MODULE - 5

SECURITY IN CURRENT DOMAINS

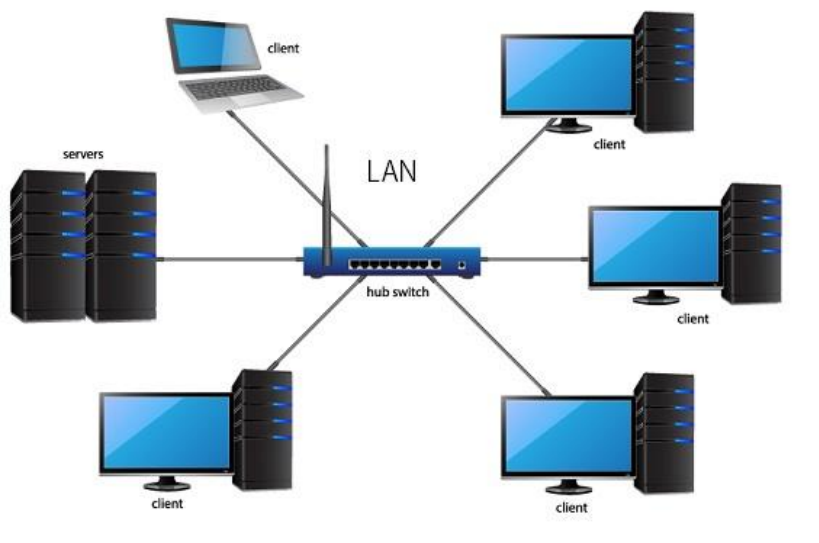
Muneera Hashim
Associate Professor
Dept. of Computer Science
Younus College of Engineering and Technology

Contents

- LAN
- Wireless LAN
- Wireless LAN Security
- Authentication using WEP
- Authentication using 802.11i
- Encryption for message integrity using WEP
- Encryption for message integrity using 802.11i
- WLAN Vulnerabilities
- Cellphone Security
- GSM and UMTS

Local Area Network

- A LAN is a network of computers located within a small physical area such as a school, a company, or a campus in order to enable the sharing of data and resources



LAN Technology

- The policy or the rules based on which the network elements of the LAN communicate with each other is known as LAN technology
- Many LAN technologies are available like
  - IEEE 802.3 CSMA/CD Ethernet
  - IEEE 802.4 Token ring
  - IEEE 802.5 Token bus
- Ethernet is the widely accepted standard because of its speed, cost and ease of installation
- As internet is the communication protocol used for the world wide network, ethernet is the communication protocol used for LAN

LAN Topology

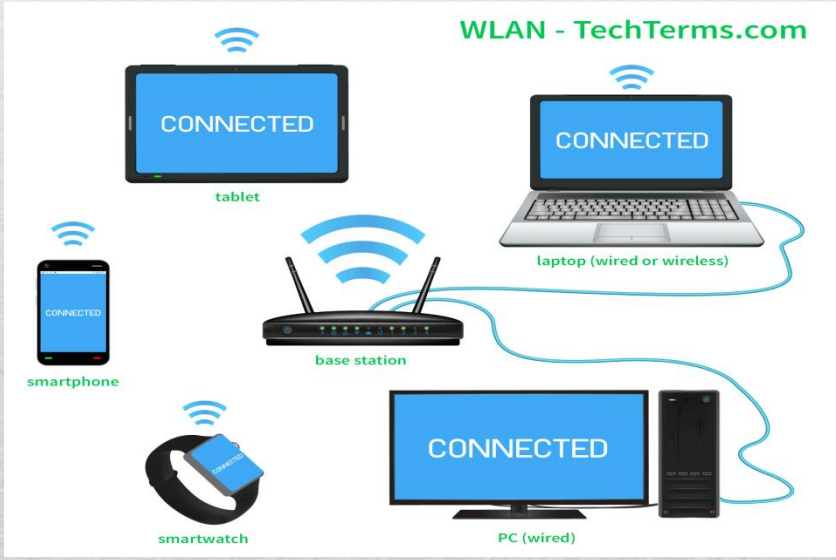
- Topology refers to the geometric arrangements of the network elements
- 4 types of topologies are available for LAN
  - bus
  - ring
  - star
  - mesh

Components of a LAN

- Hardware Components
  - PCs, workstations, all equipped with NIC
  - Server system
  - Ethernet cable and RJ45 connector
  - Hub or switch
  - Other network elements like printers, scanners, etc
- Software Components
  - NIC drivers
  - NOS for clients and servers
  - Networking protocol (TCP/IP)
  - Application software (email, browser, etc)

Wireless LAN

- A Wireless LAN is a network of computers or devices that moves within a limited area such as a school, a company, or a campus in order to enable the sharing of data and resources using wireless means of communication



Wireless LAN Technology

- The policy and rules that govern the communication of entities inside a WLAN is known as the WLAN technology
- Majority WLAN follows IEEE 802.11 standards
- In all 802.11 wireless implementations, Access Point (AP) is the central node
- It acts as an interface between the wireless network and the underlying wired network
- All components that can connect to the local network using the wireless medium are referred to as stations
- All stations must associate to some AP in order to communicate within the network

Components of a WLAN

- Hardware Components:
  - Mobile Stations equipped with WNICs
  - Access points
  - Routers
  - Repeaters
  - Antennae

Types of WLAN

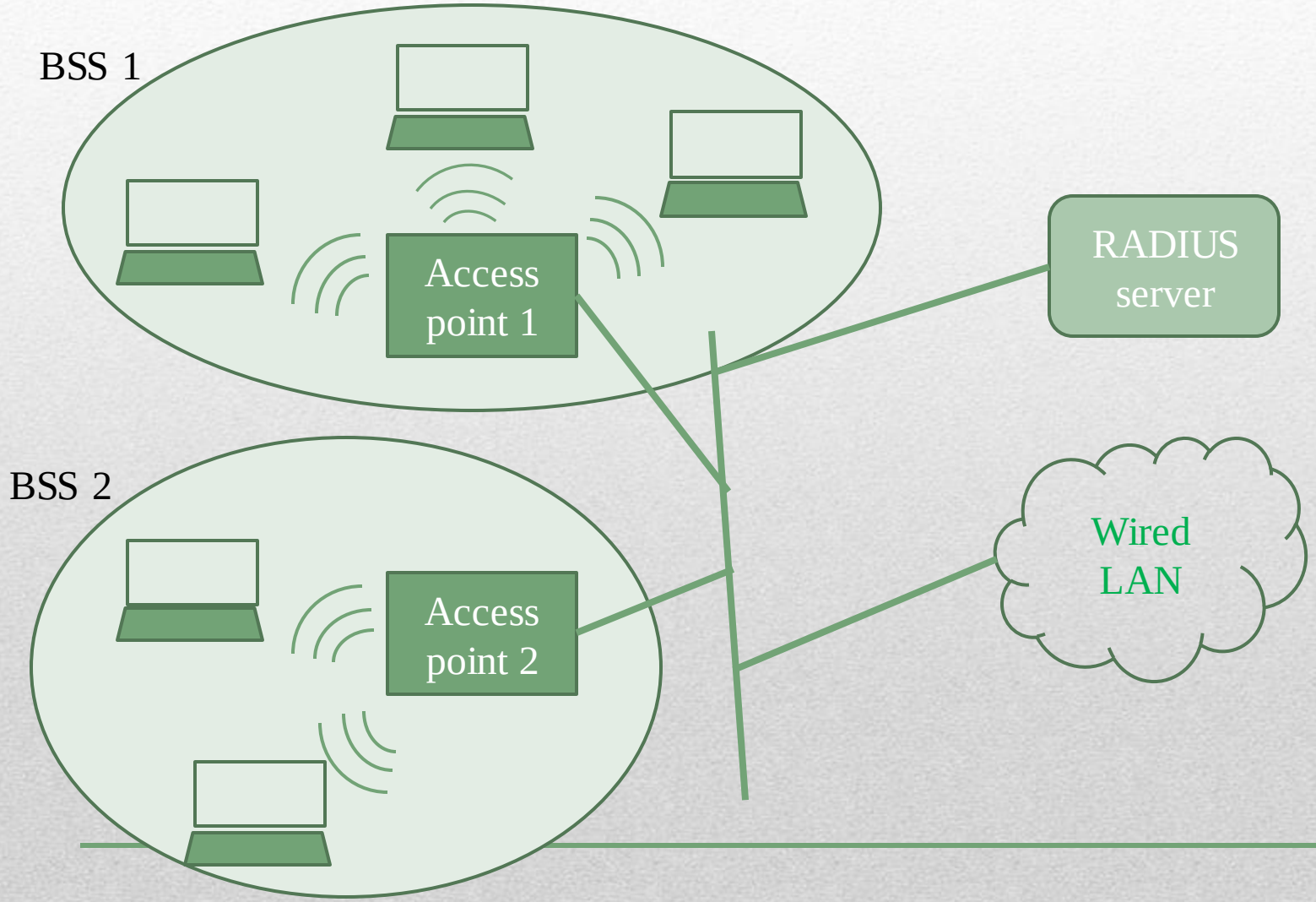
There are 2 types of wireless LANs

1. Adhoc n/w WLAN
   - Mobile stations communicate directly without the intervention of any access point
2. Infrastructure WLAN
   - Stations of the WLAN sends data to the Access point which in turn forwards the data to the destination or another access point that can forward data to the destination

Infrastructure WLAN

- Hence infrastructure WLAN contains wireless mobile stations (MS) connected to access points (AP)
- All the stations together with their AP is referred to as a basic service set (BSS)
- The union of all BSSs forms the extended service set (ESS)
- The APs of the different BSSs are connected using a wired network
- MS and AP of an ESS is uniquely identified by a 48 bit MAC address
- Each AP is also identified by service set ID (SSID) a unique string of length 32 characters

Infrastructure WLAN



WLAN - How it works?

- To become a part of a WLAN, the mobile station must associate with some AP
- At any point of time, a station can associate with only one AP
- The APs keep broadcasting a special kind of frame called Beacon at regular intervals
- When a mobile station is powered up it senses the wireless medium for any beacon frames
- If not found, the station can send a *probe request* frame in response to which, AP sends a *probe response* frame
- If a station finds many APs in its locality, it can choose the one that it desires
- The station sends a *associate request* frame to the AP with which the station wishes to associate with
- The AP responses with a *associate response* frame if it accepts the request
- All frames released by APs will contain the SSID of the AP
- Before association, the station must authenticate itself to the AP

Security

- To assure security in normal LANs, Ethernet has security structures like authentication server (AS) and remote authentication dial in user service server (RADIUS)
- RADIUS provides Authentication/ Authorization/ Accounting (AAA)
- In order to assure security in WLAN new features must be added into the existing security structure

Confidentiality

- For ensuring confidentiality of messages – user msgs or control msgs – we use encryption
- Encryption is the process whereby plain text is converted into cipher text using some key to protect the privacy of the data transmitted; only authorised persons can decrypt the message using the key, back to original plain text

Encryption

- Data encryption ciphers are grouped into two categories:

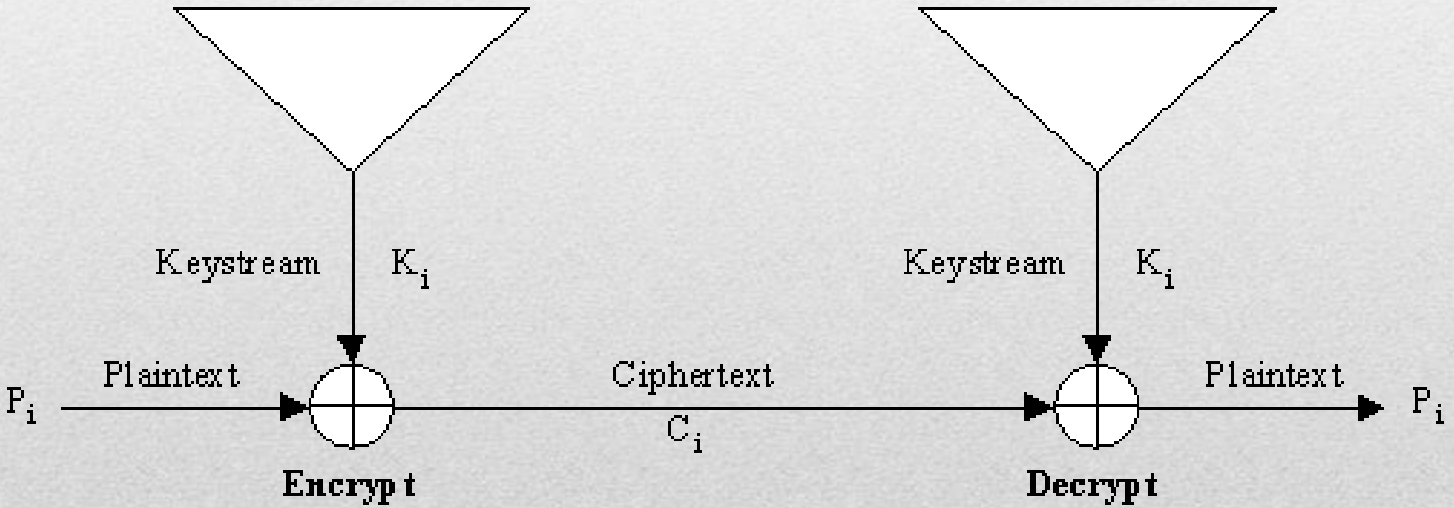
1. Stream ciphers: A stream cipher is a single-character-in, single-character-out cipher; it does the encryption one character at a time
2. Block ciphers: A block cipher encrypts whole blocks of data at a time

- We will focus on the stream cipher since stream ciphers are more suitable for hardware implementation and real-time systems where bits of data are received serially

Stream Cipher

- An example of a stream cipher implementation is the XOR algorithm
- In this implementation, the keystream generator outputs a stream of bits: $k_1, k_2, k_3, \ldots, k_i$.
- Bits of the keystream is XORed with a stream of plain text bits $p_1, p_2, p_3, \ldots, p_i$ to produce the stream of cipher text bits $c_1, c_2, c_3, \ldots, c_i$
- This operation is described by the formula: $c_i = p_i \oplus k_i$
- To recover the plaintext bits at the decryption end, the ciphertext bits are XORed with an identical keystream. This operation is described by: $p_i = c_i \oplus k_i$.

