15-496 : A Hand-on Introduction to Wireless Networks

Lecture 10: Wireless and the Internet

Peter Steenkiste
Departments of Computer Science and Electrical and Computer Engineering

Spring Semester 2008

http://www.cs.cmu.edu/~prs/wireless08/

Outline

- Wireless and the Internet
- Mobility: Mobile IP
- Security: EAP and Radius
- Diversity
  - » Loss: TCP over wireless
  - » Delay: multimedia
  - » Devices: WAP

Internet Architecture Assumptions

- Host are (mostly) stationary
  - » Address assignment, routing
- Links in the network are fairly homogeneous
  - » Transport protocols, applications
- Hosts are fairly powerful
  - » End to end principle: push functionality to end points
- Security is an end host issue
  - » No security inside the network (architecturally)

Mobility

- Many clients today are mobile
- Mobility inside a subnet is supported
  - » E.g. moving across APs that are part of a single EBSS
- Mobility across subnets is harder because the IP address is used as address and identifier
  - » Identifier: who you are
  - » Address: where you can be found
- Keep IP address: network gets confused
  - » Delivers packets to wrong “old” subnet
- New IP address: host gets confused
  - » Transport protocols, applications, etc.

Link Heterogeneity

- Original links were basically telephone lines
- Today: huge diversity
  - » Optical fiber (wavelengths) … copper … wireless
- Throughput is most visible diverse features
  - » Optical links 40 Gbps … Wireless links of Kbps
- But other features are different as well:
  - » Error characteristics: higher on wireless
  - » Latency: absolute delay and variance in delay
- Mobility adds to diversity
  - » E.g. hand off can cause delays and sudden changes in available bandwidth

Device Capabilities

- Originally: mainframes and personal computers
- Today: sensors … supercomputers
- Note: almost any networked device today is more capable than early computers!
  - » But our requirements and expectations have increased
  - » Anything at or above “PC class” is very capable
- Laptop: view as mobile PC
- PDA: view as 5 year old PC (kind of)
- Cell phone: not even close to a PC
- Sensors: often run as private networks

Security

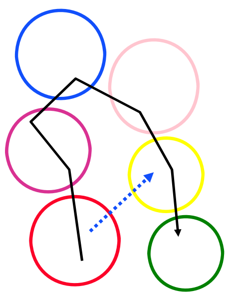
- Access to the network enables all kinds of attacks
  - » Argues for pushing security inside the network
  - » Firewalls are a very ad hoc way of doing this
- Wireless creates unique challenges
  - » Do not need physical connection to sniff or send
- Discussed (briefly) in the 802.11 lectures
  - » WEP, 802.1x, etc.
- But wireless security needs to be linked into system wide security

Outline

- Wireless and the Internet
- Mobility: Mobile IP
- Security: EAP and Radius
- Diversity
  - » Loss: TCP over wireless
  - » Delay: multimedia
  - » Devices: WAP

Mobility across IP Subnets

- When moving across IP subnets, different protocols have conflicting requirements
- Network layer wants IP address in current subnet
  - » Needed for routing of packets
- Transport layer want IP address that was used to create connection
  - » Is used to identify the connection
- Applications often do not care but in practice they want to keep the IP address the same
  - » Tied to sockets



Mobile IP Goals

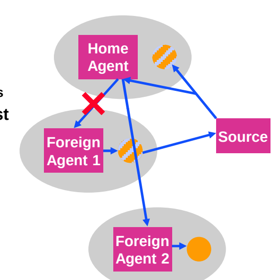
- Communicate with mobile hosts using their “home” IP address
  - » Allows any host to contact mobile host using its “usual” IP address
- Mobility should be transparent to applications and higher level protocols
  - » No need to modify the software
- Minimize changes to host and router software
  - » No changes to communicating host
- Security should not get worse

Mobile IP

- Home network has a home agent that is responsible for intercepting packets and forwarding them to the mobile host.
  - » E.g. router at the edge of the home network
  - » Forwarding is done using tunneling
- Remote network has a foreign agent that manages communication with mobile host.
  - » Point of contact for the mobile host
- Binding ties IP address of mobile host to a “care of” address.
  - » binding = (IP address, foreign agent address)
  - » binding includes time stamp

