Imperial College London

446H – Applied Network Security

4. WiFi security

Dr Sergio Maffeis
Department of Computing
Course web page: https://446h.cybersec.fun

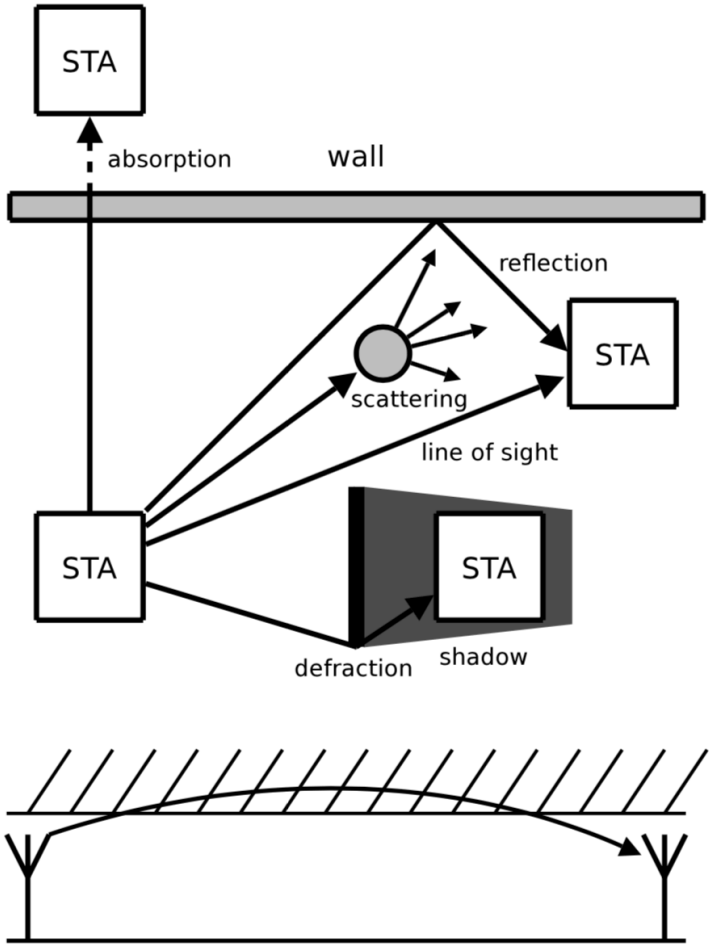
WiFi basics

Imperial College London

- terminology
  - WiFi <=> 802.11
  - AP: access point, the provider of the WiFi network
    - More generally, /base station/
    - Typically performs also a router-like behaviour connecting clients to a wired destination network
  - Client/Station: the client connecting to the network
    - More generally, /wireless host/
- *association*
  - a client can be associated to an AP
    - if it is in range
    - if it uses the AP to connect to the effective destination network
- network types
  - single- or multi-hop: one wireless hop and rest is wired, or more wireless hops
  - inftrastructure-based or -less: connects to a wider network or not
  - examples
    - SHIB: typicial home WiFi setup
    - SHIL: Bluetooth connection
    - MHIB: wifi mesh
    - MHIL: MANETs, VANETs

Wireless link

Imperial College London



- logical channel that connects wireless devices
  - characterized for example by transmission rate and distance
- issues
  - signal strength decreases with distance
  - open to interference
  - multipath propagation of same signal creates further interference

WiFi etiquette

Imperial College London

- from FCC guidelines
  - Listen before talk
  - When talking, make frequent pauses and listen again
  - Don‘t talk too loud
- Carrier Sense Multiple Access (CSMA)
  - each machine listens to see if another machine is transmitting before sending a data packet
- Packet collisions
  - hard to detect: signal at receiver is different than at source
  - strategy is to avoid
  - challenge: 2 clients may not know of each other presence
    - *fading*: out of range, but both in range of AP
    - *hidden terminal*: occlusion between clients, but not towards AP

WiFi versions

Imperial College London

- Standards IEEE 802.11 a/b/g/n/ac/ad
  - a: old, 5GHz, slow
  - b: 2.4 GHz, 11Mbps
  - g: 2.4 GHz, 54Mbps
  - n: 2.4 or 5 GHz, 100+Mbps
  - n-2009 MIMO: 600Mbps
  - ac: (2014) 1Gbps
  - ad: up to 7Gbps
- Ideal speed at 1m from AP, with no interference or multiple users

