Week 1 Class 1

- Networks connect multiple computing devices to exchange data
- There are different types, wired, wireless, optical
- We are going to focus on wireless in this class

Goals

- Understand current and emerging wireless systems from security perspective
- Insight into recent research trends in wireless sec
- Experience on steps of small research project

Terms to Know

- Symmetric cipher: Uses same key to encrypt and decrypt
- Asymmetric Cipher: Uses different key to encrypt and decrypt

Wireless Security (Research)

- in a nutshell: radio waves are broadcasted in open space and everyone can see it
    - radio waves can go through walls

Week 1 Class 2

Types of Wireless Attacks

- Passive (privacy related)
    - Intercept/Evesdrop
    - Infer (user, location, traffic)
- Active
    - Block (jamming)
    - Deceive
        - Message modification
        - Spoofing/Masquerading
        - MitM
- WPA3 is at Layer 2 and Layer 1
- The difference between physical and wireless networks are at layer 1 and 2

Cryptographic Countermeasures

- Symmetric-key cryptography

    - Encryption for confidentiality
    - Message authentication and integrity
- Public-key cryptography
    - Digital signatures for authentication
    - asymmetric encryption
- Secure hash functions
- Pseudorandom number generators
    - secret frequency hopping

Are We Still Insecure?

- Unfortunately, yes!
- Attackers are evolving too!
    - access to open source crypto
    - unexplored analysis methods
    - abuse of privacy infrastructure
    - (advanced) radio softwarization
        - decreases cost
    - Constrained devices in a highly-connected ecosystem
- More needs to be done to make the world safer

Wireless Security Research

- What is it?
    - offensive security vs defensive security
    - in research, we apply a scientific method to study/assess or design a system or protocol
- Examples
    - cryptography
    - protocol analysis
    - traffic analysis
    - formal analysis
    - testbed implementation

Above is on first quiz

Wireless Communications

Acoustic Waves

Electromagnetic Waves

- transport energy through open space, stored in propagating electric and magnetic fields

Periodic Wave

- max amplitude
- phase
- frequency
- time period
- sampling rate
- sampling interval

Wavelength

- The distance a wave travels in a time period
  - Depends on propagation speed
  - For EM waves
    - c = 3*10^8 m/s speed of light
    - f = 1/T frequecy
    - lamda = c/f (meters) wavelength

Wireless Channel

- An open, shared medium for signal propagation
  - Broadcast nature → noise, ,interference, cogestion
  - Easier for eavesdropping, jamming, etc.
- Simplified mathematical representation: y = hx + n
  - y = recieved signal
  - x = transmitted signal
  - n = noise
  - h = channel

Signals and Channel Representation

- Each signal has an amplitde and a phase
  - complex numbers have an amplitude and a phase, too
  - So, it is natural - and easier - to use a complex number to represent a symbol/signal (x) or a channel (h)
- Symbols: Short signals to convey digital bits
  - different symbols have different waveforms (e.g, phases)

Week 2 Class 1

Review of last week

- Physical layer between wire and wireless are different

Digital Modulation

- map input digital bits to analog symbols
    - modulation alaphabet: a finite set of distict symbols
    - demodulation: find bits corresponding to recieved symbols
- Basic digital modulation methods
    - amplitude shift keying (ASK)
    - Frequency Shift Keying (FSK)
    - Phase Shift Keying (PSK)
    - Quadrature Amplitude MModulation (QAM)
        - combines ASK and PSK

Constellation Diagram

- a representation of ASK and PSK symbols on a 2D diagram in the complex plane
    - it shows amplitude and phase of a symbol

Symbol (Baud) Rate

- m distinct symbols can represent log2(m) bits
    - for example to represent 4 bits we need 2^4 = 16 symbols
    - m is modulation order
- symbol rate of n:n possible changes per second
    - m and n determine the transmission (bit) rate
    - ex. assume symbol rate is 100 symbols/second and modulation order is 32 what is the bit rate?
        - 100 * log2(32) = 500 bits

Signal in Time/ Frequency Domain

- A signal may be composed of multiple waves, each with a different frequency (and phase/amplitude)
    - It can be used to send multiple symbols simultaneously

Fourier Transform (FT)

- To represent (express) a time-domain signal v(t) based on its frequency components

OFDM

- Orthogonal Frequency Division Multiplexing
    - widely used in nearly all modern systems
    - carefully selects frequency components of a signal
        - ex. use only the frequencies that are multiple of f1

        - subcarriers = frequency components
        - orthogonal subcarriers

Noise and SNR

- Noise: undesired random energy that degrades the signal's quality at Rx
- SNR: Signal-to-Noise Ratio
    - measured in dB
- Interference: Energy coming from other transmissions
    - SINR: Signal-to-interference-plus-noise ratio
    - Interntional vs. Unintentional

dBm

- dBm is the dB value when referenced to P0 = 1mw

Wireless Channel - Definitions

- Channel bandwidth
    - the width of the set of frequencies used to create a signal
    - example: 100 kHz, 5MHz, etc.
    - It is different from bandwidth (Data rate) in computing
- Channel cpacity
    - theoretical upper-bound on the data rate over a band width B
    - When noise is additive white Gaussian (AWGN)

QAM Order vs. SINR

- recall c = B * log2(1 + SINR)

Wireless DoS

- RF jamming 9 or intentional interference (Physical Layer)
    - Maliciously reduce channel capacity
    - Constant / Persistent jamming
        - signal generators, magnetrons
    - Random jamming
    - Selective/Reactive jamming
        - Jam only when a particular transmission is detected
- Flooding (deceptive jamming) (Layer 2)
    - Disassociation attacks in Wi-Fi

Week 2 Class 2

- Quiz next week
    - Equation on dB and dBm
    - Know concepts

EM Wave Phenomena over Channel

- Gain / Loss
    - Shadowing
    - Absorption
- Multi-path Distortion
    - Reflection
    - Scattering
    - Differaction
    - Refraction
- Doppler Fading (mobility)

Line of Sight

- A straight line from the Tx antenna to that of the Rx
- Non-Line-of-Sight
    - No visual LOS betweeen Tx and Rx

Free-Space Path Loss

- Attenuation of EM energy from the Tx to the Rx over the obstacle-free space (LOS channel)
- The wider the propagation area, the less power will be received by a single antenna
- Free-space path loss (sphere wavefront case)

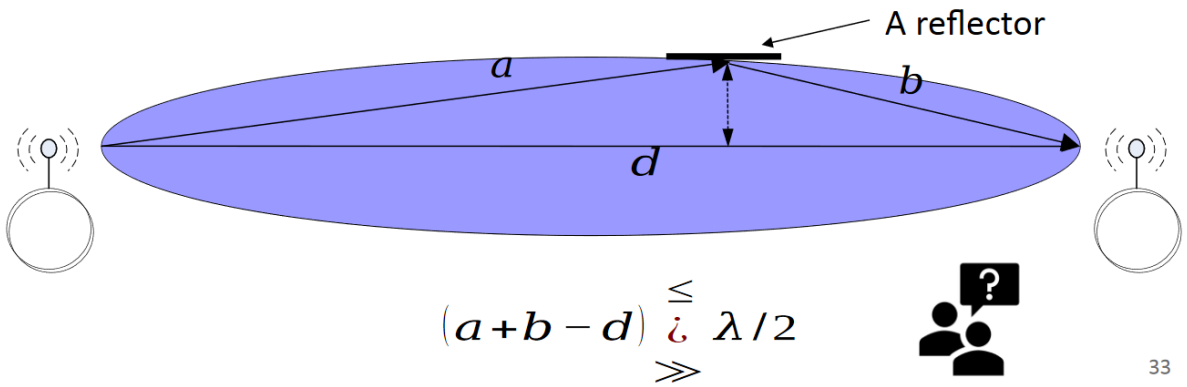
Signal Superposition - Concept

- When two signals arrive (almost) at the same time, they superpose on each other
    - We say the two signals interfere -- or collide
    - The superposed (combined) signal may look very different than the individual ones
- Its kind of like sound waves, they can combine to be stronger if they line up correctly but for the most part they collide and destroy each other
- This can be intentional (jamming) or unintentional

Multipath Propagation and Fading

- In case of signal reflections
    - constructive vs. destructive interference (fading)
    - depends on how far the reflection object is (a+b) and lamda/2

- in phase vs. out of phase

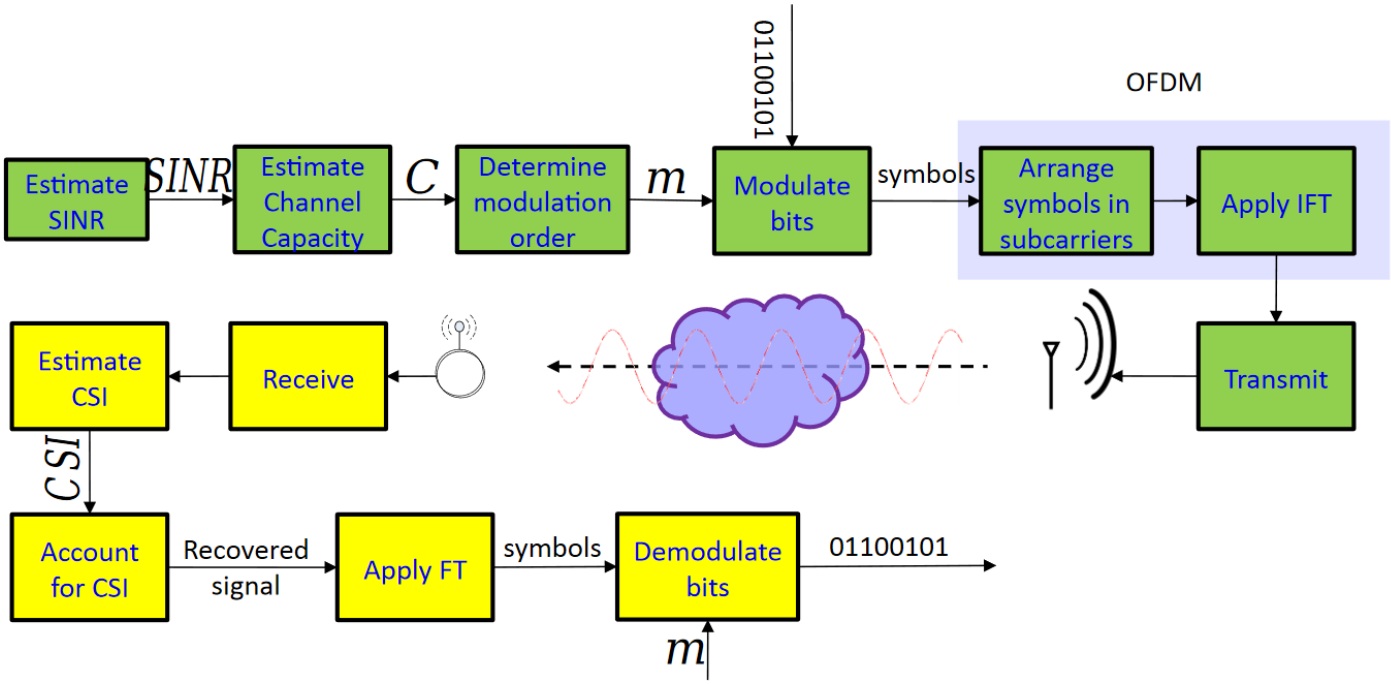


Multi-Path Channel-Mitigations

- Mitigating multi-path fading at the Rx
  - Estimate and account for LOS and NLOS channel components to recover the original symbol
  - Channel State Information (CSI): a representation of the multi-path channel
- Mitigating inter-symbol interference (ISI)
  - 1. OFDM - details not discussed here
  - 2. Spread Spectrum (SS) techniques (discussed later)

schematic View of PHY - layer

- Putting all together



- This process isnt perfect, things can go wrong

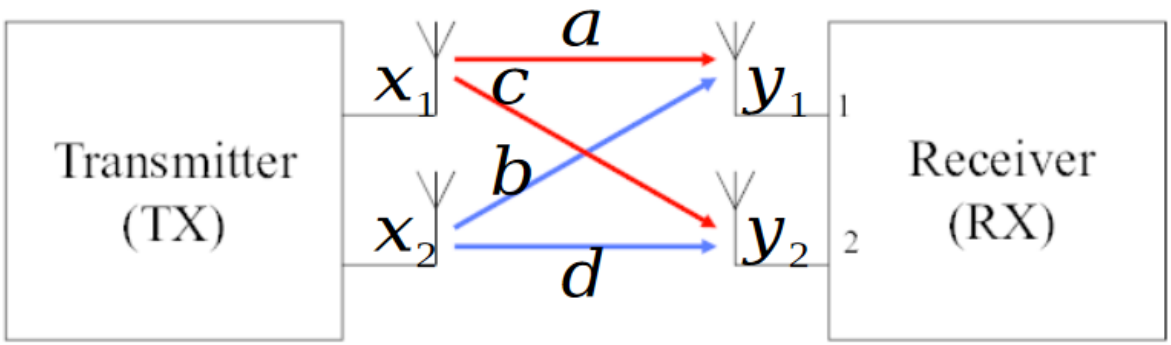
MIMO

- So far we assumed SISO system

    - single input, single output
- Tx, Rx, or both can be equipped with multiple antennas
    - Multiple-Input Multiple-Output
        - MISO, SIMO, MIMO
    - Multiple antennas can improve SNR, transmission rate, transmission security, etc.

MIMO Channel

- SISO channel model
    - y = hx + n
- MIMO channel model
    - Y = HX + N
    - p transmit antennas and q receive antennas
- Example MIMO System:



-

A PHY-Layer Approach to Security

- A paradigm to exploit features and mechanisms at the PHY layer to launch or mitigate attacks
    - Not everything can be protected by upper-layer security mechanisms!
    - PHY/MAC headers, RSS value, operating frequency, channel coefficients, hardware features, etc. are unprotected!
- PHY-layer security can complement upper-layers' approached
    - examples: friendly jamming, hardware fingerprints, uniqueness of wireless channel, hiding data in noise,...

Possible PHY-Layer Attacks

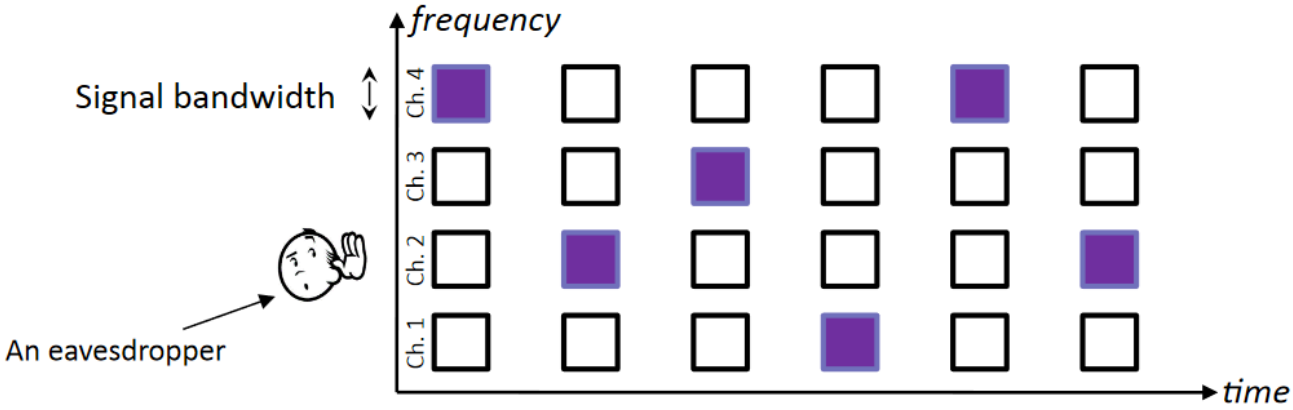
- Eavesdropping on open medium - sniffing
- RF jamming (reduce transmission rate)
- Unintentional EM emanating
    - TEMPEST
- Privacy violation
    - multipath channel coefficients - location characterization
- Modulation classification

Mechanisms/Applications

- Spread spectrum (frequency hopping)
- Authentication
  - Device fingerprints, channel characteristics, watermarking
- Traffic/Transmission attribute obfuscation
  - Header (full-frame) encryption, modulation obfuscation
- Covert communications in noise
- Key generation
  - the channel tends to be unique → Source of randomness

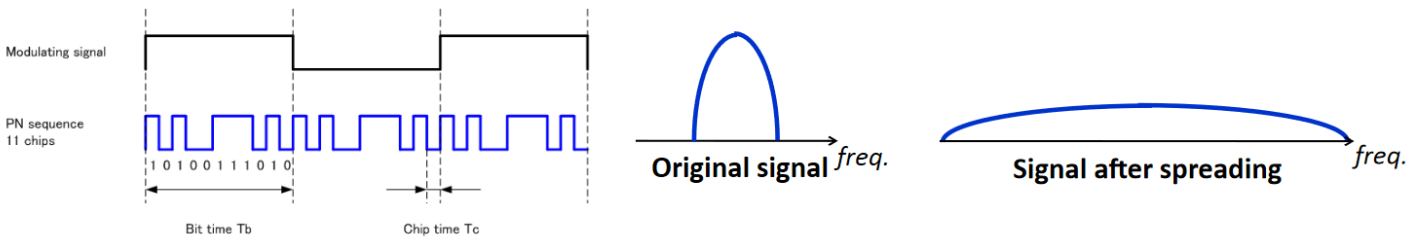
Frequency Hopping SS (FHSS)

- Continuously change transmission frequency
  - Anti-jamming - only if a subset of channels are jammed
    - Also, mitigates narrow-band interference or eavesdropping
  - It can mitigate ISI too: transmissions on a feq are spaced
  - But, requires wide/high total bandwidth and maybe a secret hopping pattern



Direct Sequence SS

- Each bit is converted to a compact bit sequence using orthogonal spreading sequence
  - If we use FT, we observe the signal bandwith is spread



  - The Rx uses the same spreading sequence to recover the bit
  - Increases resistence to ISI, interderence and eavesdropping
  - Anti-jamming/eavesdropping if spreading sequence is secret

Orthogonal Spreading Sequences

- An Rx uses this specific sequence to
    - detect and synchronize with the transmitted signal
    - eliminate a delayed copy of a spread signal, and
    - Cancel out uncorrelated noise and interference

Week 3 Class 1

Wi-Fi 802.11

- Defines MAC and PHY for a wireless (WLAN)
- First adopted in 1997 by IEEE
    - > 42 variations since then
- Address the following key issues
    - Coordination of devices within a WLAN and their mobility
    - Privacy and security of the user and its data

Infra Basic Service Set

- BSS with an Access Point (AP)
    - AP connects wireless and wired networks
    - Basic Service Set Identifier (BSSID)
        - BSSID = AP's MAC Address
- Extended Service Set (ESS)
    - Service Set Identifier (SSID/ESSID)
- Distribution System
    - connects multiple APs, increasing coverage