XOR Stream Cipher



AUTHENTICATION USING WEP

Pre-WEP authentication

1. SSID is used for authentication
   - An attacker can easily sniff that
2. APs maintain a list of MAC addresses. Only they are permitted to join WLAN.
   - Again, MAC address can be sniffed and spoofed

Wired equivalent privacy (WEP)

- Wired Equivalent Privacy (WEP) is a security standard designed to provide wireless networks with comparable security to that of wired networks
- WEP employs Shared Key Authentication to ensure that only authorized clients can access the network
- It also uses encryption to keep the data safe while it is in transit over a wireless network
- WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity

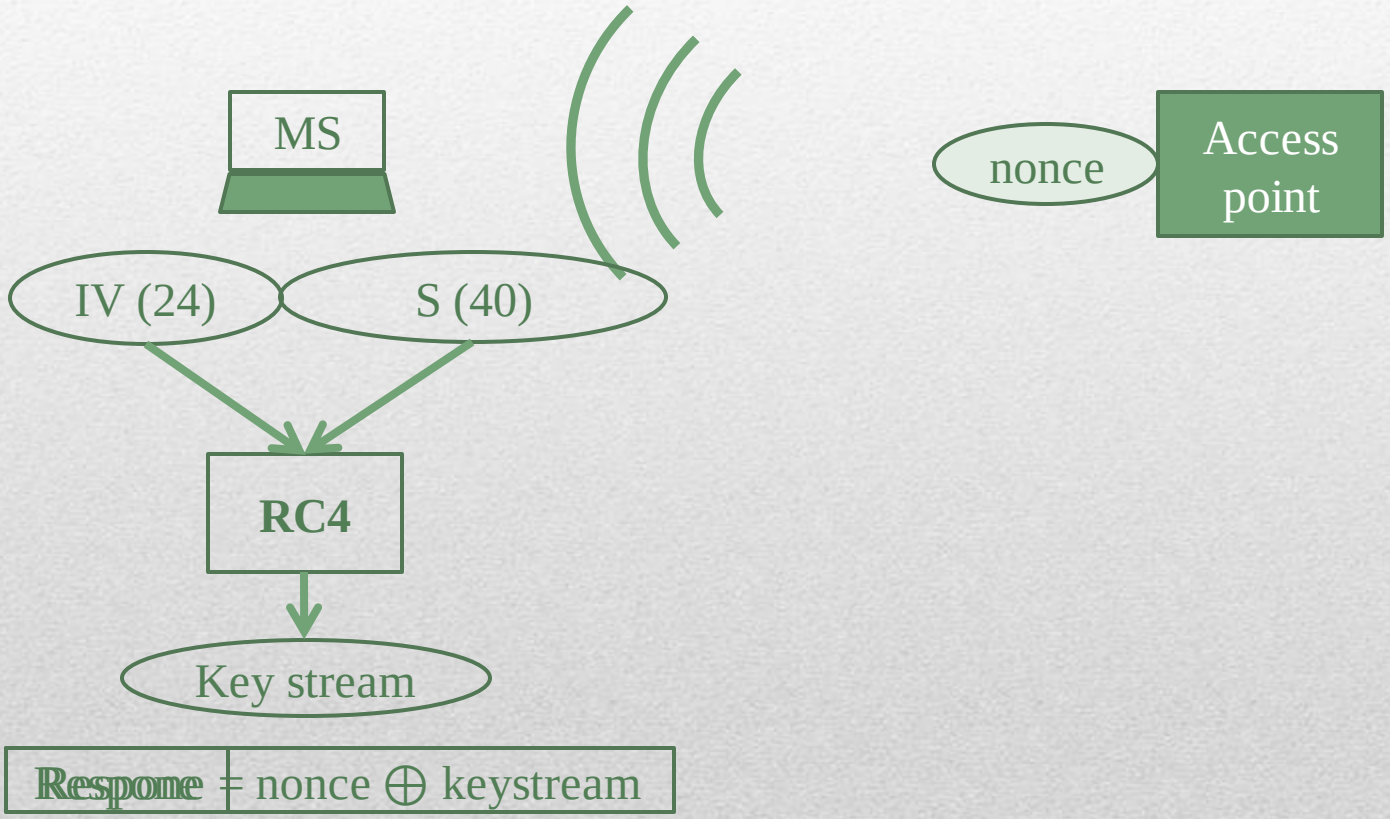
WEP Authentication process

- MS authenticates to AP by challenge response
- AP generates a challenge (nonce) & sends to MS
- Challenge is an encrypted phrase, which the MS must decrypt and send back to AS to prove that the MS has got the right key in hand
- Once identity is proved, MS can enter the network and communicate with peers

WEP Authentication details

- Every MS is provided with S and IV
  - S → shared secret key (common to all in WLAN)
  - IV → initialization vector (configured by manufacturer of WLAN card)
- MS uses RC4 to compute the 64 bit keystream(KS) which is a function of 40 bit secret S and a 24 bit initialization vector IV
- MS then XORs the challenge (received from the AP) with the keystream and sends back the result as response
- Response = challenge $\oplus$ keystream(S, IV)

WEP Authentication



Vulnerability of WEP

- An attacker monitoring a challenge response pair can easily calculate the keystream
- He can then easily authenticate himself to AP
- Or else he can deduce secret S by eavesdropping on several challenge response pairs and employing a dictionary attack
- WEP gives no support for authenticating an AP; an attacker can simply masquerade as a genuine AP and open door for man in the middle attack

AUTHENTICATION USING 802.11i

802.11i

- 802.11i uses IEEE 802.1x protocol
- Support authentication at link layer
- 3 entities
  - Supplicant (Wireless Station, WS)
  - Authenticator (Access Point, AP)
  - Authentication server (AS)
- Authentication methods are defined by Extensible authentication protocol (EAP)

- AP broadcasts its beacon frames
- WS sends associate request frame to an AP
- AP accepts the request and associates the WS
- Here authentication takes place after associating the WS to the AP
- EAP is used to authenticate WS to the AP
- EAP is not actually a protocol, it is a framework on which authentication protocols can be built

Extensible Authentication Protocol (EAP)

- Main authentication methods of EAP
  1. EAP – MD5
  2. EAP – TLS
  3. EAP – TTLS
  4. EAP – PEAP

EAP – MD5

- Basic of the EAP methods
- AS challenges WS to transmit MD5 hash of user's password
- WS sends hash of the password
- Insecure method
  - Attacker can easily eavesdrop on the message exchange and replay the hashed password

EAP – TLS

- Most secure of the EAP methods
- Based on SSL / TLS protocol
- SSL → Secure Socket Layer
- TLS → Transport Layer Security
- Provide mutual authentication and agreement on a master session key
- Requires all APs & WSs to have digital certificates
- Not feasible to impart a digital certificate for all stations

EAP – TTLS

- TTLS → Tunneled TLS
- Requires digital certificate only for the AP
- AP authenticate itself to WS & make a secure tunnel between them
- Through this tunnel WS authenticate itself
- WS may transmit attribute value pairs like
  - user_name = muneera
  - password = hadi2017
- AP forward this information to RADIUS server

EAP - PEAP

- PEAP → protected EAP
- Proposed by Microsoft, Cisco, RSA security
- Similar to EAP-TTLS
- Secure tunnel is used to start a second EAP exchange where WS authenticate itself to AS

Key hierarchy

- 2 types of keys are used in WLANs
  1. Pairwise keys : to protect messages between WS & an AP
  2. Group keys : to protect broadcast communication from an AP to multiple WSs

Generate pair-wise keys

- For a pair of AP and WS to communicate, a pair-wise key is generated for each session
- In order to assure security, key generation is done through a series of actions (4 way handshake)

Generate Pair-wise Master Key (PMK)

- Initially the AS and the WS agrees upon a Master Session Key (MSK) which is then shared to the AP by the AS
- WS and AP now have the common MSK from which they derive the same PMK
- 256 bit Pairwise Master Key (PMK) is then used for the WS and AP to communicate with each other

Optional

- Instead of this fresh-key generation method for each session, AP and WS may keep a Pre-Shared Key (PSK) which will be used as the PMK
- However, this brings about some risk
- Hence not used much

Generate PTK

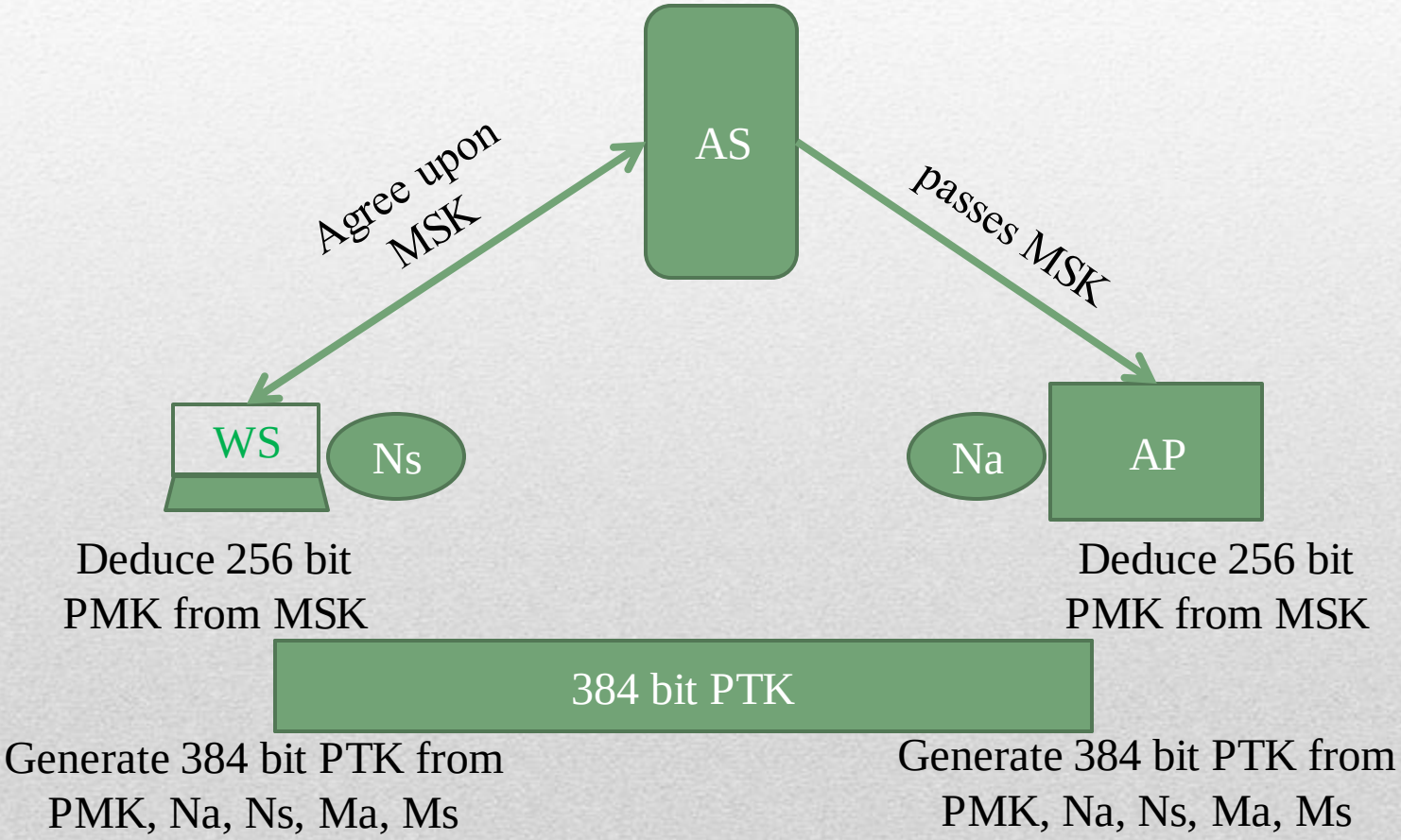
- A 384 bit pairwise transient key (PTK) is generated as a pseudo random function of PMK, Na, Ns, Ma and Ms
  - PMK→ pairwise master key
  - Na→ nonce chosen by AP
  - Ns→ nonce chosen by WS
  - Ma→ MAC address of AP
  - Ms→ MAC address of WS

Retrieve TK, KCK & KEK

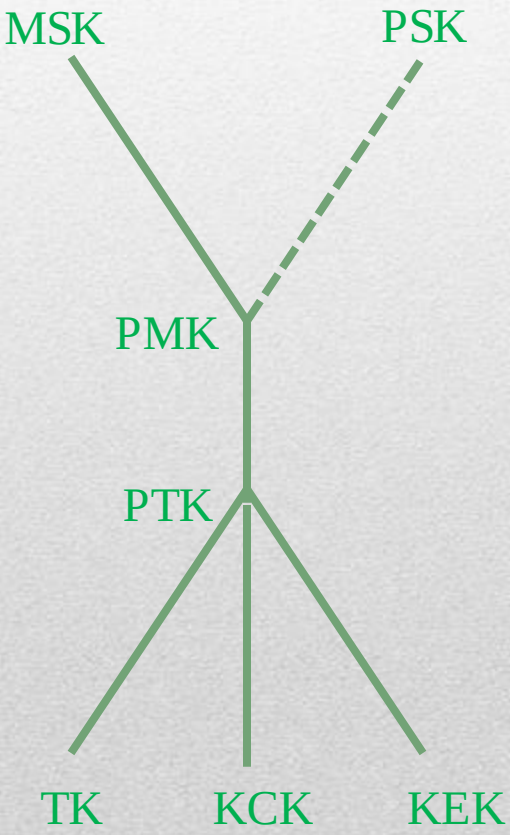
- The 384 bit PTK is separated into 3 chunks, each of length 128 bits
  - Temporal Key (TK): For data protection & integrity between AP & WS
  - Key Confirmation Key (KCK): For the integrity of some messages send during the 4 way hand shake
  - Key Encryption Key (KEK): Encrypt the message containing the group key

