

Mobile Wireless Networking
The University of Kansas EECS 983
Introduction & Motivation – Spring 2008

James P.G. Sterbenz

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



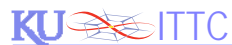
jpgs@eecs.ku.edu

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

22 January 2008

rev. 0.9

© 2004–2008 James P.G. Sterbenz



© James P.G. Sterbenz

Resilient and Survivable Networking
Outline

- IM.1 Motivation
- IM.2 Past failures (introduction)
- IM.3 Communication environment
- IM.4 Disciplines

22 January 2008

KU EECS 983 – Resilient & Survivable Nets – Introduction

RSN-IM-2

Resilient and Survivable Networking

IM.1 Motivation

- IM.1 Motivation
- IM.2 Past failures (introduction)
- IM.3 Communication environment
- IM.4 Disciplines

Resilience and Survivability

Motivation: Reliance

- Increasing reliance on network infrastructure
 - consumers
 - commerce & financial
 - government and military
- ⇒ Increasingly severe consequences of disruption
- ⇒ Increasing attractiveness as target from bad guys

Resilience and Survivability

Motivation: Consequences

- Increasing reliance on network infrastructure
 - ⇒ Increasingly severe consequences of disruption
 - threat to life and quality of life
 - threat to financial health economic stability
 - threat to national and global security
 - ⇒ Increasing attractiveness as target from bad guys

Resilience and Survivability

Motivation: Attractiveness

- Increasing reliance on network infrastructure
 - ⇒ Increasingly severe consequences of disruption
 - ⇒ Increasing attractiveness as target from bad guys
 - recreational and professional crackers
 - industrial espionage and sabotage
 - terrorists and information warfare

Resilient and Survivable Networking

IM.2 Past Failures (Introduction)

- IM.1 Motivation
- IM.2 Past failures (introduction)
- IM.3 Communication environment
- IM.4 Disciplines

Past Disasters: Hinsdale

Overview

- 1988 Hinsdale Illinois Bell central office fire
 - 100K customers lose service for *weeks*
 - also major disruptions in
 - long distance
 - 800
 - 911
 - cellular
 - ATC for O'Hare

Past Disasters: Hinsdale

Lessons

- Fault tolerance not sufficient
- Resilience requires
 - spatially diverse redundancy
 - separation of infrastructures

Past Disasters: Katrina

Timeline1

- 2005 hurricane Katrina timeline
[http://en.wikipedia.org/wiki/Timeline_of_Hurricane_Katrina]
 - Storm surge potential devastation to NO well understood
 - including Oct. 2004 *National Geographic* article
 - 23 Aug 17:00 EDT TD 12 announced
 - 24 Aug 11:00 EDT upgraded to TS Katrina
 - 25 Aug 17:00 EDT upgraded to hurricane cat 1
 - 25 Aug 18:30 EDT 1st landfall Dade/Broward FL
 - 26 Aug 01:00 EDT downgraded to tropical storm
 - 26 Aug 05:00 EDT upgraded to cat 1 hurricane
 - 26 Aug LA gov declares emergency
 - 26 Aug 23:00 EDT NHC forecasts landfall at Buras LA

Past Disasters: Katrina Timeline2

- 2005 hurricane Katrina timeline
 - 27 Aug 05:00 EDT upgraded to cat 3
 - 27 Aug NO mayor orders voluntary evac
 - 27 Aug LA gov asks fed disaster decl.
 - including NO and Jefferson Parish
 - 27 Aug US pres declares disaster for LA
 - 27 Aug FEMA issues disaster order
 - does *not* include NO or Jefferson Parish
 - 27 Aug NHC briefs pres, LAgov, NO mayor
 - 28 Aug 12:40 CDT upgraded to cat 4
 - 28 Aug 07:00 CDT upgraded to cat 5