Mobile IP Operation

- Agents advertise their presence.
  - » Using ICMP or mobile IP control messages
  - » Mobile host can solicit agent information
  - » Mobile host can determine where it is
- Registration process: mobile host registers with home and foreign agent.
  - » Set up binding
- Tunneling
  - » forward packets to foreign agent
  - » foreign agent forwards packets to mobile host
- Supporting mobility
  - » invalidating old caches in a lazy fashion



Optimizations

- Mobile host can be its own the foreign agent.
  - Mobile host acquires local IP address
  - performs tasks of the mobile agent
- Short circuit the home location by going directly to the foreign agent.
  - Routers in the network store cache bindings and intercept and tunnel packets before they the mobile host's home network
  - Need a protocol to update/invalidate caches
  - Raises many security questions and is not in the standard

Security Considerations

- Authentication of mobile host, home agent
  - avoid invalid interception of traffic
- Authentication of mobile host, foreign agent
  - Desirable, but more difficult, so not required
- Use encryption for sensitive data
- Replay of registration messages.
  - standard problem
  - use standard solutions, e.g. timestamps, nonce, ..
- Dealing with the firewalls at the foreign site.
  - most easily sent directly to destination
  - but has a "strange" IP network address in source field
  - reverse tunneling by foreign agent or mobile host
  - Can replace tunnels by UDP for NATs

Discussion

- Mobile not used in practice
- Was not designed for truly mobile users
  - I.e. for continuous operation across subnets
  - Switching between subnets is heavy weight
- Was designed for nomadic users
  - I.e. visitors are a remote site
- Value for nomadic is limited to:
  - Mobile user is contacted using home IP address
  - User maintains connections between subnets
  - Neither of them are very likely or common
  - Laptops are mostly used for accessing servers

Outline

- Wireless and the Internet
- Mobility: Mobile IP
- Security: EAP and Radius
- Diversity
  - Loss: TCP over wireless
  - Delay: multimedia
  - Devices: WAP

Wireless Security

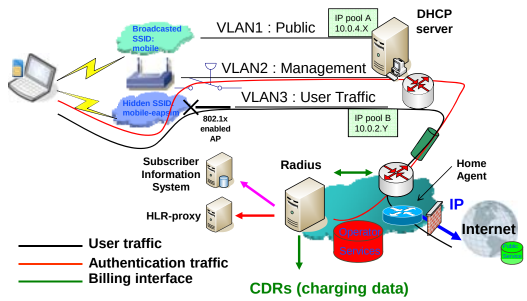
- Security is not just about authentication and encryption
- Must also consider business and deployment issues
  - AAA: Authentication, Authorization, and Accounting
  - Supporting users at different levels

Authentication in WLAN Hotspots

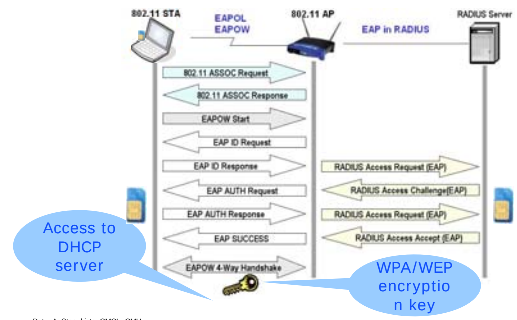
- Upon association with the AP, only authentication traffic can pass through, as defined by IEEE 802.1x

- The protocol used to transport authentication traffic is the EAP standard (RFC3748)

Dual SSID Approach



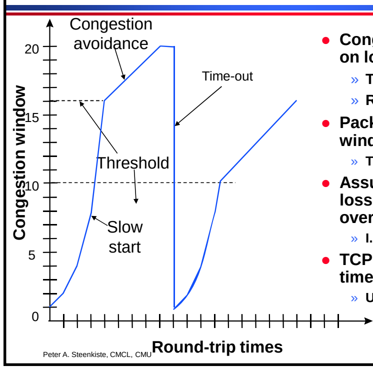
802.1x and EAP Protocol Execution



Outline

- Wireless and the Internet
- Mobility: Mobile IP
- Security: EAP and Radius
- Diversity
  - » Loss: TCP over wireless
  - » Delay: multimedia
  - » Devices: WAP