Key generation

First half of the hand shake process; exchanging nonce



Key hierarchy

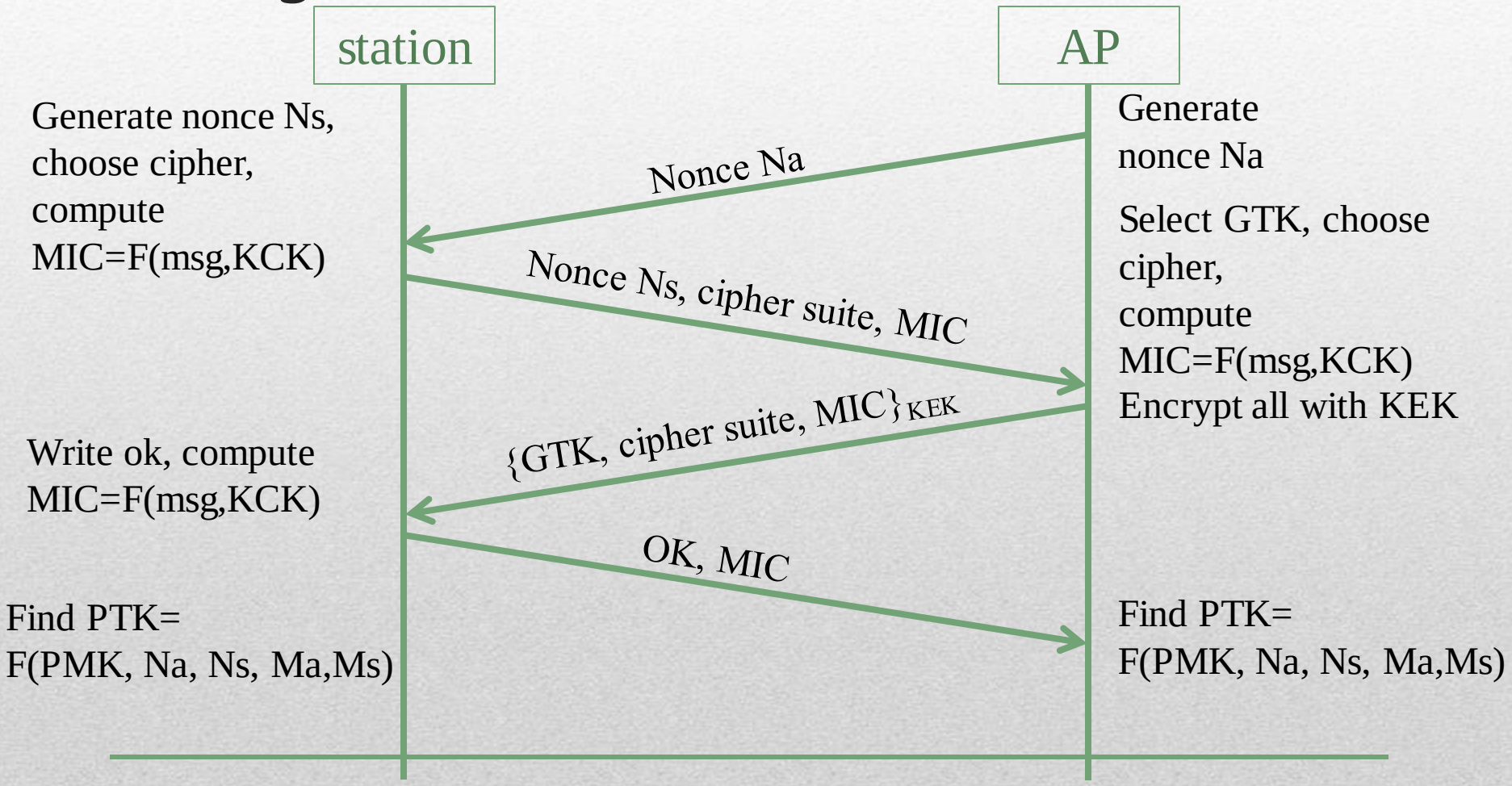


MSK – Master Session Key
PSK – Pre Shared Key
PMK – Pair-wise Masker Key
PTK – Pair-wise Transient Key
TK – Temporal Key
KCK – Key Confirmation Key
KEK – Key Encryption Key

4 way handshake

- Goals
  - Exchange the nonce and then derive PTK from PMK at both sides
  - Verify cipher suites passed in the Beacon and Associate-request frames
  - Pass the group key (GTK) from AP to WS

4 way handshake in 802.11i

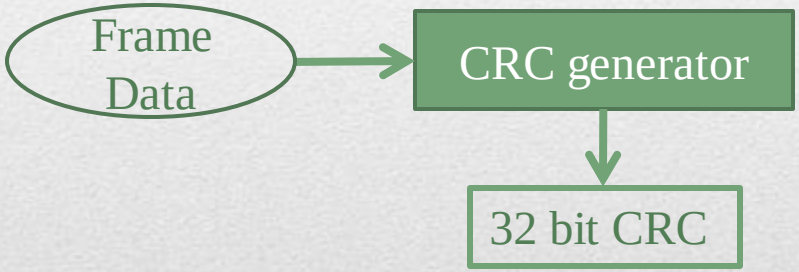


ENCRYPTION FOR MESSAGE CONFIDENTIALITY IN WEP

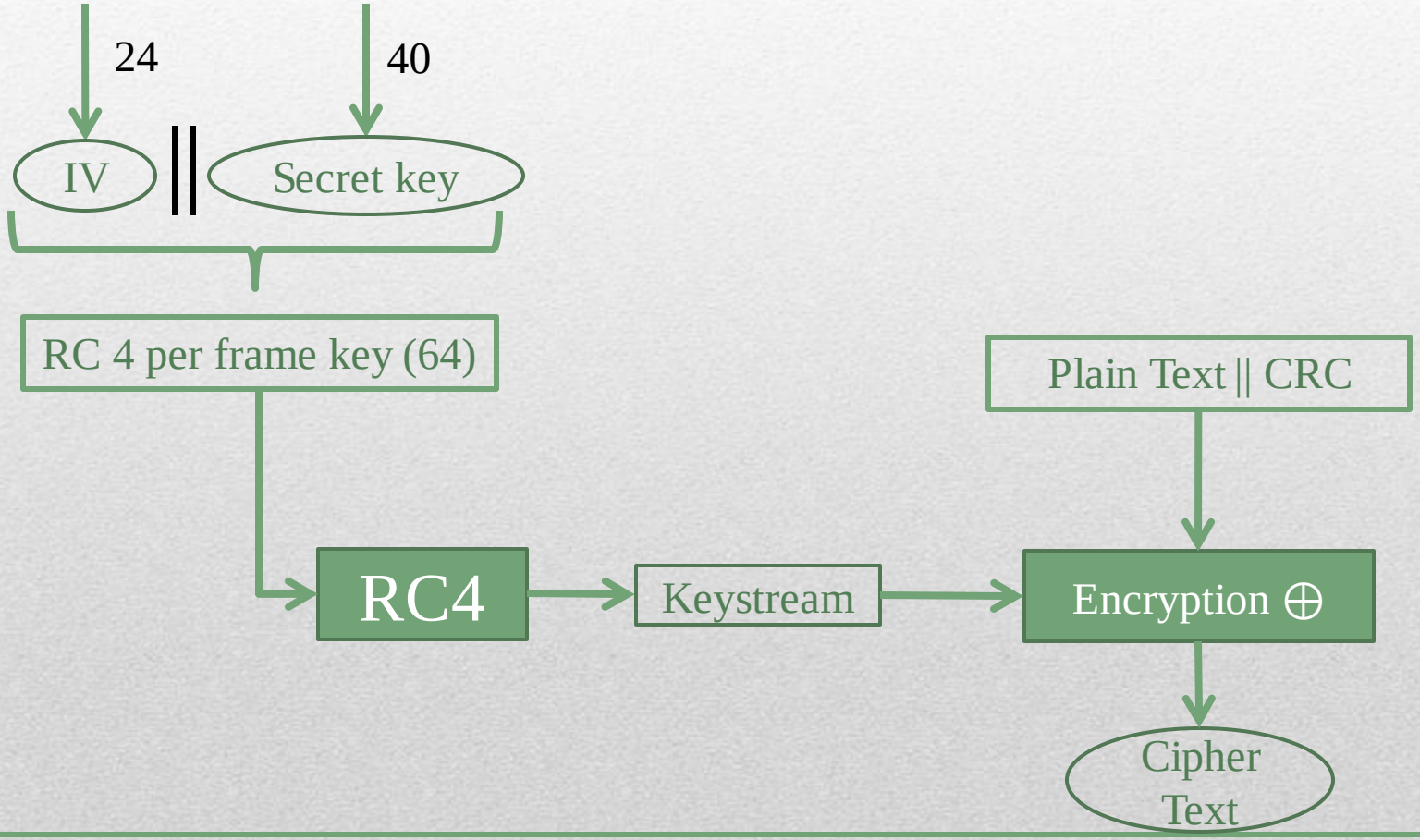
Encryption

- IV is appended to the S, using which RC4 generates a keystream
- The keystream is XORed with the plain text to generate the cipher text
- $C = P \oplus KS$
  - C → cipher text
  - P → plain text (message + 32 bit CRC)
  - KS → key stream (64 bit)
  - KS is a function of S and IV
  - S → secret key (40 bit)
  - IV → initialization vector (24 bit)
  - CRC →cyclic redundancy check

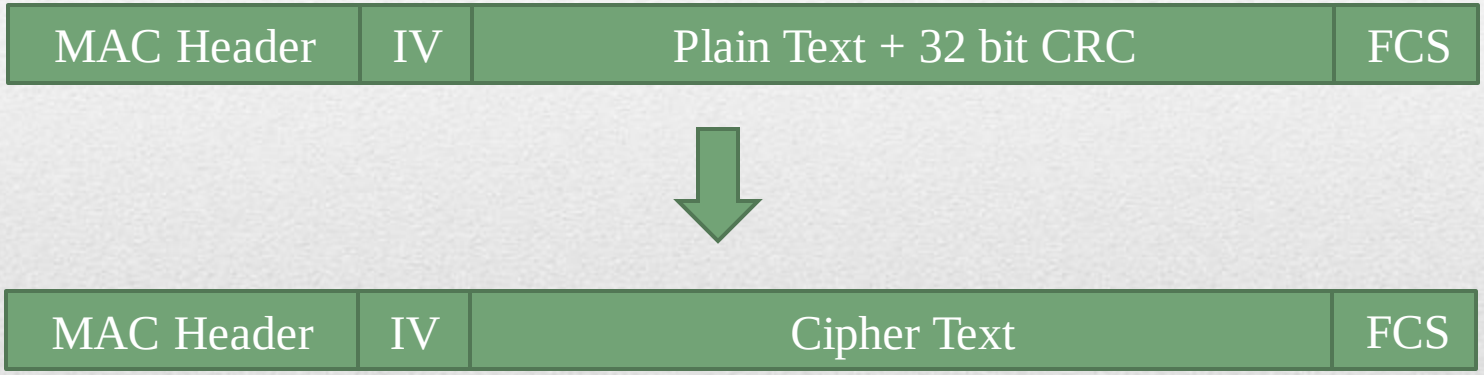
CRC generation



Encryption


24
40
IV
||
Secret key
RC 4 per frame key (64)
Plain Text || CRC
RC4
Keystream
Encryption ⊕
Cipher Text

WEP Frame


MAC Header
IV
Plain Text + 32 bit CRC
FCS
MAC Header
IV
Cipher Text
FCS

Decryption

- Decryption process is

$$P = C \oplus KS(S, IV)$$

Known Plaintext Attack

- Exploits the keystream re-use character
- There is a probability of re-using the same IV for different messages
- On a 10 Mbps channel, with an average frame size of 1000 bytes, some one who continuously eavesdrop for 4 hours may find two frames with same IV
- IVs are send as such in the frames
- Since an IV is 24 bit, 2^{24} different keystreams can be generated for a given secret S

- Suppose an attacker finds two frames that use same IV
- Let their cipher texts be C and C’
- Let P and P’ be their corresponding plain texts
- If he can know P or guess P by some means, then attack is straight forward
- He just have to XOR P with C and C’
- $P' = P \oplus C \oplus C'$
- To make things worse, most WLANs use same shared key for all stations and APs

Message Modification Attack

- Let the message send by a legitimate user be M_1FM_2 where M_1, F and M_2 are bit sequences
- Suppose the attacker wants to replace the bit string F with F'
- Such that the receives finally sees the message as $M_1F'M_2$
- For this the attacker needs to know only F and F'; No need to know M_1 and M_2

Steps involved

- First he stores the cipher text
- $((M_1 \; F \; M_2) \; || \; CRC \; (M_1 \; F \; M_2)) \oplus KS$
- Then he constructs a new string
- $0^{|M1|} \; || \; (F \oplus F') \; || \; 0^{|M2|}$
- Where $0^{|M1|}$ is a sequence of M_1 zeroes
- He then computes the CRC of his new string
- $CRC \; (0^{|M1|} \; || \; (F \oplus F') \; || \; 0^{|M2|})$

- Combines new string with its CRC
- $0^{|M1|} \,||\, (F \oplus F') \,||\, 0^{|M2|} \,||\, CRC(0^{|M1|} \,||\, (F \oplus F') \,||\, 0^{|M2|})$
- Finally XORs the cipher text with the combined string

$((M_1\ F\ M_2) \,||\, CRC\,(M_1\ F\ M_2)) \oplus KS \oplus (0^{|M1|} \,||\, (F \oplus F') \,||\, 0^{|M2|} \,||\, CRC(0^{|M1|} \,||\, (F \oplus F') \,||\, 0^{|M2|}))$

- Which is equal to $((M_1 \oplus 0^{|M1|}) \,||\, (F \oplus (F \oplus F') \,||\, (M_2 \oplus 0^{|M2|})) \,||\, (CRC\,(M_1\ F\ M_2) \oplus CRC(0^{|M1|} \,||\, (F \oplus F') \,||\, 0^{|M2|})) \oplus KS$
- Which is in turn equal to $((M_1\ F'\ M_2) \,||\, CRC\,(M_1\ F'\ M_2) \oplus KS$ which is finally send to the receiver

- At the receiver, the cipher text is decrypted to obtain the plain text ((M_1 F' M_2) || CRC (M_1 F' M_2)
- Since CRC matches with the plain text decrypted, receiver accepts it as the original message unaware of the modification made

FMS Attack

- Named after the founders Fluhrer, Mantin and Shamir
- By collecting a sufficient number of frames from the wireless medium bearing specific IVs, the encryption key used can be deduced

Solutions

- The RC4 turned out to be utter useless
- AES seemed to be a good choice for replacing RC4
- But the cost of replacing all hardware did not seem practical
- Hence solution was a firmware that can eliminate the vulnerabilities of RC4 and hence WEP
- 802.11i emerged as a solution

ENCRYPTION FOR MESSAGE CONFIDENTIALITY IN 802.11i

TKIP & CCMP

- The implementation of 802.11i was first done using RC4 and then later using AES
- TKIP uses RC4
- CCMP uses AES

Temporal key integration protocol (TKIP)

- It is a security protocol designed by 802.11i in order to replace WEP
- Also called as WPA (Wireless protected access)
- Uses RC4 itself; but in a better way
- Unlike WEP, TKIP do not simply append the IV to the secret key; instead it mixes the IV and secret key in a way so as to increase security
- Hence the probability for the keystream to repeat is very less in TKIP as compared to WEP

