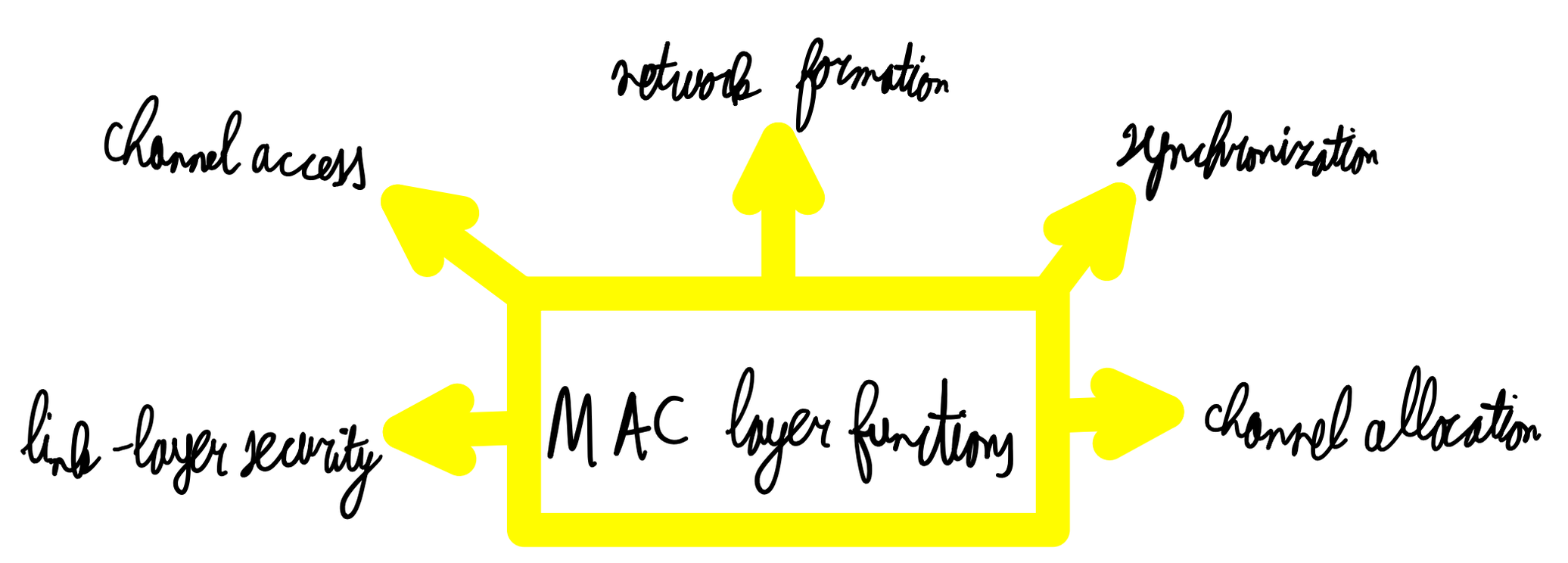
Lecture 4

Friday, 17 February 2023 08:45

link-layer security



physical layer only deals with actual data transmission

IEEE is used in eg Zigbee and Thread

bandwidth / **frequencies** 868 / 902-928 MHz
2.4 GHz

fully function devices FFD can serve as network coordinator; has capability to orchestrate network

Reduced function devices RFD can only send messages to FFD

(initially) star topology

(later also) mesh topology

channel access is based on slots

initially CSMA-CA also used by WiFi

CSMA-CA

- if channel idle: transmit frame
- if channel busy: random backoff
  - retransmit when timer expires
  - if another failure, increase backoff time, then repeat

ACK needed due to hidden terminal problem

use request-to-send (RTS) and clear-to-send

a slot groups the operations necessary to **successfully** transmit a packet and receive the corresponding ack

default slot duration: 10 ms (or multiple of 10 ms for constrained devices

alternative technique: channel hopping

a radio scheduling table can assign any of the following behaviors per node and per slot:

- TX
- RX
- TX/RX
- sleep (of radio, not of CPU)

maximum physical layer packet size 128 bytes

MTU at MAC layer: 127 bytes (= 128 − 1) length-header

approximately 100 bytes for MAC payload

---

enabling security decreases the space available for the MAC payload

two security services:

- data confidentiality
- data authenticity

also: protection against replay attacks

auxiliary security header

frame counter is not the same as sequence number

key identifier mode tells whether key is identified explicitly or implicitly (in key identifier)

MIC = message integrity code

encryption is based on AES-CCM*

AES-128 in counter mode for encryption (payload-only)

AES-CBC-MAC for data authenticity (header + payload)

pairwise or group keys can be used

secKeyIdLookupList contains 'terms of usage' of key

- key ID
- keySource, keyIndex
- set of devices that can use key
- types of frame that can be protected using this key

macSecurityLevel information on minimum required security level for each type of frame

macDeviceTable list of devices authorized for communication

OutgoingFrameSecurity
IncomingFrameSecurity
→ many implemented tasks

MAC-low operations to be executed right before/after transmitting / receiving a MAC-layer frame; no pre-computation possible...

MAC-high operations independent from TX/RX

problem: sequence number **cannot be** pre-computed

increasing time-slot duration is undesireable because it reduces the number of packets and hence the amount of data per second / the throughput

security computations are often sped up by dedicated hardware for cryptographic operations

a downside of this approach is that it makes software depend on specific hardware

key management is delegated to upper layers and not addressed by IEEE 802.15.4

allows for more tailored key management strategy

lack of standardization

Zigbee has three types of symmetric key

- network key
- link key
- master key for confidentiality of symmetric-key key establishment (SKKE)

CBKE (certificate-based key establishment)

ECQV certificates

(Elliptic-Curve Qu Vanstone)

no transmission of signatures to reduce key overhead