AP Beacon

- Broadcast every 10-100 ms by the AP
- Includes
    - Timestamp
    - SSID
    - Supported data rates (modulation and coding schemes)
    - Currect channel number
    - Supported security protocols

802.11 Medium Access Control (MAC)

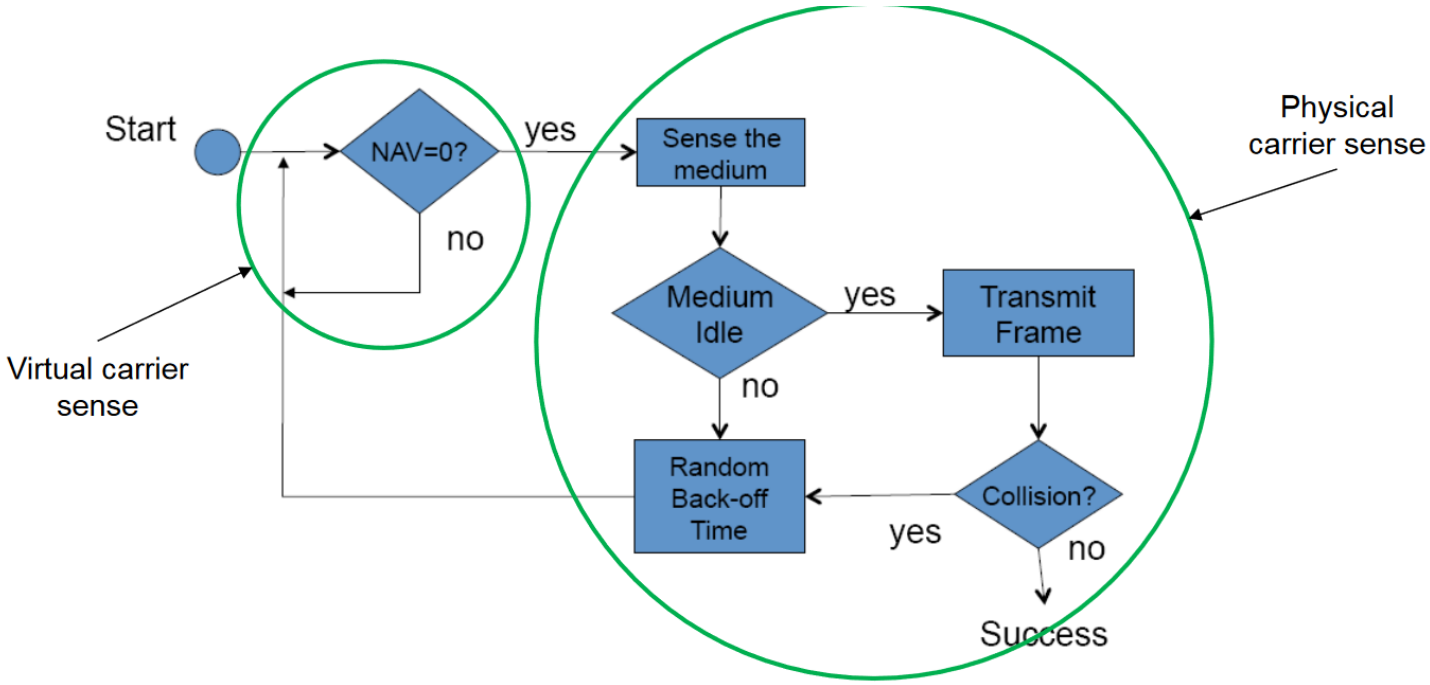
- Distributed Coordination Function (DCF)
    - For asynchronous data service (best effort service)

    - Nodes (including AP) contend for access to medium
- Point Coordination Function (PCF) (optional)
    - For time-bounded service
    - Polling from AP
- Hybrid Coordination Function (HCF)
    - Traffic categories priorities

Distributed Coordination: CSMA/CA

- Carrier Sense Multiple Access (CSMA) with Collision Avoidance
- Collision avoidance methods
    - Physical carrier sense
        - Checks if RSS (Received Signal Strength) is above a threshold
    - Virtual carrier sense
        - Wait for the duration another Tx "announced" it will be active
    - RTS (Request To Send) / CTS (Clear To Send) mode
        - explicit channel reservation

CSMA/CA Algorithm



- NAV: The remaining duration fo others' transmissions

CSMA/CA Data and ACK

- Sender (physical carrier sense)
    - If channel idle for DIFS*: transmit entire data e
        - If later on collision detected: increase backoff time next time
    - If channel bust: backoff

- Receiver
  - If received OK, return ACK after SIFS

Evolution of Wi-Fi

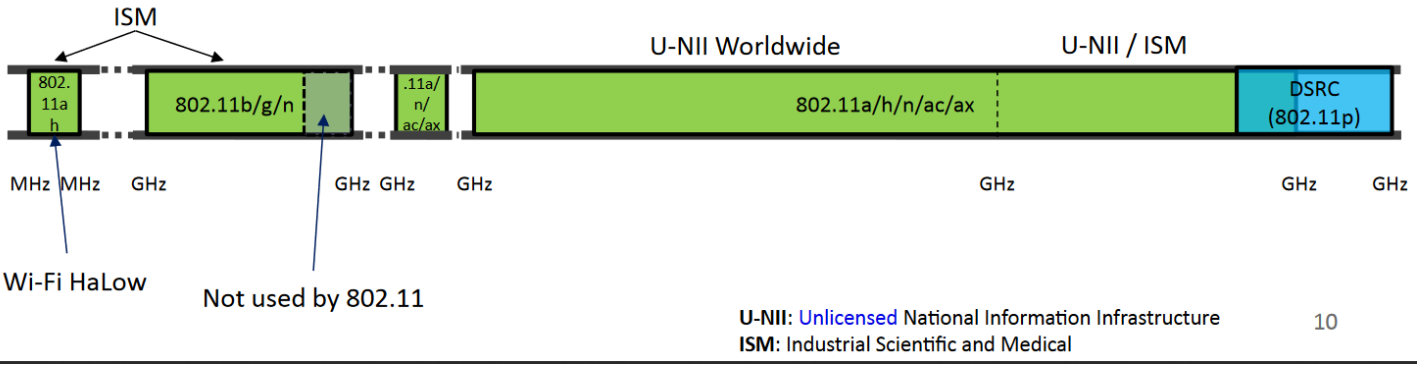
	802.11*	802.11b	802.11a	802.11g	802.11n	802.11ac	802.11ax
Year	1997	1999	1999	2003	2009	2013–16	Feb. 2021 ᴹ
Name		Wi-Fi 1	Wi-Fi 2	Wi-Fi 3	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6
Frequency (GHz)	2.4	2.4	5	2.4	2.4 & 5	5	1–7
Bandwidth (MHz)	22	22	5/10/20	5/10/20	20/40	20/40/80/160	20/40/80/160
Max Data Rate (Mbps)	2	11	54	54	Up to 600	Up to 7,000	Up to 10,530
Modulation	FHSS/ DSSS	DSSS w/ CCK	OFDM	OFDM/ DSSS	MIMO-OFDM	MU-MIMO/ OFDM	MU-MIMO/ OFDMA

*Obsolete (removed)

CCK: Complementary code keying

Wi-Fi Frequency Bands

- Supported channel bandwidths
  - 10 (.11a), 20, 40, 80 and 160 MHz
- Radio frequency range (spectrum):
  - As per FCC "New Rules" (2015)



802.11n (2009) - Wi-Fi 4

- Frequency bands: 2.4 GHz and 5GHz
  - 20 and 40 MHz channels
- Achieves high throughput using MIMO-OFDM
  - 48 subcarriers per bandwidth
  - Up to 4 antennas (2×2 MIMO up to 270 Mbps)
- Access mode: Hybrid Coordination Function (HCF)
  - Extension of DCF and PCF

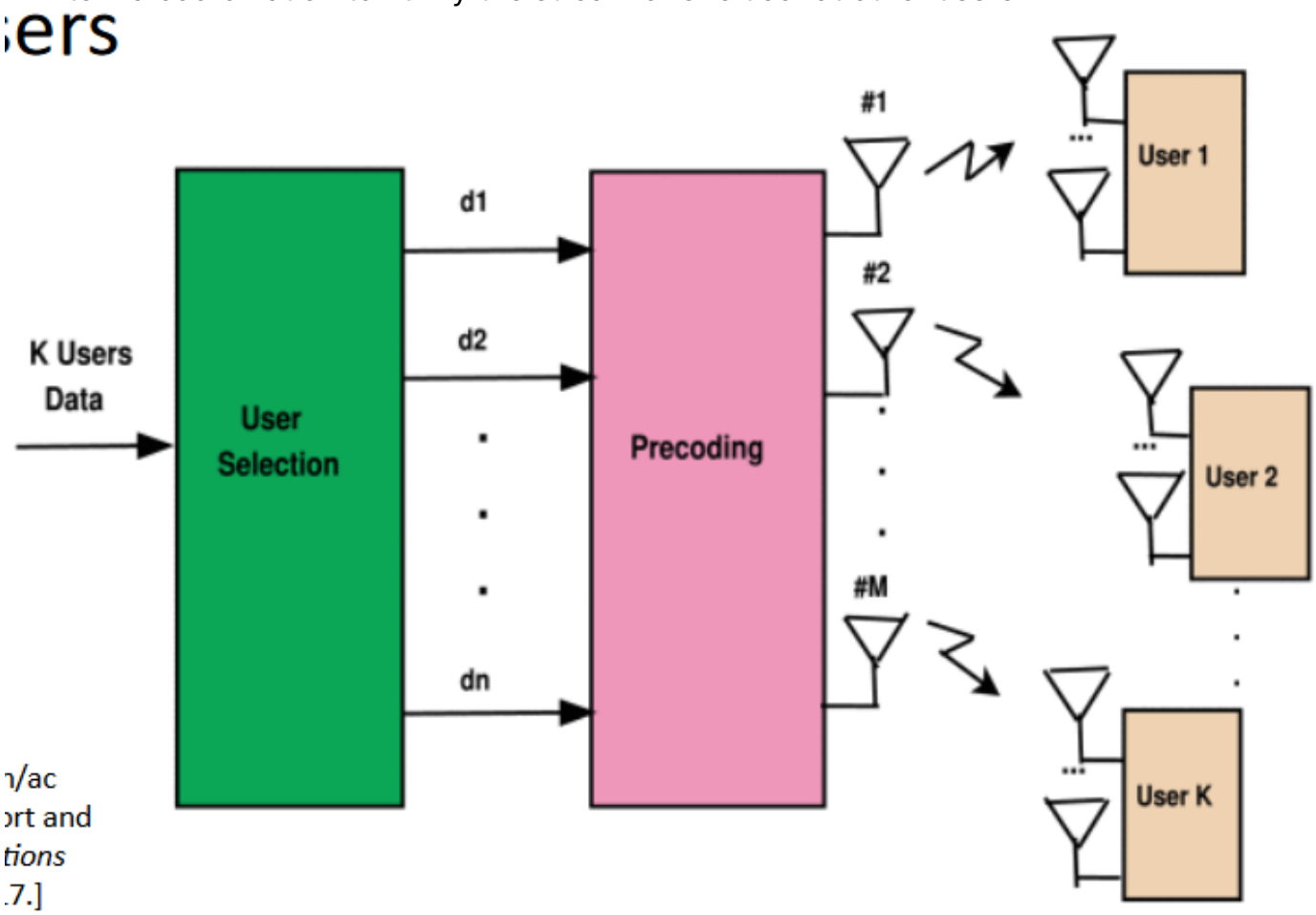
    - Different priority levels for voice, video, background and best-effort data services
- Other features
    - Beam forming using MIMO
    - Channel bonding (combining 20 MHz channels, creating 40 MHz ones)
    - HT-mixed mode
        - Backwards compatible
    - Greenfield Mode (for n devices only)

802.11ac (2013) - Wi-Fi 5

- Very High Throughput (VHT) WLAN
- 5 GHz only
- Extended channel bonding
    - Mandatory 80 MHz and option 160 MHz
- 256 QAM (up from 64 QAM in 802.11n)

Multi-User MIMO (MU - MIMO)

- One transmitting MIMO device, multiple MIMO receivers (users) simultaneously
  - Antenna coordination to nullify the stream of one user at other users



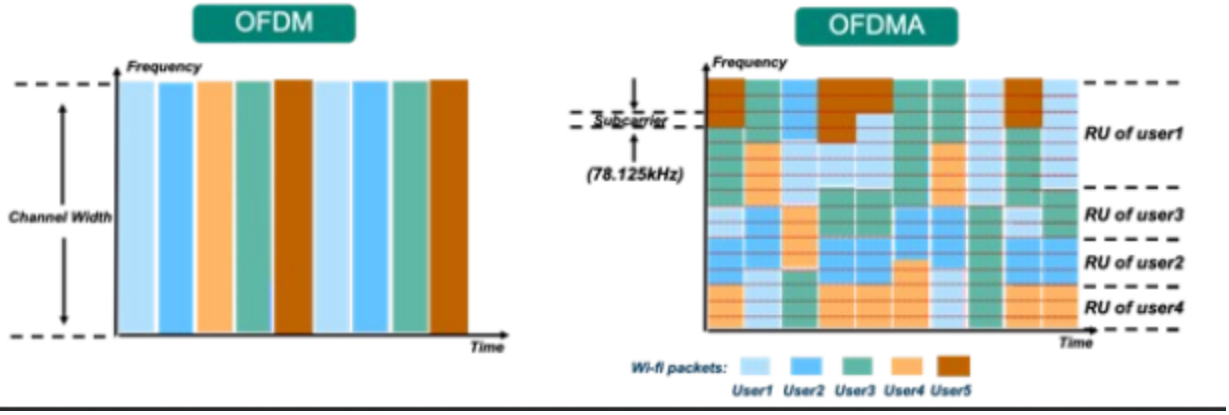
802.11ac - Wave 2 (2016)

- MU-MIMO

    - Up to four downlink clients
- More antennas for up to eight spatial streams (vs. up to four in 802.11n)
    - Explicit CSI feedback for better antenna coordination
    - In practice, Wave 2 devices only have 4 antennas
- Support for more 5 GHz channels

802.11ax (2021) - Wi-Fi 6

- Technical name: High Efficiency WLAN (HEW)
    - GHz band, whatever allowed to use
        - Wi-Fi 6E: Wi-Fi 6 Extended to the 6GHz band
    - Wake time scheduling (for power savings)
    - Multi-user MIMO in both downlinks and uplink
- OFDMA (Orthogonal FD Multiple Access)
  - Time-frequency resource units (RUs)
  - Per user RUs



- Data rate: up to 11 Gbps
    - Supports 1024-QAM (Higher than 256-QAM in 802.11ac)
- Spatial frequency reuse
    - Dynamically adjusting transmit power and signal detetion threshold for simultaneous transmissions
- 802.11be (Wi-Fi 7)
    - Extremely High Throughput (EHT)
    - Currently at its early development stages, targeting 2024
    - 320 MHz bandwidth? 16 spatial streams/ MIMO

Week 3 Class 2

Wi-Fi Security Protocols

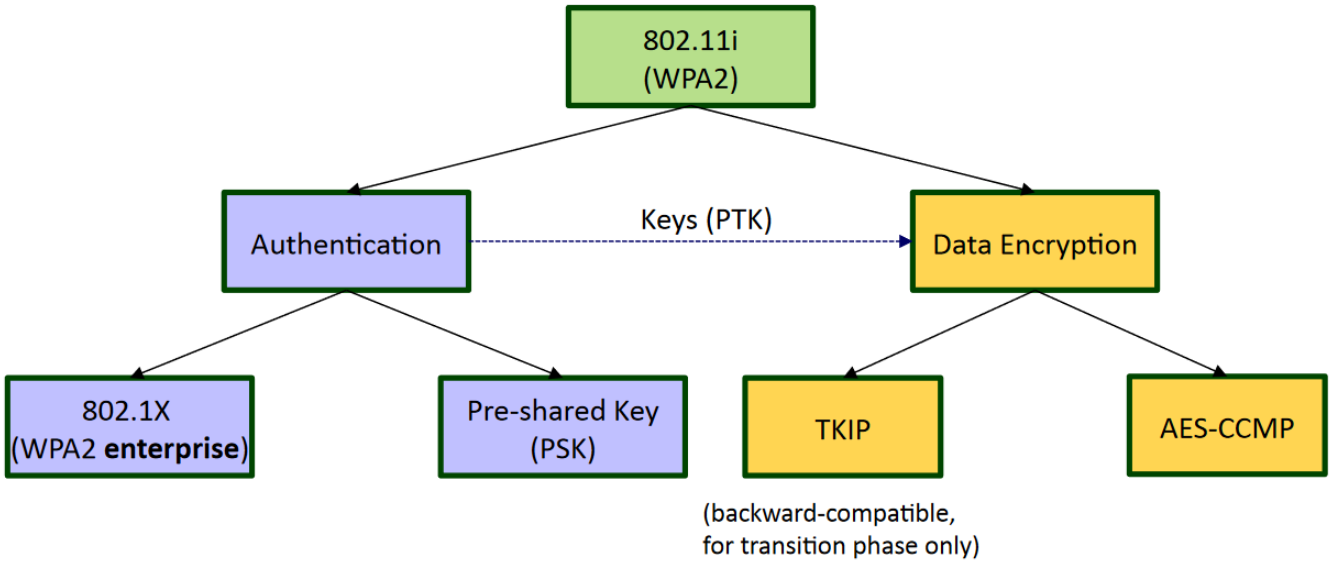
Timeline

- 1999: Wired Equivalent Privacy (WEP)

    - 2000 first weakness
    - 2004 derecated
    - 2020 obsolete
- 2004 802.11i (WPA2)
    - 2012 WPA (TKIP- only) deprecated

WPA2 in a nutshell

- Wi-Fi Protected Access II



Joining WLAN - Initiation

1. Probing (scanning) to find an AP
    - Active scanning
        - Prob request/response frames
    - Passive Scanning
        - Listen for beacon frames
2. Auth - default mode in WPA2: open
    - Auth request/response frames
3. Association: AP and stations swap info
    - Association request/response frames
    - Transmit rates, cipher suite, MAC addresses, etc.