- TKIP generates a random & different encryption key for each frame sent
- Uses a process called two-phase key mixing
- Employs a frame sequence counter that generates a 48 bit sequence number (SN) for each frame which is used as IV
- Phase 1 uses a pseudo random function (PRF1) on 128 bit TK, sender's 48 bit MAC address and the 32 bits from the MS bytes of the SN

- Phase 1 outputs an 80 bit sequence which forms an input for phase 2
- Phase 2 uses a pseudo random function (PRF 2) on the 80 bit sequence and 16 bits from the LS bytes of the SN to generate a 104 bit output
- 24 bits from the SN appended with the 104 bit output of PRF 2 forms the final RC4 key

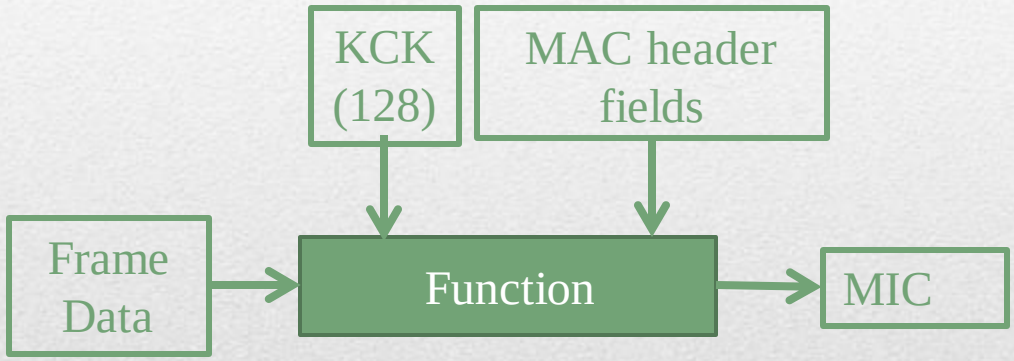
- Unlike WEP, TKIP does not employ CRC for message integrity check
- Instead it uses MIC which is computed as a function of data in the frame, some fields in the MAC header and KCK derived during the 4 way handshake process
- Unlike CRC, MIC is not a linear function

Advantages of TKIP

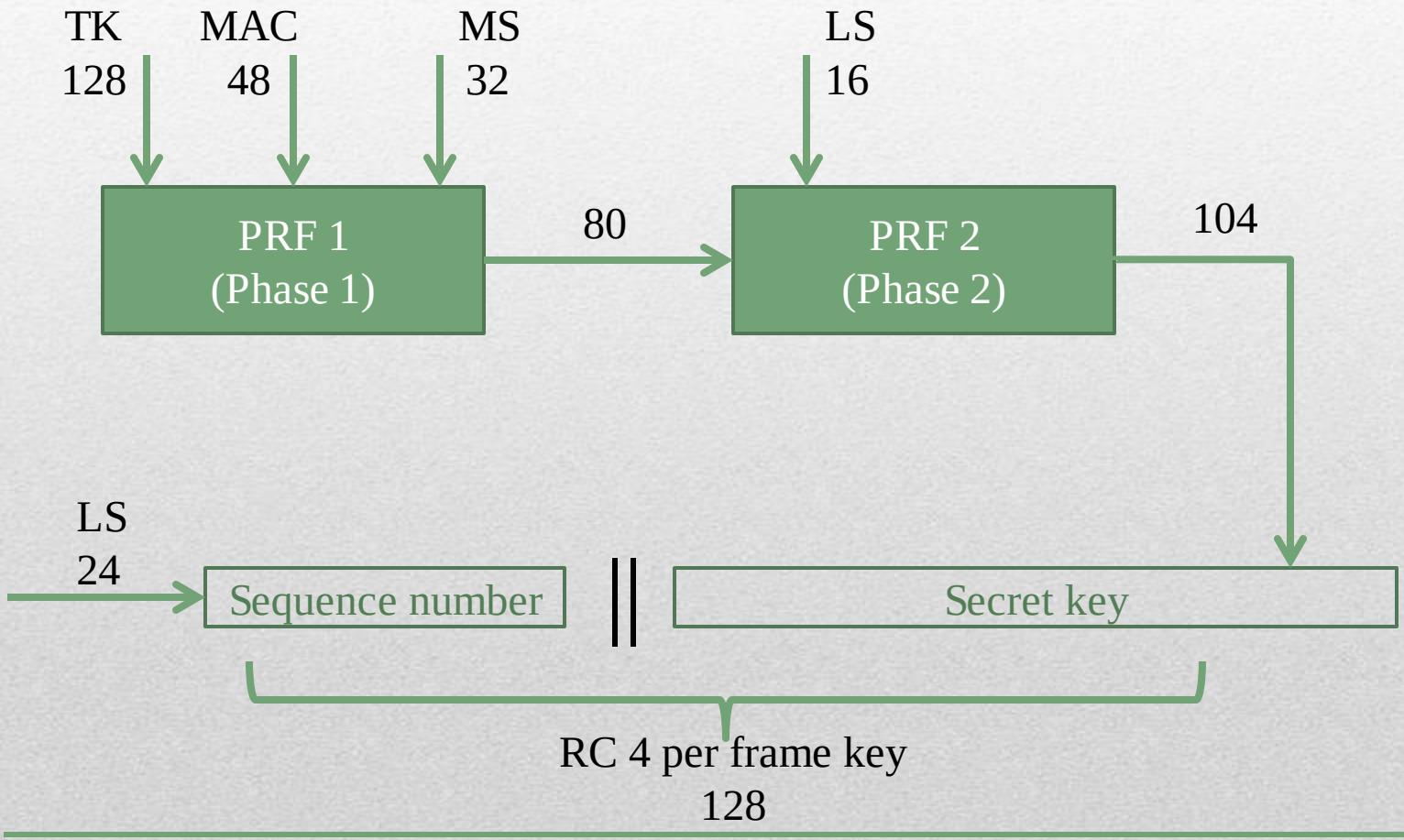
- Since the sequence number is transmitted within each frame, and the sender and the receiver keeps track of the number of the last frame send or received, the receiver accepts a frame only if its number is greater then the previous frame; this helps to protect from replay attacks
- The randomizing capability of the key mixing function and the large size of the keyspace narrows down the probability of two frames having same keystream

- Since the LSB of the sequence number is fed to PRF 2, output changes for each frame sent, thus letting a new key for each frame
- At the same time, since the MSB is fed to PRF1, it will change only after every 65536 frames, there by saving the computation time and overhead
- And finally MIC is efficient than CRC

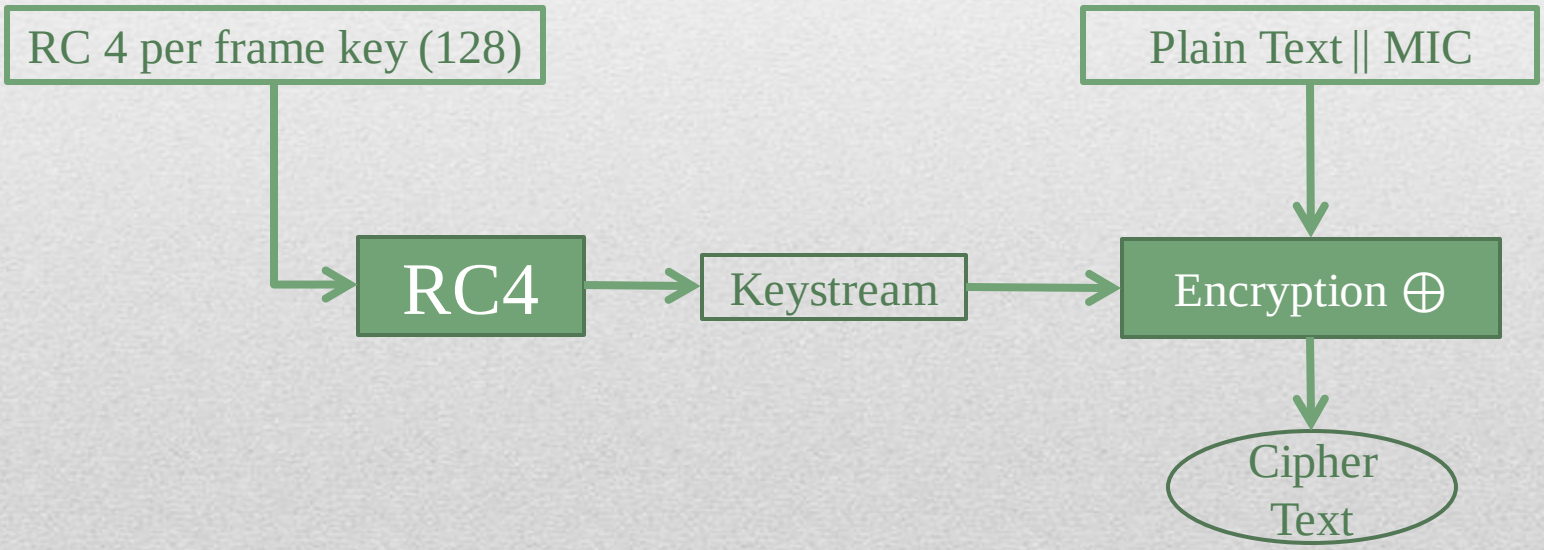
MIC computation



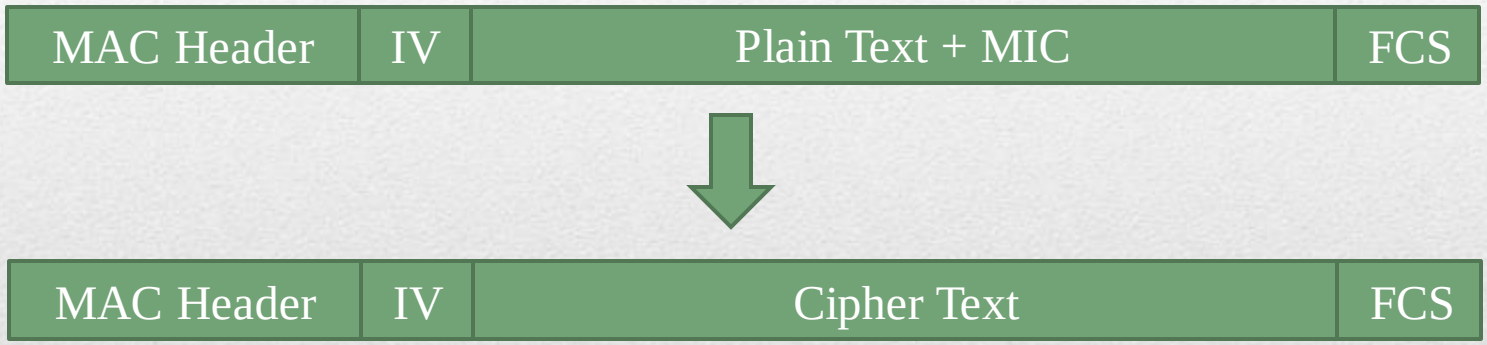
Two-phase key mixing



Encryption


RC 4 per frame key (128)
Plain Text || MIC
RC4
Keystream
Encryption ⊕
Cipher Text

TKIP Frame


MAC Header
IV
Plain Text + MIC
FCS
MAC Header
IV
Cipher Text
FCS

CCMP

- Counter mode with CBC MAC Protocol
- Also known as WPA-2
- Uses AES algorithm for authentication and message integrity
- Same key, TK is used for encryption and MIC computation
- Since AES itself is a block cipher, there is no need to compute a fresh key for each frame

- Like TKIP, CCMP initializes a 48 bit sequence counter when a session is started between a sender and a receiver
- Counter is maintained at both sender and receiver
- In CCMP, it referred to as Packet Number (PN)
- PN is send as a part of the CCMP frame
- PN is incremented for each frame sent
- Receiver accepts a frame only if its PN is greater than that of the previous one

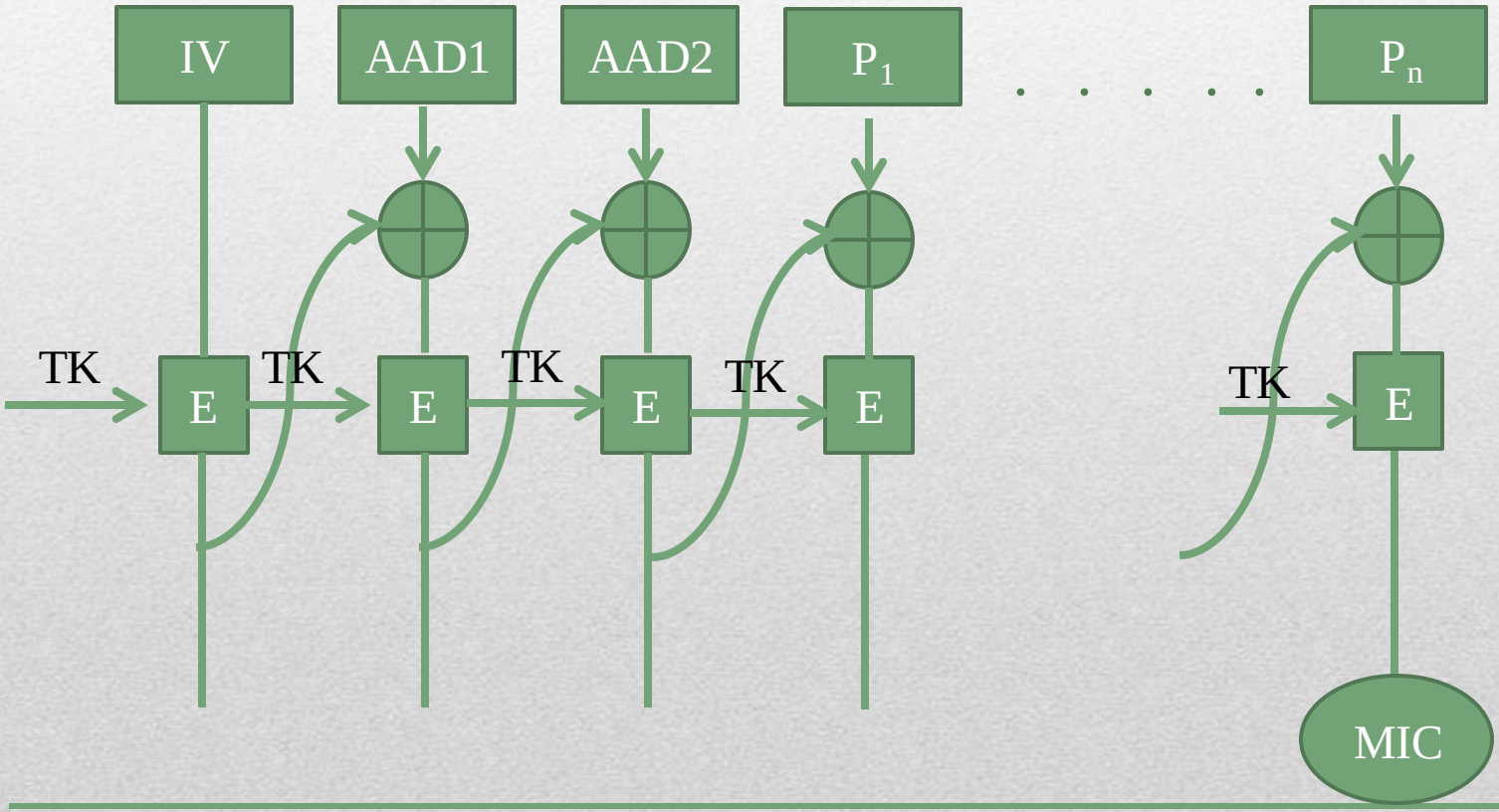
MIC Computation

- MIC is computed using AES in Cipher Block Chaining mode with block size, 128bits
- The 8 byte MIC is computed as a function of data of the frame, IV (nonce) and some fields from the MAC header such as MAC address, sequence control and frame type using the key TK