Past Disasters: Katrina Timeline3

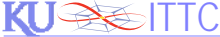
- 2005 hurricane Katrina timeline
 - 27–28 NO surge inundation predicted
 - Weather Channel, Wunderground, etc.
 - 28 Aug 11:01 CDT NWS predicts devastating damage:
 - major structural failure; uninhabitable for weeks
 - power outages lasting for weeks
 - 28 Aug mandatory NO evacuation ordered
 - 28 Aug pres issues disaster for AL, MS, FL
 - 28 Aug LA gov requests Nat. Guard
 - (but not authorised until 1 Sep)
 - 29 Aug 06:10 CDT landfall near Buras and NO

Past Disasters: Katrina Timeline4

- 2005 hurricane Katrina timeline
 - 29 Aug 08:00 CDT flooding reported Industrial Canal
 - 29 Aug 14:00 CDT NO confirms 17th St. Levee breach
 - 29 Aug FEMA director discourages outside help
 - 30 Aug 60–80% of NO under water
 - 30 Aug pres announces task force to meet 31 Aug
 - 30 Aug DHS sec. decl. Incident Nat. Significance
 - 31 Aug first relief supplies to NO Superdome
 - 31 Aug BNSF and NS restore most rail service

Past Disasters: Katrina Timeline5

- 2005 hurricane Katrina timeline
 - 01 Sep aft CNN broadcasts from conv. center
 - drove in on Crescent City Connection (Bus. US-90)
 - 01 Sep eve DHS sec dismisses con. ctr. as rumor
 - 01 Sep Gretna LA seals Bus. US-90 with force

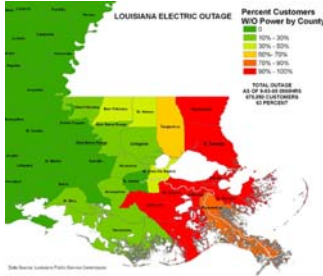

© James P.G. Sterbenz

Past Disasters: Katrina


Infrastructure Relationships

- Power grid fails
 - lines downed by trees/wind; facilities flooded
 - 2.6M w/o power
 - NO power out for a month
 - restoration crews unavailable
 - still in FL
 - lack food, water, shelter
- Communication and network infrastructure
 - insufficient battery and generator backup
 - backup not robust (time duration and spatial diversity)

[\[http://www.oe.netl.doe.gov/hurricanes_emer/katrina.aspx\]](http://www.oe.netl.doe.gov/hurricanes_emer/katrina.aspx)



22 January 2008
KU EECS 983 – Resilient & Survivable Nets – Introduction
RSN-IM-15


© James P.G. Sterbenz

Past Disasters: Katrina

Emergency Communications Impact

- Incompatible communications
 - NO 1992 M/A-Com
 - LA 1996 Motorola
 - multiple incompatible federal systems
 - MS national guard used sneakernet
- NO communication not survivable
 - Energy Center tower lost power
 - backup power transformer taken out by glass shard
 - MA-Com repair crews denied entry for 3 days by state police
- Amateur radio again critical

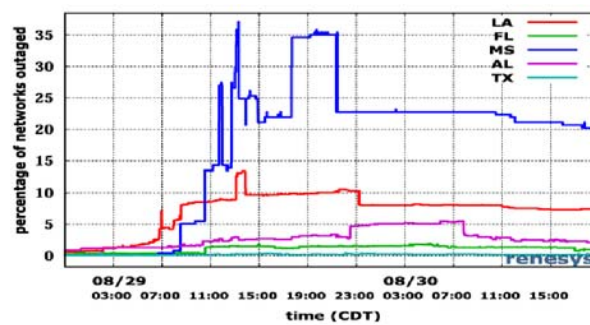
22 January 2008
KU EECS 983 – Resilient & Survivable Nets – Introduction
RSN-IM-16

Past Disasters: Katrina PSTN Impact

- 1.3 million Bellsouth customers out
[<http://www.networkworld.com/news/2005/090505-katrina.html>]
- Most cellular telephone service fails
 - cell towers have insufficient battery backup
 - remaining network severely overloaded
 - Wireless operators
 - refuse to release data on outages
 - claim network is robust – regulation for backup life not needed
 - regulation proposed after 9/11
[http://schumer.senate.gov/SchumerWebsite/pressroom/press_releases/PR01953.html]
- Few satellite phones
 - many with dead batteries