IEEE 802.1X

- Auth for IEEE 802-based WLANs
    - Flexible, mature, scalable, and interoperable framework
        - Not an auth method
        - Requires deploying a server (not always possible)
    - Prevents unauth access to layer 2 (port-based)
    - User-specific key and user-based authentication

- Roles
    - Supplicant - the visitor (laptop)
    - Authenticator - the gate keeper (AP)
    - Authentication server - the decision maker

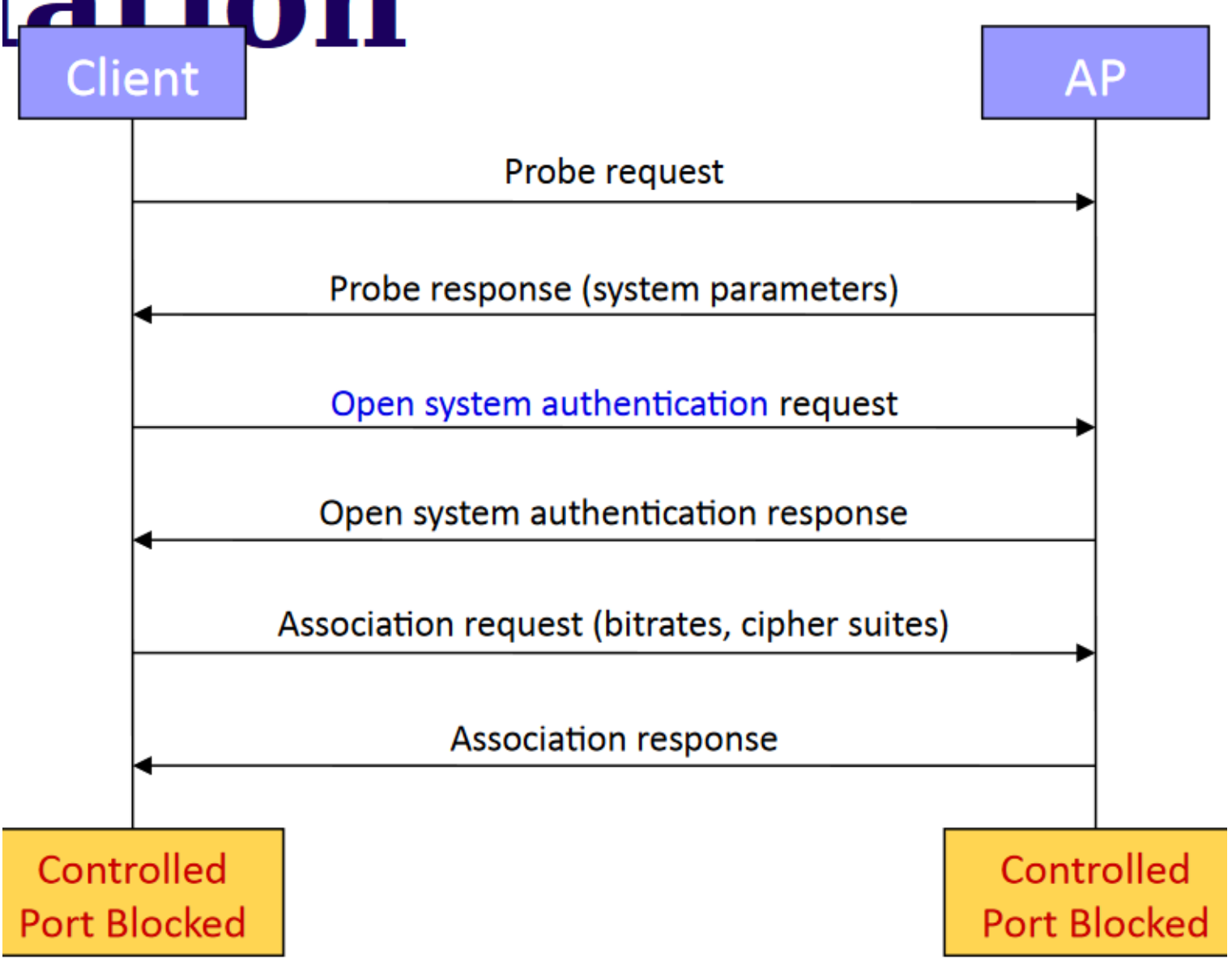
802.1X/EAP - Definitions

- EAP: Extensible Authentication Protocol
    - A variety of auth methods
    - EAPOL: Encapsulation of EAP over LAN
- RADIUS: Remote Access Dial-In User Service
    - Set of common functionalities across auth servers
    - a protocol that allows access those functionalities/services
- WPA2 with 802.1X is called WPA2-enterprise
    - Appropriate for medium and large enterprises, and more recently, public Wi-Fi networks

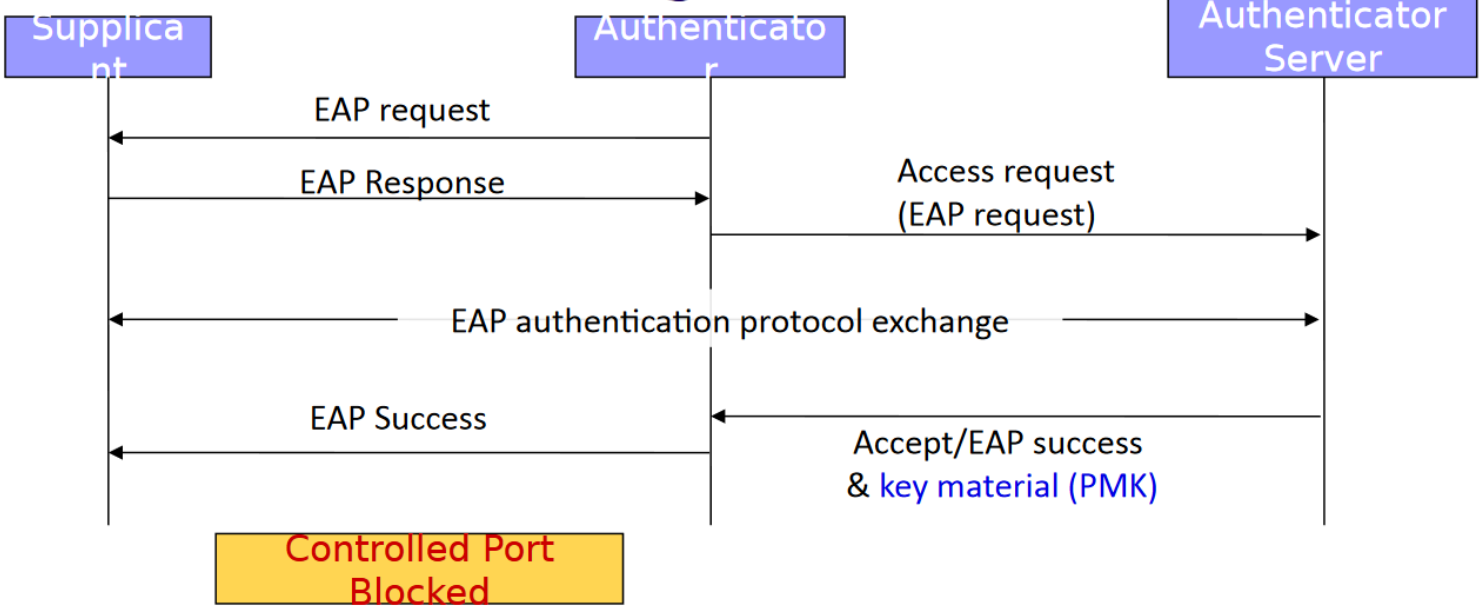
Pairwise Key Hierarchy

1. Maser Session Key (MSK)
    - Generated after mutual authentication for the supplicant and auth server (AS)
2. Pairwise Master Key (PMK)
    - In 802.1X mode: derived from MSK, and is client-specific
    - In pre-shared key mode: PMK = PSK (based on passphrase)
3. Pairwise Transient Key (PTK) - Derived from PMK
    - Generated after supplicant and AP's mutual auth

First Step 802.11 Association



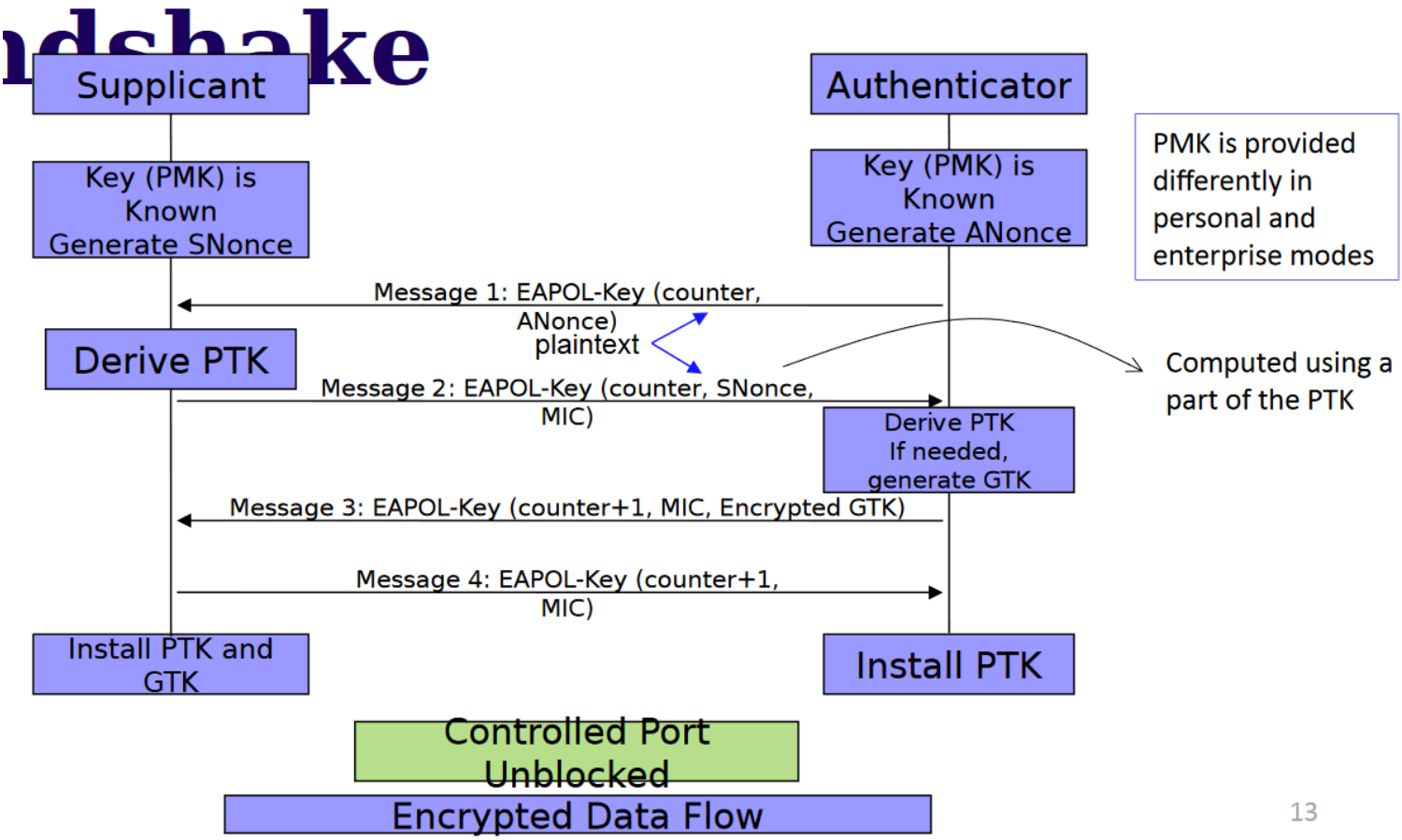
EAP Authentication (802.1X Only)



At this point, supplicant and AS have authenticated each other, but not the supplicant and the authenticator

1

Final Step: 4-Way Handshake



13

Results of 4-way Handshake

1. Supplicant and authenticator both proved the knowledge of the shared PMK
    - Mutual auth
    - A common step in both enterprise and personal

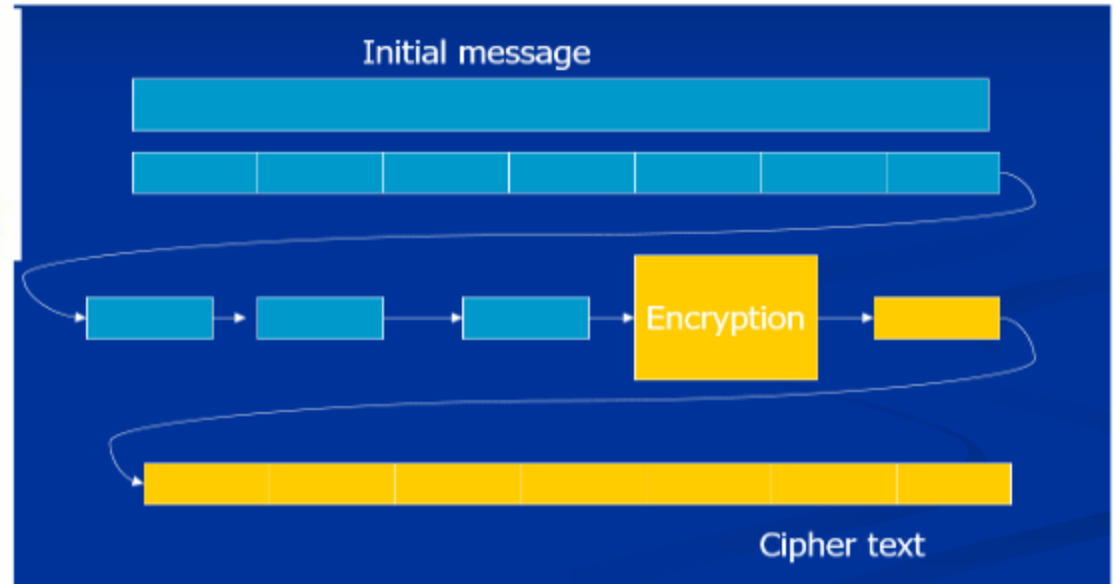
2. A fresh PTK is derived
3. both parties have synced and turned on encryption of unicast (and group) packets

AES-CCMP

- provides a very high level of confidentiality, integrity and replay protection of 802.11
- Relies on AES
  - 128 bit key
- CCMP: Counter mode with cipher-block chaining MAC protocol
  - 1. AES counter mode block cipher for encryption
  - 2. AEES cipher-block-chaining MAC (CBC-MAC) for integrity

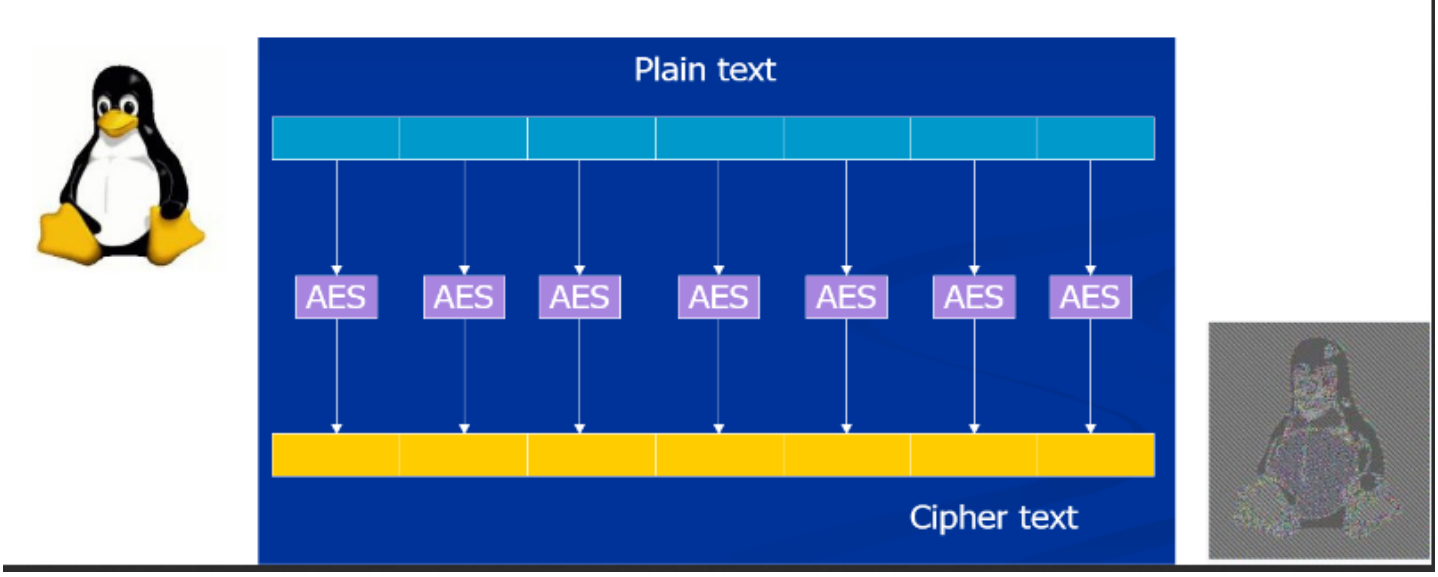
Block Cipher Modes (1)

- Electronic Codebook (ECB) - serial mode
  - reveals the patterns in the original data - not used in WPA2



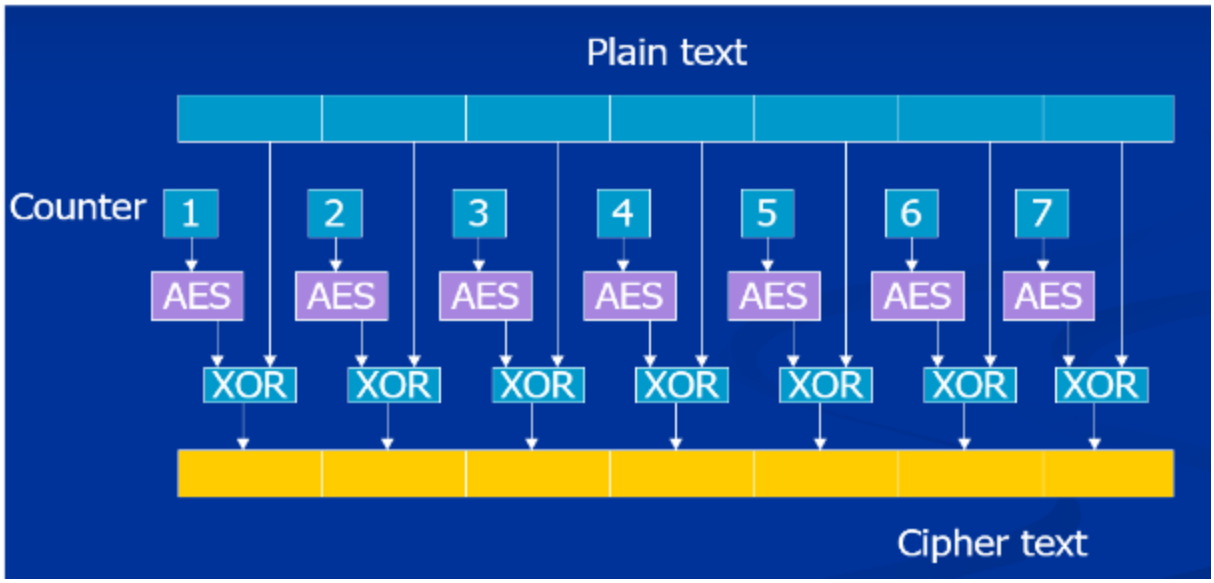
Block Cipher Modes (2)

- Electronic Codebook (ECB) - parallel mode
  - Reveals the patterns in the original data - not used in WPA2



Block Cipher Modes (3)

