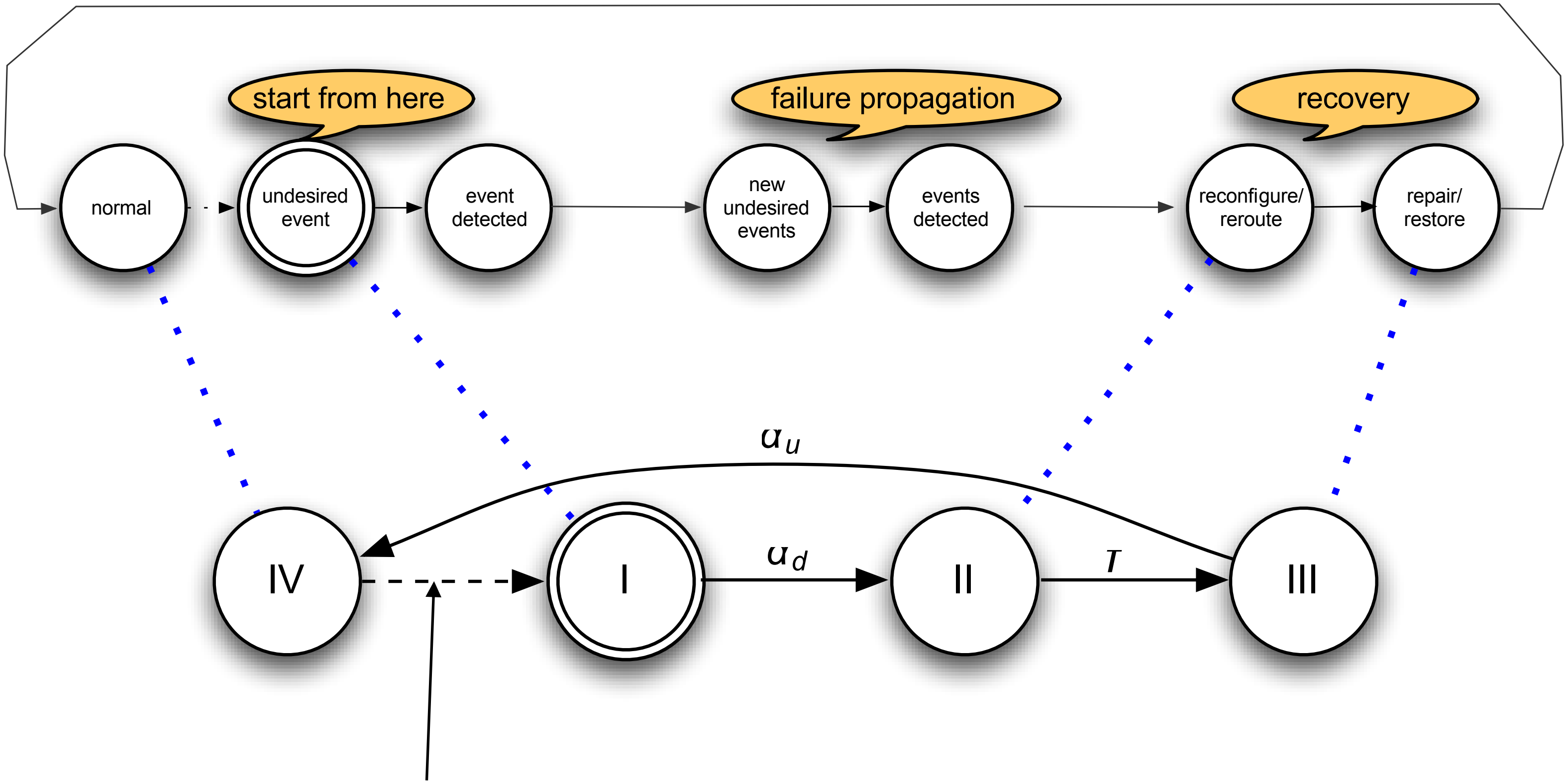
Exponential service time

Source:
Poisson arrivals

Network survivability models

- Phased recovery model
- Modeling approach
- Complete composite model
- Space-decomposed model
- Time-decomposed model



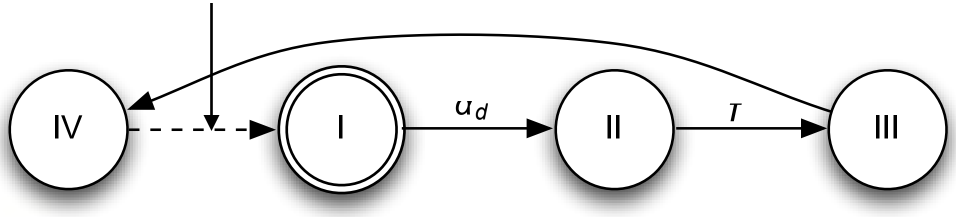


Undesired event is node failure

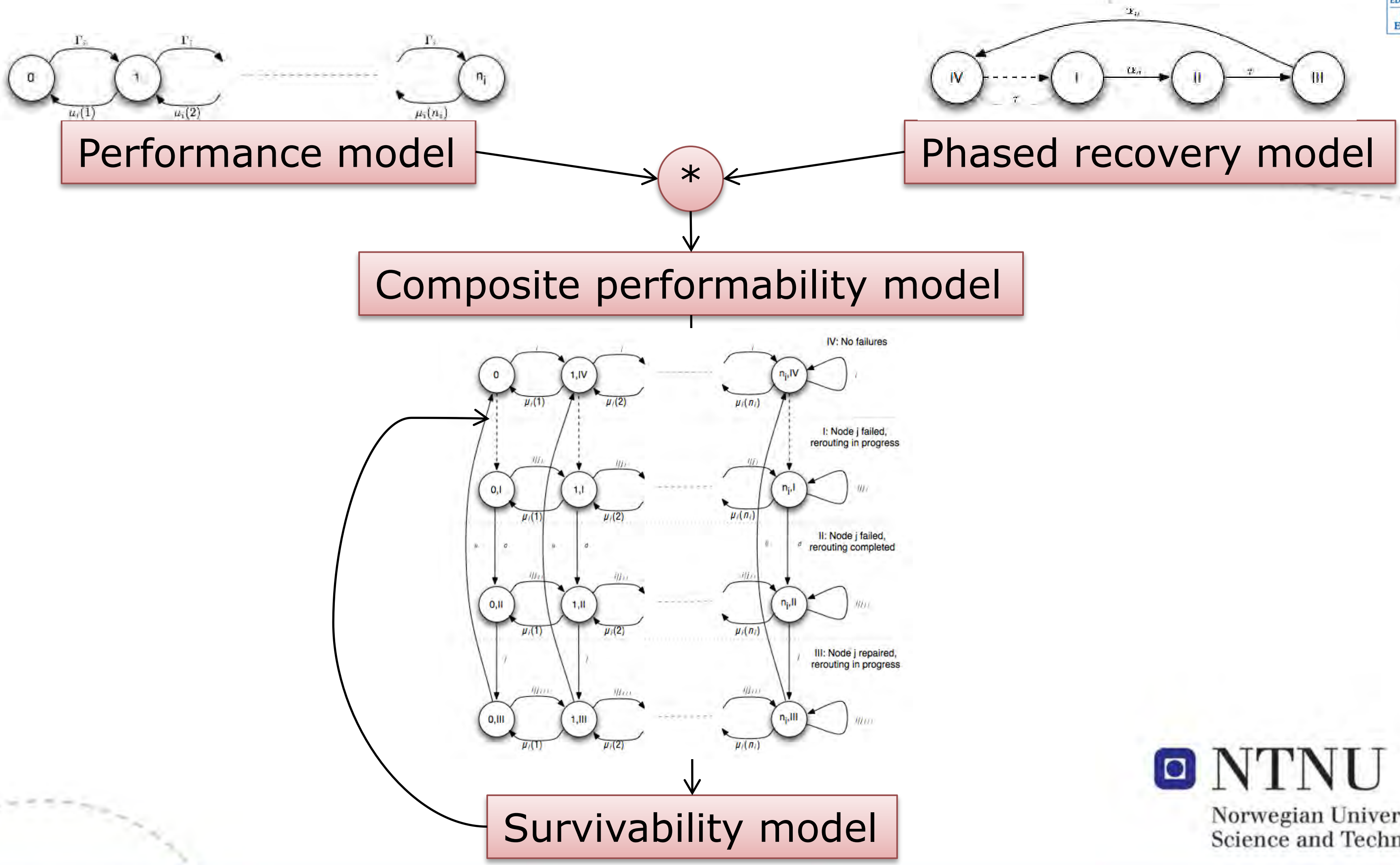
Phased recovery model

- Phase I:
  - Rerouting after failure is $T_D \sim \exp(\langle_D)$
- Phase II:
  - Restoration time is $T_R \sim \exp(|)$
- Phase III:
  - Rerouting after failure is $T_U \sim \exp(\langle_U)$
- Phase IV:
  - Fault free network with default routing

