# Survivable Mobile Wireless Networks

## Issues, Challenges, and Research Directions

James Sterbenz*

*jpgs@acm.org*

**+1 508 944 3067**

Rajesh Krishnan
Regina Rosales Hain
Alden W. Jackson
David Levin
Ram Ramanathan
John Zao





*Work originally performed while at BBN technologies, supported by DARPA contract F30602-99 C-0131

# Survivable Mobile Wireless Networks

## Abstract

In this presentation we summarise the characteristics of mobile wireless links and networks, and then survey the issues and challenges in enhancing their survivability. Conventional fault tolerance methods are necessary but not sufficient for survivability, since failures due to a coordinated attack are not random.

Research focus on three key areas can significantly enhance network survivability:

1. establishing and maintaining survivable topologies that strive to keep the network connected even under attack
2. design for end-to-end communication in challenging environments in which the path from source to destination is not wholly available at any given instant in time; this requires new routing and forwarding mechanisms
3. the use of technology to enhance survivability such as adaptive networks and satellites

We describe some of the issues and potential research directions to address each of these areas.

# Outline

- Introduction to survivability
- Survivability strategy
  1. maintain survivable connectivity when possible
  2. survivable communication even when not connected
  3. technologies to enhance survivability
- Summary

# Introduction to Survivability

- Introduction to survivability
  - definition
  - mobile wireless environment
  - changing environment challenges
  - assumptions and principles
  - requirements and problem
- Survivability strategy
- Summary

# Survivability
## Definition

*Survivability is the capability of a system to fulfill its mission in a timely manner, even in the presence of attacks or failures* [SEI]

# Communication Environment
## Wireless Channel Characteristics

- Open channel subject to *attack*
  - subject to eavesdropping: privacy issues
  - subject to interference: jamming and denial of service
- QOS different from wired communications
  - channel fades
    - between bit errors and failed links in consequence
  - interference and jamming
    - weakly and intermittently connected links
    - difficult to achieve routing convergence
  - bandwidth scarcity issues in shared medium

    note: wireless doesn't only mean RF, eventually light

# Communication Environment
## Impact of Mobility

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

# Survivability Challenges
## Changing Assumptions$_1$

- Disappearing distinction between wireless and wired
  - users don't want to worry about the difference
  - some devices will have multiple interfaces
  - ultimate vision: wireless access to optical backbones
- Increasing number of end systems per user
  - at least tens of devices per user
  - perhaps thousands of devices per user
- Disappearing distinction between host and switch
  - ad hoc networks: end systems relay other traffic
  - active nets: switches execute code

# Survivability Challenges
## Changing Assumptions$_2$

- Nodes may not correspond to users or have owners
  - sensor arrays
  - ubiquitous public devices (displays in rooms, keyboards)
- Addressing limits and problems will not get fixed
  - plan for tera- or petanode networks
  - even if IPv6 is deployed, it doesn't solve the problems
  - NATs, middleboxes
- Nodes may not have addresses
  - rather some only have names (unique persistent identifier)
  - some are anonymous (no name or address)
  - characteristics matter (e.g. color printer)

# Survivability
## Assumptions and Principles

- Security and survivability are not binary
  - level of security must be traded against resource cost ...
    - limited node power
    - limited channel bandwidth

    ... based on application requirements
- Network / security infrastructure may be unavailable
  - node failure or overrun (capture)
  - radio silence
  - jammed channel
  - compromised node software

# Survivability
## Requirements

- Survivability requirements [SEI]
  - resistant to attack
  - recognition when attack has occurred
  - recovery from attack after occurrence
  - refinement in future response to attack
    - [desirable rather than hard requirement]
- Survivability concerns
  - survivable information access by the user or application
  - end-to-end communication association survivability

# Survivability
## Beyond Fault Tolerance and Cryptography

- Fault models do not hold under malicious attack
  - we cannot assume independence and random failures
  - therefore, fault tolerance is necessary, but *not* sufficient
- Cryptography does not ensure survivability
  - threat of traffic flow analysis leading to attack
  - control plane and physical infrastructure attacks