TCP Congestion Control

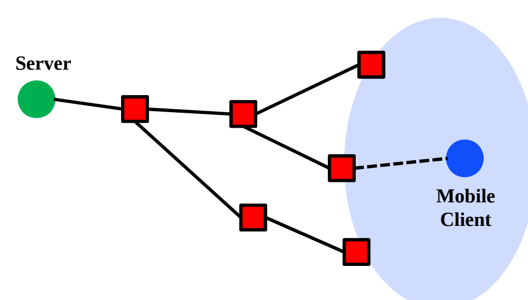


- Congestion detection based on lost packets:
  - » Timeout or
  - » Receipt of duplicate ACKs
- Packet loss results in cutting window in half
  - » To reduce congestion in network
- Assumes all (or most) packet losses are due to queue overflow
  - » I.e. two are equivalent
- TCP also estimates roundtrip time
  - » Used to set timeout value

Challenges in Wireless

- Wireless network may drop packet due to link errors
  - » Will be interpreted as congestion losses by TCP sender
  - » Will result in backoff and loss of throughput
  - » TCP tends to perform poorly when error rates go above 1%
- High variability of properties wireless links could also confuse TCP
  - » TCP likes nice predictable paths
- Roundtrip time can be variable
  - » Due to wireless retransmissions, handoff, …
- Available bandwidth can fluctuate
  - » Rate adaptation, interference, handoff, …

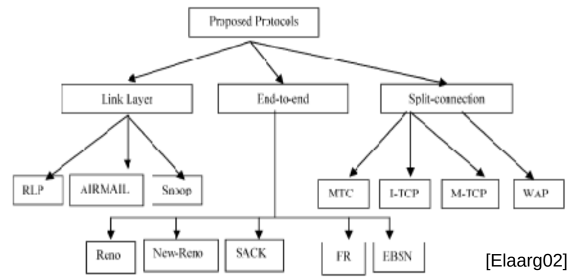
Solution Ideas?



Solution Space

- Modify TCP for wireless paths
  - » Would maintain status quo for wired paths
  - » What would wireless TCP look like?
  - » Difficult to do: there are many Internet hosts
  - » Traditionally, hosts have no information about path properties
- Modify TCP for all paths
  - » Not clear what that modification would be!
  - » Similar problems: need to modify many hosts
- Modify TCP only on the mobile host
  - » Interesting idea – kind of what WAP does in an extreme way
- Keep end hosts the same but tweak things at the wireless gateway
  - » Keep end-end TCP happy despite wireless links

Possible Classification of Solutions

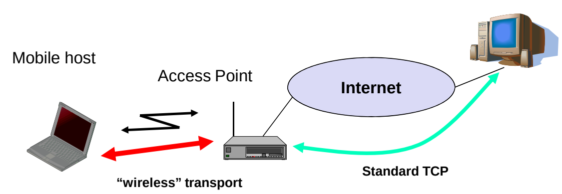


[Elaarg02]

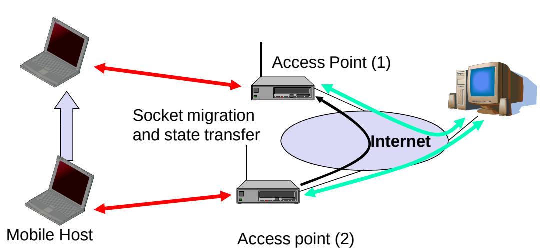
Connection Split: Indirect TCP or I-TCP

- Do not change TCP on the wire-line part
- Split the TCP connection at the wireless gateway into two parts
  - » One optimized for the wireless link
  - » The second for the wire-line communication (TCP)
- No real transport-layer end-to-end connection
  - » Although host on wired network does not know this
- Wired host should not notice the characteristics of the wireless part
  - » This is a challenge since wireless gateway is limited in what it can send and when, e.g. cannot prematurely acknowledge data
  - » Certain things cannot be hidden: delay, dramatic throughput variations

