

Resilient and Survivable Networking

The University of Kansas EECS 983

Survivability – Spring 2008

James P.G. Sterbenz
Abdul Jabbar Mohammad

Department of Electrical Engineering & Computer Science
Information Technology & Telecommunications Research Center
The University of Kansas



jpgs@eecs.ku.edu

<http://www.ittc.ku.edu/~jpgs/courses/rsnets>

Resilient and Survivable Networking

Survivability

- SV.1 Overview and definitions
- SV.2 Survivability strategies
- SV.3 Techniques and mechanisms
- SV.4 Evaluation and measurement

Survivability

SV.1 Overview and Definitions

SV.1 Overview and definitions

SV1.0 Evolution of the survivability discipline

SV1.1 Survivability definition and characteristics

SV1.2 Relationship to other disciplines

SV.2 Survivability strategies

SV.3 Techniques and mechanisms

SV.4 Evaluation and measurement

Survivability

SV.1.0 Evolution of Survivability

SV.1 Overview and definitions

SV1.0 Evolution of the survivability discipline

SV1.1 Survivability definition and characteristics

SV1.2 Relationship to other disciplines

SV.2 Survivability strategies

SV.3 Techniques and mechanisms

SV.4 Evaluation and measurement

Survivability

Evolution

- Earlier than 70's
 - two independently studied fields: reliability and performance
 - reliability : system provides service without interruption
 - redundancy was the chosen mechanism
 - performance: characteristics of the service/system

Survivability Evolution

- Late 70's / Early 80's
 - realization: inability to provide adequate redundancy to overcome all failures [Losq-1977] [Ng-1977] [Beaudry-1978]
 - failures: random faults with a probability of occurrence (ROF)
 - new concept: *degradable systems*
 - relationship between performance and reliability
 - degraded performance during failures, without complete service failure

Survivability

Evolution

- Degradable systems
 - Meyer coined the term *performability*
 - probability that the system will stay above a certain accomplishment level over a fixed period of time
 - performance: 2nd dimension of reliability [Huslende-1981]
 - Markovian system analysis
 - [Gay-1979] [Meyer-1980] [Huslende-1981]
 - performance levels represented by continuous time discrete states
 - reliability and availability analysis
 - how long will system stay in a given state
 - aggregate performance based on all visited states

Survivability

Evolution

- Fault tolerance to survivability
 - research in 80's focussed on random faults (ROF)
 - late 80's and early 90's addressed the ability of the network to survive large scale attacks and disasters
 - [Newport-1990] [ATIS-1993] [Liew-1994] [Ellison-1999]
 - hence the concept of survivability

Survivability

SV.1.1 Definition and Characteristics

SV.1 Overview and definitions

SV1.0 Evolution of the survivability discipline

SV1.1 Survivability definition and characteristics

SV1.2 Relationship to other disciplines

SV.2 Survivability strategies

SV.3 Techniques and mechanisms

SV.4 Evaluation and measurement

Survivability

Definitions

- *Survivability*
 - capability of a system to fulfill mission in a timely manner
 - in presence of large-scale natural disasters, attacks, failures
- Characteristics [Ellison-1999]
 - mission: set of high-level requirements or goals
 - reasonable/expected behaviour during impairments
 - lacks multilevel view
 - often measured with dependability & performance metrics
 - applied to unbounded systems
 - distributed control, limited visibility and unpredictable growth
 - *mission fulfilment* must survive, even when system does not

Survivability

Challenges Addressed

- *Subset of challenges addressed*
 - unintentional misconfiguration or operational mistakes
 - malicious attacks
 - large-scale natural disasters
 - environmental challenges
 - mobility
 - weak and episodic channels (typically wireless)
 - unpredictably long delay
 - unusual but legitimate traffic (e.g. flash crowd)
 - service failure at a lower level

