



---

# **On Survivability and Security in Wireless Infrastructure Networks and their Interaction**

**Yi Qian, University of Puerto Rico at Mayagüez**

**August 5, 2004**

Presentation based on the paper recently submitted to IEEE Wireless Communications Magazine:  
by Prashant Krishnamurthy, David Tipper, and Yi Qian,  
“On Survivability and Security in Wireless Infrastructure Networks and their Interaction”

# Agenda

- Introduction
  - What is Information Assurance?
  - 4G/Hybrid Wireless Networks
- Security in Wireless Networks
  - Current approaches
  - Issues and problems
  - Research areas and some results
- Survivability in Wireless Networks
  - Network design for wireless wide area networks
  - Traffic restoration protocols for recovery under failure
- Ongoing work and conclusions

# Introduction



- Wireless networks are becoming ubiquitous
  - Hospitals, homes, m-commerce, gaming, transportation, etc.
  - 20% of physicians will use handheld devices for daily medical transactions by 2004 (*Source: W.R. Hambrecht & Co.*)
  - Wireless gaming market estimates (*Source: Datamonitor*)
    - Asian-Pacific market
      - \$10.3 billion in 2006 from \$827 million in 2001
    - The U.S. market
      - \$3 billion in 2006 from \$20 million in 2001
  - Banking services, bill payment, ordering, reserving or paying for goods or infotainment using PDAs or Cellphones
- Information Assurance?

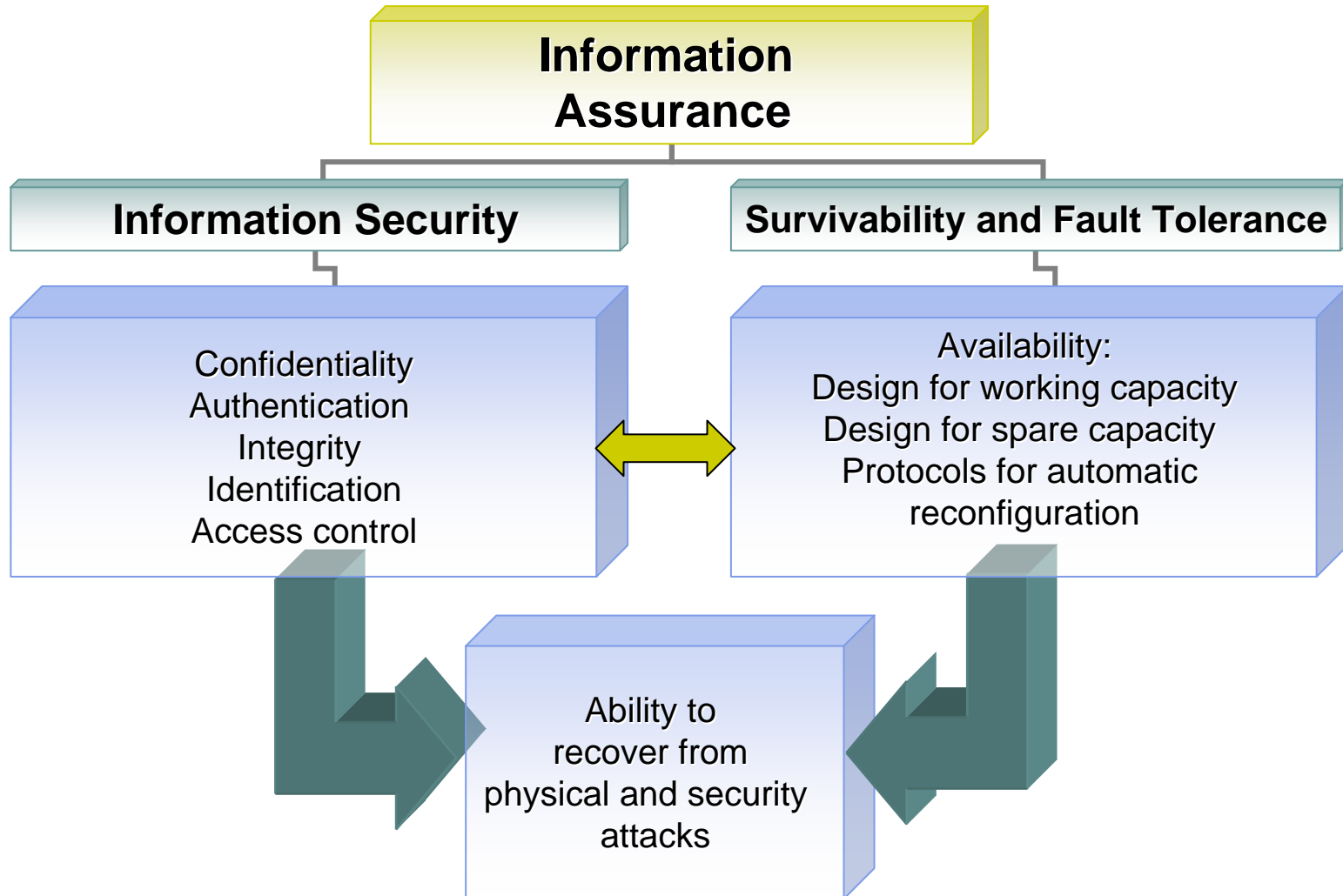


# Information Assurance

- Definition<sup>1</sup>:
  - *“Operations undertaken to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation”*
- Availability
  - Survivability and Fault Tolerance
    - Sufficient Working & Spare Capacity
    - Traffic Restoration Protocols, Alarms and Network Management
- Security
  - Integrity, authentication, confidentiality and non-repudiation