I-TCP



I-TCP and Mobility



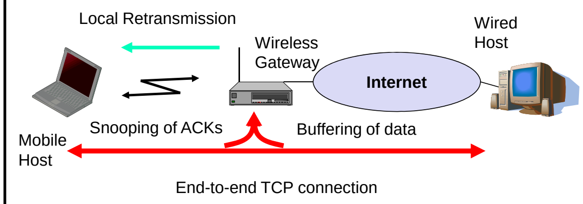
I-TCP Discussion

- I-TCP Advantages
  - » No changes in the fixed network or hosts (TCP protocol), all current TCP optimizations still work
  - » Wireless transmission errors do not "propagate" to the wire-line network
  - » Simple, effective (in the best case)
- I-TCP Disadvantages
  - » End-to-end semantics become less clear, e.g. what happens if the wireless gateway crashes
  - » Higher end-to-end delays due to buffering and forwarding to the gateway

Snooping TCP

- "Transparent" extension of TCP within the wireless gateway
  - » End hosts are not modified
- Hides wireless losses from wired host
  - » Buffer packets sent to the mobile host
  - » Local retransmission: Lost packets on the wireless link, for both directions, are retransmitted immediately by the mobile host or foreign agent
- Wireless gateway "snoops" the packet flow so it can cover up signs of packet loss
  - » E.g. recognizes acknowledgements in both directions and suppresses duplicate ACKs

Snooping TCP



Snooping TCP Discussion

- Data transfer to the mobile host
  - » FA buffers data until it receives ACK from the MH
  - » FA detects packet loss via duplicated ACKs or time-out
- Data transfer from the mobile host
  - » FA detects packet loss on the wireless link via sequence numbers
  - » FA answers directly with a NACK to the MH
  - » MH can now retransmit data with only a very short delay
- Integration of the MAC layer
  - » MAC layer often has similar mechanisms to those of TCP
- Problems
  - » Snooping TCP does not isolate the wireless (as I-TCP)
  - » Snooping might be useless if encryption is used

How about Mobility?

- Split connection approach
  - » Hard state at access point must be moved to new base station
- Snoop approach
  - » Soft state need not be moved
  - » While the new access point builds new state, packet losses may not be recovered locally
- Frequent handoffs remain a problem
  - » Hard state should not be lost
  - » Soft state needs to be recreated for performance

Mobile TCP

- Handling of long and frequent disconnections
- M-TCP splits connection as I-TCP does
- Wireless gateway monitors all packets but
  - » Does no caching, no retransmission
  - » If it detects a disconnection
    - – It sets the sender's window size to 0
    - – Sender automatically goes into "persist" mode
- Advantages
  - » ETE semantics are maintained, no buffer forwarding
- Disadvantage
  - » Wireless link loss propagates to the wire-line network

An Internet Style Approach

- Use aggressive retransmission in the wireless network to hide retransmission losses
  - » Most deployed wireless network in fact do that already
  - » Would sell few products if they did not
- Wireless losses are translated into increased delay
  - » But TCP roundtrip time estimation is very conservative, e.g. increases if variance is high
- Also: persistent high loss rate results in reduced available bandwidth -> congestion response is appropriate and needed
- Works remarkably well!

Outline

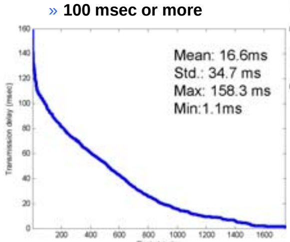
- Wireless and the Internet
- Mobility: Mobile IP
- Security: EAP and Radius
- Diversity
  - » Loss: TCP over wireless
  - » Delay: multimedia
  - » Devices: WAP

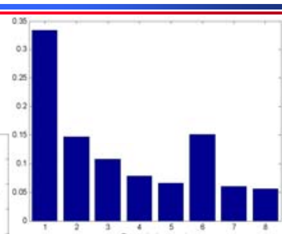
Outline

- Wireless and the Internet
- Mobility: Mobile IP
- Security: EAP and Radius
- Diversity
  - » Loss: TCP over wireless
  - » Delay: multimedia
  - » Devices: WAP