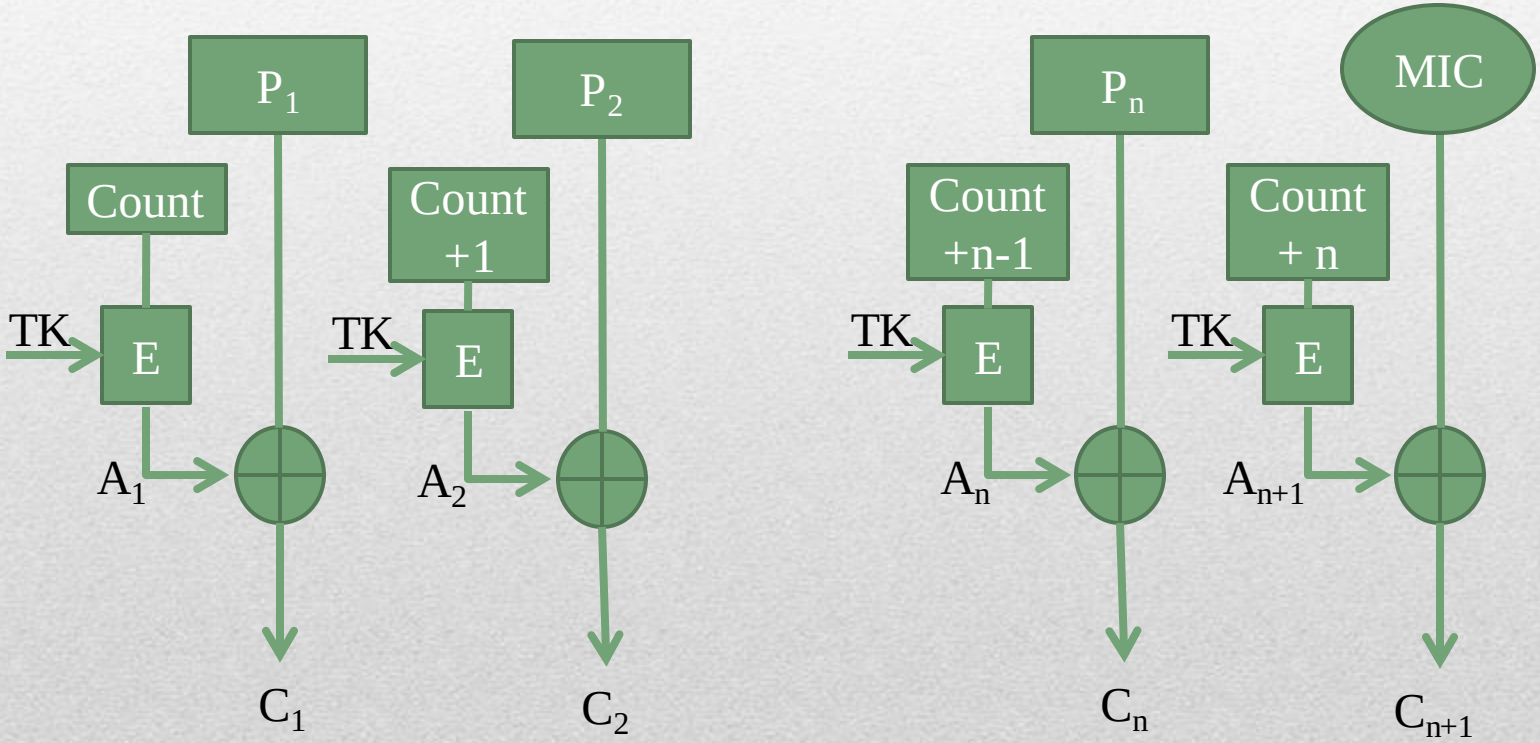
Encryption

- Frame data and the computed MIC are concatenated and encrypted using AES in counter mode
- Let n be the total number of blocks after concatenation
- The ith block is encrypted as:
  - $A_i = E_{TK}(PN + i * j)$
  - $C_i = Ai \oplus Pi$

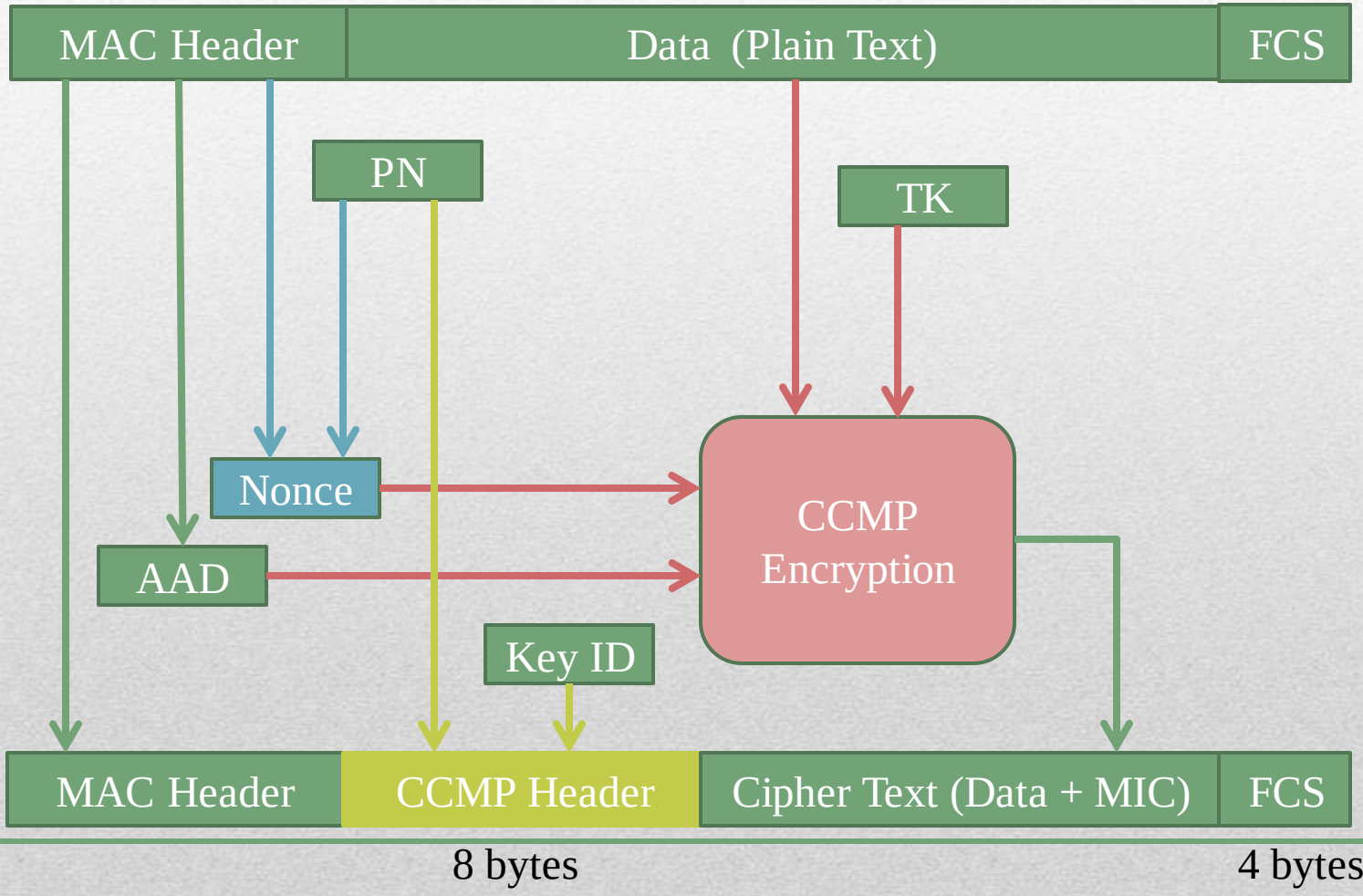
MIC Computation



Encryption


P1
P2
Pn
MIC
Count
Count +1
Count +n-1
Count + n
TK
E
A1
A2
An
An+1
C1
C2
Cn
Cn+1

CCMP frame


MAC Header
Data (Plain Text)
FCS
PN
TK
Nonce
AAD
CCMP Encryption
Key ID
MAC Header
CCMP Header
Cipher Text (Data + MIC)
FCS
8 bytes
4 bytes

WEP, TKIP, CCMP

	WEP	TKIP	CCMP
Authentication	WEP key	802.1x & EAP	802.1x & EAP
Encryption	RC4	RC4	AES
Message integrity	32 bit CRC	MIC	CCM
Key size	40 bits (S)	128 bits (TK)	128 bits (TK)
IV length	24 bits	48 bits (SN)	48 bits (PN)
IV & key combining	appending	2 phase key mixing	AES mixer
Key mgmt	-	4 way hand-shake	4 way hand-shake

WLAN Vulnerability

WLAN Vulnerability

- A wireless network is more prone to attacks than a wired network
- The medium access control (MAC) layer monitors and controls, access to the shared medium of the WLAN by the stations
- Protocols like ethernet (LAN) and 802.11 (WLAN) has a well defined set of rules that the nodes must follow so as to ensure the smooth functioning of networks

WLAN attacks

I. Frame spoofing
   1. Spoofing de-authentication frame
   2. Spoofing poll control frame

II. Violating MAC Etiquette
   1. Violating inter-frame spacing rules
   2. Abusing virtual carrier sensing

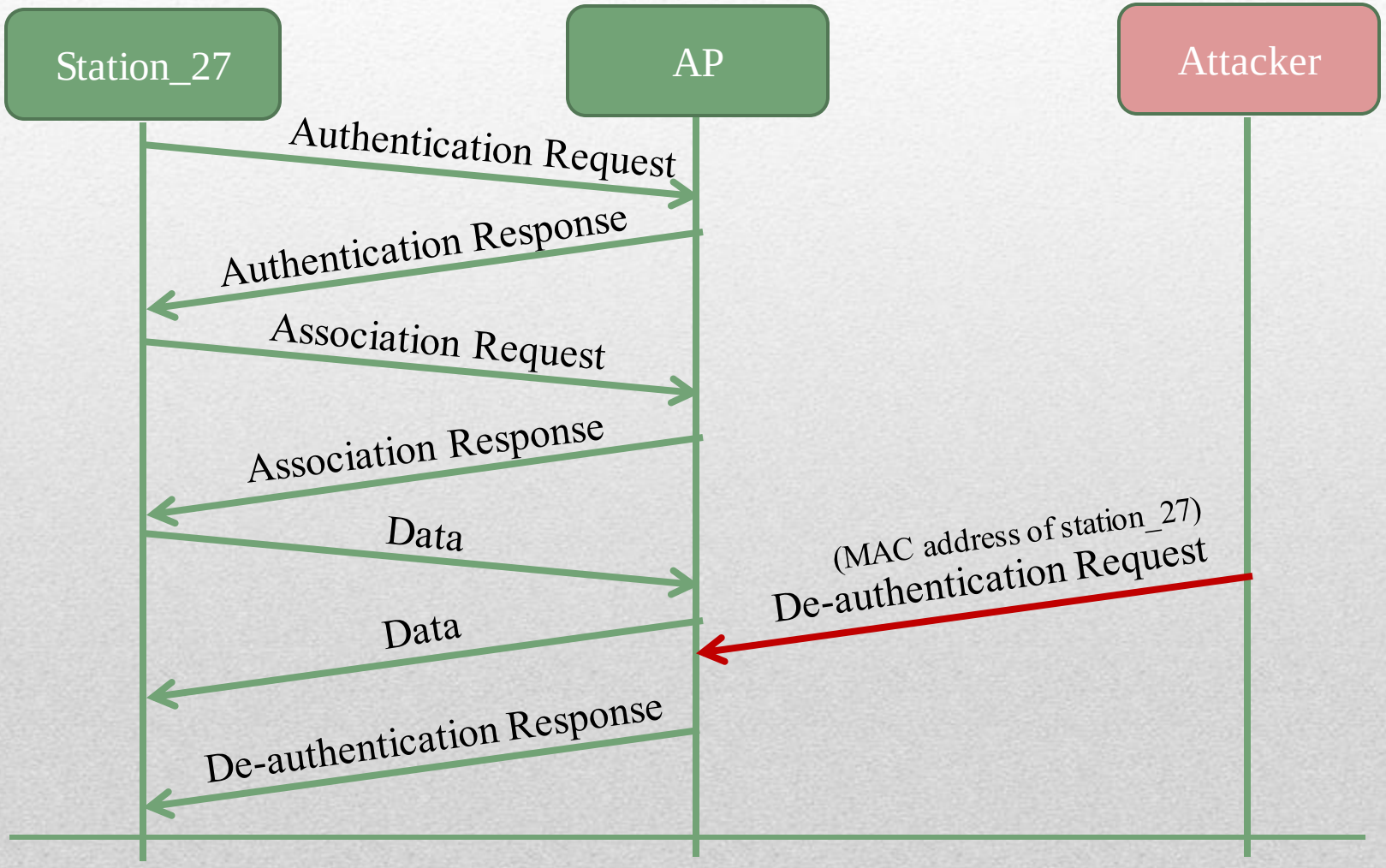
Frame spoofing

- Attacks exploit features of MAC protocol and disrupt communication between legitimate users by transmitting spoofed management and control frames
  1. spoofing de-authentication frame
  2. spoofing poll control frame

