

18-759: Wireless Networks

Lecture 12: 802.11 Management

Peter Steenkiste
Dina Papagiannaki
Spring Semester 2009
<http://www.cs.cmu.edu/~prs/wireless09/>

Peter A. Steenkiste, CMU

1

Announcements

- **Midterm: next week Wednesday**
 - » Closed book
 - » Lectures 1-13
 - » Questions similar to what is on the homeworks
- **Surveys: will announce schedule soon**
 - » You can get started right away
 - » Don't forget to hand in draft slides (see handout)
 - » TAs will present example survey this Wednesday
- **Homework 2 has been posted**
 - » Answers will be posted right after deadline
- **Project assignment has been posted**
 - » Send e-mail right away if you have questions

Peter A. Steenkiste, CMU

2

Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 management
- 802.11 security
- 802.11 power control
- 802.11*
- 802.11 QoS

Peter A. Steenkiste, CMU

3

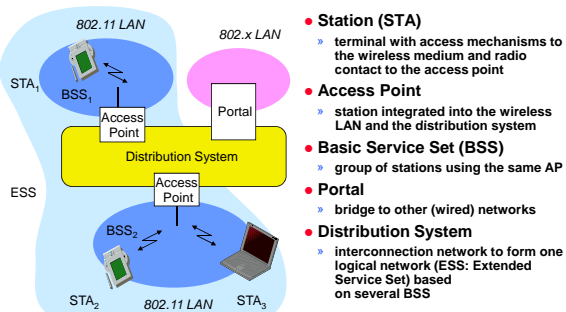
Management and Control Services

- Association management
- Handoff
- Security: authentication and privacy
- Power management
- QoS

Peter A. Steenkiste, CMU

4

802.11: Infrastructure Reminder



Peter A. Steenkiste, CMU

5

Service Set Identifier - SSID

- **Mechanism used to segment wireless networks**
 - » Multiple independent wireless networks can coexist in the same location
 - » Effectively the name of the wireless network
- **Each AP is programmed with a SSID that corresponds to its network**
- **Client computer presents correct SSID to access AP**
- **Security Compromises**
 - » AP can be configured to "broadcast" its SSID
 - » Broadcasting can be disabled to improve security
 - » SSID may be shared among users of the wireless segment

Peter A. Steenkiste, CMU

6

Association Management

- Stations must associate with an AP before they can use the wireless network
 - › AP must know about them so it can forward packets
 - › Often also must authenticate
- Association is initiated by the wireless host – involves multiple steps:
 1. Scanning: finding out what access points are available
 2. Selection: deciding what AP (or ESS) to use
 3. Association: protocol to “sign up” with AP – involves exchange of parameters
 4. Authentication: needed to gain access to secure APs – many options possible
- Disassociation: station or AP can terminate association

Peter A. Steenkiste, CMU

7

Association Management: Scanning

- Stations can detect AP based by scanning
- Passive Scanning: station simply listens for Beacon and gets info of the BSS
 - › Beacons are sent roughly 10 times per second
 - › Power is saved
- Active Scanning: station transmits Probe Request; elicits Probe Response from AP
 - › Saves time + is more thorough
 - › Wait for 10-20 msec for response
- Scanning all available channels can become very time consuming!
 - › Especially with passive scanning
 - › Cannot transmit and receive frames during most of that time – not a big problem during initial association

Peter A. Steenkiste, CMU

8

Association Management: Selecting an AP and Joining

- Selecting a BSS or ESS typically must involve the user
 - › What networks do you trust? Are you willing to pay?
 - › Can be done automatically based on stated user preferences (e.g. the “automatic” list in Windows)
- The wireless host selects the AP it will use in an ESS based on vendor-specific algorithm
 - › Uses the information from the scan
 - › Typically simply joins the AP with the strongest signal
- Associating with an AP
 - › Synchronization in Timestamp Field and frequency
 - › Adopt PHY parameters
 - › Other parameters: BSSID, WEP, Beacon Period, etc.