Undesired event is node failure



Modeling approach



Performance model

Phased recovery model

Composite performability model

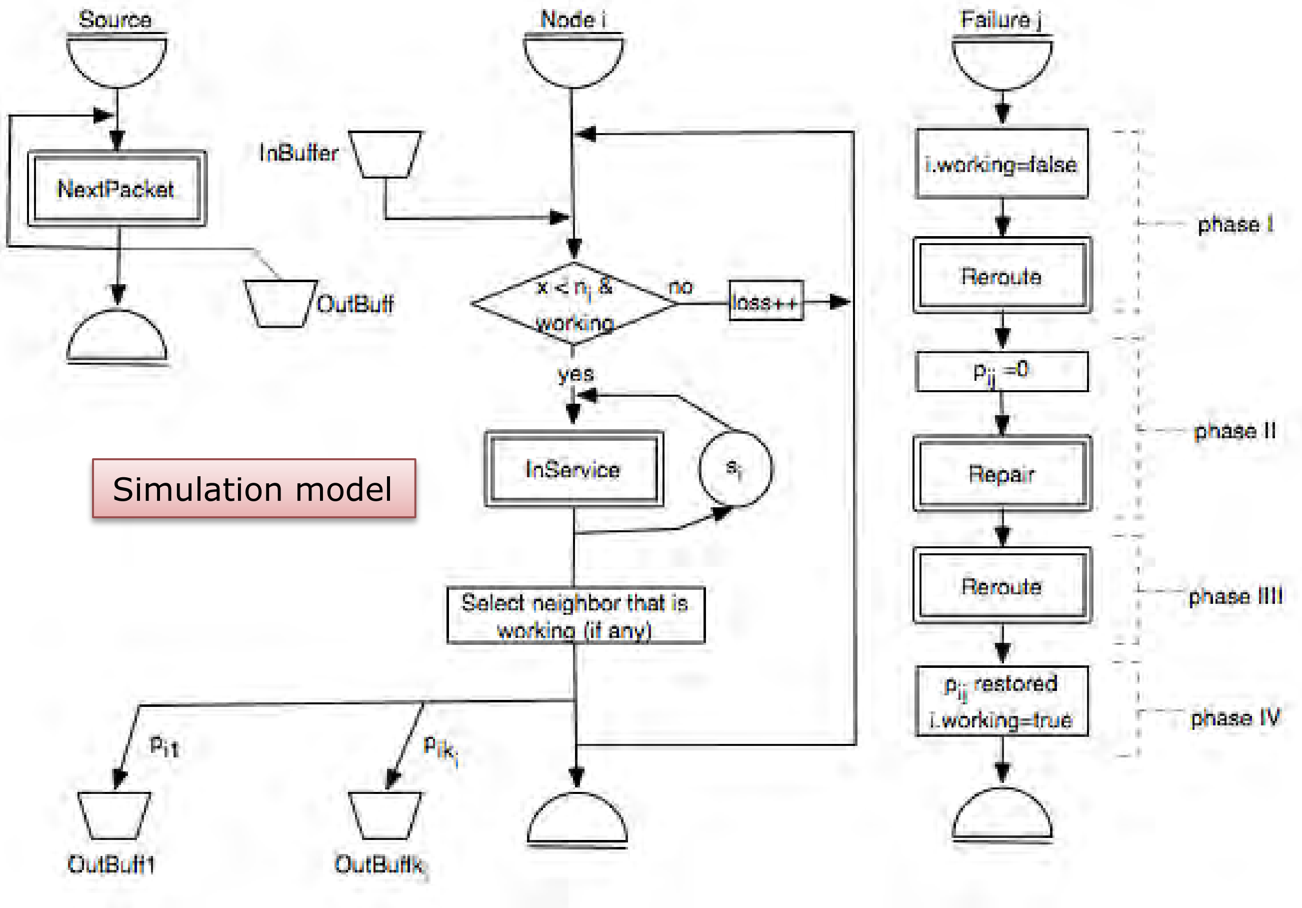
Survivability model

0
1
n_j
$\mu_j(1)$
$\mu_j(2)$
$\mu_j(n_j)$
IV
I
II
III
*
0
1,IV
n_j,IV
0,I
1,I
n_j,I
0,II
1,II
n_j,II
0,III
1,III
n_j,III
IV: No failures
I: Node j failed, rerouting in progress
II: Node j failed, rerouting completed
III: Node j repaired, rerouting in progress

Complete composite model

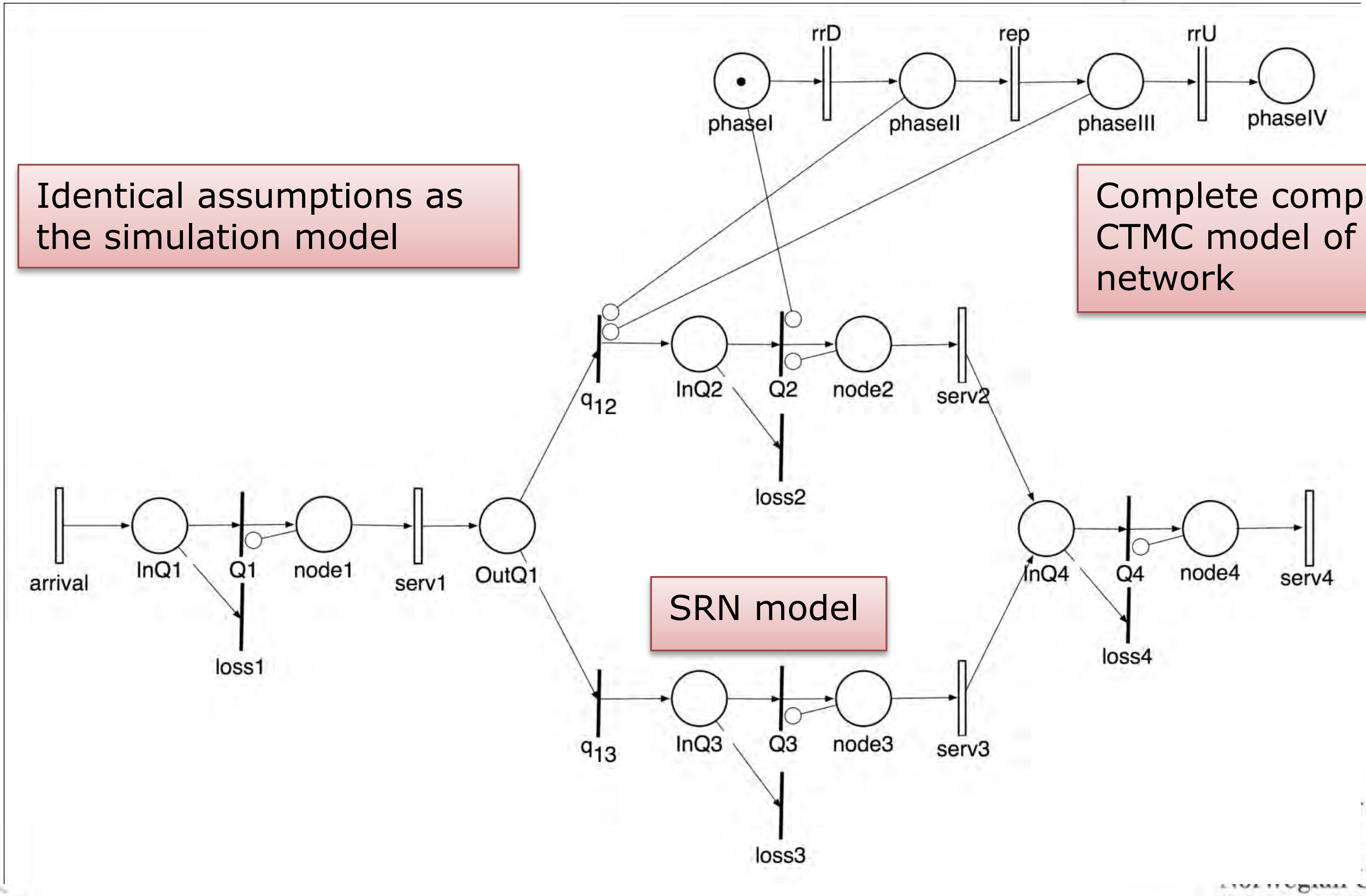
- Simulation
  - DEMOS/Simula
  - Discrete event, process-oriented simulation model
- Analytical
  - SRN: Stochastic Reward Nets
  - Full CTMC
  - Solved by SPNP and SHARPE

Complete composite model



Simulation model

Complete composite model



Identical assumptions as the simulation model

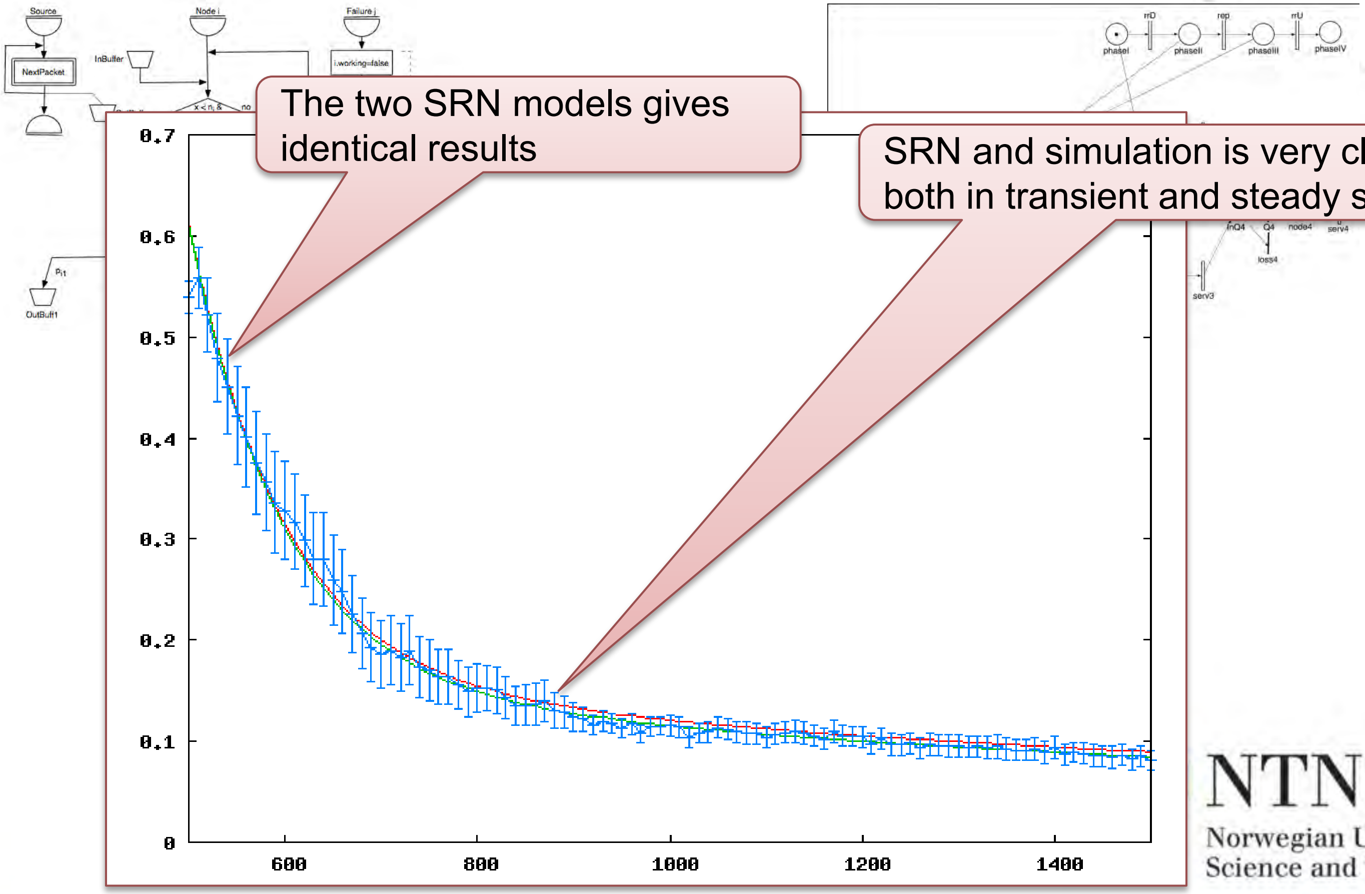
Complete composite CTMC model of 4 node network