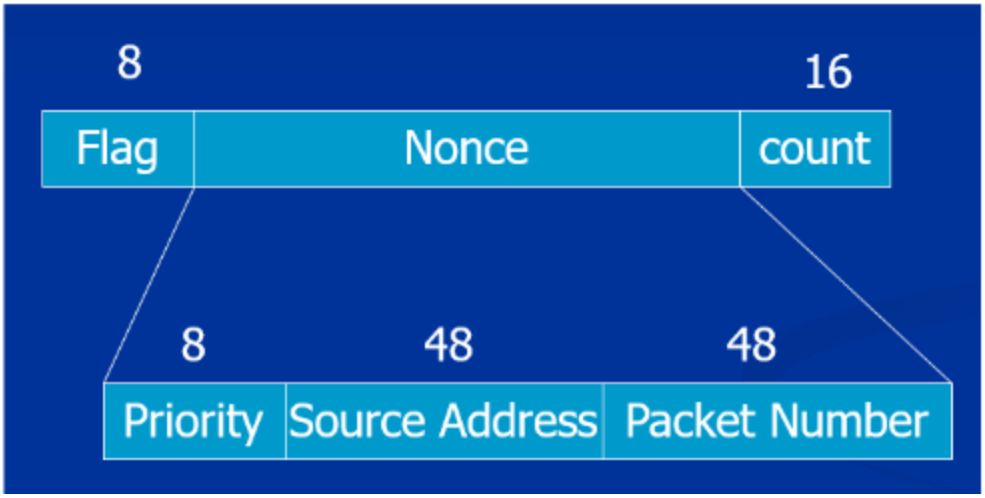
- Counter mode with AES - used in WPA2
  - Hide any pattern by using counter



Nonce + Counter

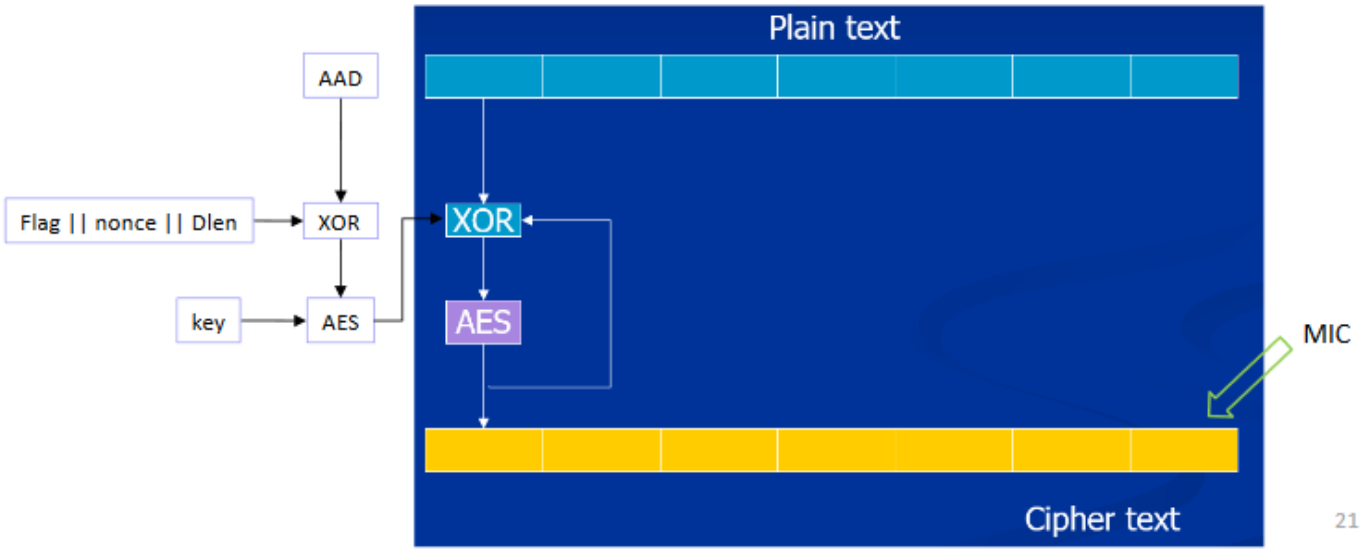
- The counter is prepended by a nonce
  - 104-bit nonce only changes from one packet to another

- The counter starts at , and counts up as encryption proceeds



Cipher-Block Chaining (CBC)

- Used to generate message integrity code (MIC)
  - Algorithm is initialized by nonce



Computing MIC

- Used CBC-MAC with 128-bit blocks
- The first block for computing MIC is comprised of
  1. Flag, which is a constant
  2. The same 104-bit nonce used in counter mode encryption
     - Dlen, which is the length of data
- Second block: Additional Authentication Data
  - MAC Addresses, the fragment number, and QOS identifier
- Then data blocks

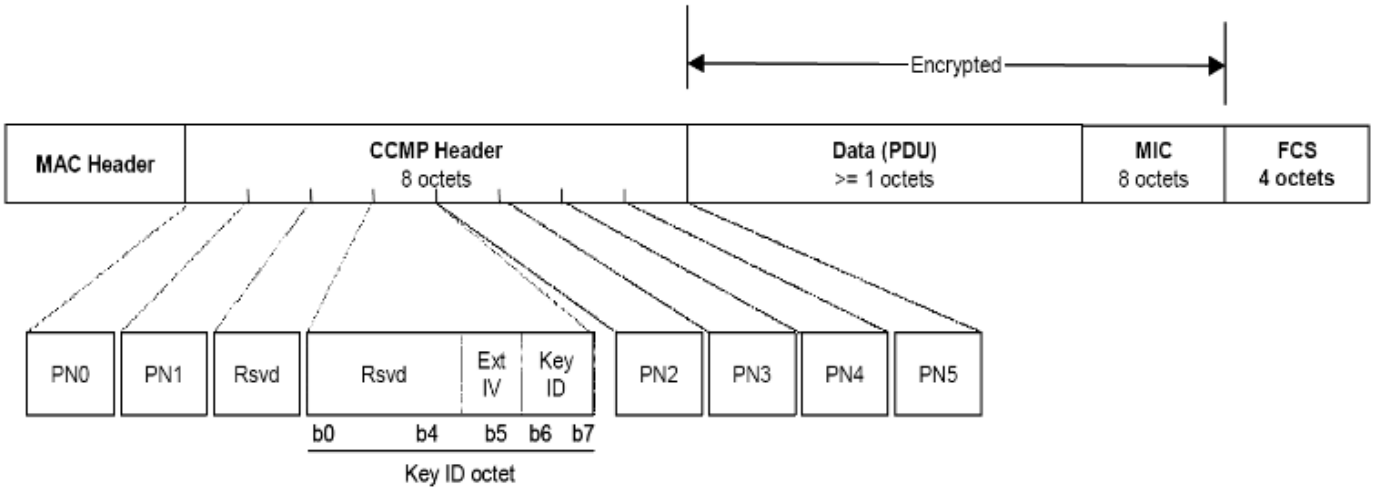
CCM Protocol (CCMP)

- CCM: Counter with CBC-MAC combination

- Three features
  - Specification of a nonce for each packet
    - Successive packets encrypted separately
    - Detects replay attacks
  - Achieve both message integrity and encryption with single PTK
  - Extension of integrity to cover data not encrypted (e.g., MAC addresses)

CCMP MPDU

- MAC and CCMP headers are not encrypted

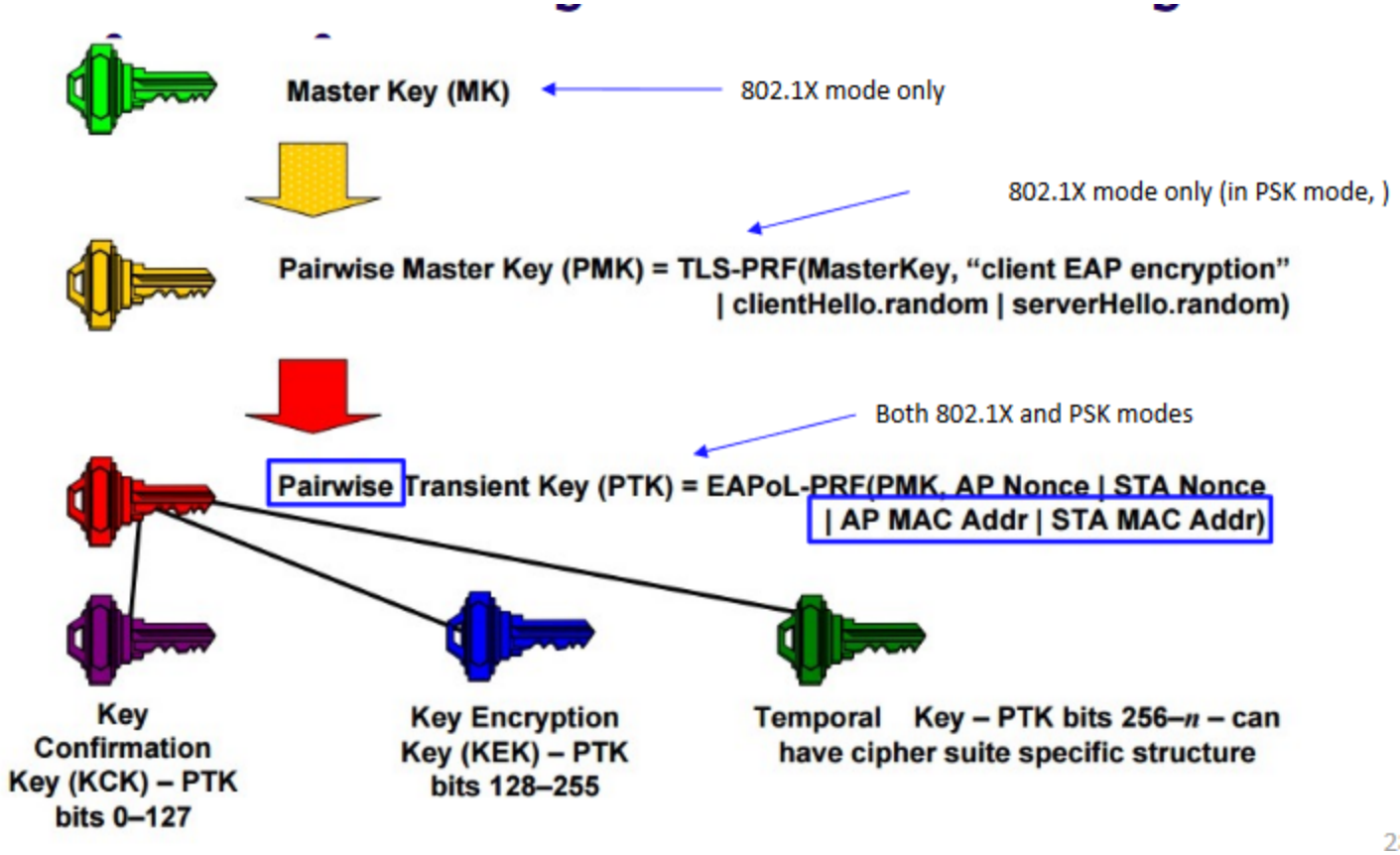


Week 4 Class 2

Pairwise Key Hierarchy - Review

1. Master Session Key (MSK) - Generated after 802.1X auth
2. Pairwise Master Key (PMK)
   - In 802.1X mode: derived from MSK
   - In pre-shared key mode:
3. Pairwise Transient Key (PTK) - Collection of operational keys
   - Key Confirmation Key (KCK) - used for integrity-checks for key distribution and to prove possession of PMK
   - Key Encryption Key (KEK) - used to encrypt and distribute keys, e.g., Group Transient Key (GTK)

- Temporal Key (TK) - used to encrypt data traffic



2

WPA2-Personal is Vulnerable

- Simple passphrases → dictionary attacks
  - PSK = PBKDF2(HMAC-SHA1, passphrase,ssid,4096,256)
    - PBKDF2: A password-based key derivation function
  - Capture one MIC, try different passphrases offline
    - Deriving PTK needs SNonce and ANonce too (sent in plaintext)
    - Even easier for other clients of the same network
  - coWPAtty: A tool for cracking/auditing pre-shared key (PSK)
- Fixed in WPA3

IEEE 802.11w (2009)

- Protected management frames
  - Confidentiality, integrity, authenticity, and replay (via CCMP)
- Frames protected by 802.11w
  - Disassociation and deauthentication
  - Radio measurement action frame
  - QoS action frame
- Frames infeasible to protect
  - Any packet sent before 4-way handshake (e.g., beacon, probe, authentication and association)

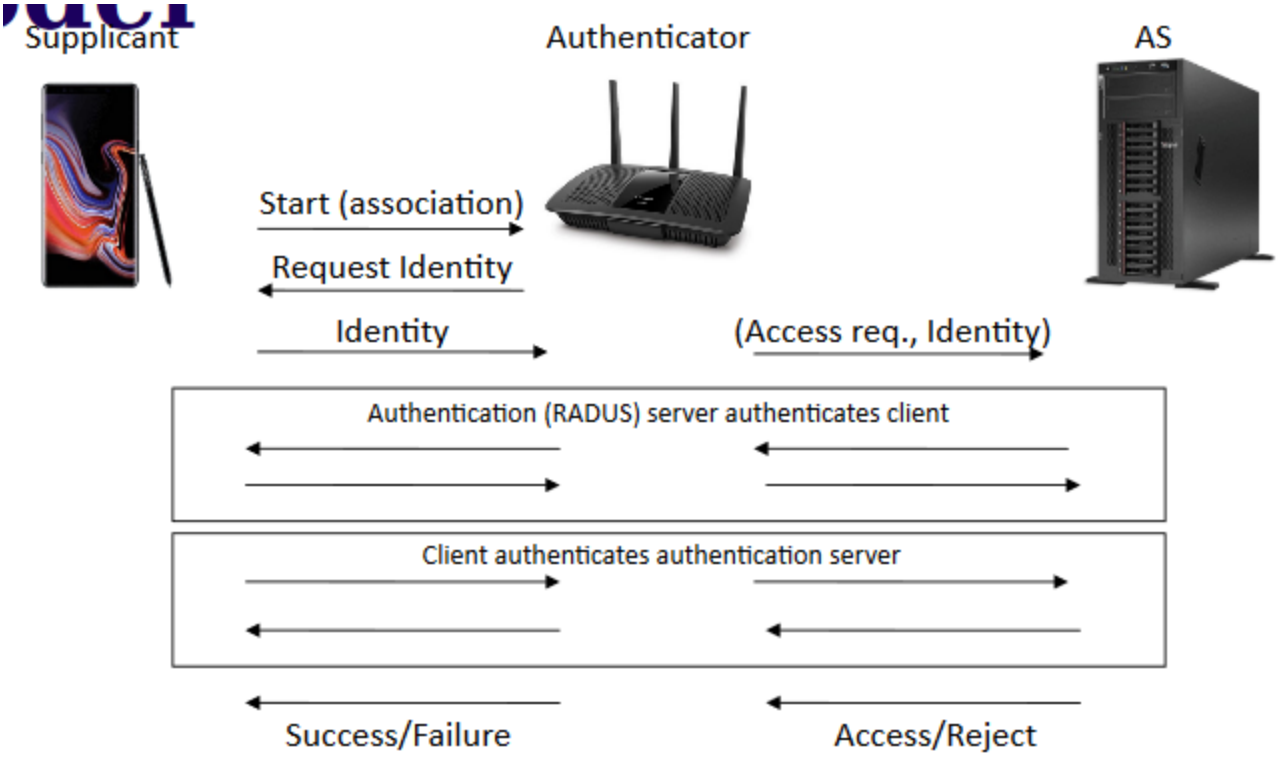
Challenges of Header Encryption

- interruption in virtual carrier sense
  - Other stations cannot read Duration field
- Sender identification dilemma
  - When MAC address is encrypted, the Rx (Bob) cannot easily retrive the right decryption key

Exposed MAC Address

- One can use unique, plaintext MAC addresses to track and identify users
  - Ex
    - smart trash cans to track/learn peoples shopping patters
    - Grocery stores created profile for their shoppers
- MAC address randomization for higher privacy
  - Standardized as part of IEEE 802.11aq amendment (2018)
- It should not disrupt an ongoing (encrypted) session
  - So it can be changed only in unassociated state (why?)
    - Used for prob requests per connection or per network/SSID

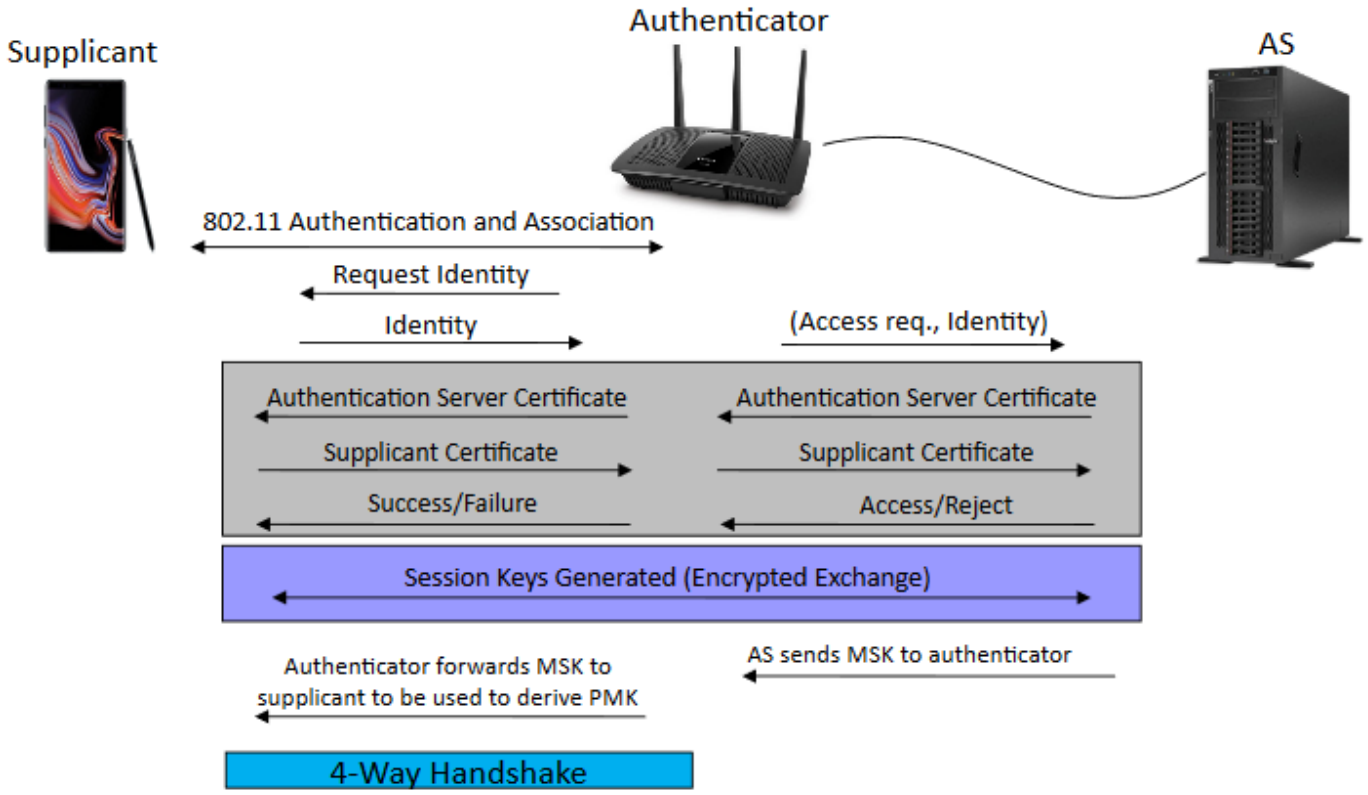
802.1X/EAP -WLAN Model



EAP-TLS

- Based on Transport Layer Security (TLS) protocol
  - One of the most secure EAP standards