<sup>1</sup>From the Information Assurance Advisory Council (IAAC)

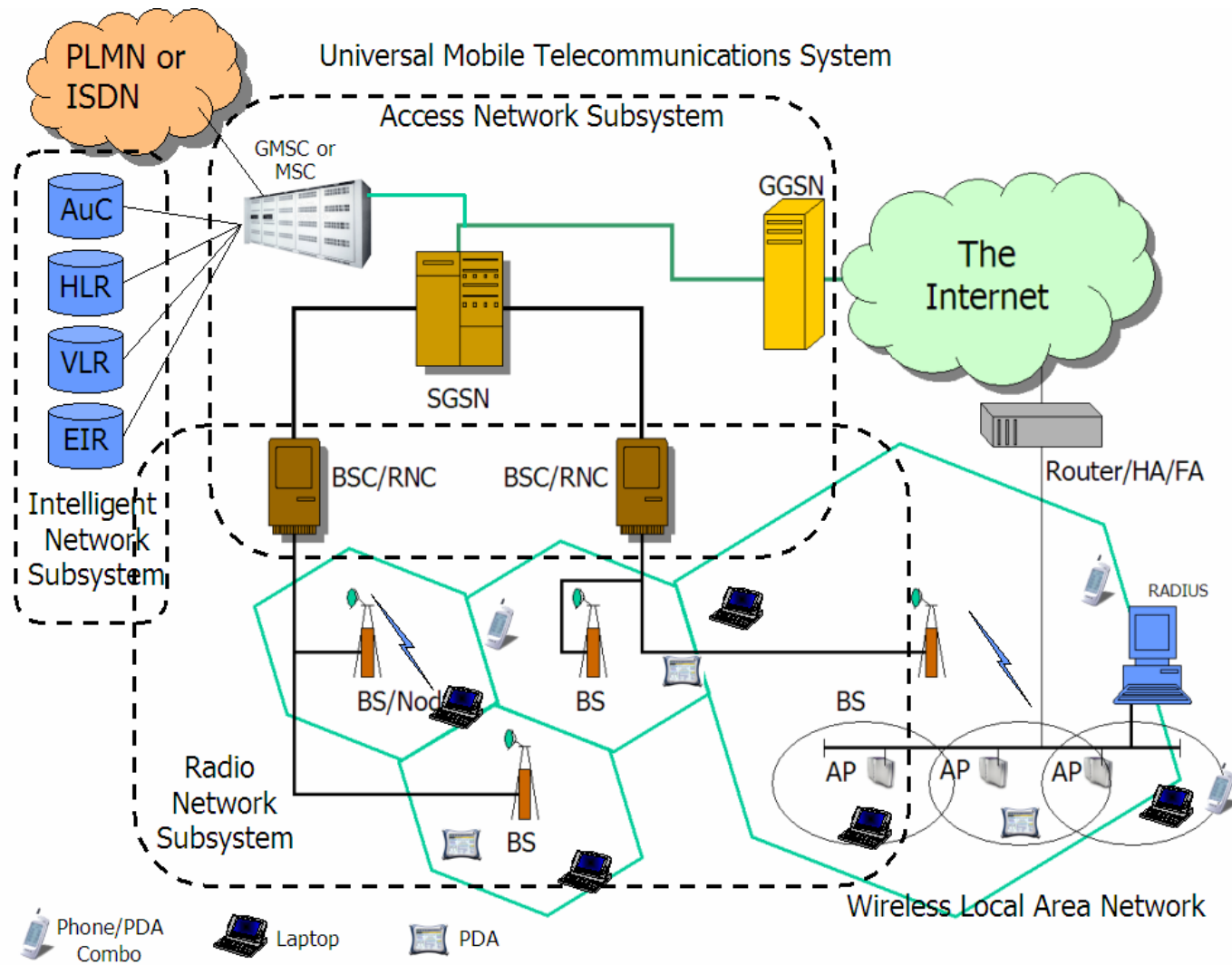
# Information Assurance



# 4G/Hybrid Wireless Networks

- All traffic is packet data
  - e.g. Voice will be carried using VoIP
- There will be a mix of many types of technologies
  - Wide area – 2.5G, 3G or 3G-like systems
  - Local area and hot spots - 802.11/HIPERLAN systems
  - Personal area – Bluetooth & 802.15 systems (sensors etc.)
- There must be *seamless* roaming between such systems
  - Already service providers are using 802.11 (BT, T-Mobile and Sprint) for broadband access
- Information assurance becomes more important
  - Link and node failures, congestion, interference
  - Fraud, exposure of sensitive data, denial of service, etc.

