Lecture 11: Energy and security considerations in wireless PHY + link layers

Mythili Vutukuru

CS 653 Spring 2014

Feb 10, Monday

Energy and Security

- We will look at energy and security considerations in the wireless PHY and link layers
- Wireless PHY operates in broadcast mode – the reason behind the energy and security problems we will see in this lecture
  - Radio is on for long periods of time, often decoding unnecessary packets addressed to others
  - Broadcast nature makes it easy to snoop and manipulate wireless traffic
- We will look at solutions to address energy and security issues arising in the physical and link layers
- We will revisit energy and security later in the course as well, from the perspective of higher layers

Energy efficiency in WiFi

- WiFi radio is in one of the four states
  - Transmitting a frame
  - Receiving a detected transmission on the air
  - When it is not sending or receiving, it listens to the medium to identify start of packet.
  - When it is not sending or receiving, and when it has a packet to send, it also waits for backoff to count down to 0. During this time, it performs carrier sense in every time slot to decrement backoff.
- Thus, WiFi radio is spending energy even when it is idle (i.e., not TX or RX)

Energy efficiency in WiFi (2)

- 802.11 has a power save mode of operation. Client periodically schedules a “sleep” time. Any incoming packets for this client in this time are buffered and transmitted by the AP at a later time after the client has woken up.
- Sleeping can be at scheduled intervals or in an unscheduled fashion (but coordinated with explicit messages between client and AP)
- This power save mode still does not eliminate the wait time during backoff, which is a significant portion in busy networks

Energy efficiency in cellular networks

- When a user has data to send or receive, the user goes from idle to active state by exchanging several signaling messages. In the active state, the user is allocated resources to transmit on the wireless channel, among other things. Power consumption of a mobile phone is higher in active state.
- The mobile waits in the active state for a little while longer after the last data is sent, in case more information arrives shortly afterwards
- If this wait time is too small, the system will have to process extra signaling messages and deal with frequent transitions between idle and active states
- If wait time is too large, it will be a waste of resources and energy
- Currently, wait time is a fixed constant. But proposals exist to dynamically tune the wait time based on various other factors

Security in WiFi

- Currently, the physical layer can detect and decode traffic sent to all other nodes in the network
- Spread spectrum based modulation schemes (e.g., 1 and 2 Mbps rates of 802.11) are based on spreading the signal over a wider band. These are harder to detect without the right despreading code. But higher rates like OFDM are easy to detect and decode by anyone.
- Link layer filters out frames destined for itself. Can allow all frames through in promiscuous mode.
- Link layer addresses are easy to spoof, so a node can send and receive frames with any MAC address easily

Security in WiFi (2)

- Currently, most link layers provide mechanisms for encryption.
  - Shared key between client and AP is used to encrypt link layer payloads
  - Key management is tricky
  - Many encrypting algorithms based on the idea of symmetric key cryptography
- Many threats still exist
  - E.g., rogue APs or fake APs to steal data, man-in-the-middle attacks
- Higher layer security mechanisms still needed

Security in cellular networks

- 2G networks were susceptible to attacks by rogue base stations, but current cellular networks are fairly secure at the PHY + link layers
- The SIM card itself holds the secret keys and identifiers, so harder to spoof and compromise
- We will revisit security at higher layers (e.g., mobile application security) later in the course