Survivability

SV.1.2 Relationship to other disciplines

SV.1 Overview and definitions

SV1.0 Evolution of the survivability discipline

SV1.1 Survivability definition and characteristics

SV1.2 Relationship to other disciplines

SV.2 Survivability strategies

SV.3 Techniques and mechanisms

SV.4 Evaluation and measurement

Survivability

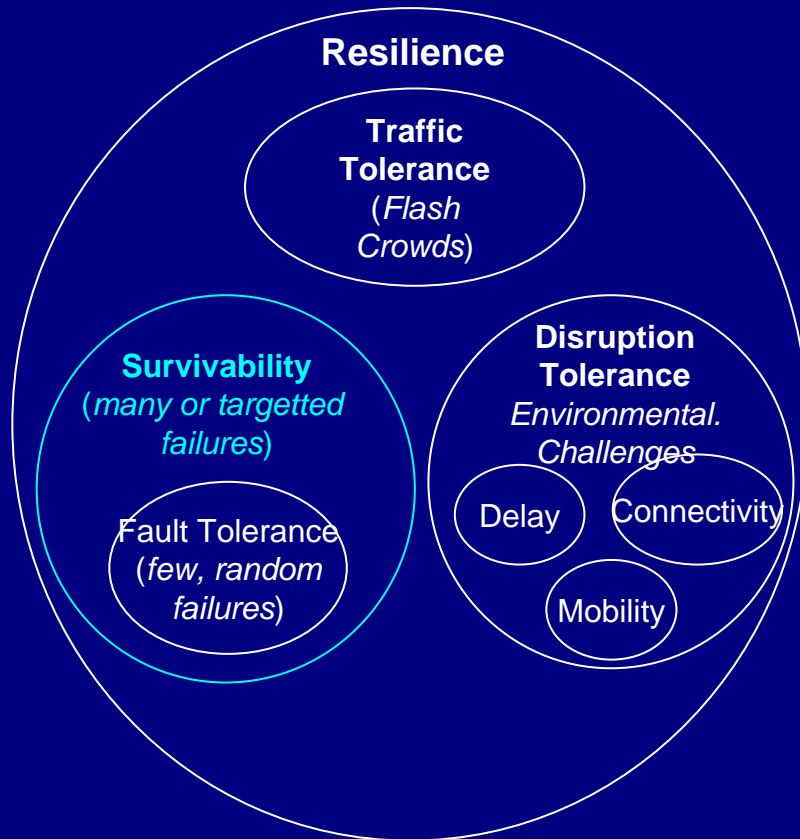
Relationship to other disciplines

- Survivability is related to challenges
 - subset of resilience
 - peer to disruption-tolerance and traffic-tolerance
- Survivability measured by other disciplines
 - performance
 - dependability: availability, reliability, etc.
 - security

Survivability

Relationship to Other Disciplines

Challenge Based Concepts



Measurement and Metrics



Survivability

Relationship to Other disciplines

- Survivability
 - deals with highly correlated failure events
 - includes both malicious attacks & non-malicious events
 - considers failures by intelligent adversaries as well
- Fault tolerance
 - considers random failures at component level
 - includes only non-malicious events
 - considers statistical probabilities of failures

Survivability

Relationship to Other disciplines

- Survivability
 - survivability is robustness under attack
 - considers a range of survivability levels
 - emphasizes performance of a compromised system
- Security
 - security is hardness to attacks
 - security is *considered* binary (true/false?)
 - does not consider performance of a compromised system

Survivability

SV.2 Survivability Strategies

- SV.1 Overview and definitions
- SV.2 Survivability strategies
- SV.3 Techniques and mechanisms
- SV.4 Evaluation and measurement

Survivability

SV.2 Survivability Strategies

SV.1 Overview and definitions

SV.2 Survivability Strategies

SV2.1 CERT strategy

SV2.2 ANSA strategy

SV2.3 SUMOWIN strategy

SV2.4 ResiliNets strategy

SV.3 Techniques and mechanisms

SV.4 Evaluation and measurement

Survivability Strategies

- Survivability strategy
 - set of architectural properties and techniques
 - typically a multi-step strategy
 - several research groups have proposed strategies