Past Disasters: Katrina Internet Impact

- Little impact on national Internet service
- Significant impact on local Internet service [Renesys]

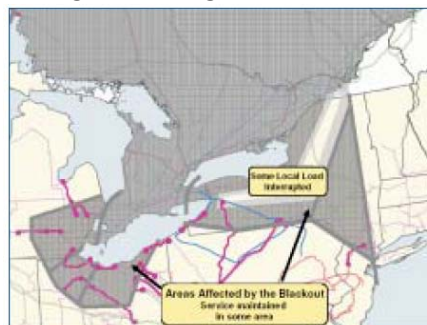


Past Disasters: Katrina Failures

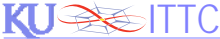
- Disaster preparedness
 - long-term planning and infrastructure deployment
 - brittle power grid: lines above ground, facilities floodable
 - non interoperable first-responder infrastructure
 - brittle network infrastructure
 - short-term planning
 - insufficient preparation for storm
- Response
 - long-term planning for rapid deployment
 - almost non-existent
 - short-term response
 - insufficient equipment staging for response

Past Disasters: NE Power Failure Overview

- 265 power plants with 508 generating units offline
- ~10M without power
 - OH, MI
 - PA, NY
 - QC



[<https://reports.energy.gov/BlackoutFinal-Web.pdf>]

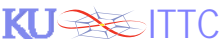

© James P.G. Sterbenz

Past Disasters: NE Power Failure

Timeline Stage 1: Ohio Grid Collapse

- Phase 1: 12:15 – 14:14
 - two plants down
 - high load summer day; third goes offline
- Phase 2: 14:14 – 15:59
 - alarm process stalls; servers fail
 - operations doesn't know for 1 hr even though IT does
- Phase 3: 15:05 – 15:57
 - three 345kV transmission lines downed
- Phase 4: 15:39 – 16:08
 - 138kV grid collapse in N OH

22 January 2008
KU EECS 983 – Resilient & Survivable Nets – Introduction
RSN-IM-21


© James P.G. Sterbenz

Past Disasters: NE Power Failure

Timeline

	12:00	13:00	14:00	15:00	16:00
Grid Events	Phase 1: A normal afternoon degrades 12:15-14:14	13:31 Eastlake 5 trips	14:02 Stuart-Atlanta 345 kV fails (tree)	14:27 Star-S Canton 345 kV trips & recloses (tree)	15:05 Hanna-Juniper 345 kV fails (tree) 15:32 First FE 138 kV line fails 15:39 Star-S Canton 345 kV fails (tree)
Computer Events	12:15 MISO SE problems begin	14:02 Stuart-Atlanta 345 kV line trip confuses MISO SE	14:14 FE EMS alarms fail 14:20 FE loses half its remote consoles	14:41 FE primary EMS server fails 14:54 FE back-up EMS server fails	15:08 FE primary EMS server restarts 15:46-15:59 FE IT rebooting H4, H1
Human Events		14:32 FE EMS doesn't update	14:32 AEP calls FE re: Star-S Canton trip	15:19 AEP again calls FE re: Star-S Canton 15:36 MISO calls FE re: Star-Juniper 15:42 FE operator tells IT alarms out	15:45 AEP calls FE re: multiple line overloads 15:46 FE says system could fail 15:48 FE manning substations 15:56 PJM calls FE re: Star-South Canton 15:57 FE calls MISO re: line outages

22 January 2008
KU EECS 983 – Resilient & Survivable Nets – Introduction
RSN-IM-22

Past Disasters: NE Power Failure

Timeline Stage 2: NE Cascade Collapse

- Phase 5:
 - 345kV cascade in northern OH and south-central MI
 - race between surges and detection relay trips
- Phase 6: 16:10 – 16:13
 - MI and OH grid collapses; separates from PA
- Phase 7: 16:10 – 16:12
 - northeast grid separates into islands