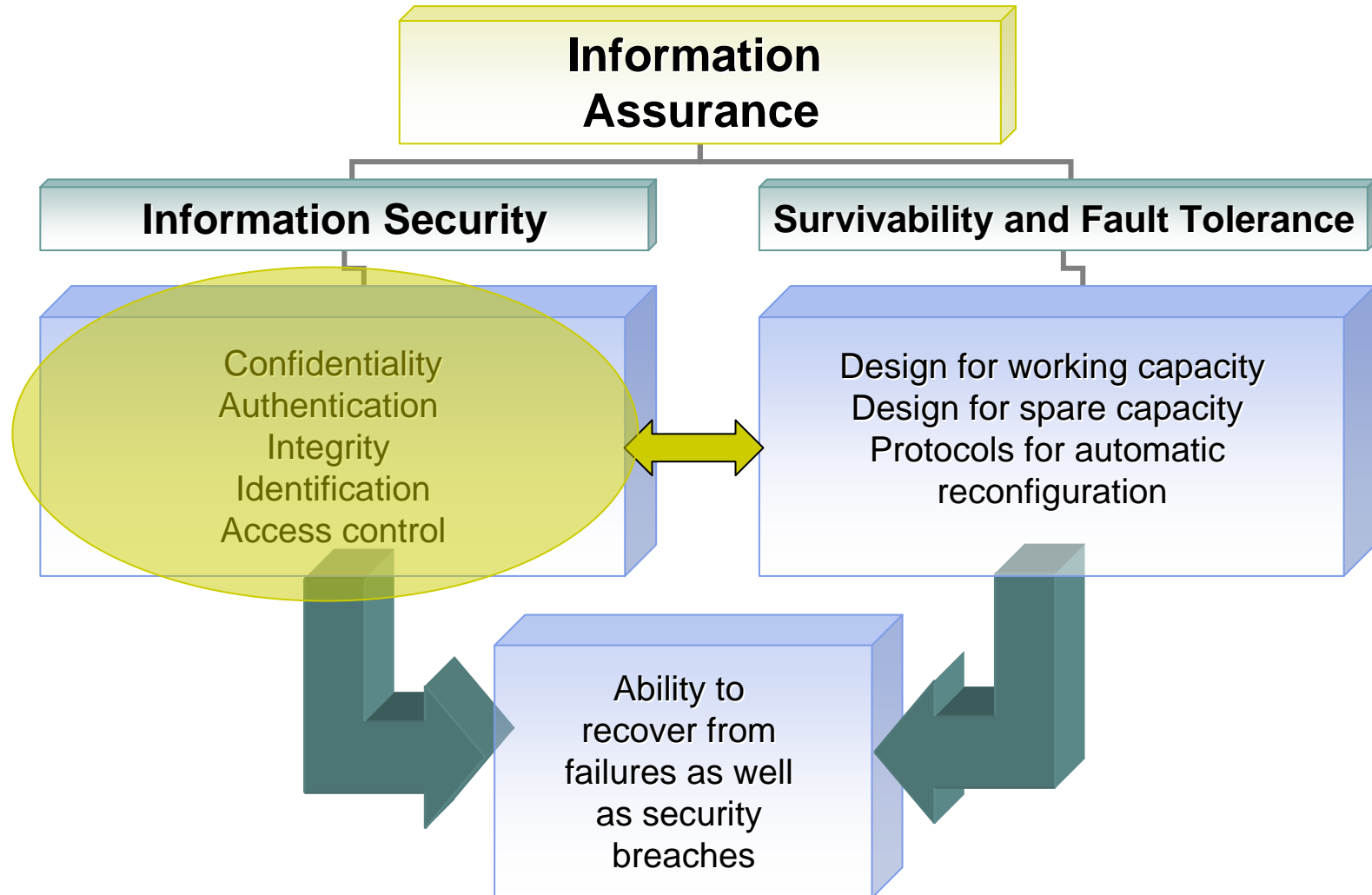
# 4G/Hybrid Wireless Networks



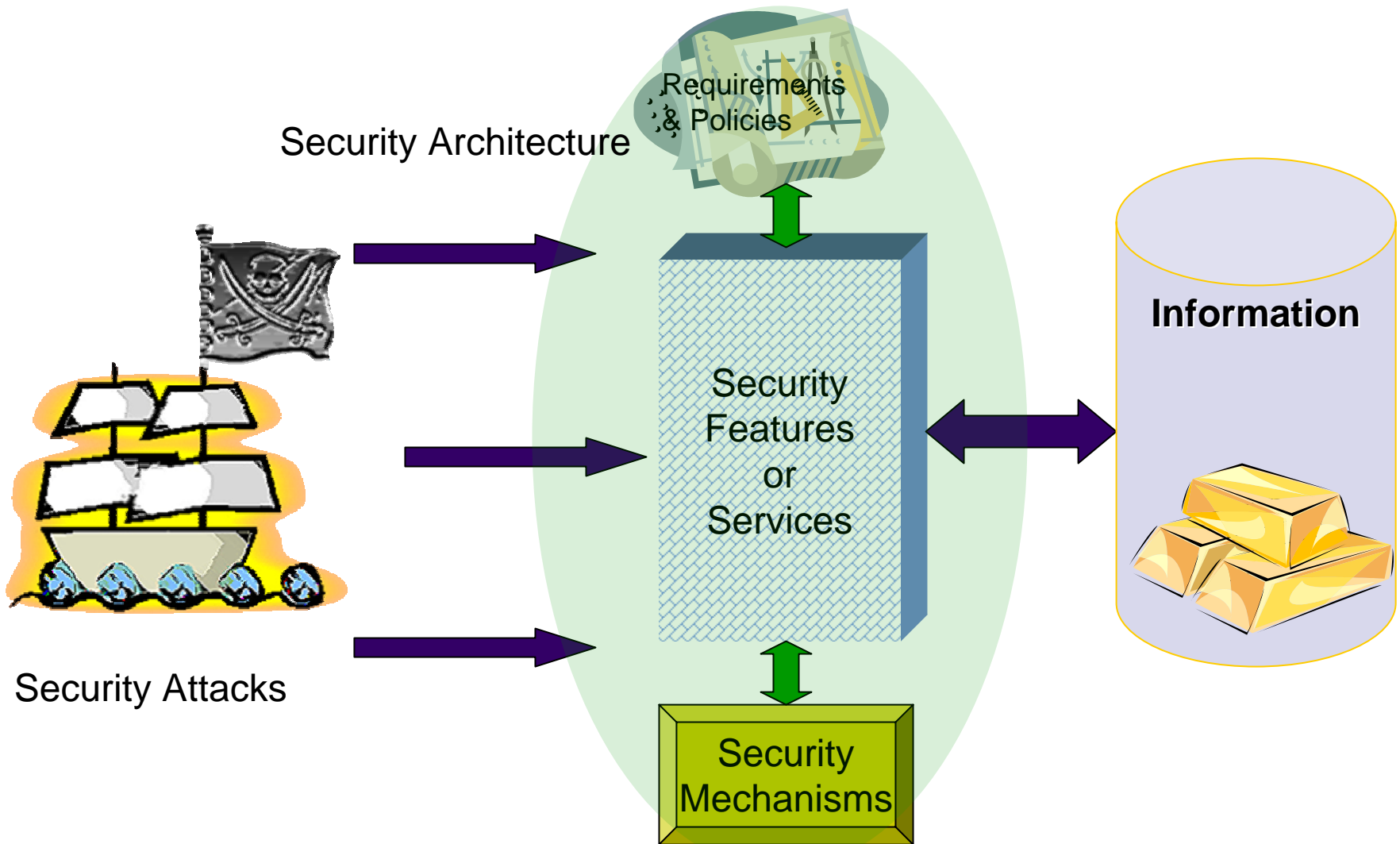
# Wireless security/survivability framework