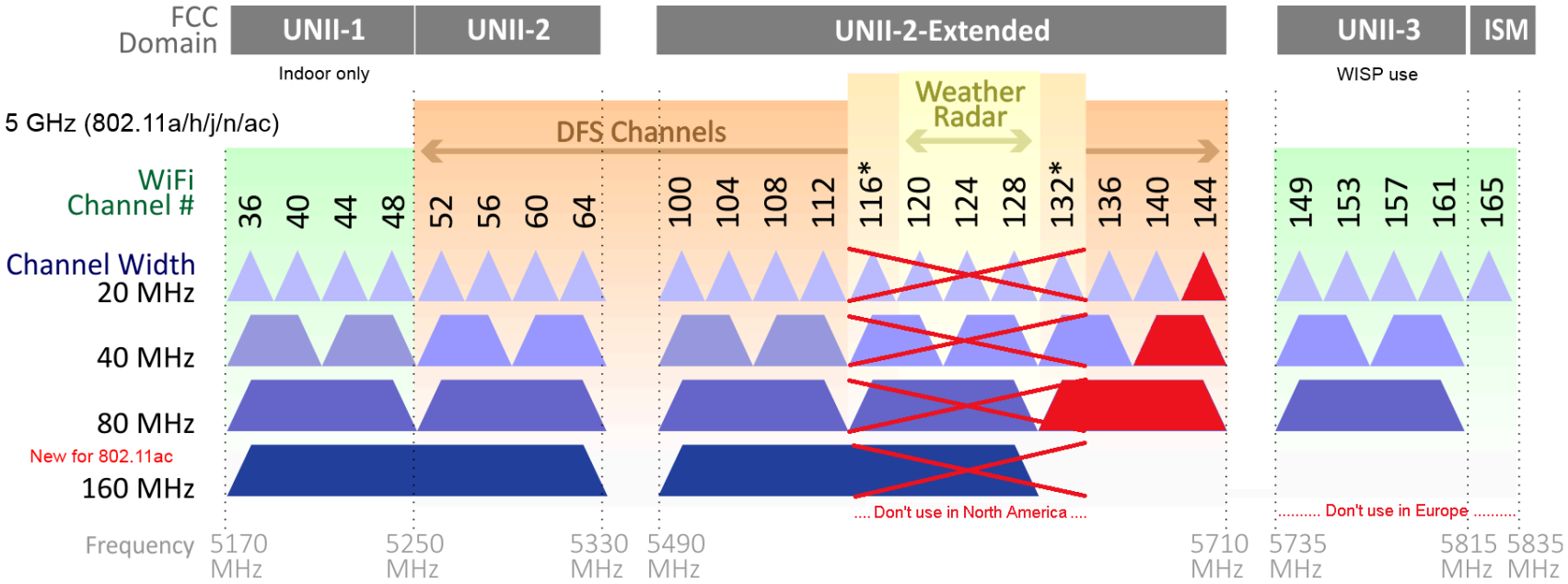
Spread spectrum

Imperial College London

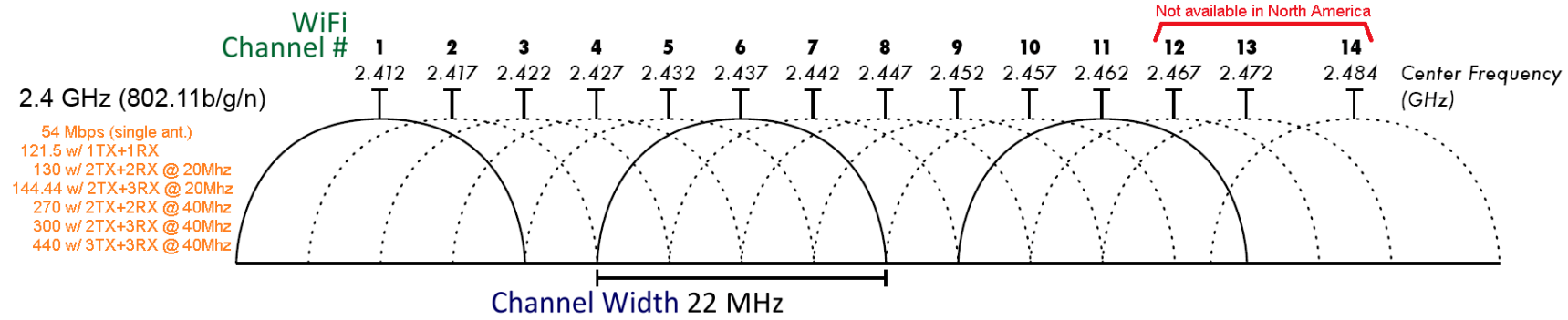
- if communication is concentrated on one frequency, interference there may render channel unusable
- idea is to spread over the available spectrum
- original 802.11 allowed Frequency Hopping (FH) and Direct Sequence (DS)
- 802.11b uses DS in 2.4GHz band
- 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM) on the 5MHz band
- 802.11g uses OFDM on 2.4GHz band
- 802.11n adds multiple antennas
  - MIMO (multiple input, multiple output)
  - 2 or more antennas on client and AP sending different signals
- 2.4GHz channels are separated by 5MHz
  - spread-spectrum usage centers on channel frequency but bandwidth has diameter of 22MHz
  - only 1,6,11 are interference free in that band
- 5GHz are a big mess, depending on regional laws
  - some channels are used by radar, so can be used indoor only and if radar usage is not detected
  - dynamic frequency selection (DFS) channels should not be actively scanned
  - AP ensures there is no radar communication on a channel and then advertises it in a beacon
  - if things change, AP tells clients to stop using channel and looks for another channel

WiFi spectrum

Imperial College London



*Channels 116 and 132 are Doppler Radar channels in some cases.



Service Sets

Imperial College London

- Basic Service Set (BSS), infrastructure mode
  - AP and its hosts
  - SSID: name of the network, a string
  - BSSID: MAC of AP
- Extended SS (ESS), infrastructure mode
  - group of BSS interconnected by a distribution system (DS)
    - typically an Ethernet LAN, Wireless (WDS) also possible
  - ESSID: several APs share same SSID (possibly BSSID)
- Independent BSS (IBSS), ad-hoc mode
  - devices talk directly to each other

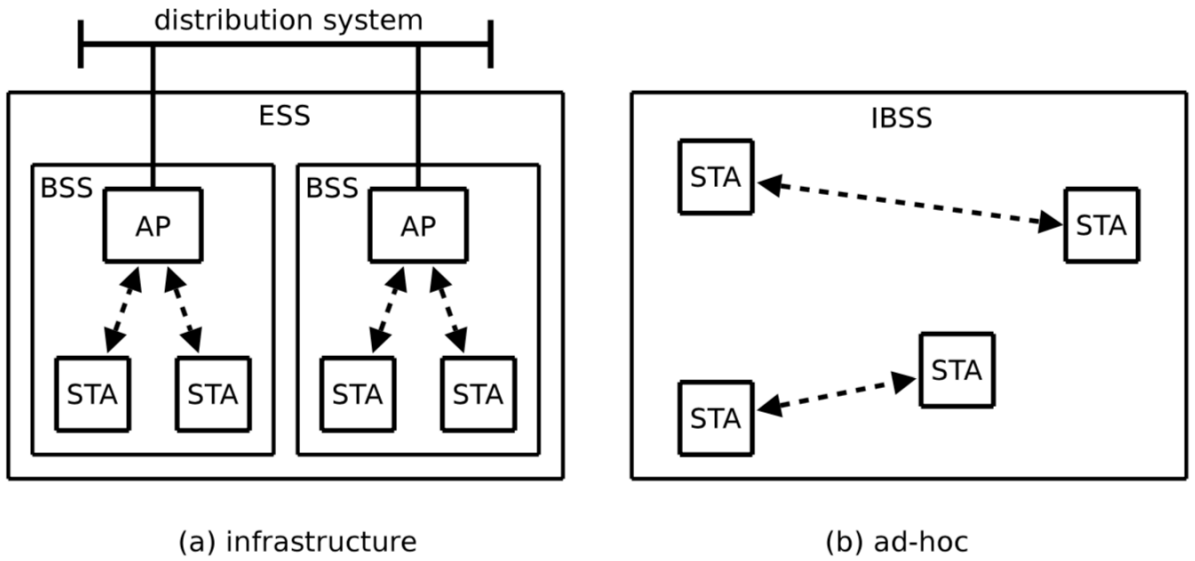
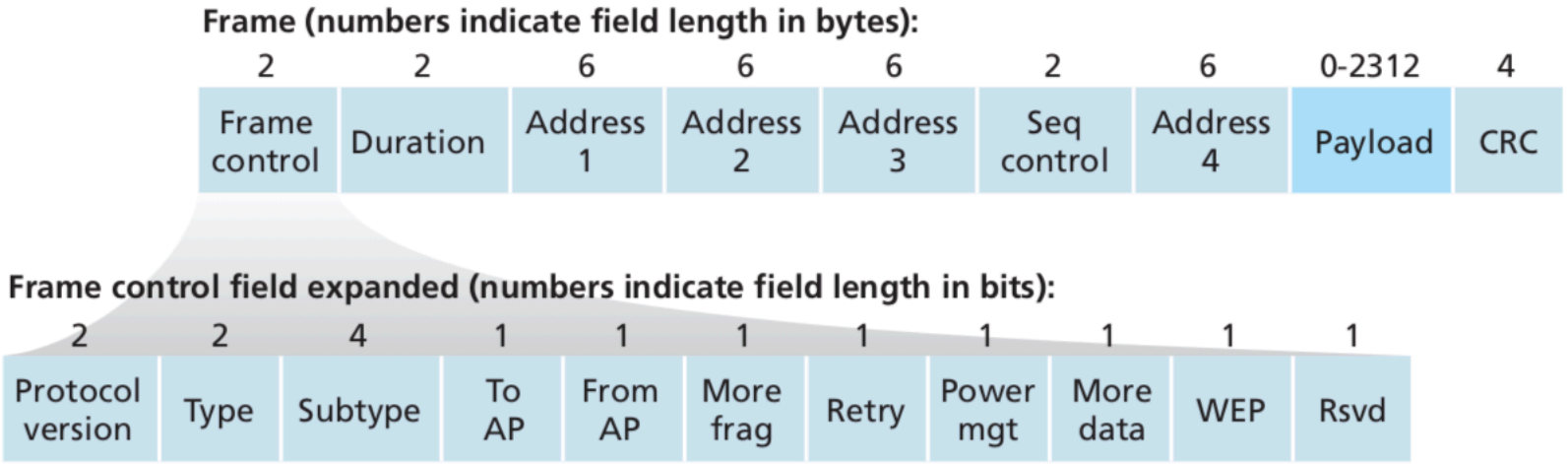


