

RAM CONSIDERATIONS IN COMPLEX SYSTEMS

Jose Emmanuel Ramirez-Marquez, Ph.D.
Stevens Institute of Technology

BACKGROUND ON SYSTEM RELIABILITY ANALYSIS

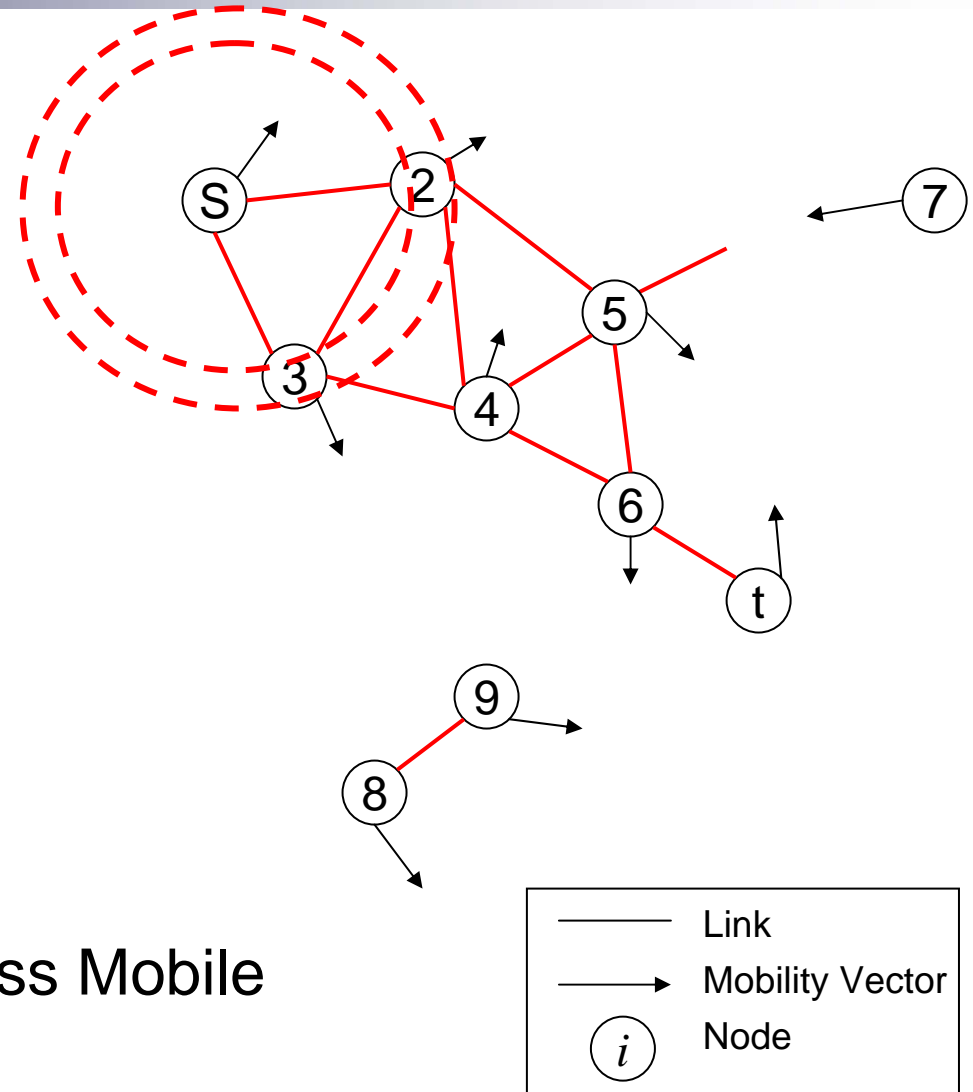
- Reliability:
 - Probability a system (collection of components) works for a specified period of time under specified operating conditions
- Analysis:
 - Understand how system components interact (**build reliability block diagram or network graph**)
 - Obtain component reliability data
 - Use technique to obtain system reliability

TOPIC

- Traditional RMS analyses focused on fixed hardware systems
- Not adequate for 21st century systems
- Survivability & vulnerability not considered
- Lack of customer perspective:
 - Customers want the services to be reliable even if the system isn't
- Current research programs lead to some answers

New Complex Systems

- Mobile Elements
- Free of Infrastructure
- Mobile Network
- Dynamic topology
 - Link creation
 - Link termination
- Examples: UAV, Wireless Mobile Systems, SoS, Internet



COLLABORATORS & SPONSORS

■ Collaborators

- Prof. Michael Tortorella, Rutgers University
- Prof. Patrick Driscoll, USMA
- Prof. Ed Pohl, University of Arkansas