# Survivability
## Mobile Wireless Survivability

- Traditional communication models
  - adapt to mobile wireless as faults that must be recovered
- What breaks
  - when mobility exceeds reactivity of traditional control loops
  - when channel conditions don't allow end-to-end path
  - routing protocols rarely or never converge
- New way of thinking needed
  - *expect* challenging channel environments
  - *expect and exploit* mobility
- Don't give up! New mechanisms for survivability

# Survivability Strategy

- Introduction to survivability
- Survivability strategy
  1. maintain survivable connectivity when possible
  2. survivable communication even when not connected
  3. technologies to enhance survivability
- Summary

# Survivability Strategy
## Survivable Connectivity

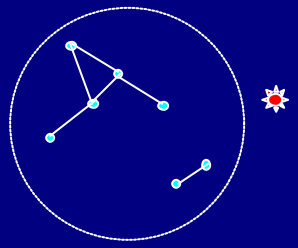
- Introduction to survivability
- Survivability strategy
  1. maintain survivable connectivity when possible
     - establishing the network
     - low probability of detection
     - survivable topological connectivity
  2. survivable communication even when not connected
  3. technologies to enhance survivability
- Summary

# Survivable Connectivity
## Establishment and LPD

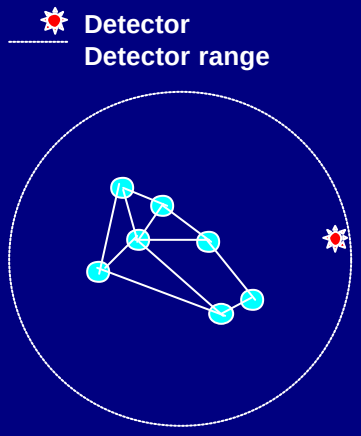
- Establish network structure and connectivity
  - secure auto-configuration and self-organisation
  - use infrastructure when available ...
    ... but don't depend on it
- Low probability of detection (LPD)
  - stealthy network is more resistant to attack ...
    ... but stealth makes legitimate communication difficult
    - low transmission power
    - encryption and authentication of network control

# Survivable Connectivity
## Topological Connectivity

- Survivable connectivity
  - requires sufficient transmission power
  - in tension with
    - LPD
    - degree of connectivity (density overhead)
  - determine connectivity to be survivable
  - adjust topology to evade problems
    - route around
    - movement control for mobile nodes



**low transmission power**




**high transmission power**

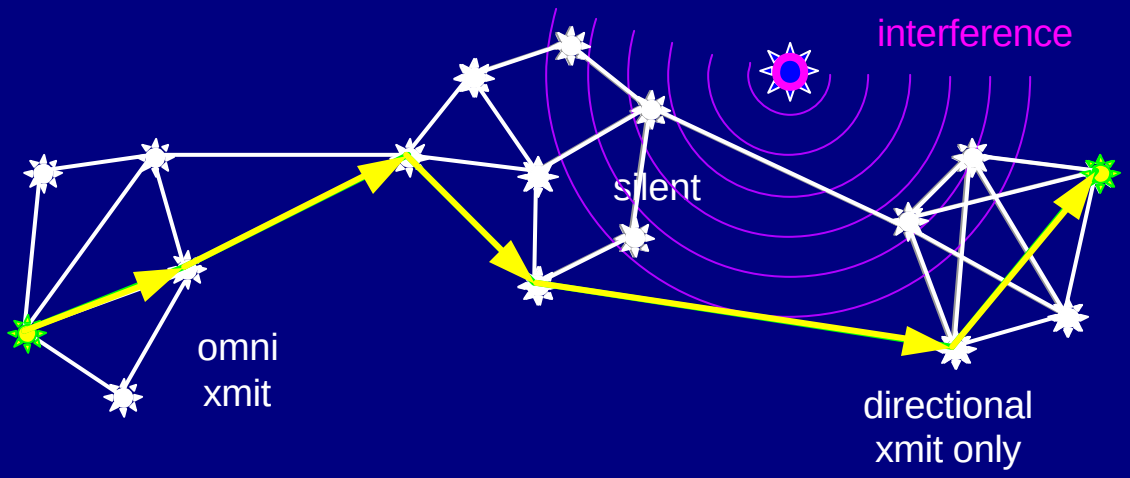
# Survivability Strategy
## Survivable Communication