Spoofing de-authentication frame

- A station needs to authenticate and associate with an access point in order to enter the network for which they uses beacon, authentication and association frames
- similarly, to leave a network, a station may send a de-authentication frame indicating to terminate the connection
- The recipient identifies the sender using the 48 bit MAC address in the frame
- An attacker can spoof such a de-authentication frame by spoofing the sender address in the frame

- Hence premature termination of communication between AP and WS occurs
- For example, consider a frame with the sender and receiver addresses as
  - Sender Address: Station_27
  - Receiver Address: AP
- Upon reception of this frame, the AP thinks that station 27 wishes to terminate the existing connection
- AP sets state of connection between itself and the WS as "unauthenticated and unassociated"
- Station 27 will then have to do the time-consuming process of re-authenticate and re-associate to restore the connection
- If the attacker repeats the act, situation becomes worse


Station_27
AP
Attacker
Authentication Request
Authentication Response
Association Request
Association Response
Data
Data
(MAC address of station_27)
De-authentication Request
De-authentication Response

Spoofing poll control frame

- Since they work on batteries, the MS often goes to power saving modes after informing APs
- Meanwhile, the APs buffers all frames
- Once the MS wakes up, it informs the AP using Poll Control Frame
- Upon receipt of which, AP delivers all buffered frames
- An attacker can spoof the Poll Control Frame by using the MAC address of the genuine WS

- The AP then sends all buffered frame to the genuine sender
- But since the station is not awake yet, it fails to notice and capture the frames
- When the genuine station is actually awake, it sends the Poll Control Frame to the AP
- Unfortunately the AP do not have any copy of the sent frames, hence the WS suffers the lose

Violating MAC Etiquette (Protocol)

- There can be more subtle attacks, if some re-engineering of wireless interface card is done

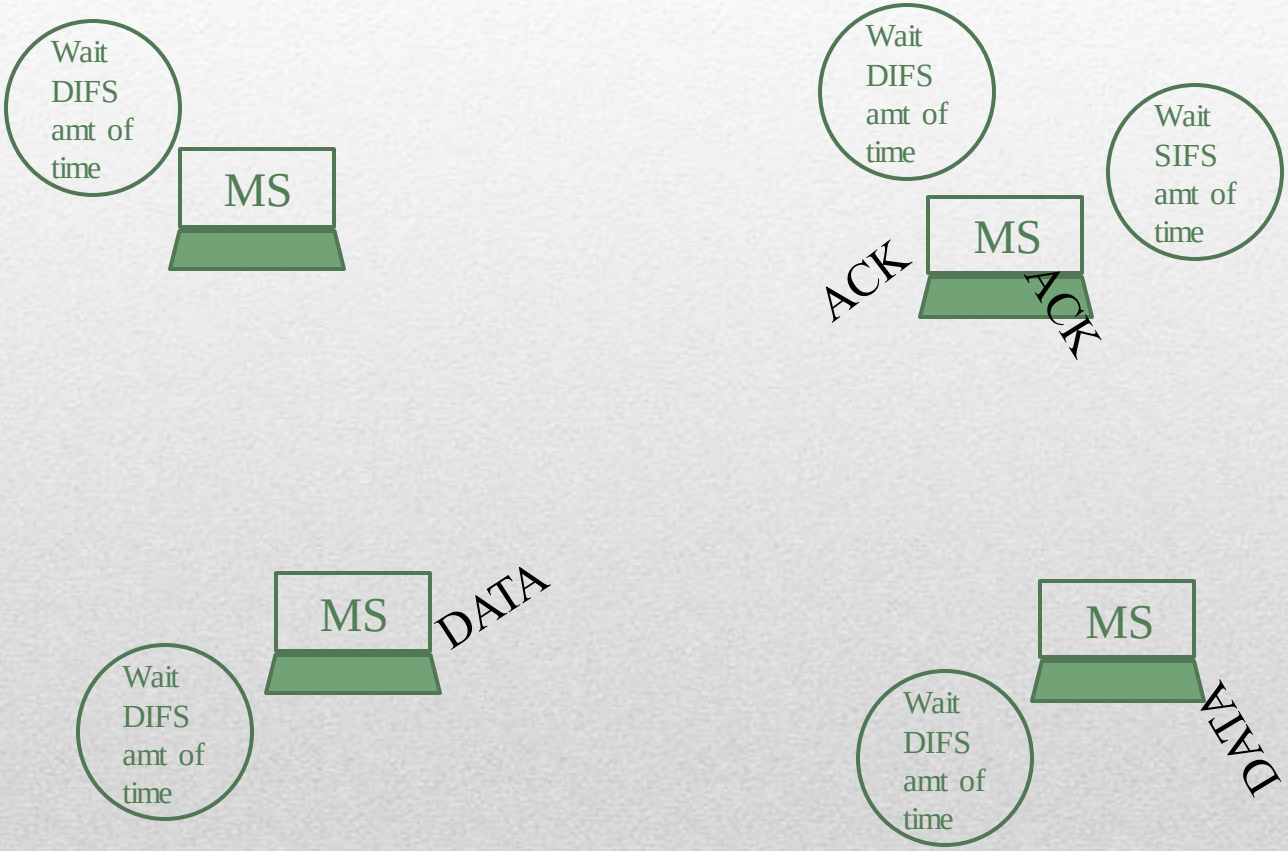
1. Violating inter-frame spacing rules
2. Abusing virtual carrier sensing

MAC Protocol

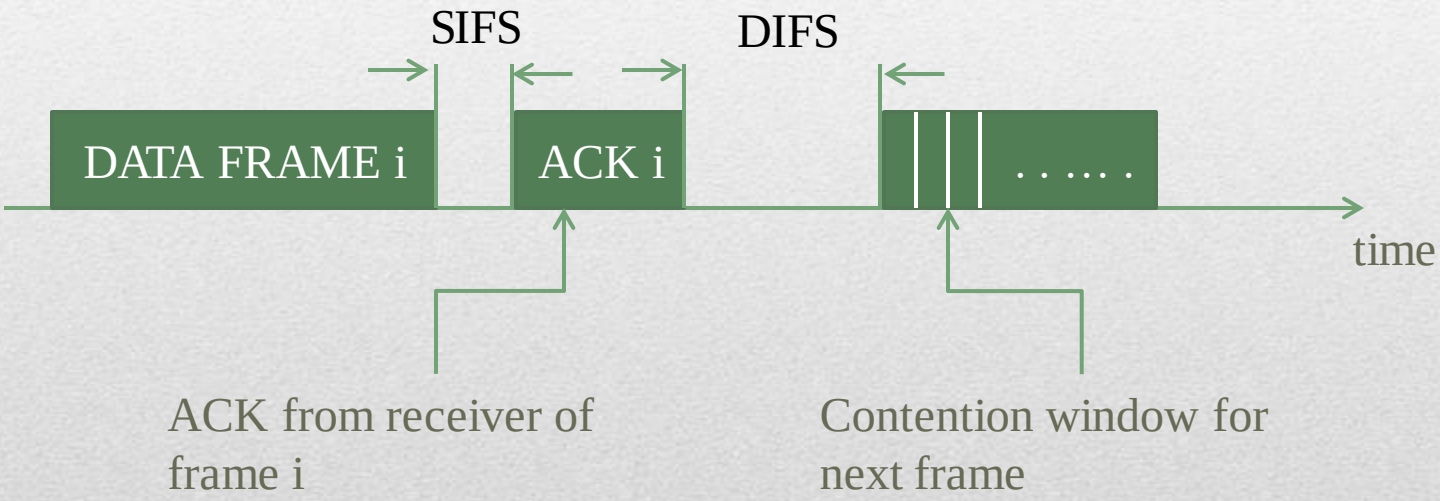
- The MAC protocol is CSMA/CD
- The rule is that, every station must sense the medium before it can send a frame
- If the channel seems to be busy, the station must initialise a counter with a random value
- The value indicates the number of slots the station must wait before it can send
- At the beginning of each slot, station senses the medium; if found free, counter is decremented
- When the counter reaches zero, the station can send its frame

Inter-frame Spacings

- 802.11 uses two inter-frame spacings
  - SIFS: Short Inter-Frame Space
  - DIFS: Distributed co-ordination function Inter-Frame Space
- When a station receives a DATA frame without any error, it must wait for a time period of SIFS and soon send an ACK frame to the sender
- After a pair of DATA and ACK sent between two stations, all station must wait for a period of DIFS before they can attempt to send a data frame
- Hence the spacing between a DATA and its ACK is SIFS and the spacing between previous ACK and a new DATA is DIFS


Wait DIFS amt of time
MS
Wait DIFS amt of time
Wait SIFS amt of time
MS
ACK
ACK
MS
DATA
Wait DIFS amt of time
MS
DATA
Wait DIFS amt of time

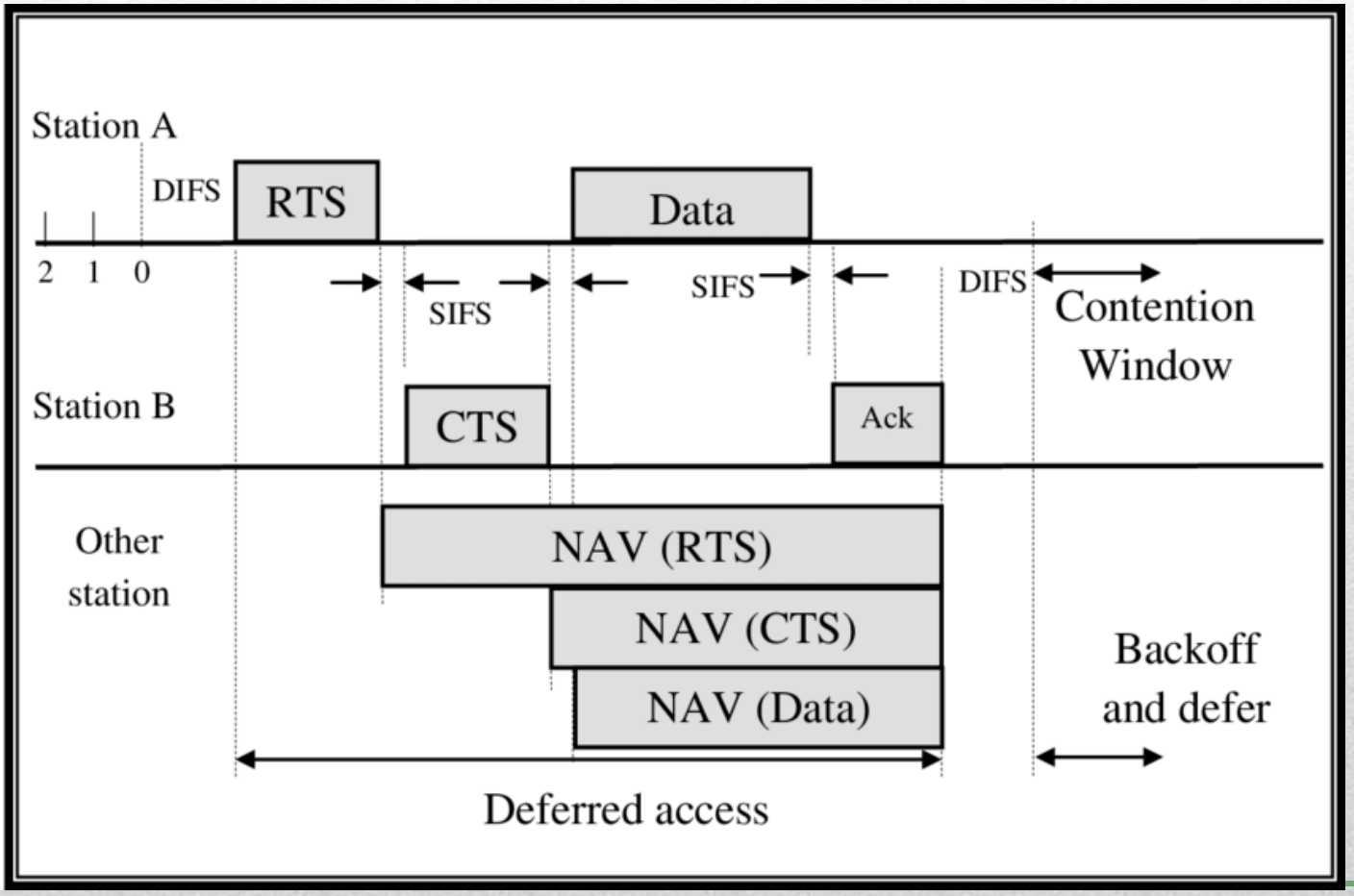
Inter-Frame Spacing



Transmission using CSMA/CD

- Transmission begins with a Request To Send (RTS) frame from the sender to the receiver
- If the receiver is ready to accept the data from the sender, receiver sends back a Clear To Send (CTS) frame
- Both RTS and CTS will contain a duration field that stores the amount of time left to complete the current communication including the time for sending ACK frame
- All other stations notes this value from these frames and store in their Network Allocation Vector (NAV) timer
- They all wait until the NAV timer expires indicating that the channel might be free

Transmission using CSMA/CD



Violating inter-frame spacing rules

- An attacker can re-engineer his wireless card to start transmission in the very first slot following a DIFS interval thereby starving a large number of wireless stations
- He can do this by setting his random back-off value to zero always, so that he don't have to wait for the counter to reach zero

Abusing virtual carrier sensing

- AN attacker can initialize the duration field in its RTS or CTS to be a large value so that all other stations will wait long to get their NAV timer expired
- By frequently transmitting such frames, legitimate users could be starved of bandwidth

CELL PHONE SECURITY

Cellular networks

- GSM – Global System for Mobile communications
- Or 2G – Second Generation cellular networks
- UMTS – Universal Mobile Telecommunication Systems
- Or 3G – Third Generation cellular networks

Cell phone security

- Types of security
  1. Mobile device security
     - Phone lock
     - PIN lock
     - GPS security
     - Remote wiping (delete all app remotely)
     - Application control
  2. Mobile application security
     - Encryption
     - Authentication
     - Application white listing
     - Geotag (tag location, date, time with photos)

Mobile threat

- Application threat
- Web based threat
- Network based threat

GSM

Global System for Mobile communication

GSM (2G)