Fig. 3.2 802.11 Infrastructure Network

WiFi headers

Imperial College London

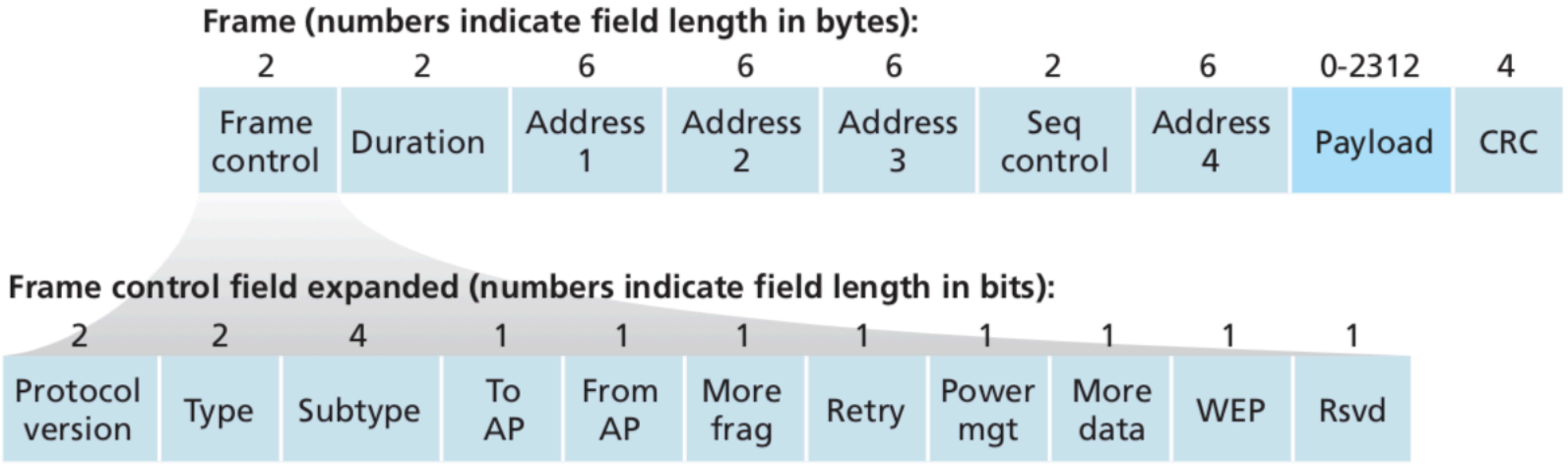
- different frames use different parts of the headers
- Duration
  - how long will it take to receive a frame, used in particular on RTS/CTS
- 3 MAC Addresses
- 1. WiFi dest
- 2. WiFi source
- 3. infrastructure network source/destination
- Seq Control
  - to handle retransmisisons
- MAC Address
  - used in ad-hoc mode to forward frames between APs and in a WDS (wireless distribution system)
- Payload
  - up to 2312B but typically up to 1500B (Ethernet data payload size)
- CRC
  - 32b, used a lot because of frequent corruption



WiFi control headers

Imperial College London

- Protocol version
- Type and Subtype: RTS,CTS,ACK, ...
- To AP/From AP: determine meaning of addresses 3,4
- More frag: in case of fragmentation, 0 for control frames
- Retry: set to 0 cor control frames, should not be retransmitted
- Power mgt
  - client sets this to tell AP it's going to sleep until next probe
  - AP buffers frames for this client
  - next AP beacon says if it has frames for the client awaiting transmission
  - if so, client can poll for the buffered messages, if not, goes back to sleep
- More data: used in management frames only, 0 in data and control
- Protected: encryption used or not
- Order: can frame be delivered out of order? (no for control frames)



WiFi main steps

Imperial College London

- client scans to find a BSS to join
  - it receives all the information necessary to join as part of this process
- client joins BSS by adopting the advertised parameters
  - and synchronising time
- client authenticates and associates to AP
  - once successful, client can send data frames, network-layer data
- client is ready to use the network
  - client sends DHCP discovery message
  - in infrastructure mode, each WiFi client has an IP visible on the "wired" network and the AP acts as a sort of router
    - AP is not transparent wrt to the client: see address 3 in WiFi frame

WiFi frame types

Imperial College London

- management frames (aka MMPDU frames)
  - used by stations to join and leave BSS
  - some subtypes
    - (Re)Association request/response
    - Probe request/response
    - Beacon
    - Disassociation
    - (De)Authentication
- control frames
  - they only have header, no payload
  - they cannot be encrypted
  - Order bit is set to 1, because order must be preserved
  - assist delivery of data
  - aquire/clear channels
  - some subtypes
    - Request to send (RTS)
    - Clear to send (CTS)
    - Acknowledgment (ACK)
- data frames
  - main purpose is to carry payload that AP gets from or puts into Ethernet frame
  - Null function frames can be used by client to signal change of Power Save status to AP
  - some subtypes
    - Data (simple data frame)
    - Null function (no data)
    - QoS Data [HCF]