Survivability Strategies

SV.2.1 CERT at CMU

SV.1 Overview and definitions

SV.2 Survivability Strategies

SV2.1 CERT Strategy

SV2.2 ANSA Strategy

SV2.3 SUMOWIN strategy

SV2.3 ResiliNets strategy

SV.3 Techniques and mechanisms

SV.4 Evaluation and measurement

Survivability Strategies

CERT Scheme

- CERT Coordination Center at CMU proposed strategy [Ellison 1999]
 - three R's: resistance, recognition, recovery
 - adaptation and evolution

Survivability Strategies

CERT Scheme

- CERT Coordination Center at CMU proposed strategy
 - resistance
 - traditional security
 - diversity, redundancy
 - specialization
 - trust validation and
 - observed stochastic properties
 - recognition
 - recovery
 - adaptation and evolution

Survivability Strategies

CERT Scheme

- CERT Coordination Center at CMU proposed strategy
 - resistance
 - recognition
 - analytical redundancy and testing
 - intrusion monitoring
 - system behavior
 - integrity monitoring
 - recovery
 - adaptation and evolution

Survivability Strategies

CERT Scheme

- CERT Coordination Center at CMU proposed strategy
 - resistance
 - recognition
 - recovery
 - redundancy
 - diverse location of information resources
 - contingency planning and response teams
 - adaptation and Evolution

Survivability Strategies

CERT Scheme

- CERT Coordination Center at CMU proposed strategy
 - resistance
 - recognition
 - recovery
 - adaptation and evolution
 - changes to above steps based on past experiences
 - broadcast of warnings
 - adaptations
 - retaliation

Survivability Strategies

CERT Scheme Principles

- Principles of (observations from) survivability
 - tradeoff between survivability and cost/complexity
 - survivability is emergent and stochastic
 - survivability analysis is protocol based (not topology based)
 - requirements should be specified for all phases and services
 - system and survivability
 - usage and intrusion
 - development, operations and evolution

Survivability Strategies

SV.2.2 ANSA Strategy

SV.1 Overview and definitions

SV.2 Survivability Strategies

SV2.1 CERT Strategy

SV2.2 ANSA Strategy

SV2.3 SUMOWIN strategy

SV2.4 ResiliNets strategy

SV.3 Techniques and mechanisms

SV.4 Evaluation and measurement

Survivability Strategies

ANSA

- ANSA: Advances Systems Network Architecture
 - large 1980's system design project
 - dependability one aspect [Edwards et al.]

Survivability Strategies

ANSA Strategy

- ANSA multi-aspect strategy
 - fault confinement
 - fault detection (should be error/failure detection)
 - fault diagnosis
 - reconfiguration
 - recovery
 - restart
 - repair
 - reintegration

Survivability Strategies

SV.2.3 SUMOWIN Strategy

SV.1 Overview and definitions

SV.2 Survivability Strategies

SV2.1 CERT Strategy

SV2.2 ANSA Strategy

SV2.3 SUMOWIN strategy

SV2.4 ResiliNets strategy

SV.3 Techniques and mechanisms

SV.4 Evaluation and measurement

Survivability Strategies

SUMOWIN

- SUMOWIN: Survivable Mobile Wireless Networks
 - DARPA seedling project under Doug Maughan
 - work done at BBN by Sterbenz, Krishnan, et al. [Sterbenz-Krishnan 2002]
- Three steps
 - maintain connectivity when possible
 - communicate when stable end-to-end path not possible
 - use new and enabling technologies
 - airborne nodes and satellites
 - active and programmable networks

Survivability Strategies

SV.2.4 ResiliNets Strategy

SV.1 Overview and definitions

SV.2 Survivability Strategies

SV2.1 CERT Strategy

SV2.2 ANSA Strategy

SV2.3 SUMOWIN strategy

SV2.4 ResiliNets strategy

SV.3 Techniques and mechanisms

SV.4 Evaluation and measurement

Survivability Strategies

ResiliNets

- ResiliNets:
Resilient and Survivable Networks and Services
[Sterbenz, Hutchison et al.]
 - recall: D^2R^2 + DR two phase strategy
- D^2R^2 real-time operational loop
 - defend, detect, remediate, recover
- DR background loop
 - diagnose, refine