SRN model

Numerical example: packet loss probability

Simulation model

SRN model

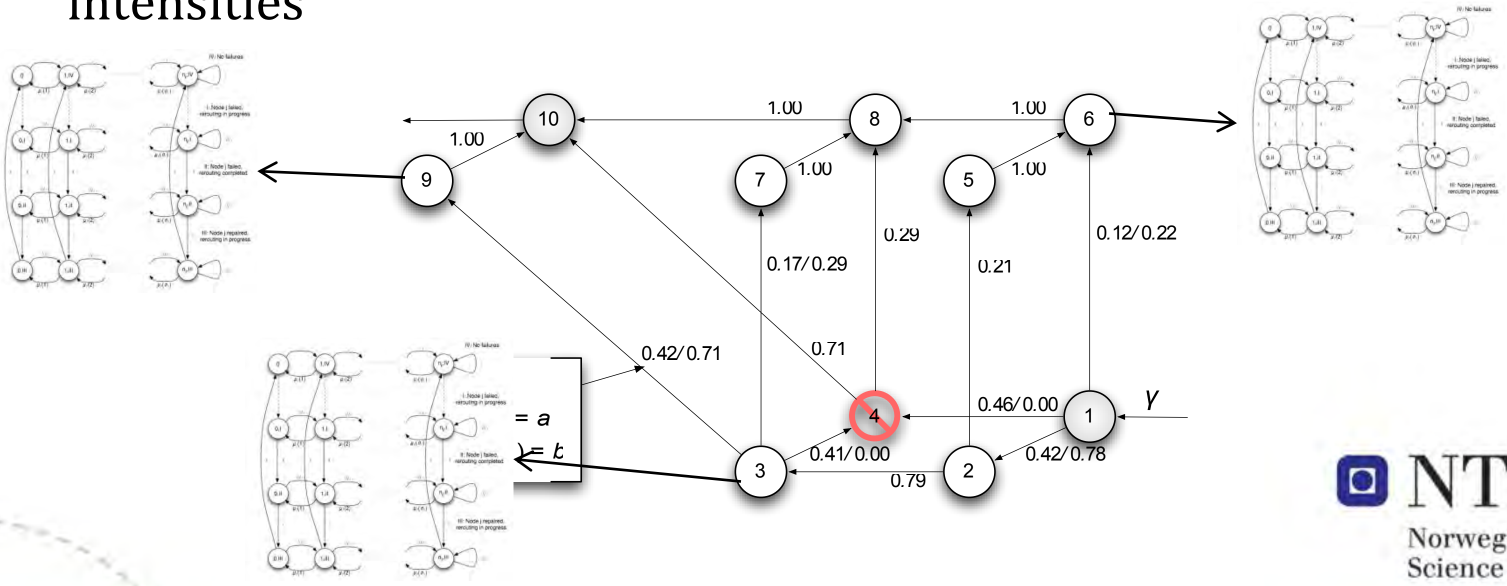


The two SRN models gives identical results

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

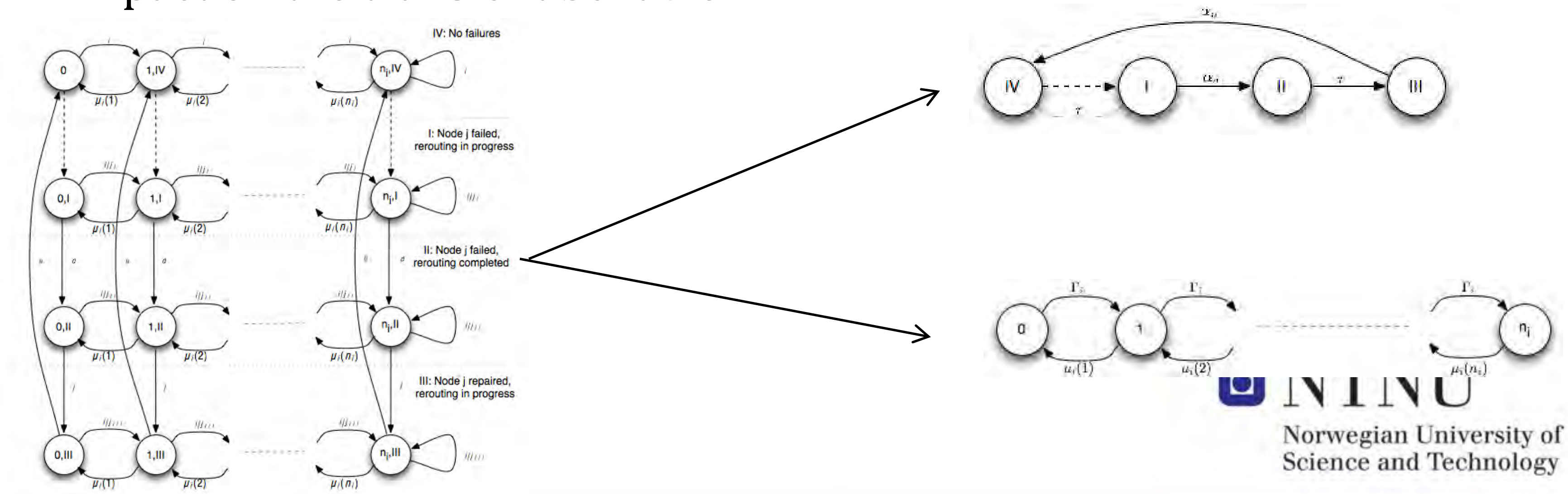
Space-decomposed model

- 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



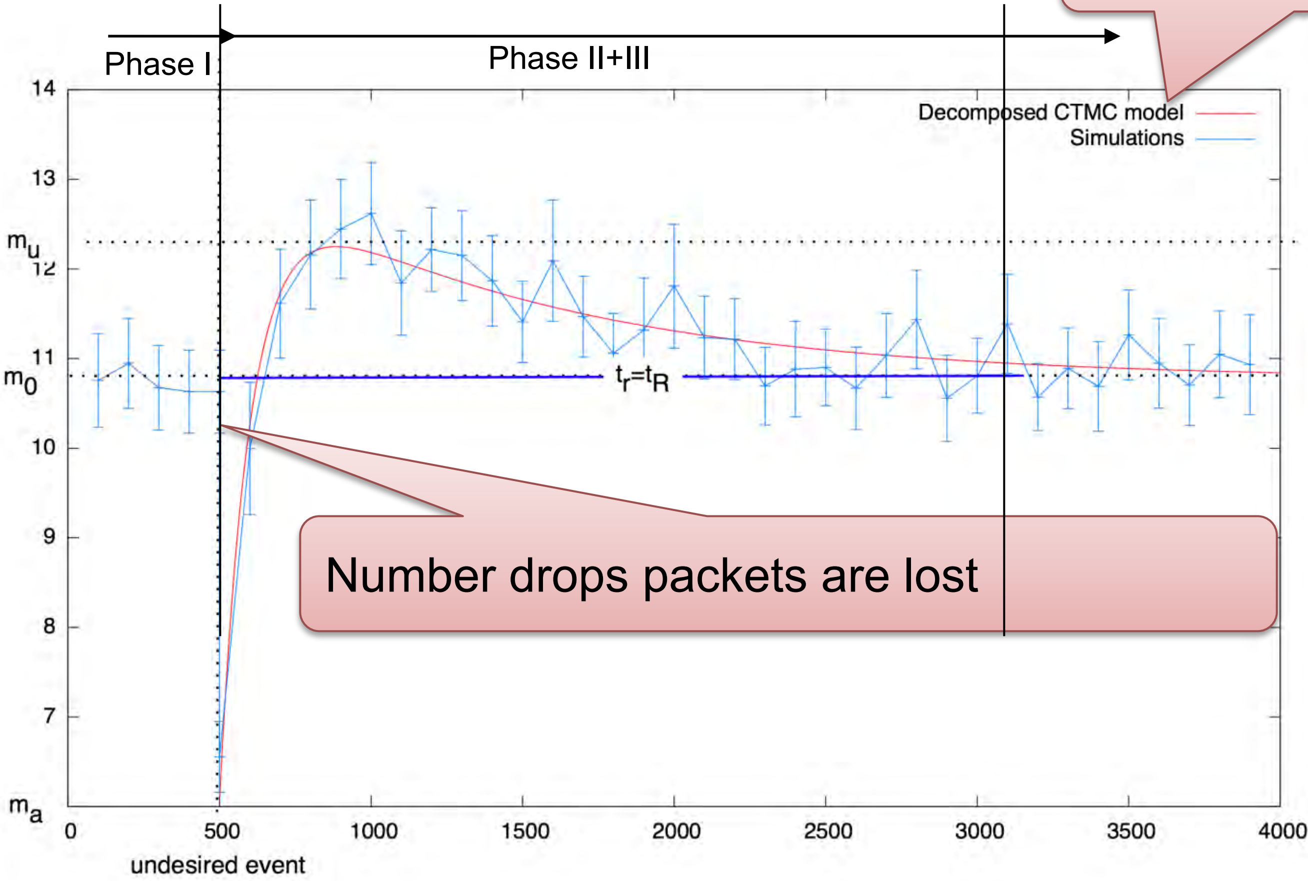
Time-decomposed model

- 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

Compares decomposed models and simulations



Number drops packets are lost

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

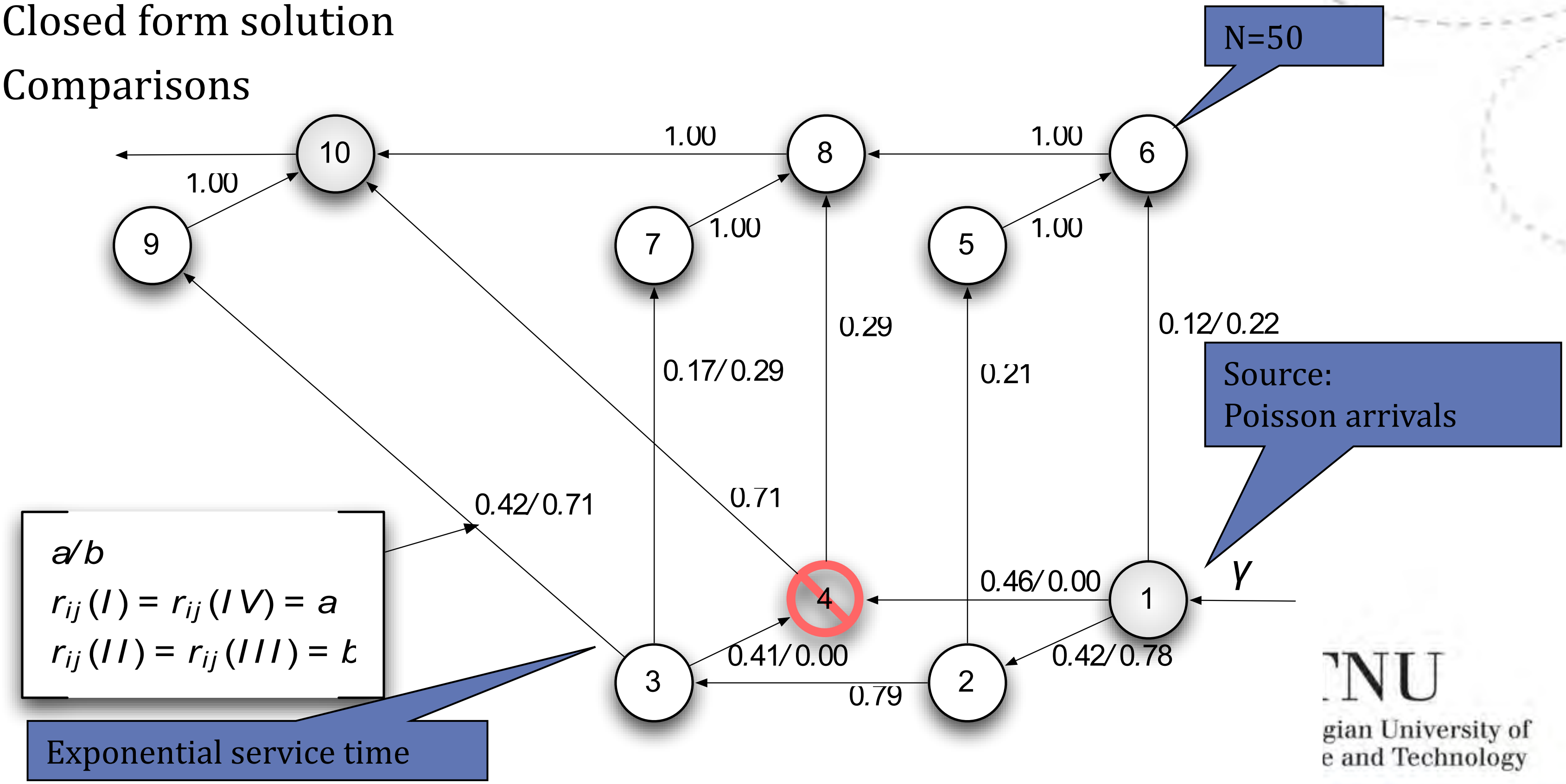
- Complete composite model - SRN
  - Transient solution of model with $N_{\text{node}} \times N_{\text{res}} \times N_{\text{phase}}$ states
- Space decomposed CTMC
  - Transient solution of N_{node} models with $N_{\text{res}} \times N_{\text{phase}}$ states
- Time decomposed CTMC
  - Steady state solution of $N_{\text{node}} \times N_{\text{phase}}$ 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