Peter A. Steenkiste, CMU

9

Association Management: Roaming

- Reassociation: association is transferred from active AP to a new target AP
 - › Supports mobility in the same ESS – layer 2 roaming
- Reassociation is initiated by wireless host based on vendor specific algorithms
 - › Implemented using an Association Request Frame that is sent to the new AP
 - › New AP accepts or rejects the request using an Association Response Frame
- Coordination between APs is defined in 802.11f
 - › Allows forwarding of frames in multi-vendor networks
 - › Inter-AP authentication and discovery typically coordinated using a RADIUS server
 - › “Fast roaming” support (802.11r) also streamlines authentication and QoS, e.g. for VoIP

Peter A. Steenkiste, CMU

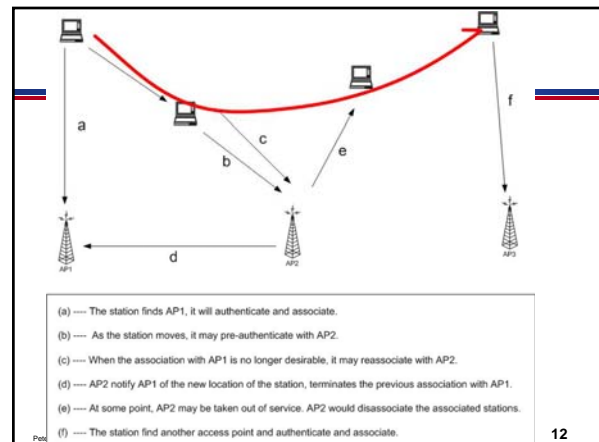
10

Association Management: Reassociation Algorithms

- Failure driven: only try to reassociate after connection to current AP is lost
 - › Typically efficient for stationary clients since it not common that the best AP changes during a session
 - › Mostly useful for nomadic clients
 - › Can be very disruptive for mobile devices
- Proactive reassociation: periodically try to find an AP with a stronger signal
 - › Tricky part: cannot communicate while scanning other channels
 - › Trick: user power save mode to “hold” messages
 - › Throughput during scanning is still affected though
 - Mostly affects latency sensitive applications

Peter A. Steenkiste, CMU

11



12

Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 management
- 802.11 security
- 802.11 power control
- 802.11*
- 802.11 QoS

Peter A. Steenkiste, CMU

13

WLAN Security Requirements

- **Authentication:** only allow authorized stations to associate with and use the AP
- **Confidentiality:** hide the contents of traffic from unauthorized parties
- **Integrity:** make sure traffic contents is not modified while in transit

Peter A. Steenkiste, CMU

14

Security in 802.11b

- **WEP: Wired Equivalent Privacy**
 - › Achieve privacy similar to that on LAN through encryption
 - › Intended to provide both privacy and integrity
 - › RC4 and CRC32
 - › Has known vulnerabilities
- **WPA: Wi-Fi Protected Access**
 - › Larger, dynamically changed keys
- **802.1x: port-based authentication for LANs**
 - › Port-based authentication for LANs
- **802.11i (WPA2)**
 - › Builds on WPA
 - › Uses AES for encryption

Peter A. Steenkiste, CMU

15

WLAN Security Exploits

- **Insertion attacks**
 - › Unauthorized Clients or AP
- **Client-to-Client Attacks**
 - › DOS - duplicate MAC or IP addresses
 - › Can also be used to get free service on “secured” APs
- **Interception and unauthorized monitoring**
 - › Packet Analysis by “sniffing” – listening to all traffic
- **Jamming – denial of service**
 - › Cordless phones, baby monitors, leaky microwave oven, etc.

Peter A. Steenkiste, CMU

16

WLAN Security Exploits

- **Brute Force Attacks Against AP Passwords**
 - › Dictionary Attacks Against SSID
- **Encryption Attacks**
 - › Exploit known weaknesses of WEP
- **Misconfigurations**
 - › APs ship in an unsecured configuration
 - › Many people use APs with default configuration

Peter A. Steenkiste, CMU

17

MAC Filtering

- Each client identified by its 802.11 NIC Mac Address
- Each AP can be programmed with the set of MAC addresses it accepts
- Combine this filtering with the AP's SSID
- Very simple solution
 - › Some overhead to maintain list of MAC addresses
- But it is possible to forge MAC addresses ...
 - › Unauthorized client can “borrow” the MAC address of an authenticated client
 - › Built in firewall will discard unexpected packets

Peter A. Steenkiste, CMU

18

Wired Equivalent Privacy WEP

- **Employs RC4 to Encrypt/Decrypt data**
 - » RC4 is a stream cypher based on a symmetric algorithm
 - » 40 bit encryption key is supplied by the user
 - » 24 bit initialization vector (IV) is supplied in the header
 - » 64 bit string is seed for PRNG to generate a "key sequence"
 - » 40 and 64 bit WEP are the same thing
- **ICV (integrity check value) is computed for plaintext (CRC-32)**
- **ICV is appended to plaintext to create data string**
- **Key Sequence is XORed to data string to create ciphertext**
- **Ciphertext and IV are sent to receiver**
- **128-bit encryption uses a 104+24 bit key**

