Week 10 Lecture 1

Wireless Network + security

# 7.1 Introduction (Week 9 lecture 2)

Last week we talked about the introduction of wireless network, things covered

* Typical setup
* Base station (compared to wired network)
  + Cell towers,
  + Access point
* Hops and infrastructure in network
* Wireless network characteristics

# 7.2 IEEE 802.11 Wireless LAN

Graphical user interface, text

Description automatically generated

The evolution of these protocols happened in the physical layer, the Wi-Fi communication are made more robust and the data rate increased significantly. We use multiple antennas.

* all use CSMA/CA for multiple access
* all have base-station and ad-hoc network versions

## 802.11 LAN architecture

Diagram

Description automatically generatedBase station = access point (AP)

Basic Server Set (BSS or cell) in infrastructure mode contains:

* Wireless hosts
* Access point: base station
* Ad hoc mode: hosts only

## 802.11b 2.4GHz-2.485:

Spectrum divided into 11 channels at different frequencies:

* Modern access point automatically assigns channel.
* interference possible: channel can be same as that chosen by neighbouring AP

Chart

Description automatically generated with medium confidence

We don’t want overlapping channels, so it is intuitive to use combination of ch1 ch6 and ch11. But overlapping can happen.

## Host must associate with an AP

**Passive scanning:** host listens to the beacons, pick the strongest one and associate.

1. beacon frames sent from Aps
2. association request frame sent: H1 to selected AP
3. association response frame sent from selected AP to H1

Diagram, shape

Description automatically generated

**Active scanning:**

A picture containing text, clock

Description automatically generated

1. Probe request frame broadcast from H1
2. Probe response frames sent from Aps
3. Association request frame sent: Host 1 to select the AP with strongest signal
4. Association response frame sent from selected AP to H1

## Multiple access issue

* 802.11: CSMA - sense before transmitting
* 802.11: no collision detection!

1. difficult to receive (sense collisions) when transmitting due to weak received signals (fading), this is very common in wireless network, when the distance is far away, signal is weak
2. can ’t sense all collisions in any case: hidden terminal, fading

## Avoid collisions: CSMA/C(ollision)A(voidance)

The collision only matters at the receiver, the receiver can only hear one node at any given time.

Chart, funnel chart

Description automatically generated**Distributed Coordination Function (DCF)**

802.11 sender

* If sense channel idle for DIFS then transmit entire frame
* If sense channel busy, then start random backoff time timer counts down while channel idle transmit when timer expires. If no ACK, increase random backoff interval repeat 2

802.11 receiver

* return ACK after SIFS (ACK needed due to hidden terminal problem)

idea: allow sender to “reserve” channel rather than random access of data frames: avoid collisions of long data frames

1. sender first transmits small request-to-send (RTS) packets to base station using CSMA
2. Base station broadcasts clear-to-send CTS in response to RTS
3. CTS heard by all nodes:
   1. sender transmits data frame
   2. other stations defer transmissions
4. RTS and CTS contain the direction for transmitting the subsequent data frame

Diagram

Description automatically generated with medium confidence

Figure 1 nodes are using 802.11 MAC with RTS/CTS enabled

In this situation here, B know exactly how long it should defer its transmission because the CTS will contain the duration, including the ACK time.

# Network Security

## Cryptography

* m is plain text
* KA(m) ciphertext, encrypted with key KA
* M = KB(KA(m))

**Symmetric key cryptography**: requires sender, receiver know shared secret key

Simple encryption scheme

Substitution cipher: substituting one thing for another:

* Monoalphabetic cipher
* Caesar cipher

Permutation of keys

Breaking an encryption

* Brutal force
* Statistical analysis
* known-plaintext attack: has (part of) plaintext corresponding to ciphertext
* chosen-plaintext attack: get ciphertext for chosen plaintext

**Sophisticated encryption approach**

Encryption key: n substitution ciphers, and cyclic pattern

* Polyalphabetic ciphers

## Stream Cipher

encrypt one bit at time, RC4 is a popular stream cipher, key can be from 1 to 256 bytes

Diagram

Description automatically generated

## Block Cipher

Break plaintext message in equal-size blocks and then encrypt each block as a unit, for example, take 3 bits at a time and look it up in the table.

Text

Description automatically generated with medium confidence

However, when the table is too big, it slows things down

DES: Data Encryption Standard => AES: Advanced Encryption Standard

## Cipher Block Chaining (exam contents)

cipher block chaining: send only one random value alongwith the very first message block, and then have the sender and receiver use the computed cipher block in place of the subsequent random number

Text

Description automatically generated

## Public Key Cryptography

Diagram, timeline

Description automatically generated

## RSA

Diagram, text

Description automatically generatedA picture containing text, person, screenshot, document

Description automatically generatedCreate public/private key pair

## Session keys

exponentiation in RSA is computationally intensive, therefore,

* In practice, we use RSA to exchange a symmetric key Ks
* Once both have Ks, they use symmetric key cryptography

## Message integrity (Lecture 2)

sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

## Authentication (Lecture 2)

sender, receiver want to confirm identity of each other

## Securing Email (Lecture 2)