N=50

Source:
Poisson arrivals

a/b

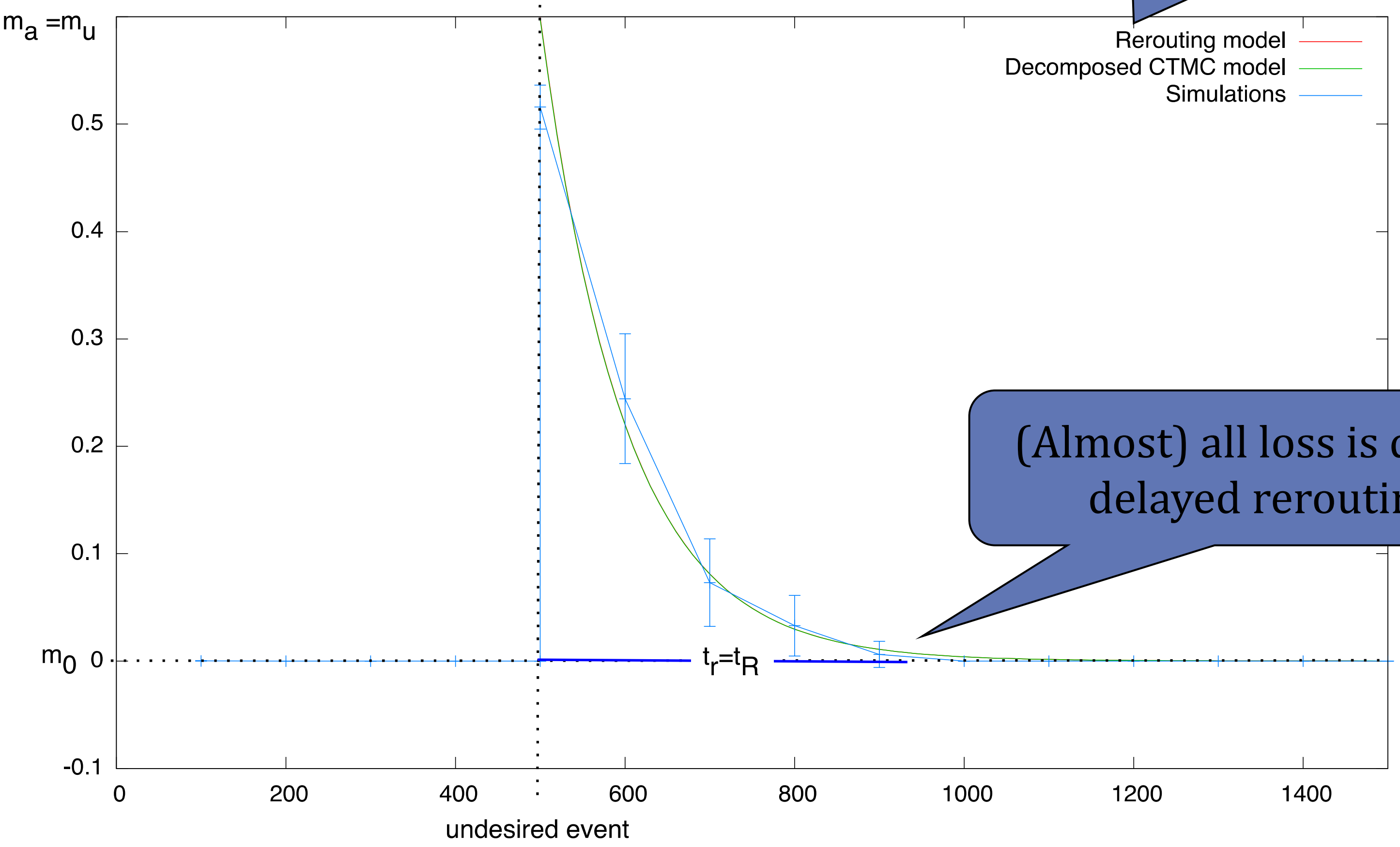
$r_{ij}(I) = r_{ij}(IV) = a$

$r_{ij}(II) = r_{ij}(III) = b$

Exponential service time

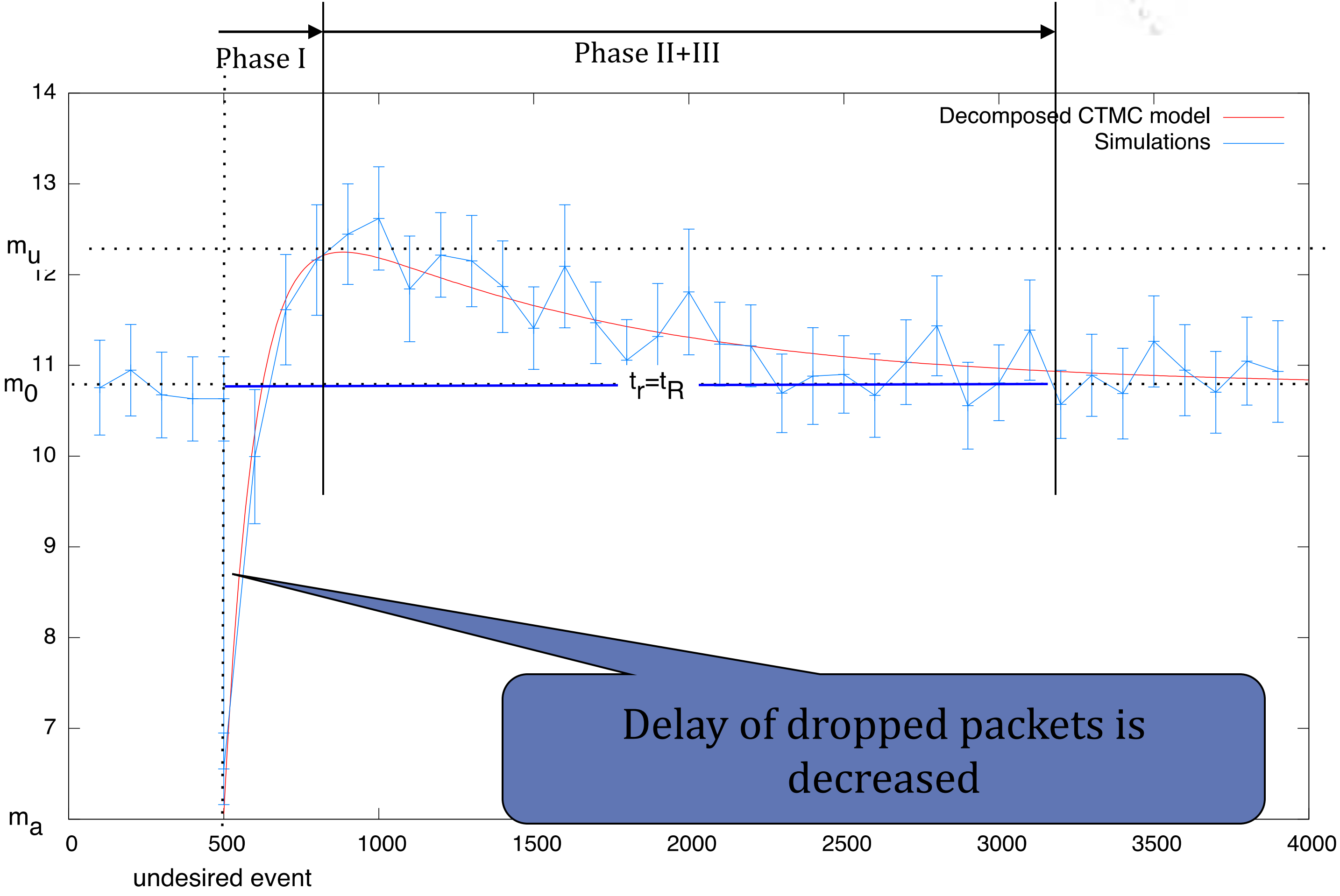
Network 10 nodes: loss delay

Rerouting model is F(t)=p* exp(-t α_D)