| Subsystem                           | Components  | Communication Links   | Function  |
|-------------------------------------|---|---|---|
| Radio Network Subsystem (RNS)       | Mobile units, base stations, WLAN access points, BS controllers | Digital radio channels with TDMA, FDMA, or CDMA, or CSMA, wireline links and/or terrestrial microwave | Define physical interface for radio communication<br>BS cluster management,<br>Radio channel management,<br>MAC signaling |
| Access Network Subsystem (ANS)      | BS, BSC, MSC, AP signaling network, SGSN, GGSN                  | Wireline links and/or terrestrial microwave   | Connection management,<br>Mobility management   |
| Intelligent Network Subsystem (INS) | MSC, HLR, VLR, EIR, AUC, mobileIP signaling, RADIUS             | Wireline links and/or terrestrial microwave   | Service management,<br>Mobility management  |

# Information Assurance



# Network Security Basics



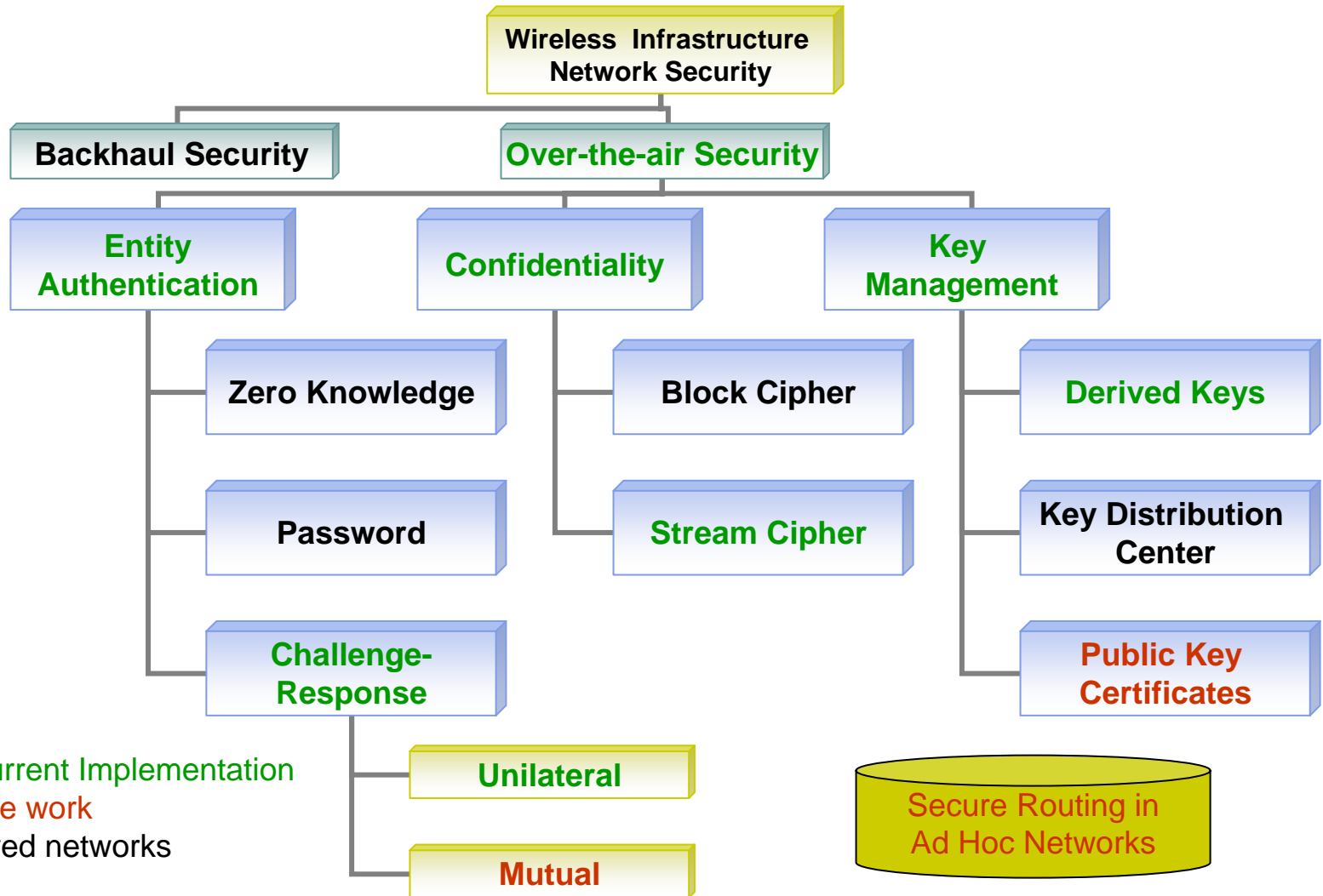
# Terminology

- Security Attack
  - Any action that compromises the security of information
- Security Feature or Service
  - Measures intended to counter security attacks by employing *security mechanisms* based on the security requirements
- Security Mechanism
  - An element, protocol, or technique used to defend, prevent or recover against security attacks
- Security Architecture
  - **All** security features and mechanisms taken together
- Examples of Security Attacks
  - Interception, masquerade, fabrication, modification, traffic analysis
- Examples of Security Features
  - Data confidentiality, user authentication, entity authentication, non-repudiation
- Examples of Security Mechanisms
  - To implement data confidentiality, a stream cipher using a cipher key derived from a master key
    - No single security mechanism can provide all security features
    - Encryption of some sort is necessary for most security features

# General Remarks

- No single security mechanism can provide all security features
- Encryption of some sort is necessary for most security features
- Secrecy of encryption algorithms is not a guarantee of security
- Most secret key encryption schemes can only be broken by brute force
  - They need key sizes that are at least 80 bits
- Public key encryption schemes have mathematical attacks
  - They need larger key sizes (1024 bits)
  - They are computationally more intensive
- Key management is an onerous task
  - Certificates (based on public-key schemes) have reduced this problem significantly in wired networks
- Emerging trends – AES, Elliptic curves, and *N'tru*

# Wireless Network Security



# Security Issues and Problems in 4G/Hybrid Networks

- Data is bursty, not continuous
    - Security features/services need to be different
      - e.g: No message authentication in current networks
        - Encryption is used primarily for confidentiality
        - There is entity authentication when the call is set-up => In current cellular networks, ciphering mode is used on a per-call basis
  - Roaming between networks
    - When there is an inter-tech or vertical handoff, there is need for migrating the “security association”
  - Variety of security levels & capabilities in devices and networks
  - Wireless specific issues
    - Battery life of the MS
    - Computational complexity
    - Bandwidth
    - Effects of the radio channel
- Will affect the encryption algorithms and security protocols and thus the security policies