Past Disasters: NE Power Failure

Timeline: End of Cascade

- Cascade end:
 - voltage swings dampen with time and distance
 - more robust parts of grid helped isolate
 - higher voltage lines more densely connected
 - line trips isolated least stable parts of grid

Past Disasters: NE Power Failure

Official US + Canada Causes

- Official causes [<https://reports.energy.gov/BlackoutFinal-Web.pdf>]
 - inadequate system understanding
 - inadequate situational awareness
 - inadequate tree trimming
 - three 345kV 3phase lines downed 14 Aug 2003 15:05–15:32
 - inadequate RC (reliability coordinator) diagnostic support
- Blaster & other worms did not have “significant” role
 - CERT, RCMP, NCS joint study

Past Disasters: NE Power Failure

Official US + Canada Recommendations

- Official recommendations
 - implementation of mandatory reliability standards
 - strengthening North American Electric Reliability Council
 - develop independent NERC regulator funding mechanism
 - address specific deficiencies (FirstEnergy & reliability orgs)
 - strengthen NERC technical recommendations
 - improving training and certification requirements
 - *increasing the physical and cyber security of the network*

Past Disasters: NE Power Failure

Lessons and Risks

- Lessons: power grid very brittle
 - SCADA systems inadequate
 - control and monitoring
 - operators poorly prepared and trained
 - overall architecture of grid?
- Risks
 - SCADA system insecure
 - security by obscurity doesn't deter serious attackers
 - share fate with Internet
 - back-end interconnection provides back door
 - Slammer took down Davis-Besse nuke monitoring in Jan 2003
 - common links subject to congestion and DDOS

Internet

Lessons and Risks₁

- Internet relatively resilient *as a whole* but...
 - significant risks exist
 - infrastructure insecure
- Internet best effort infrastructure subject to
 - congestion and flash crowds
 - DDoS attacks

Internet

Lessons and Risks₂

- Internet infrastructure protocols not secure
 - BGP and DNS fragile and insecure
 - S-BGP and DNSsec deployment unlikely
 - disruptions not uncommon, e.g.:
 - 2005: Level3 cancels Cogent peering agreement
 - 2005: Comcast DNS meltdown
 - large scale disruptions possible

Internet

Lessons and Risks₃

- Wireless access links significant vulnerability
 - insecurity of 802.11 WEP
 - DOS jamming potential of 802.11 and 802.16
- System insecurity provide vector, allow rapid spread
 - insecure Windows boxes with clueless users
 - vulnerable routers (Cisco IOS vulnerabilities)
 - vulnerable Web servers
 - no diversity to limit platform-specific threats, insider attacks
 - Intel x86
 - Microsoft Windows, IE, Outlook, Servers
 - Cisco IOS

9/11 Lessons

- Significant disaster but in very localised area
- Non-interoperable first-responder communications
- Mobile telephony
 - not sufficiently over-provisioned for emergency load
 - not sufficiently over-provisioned to absorb wireline traffic
 - unreasonable reliance for first-responder backup
- Internet effects very limited due to localisation
 - flash crowd effects on news servers

Resilient and Survivable Networking IM.3 Communication Environment

- IM.1 Motivation
- IM.2 Past failures (introduction)
- IM.3 Communication environment**
- IM.4 Disciplines

Communication Environment

Impact of Wireless Channel₁

- Open channel subject to *attack*
 - eavesdropping
 - network and traffic analysis
 - interference
 - jamming and denial of service
 - injection of bogus signalling and control messages
- Weak, intermittent, and episodic connectivity

Communication Environment

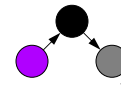
Impact of Wireless Channel₂

- Open channel subject to attack
- Weak, intermittent, and episodic connectivity
 - limited bandwidth of shared medium
 - time-varying available bandwidth
 - noise, weather (latter for free-space laser as well as RF)
 - episodic connectivity
 - channel fades between bit errors & failed links in consequence
 - difficult to achieve routing convergence