(Almost) all loss is due to delayed rerouting

Network 10 nodes: average number in system



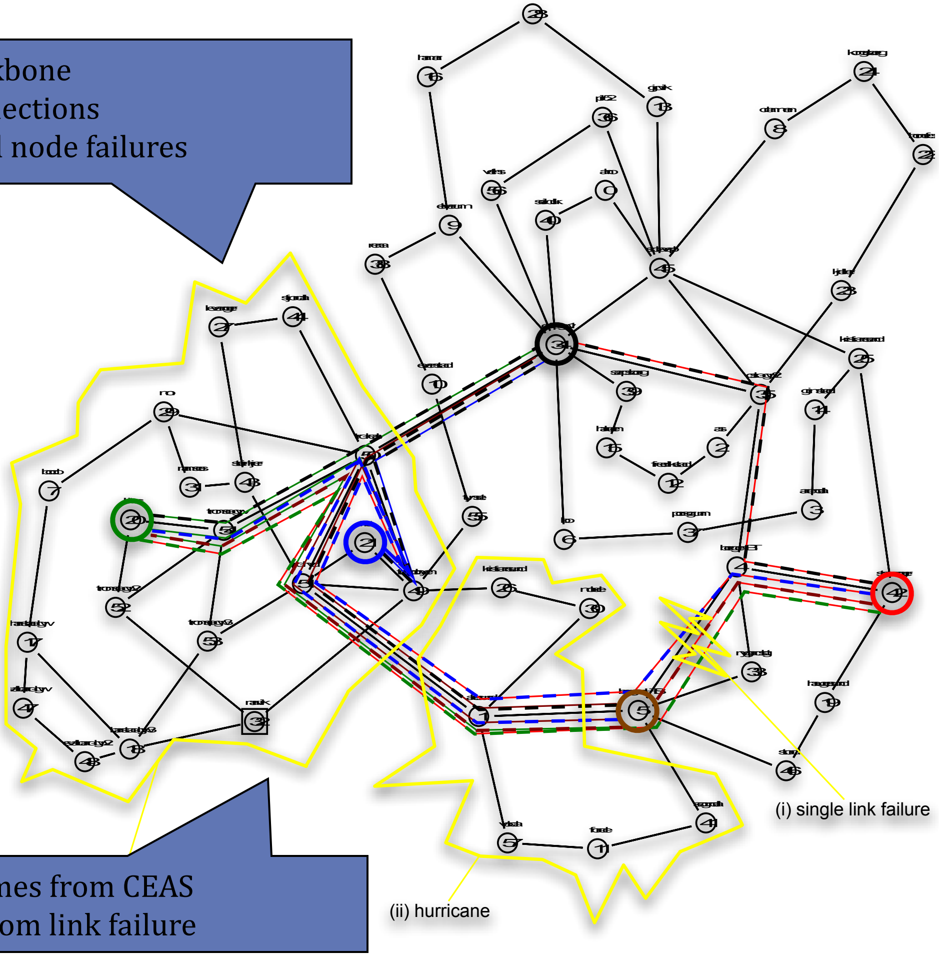
Delay of dropped packets is decreased

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

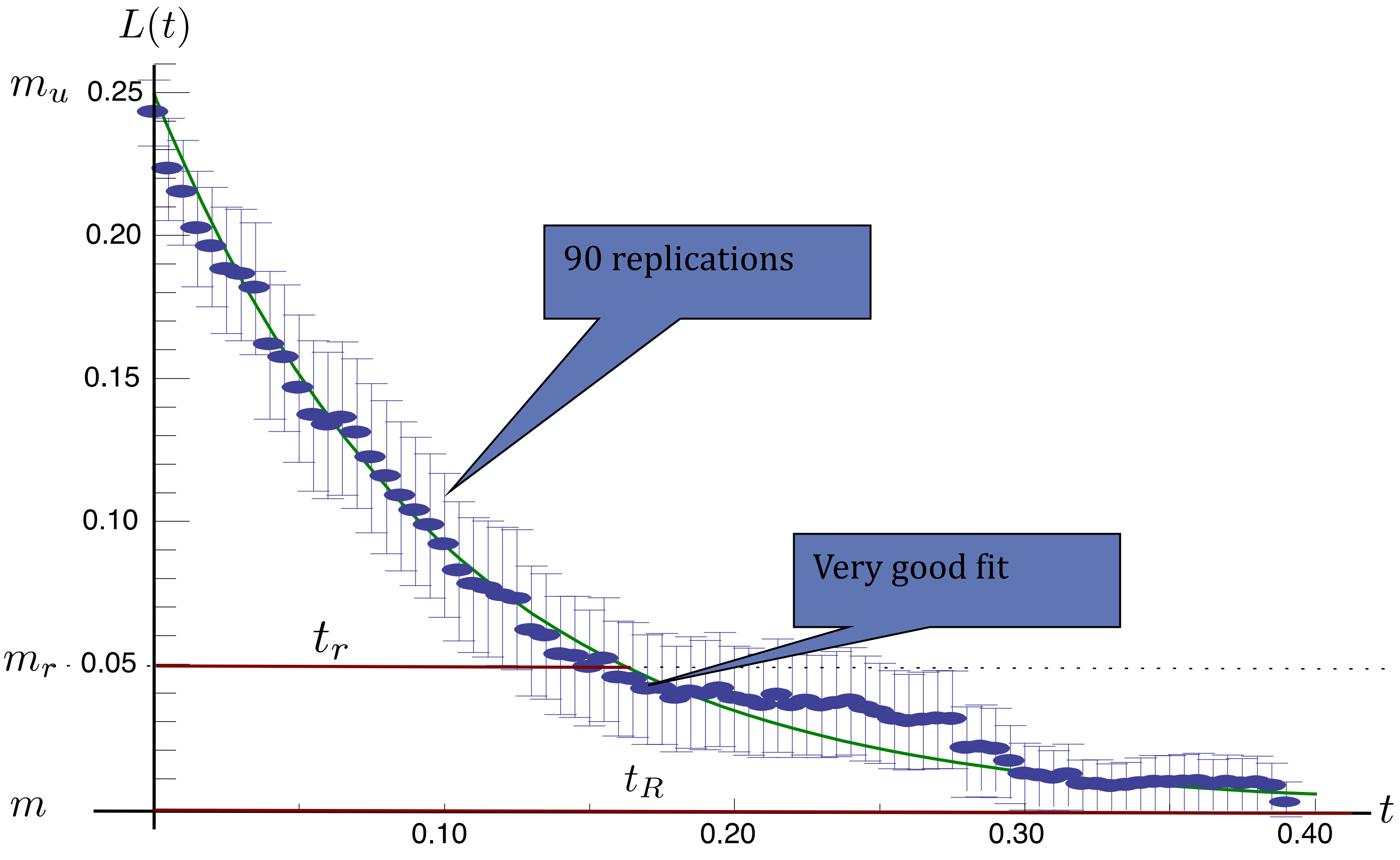
Network with 58 nodes

- Each phase has a routing scheme
- Determine (steady state) performance for each phase
  - Jacksson 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