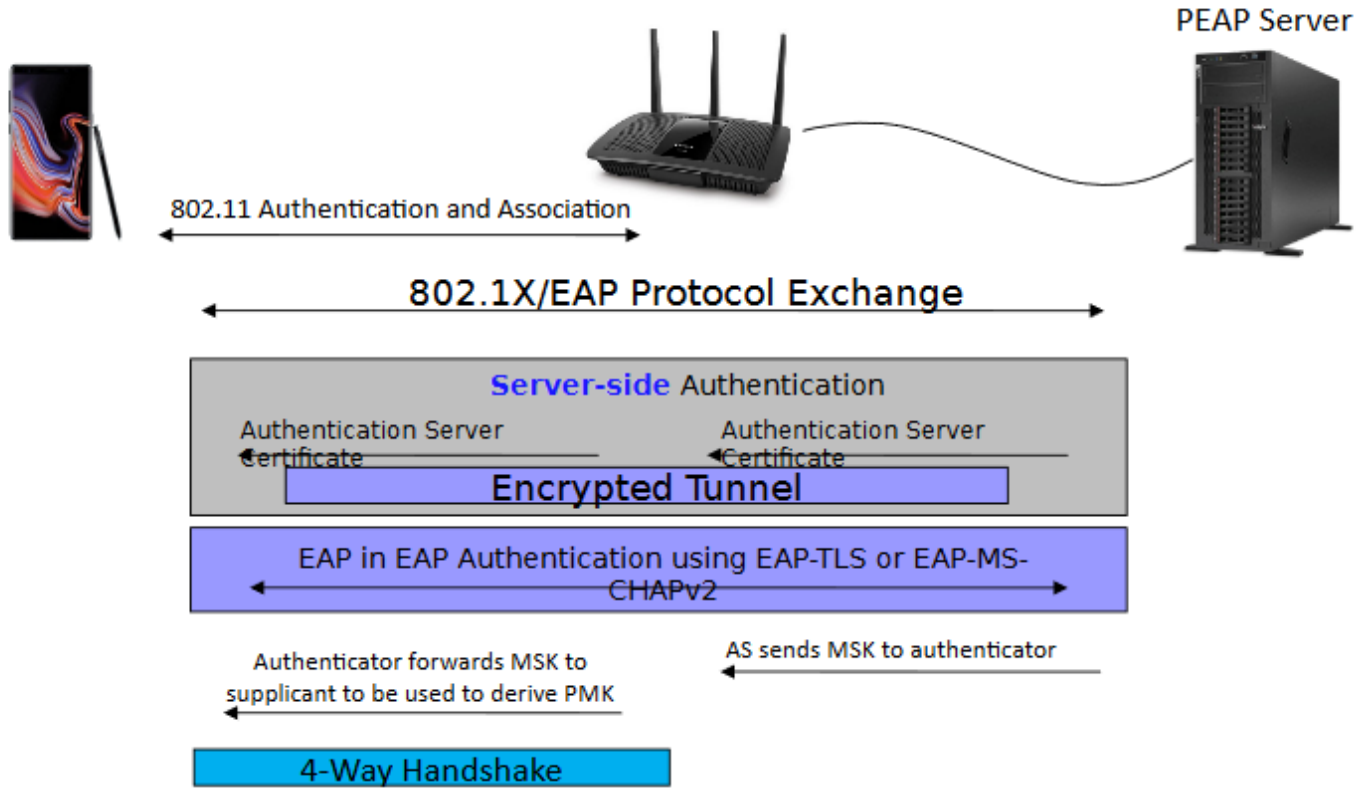
- Needs public key infrastructure
  - Requires certs for server and client (mutual auth)
  - Advantages
  - A compromised client password is not enough to illegitimately connect to the network
  - MitM attack against a client is difficult too; the attacker would need a valid server certificate



PEAP

- Protected EAP
- In EAP, identity request/response messages are not encrypted
  - PEAP provides secure communication channel (tunnel)
- PEAP auth has two phases
  - 1. EAP-TLS with anon users
    - Server-side public key certs (optional client auth)
  - 2. Regular EAP

- EAP in EAP



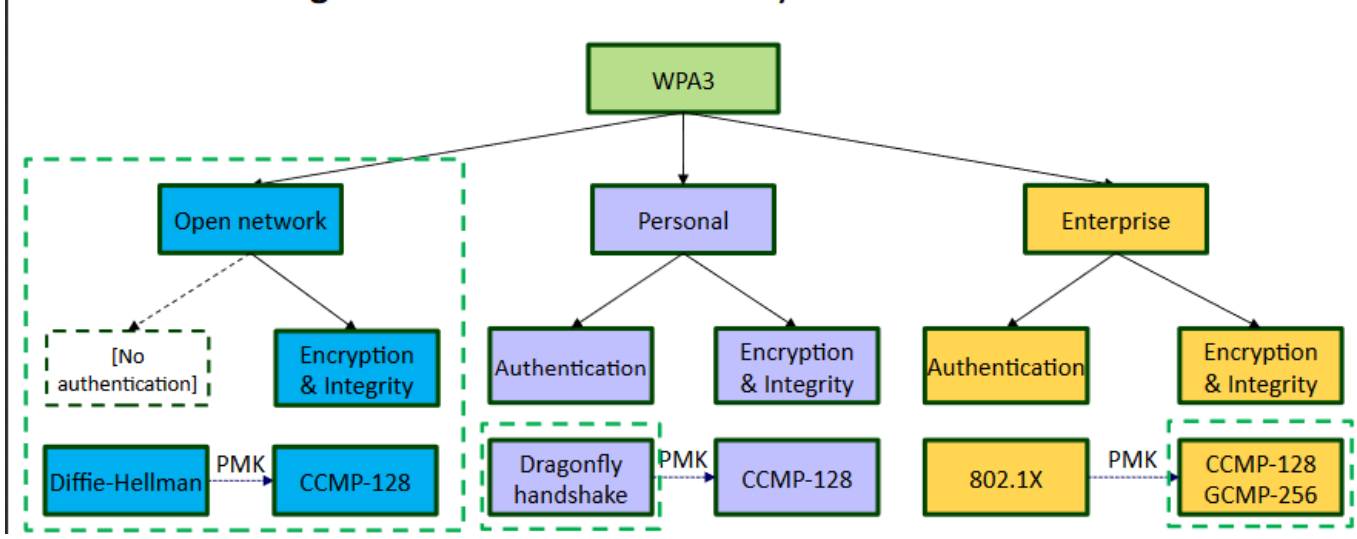
Passpoint for Public Networks

- What if you want auth in a public network
- Wi-Fi Passpoint (Hotspot 2.0)
    - Secure Wi-Fi enterprise was a success → extend it beyond an enterprise
    - Requires online sign-up and 802.1X
        - Auth using creds or the SIM
    - Automatic network discovery & selection, seamless roaming
        - Based on 802.11u (2011)
    - Used, among others, for WiFi4EU (Free Wi-Fi for Europeans)

WPA3 and Public Wi-Fi

WPA3 in a nutshell

- WPA3: Wi-Fi Protected Access III - 2018
  - Next generation of Wi-Fi security



- Dotted box is new in WPA3

WPA3 - New Features

1. Mandatory Protected Management Frames - PMF (802.11w)
2. Individualized encryption in public/open networks
    - Enhanced Open
3. Interact with the AP for each password attempt in WPA3-personal (dragonfly handshake)
4. 192-bit security for WPA3-enterprise (optional)
5. Alternative interface for configuring IoT devices
    - Easy Connect

WPA3-Personal

- Simultaneous Authentication of Equals (SAE)
    - Also called dragonfly handshake
    - Replaces PSK generation in WPA2-personal
    - Robust against offline dictionary attacks
        - Allows Natural Password Selection - select easy passwords
        - Also, provides forward Secrecy; unlike the passphrase, the PMK will have high entropy and no longer will be constant
- Manage (IoT) devices with limited or no interface
    - Device Provisioning Protocol (DPP)
    - Device's public key is communicated using QR, NFC, or BT

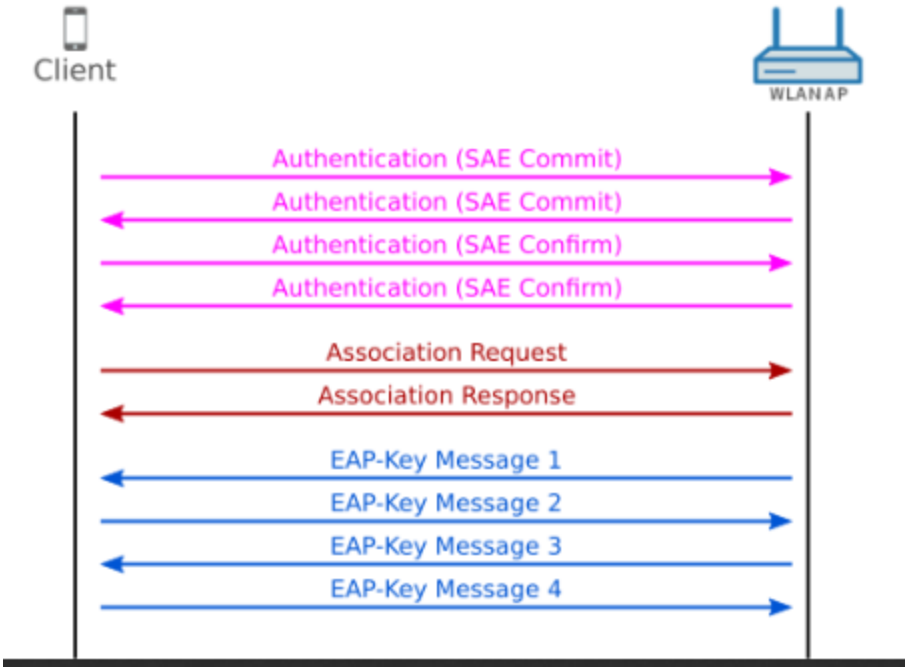
Dragonfly Handshake

- Two phases: Commit and Confirm
    1. Commit exchange: at both sides
       a.) commit to a signle guess of the password
       b.) exchange a random scalar and a masked password element (can be a point on an Elliptic curve), then

c.) generate a common key (PMK) using the exchanged random numbers and the password element
2. Confirm: derive a token using the secret, then exchange to confirm the guess

SAE Messages

- WPA2 authentication messages (with open-system auth) were almost useless, SAE uses and expands them!



Cracking SAE?

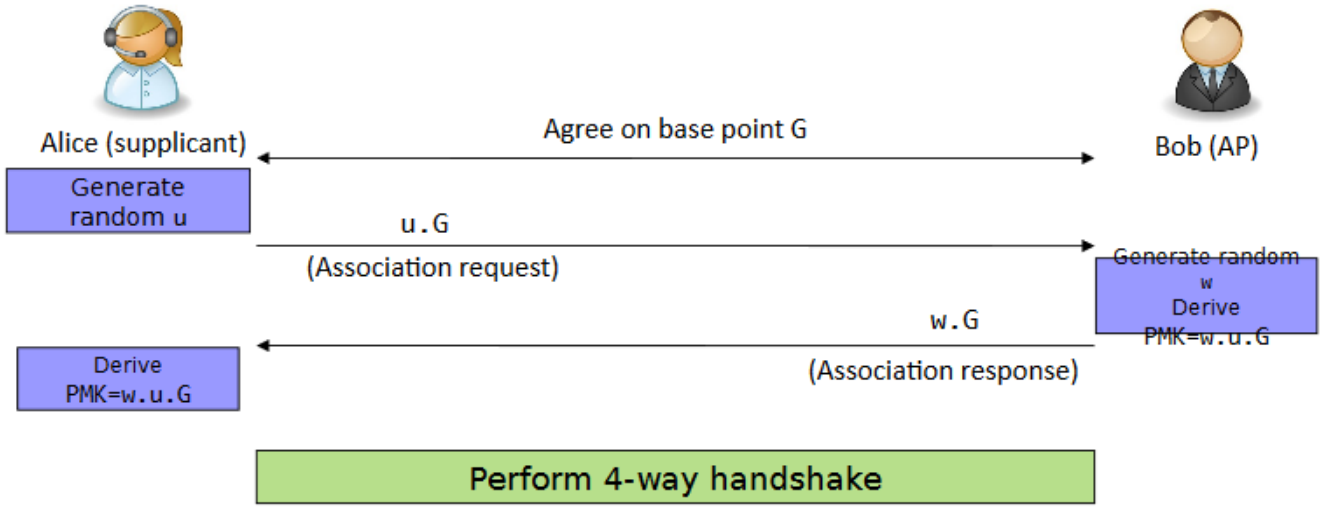
- Random numbers and password element are masked→Attacker cannot obtain them to check if a guessed passphrase (from dictionary) is correct
  - In contrast, the inputs to PBKDF2 function were known
  - ANonce and SNonce were also easy to capture
- Attacker would need a network interaction to confirm each guessed password
  - Idea: slow down the rate of an attempted attack
  - Temporal limit on password checks

After All, Why Public/Open Wi-Fi?

- A public open network may not be secure
  - In a restaurant/cafe, stadium, library, airport/airplane, hotel
- Possible reasons
  - Lower cost (free Wi-Fi)
  - Better indoor coverage than cellular
  - Running out of cellular data allowance (<30% remaining)

WPA3 for Open Networks

- Unauthenticated encryption
- Based on Opportunistic Wireless Encryption (OWE)



Lecture based Quiz 2

- Review the slides
- Take the baseline understanding

Week 7 Class 2

Staelliate Communications (SATCOM)

- Three main types
  - Relay commuications between ground stations
    - Beyond LOS communications
    - Signal is amplified via a transponder
  - Sense precipitation, temp, emissions, etc
  - Track and control objects on the ground
- Applications
  - TVs, phone, positioning, radio, internet, military
  - Over 2,000 satellites are orbiting

Communication Satellites

- Types of geocentric satellites
  - Low Earth Orbit (LEO) - below 2,000 km
  - Medium Earth Orbit (MEO) - below 35,000 km
  - Geostationary Orbit (GEO) - move at same speed as earth
  - High Earth Orbit

GPS Global Positioning System

- Sat-based radio navigation system owned by US gov, operated by the US air force
  - Global navigation sat system (GNSS) provides geolocation and time info to a GPS receiver
  - Requires an unobstructed LOS to four or more GPS satellites
- There are 31 satellites

SATCOM Security Challenges

- End-to-end encryption - costly (multibillion dollar investment)
- Denial of service attacks (jamming)
- Autonomous attack detection and incident response
- Secure networking for a large number of satellites in multiple orbits with multiple communications links
- In particular, how about GPS?
  - Authentication? no
  - Confidentiality? no
  - Availability? no

Secure SATCOM - Spread Spectrum

- First line of defense against jamming and eavesdropping
  - Also, mitigates interference

1. Direct sequence spread spectrum
   - Example: GPS
2. Frequency hopping spread spectrum
   - More robust to interference/attacks
     - Dynamic FH sequence → hard to learn by adversaries
   - Examples: Military Strategic and Tactical Relay (MILSTAR)

Lit Review

Expectations

- get 4 main things
  - baseline understanding of wireless security
  - presentation skills
  - get a good sense of things coming up in wireless security (emerging topics)
  - practice steps of the research process (think independently)
- Read 5-7 good papers
- 2 pages including introduction
- you are then expected to know exactly what the next steps are to complete the project
- Make a case that what you come up with is different than what others have done

- Threat model: What are the capabilities and goals of the attacker

Cellular Networks Security

- Base station (eNodeB) in a Radio Access Network (RAN)

Subscriber Identity Module (SIM)

- Secure storage for
  - Administrating data
    - PIN
  - International Mobile Subscriber Identity - IMSI
  - Temporary Mobile Subscriber Identity - TMSI (or GUTI)
  - Authentication and Ciphering Keys
  - Roaming data, SMS, telephone numbers, etc
    - Mobile Station International Subscriber Directory Number - MSISDN
  - SIM card is also a computing device
    - Implementation of encryption

Mobile Equipment Identification

- International Mobile Equipment Identifier (IMEI)
  - Allows unique identifying phones, independent of SIM
- Equipment Identity Register (EIR)
  - White list - valid mobiles
  - Black List - stolen
  - Gray List - local tracking mobiles
- Central Equipment Identity Register (CEIR)
  - Approved mobile type
  - Consolidated black list

IMSI

- To uniquely identify a subscriber/SIM
  - It is different than telephone number (MSISDN) and IMEI
  - TMSI, assigned by the network, is used to hide the IMSI
- 15 digits (or less)
  - 3 digit mobile code - MCC
  - 3 digit mobile network code (MNC) - in the US
  - 9-10 digit mobile subscriber identification number - MSIN

Key Management Scheme

- K - Subscriber Authentication Key

    - Shared 128-bit key
    - Used for subscriber (SIM holder) authentication and session key generation
- Stored in 2 locations
    1. Subscribers SIM (owned by operator, trusted)
    2. Home Locator Register (HLR) of the subscribers carrier
- SIM can be used with different equipment
    - Key management is independent

Cellular Networks - Generations

- 1G - 1980's
    - Analog radio signals
    - FDMA (frequency-division multiple access)
    - Voice-only
- 2G (GSM) - 1990s
    - Global System for Mobile Comms
    - Digital radio signals, using digital modulation
    - TDMA (time-division multiple access)
    - Data services (SMS and MMS)
    - Digital encryption, one-way auth

A5 - A Stream Cipher

- Implemented very efficiently on SIM for 2G
    - Design was never made public
    - Disclosed by Ross Anderson and Bruce Schneier
- Variants
    - A5/1 - the strong version
    - A5/2 - the weak version (for certain export regions)
    - A5/3
        - GSM Association Security Group and 3GPP design
        - Based on KASUMI Algorithm

Encryption in GSM (2G)

- Stream cipher using A5/1 Algorithm
    - Security through obscurity? A5 was initially kept secret, but became public through reverse engineering
    - Within 2 minutes of intercepted call, the attack takes only 1 second