- A cell phone is connected to a BTS using radio waves
- Multiple BTSs are connected to a BSC using microwave or optical signals
- Multiple BSCs are connected to a MSC using microwave or optical signals

Base Transceiver Station (BTS)
Base Station Controller (BSC)
Mobile Switching Centre (MSC)

SIM

- A cell phone is equipped with a SIM
- A SIM contains 3 secrets:
  1. International Mobile Subscriber Identity(IMSI): a unique 15 digit subscriber identification number
  2. Secret key: a 128 bit subscriber authentication key Ki
  3. Pin: known only to the owner to unlock the SIM (seldom used)

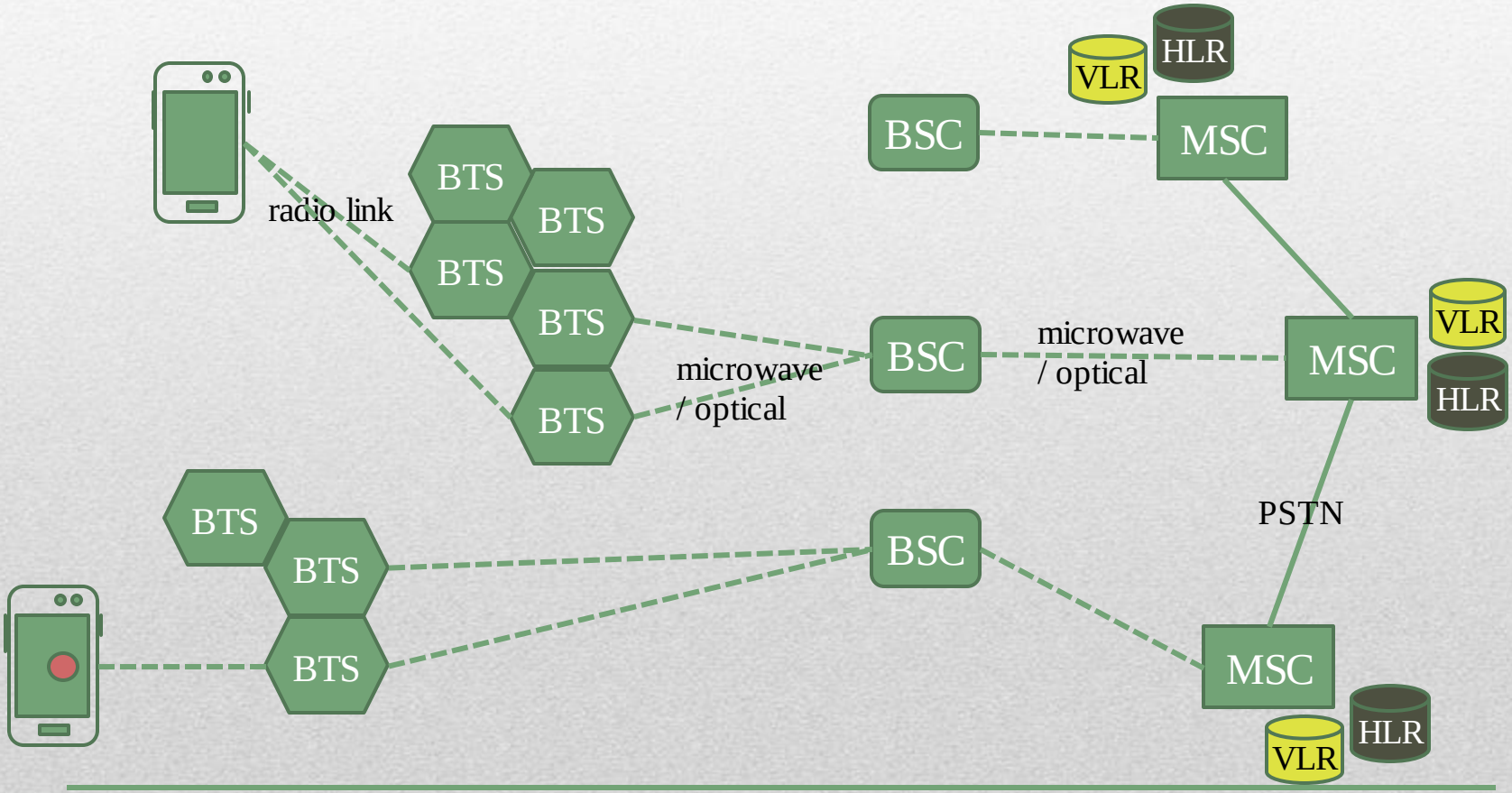
HLR

- A user's home network is the one where he has a subscription
- Every network has one MSC
- An MSC has a database called home Location Register (HLR) that stores all information about its subscribers
  1. subscribers mobile number (IMSI)
  2. secret key
  3. services subscribed to
  4. location details of its subscribers currently roaming

VLR

- An MSC also maintains a visitor location register (VLR) to store details of users currently using the network but not subscribers
- MSC also handles billing accounting functions

GSM Architecture



Security goals

- The major security goals of GSM are:

1. User identity confidentiality
2. Entity authentication
3. Message confidentiality
4. Message origin authentication and message integrity

1. User Identity Confidentiality

- IMSI is the main identity of the user
- For the matters of user identity privacy, the GSM does not require a user to transmit its IMSI for each call made
- Instead assigns a temporary TMSI, which has a limited time validity which can be transmitted by users while making calls
- Only while entering a new network, a user needs to communicate its actual IMSI
- MSC keeps track of TMSI and corresponding IMSI in the HLR

2. Entity Authentication

- The MSC needs to be sure that the call is billed to the original caller
- The caller need to be sure that he is talking to the called person
- Authentication of the subscribers take place at periodic intervals as well as when they enter a new network
- Authentication uses a challenge-response protocol

- Authentication proceeds in four steps

1. Authentication request from cell phone
2. Creation and transmission of authentication vector
3. Cellphone response
4. Computation of encryption key

Step 1: Authentication Request

- The cell phone sends to the base station the encryption algorithms that it can support
- The phone sends its IMSI/TMSI number to its home network MSC
- If the subscriber is inside some foreign network, the call request will made to the foreign MSC
- Foreign MSC checks its VLR and communicates with the MSC of the subscriber's home network

Step 2: Authentication Vectors

- MSC retrieves the secret key K_i of the requested subscriber from its HLR
- HLR generates a 128 bit random number RAND and computes
  - XRES= A3(RAND, K_i)
  - K_c =A8(RAND, K_i)
- The HLR generates 4 more random numbers and computes XRES and K_c for each of them
- Hence the HLR forms five authentication triplets

  <RAND, XRES, K_c>

- The triplets are then handed over to the MSC by the HLR
- If the subscriber is roaming, Foreign MSC obtains the five authentication triplets from home network MSC
- The MSC then sends the challenge- RAND from the first triplet to the BTS of the requesting subscriber
- The BTS in turn forwards it to the cell phone

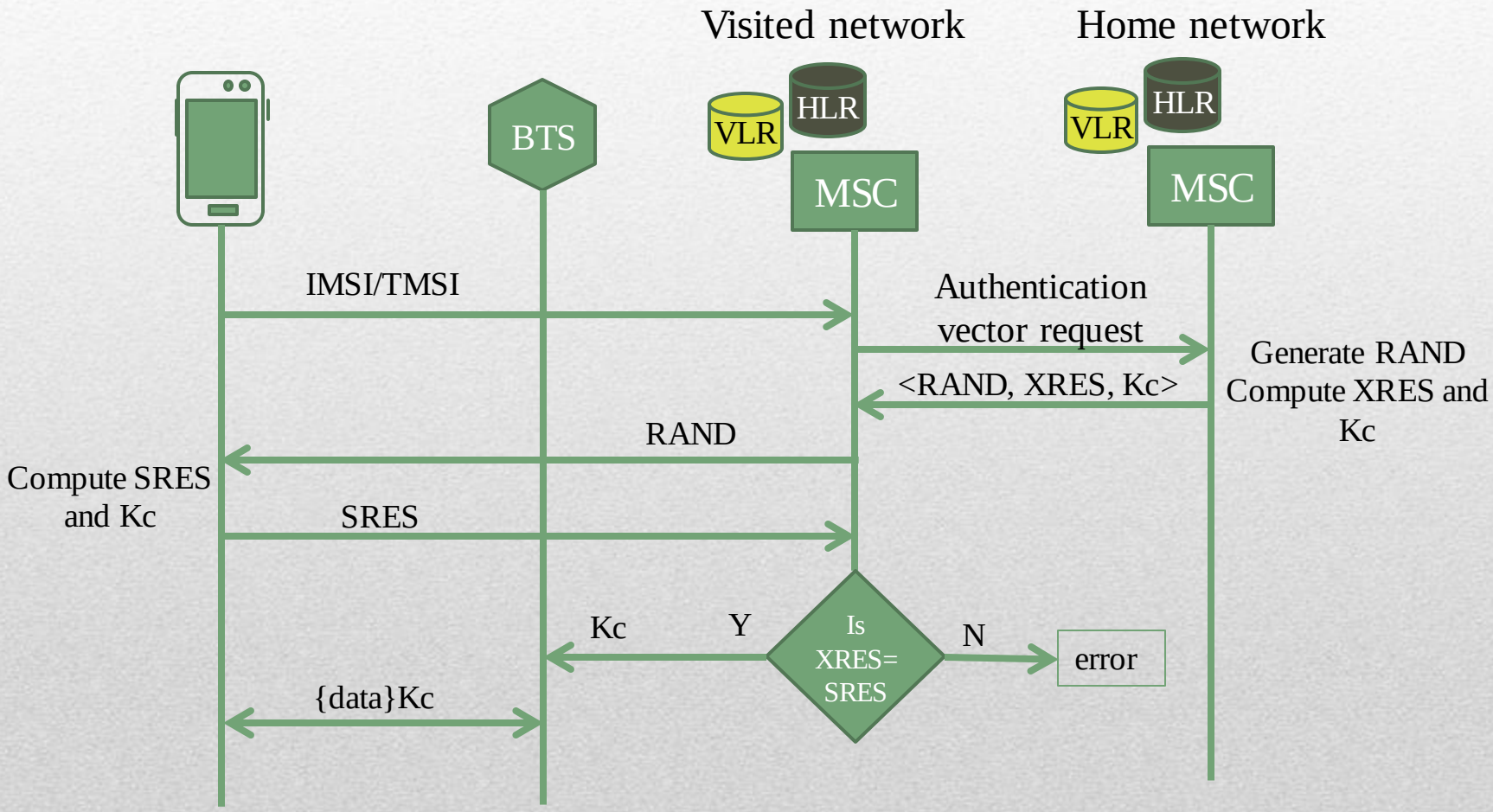
Step 3: Response

- Once the SIM receives RAND, it computes SRES
- SRES= A3(RAND, K_i)
- The subscriber sends response- SRES to the BTS which forwards it to the MSC
- MSC checks if XRES ==SRES ; if so, approves the identity of the user, otherwise rejects

Step 4: Computation of Kc

- The subscriber computes the Kc using K_i
  - K_c =A8(RAND, K_i)
- The BTS obtains the Kc from the MSC
- All messages between the cell phone the BTS is encrypted using Kc

Authentication in GSM



3.Message Confidentiality

- Message encryption between the BTS and the cell phone is done by a stream cipher
- A5 is the keystream generator
- Keystream is a function of 64 bit Kc and 22 bit frame number
  - Keystream=A5(Kc, FRAME#)
  - Cipher text=plain text $\oplus$ keystream
- This step is performed by the cell phone and not the SIM as it does not require any data from the SIM
- Computation of SRES and Kc is done by the SIM

Drawbacks

- The algorithms A3, A5 and A8 are based on Comp-128 a keyed hash function; Soon after their implementation, its major vulnerabilities were exposed
- With access to the SIM card, one can easily deduce Ki using a side channel attack, involving 8 adaptively chosen plain texts
- Once Ki is known, SIM card can be cloned defeating the security goals of GSM

- Though many versions of A5 are available, all are equally prone to attacks
- By eavesdropping on the first two minutes of conversation, a cipher- text-only attack on A5/2 can reveal the encryption key in few milliseconds
- A5/1 can also be compromised similarly
- The 64 bit encryption key Kc was truncated to 54 bits and padded with 10 zeroes which made it further weaker

- The GSM protocol does not provide any means to authenticate the base station to the subscriber which can pave the way for false base station attack
- Such attackers can send cipher mode command which will lead the cell phone to send messages without encryption
- Only the messages between the cell phone and the base station are encrypted, not beyond
- Links between BTS and BSC and MSC can all be eaves dropped

UMTS

Universal Mobile Telecommunication Systems

Security goals

- The security goals of UMTS are the same:

1. User identity confidentiality
2. Entity authentication
3. Message confidentiality
4. Message origin authentication and message integrity

1. User Identity Confidentiality

- IMSI is the main identity of the user
- For the matters of user identity privacy, the network does not require a user to transmit its IMSI for each call made
- Instead assigns a temporary TMSI, which has a limited time validity which can be transmitted by users while making calls
- Only while entering a new network, a user needs to communicate its actual IMSI
- MSC keeps track of TMSI and corresponding IMSI in the HLR

2. Entity Authentication

- Authentication proceeds in four steps

1. Authentication Request from Cell Phone
2. Creation and Transmission of Authentication Vector
3. Verification of Authentication Token and Cellphone Response
4. Agreement on Encryption and Integrity Check Algorithms

Step 1: Authentication Request

- The cell phone sends to the base station the encryption algorithms that it can support
- The phone sends its IMSI/TMSI number to its home network MSC
- If the subscriber is inside some foreign network, the call request will made to the foreign MSC
- Foreign MSC checks its VLR and communicates with the MSC of the subscriber's home network

Step 2: Authentication Vectors

- MSC retrieves the secret key K_i of the requested subscriber from the HLR
- HLR generates a 128 bit random number RAND and computes
  - XRES= F2(RAND, K_i) Expected Response
  - CK =F3(RAND, K_i) Cipher Key (Encryption)
  - IK=F4(RAND, K_i) Integrity Check Key
  - AK=F5(RAND, K_i) Anonymity Key
  - MAC=F1(RAND, K_i, AMF, SQN) Message Authentication Code
  - AUTN= <SQN $\oplus$ AK, AMF, MAC> Authentication Token

- AMF is the authentication management field that stores the lifetime of the key
- SQN is a sequence number known only to SIM and HRC (like the key Ki) for a sync between the two
- The HLR generates 4 more random numbers and computes all values for each of them
- The value of SQN gets incremented by one for each new vector
- Hence the HLR forms five authentication quintuplets