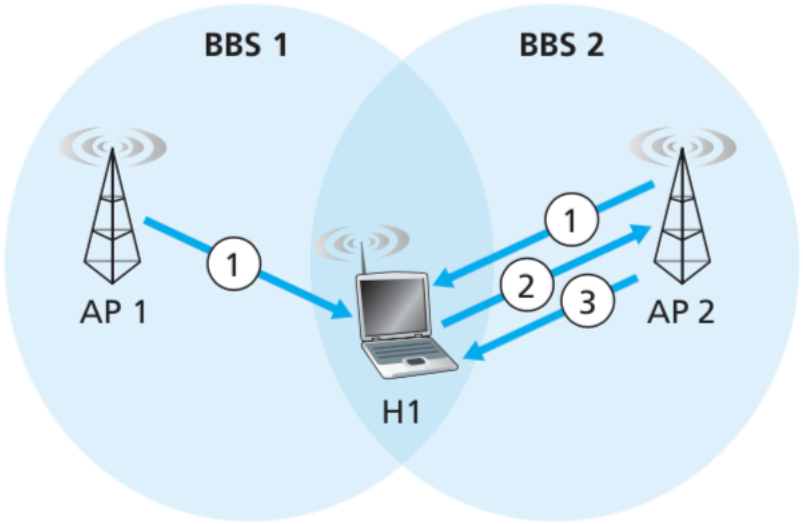
Beacon frames

Imperial College London

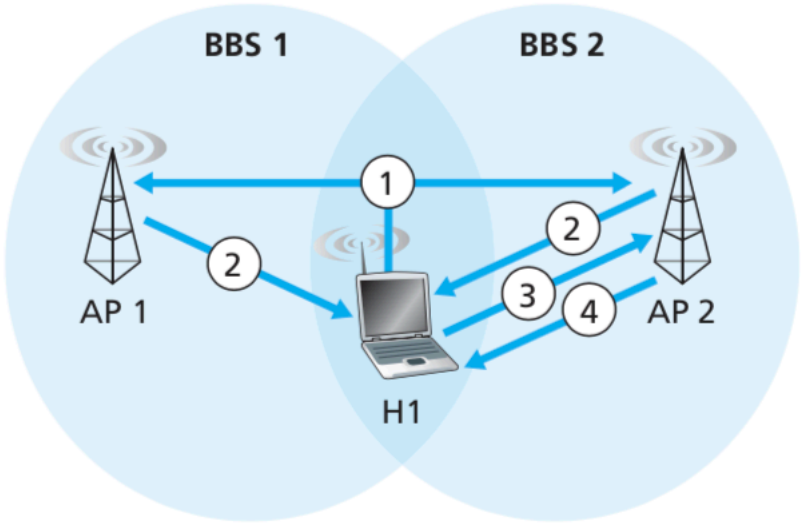
- Normally broadcasted by the AP of a BSS
- Clients only send beacons when participating to an IBSS
- Beacons contains time stamps so clients can synch their clocks wrt to AP
  - Synch is crucial because of collisions, etc
- Beacons contains necessary parameters for a client to consider joining the BSS
- Typically sent every 100ms

WiFi scanning

Imperial College London



a. **Passive scanning**
1. Beacon frames sent from APs
2. Association Request frame sent: H1 to selected AP
3. Association Response frame sent: Selected AP to H1



a. **Active scanning**
1. Probe Request frame broadcast from H1
2. Probes Response frame sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent: Selected AP to H1

Figure 6.9 ♦ Active and passive scanning for access points

Passive scanning

Imperial College London

- AP periodically sends beacon frame advertising its (B)SSID on chosen channel
- client listens for beacons on all channels
  - client could send further probe request to chosen AP if some parameters are not visible in beacon
  - in that case, server sends probe response
- how to chose what AP to associate to is not specified by the standard
  - stronger signal is one common option
  - may not be best choice if oversubscribed
- client sends association request
- AP replies with association response

Active scanning

Imperial College London

- may or may not be allowed depending on the "regulatory domain" of the BSS
- client sends probe requests on all channels
  - SSID
    - specific, for a hidden SSID
    - NULL, for any SSID
      - it's a way not to sit around and wait to receive a beacon
  - BSSID
    - probe request is the only frame that can use the broadcast BSSID FFFFFF
    - or it can use BSSID of known hidden AP
  - Destination Address (DA)
    - broadcast or MAC of AP if known
- AP replies with probe response if appropriate
- client sends association request
- AP replies with association response
- sometimes client keep periodically doing active scanning also while already associated, to be ready for mobility
- *Closed networks*
  - Network “hides” SSID to prevent privacy leaks
  - Clients have to know the SSID and use active scanning
  - But when they do, an eavesdropper can sniff it
  - So secure during the time no client connects

Association states

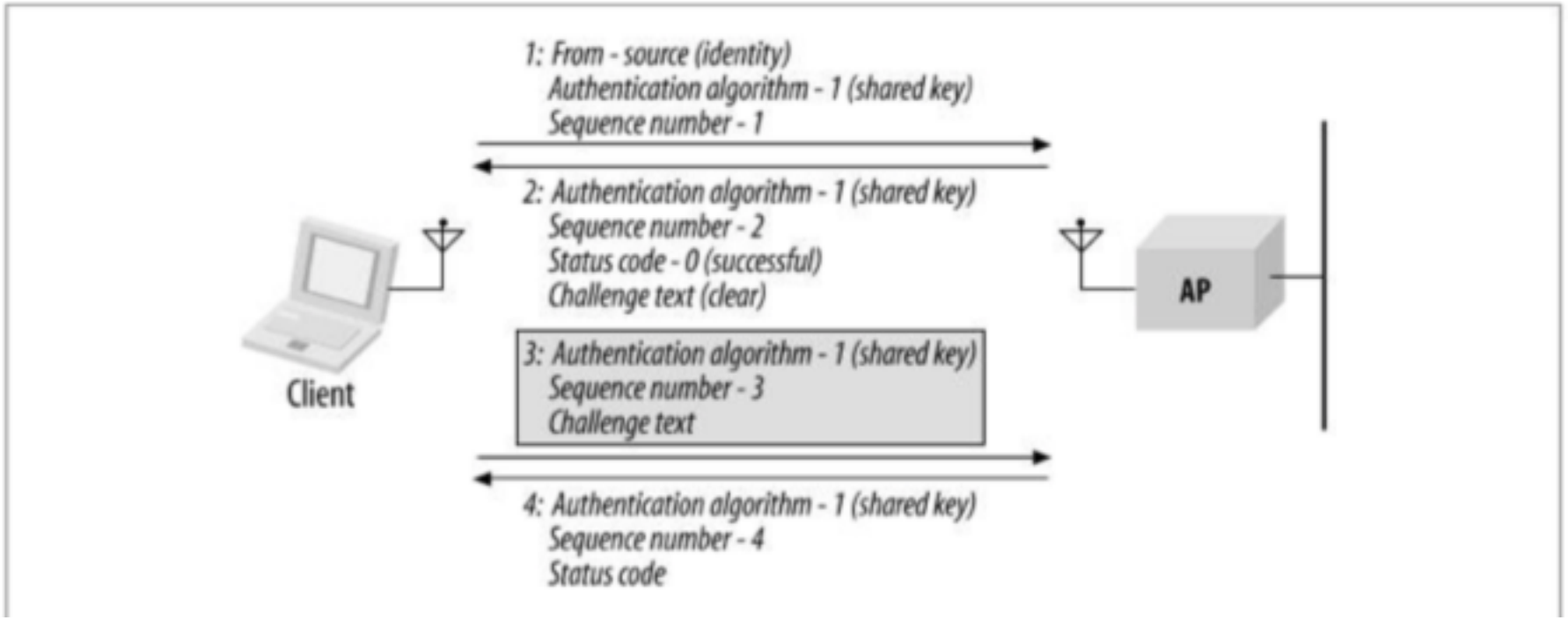
Imperial College London

- UU: unauthenticated and unassociated
  - clinet can transmit some control (FTS/CTS/ACK etc) and management frames (Probe req/res, beacon, auth/deauth, ATIM)
- AU: authenticated, unassociated
  - client can send also association-related frames
  - client can be deauthenticated
- AA: authenticated, associated
  - client can fully participated to the network
  - can be deassociated, deauthenticated