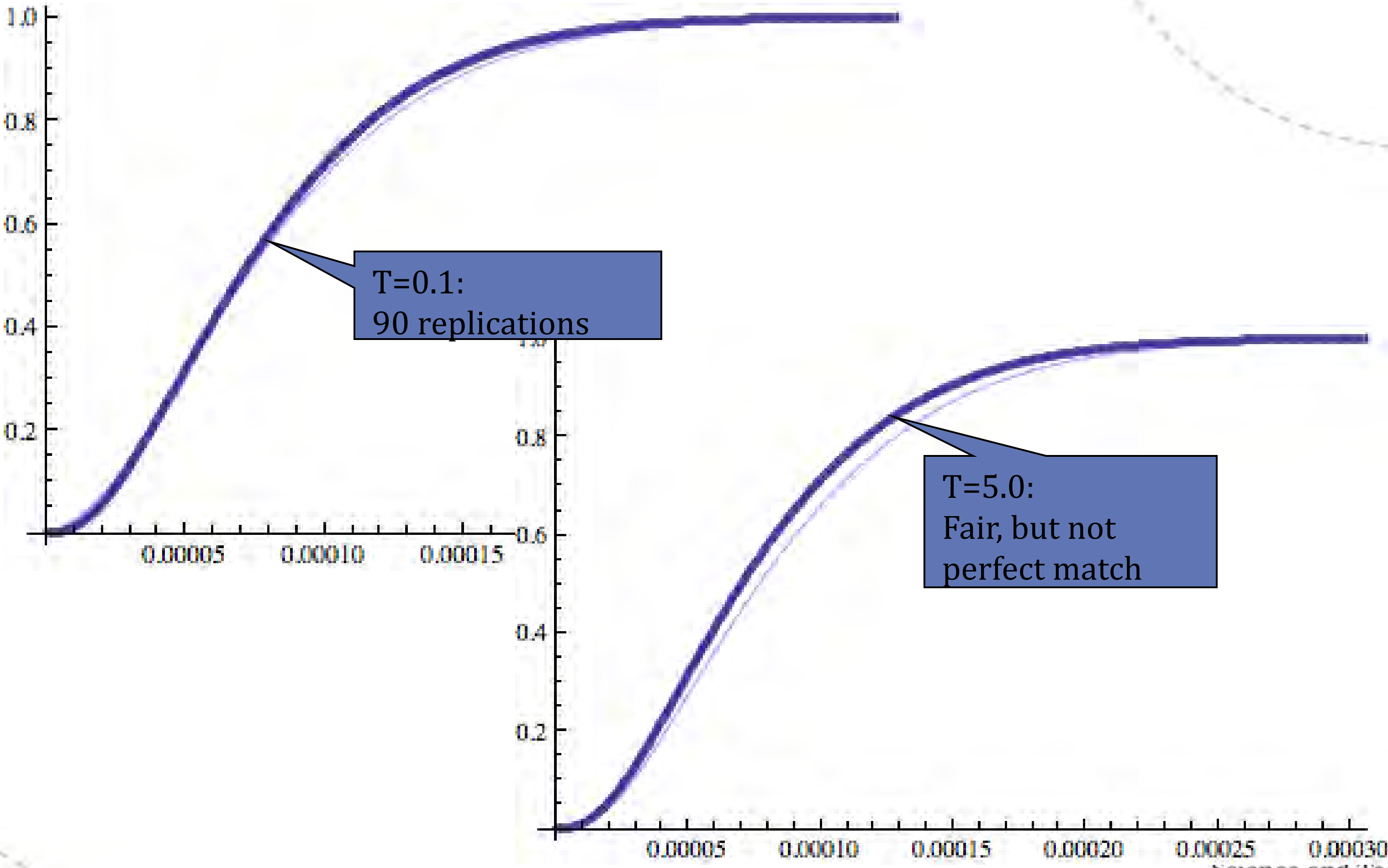
Network with 58 nodes: loss ratio



90 replications

Very good fit

Network with 58 nodes: delay distribution

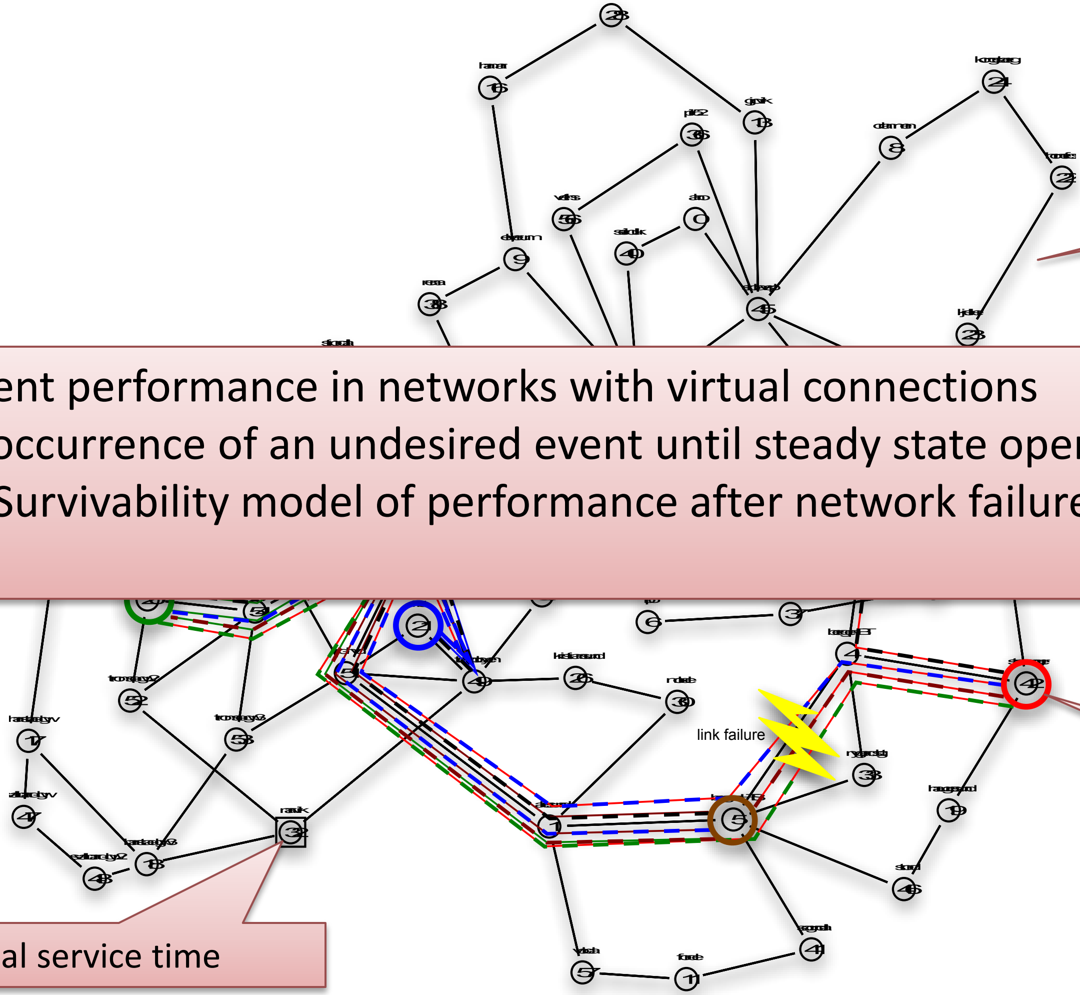


T=0.1:
90 replications

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)



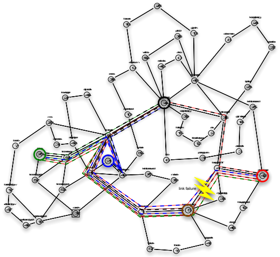
58 nodes

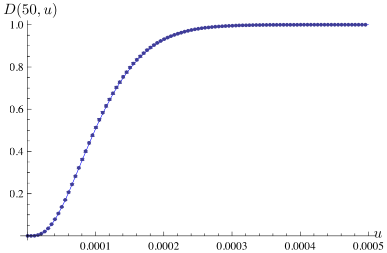
Source:
Poisson arrivals

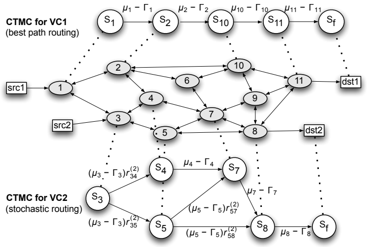
Exponential service time

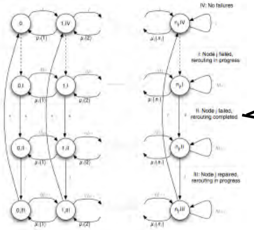
Modeling approach

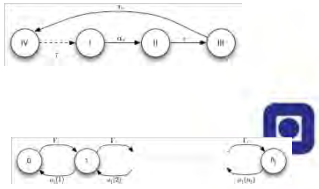
- Response time blocks for delay distributions
- Space-time decomposition to reduce models
- Time samples to model routing protocol behavior





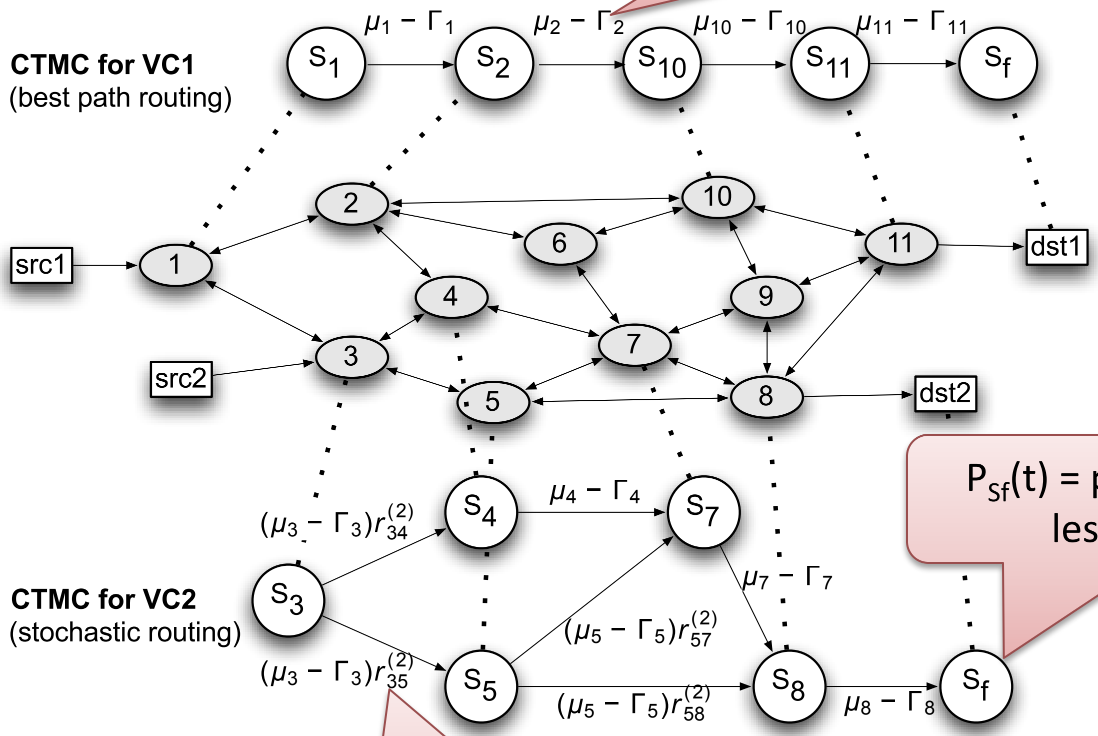



IV: No failures
I: Node j failed, rerouting in progress
II: Node j failed, rerouting completed
III: Node j repaired, rerouting in progress



Resp

Γs are determined by traffic equations

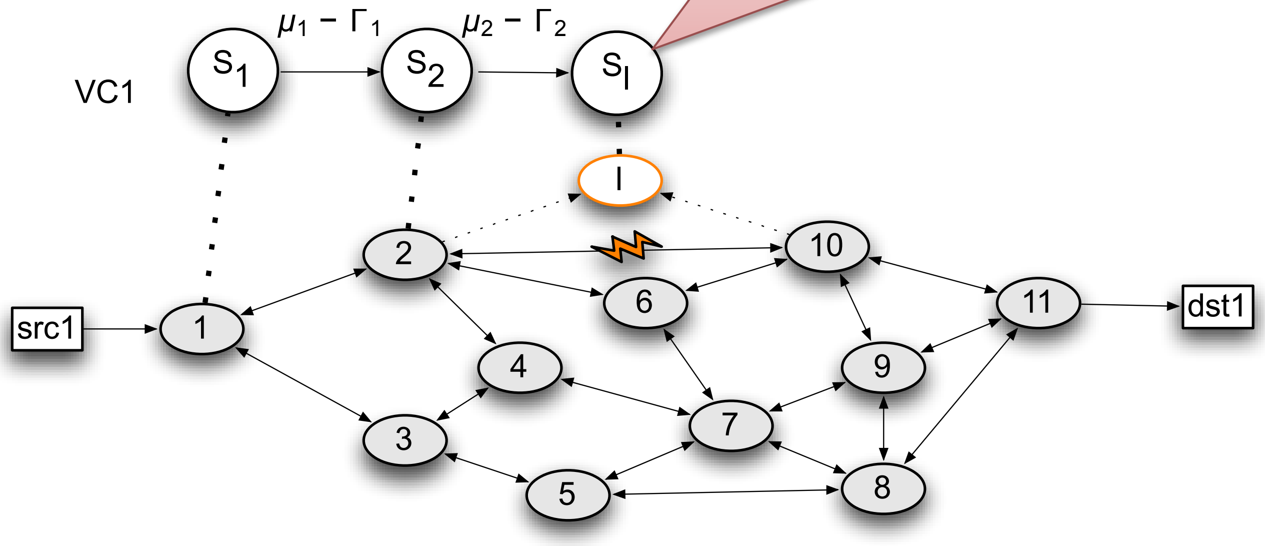


$P_{Sf}(t)$ = probability of delay less or equal to t

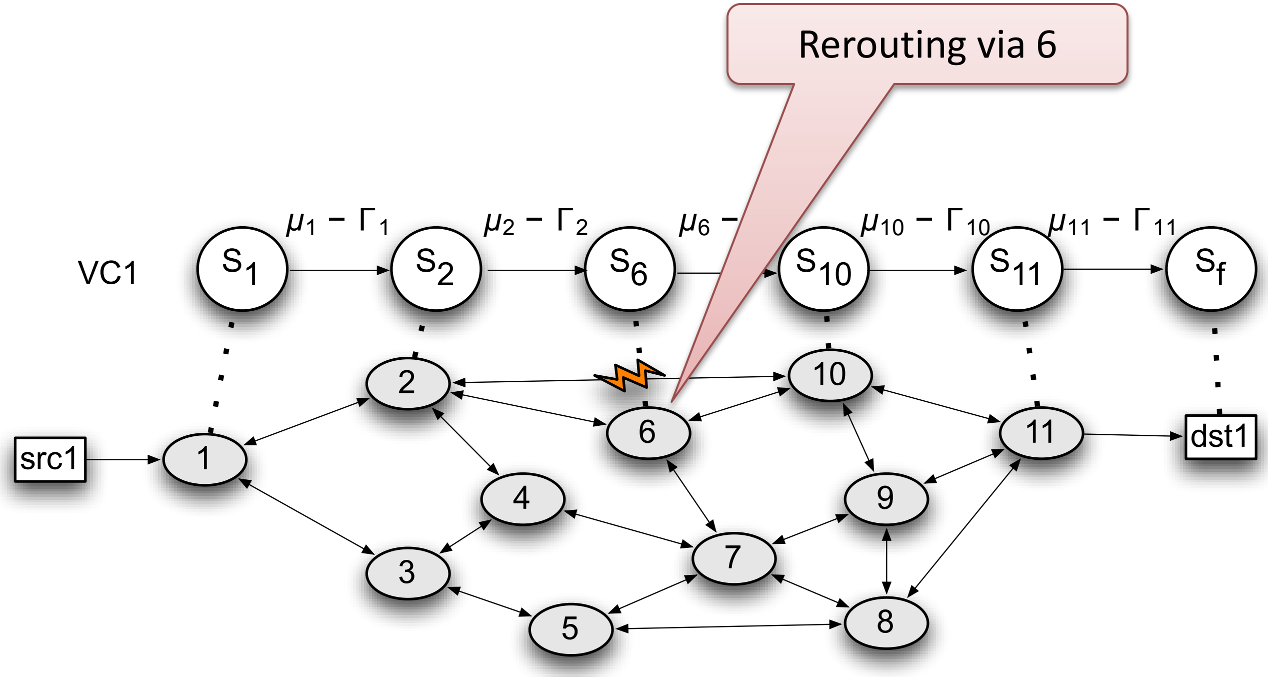
Routing probability from node 3 to 5 of VC2