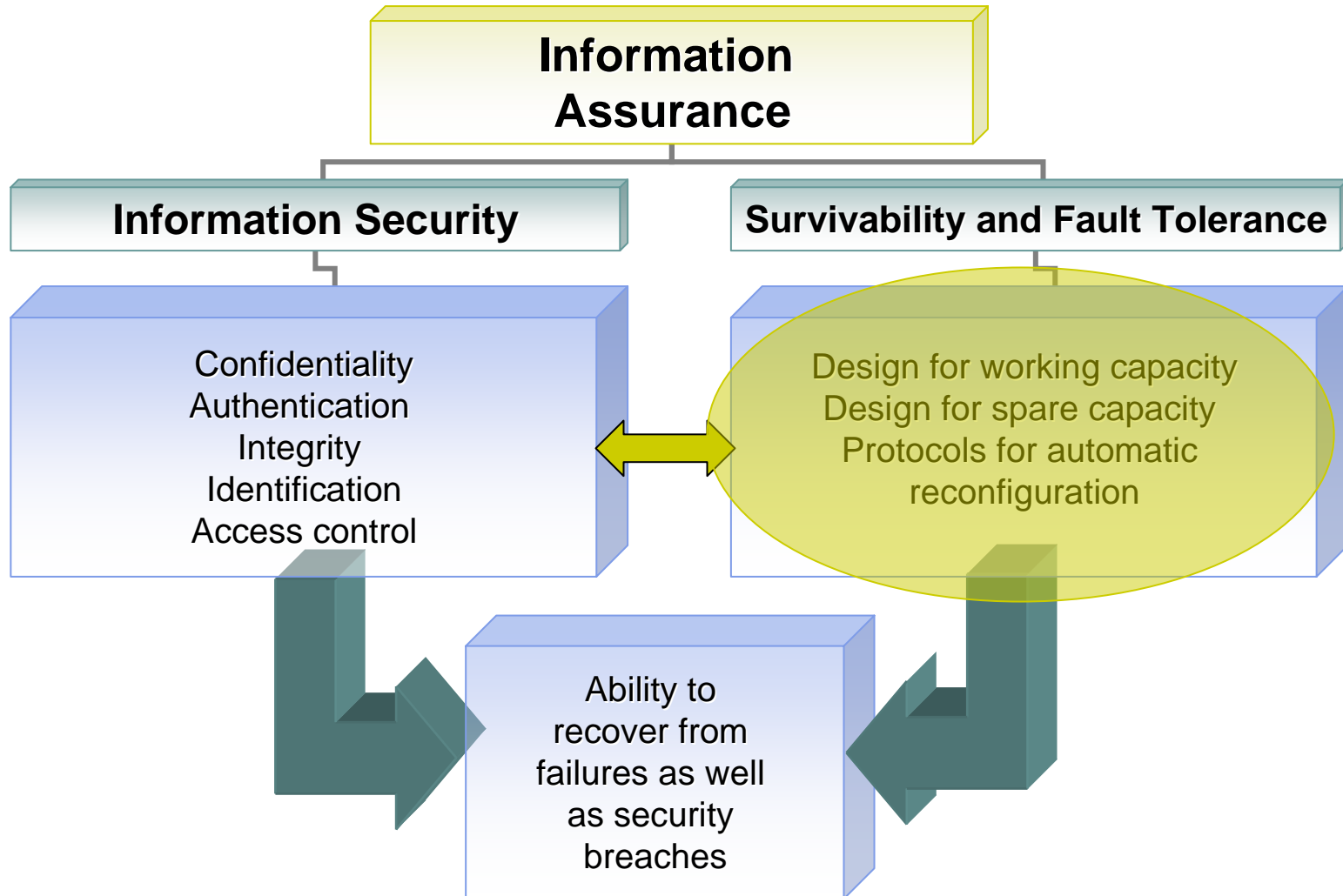
# The Large Questions

- What security features or services must be enforced when a mobile station (MS) roams from one system to another?
  - Entity authentication, key agreement or set-up, message authentication at the point of access (BS or AP), etc.
- At what layers should the services be implemented?
  - MAC level, network level, application level, physical layer, etc.
  - Which is more efficient and why?
- What security architecture must be in place to support such roaming seamlessly?
  - Authentication centers, algorithm-agile base stations, multiple repositories of master keys, separated sets of master keys, certificate infrastructure, etc.
- What security policies need to be in place in this architecture?

# Typical Security Issues

| Sub System | Network Components                          | Secret Information   | Messages  | Information to be secured   |
|------------|---|--|---|---|
| RNS        | MS, BS, WLAN AP                             | Subscriber identity, Shared secret master key, Session key(s), Random nonces | Signaling messages (RRM, MM)<br>Challenge, Response<br>Voice/data traffic | Beacon, BCCH, Pilot need to be checked for integrity; Challenge, response, nonces need to be authenticated; Voice/data traffic needs to be confidential |
| ANS        | BS, BSC, SGSN, MSC, GGSN                    | Shared keys between entities for each session, random nonces                 | Signaling messages<br>Voice/Data traffic                                  | All traffic need authentication and data integrity especially nonces and RRM, MM messages   |
| INS        | SGSN/GGSN, MSC, VLR, AuC, RADIUS server, AP | Certificates, Shared secret master key, Subscriber ID, session keys, nonces  | Challenge, Response, Session key, key distribution & agreement, Nonces    | Session key needs to be confidential; Challenge, response and nonces need to be tested for integrity and authentication                                 |