802.11 Authentication

Imperial College London

- identifies the client to the AP, not viceversa
- *open system*
  - the only method *required* by WiFi standard
  - trivial req/res exchange without any interesting parameters
  - source MAC of request taken as identity of client
- *shared-key*
  - a pre-shared key (PSK) must be manually configured on both the client and AP
  - this is not the flow for WPA/WPA2: they use a PSK after association, first they authenticate via open system



Association

Imperial College London

- used only in infrastructure mode, not in ad-hoc mode
- standard mandates that clients can be associated to one AP at most
- association is necessary to obtain full access to the network
  - helps keeping track of what client is associated to an AP, so frames for client can be routed
- after association is complete, AP must register client on the network
  - one way is to send "gratuitous" ARP message, so client MAC is associated to AP's switch port
- association steps
  - client sends association request frame
    - includes capabilities and parameters such as available transmission rates
  - server replies with
    - association response if client was already authenticated
      - containing Association ID (AID), which is used to identify the client for delivery of buffered frames when power-saving is enabled
    - other capabilities and parameters for connection
    - deauthentication frame if client was not authenticated

Disassociation

Imperial College London

- can be sent either way between AP and client
- does not need a response
  - the party that sees it should consider the association terminated
  - still an ack should be sent
- clients should send Disassociation frame before leaving AP
- APs will also terminate associations based on timeouts (in case disassociation frame was lost)

Collision avoidance

- since there is no collision detection, DATA frames are sent in full
- if sender hears nothing on the channel, awaits DIFS (distributed inter-frame sapce) interval and sends frame
- DATA frames are acknowledged at the link layer by an ACK frame
- receiver waits a SIFS (short inter-frame spacing) interval before ACKing
- if ACK does not come in due time, sender re-transmits the frame
- Seq Control header field help resolve duplicates
- optional: use of RTS/CTS frames
  - worth doing for large DATA frames only
  - AP variant: CTS-to-Self

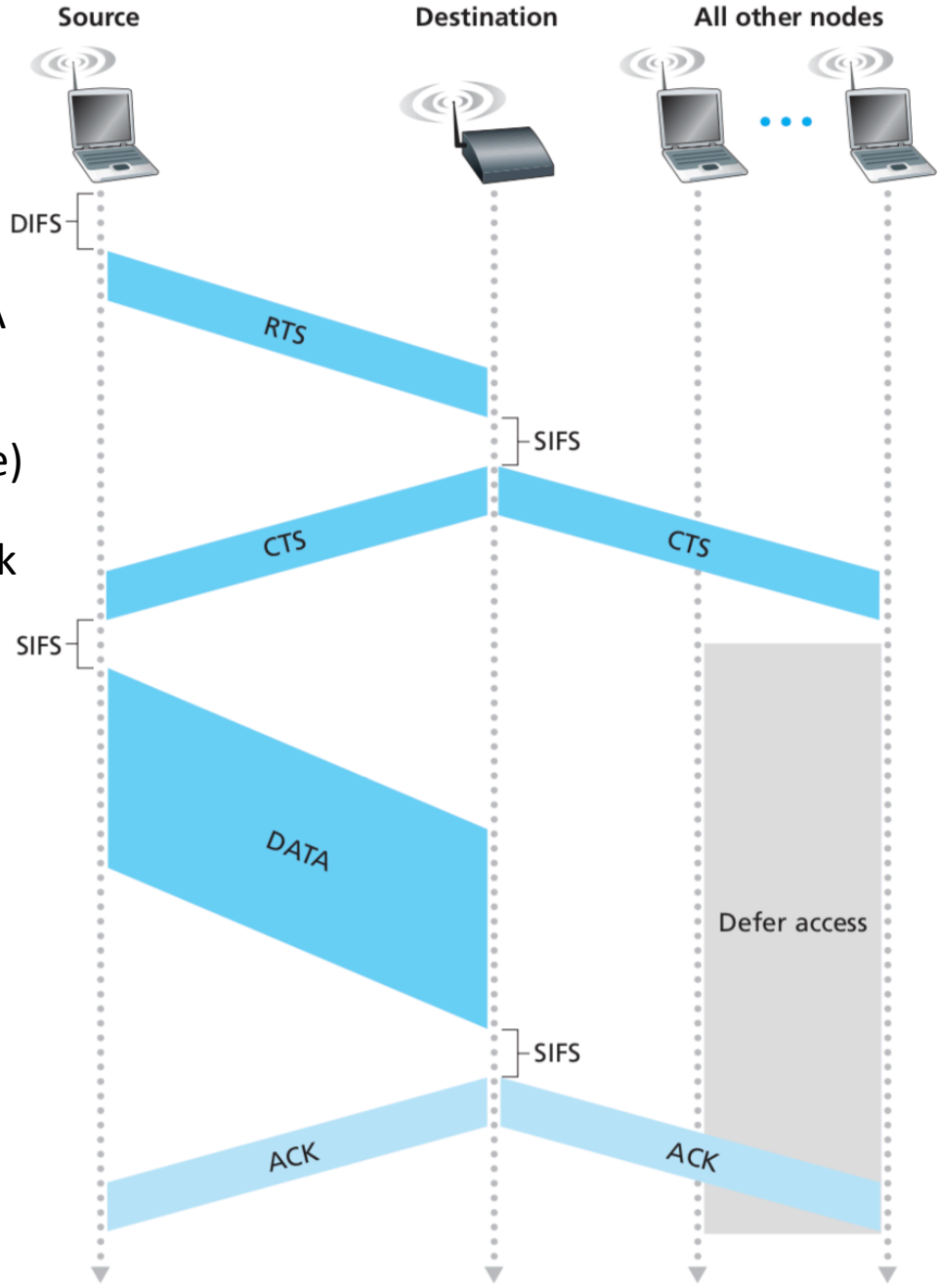
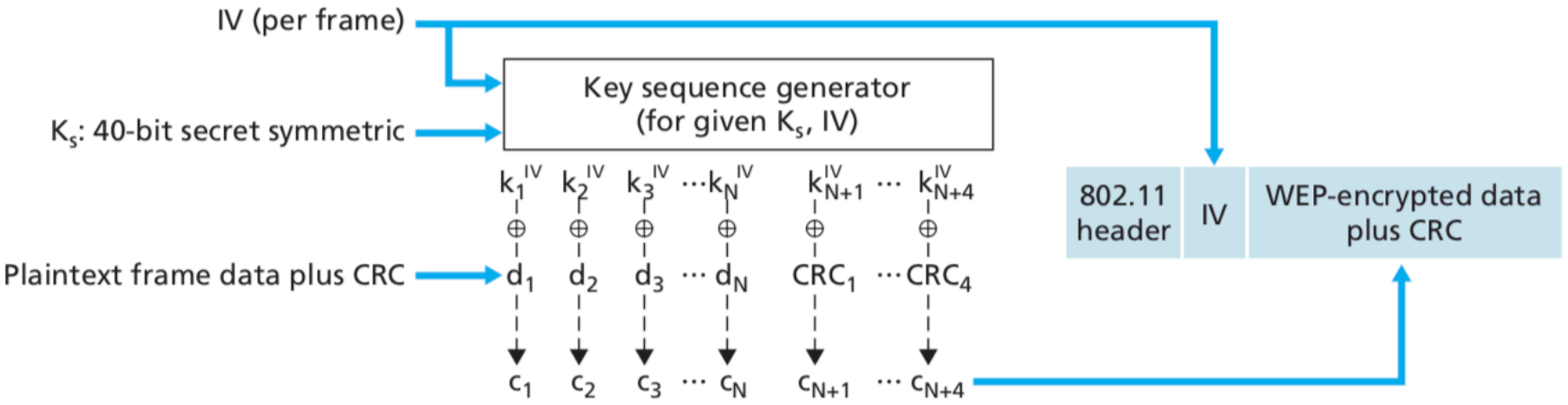