Response time blocks –link down

All traffic lost until rerouting takes effect, $P_{Sf}(t) = 0$



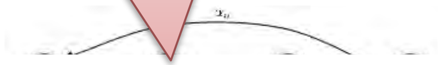
Response time blocks – rerouting

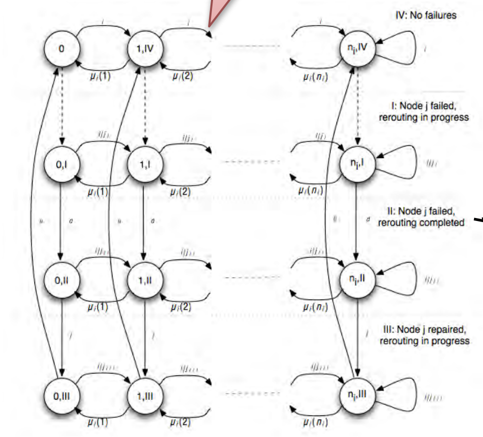


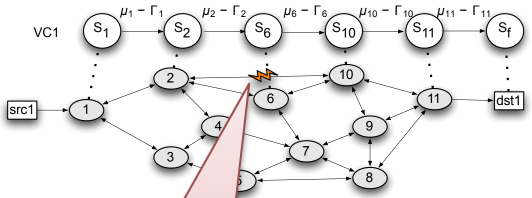
Space-time decomposition

State space explosion!

Each phase (routing time sample) reaches stable state



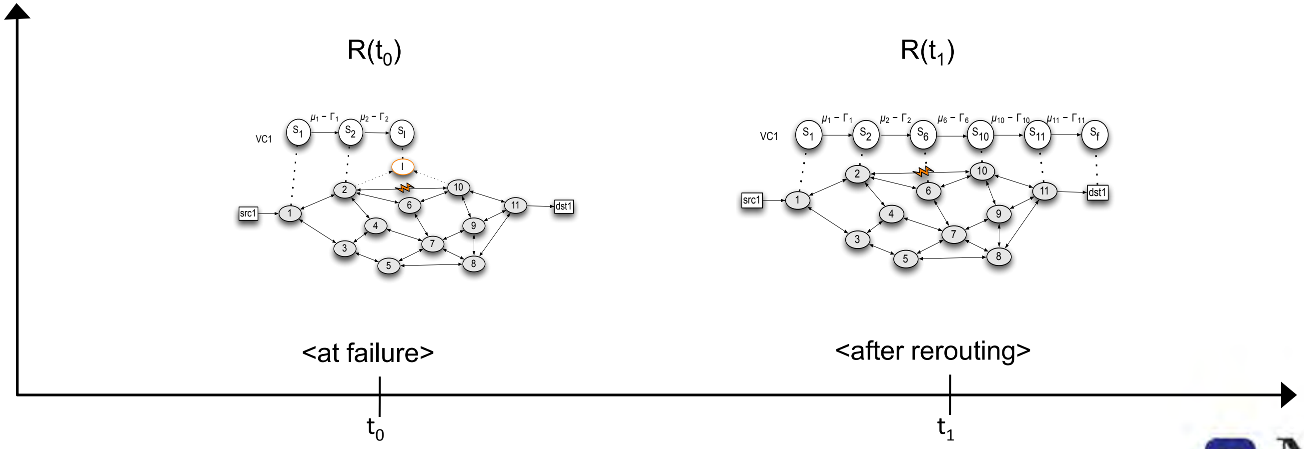

0
1,IV
n_j,IV
IV: No failures
$\mu_j(1)$
$\mu_j(2)$
$\mu_j(n_j)$
0,I
1,I
n_j,I
I: Node j failed, rerouting in progress
0,II
1,II
n_j,II
II: Node j failed, rerouting completed
0,III
1,III
n_j,III
III: Node j repaired, rerouting in progress



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, $R(t) = \{r_{ij}^{(vc)}(t)\}$



$R(t_0)$

$R(t_1)$

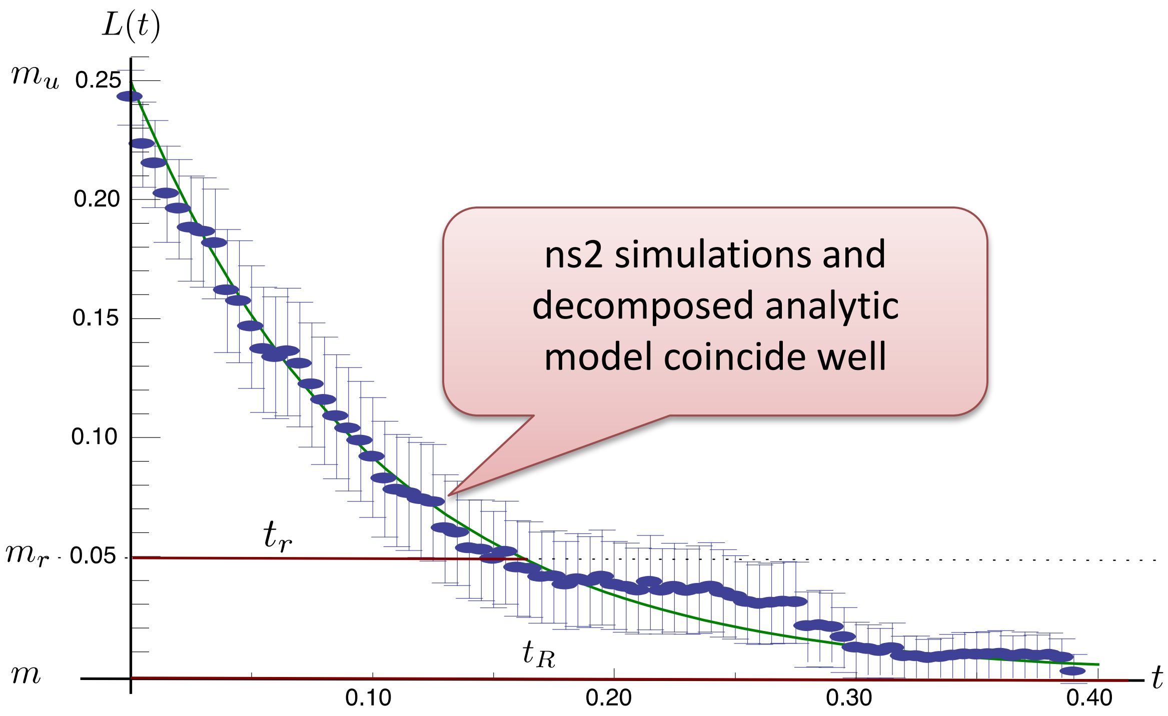
<at failure>

<after rerouting>

t_0

t_1

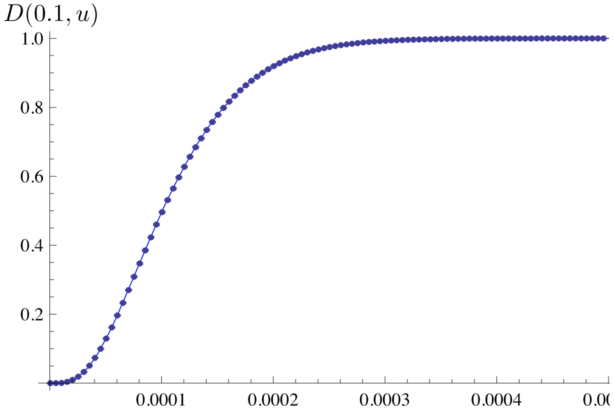
Numerical example: packet loss probability



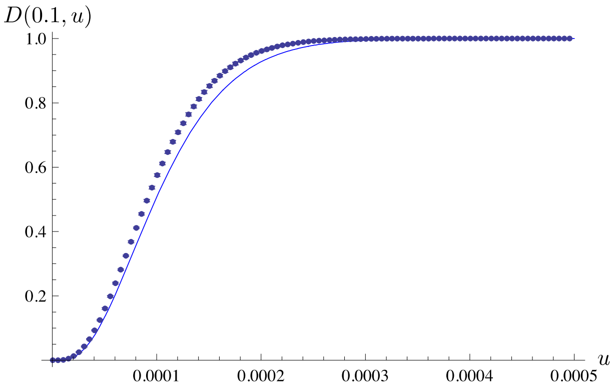
ns2 simulations and decomposed analytic model coincide well