■ Sponsors

- ARDEC
- Department of Homeland Security
- Assured Networks, LLC

OVERVIEW

- Concepts
 - Survivability & Resiliency
 - Robustness
 - Vulnerability
- Resiliency Figures of Merit and Metrics
- Design for Resiliency Principles & Practices
- Role of Robust Design
- Vulnerability Analysis and Reliability Importance
- Conclusions

CONCEPTS

- SURVIVABILITY: “Enough” network elements continue to operate so that system still works
 - Connection-oriented concept
 - Focus is on the infrastructure
 - Lots of diversity and redundancy
 - Cold-war mentality
 - Adds little value in a connectionless system

CONCEPTS

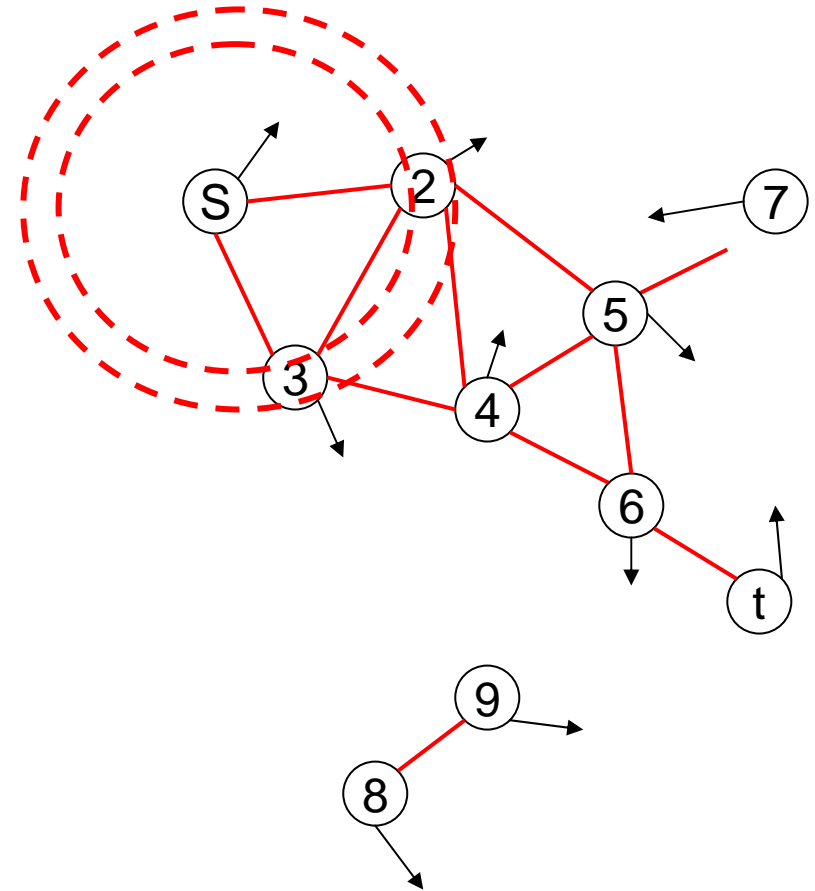
- RESILIENCY: System continues to deliver services at an adequate level despite failures
 - Focus is on the services/applications
 - Generalizes to connectionless system
 - Recognizes a greater variety of threats
 - Requires understanding of the flow
- “Adequate” means there’s a matter of degree to be settled
 - Utility and risk analysis

CONCEPTS

- ROBUSTNESS: An engineering concept referring to stable operation in the face of perturbations
 - Robust Design is a standard discipline in, *e. g.*, hardware engineering
 - Designed experiments
 - Response surface analysis
 - Taguchi methods
 - If properly interpreted, can apply to connectionless systems
 - But....possible confusion due to application to system elements

CONCEPTS

- VULNERABILITY: The degree to which resiliency changes (decreases) when system elements fail
 - Individually or in groups
 - Different kinds of risks
 - Physical risks
 - Attacks
 - Viruses, worms



CONCEPTS-CAUTIONS

- Words are important
- These concepts are all different
- Rubber meets road when specific Figures of Merit (FOM) are chosen
- Vulnerability can be interpreted two ways
 - System level
 - Vulnerability to system element failures
 - System element level
 - Vulnerability to attacks

FIGURES OF MERIT-RESILIENCY

- % service reliability requirements met vs. time
 - Aggregation:
 - All services together
 - Real-time vs. best-effort services
 - Services individually
- Time required for services to return to “normal” level of reliability after a system event
- Geographic extent to which services are disrupted by a system event
- Others?