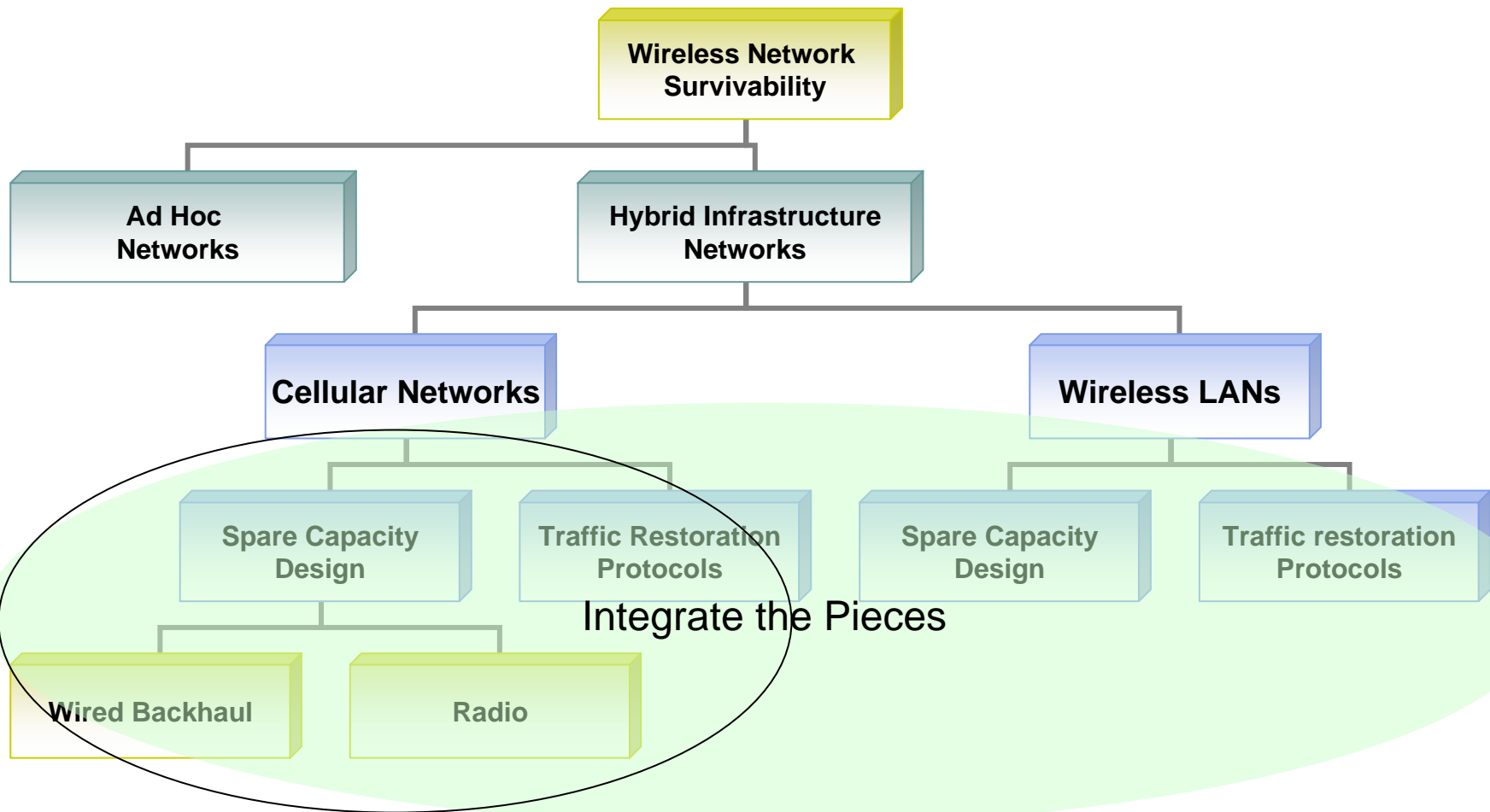
# Information Assurance



# Network Survivability

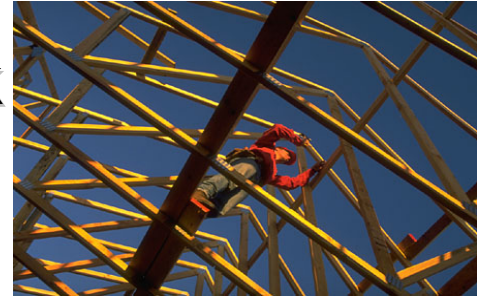
- **Goal**
  - Maintain service for certain failure scenarios at a reasonable cost
- **Analysis**
  - Understand system functionality after failures
- **Design**
  - Adopt network architecture to minimize the impact of failures/attacks on network services
    - Prevention (e.g. backup power supply), security, etc.
    - Topology design and capacity allocation
    - Network management/restoration procedures