Figure 6.12 ♦ Collision avoidance using the RTS and CTS frames

WEP

Imperial College London

- based on RC4
- provides authentication and data encryption
- authentication steps
  - client and server must share a 40b or 104b symmetric key Ks in advance
  - client requests authentication like for open system, but AAI bit is 1
  - server sends cleartext 128b nonce
  - client sends nonce encrypted with Ks
  - server responds with status code
    - if access points decrypts with Ks and nonce matches, client is authenticated
- broken in many ways, mostly due to reuse of IV and weak integrity protections



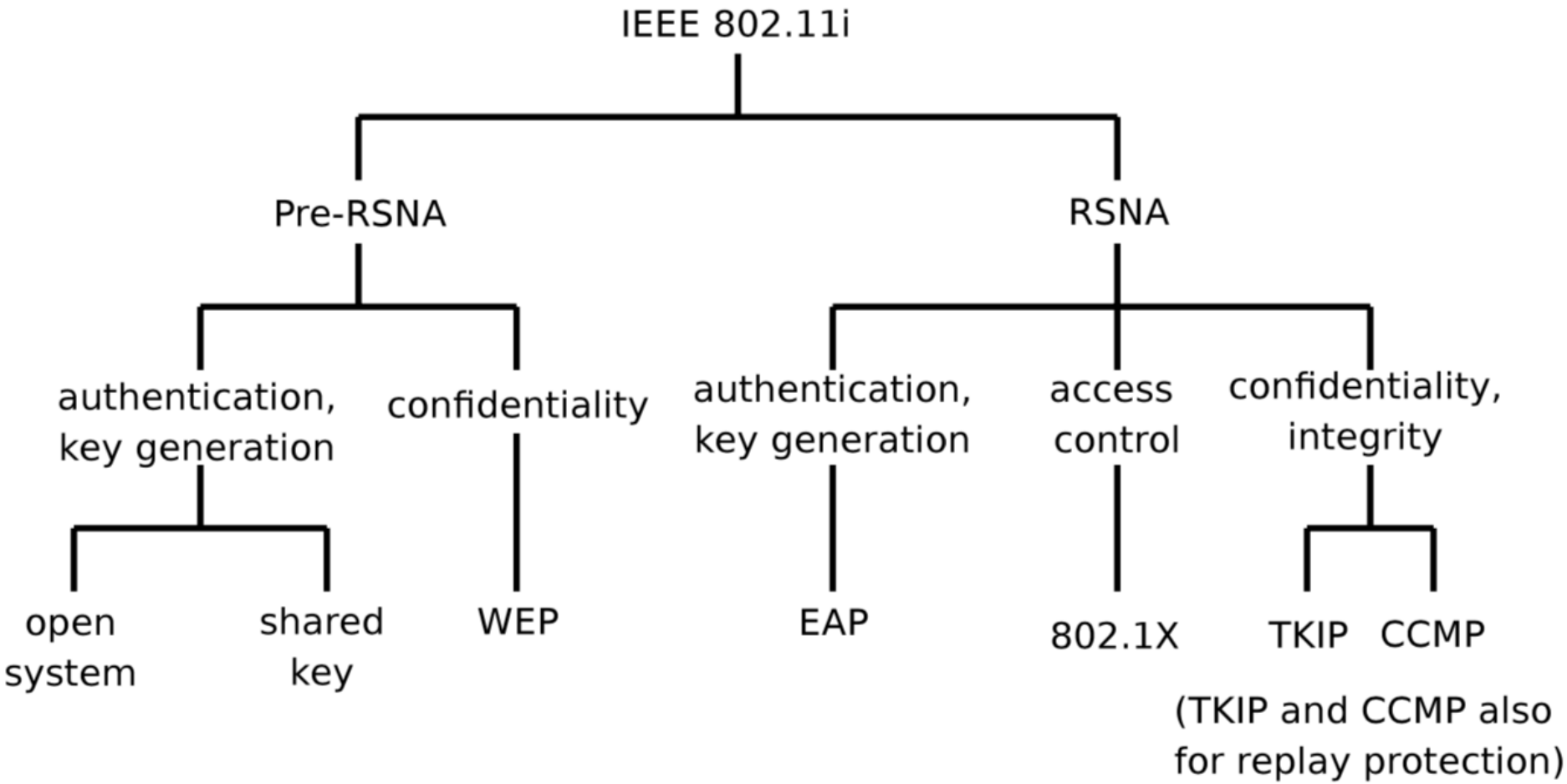
Non-standard security

Imperial College London

- MAC based authentication at the AP level
  - MAC is easy to spoof
- AP may redirect to captive portal until external form of authentication in granted
  - for example, restrict web based on IP and presence of valid SSH connection from that IP
  - AP redirects all IP packets to IP address on LAN of custom authentication portal
    - but may still allow DNS queries to go outside, so a channel for abuse