Survivability

SV.3 Techniques and Mechanisms

- SV.1 Overview and definitions
- SV.2 Survivability Strategies
- SV.3 Techniques and mechanisms
- SV.4 Evaluation and measurement

Survivability

SV.3 Techniques and Mechanisms

- SV.1 Overview and definitions
- SV.2 Survivability Strategies
- SV.3 Techniques and mechanisms
 - SV3.1 Redundancy
 - SV3.2 Diversity
 - SV3.3 ATIS recommendations
- SV.4 Evaluation and measurement

Survivability Techniques

SV.3.1 Redundancy

- SV.1 Overview and definitions
- SV.2 Survivability Strategies
- SV.3 Techniques and mechanisms
 - SV3.1 Redundancy
 - SV3.2 Diversity
 - SV3.3 ATIS recommendations
- SV.4 Evaluation and measurement

Survivability Techniques

Redundancy for Fault Tolerance

- Redundancy: multiple components or mechanisms
 - fundamental and primary technique for fault-tolerance
 - Lecture FT*
 - recall: fault tolerance is a subset of survivability

Survivability Techniques

SV.3.2 Diversity

- SV.1 Overview and definitions
- SV.2 Survivability Strategies
- SV.3 Techniques and mechanisms
 - SV3.1 Redundancy
 - SV3.2 Diversity
 - SV3.3 ATIS recommendations
- SV.4 Evaluation and measurement

Diversity

Definition and Measure

- *Diversity* consists of providing different alternatives
 - when challenges impact particular alternatives other alternatives prevent degradation
 - *degree of diversity*: number of different alternatives
 - alternative can either be:
 - simultaneously operational to defend
 - available for use as needed to remediate

Diversity

Spatial

- *Diversity* consists of providing different alternatives
- *Spatial diversity*: diversity across space
 - requires degree of at least redundancy degree
 - *topological diversity*: across logical network topology
 - *geographic diversity*: across physical network topology
 - both are necessary *why?*
- Temporal diversity
- Operational diversity

Diversity

Spatial

- *Diversity* consists of providing different alternatives
- *Spatial diversity*: diversity across space
 - requires degree of at least redundancy degree
 - *topological diversity*: across logical network topology
 - *geographic diversity*: across physical network topology
 - both are necessary: logical and physical topology entwined
- Temporal diversity
- Operational diversity

Diversity

Temporal

- *Diversity* consists of providing different alternatives
- *Spatial diversity*: diversity across space
- *Temporal diversity*: diversity in time
 - e.g. variation to resist traffic analysis
- Operational diversity

Diversity

Operational

- *Diversity* consists of providing different alternatives
- *Spatial diversity*: diversity across space
- *Temporal diversity*: diversity in time
- *Operational diversity*: implementation & mechanism
examples?

Diversity

Operational

- *Diversity* consists of providing different alternatives
- *Spatial diversity*: diversity across space
- *Temporal diversity*: diversity in time
- *Operational diversity*: implementation & mechanism
 - implementation: e.g. protocol or OS choices
 - monoculture avoidance (MS-Windows, IOS, TCP/IP)
 - medium: e.g. wired and wireless
 - mechanism: e.g. open vs. closed loop (ARQ vs. FEC)

Survivability Techniques

SV.3.3 ATIS Recommendations

- SV.1 Overview and definitions
- SV.2 Survivability Strategies
- SV.3 Techniques and mechanisms
 - SV3.1 Redundancy
 - SV3.2 Diversity
 - SV3.3 ATIS recommendations
- SV.4 Evaluation and measurement

Survivability Techniques

SV.4 Evaluation and Measurement

- SV.1 Overview and definitions
- SV.2 Survivability Strategies
- SV.3 Techniques and mechanisms
- SV.4 Evaluation and measurement

Techniques and Mechanisms

ATIS Recommendations

- [TBD]

Survivability

References and Further Reading

- References on wiki.ittc.ku.edu/resilinet/Survivability

End of Foils