Resilient Networks
Missouri S&T University CPE 6510
Wireless Network Resilience

Egemen K. Çetinkaya
Department of Electrical & Computer Engineering
Missouri University of Science and Technology

cetinkayae@mst.edu

http://web.mst.edu/~cetinkayae/teaching/CPE6510Spring2017
Wireless Network Resilience

Outline

• Overview
• Resilience
• Security
Wireless Network Resilience

Overview

- Overview
- Resilience
- Security
Wireless Networks

Geographic Scope

• Body area network – WBAN
• Personal area network – WPAN
• Local area network – WLAN
• Metropolitan area network – WMAN
• Wide area network – WWAN
• Example protocols?
Wireless Networks
Protocol Examples

- Body area network – WBAN
  - e.g. ?
- Personal area network – WPAN
  - e.g. ?
- Local area network – WLAN
  - e.g. ?
- Metropolitan area network – WMAN
  - e.g. ?
- Wide area network – WWAN
  - e.g. ?
Wireless Networks
Protocol Examples

• Body area network – WBAN
  – e.g.: wearable computing, sensor networks: IEEE 802.15.6

• Personal area network – WPAN
  – e.g.: personal computing devices: IEEE 802.15

• Local area network – WLAN
  – e.g.: coverage area of home or office: IEEE 802.11

• Metropolitan area network – WMAN
  – e.g.: coverage area 10-20 km: IEEE 802.16

• Wide area network – WWAN
  – e.g.: cellular telephony: CDMA, GSM
Link Layer Background
MAC Protocol Taxonomy

• *What are the types of MAC protocols?*
  – *How can the access to wireless channel be arbitrated?*
Link Layer Background
MAC Protocol Taxonomy

- Channel partitioning
- Random access
- Coordinated access
- Spread spectrum
- *Examples?*
Link Layer Background
MAC Protocol Taxonomy

• Channel partitioning
  – channel divided into smaller pieces
    • e.g. TDMA, FDMA, OFDMA, WDMA

• Random access
  – channel not divided, collisions occur
    • e.g. ALOHA, slotted ALOHA, CSMA, CSMA/CD

• Coordinated access
  – nodes takes turns
    • e.g. token ring, polling

• Spread spectrum
  – multiple users spread across the spectrum
    • e.g. CDMA
Wireless Networks

Types

- Wireless local area network
- Mobile cellular network
- Satellite network
- MANET – mobile ad hoc network
- Wireless sensor network (WSN)
- Vehicular ad hoc network (VANET)
- Airborne network
Wireless Local Area Networks

Characteristics

• Wireless LAN – local area network
  – $O (1 \text{ km})$

• IEEE 802.11 standard families
  – covers physical and MAC layer implementation specification
  – standards: 802.11 a – ay

• Wi-Fi ≠ IEEE 802.11
  – Wi-Fi is the alliance that performs tests

• Security is covered in IEEE 802.11i standard families
  – WEP, wired equivalent privacy, 1999-2004
  – WPA, Wi-Fi protected access, 2003-2004
  – WPA2, 2004-?
Mobile Cellular Networks
Generation Evolution

- First generation – 1G; 1980s, analog voice
- Second generation – 2G; 2000s, digital voice
  - 2.xG – 2G with data service, GPRS
    - x can be 5, 75, 9, etc.
- Third generation – 3G; 2010s, higher data rate
  - UMTS for GSM, EVDO for CDMA; 3.x: LTE, WiMAX
- Fourth generation – 4G; 2015s, higher data rate
  - 1 Gb/s stationary rate, 100 Mb/s mobile rate
- Fifth generation – 5G; 2020s, higher data rate
- Generations: number of bits per second per Hz
  - spectral efficiency (b/s)/Hz
Mobile Cellular Networks

Challenges

• Traffic engineering
  – dropped call probability
  – attempt/success ratio
• Handoff failures between base stations
• Roaming failures between providers
• Phone phreak
  – similar to computer hacker
• Privacy concerns
  – listening calls
  – location tracking
Satellite Networks
Characteristics

• Orbital types
  – LEO – low earth orbit, 400-1,500 km altitude
  – MEO – medium earth orbit, 8,000-18,000 km altitude
  – GEO – geostationary earth orbit, 35,786 km altitude

• Challenges
  – satellite collision
    • in 2009 Iridium 33 collided with Kosmos-2251
  – many vulnerabilities recently found
Mobile Ad Hoc Networks
Characteristics

• Does not have infrastructure
  – peer to peer communication
    • access to Internet through a gateway or base station
  – self-organized to form the network

• Application areas:
  – e.g. environmental and health monitoring, military, disaster