# Wireless Network Survivability Approach

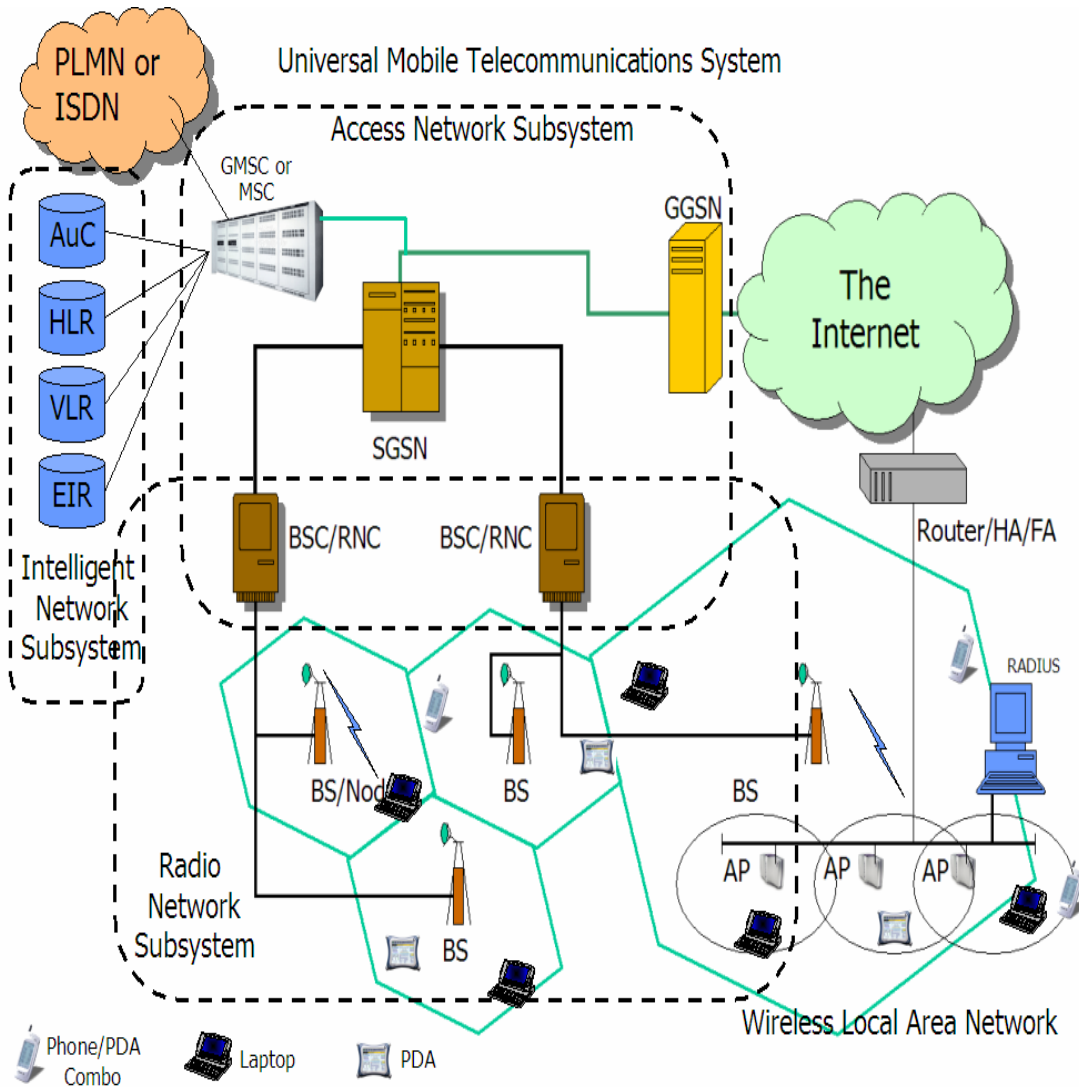


# Survivability Approach

- Develop a survivability framework
  - (IEEE Com. Mag, Jan 2002)
- Conduct a survivability analysis
  - Quantify impact of different failures/attacks
- Develop survivable network design algorithms
  - Wide Area cellular network
    - Backhaul (wired) part of network <= focus here
    - Wireless part of network
  - WLAN Design
- Develop survivable network protocols
  - Split into wireless and wired parts, cellular and WLAN parts
- Integrate pieces