Communication Environment

Impact of Mobility₁

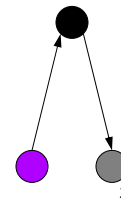
- Dynamic nodes and topologies
 - changing links, clustering, and federation topology
 - difficult to achieve routing convergence
- Control loop delay
 - mobility may exceed ability of control loops to react
- QoS



Communication Environment

Impact of Mobility₂

- Dynamic nodes and topologies
 - changing links, clustering, and federation topology
 - difficult to achieve routing convergence
- Control loop delay
 - mobility may exceed ability of control loops to react
- Impacts QoS
 - changes in inter-node distance
 - requires power adaptation
 - changes density and impacts degree of connectivity
 - latency issues (routing optimisations temporary)

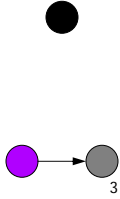


KU ITTC © James P.G. Sterbenz

Communication Environment

Impact of Mobility₃

- Dynamic nodes and topologies
 - changing links, clustering, and federation topology
 - difficult to achieve routing convergence
- Control loop delay
 - mobility may exceed ability of control loops to react
- Impacts QoS
 - changes in inter-node distance
 - requires power adaptation
 - changes density and impacts degree of connectivity
 - latency issues (routing optimisations temporary)



22 January 2008 KU EECS 983 – Resilient & Survivable Nets – Introduction RSN-IM-37

KU ITTC © James P.G. Sterbenz

Communication Environment

Impact of Unpredictably High Latency₁

- Long inter-application delay appears to be disruption
 - long path (c)
 - store-and-forward queueing due to episodic connectivity
 - latency masking techniques mitigate: caching, prefetching
 - but *don't always* help

22 January 2008 KU EECS 983 – Resilient & Survivable Nets – Introduction RSN-IM-38

Communication Environment

Impact of Unpredictably High Latency₂

- Long inter-application delay appears to be disruption
- Severely impacts transport and network protocols
 - signalling latencies dominate at high data rates
 - very long control loops
 - long delays may cause data transfer to stall (window-based)
 - wrapped sequence number spaces
 - high-bandwidth- \times -delay products
 - real-time reaction to many bits in flight difficult or impossible
 - massive buffering required for error control

Resilience and Survivability

Assumptions and Challenges₁

- Problem cannot be solved at physical and link layers
 - assume that best physical, MAC, link techniques in use
 - diminishing returns on further research
- Strong connectivity will not always be achievable
 - economics and policy preclude connectivity everywhere
 - faraday cages for security
 - caves
 - nomadic hunters in northern Sweden; search and rescue in UK
- Network / security infrastructure may be unavailable
 - node failure or overrun (capture)
 - radio silence or jammed channel (enemy, cracker, DDOS)
 - compromised node software

Resilience and Survivability

Assumptions and Challenges₂

- Very long delay inevitable in some scenarios
 - path (speed of light) latency
 - satellite links
 - interplanetary (and intergalactic?) Internet
 - object transmission delay
 - large objects over modest data rates
 - weakly connected and congested links
 - store-and-forward over episodically connected paths
- Security and survivability are not binary choices
 - level of security must be traded against resource cost ...
 - limited node power
 - limited channel bandwidth
 - ... based on application requirements and user desires

Resilient and Survivable Networking

IM.4 Disciplines

- IM.1 Motivation
- IM.2 Past failures (introduction)
- IM.3 Communication environment
- IM.4 Disciplines

Fault Tolerance

Faults, Errors, Failures

- *Fault tolerance*
 - avoid service *failures* in the presence of *faults*
- Mature discipline
 - generally assumes *independent random* faults
 - traditional fault models do *not* hold under
 - malicious attack and large-scale natural disaster
- Canonical example:
 - 1988 Hinsdale Illinois Bell central office fire
 - 100K customers lose service for *weeks*
 - major disruptions in long distance, 800, 911, cellular, ATC
- FT is necessary but not sufficient for resilience