• Communication among vehicles
  – VANET – vehicular ad hoc network
Mobile Ad Hoc Networks
Routing

• Routing algorithm discovers paths
  – between source and destination

• *Routing algorithm classes*?
Mobile Ad Hoc Networks

Routing

- Routing algorithm discovers paths
  - between source and destination
- Routing algorithm classes:
  - distance vector (e.g. RIP)
  - link state (e.g. OSPF)
  - source routing (e.g. DSR)
- Traditional routing does not work for MANET
- Many MANET routing protocol exist:
  - AODV, OLSR, DSDV, DSR
  - mostly scenario specific
    - mobility, topology change, geographic, etc.
Wireless Sensor Networks
Characteristics

- Small nodes
- Large scale
- Low cost
- Energy constrained
- Data centric vs. address centric
- In-network processing
  - aggregation, fusion
  - makes it impossible for E2E security
- Military, healthcare, environmental monitoring
- Similar to MANET except limited resources and fusion
Airborne Networks
Scenario and Environment

- Very high relative velocity
  - Mach 7 ≈ 10 s contact
  - dynamic topology

- Communication channel
  - limited spectrum
  - asymmetric links
    - data down omni
    - C&C up directional

- Multihop
  - among ANs
  - through relay nodes
Wireless Network Resilience

- Overview
- Resilience
- Security
Scope of Resilience
Relationship to Other Disciplines

Challenge Tolerance

Survivability
- many \( \lor \) targeted failures

Fault Tolerance
- few \( \land \) random

Disruption Tolerance
- environmental
- delay
- mobility
- connectivity
- energy

Traffic Tolerance
- legitimate
- flash crowd
- attack
- DDoS

Robustness Complexity

Trustworthiness

 Dependability
- reliability
- maintainability
- safety

 Dependability
- availability
- integrity

Security

AAA
- confidentiality
- nonrepudiability

Performability

QoS measures

Fault Tolerance

Survivability

Disruption Tolerance

Traffic Tolerance

Challenge Tolerance

Trustworthiness

Dependability

Security

Performability

Scope of Resilience
Relationship to Other Disciplines
Resilient Networks

Sub-Disciplines: Challenge Tolerance

- **Survivability**
  - many \( \lor \) targetted failures

- **Fault Tolerance**
  - few \( \land \) random

- **Traffic Tolerance**
  - legitimate, flash crowd, attack, DDoS

- **Disruption Tolerance**
  - environmental
    - delay, mobility, connectivity, energy

- **Trustworthiness**
  - Dependability
    - reliability, maintainability, safety
  - Availability
    - availability, integrity, confidentiality
  - Security
    - AAA
      - nonrepudiability, auditability, authorisability, authenticity
  - Performability
    - QoS measures

- **Fault Tolerance**
  - (few \( \land \) random)

- **Traffic Tolerance**
  - legitimate, flash crowd, attack, DDoS

- **Disruption Tolerance**
  - environmental
    - delay, mobility, connectivity, energy

- **Trustworthiness**
  - Dependability
    - reliability, maintainability, safety
  - Availability
    - availability, integrity, confidentiality
  - Security
    - AAA
      - nonrepudiability, auditability, authorisability, authenticity
  - Performability
    - QoS measures
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 behavior
    - unpredictably long delay
Disruption Tolerance
Overview of Challenges

- **Mobility**
  - handoff, roaming failures
  - topology, routing, location management

- **Connectivity**
  - jamming
  - lossy wireless links

- **Delay**
  - interplanetary communication
  - disconnected operations

- **Energy**
  - resource constrained networks
  - e.g. WSN (wireless sensor networks)
Communication Environment

Impact of Wireless Channel

• 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 Channel

• 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 Mobility

- 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 Mobility

• 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 optimizations temporary)
Communication Environment

Impact of Mobility

- 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 optimizations temporary)
Communication Environment
Impact of Unpredictably High Latency

- 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
Communication Environment
Impact of Unpredictably High Latency

- 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-×-delay products
    - real-time reaction to many bits in flight difficult or impossible
    - massive buffering required for error control
Resilience and Survivability
Assumptions and Challenges

- 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 Challenges

- 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
Wireless Network Resilience

Security

• Overview
• Resilience
• Security
Resilient Networks
Sub-Disciplines: Trustworthiness

- Challenge Tolerance
- Survivability
  - many \( \lor \) targeted
- Fault Tolerance
  - (few \( \land \) random)
- Disruption Tolerance
  - environmental
- Traffic Tolerance
  - legitimate, flash crowd
  - attack, DDoS