- Introduction to survivability
- Survivability strategy
  1. maintain survivable connectivity when possible
  2. survivable communication even when not well connected
  3. technologies to enhance survivability
- Summary

# Non-Survivable Communication
## Routing Convergence and Mobility

- Current routing algorithms assume *eventual stability*
  - converge to stable communication paths
  - complete end-to-end path must exist at some point in time
  - link outage treated as *fault* that must be repaired
- Moderate mobility is *tolerated* as a topology change

# Non-Survivable Communication
## Eventual Stability: Wait for Complete Path

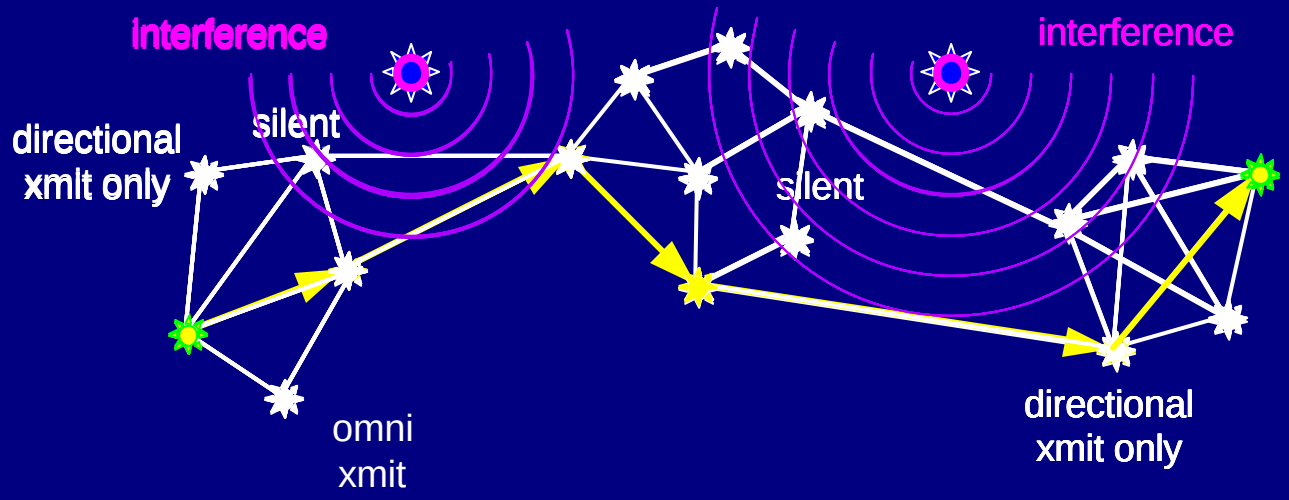



- Waiting while interference or eavesdropped...
- Finally, routing algorithms recompute and converge
  - all nodes along a path can simultaneously communicate
  - and path remains stable long enough for transfer