Fault Tolerance

Byzantine Behaviour

- Conflicting information to different parts of system
 - may be malicious
- *Byzantine fault tolerance*
 - avoid *failures* in the presence of *Byzantine faults*
- Preventing Byzantine failures
 - less than 1/3 Byzantine components if not authentication

[Lamport-Shostak-Pease-1982]

Reliability and Availability

Reliability Definition

- *Reliability*
 - probability of a of system performing its purpose adequately
 - for the period of time intended
 - under the operating conditions intended

Reliability and Availability

Availability Definition

- *Availability*
 - probability of a of system operational at a given time
 - initially follows reliability curve
 - but then repairs keep availability higher
 - steady state: uptime / observation time

Dependability Definition

- *Dependability*
 - reliance can be placed on delivered service
- Dependability aspects
 - availability: readiness for usage
 - reliability: continuity of service
 - safety: non-occurrence of catastrophic consequences
 - confidentiality: non-occurrence of unauthorised disclosure
 - integrity: non-occurrence of improper information alterations
 - maintainability: aptitude to undergo repairs and evolution

Survivability Definitions

- *Survivability*
 - capability of a system to fulfill mission in a timely manner
 - in presence of large-scale natural disasters, attacks, failures

Security Definitions

- *Security*
 - confidentiality
 - integrity (message hasn't been altered)
 - nonrepudiation (sender can't deny sending)
 - authentication: source of a message
 - AAA: authentication, authorisation, accounting

Robustness Definitions

- *Robustness*
 - control system operates in the face of uncertainty
 - remains stable under varying inputs

Delay- and Disruption- Tolerance Definitions

- *Delay tolerance*
 - network provides service to user even under long delay
- *Disruption tolerance*
 - network provides service to user even when disrupted
 - stable end-to-end path doesn't exist
- *Challenged networks*
 - networks subject to environmental challenges
 - weak, episodic, and asymmetric connectivity from wireless links
 - mobility-induced dynamic behaviour
 - unpredictably long delay

Challenges Definition

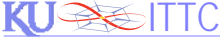
- *Challenges to normal operation*
 - unintentional misconfiguration or operational mistakes
 - malicious attacks
 - large-scale natural disasters
 - environmental challenges
 - mobility
 - weak and episodic channels (typically wireless)
 - unpredictably long delay
 - unusual but legitimate traffic (e.g.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

Resilience Definition

- *Resilience*
 - the capability of network to provide and maintain
 - acceptable level of service
 - in the face of various challenges to normal operation

Resilience Service

- Resilient service to applications
 - ability to access information
 - e.g. Web browsing, sensor monitoring
 - maintenance of end-to-end associations
 - e.g. video- and teleconference
 - operation of distributed processing and networked storage


© James P.G. Sterbenz

Challenges to Normal Operation

Resilience \supset Survivability \supset FT


- **Unusual (legitimate) traffic load**
 - e.g. flash crowds
- **Environmental challenges**
 - high-mobility of nodes and subnets
 - wireless channels
 - weak, episodic, asymmetric connectivity
 - unpredictably long delay paths
 - distance, transmission delay
- **Attacks against**
 - network hardware, software, protocol infrastructure
- **Large-scale natural disasters**
- **Misconfiguration and operational errors**
- **Natural faults of network components**

resilience

survivable & challenged

FT

22 January 2008
KU EECS 983 – Resilient & Survivable Nets – Introduction
RSN-IM-55


© James P.G. Sterbenz

Resilience

Motivation and Threats

- Distinguishing attacks can be *very* hard
 - a sufficiently sophisticated distributed denial of service attack is indistinguishable from legitimate traffic
 - it doesn't matter
 - to other users (cross traffic)
 - network provider (resource exhaustion)

22 January 2008
KU EECS 983 – Resilient & Survivable Nets – Introduction
RSN-IM-56