Trustworthiness
- Security
  - AAA
    - availability
    - integrity
    - nonrepudiability
    - confidentiality
    - authorisability
    - authorisability
    - auditability
    - authenticity
- Dependability
  - reliability
  - maintainability
  - safety
- Performability
  - QoS measures

Survivability, many \( \lor \) targeted
Fault Tolerance, (few \( \land \) random)
Disruption Tolerance, environmental
Traffic Tolerance, legitimate, flash crowd, attack, DDoS

Trustworthiness, security, AAA, availability, integrity, nonrepudiability, confidentiality, authorisability, authorisability, auditability, authenticity
Dependability, reliability, maintainability, safety
Performability, QoS measures

Fault Tolerance, environmental
delay, mobility, connectivity
Security in Wireless Networks

Attacks

- Node compromise
- Eavesdropping
- Privacy of data
- Denial of service attacks
- Malicious use of commodity networks
Security in Wireless Networks

Node Compromise

• Node compromise
  – node physically captured by an adversary
  – countermeasures?

• Eavesdropping
• Privacy of data
• Denial of service attacks
• Malicious use of commodity networks
Security in Wireless Networks

Node Compromise

- Node compromise
  - node physically captured by an adversary
  - countermeasures:
    - tamper-resistant hardware – expensive
    - node-to-node authentication in software
    - erasable memory

- Eavesdropping
- Privacy of data
- Denial of service attacks
- Malicious use of commodity networks
Security in Wireless Networks

Eavesdropping

- Node compromise
- Eavesdropping
  - passive attack – easy due to open channel
  - countermeasures?
- Privacy of data
- Denial of service attacks
- Malicious use of commodity networks
Security in Wireless Networks

Eavesdropping

- Node compromise
- Eavesdropping
  - passive attack – easy due to open channel
  - countermeasures:
    - encryption – harder for large-scale sensor networks
    - multipath routing – parts of message sent on different paths
- Privacy of data
- Denial of service attacks
- Malicious use of commodity networks
Security in Wireless Networks

Privacy

- Node compromise
- Eavesdropping
- Privacy of data
  - unauthorized access to information
  - countermeasures?
- Denial of service attacks
- Malicious use of commodity networks
Security in Wireless Networks

Privacy

• Node compromise
• Eavesdropping
• Privacy of data
  – unauthorized access to information
  – countermeasures:
    • encryption
    • access control
    • reduction in data details – e.g. aggregation in sensor networks
• Denial of service attacks
• Malicious use of commodity networks
Security in Wireless Networks

Denial of Service Attacks

• Node compromise
• Eavesdropping
• Privacy of data
• Denial of service attacks
  – aims for network resource exhaustion
  – physical, link, network, transport layer perspectives
• Malicious use of commodity networks
DoS Attacks and Countermeasures

Physical Layer

- Attacks?
- Countermeasures?
DoS Attacks and Countermeasures

Physical Layer

• **Attacks:**
  – jamming
    • simple
  – battery exhaustion

• **Countermeasures:**
  – spread spectrum techniques
  – buffering during attack
    • requires memory
  – authentication
  – use of alternative transmission during attack
    • IR or optical

[WS2002]
DoS Attacks and Countermeasures

Link Layer

- Attacks?
- Countermeasures?
DoS Attacks and Countermeasures
Link Layer

• **Attacks:**
  – collision or corrupting frames for checksum mismatch
  – battery exhaustion by retransmissions
  – unfairness

• **Countermeasures:**
  – error correcting codes against collisions
    • expensive; requires more bandwidth
  – link layer admission control and rate limiting
  – use of small frames against unfairness
DoS Attacks and Countermeasures

Network Layer

- Attacks?
- Countermeasures?
DoS Attacks and Countermeasures
Network Layer

• **Attacks:**
  – neglecting or greedy nodes
  – misdirection of packets
  – black holes partitions network
    • by advertising zero-cost routes

• **Countermeasures:**
  – authorization
  – redundant messages
  – multipath routing
  – monitoring
  – probing

[WS2002]
DoS Attacks and Countermeasures

Transport Layer

- Attacks?
- Countermeasures?
DoS Attacks and Countermeasures
Transport Layer

- **Attacks:**
  - flooding
    - memory exhaustion for stateful connections
  - desynchronization
    - forged messages (e.g. control flag, seq. #) for retransmission

- **Countermeasures:**
  - authentication
  - limiting number of connections
  - client puzzles
    - computationally expensive

