Lecture 12

Friday, 24 March 2023 08:45

Bluetooth → very constrained devices

IEEE 802.11 / Wi-Fi → usually no energy constraints

BT → today, BLE (Bluetooth v5)

mesh (earlier on, only star topology was supported)

→ increases e.g. robustness to interference

different layer architecture, some of which is closed source

physical/MAC layer IEEE 802.15.1

range 10 – 100 m

FHSS with hopping frequency 1600 per second

data rate 2 Mb/s

3 channels for advertising, 37 data channels

the same channel is not used for two consecutive transmission

packet size PHY layer 2 – 39 bytes, MAC layer ≤ 37 bytes

mode 1 : encryption → level 4: authenticated LE secure connection pairing with encryption

mode 2 : signing

security fundamentals

- encryption + authentication in BT mesh, always used → mandatory, so downgrading not allowed
- message obfuscation
- trashcan attack protection i.e. forward secrecy
- secure device provisioning

separation of concerns

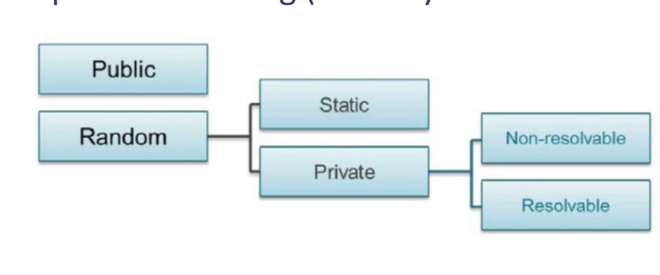
BT uses AES-CCM → fixed MIC length

not AES-CCM*, which generalizes of AES-CCM

Salt 1 ≈ AES-CCM with 'give' input

BLE Devices Addressing

- Public: Organization Unique Identifier (OUI) obtained by IEEE Registration Authority
- Static: do not change until power-cycling the device
- Resolvable: can be used to derive the long-term address
- Non-Resolvable: prevent tracking (recently attacked in BT 4.0)



BT keys

- network key — shared during provisioning with all nodes in subnetwork
- device key — shared during provisioning between 2 nodes
- application key ?

similar to Zigbee

joining BT network based on publish subscribe

generic access profiles?

five phases

1. beaconing — new devices emit beacons; here: new devices emit, Zigbee: wait after join; BT's approach has lower duty cycle, likely more efficient
2. invitation — the provisioner understand what to do next; 2a. provisioning invite sent 2b. new device reports with provisioning capabilities
3. exchanging public keys — use public key algorithm (ECDH) (usually hardware-supported) to exchange shared key; two options: with / without available out of band (OOB) channel (e.g. code on display, sound)
4. authentication — can be done over OOB channel, concludes with confirmation value check
   - output OOB: select random number, output, and let user input on other device — preferred over input OOB
   - input OOB: input on unprovisioned device, output on provisioner
   - static / no OOB: generate random numbers, checked later
   - confirmation value check: checks whether exchanged materials were correctly shared
5. provisioning data distribution
   - network key
   - device key
   - key index
   - flags
   - IV index
   - unicast address

AES-CCM used to generate network + device key

IEEE 802.11

bandwidth different

2.4 GHz and 5 GHz

can have high data rates

Channels interfere in blocks of 4!