# Survivable Communication
## Routing Convergence

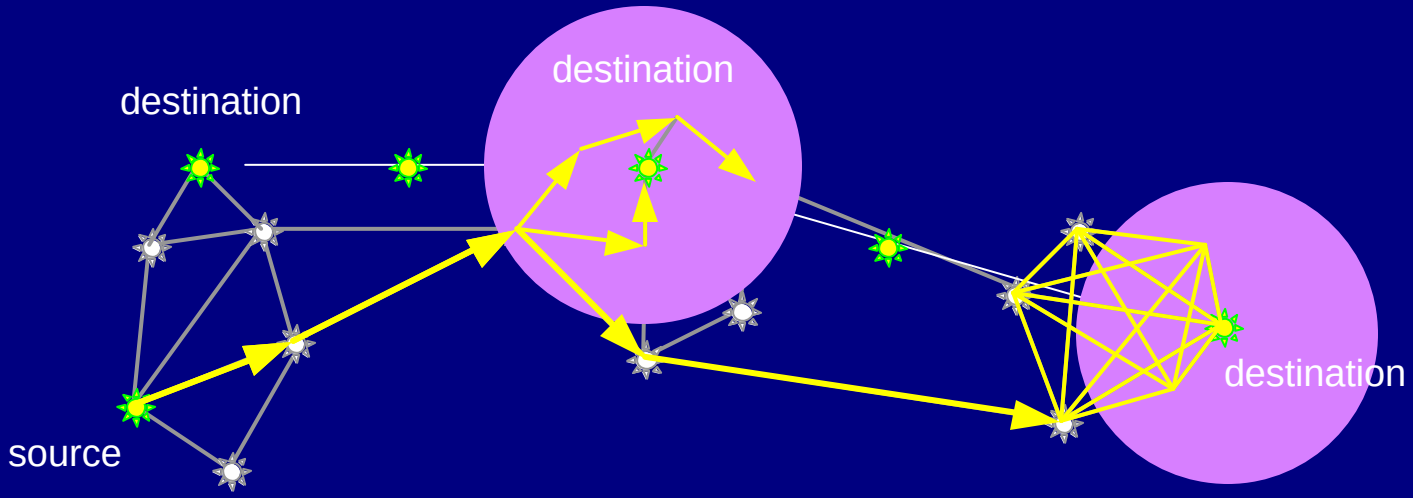
- Assume weak and episodic connectivity
  - routine occurrence for which network is designed
- Survivable communication: *eventual connectivity*
  - communicate as far as possible, whenever possible
  - hold data when necessary (store-and-forward)
    - deflection when necessary (buffer limitations)
  - schedule transmission for optimum LPI and energy
  - optimise for eventual stability when possible
    - store-and forward avoidance
    - cut-through

# Survivable Communication
## Eventual Connectivity




- Multiple interferences or suspected eavesdroppers
  - prevent an end-to-end path from *ever* existing
  - store data as necessary before forwarding

# Survivable Communication
## Expect Mobility

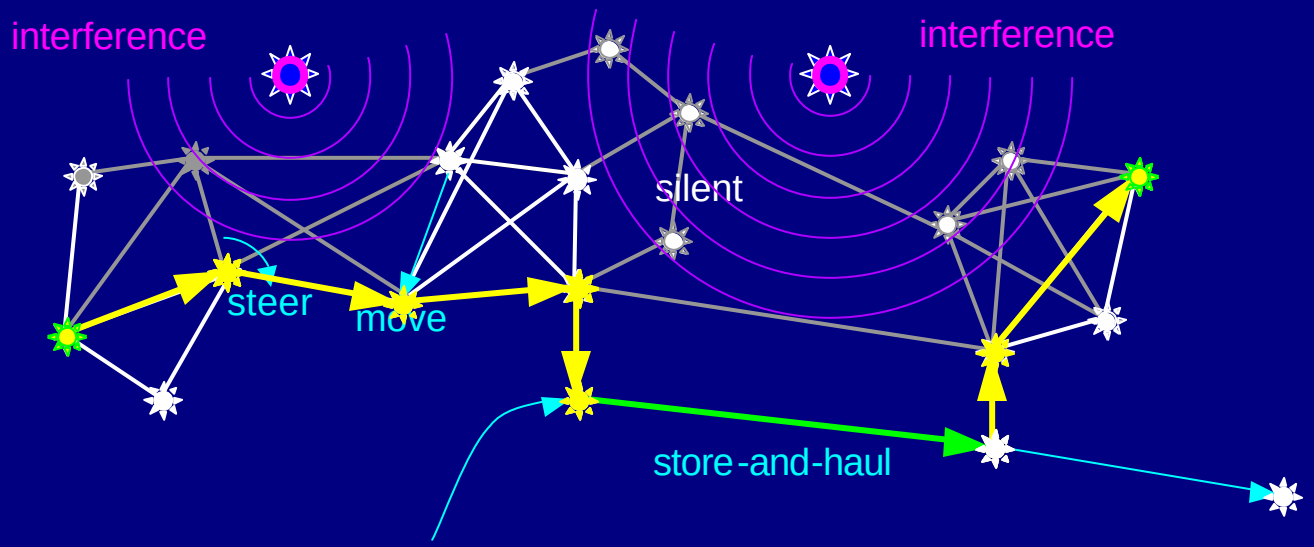



- Routing and forwarding expect mobility
  - use location and trajectory information when available
  - spray routing: probabilistic multicast
    - exploit cluster hierarchy when possible