Norwegian University of Science and Technology

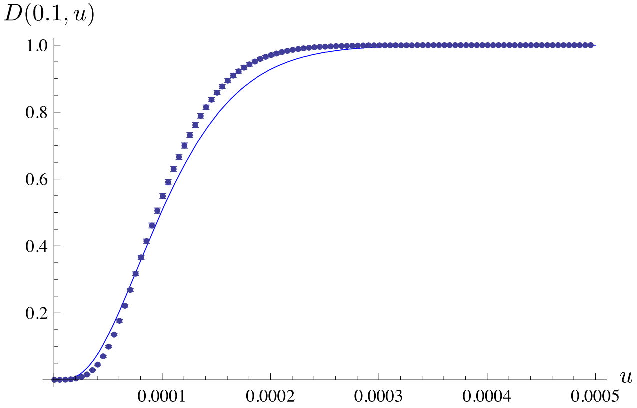
Numerical example: delay distribution



All exponential

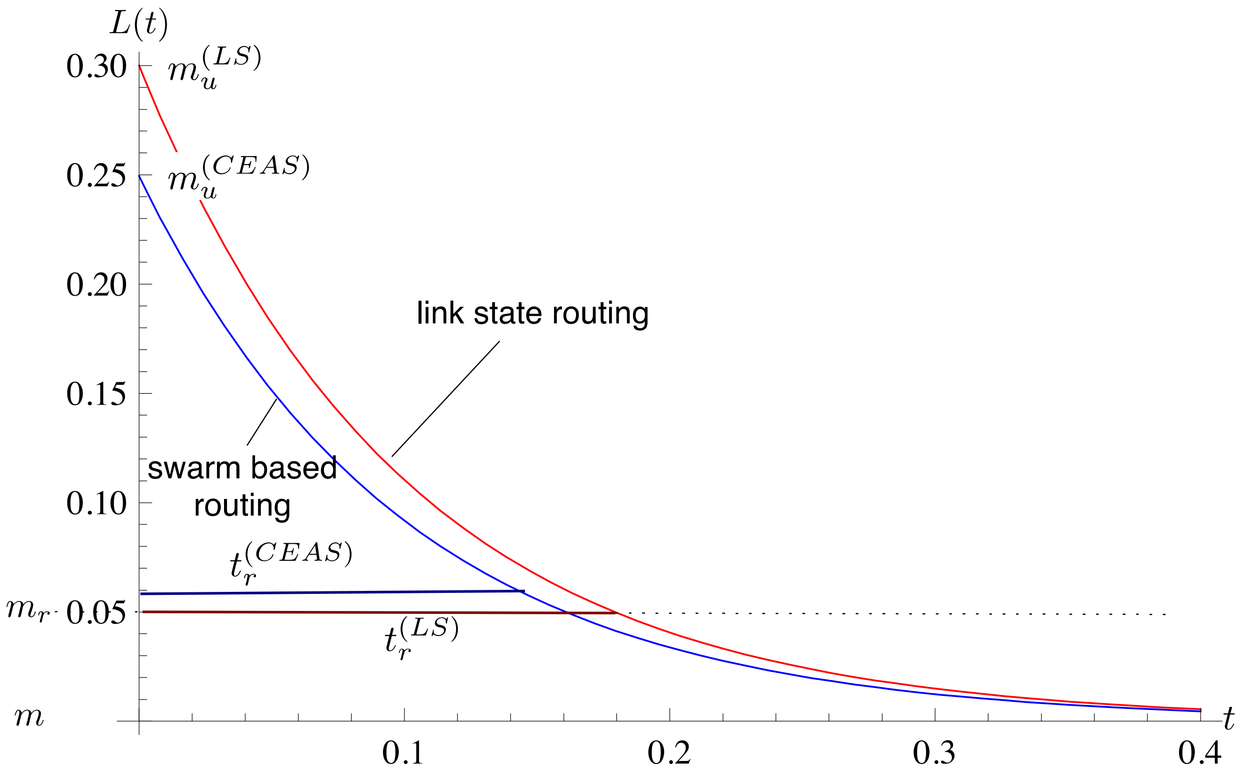


Pareto service times

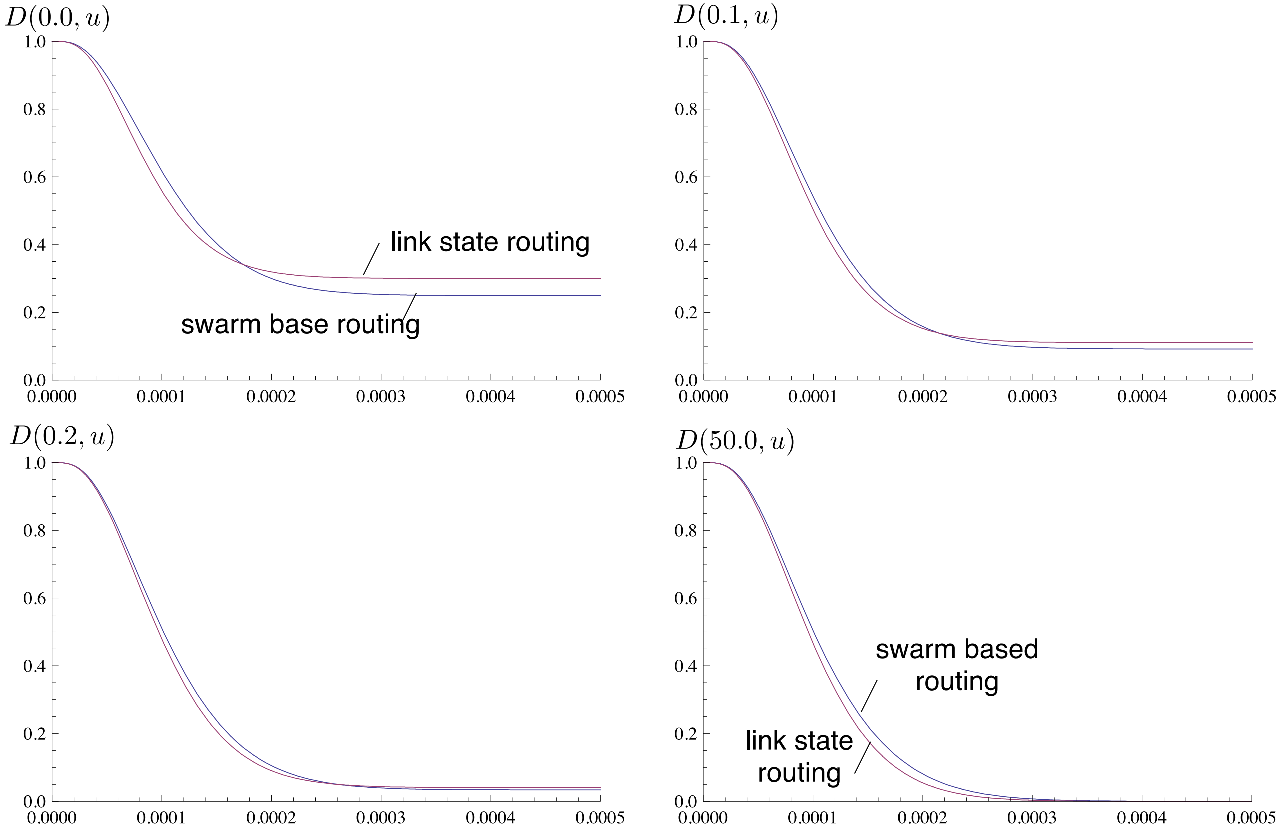


Pareto arrival times

Numerical example: packet loss probability



Numerical example: delay distribution



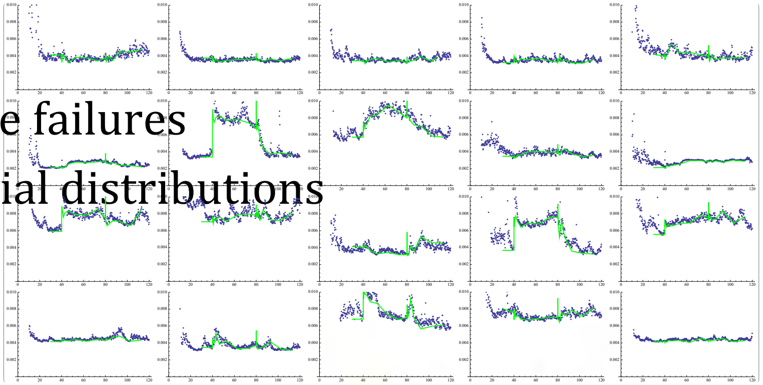
NTNU
Norwegian University of Science and Technology

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



NTNU
Norwegian University of
Science and Technology

References

- A. Avizienis, J. Laprie and B. Randell, Fundamental Concepts of Computer System Dependability, IARP/IEEE-RAS Workshop on Robot Dependability, Seoul, Korea,
May 2001.
- G. Bischoff, Is Telecom Ready for Emergencies? Telephony, September 8, 2003,
pp. 46-50.
- D.Y. Chen, S. Garg, and K.S. Trivedi, Network survivability performance evaluation: a quantitative approach with applications in wireless ad-hoc networks ,, ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM' 02), Atlanta, GA, September 2002.
- R.J. Ellison, D.A. Fischer, R.C. Linger, H.F. Lipson, T. Longstaff, and N.R.Mead. Survivable network systems: an emerging discipline. Technical report, Technical Report CMU/SEI-97-TR-013, November 1997, revised May 1999.
- Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) VI Homeland Security Physical Security Focus Group Report, December 2002, Issue 1.
- L. Garber, Denial-of-Service Attacks Rip the Internet, Computer, Vol 33, Issue 4, April 2000, pp. 12-17.
- R. Huslende, A combined evaluation of performance and reliability for degradeable systems, ACM/SIGMETRICS, pp. 157-164, ACM, 1981.
- M. L. Jones, R. K. Butler, and W. C. Szeto. Sprint long distance network survivability: today and tomorrow. IEEE Communications Magazine, 37(8):58–62, August 1999.
- J. Knight and K. Sullivan, On the definition of survivability, TR-CS-00-33, University of Virginia, Dec., 2000.
- J. Knight, E. Strunk and K. Sullivan, Towards a Rigorous Definition of Information System Survivability, DISCEX 2003.
- S. Liew and K. Lu, A framework of characterizing disaster-based network survivability, IEEE JSAC, 12(1):52-58, Jan, 1994.

Reference

- Y. Liu , V. B. MendirattaS and K. S. Trivedi, Survivability analysis of telephone access network Proc. of 15th IEEE International Symposium on Software Engineering (ISSRE'04)
- Y. Liu and K. S. Trivedi, Survivability Quantification: The Analytical Modeling Approach, Int. J. Performability Engineering, 2(1) 2006.
- B.B. Madan, K. Gogeva-Popstojanova, K. Vaidyanathan, K.S. Trivedi, Modeling and quantification of security attributes of software systems, Dependable Systems and Networks, 2002. Proceedings. International Conference on, pp505-514, June 2002.
- J. Manchester, P. Bonenfant, and C. Newton. The evolution of transport network survivability, IEEE Communications Magazine, 37(8):44–51, August 1999.
- Marsh, T. (ed.), Critical Foundations: Protecting America's Infrastructures, Technical Report, President's Commission on Critical Infrastructure Protection, October 1997.
- D. Medhi and D. Tipper, "Multi-layered Network Survivability Models, Analysis, Architecture, Framework and Implementation: An Overview," DARPA Information Survivability Conference and Exposition, DISCEX 2000, January 2000.
- V. B. Mendiratta and C. A. Witschorik. Telephone service survivability. In IEEE workshop on the design of reliable communication networks (DRCN2003), October 2003.
- C. Metz, "IP Protection and Restoration," IEEE Internet Computing, Vol 4, Issue 2, March-April 2000, pp. 97-102.
- J. F.Meyer. On evaluating the performability of degradable computing systems. IEEE Transactions on Computers, 29(8):720–731, August 1980.
- P. G. Neumann. Practical architectures for survivable systems and networks. Technical report, Computer Science Laboratory, SRI International, CA, 2000.
- R. A. Sahner, K. S. Trivedi, and A. Puliafito. Performance and Reliability Analysis of Computer Systems: An Example-Based Approach Using the SHARPE Software Package. Kluwer Academic, December 1995.
- T1A1.2 Working Group on Network Survivability Performance, Technical report on enhanced network survivability performance, Feb., 2001

NTNU
Norwegian University of Science and Technology

Reference

- R. M. Smith, K. S. Trivedi, and A. Ramesh, Performability Analysis: Measures, An Algorithm and a Case Study, IEEE Transactions on Computers, Vol. C-37, No. 4, pp. 406-417, Apr. 1988. This paper is a standard reference for performability.
- D. Tipper, J. L. Hammond, S. Sharma, A. Khetan, K. Balakrishnan, S. Menon, An analysis of the congestion effects of link failures in wide area networks, Selected Areas in communications, IEEE Journal on , Volume: 12 , Issue: 1 , Jan. pp.179-192, 1994.
- K. S. Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications, John Wiley & Sons, 2nd edition, 2001.
- C.-Y. Wang, D. Logothetis, K. S. Trivedi, and I. Viniotis. Transient behavior of ATM networks under overloads. In IEEE INFOCOM' 96, pages 978–985, San Francisco, CA, March 1996.
- Federal standard 1037C, Telecommunications: Glossary of telecommunication terms, 1996