channel 14 used only in e.g. Japan

wireless hosts

ad-hoc networks do not have external connection, infrastructure networks do

coordination function

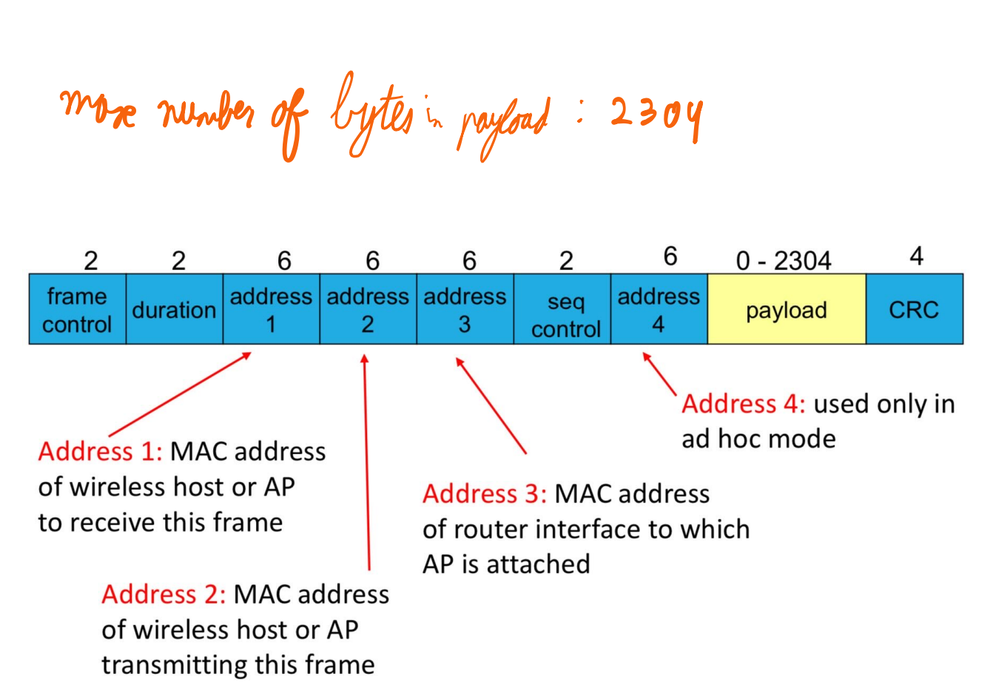
CSMA-CA ↑ collision avoidance

hidden terminal problem

CTS-RTS

in Wi-Fi, time is usually slotted but specifying message length may be necessary

max number of bytes in payload : 2304



most IoT devices nowadays use WPA2.

RSN security services

- authentication
- access control
- confidentiality with message integrity

EAP = Extensible Authentication Protocol

IEEE 802.11i provides security between STA and AP — not end-to-end security

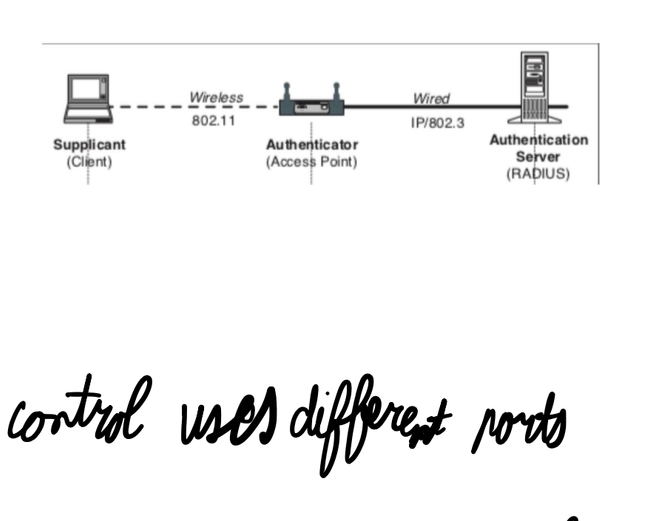
only e.g. DTLS provides end-to-end security

(joining) phases similar to BT, but with authentication before key management

802.1x controlled port remains blocked until keys are received (for transmitting data)

IEEE 802.1x Architecture

- IEEE 802.1x defines three additional elements
  - **Supplicant**, the client that wishes to perform authentication
  - **Authenticator**, element that receives requests from supplicant, and proxies traffic to authentication server
  - **Authentication Server (AS)**, element that oversees actual authentication of the supplicant. Could also reside together with the Authenticator.



access control uses different ports

- uncontrolled port for traffic to authentication server
- controlled port allows data only if authorized (if authentication passed?)

EAP phases

- EAP over LAN
- RADIUS between AP & AS
- at end, ports still blocked; temporary keys should be generated

regarding keys, main thing to remember: pairwise keys (includes temporal keys?), group keys

4-ways handshake includes nonces, MAC (for detecting MitM), pairwise temporal key (is a combination of different keys) → important, used for group key handshake

WPA personal

WPA enterprise uses MSK/AAA key

protected data transfer in WPA2 → CCMP → more complex hardware

provides confidentiality + integrity

connection termination used to teardown communication + restore communication to original state

WPA3 improves on too-short keys of WPA2

4-way handshake replaced by simultaneous authentication of equals (SAE) → extension of dragonfly key exchange, modular arithmetic?

→ forward secrecy

WPA3 enterprise

- increased cryptographic robustness
- enhanced network resiliency

to remember

- BT phases + order + scope
- Wi-Fi phases + order + scope
- how to join Wi-Fi networks