# Wireless Access Network Survivability



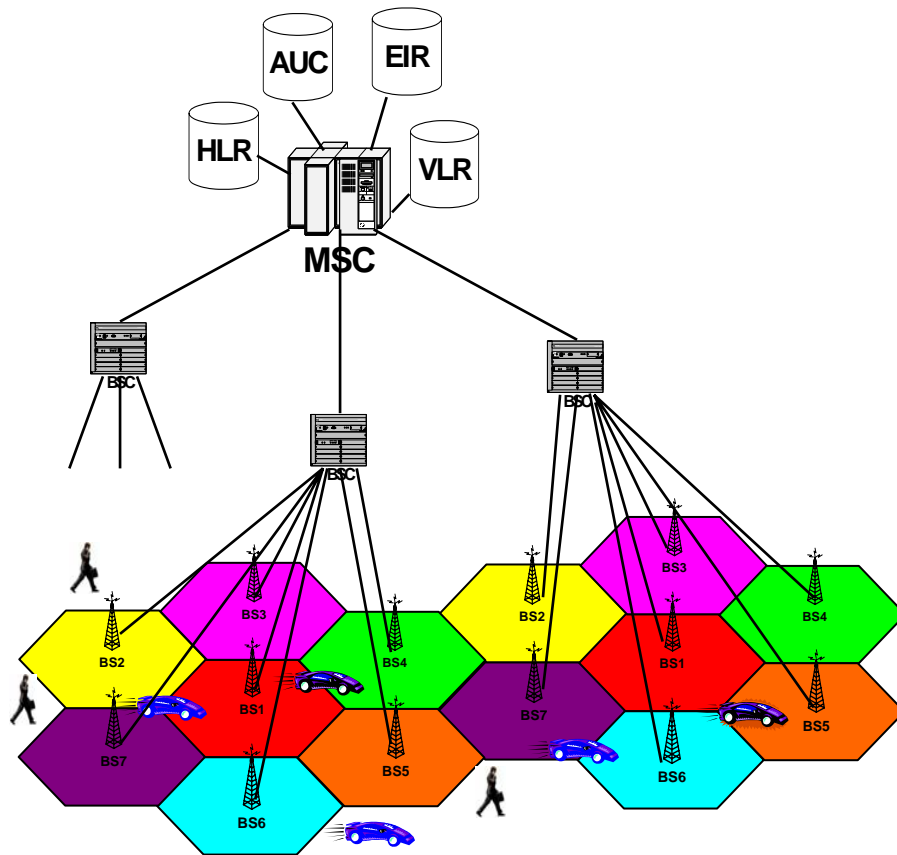
- Wireless network characteristics make survivability issues different than wired networks
  - Tree-like network topology
  - **Wireless Links**
  - **User mobility**
  - Power conservation
  - Security
- Emerging high data-rate and multimedia services place additional requirements on survivability issues

# Wireless Survivability Strategies



| Subsystem                     | Robustness and Redundancy   | Traffic Management and Restoration  |
|-------------------------------|---|---|
| Radio Network Subsystem       | Spare RF components, Overlapping/scaleable cells for multi-homing, Survivable soft capacity and coverage planning | Adaptive radio resource management: admission control, packet scheduling, bandwidth management, channel switching, power control, load sharing/adaptation |
| Access Network Subsystem      | Spare links, Ring topologies, Multi-homing  | Automatic protection switching, Dynamic rerouting protocols, Self-healing rings, Call gapping,  |
| Intelligent Network Subsystem | Physical diversity in signaling network links, Physical database diversity  | Dynamic routing, Checkpoint protocols   |

# Survivable Cellular Backhaul Network Design Problem



Minimize

- Total Network Cost

Given:

- Traffic requirements

Variables:

- Topology

- Channel capacity

- Traffic Routing

- Location of BSC, MSC

Constraints:

- Link capacity

- Reliability

- Quality of service

Split into wireless and wired part

# Survivable Backhaul Network Design

- Formulated a set of survivable network design optimization problems
  - APS, Ring, Mesh, look at tradeoffs.
  - Optimization problems are Mixed Integer Programming Problems
  - Include parameters in the model to oversize signaling and spare resources to absorb transients from user movement
  - Consider green field and incremental design cases
  - NP- Hard – solve for small networks using CPLX
  - Developing heuristics for scaling solution to larger cases

# Wireless Network Survivability: Summary

- Survivable network design needs to incorporate unique characteristics of wireless access networks
- Different survivability strategies could be used to guard against various network failures
  - 2-phase network design (minimum cost + mesh restoration) was proposed for designing survivable wireless access networks
  - Adaptive QoS on radio level and overlapping cells.
- Constraint satisfaction based design of WLANs
- Ongoing work focuses on 3G/4G including hybrid WLAN/3G wireless networks

# Ongoing Work

- Security in 4G/Hybrid Wireless Networks
  - Identification of vulnerabilities and attacks and development of a security architecture
  - Protocol development for seamless roaming between WWANS and WLANs
  - A containment based secure routing scheme for WLANs
- Survivability in 4G/Hybrid Wireless Networks
  - Network design for 3G and 802.11 systems
  - Network design for 4G/Hybrid wireless networks
  - Traffic restoration protocols for fault tolerance
- Interaction between security and survivability