[WS2002]
Security in Wireless Networks
Malicious Use of Commodity Networks

- Node compromise
- Eavesdropping
- Privacy of data
- Denial of service attacks
- Malicious use of commodity networks
  - use of sensor for illegal purposes
    - e.g. planting them in computers to extract data
  - countermeasure
    - deployment of sensor networks to detect malicious activity
    - this makes attack expensive, but cannot defend
Routing Security Overview

- Network layer functions?
Routing Security
Overview

• Network layer functions
  – addressing: node identifiers
  – routing: path discovery
  – forwarding: next-hop decision and transfer
  – signalling: control messages
  – traffic management:

• Attacks are similar for MANETs and WSNs
• Public-key cryptography is computationally expensive
  – in particular for energy-constrained large-scale WSNs
• Fast symmetric-keys must be used sparingly
Routing Security
Attacks on Routing Protocols

- Spoofed, altered, or replayed routing information
- Selective forwarding
- Sinkhole attacks
- Sybil attacks
- Wormholes
- **Hello** flood attacks
- Acknowledgement spoofing
Attacks on Routing Protocols

Spoofed Routing Information

- Spoofed, altered, or replayed routing information
- Targets the routing info exchanged between nodes
- Impacts:
  - creates routing loops
  - partitions network
  - increases end-to-end delay
Attacks on Routing Protocols
Sybil Attack

- A node presents multiple identities to other nodes
- Significant threat to geographic routing protocols
- Impacts:
  - significantly reduces effectiveness of fault tolerance schemes
    - distributed storage
    - dispersity/heterogeneity/multipath routing
    - topology maintenance
- Sybil attack can be prevented via identity verification
  - using digital signatures
Attacks on Routing Protocols

Spoofed Message Example

- Spoofed, altered routing information
- Sybil attack
Attacks on Routing Protocols

Selective Forwarding

- Malicious nodes refuse to forward certain messages
  - if all messages are dropped a black hole is created
  - black holes are easy to detect
    - i.e. may not serve an attackers objective
- Most effective when malicious node is on data path
  - if not on data path, sinkhole or Sybil attacks are effective
- Multipath routing to counter selective forwarding
Attacks on Routing Protocols

Selective Forwarding Example

- Selective forwarding, adversary on the data path
  - between source and destination
Attacks on Routing Protocols

Sinkhole Attack

- Attacker attracts all traffic nearby
- Attraction occurs w.r.t. routing algorithm
  - e.g. high quality route advertisement via adversary
- Enables selective forwarding (SF) but makes SF trivial
- Geographic routing protocols are resistant to sinkhole
Attacks on Routing Protocols

Wormhole

- Adversary tunnels messages
  - in one part of network to a different part via low latency link
- Involvement of two adversaries is more common
- Essentially a sinkhole attack
- Exploits the routing race condition
  - ignoring later messages
- Detection is difficult when used with sybil attack
- Wormhole and sinkhole attacks are hard to defend
  - harder when used in combination
Attacks on Routing Protocols
Wormhole and Sinkhole Example

- Wormhole and sinkhole
Attacks on Routing Protocols

Flood Attack

- Nodes broadcast **HELLO** messages
  - adversaries announce themselves to neighbors
- Powerful devices needed
  - to convince network that the adversary is node’s neighbor
- Nodes hearing this message will use this route
- Prevented via verification of bidirectionality of links
  - this is useless if the attacker has a sensitive receiver
- Detection of flood attacks:
  - alarm if node is neighbor of unusual large number nodes
Attacks on Routing Protocols
HELLO Flood Example

- **HELLO** messages flood the network by powerful node
Attacks on Routing Protocols
Acknowledgement Spoofing

- Routing protocols rely on link layer acknowledgement
- Adversary spoofs these messages
  - to notify neighboring nodes
    - a weak link is strong
    - a dead node is alive
- Spoofed messages can be used to launch SF attack
Key Management
Comparison of Schemes

• A networkwide shared key
  – simple
  – even one node compromise can reveal everything

• Multiple keys:
  – one for link establishment, one per pair for communication
  – erase networkwide key after session establishment
  – cannot add new nodes after initial key-establishment

• Public-key cryptography
  – any node can set-up secure key with any other node
  – expensive for WSNs

[PSW2004]
Key Management
Comparison of Schemes

- A unique key between each pair of nodes
  - does not scale well
    - need \( n(n-1)/2 \) keys
- Bootstraping keys using a base station
  - base station becomes single point of failure
- Random-key predistribution
  - require less keys (memory) in the node
  - sufficient amount of compromised nodes can reveal scheme

[PSW2004]
References and Further Reading


• Some slides are adopted from “KU EECS 983 – Resilient and Survivable Networking” class taught by Prof. James P.G. Sterbenz
References and Further Reading