# Survivable Communication
## Exploit Mobility

- Position node/antenna for survivability
  - use trajectory information when available
  - exert control on movement of other nodes
- Node can carry data as they move
  - *store-and-haul* data without radiating transmissions
  - transit areas of *no* connectivity

# Survivable Communication
## Exploit Mobility




- Move nodes and steer antenna around interference
- Mobile nodes haul data without radiating
  - interference and adversary node avoidance
  - transit disconnectivity

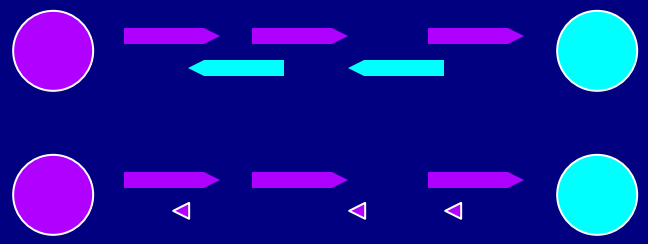
# Survivable Communication
## Adjust Data Transfer to Environment

- Cut-through
  - lowest latency for node that are capable
  - exploit “traditional” physical layer techniques
- Store-and-forward
  - immediate when link available to next node & empty queues
  - move burst to other nodes for load balancing
- Scheduled transfer
  - wait until link available to next node
  - new physical layer opportunities for burst transfer
- Store-and-haul data

*Design for eventual connectivity, optimize for eventual stability*

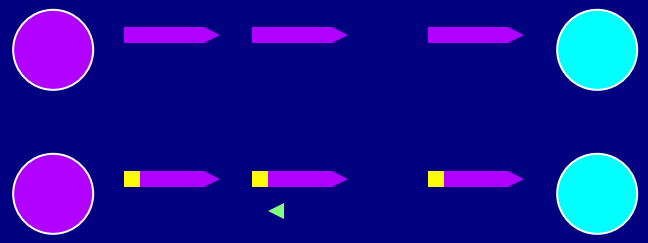
# Survivable Communication
## Asymmetric Channels

- Asymmetric channels result from
  - weak connectivity
  - asymmetric transmission power
  - radio silence
- Bidirectional channel *required* for
  - bidirectional communication
    - application issue
  - closed-loop feedback control
    - ACKs for reliable data transfer



# Survivable Communication
## Asymmetric Channels

- Current transport protocols assume reliable medium
  - TCP has combined feedback error+flow+congestion control
- Survivability with asymmetric channels needs
  - open-loop flow and congestion control (rate control)
  - increased reliance on open-loop error control (e.g. FEC)
    - unreliable transfer
      optional FEC to strengthen
    - reliable transfer
      FEC for probabilistic reliability
      infrequent adaptive selective ACKs
  - note: SCTP does *not* do most of this!