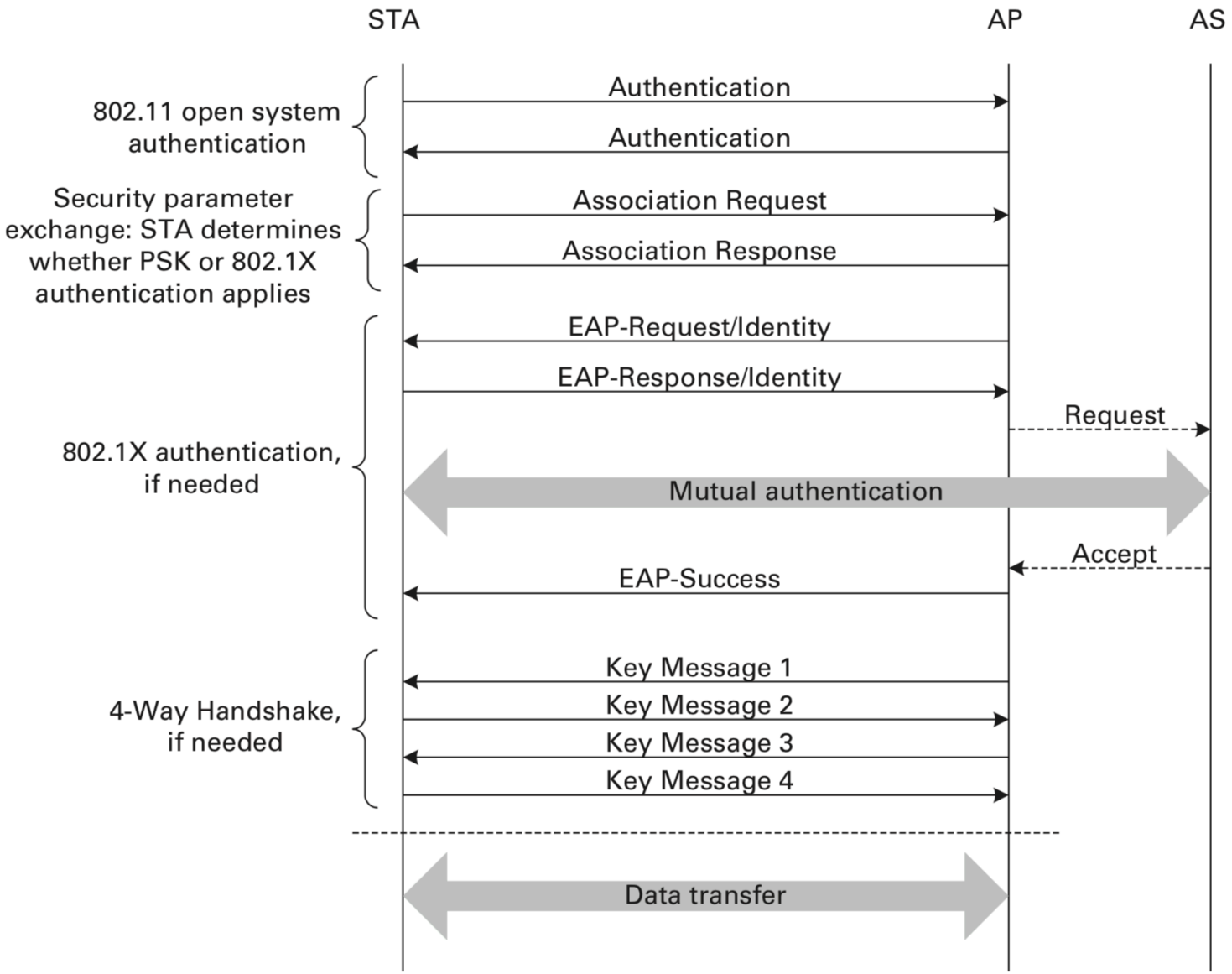
802.11i standard

Imperial College London



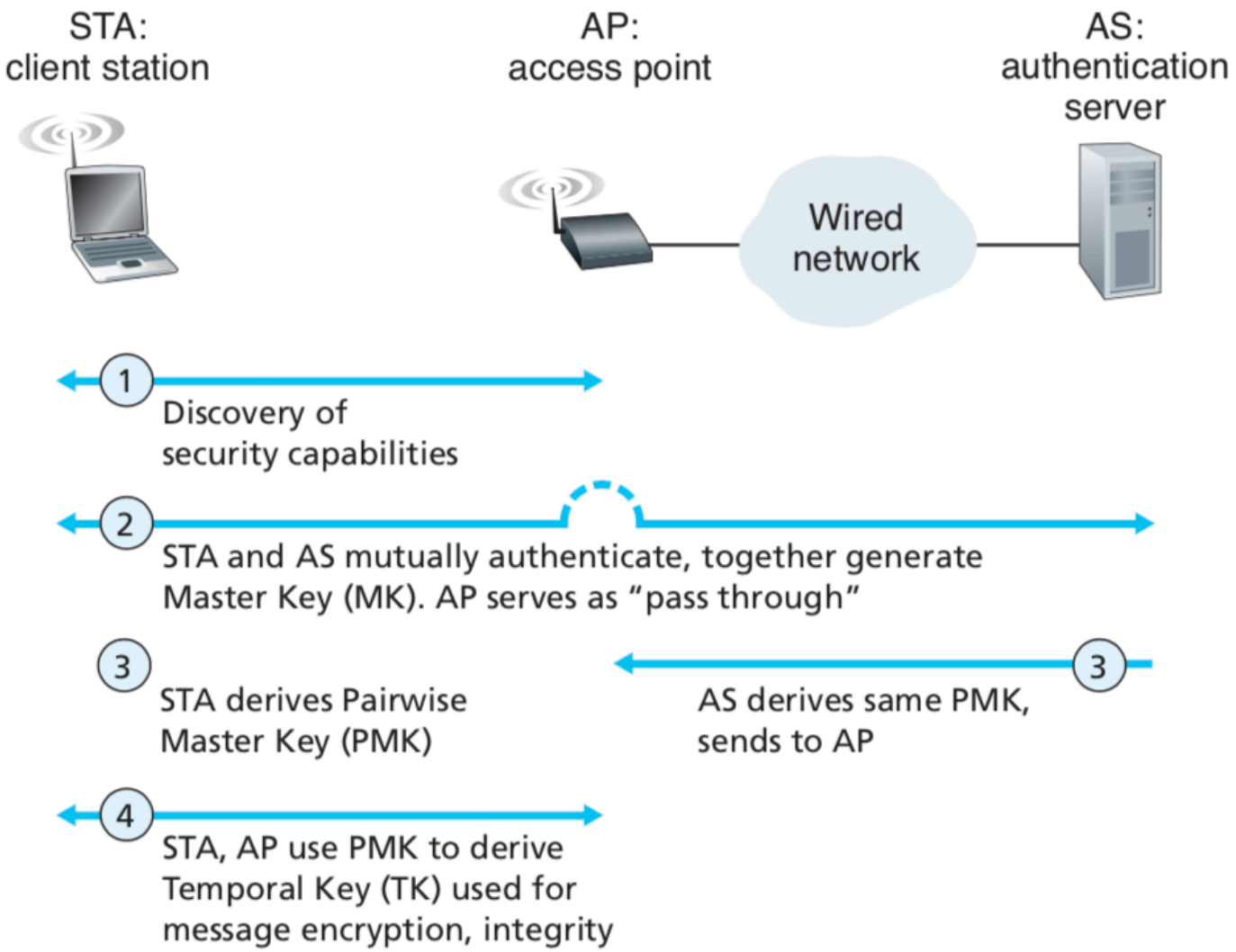
802.11i exchange

Imperial College London



802.11X main phases

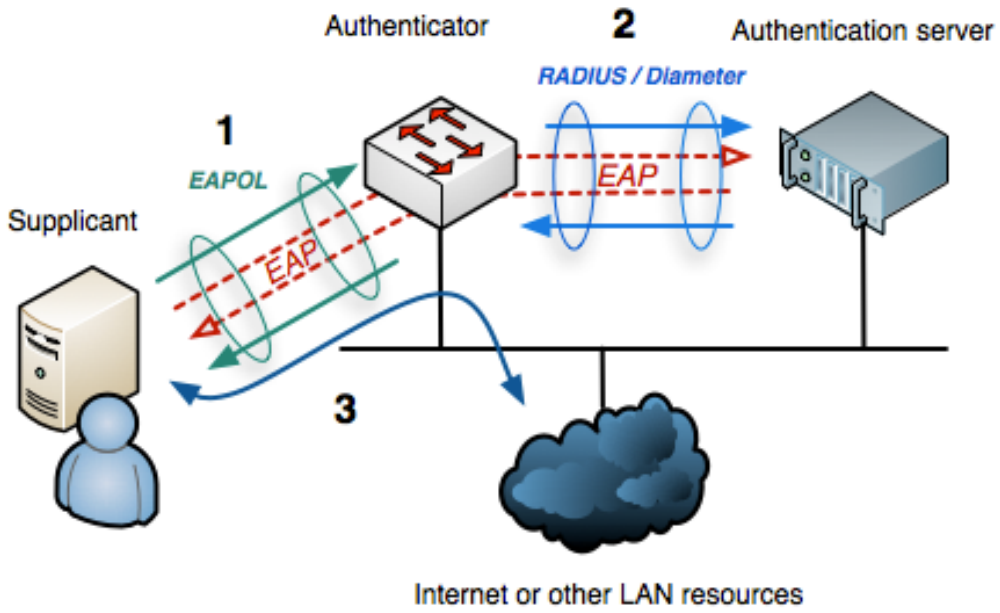
Imperial College London



802.11X

Imperial College London

- a layer-2 protocol for port-based network access control
  - allows separation of Authentication Server (AS) from AP: same AS it can be shared with other Aps
  - mutual authentication of client and AS
- client-AS authentication protected by EAP
  - EAP-PSK/TLS/TTLS/MD5, LEAP, PEAP, MSCHAPv2
  - EAP over LAN (EAPoL) is used to protect authentication on client-AP link
- the AP forwards only EAP packets at level 3 to the AS IP, until authentication is successful
- Remote Authentication Dial-In User Service (RADIUS) or DIAMETER to protect authentication on AP-AS link



PSK handshake

Imperial College London

- in this mode, PSK is used as PMK
  - keys should be changed frequently (e.g. every 24hrs)
  - pairwise transient key (PTK) protects traffic between the AP and client S