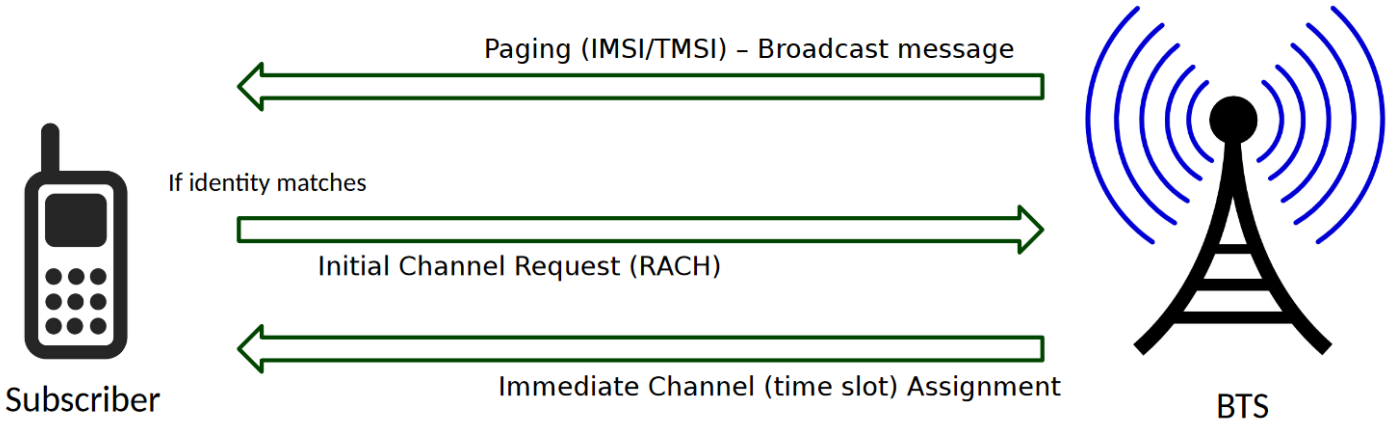
IMSI Catchers

- Eavesdroppers who intercept users' IMSI to track their location and other things
    - Attacker is afake (portable) BTS, a form of MitM attack

        - the fake base station send an identity_request to the victim mobile phone, forcing it to respond with its IMSI
    - Easy to launch GSM (why?)
        - phones dont auth network, they automatically trust the network
- StingRay:Harris Corp IMSI Catcher for phone surveillance
    - Intercept GSM communications
    - Stingray II: Crossbow (U.S. ICE)

Paging

- An incoming call or SMS for the subscriber



Paging and Identity Harvesting

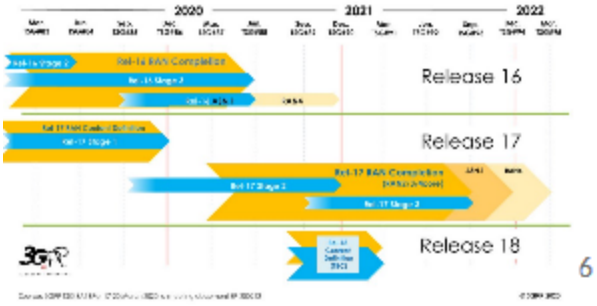
- Paging
    - When the network/BTS needs to notify the mobile phone of an incoming call/SMS
    - The paging request message contains IMSI/TMSI in cleartext
- Identity harvesting attack
    - Dial and disconnect immediately, forcing the BTS to keep sending paging request messages

Next Generations - 2.5G

- 2G retirement
    - AT&T (2017) and Verizon (2020) already shut down 2G
    - T-Mobile is expected to shutdown 2G by December 2022
        - T-Mobile already blocks new 2G or 3G activations (Jan. 2021)
- 2.5G (GPRS) - early 2000s
    - Packet switching (billing based on data volume)
        - GSM was circuit-switched telephony
        - best-effort service
    - GEA3 (based on KASUMI) for keystream generation

3GPP

- 3rd Generation Partnership Project
  - Standards organization of mobile broadband protocols
  - Formed in 1998 for developing 3G
- Three Technical Specification groups
  1. Radio Access Network (RAN)
  2. Services & Systems Aspects (SA)
  3. Core Network & Terminals (CT)
- Releases



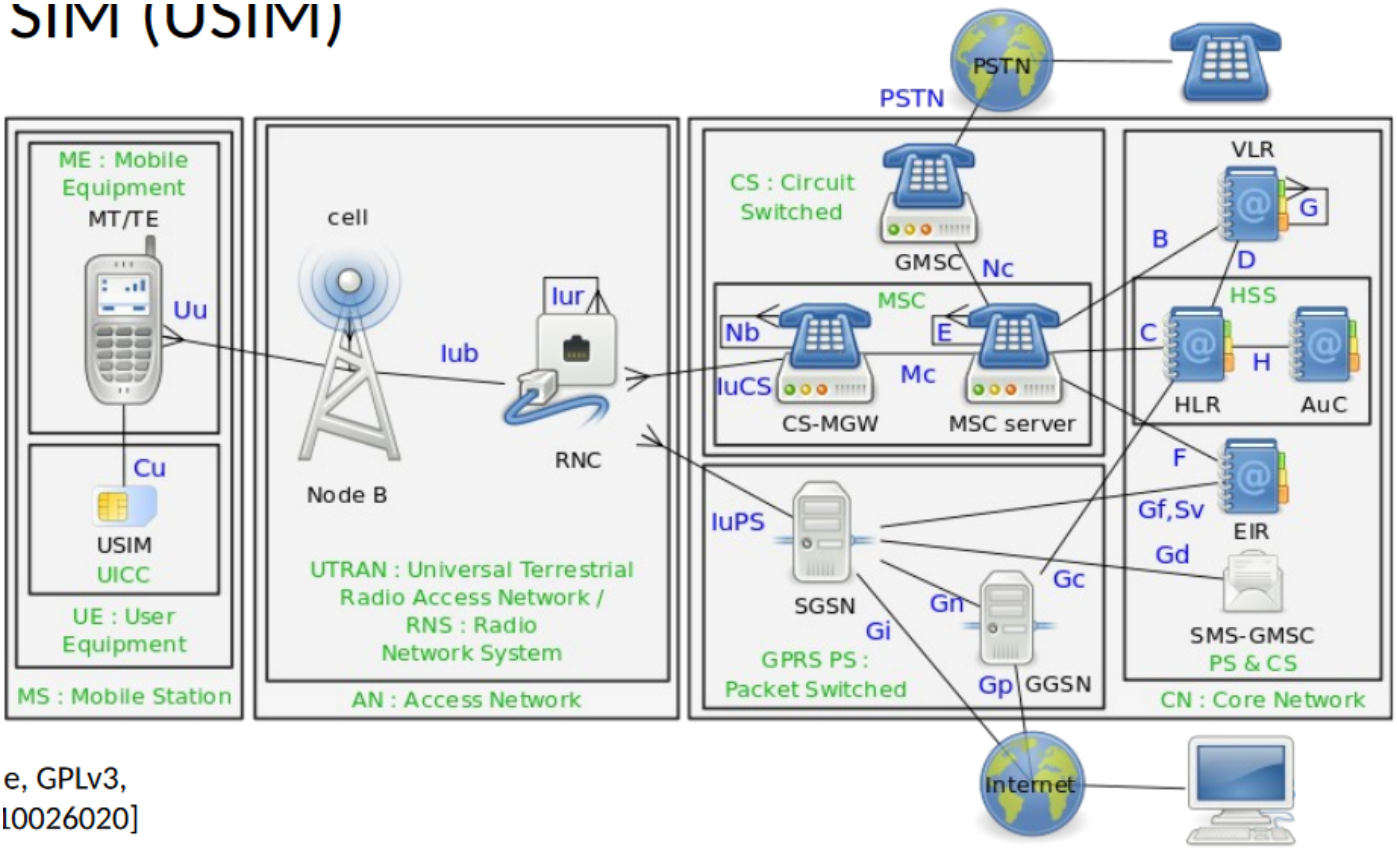
3rd Generation (3G)

- 3G - early 2000s
  - Higher data rate (up to 14 mbps)
  - code division multiple access (CDMA)
    - Based on DSSS, each user is assigned a dedicated code
- Competing Techs
  - UMTS (Universial Mobile Telecommunications Service)
    - Europe, Japan, China
  - CDMA2000: Adopted by Verizon Wireless in 2002, will shut down by the end of 2020 (ATT: 2022)

UMTS Architecture

- very similar to GSM
  - Mobile station→ User equipment (UE)
  - SIM → Universal SIM (USIM)

- BTS → Node B



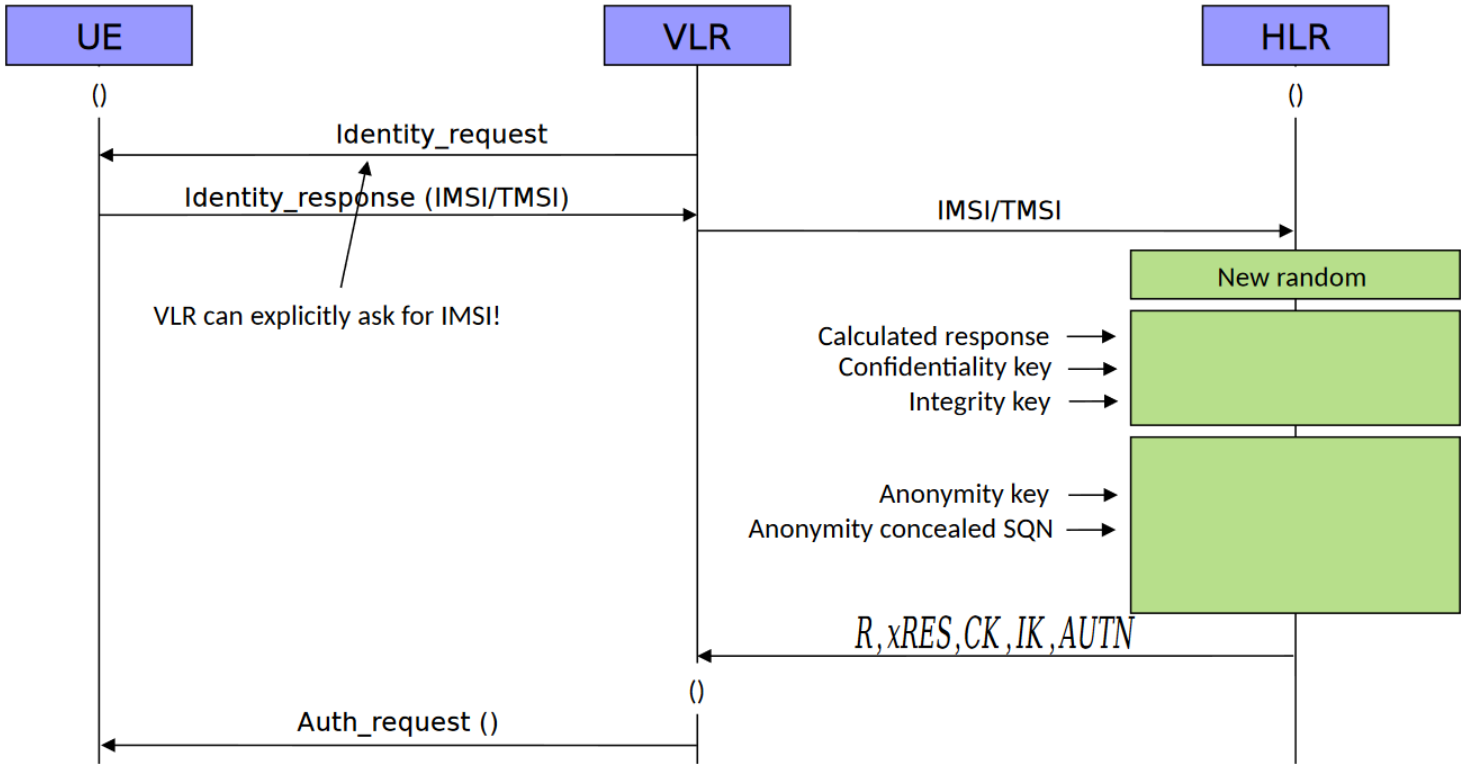
3G Mutual Auth

- New! Allow the UE to authentication the network,mitigating impersonation attacks
- Authentication and Key Agreement (AKA) protocol
  - The basis for security in 3G, 4G, 5G
  - Challenge-response for UE authentication (like GSM)
  - SQN: sequence number to prevent replay attacks
  - Establish keys to protect subsequent communications
    - using f1--f5: A set of one-way keyed cryptographic functions
    - That includes f4 for integrity key generation

AKA Main Features

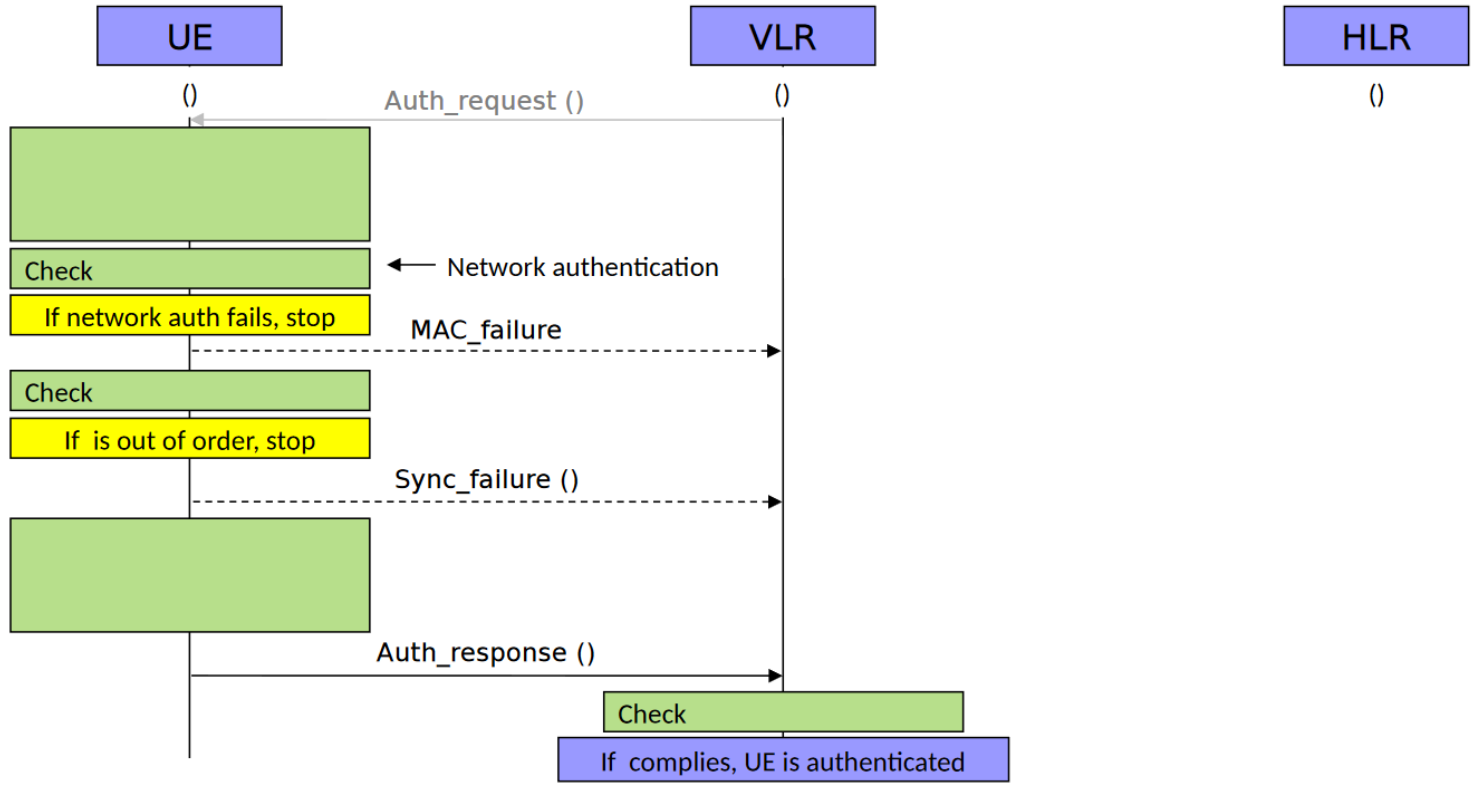
- A unique permanent pre-shared symmetric key K
- The network generates a challenge R
  - It authenticates the UE through verifying UE's response RES
- The network also generates a MAC (Message authentication code) for SQN and R
  - UE authenticates the network via verifying its MAC
- SQN is not transmitted in plaintext
  - To prevent eavesdropping and correlating attacks

AKA - 1st Phase



HLR - Home Location register
xRES - expected Response from UE
CK - Confidentiality Key
IK - Integrity Key

AKA - 2nd Phase

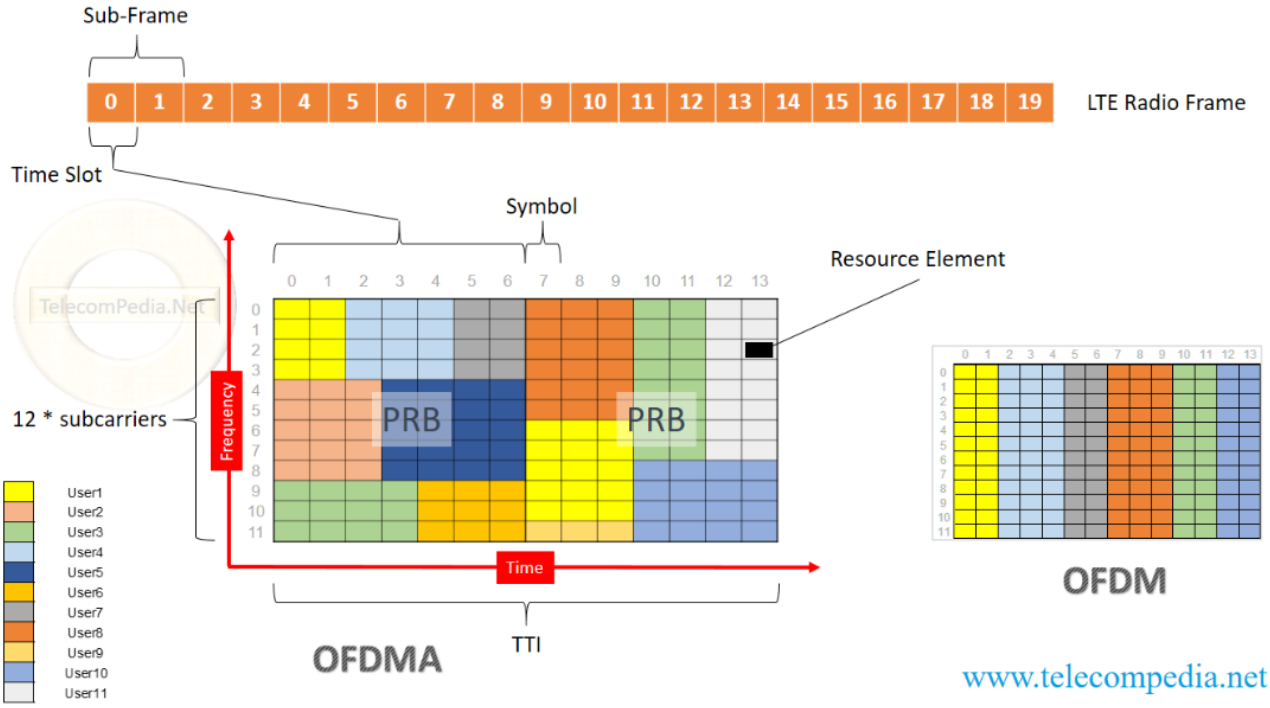


4th Generation (4G)