# Survivability Strategy
## Survivability Technologies

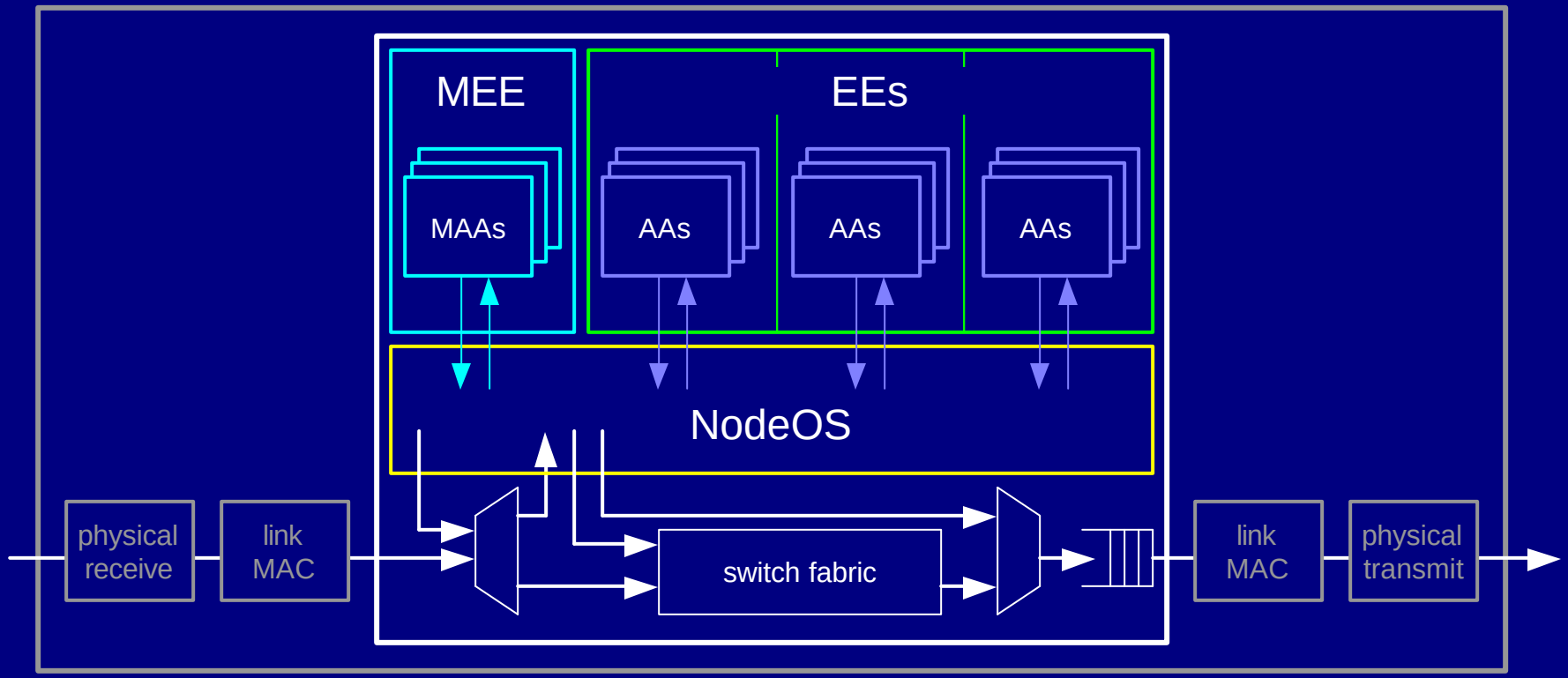
- Introduction to survivability
- Survivability strategy
  1. maintain survivable connectivity when possible
  2. survivable communication even when not connected
  3. technologies to enhance survivability
     - adaptive and agile networking
     - directional antennæ
     - role of satellite and airborne nodes
- Summary