Variable Latency in Wireless Networks

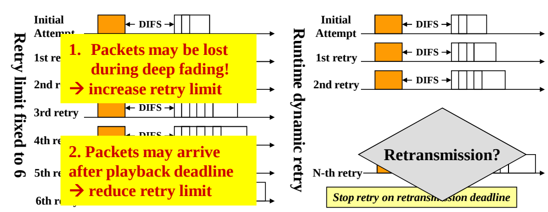
- Retransmissions in 802.11 results in variable e-e latency
  - » 100 msec or more





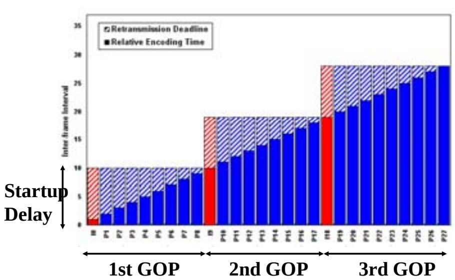
- Variability is increased by
  - » Use of exponential backoff
  - » Freezing of backoff counter when the medium is busy

Time Aware Adaptive Retry



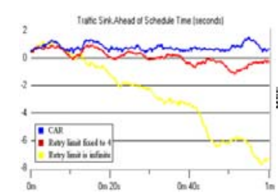
- 802.11 retransmission takes a fixed try limit for every packet (count based)
- CAR dynamically determines retry limit for each packet using its "retransmission deadline"

TAR: Retransmission Deadline

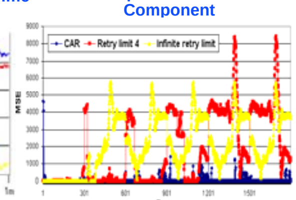


Comparison of Visual Quality

Results of the Ahead of Schedule Time



Mean Square Error of the Y Component



Packets with a value smaller than zero is behind its playback schedule

$$MSE = \frac{1}{M \times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[x(i,j) - \hat{x}(i,j)]^2$$

42

What About Cell Phones?

- Cell phones have very limited capabilities:
  - » Low bandwidth
  - » Small display and limited "keyboard"
  - » Small memory and processing capabilities
- Raises issues at different layers:
  - » HTML is too rich for cell phone I/O capabilities
  - » General purpose protocol likely to be too inefficient, big, and unresponsive
- Result: define a completely new stack and glue it to the IP stack using a gateway
  - » Ugly but practical

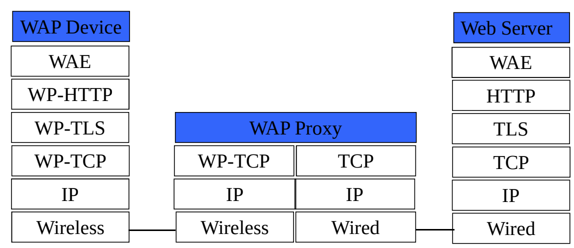
Wireless Access Protocol (WAP)

- Protocol stack for small low-powered devices
  - » E.g. cell phones
- Layered Protocol, like IP stack
  - » Two versions of protocol stack
    - – WAP1.x Protocol Stack
    - – WAP2.0 Protocol Stack
  - » Based on some older, proprietary protocols
  - » Provide security
- Connects WAP devices with a WAP gateway
- Gateways translate wireless protocols into Internet protocols
  - » Located near Mobile Telephone Exchange

WAP 2.x Protocol Stack

WAP Device	
WAE	Wireless Application Environment
WP-HTTP	Wireless Profiled HTTP
WP-TLS	Wireless Profiled TLS (SSL)
WP-TCP	Wireless Profiled TCP
IP	Internet Protocol
Wireless	2.5G and 3G

WAP 2.0 Proxy



Wireless Markup Language

- Very specialized for cell phones
  - » Needs to be compact
- Window has limited size
  - » Server needs to optimize for specific devices
  - » Standards ways of chaining windows and window layout
- Keyboard is limited
  - » Supports concise ways of using standard buttons on cells phones