  - group transient key (GTK) protects the broadcast and multicast traffic sent by the AP
- keys are established via 4-way handshake

1. AP->S: ANonce

   S can generate PTK based on ANonce, SNonce, PMK

2. S->AP: SNonce

   AP can also generate PTK, and use it to verify MIC (a PTK-based signature), so it knows S knows PMK

3. AP->S: if needed, it contains {GTK}PTK, plus MIC so also S knows AP knows PMK

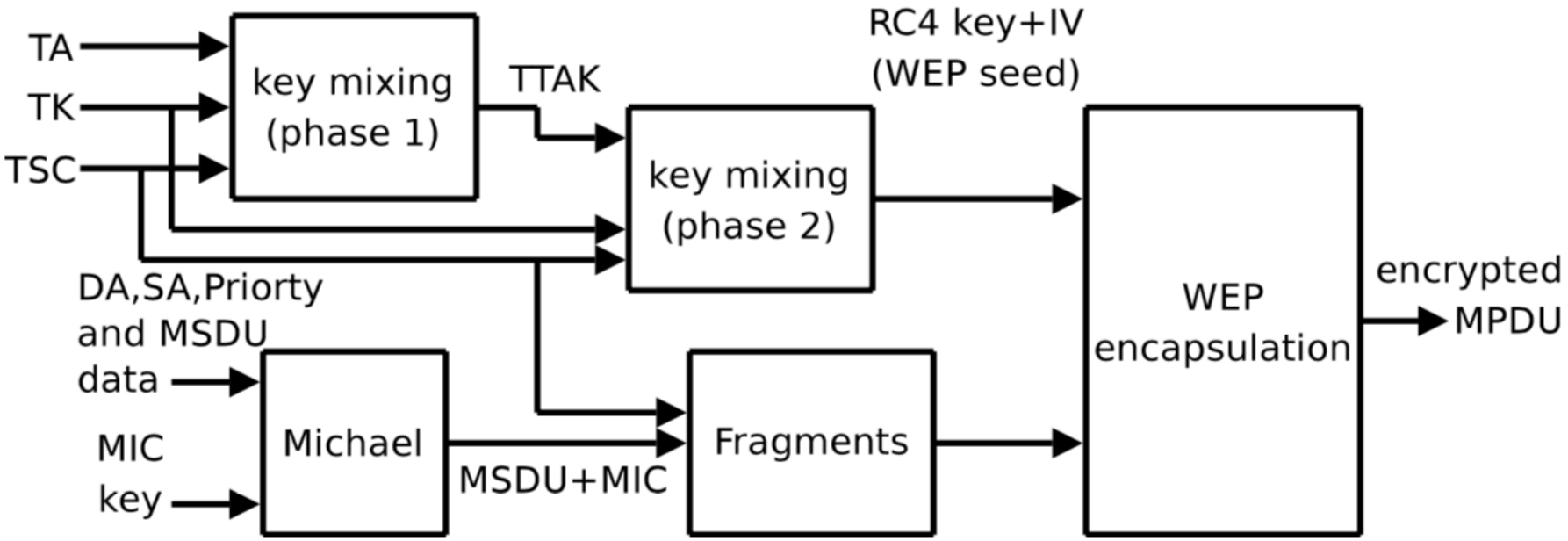
4. S->AP closes handshake

   S<->AP session is established

TKIP

Imperial College London

- Used in WPA
- Still based on RC4
  - Fixes WEP weaknesses as possible while retaining hardware compatibility
  - Not the ideal solution, still weak overall
  - Michael and some replay protection instead of CRC



CCMP

Imperial College London

- Used in WPA2
- Based on AES Counter mode for encryption and CBC-MAC for integrity
  - Proven secure using formal methods
  - Main attack is offline dictionary attack against passphrase
  - 2017 key reinstallation attack leads to resetting PN, enabling cryptoanalysis
    - Needs a channel-based MITM to replay message 3 of PMK handshake