# Survivability Technologies
## Adaptive and Agile Networking

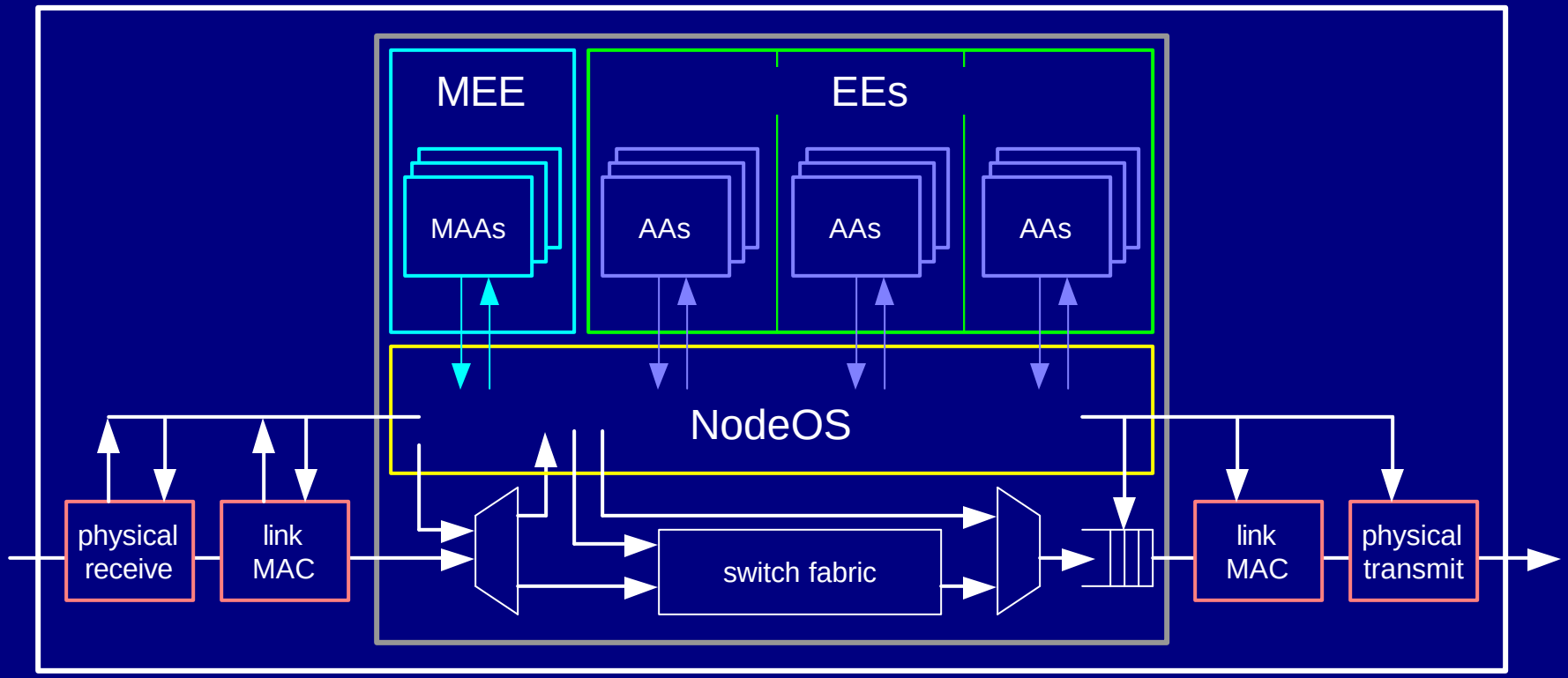
- Adaptive networking at all layers
  - physical layer transmission and coding
  - MAC protocols and parameters
  - network routing, signalling, and addressing
    - geographical, topological, and characteristics-based
  - end-to-end protocols
- Enabled in systematic manner by
  - software radios
  - active networking technology
    - protocols and algorithms dynamically provisioned
    - don’t need to standardise a network and MAC protocol

# Survivability Technologies

## Active Node Architecture



# Survivability Technologies
## Mobile Wireless Active Node Architecture



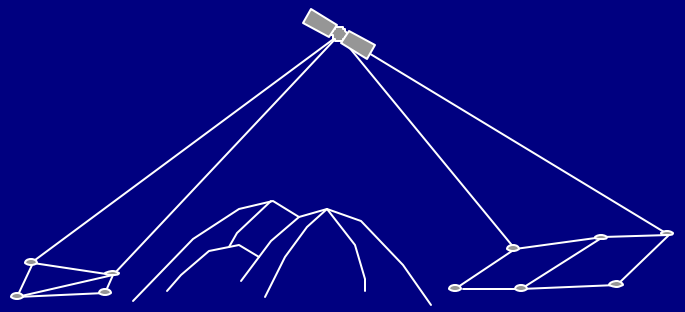
# Survivability Technologies
## Directional Antennæ