Peter A. Steenkiste, CMU

19

WEP-Based Security Discussion

- **WEP has known vulnerabilities**
- **Key can be cracked with a couple of hours of computing**
 - » IV transmitted in the clear
 - » No protocol for encryption key distribution
 - » Clever optimizations can reduce time to minutes
- **All data then becomes vulnerable to interception**
 - » WEP typically uses a single shared key for all stations
- **The CRC32 check is also vulnerable so that the data could be altered as well**
 - » Can make changes without even decrypting!
- **128-bit WEP encryption is recommended**

Peter A. Steenkiste, CMU

20

WEP Authentication

- **Access request by client**
- **Challenge text sent to client by AP**
- **Challenge text encoded by client using shared secret then sent to AP**
- **If challenge text encoded properly, AP allows access; else access is denied**

Peter A. Steenkiste, CMU

21

Port-based Authentication

- **802.1x is the IEEE standard for port-based authentication**
- **Users get a username/password to access the access point**
- **Was originally defined for switches but extended to APs**
- **Can be used to bootstrap other security mechanisms**
 - » Effectively creating a session

Peter A. Steenkiste, CMU

22

Wi-Fi Protected Access WPA

- **Introduced by Wi-Fi Alliance as an interim solution after WEP flaws were published**
 - » Uses a different Message Integrity Check
 - » Encryption still based on RC4, but uses 176 bit key (48bit IV) and keys are changed periodically
 - » Also frame counter in MIC to prevent replay attacks.
- **Can be used with 802.1x authentication (optional)**
 - » It generates a long WPA key that is randomly generated, uniquely assigned and frequently changed.
 - » Attacks are still possible since people sometimes use short, poorly random WPA keys that can be cracked
- **802.11i is a "permanent" security fix**
 - » Builds on the interim WPA standard (i.e. WPA2)
 - » Replaces RC4 by the more secure Advanced Encryption Standard (AES) block encryption
 - » Better key management and data integrity
 - » Uses 802.1x for authentication.

Peter A. Steenkiste, CMU

23

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

Peter A. Steenkiste, CMU

24

Authentication in WLAN Hotspots

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

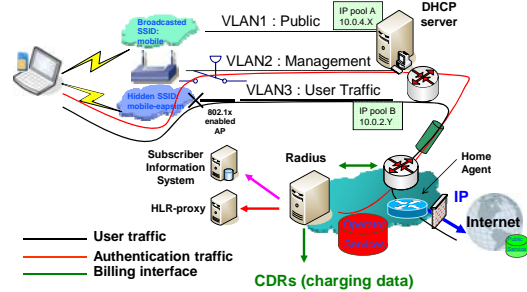


- The protocol used to transport authentication traffic is the Extensible Authentication Protocol (EAP - RFC3748)

Peter A. Steenkiste, CMU

25

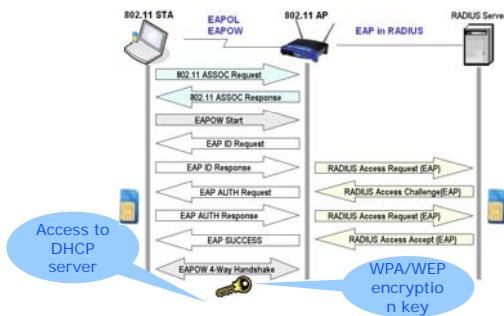
Dual SSID Approach



Peter A. Steenkiste, CMU

26

802.1x and EAP Protocol Execution



Peter A. Steenkiste, CMU

27

Best Practices for WiFi Security

- Use WEP
 - » But change default key and change WEP key frequently
 - » Better than no security plus some possible legal benefits
 - » APs support WAP today
- Change the default configuration of your AP:
 - » Change default passwords on APs
 - » Don't name your AP by brand name
 - » Don't name your AP by model #
 - » Change default SSID
- Use MAC filtering if available
- Use a VPN
 - » Must assume that wireless segment is untrusted
 - » Provides end-to-end encryption – is what you want!

Peter A. Steenkiste, CMU

28

Wardriving

- The act of locating and possibly exploiting to a wireless network while driving around a city
- You need a vehicle, a laptop, a wireless PC card and some kind of antenna
- People can intercept your wireless signal when the signal exceeds your building
- <http://www.wardriving.com>
- Is this legal??

Peter A. Steenkiste, CMU

29