Challenges of WiFi

Meng Cao
Ziyue Chen
Xiangqing Sun

Content

1. Introduction
2. Ease of Use
3. Security
4. Mobility
5. Network Management

1. Introduction

- WLAN based on IEEE 802.11b standard

- challenges:
  - ease of use - simplicity of operation;
  - security - adequate protection in public network;
  - mobility - in public hotspots with secure always-on connectivity is difficult;
  - network management - prevent hacker attacks and interference from other systems.

2. Ease of Use

- WiFi configuration is complicated
  - for "automatic wireless configuration", typically 18 steps are required for initial setup, errors may occur.
- WEP(Wired Equivalent Privacy)
  - the native security capability offered by WiFi;
  - designed for simplicity of operation;
  - difficult to use in many WiFi installations where security is important.
- other problems
  - browser-based authentication is convenient, but vulnerable to theft-of-service attacks;
  - more comprehensive approaches specified in 802.1x protect attacks but more complex.

3. Security

- problem -- vulnerable to eavesdroppers and other hackers.

even WEP is on, the encryption key can be recovered by a hacker.

- two solutions:

1. Native Security(Enhanced WEP)
   - addressed in 802.1x standard;
   - focus on access control and encryption;
     - access control: mutual authentication, that is, network authenticates itself to the user and vice versa;
     - encryption: Temporal Key Integrity Protocol(TKIP), an improved encryption procedure to deal with the key recovery attack.

3. Security

2. Virtual Private Network(VPN)

- provides a VPN tunnel running on top of the wireless network and extending from users' computer to a VPN gateway;
- end-to-end protection;
- the cost is significant:
  - a distinct and independent wired network must be installed and maintained;
  - scaling to large number of users is difficult because all WiFi communications in the community must be processed by a VPN gateway.

4. Mobility

- Core feature of WiFi networking
  - roaming with the vicinity of a given Access Point
  - global roaming capability

4. Mobility: Technology

- Device-level multivendor interoperability
  - 802.11b standard
  - Wireless Ethernet Compatibility Alliance (WECA)
  - Wireless Internet Service Provider roaming (WISPr)
- Always-on mobility
  - Promptly on demand, close-and-go, open-and-resume operation
  - Mobile IP (MIP):
    - Central mobility manager to keep track of mobile user
    - Mobility client to handle connection details in the vicinity of user
    - Slow handoff
    - Poor OS support

4. Mobility: Service Providers

- Economic viability
- Three major approaches
  - Franchisor:
    - pays internal WiFi network to offer public access
  - Carrier:
    - owns and operates a number of APs in public places
  - Aggregator:
    - partnership with WiFi operators and resells their services

5. Network Management

- Why Manage Network?
  - Ensure that the network is robust and secure

- Comparisons
  - WLANs vs. Wired LANs
    - Physical layer: the air links
      -Unpredictable

  - WLANs vs. Cellular Networks
    - Cellular systems: Designed as complete systems
    - WLANs: Overlays onto existing infrastructure

5. Network Management

- Challenges
  - Signal Strength
  - Interference Management
  - The Rogue AP

5. Network Management

- Signal Strength
  - in Wired LANS
    - Failure: Broken wires, faulty interface card…
      - Binary, work or not work
  - in WLAN
    - Routine changes in the location - 30dB variation of Signal Strength
  - Distinguish between variations
    - normal operation? failure?

5. Network Management

- Signal Strength
  - Manually
    - For small networks: dozens of AP
    - Local experts: familiar with the network
  - Tools
    - Larger networks: impossible to be managed manually
    - Physical layer management tools:
      - Radio Resource Measurement Study Group

5. Network Management

- Interference Management

  - Enviroment
    - Cellular: licensed frequency bands
    - WiFi: cope with multiple sources of interference

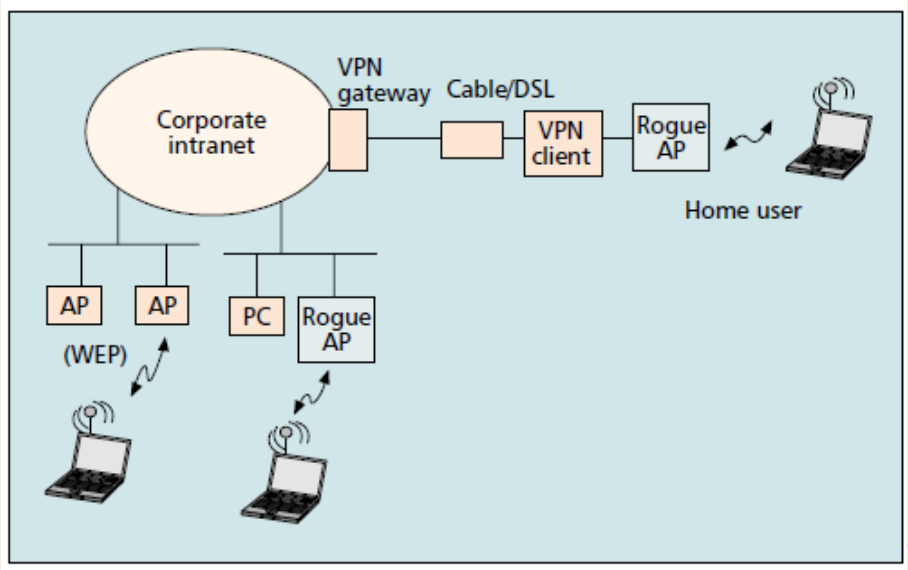
  - Strategies
    - Managing mutual interference among users
      - MAC-layer techniques, frequency channelization
    - IEEE 802.11e tools:
      - Dealing with bandwidth hogs

5. Network Management

- Interference Management
  - WiFi networks are still vulnerable
    - Other sources:
      - Microwave Oven…
    - Not serious at the moment but increasingly severe

5. Network Management

- Rogue AP
  - An unauthorize AP in the network



Thank you!