Exploitation desirable multihop characteristics

- Increase spatial reuse
  - antenna steering combined with power control
  - allow high power long links overlays
- Enhance ability to hop around:
  - failed or overrun nodes
  - failed links
  - jammed / eavesdropped links
- Help to utilise satellite infrastructure
  - high power focused uplinks with low terrestrial radiation

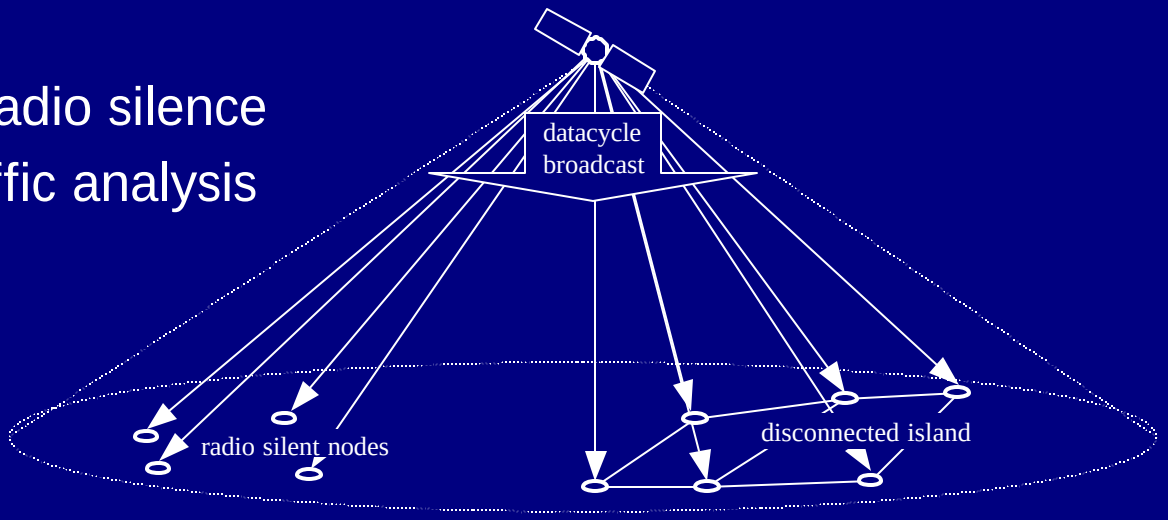
# Survivability Technologies
## Satellites and Airborne Nodes

- High altitude vehicles (satellites and airborne nodes)
  - less subject to line-of-sight obstructions
  - less susceptible to attack
- Large transmission footprint
  - inherent broadcast capability
  - mitigates node mobility
  - connect disconnected islands
- Disadvantages
  - expensive and infrequent deployment
  - high transmission power required for uplink



# Satellites and Airborne Nodes
## Information Dissemination

- Broadcast information dissemination
  - routing and topology updates
  - name services
  - certificates and CRLs
- Datacycle
  - supports radio silence
  - resists traffic analysis



# Survivable Mobile Wireless Networks
## Summary

- Introduction to survivability
- Survivability strategy
  1. maintain survivable connectivity when possible
  2. survivable communication even when not connected
  3. technologies to enhance survivability
- Summary

# Survivable Mobile Wireless Networks
## Summary

- Beyond fault tolerance and crypto
  - necessary, but not sufficient
- Design for survivability
  - expect challenging communication channel environment
  - expect and exploit mobility
- New communication mechanisms needed to:
  - maintain connectivity when possible
  - operate under eventual connectivity
  - use asymmetric channels
  - adaptive and agile networks
  - exploit satellite and airborne nodes

# Acknowledgements


- DARPA
  - Doug Maughan
  - Rob Ruth*

- BBN
  - Isidro Castiñeyra
  - Craig Partridge
  - Martha Steenstrup*
  - Fabrice Tchakountio
  - Greg Troxel

* former affiliation

# Presentation Venues

- WiSe 2002 at Mobicom 2002
  - Atlanta, GA Oct 2002
- University of Kentucky – Oct 2002
- Northeastern University – Nov 2002
- IEEE ComSoc Boston – Dec 2002

WiSe paper and presentation available at

**`http://jpgs.sterbenz.org/sumowin`**

# End of Foils