RESILIENCY METRICS

- Challenging data collection and management issues
 - Many services
 - Many locations
 - Many service reliability requirements
- Statistical sampling
- Control chart
 - Problem diagnosis
 - Communication

DESIGN FOR RESILIENCY PRINCIPLES

- No single element outage significantly affects service reliability
- Service degradation is a continuous function of system degradation
- Outages that do affect service reliability are restored quickly
- Element failures do not propagate failure conditions to other elements elsewhere

DESIGN FOR RESILIENCY PRACTICES

- Provision System to deliver required service reliability under normal conditions
 - Reasonably anticipated behavior
 - Manageable number of infrastructure failures
- Teach network engineers about how failures affect system and services

DESIGN FOR RESILIENCY

ROBUSTNESS

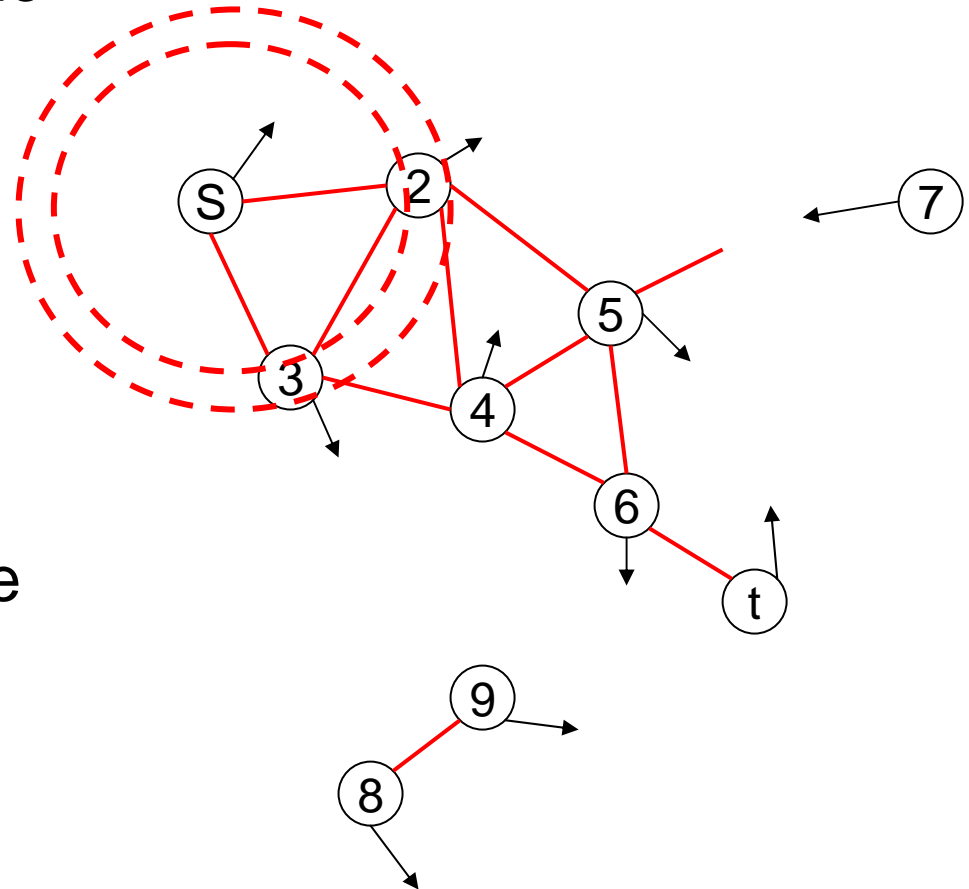
- Internet is an example of a “small world” system
 - Lots of nodes with small degree
 - Few nodes with huge degree
 - Power law distribution of degree (Zipf’s law)
- About 3% of the routers in the Internet are out of service at any time
- Random failures won’t affect Internet much
- Need to protect the big nodes
 - System is resilient, but fragile

ROLE OF ROBUST DESIGN

- Goal is to promote reliable services
 - Instead of Reliable System
- Designed experiments to locate factors having the greatest impact on service reliability
 - Control factors
 - Noise factors
- Difficult to do in real systems
- Simulation may be a reasonable approach

VULNERABILITY ANALYSIS

- Two ways to look at this
 - How vulnerable is the system (really, the services it provides) to specific element disruptions
 - How vulnerable is a particular system element to failure & attack
- Analysis for the first case relies on generalized reliability importance measures



RELIABILITY IMPORTANCE

- Assess the degree to which loss of a component changes the reliability of the system
- Classical RI measures based on derivatives
 - Birnbaum
 - Birnbaum and Saunders
 - etc.
- Translate to new complex systems

RELIABILITY IMPORTANCE

- Generalize these to
 - More descriptive figures of merit
 - Service reliability FOM
 - Information quality FOM
 - Multi-state components
 - Partial loss of capacity

CONCLUSION

- Connectionless systems pose new challenges for resiliency, vulnerability, and systems management
- Current research programs in network flows, IP control schemes, and generalized reliability importance offer new opportunities for successful solution of these problems

Reliability Block Diagram & System Graph