- 4G - 2011
  - All IP-based communications (IP telephony)
    - Voice over LTE (VoLTE) - HD voice call
  - Increases speed (up to 1 Gbit/s)
  - OFDMA multi-carrier (instead of CDMA)
  - MIMO capability
- Two techs
  1. LTE Advanced (long term evolution advanced)
  2. Mobile WiMAX (IEEE 802.16e) - not very popular in the US
     - last mile wireless broadband access instead of cable and DSL

OFDMA vs OFDM - A Review

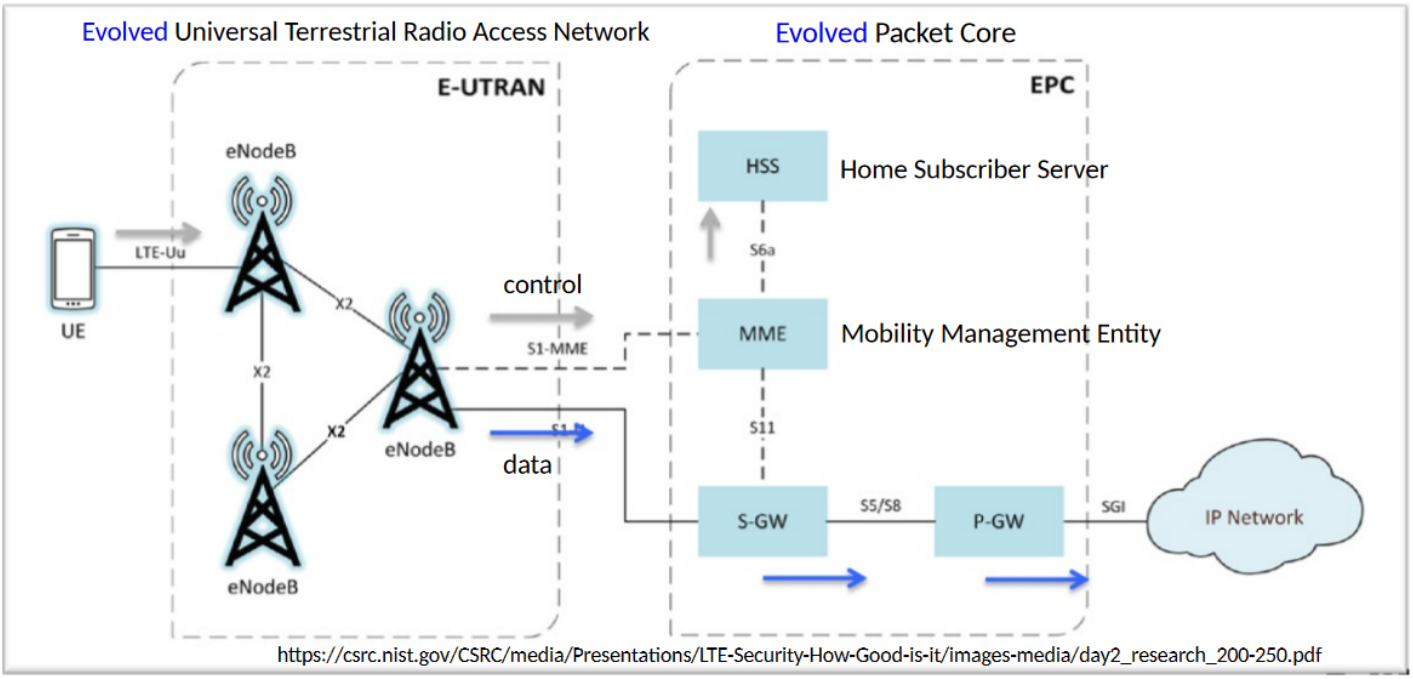
- Orthogonal Frequency Division Multiple Access



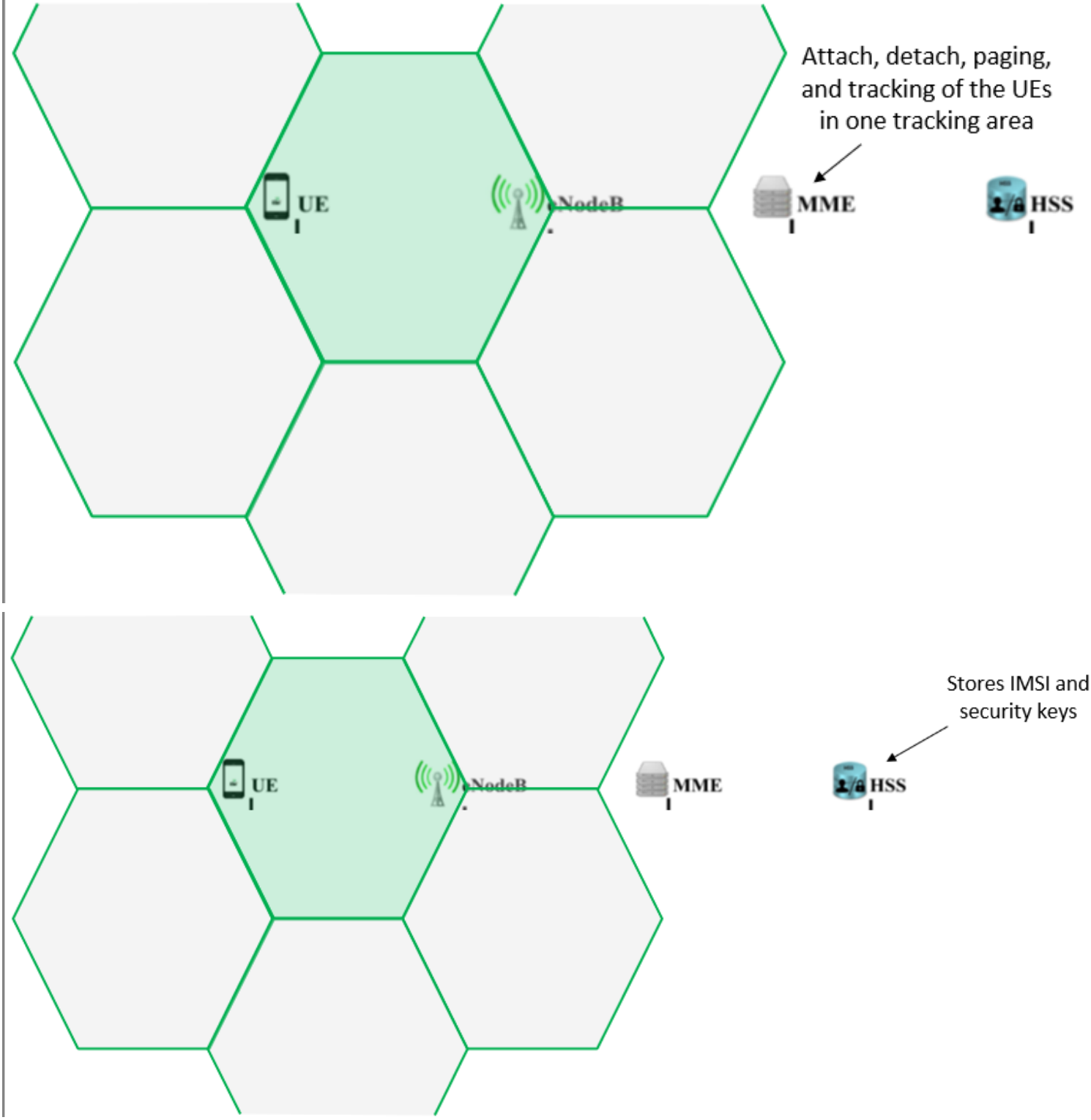
LTE Network Architecture

- Node B → Evolved Node B (eNodeB) - more responsibilities

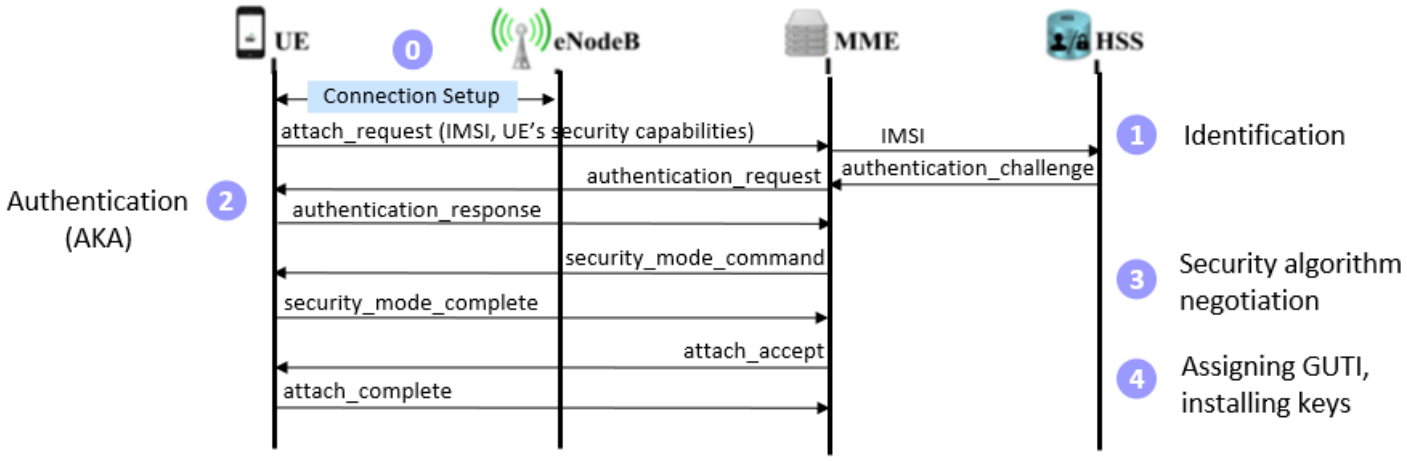
- HLR → Home Subscriber Server (HSS)



Attach Procedure in LTE


Attach, detach, paging, and tracking of the UEs in one tracking area
UE
eNodeB
MME
HSS

Stores IMSI and security keys
UE
eNodeB
MME
HSS



- GUTI (Globally Unique Temporary Identity) = MME + TMSI

How NSA Tracks People

- A mobile device continuously announces its location

IMSI Catchers (Again!)

- Malicious eNodeB advertises itself as legitimate
  - Sniff and duplicate the configuration of a legitimate eNodeB
  - Create higher received signal strength than the legitimate's
- Force all UEs to disclode their IMSI in the clear
  - UE trusts any eNodeB who claims it has never seen that UE
- No need to downgrade to GSM
  - identity_request message is still unauthenticated!
- Open source tools
  - srsRAN (with SDR inside Faraday cage - why?) Against the law

4G - Crypto Algorithms

- Available encryption and integrity algorithms
  - Snow 3G (EIA1/EEA1) - mandatory
    - Stream cipher, employs an LFSR (initiated by the key and a 128-bit initialization variable) and a state machine to generate a sequence of 32-bit words
  - AES (EIA2/EEA2) - mandatory
    - Block cipher - Counter mode for confidentiality and cipher-based MAC mode for integrity
  - ZUC (EIA3/EEA3) - optional
    - Stream cipher, with a 128-bit initialization vector
- They all use 128-bit keys

4.5th Generation - 2015

- LTE Advanced Pro (4.5G)
  - Up to 3 Gbps (3x LTE Advanced)
    - Aided by 256-QAM support
  - Employs MU-MIMO
- Introduces narrowband IoT (NB-IoT)
  - Bring IoT devices to the cellular networks ecosystem
  - Low cost, long battery life, and high connection density
  - Uses the same security and privacy features of LTE

5th Gen (5G) - 2019

- New applications beyond mobile internet
  - drones
  - vehicles
  - IoT/sensors
  - ...
- New frequency bands: 2.5-3.7 GHz, 25-39 GHz
  - In addition to the traditional 600 - 850 MHz band for LTE
  - Different coverage ranges (why?) physics of waves
  - eNodeB → gNB

5G Design Goals

- Extremely low latency
  - ultra-reliable and low-latency communications (URLLC)
    - Less than 1 millisecond
  - Applications: remote surgery, VR, interactive/autonomous vehicles (smart transportation), etc.
- Ubiquitous, high density, high speed connectivity
  - Extreme mobile broadband (xMBB) - up to 10 Gbps
  - Massive machine-type communications (mMTC) - smart city
  - Support higher densities
    - Concerts, stadium, malls, etc

5G Ecosystem

- A massively connected community
  - wearables
  - Smart vehicles
  - Appliances
  - Virtual Reality
  - Augmented Reality
  - Public Safety
  - Smart classroom :)
  - Remote surgery
  - ...

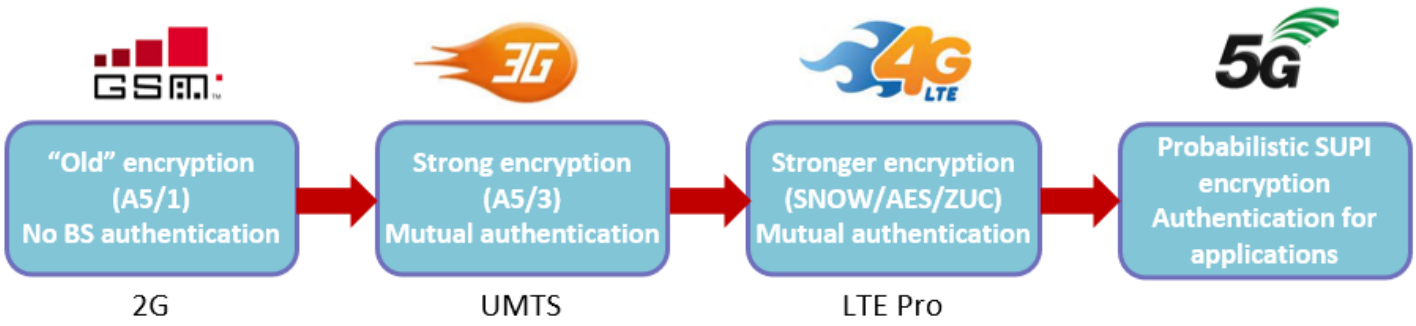
What Brings About 5G?

- Key enabling technologies
  - Millimeter waves and small cells
  - Massive MIMO
  - Beamforming
  - Full duplex
  - Network slicing/virtualization
- Implications:
- Challenges
  - Fast signal decay (why?) needs more gNBs, new hardware, wider attack surface, privacy concerns, ...

5G Security

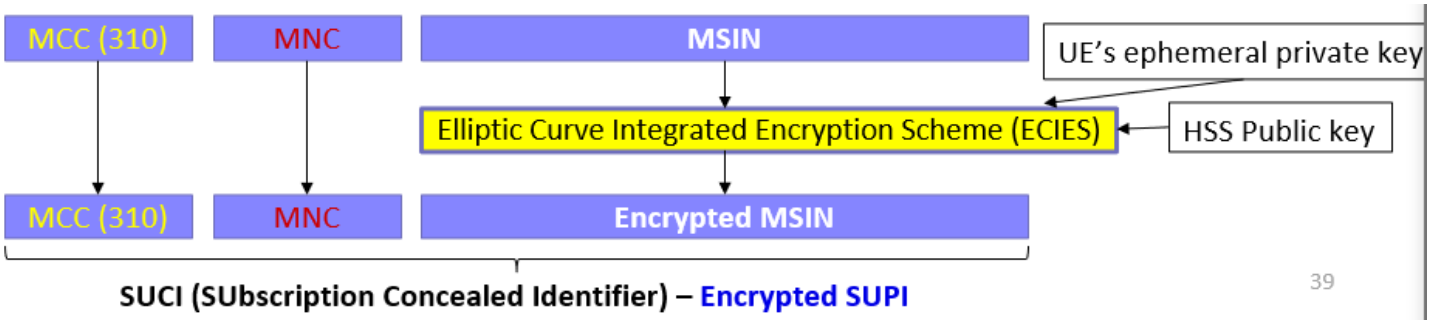
- The same encryption and integrity algorithms as LTE
- IMSI → SUbscription Permanent Identifier (SUPI)

- 5G-GUTI is still supported
- Evolution of security from 2G to 5G:



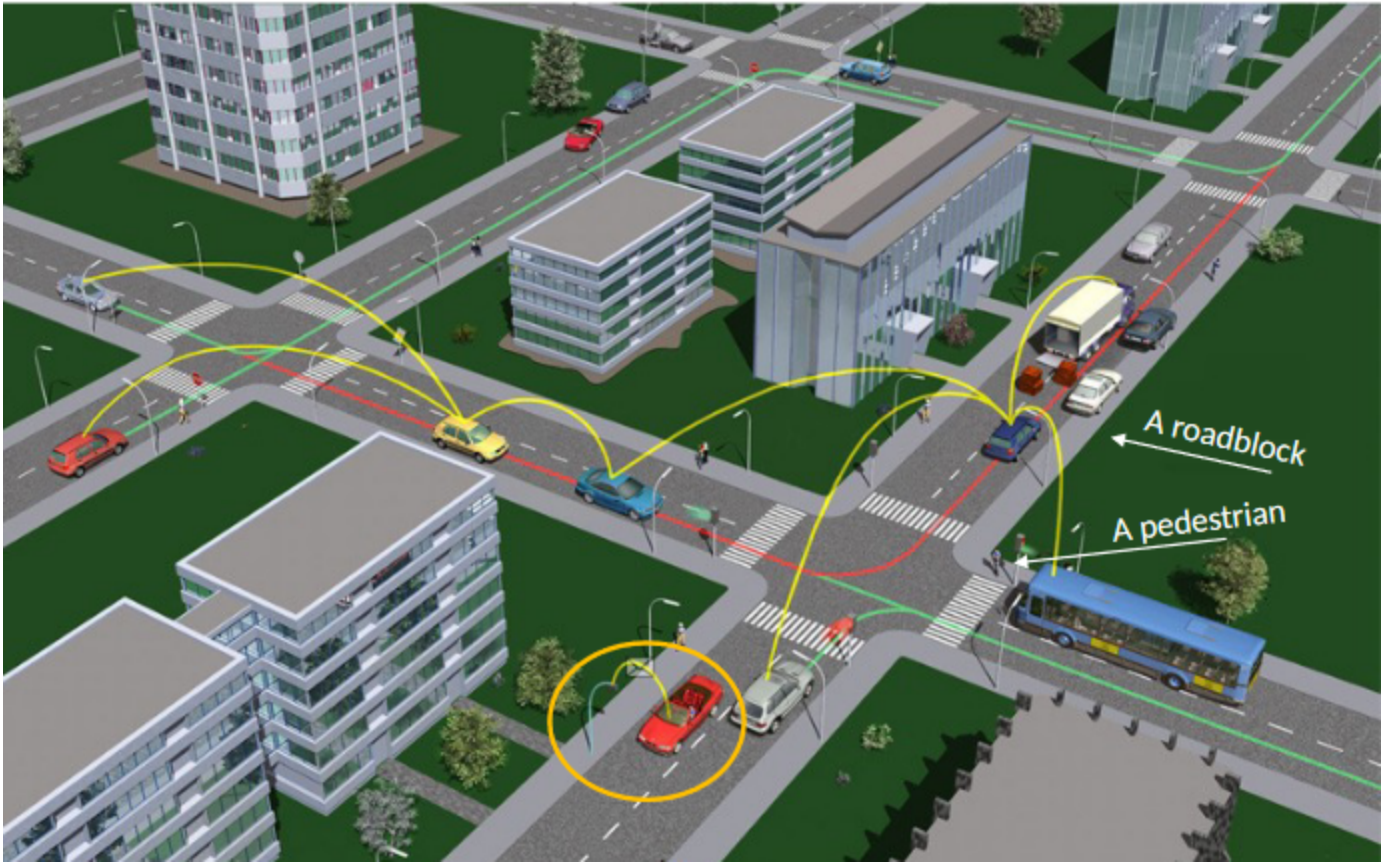
5G Security - SUPI Encryption

- SUPI obfuscated and encrypted (concealed) using public key of HSS
  - HSS (home network) public key is stored in USIM
  - Probabilistic asymmetric encryption using ECC
  - Each time, same SUPI is encrypted with a different ephemeral key to generate a different SUCI (to avoid creating a fixed ID)



Security of Vehicle-to-Everything Communications

Roadways of the Future



Connected Vehicles (CV)

- Let vehicles "talk" to enhance proximity awareness
  - Can reduce > 60% of the deaths on the roads
    - 98% of accidents today are due to human errors :(
  - Increase transportation system efficiency
    - Reduced travel time, less traffic, and less pollution
  - Comfort while driving, social inclusion (mobility for all), ...
    - Autonomous, semi-autonomous, and non-autonomous cars
- Emerging technology with rapid growth
  - Projected market value by 2028: $12.8 Billion
  - Volkswagon, BMW, Ford, Tesla, Nissan, Cadillac, Audi, etc.