  <RAND, XRES, CK, IK, AUTN>

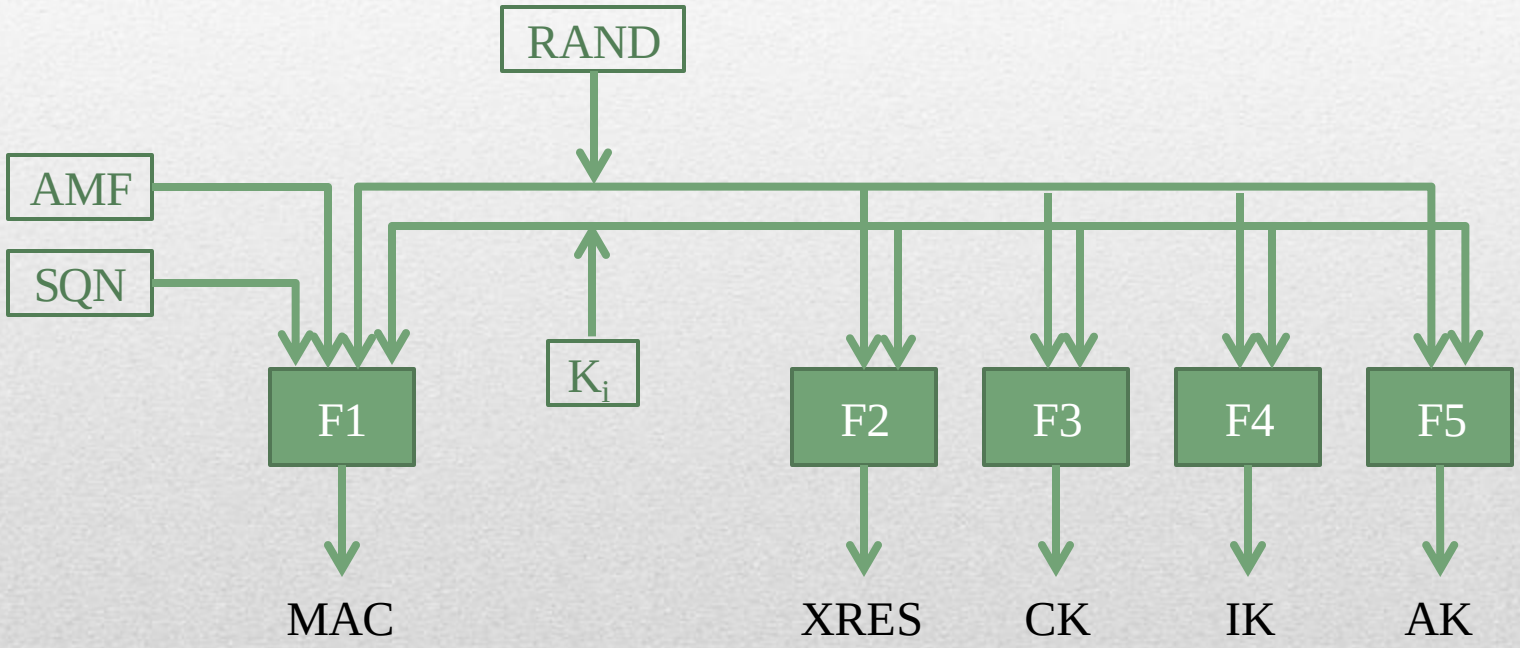
- The triplets are then handed over to the MSC by the HLR
- If the subscriber is roaming, Foreign MSC obtains the five authentication quintuplets from home network MSC
- The MSC then sends the challenge- RAND and AUTN from the first quintuplet to the BTS of the requesting subscriber
- The BTS in turn forwards them to the cell phone

Step 3: Response

- Once the SIM receives RAND and AUTN, it retrieves the first element from the AUTN
  - Retrieve SQN $\oplus$ AK
- Computes value of SQN by
  - (SQN $\oplus$ AK) $\oplus$ AK)
- Compares the values of received SQN and stored SQN
  - Computed SQN== stored SQN ?
- If the difference is acceptable, it computes the MAC
  - MAC=F1(RAND, K_i, AMF, SQN)

- Retrieves the third element from the AUTN, the MAC
  - Retrieve MAC
- Compares the values of MAC
  - received MAC==computed MAC ?
- If they are equal, the subscriber concludes
  - The authentication vector has been created by the HLR of its home network
  - The vector is fresh and not any replay

- Computes SRES
  - SRES= F2(RAND, K_i) Signed Response
- The subscriber sends response, SRES to the BTS which forwards it to the MSC
- MSC checks if XRES ==SRES ; if so, approves the identity of the user, otherwise rejects
- Finally the SIM computes CK and IK and conveys them to its own phone for encrypting and integrity checking all future messages between the cell phone and the base station

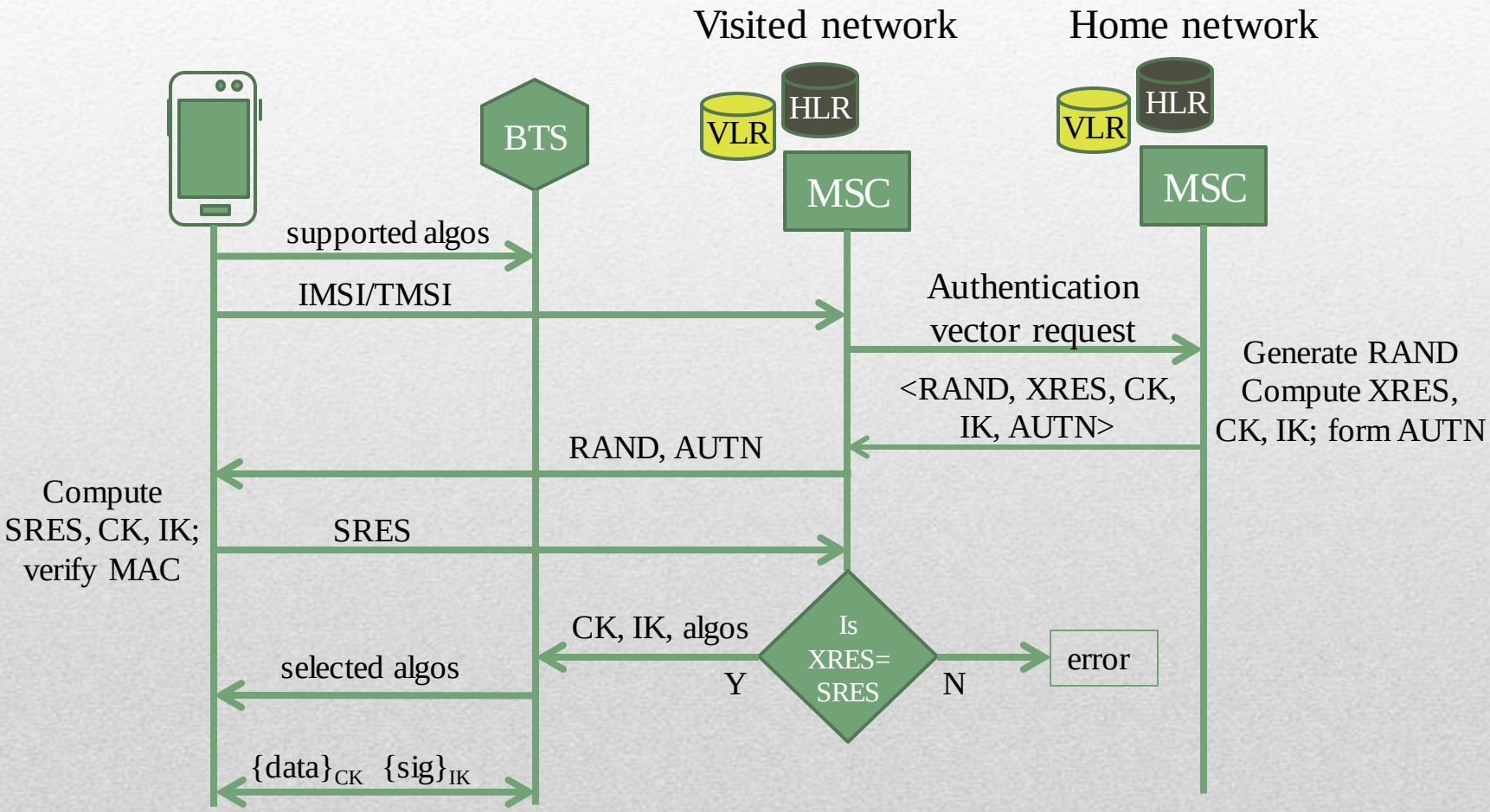


Computing components of authentication vector

Step 4: Agreement on Algorithms

- The MSC sends all permissible MACs and algorithms to the BSC
- The BSC decides which of them can be used and sends them to the cell phone (encrypted msg)
- The BSC obtains the CK and IK from the MSC
- All messages between the cell phone and the BSC is encrypted an integrity protected using them

Authentication in UMTS

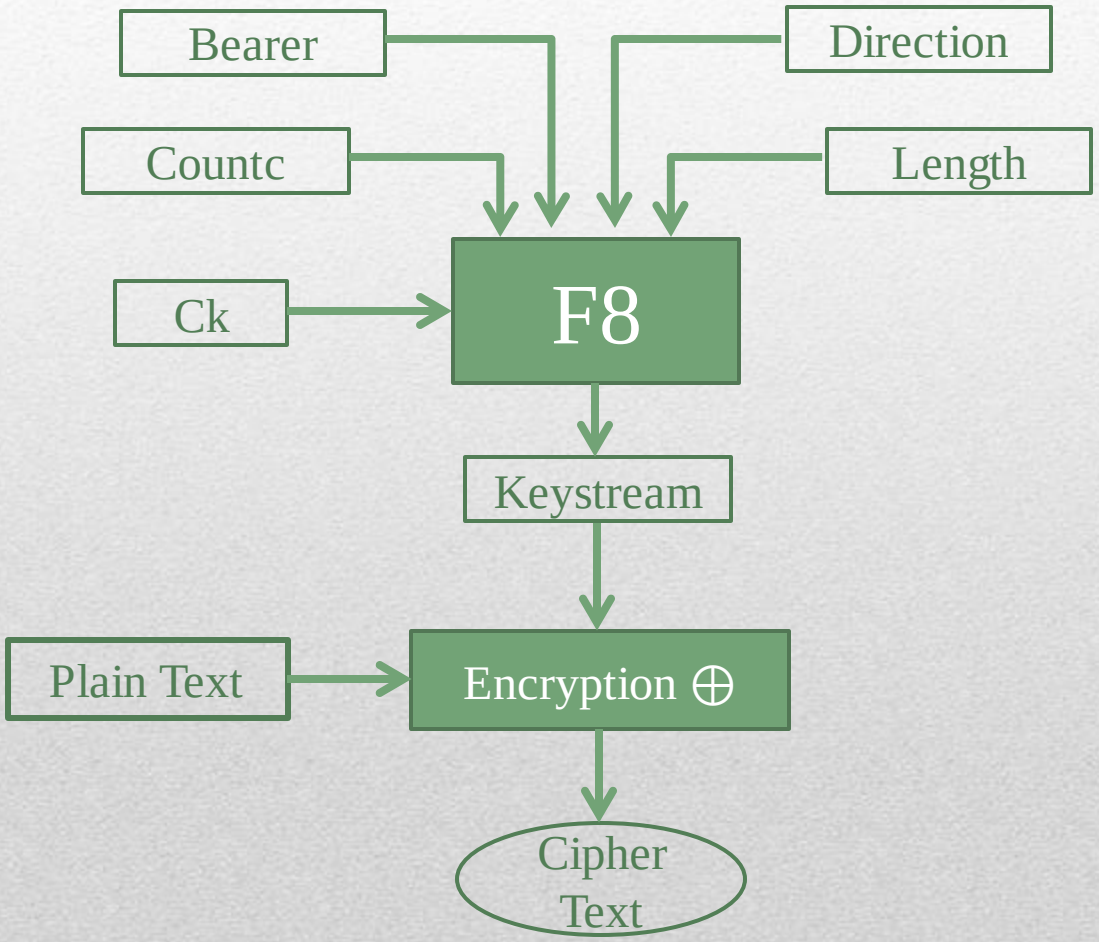


3.Message Confidentiality

- For message confidentiality, encryption is done on signalling data as well as user data
- A stream cipher is used where the keystream is
- Keystream= F8(CK, $count_c$, bearer, direction, length)
  - CK→ cipher key
  - $count_c$ →frame count
  - bearer → radio channel indication
  - direction→ msg sent by phone or BSC

- The functions F8 and F9 are both based on KASUMI
- It is an 8 round Fiestel cipher with 64 bit block size and 128 bit keys

Encryption


Bearer
Direction
Countc
Length
Ck
F8
Keystream
Plain Text
Encryption ⊕
Cipher Text

4.Message origin authentication

- Integrity protection is provided using MAC
- Most of the signalling messages are MAC protected
- User messages are not integrity protected in UMTS
- Per-message MAC = F9(IK, count, fresh, direction, message)
- The integrity key IK is used to generate and verify MAC
- Two variables $count_I$ and *fresh* are used to prevent replay attacks

- At connection setup, $count_I$ is initialised by the cell phone
- *Fresh* is generated by the BSC
- The 1 bit *direction* specifies whether the message originated from the cell phone or the BSC
- F8 is based on KASUMI
- It is an 8 round Fiestel cipher with 64 bit block size and 128 bit keys
- For generating the keystream required for encryption, KASUMI is used in a variant of OFB (Output feedback) mode

Enhancements in UMTS

- Signalling massages are individually authenticated and integrity protected, preventing false-base-station attacks
- Supports mutual authentication between cell phone and the network
- Uses sequence numbers and nonces preventing replay attacks
- Messages between BTS, BSC and MSC are all encrypted
- UMTS also addresses "network domain security" – protecting signalling as well as user messages between all nodes in the provider domain
- A variant of IPSec is proposed to secure messages in the wired network connecting the MSCs, HLRs and nodes in the GPRS core

- UMTS architecture is carefully designed so as to maximise compatibility with the GSM to enable smooth upgrading
- Encryption is based on KASUMI – a 128 bit block cipher; unlike COMP-128 used in GSM, KASUMI has withstood public scrutiny for several years
- KASUMI has an excellent combination of security, performance and implementation characteristics
- Is based on block cipher called MYSTY1 which is secure against a variety of cryptanalytic attacks
- It is space efficient; hardware requires less than 100 gates
- Can perform encryption at a sustained rate of 2 Mbps with a clock speed of about 200 MHz

THANK YOU