Types of Connected Vehicles

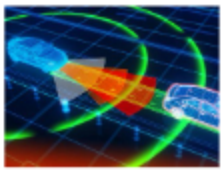
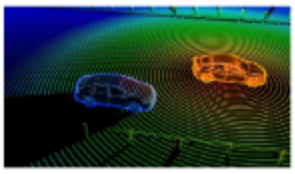
- exploit wireless waves to talk
- Depending on whom a vehicle talks to
  - Vehicle-to-Vehicle (V2V)
  - Vehicle-to-Netowkr
  - Vehicle-to-Pedestrian
  - Vehicle-to-Infrastructure
  - Vehicle-to-[insert your choice] → V2X
    - Cellular V2X - Vehicles as new citizens in future 5G ecosystem

Vehicle to Infrastructure

- Roadside Units (RSU)
  - Devices installed along the roadway
  - Capable of relaying V2X messages
  - Can interface with traffic management systems like traffic light controllers

Vehicle to Vehicle Communications

- Provide 360 degree awareness of nearby vehicles
  - Wirelessly exchange safety and non-safety messages
  - Complement the sensors: see (in NLOS) wjat sensors cant

Camera Radar LiDAR

  - Sensors
  - V2V

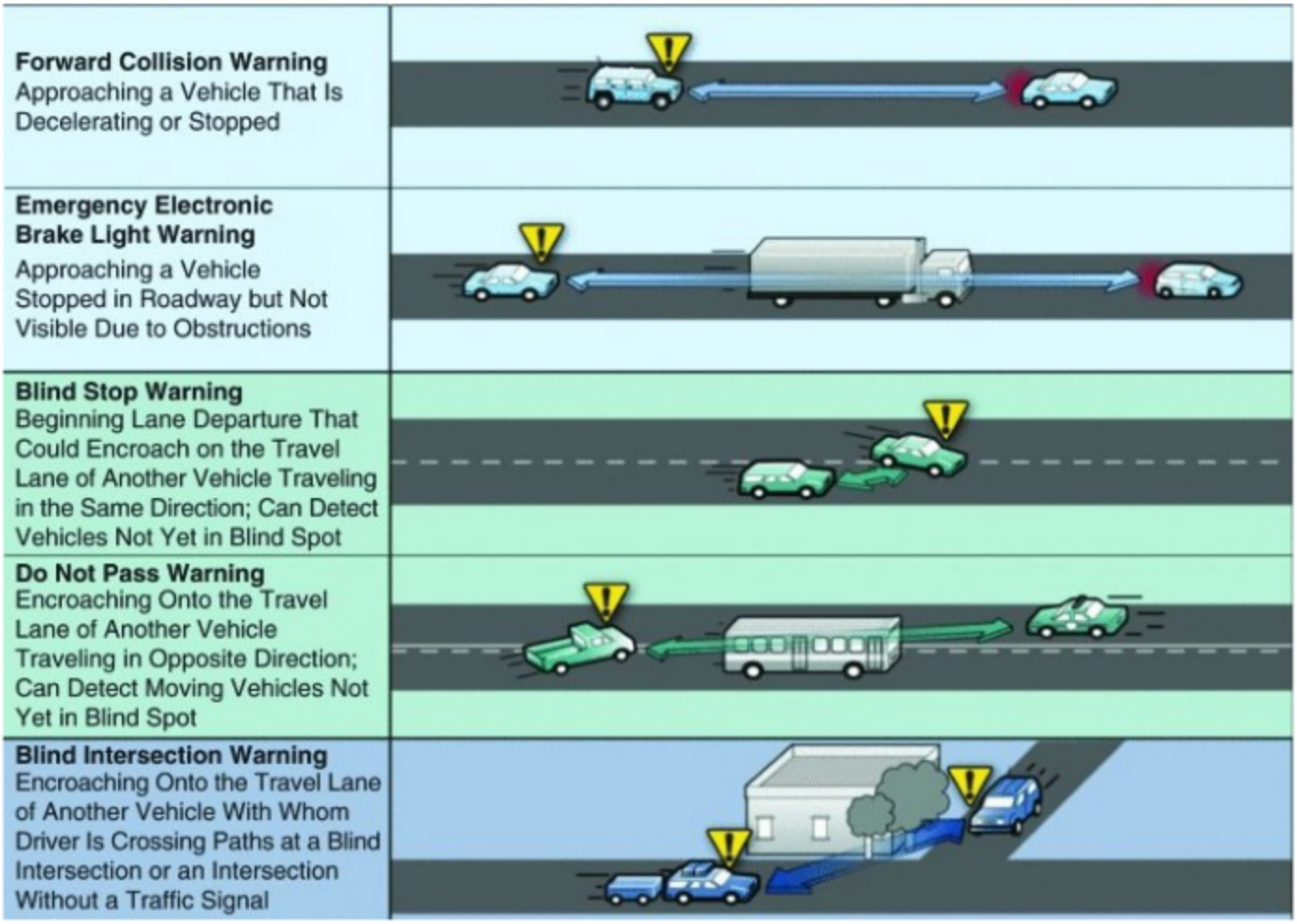

Cameras can only detect what they can see (LOS) V2V can often penetrate obstructions (NLOS)

  - V2V is expected to have the largest share of the CV market

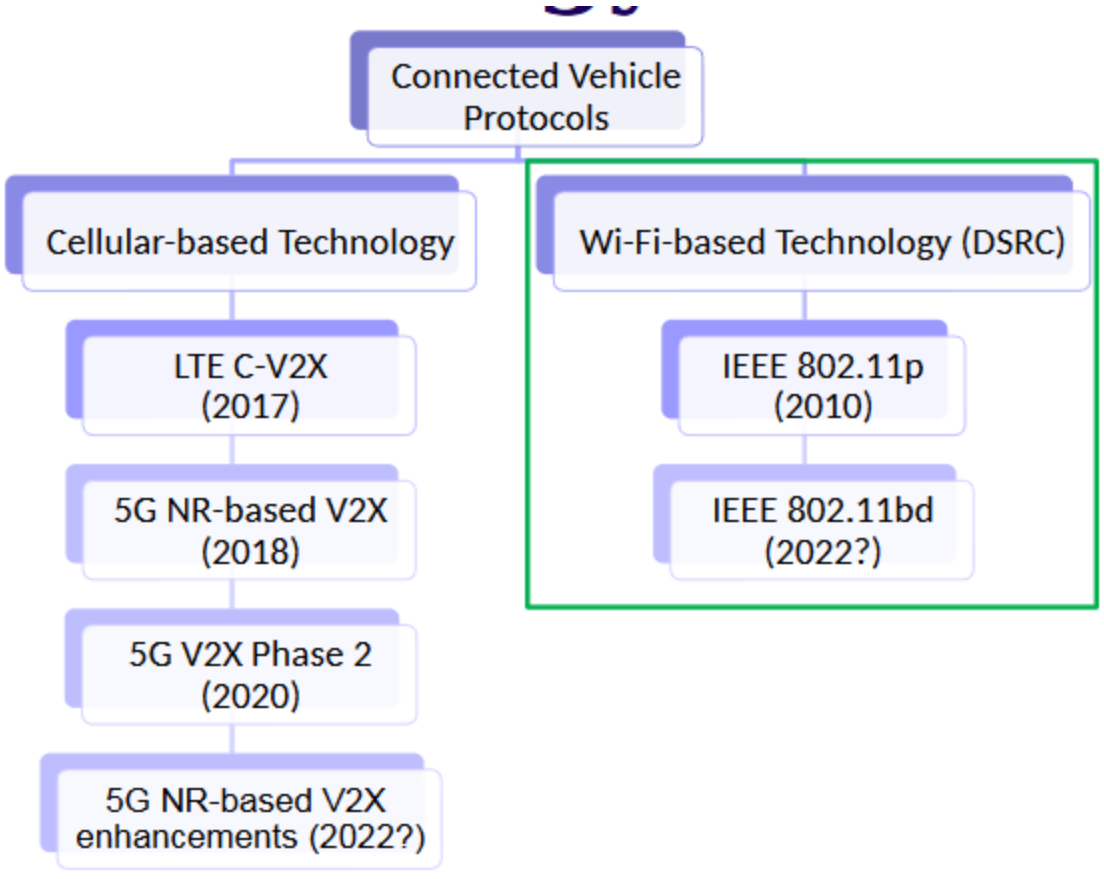
Basic Safety Messages (BSMs)

- Broadcasted periodically by each vehicle
  - Contains position, velocity, direction, acceleration, ...
- BSM examples
  - Forward Collision Warning
  - Emergency Electronic Brake Light
  - Blind Spot Warning
  - Do not Pass Warning
  - Left Turn Assist

- Intersection Movement Assist



V2X Technology Evolution



DSRC Basics

- Dedicated Short-Range Communications
  - Commonly deployed in EU and Japan
    - Somewhat limited in the US, < 0.0057% of the current 274 million vehicles on the road
  - Based on Wi-Fi technology (IEEE 802.11p or 802.11bd)
    - Layers 1 & 2 (PHY and MAC)
- Network and transport layers, and security services: IEEE 1609 family
- Payload definitions and performance requirements: SAE standards

IEEE 802.11bd (2022?)

- Enhancements for next-gen V2X
  - Maneuver, live camera feeds, platooning, remote driving, ...
- Design goals
  - Latency < 5ms
  - Double the throughput of 802.11p
  - Double the relative velocities to 500 km/h
  - Double the communication range to > 1 km
  - Coexistence & backward compatibility
- How? Using advanced Phy-layer tech

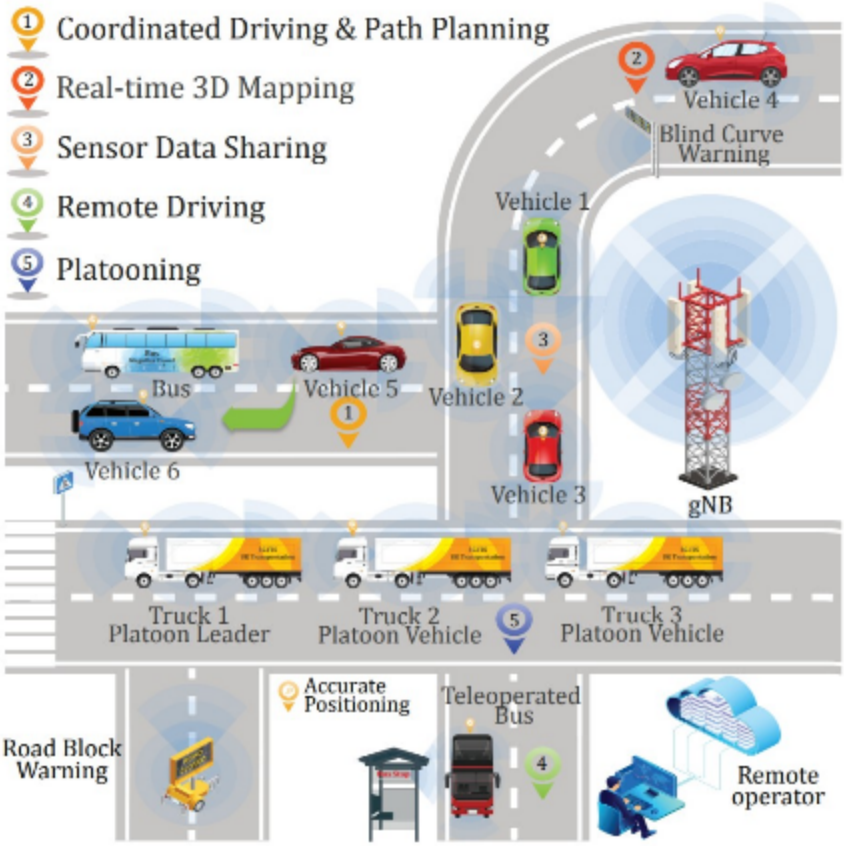
C-V2X

- 3GPP Cellular V2X
  - Release 16 (2020): platooning, automated/remote driving
  - Direct communication vs. Network communication
- Direct C-V2X compared with 802.11p-based V2X
  - Increases communication range
  - Provides better non-line-of-sight (NLOS) performance
  - Enhances reliability and latency with low complexity

5G New Radio (NR) V2X

- NR-V2X
  - Phy & MAC layers
  - Upper layers: like DSRC
    - IEEE 1609
    - SAE
- Advanced use cases
  - URLLC for latency

- eMBB for 3D maps



V2V Security

Possible Attacks

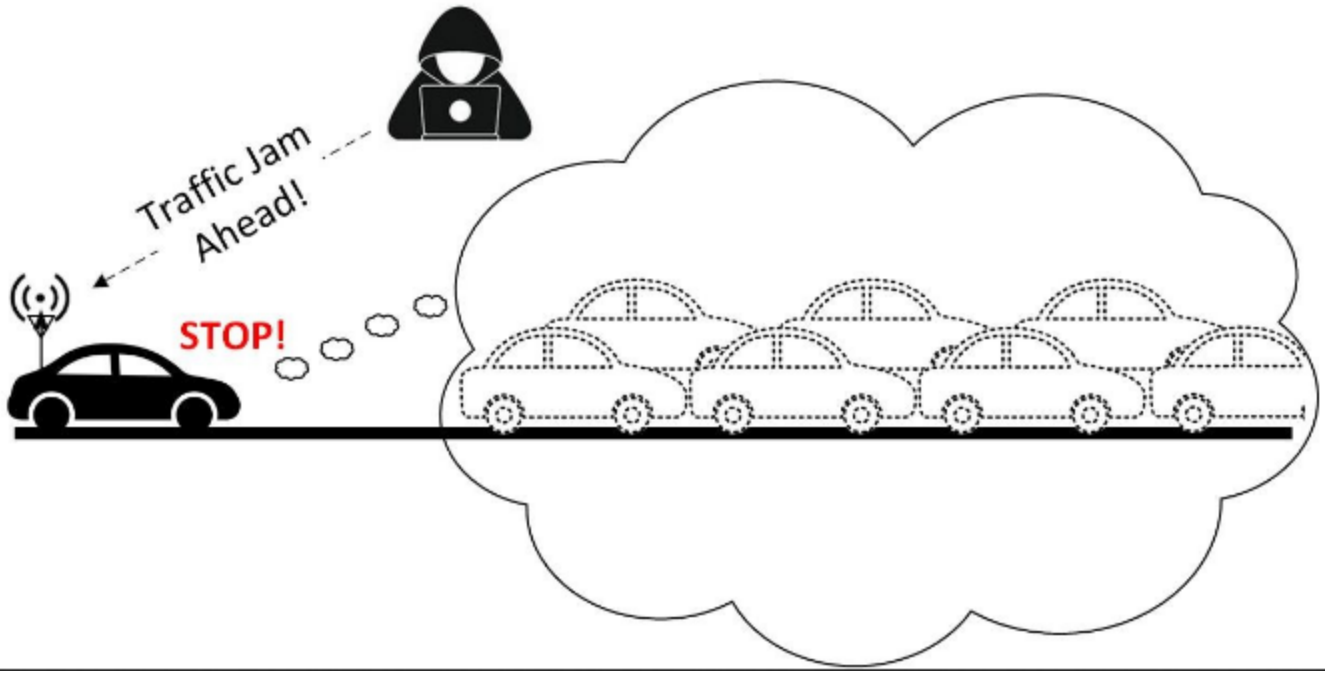
- V2V creates new attack surfaces!
  - Eavesdropping and tracking (identity,velocity, trace, etc.)
  - Spoofing, including replaying (manipulated) messages
  - Jamming
- BSM-specific attacks
  - Spoofing, message modification, replay, etc.
  - Can be life threatening, specifically for autonomous vehicles

Attack Example 1

- With jamming and then BSM spoofing, an attacker can feed false information and cause an incident

Attack Example 2

- Falsified BSMs indicating a traffic jam ahead could cause vehicles to stop suddenly for no reason



Security Requirements for V2V

1. A message originates from a trustworthy and legitimate vehicle
2. A message is no modified between sender and receiver - integrity
3. Misbehaving units are removed from the system
4. Tracking vehicles is not possible beyond a short interval
5. Life-long solutions

BSM Authentication and Integrity

- Achieved by using Elliptic Curve digital signature algorithms (ECDSA)
    - Includes time and location (to prevent replay/relay attacks) Defined in IEEE 1609.2 standard
- Uses PKI and (short) certificates to sign BSMs
    - A public-key infrastructure (PKI) is needed to verify the certs of the public keys
    - Why using asymmetric keys instead of symmetric ones?
    - Short-lived pseudonym certificates to prevent tracking

V2X Public Key Infrastructure