Cristina Nita-Rotaru

CS526: Information security

Wireless security

Wired Equivalent Privacy

- Security goals: protect link-level transmission
  - Confidentiality
  - Access control
  - Data integrity
- Security relies on the difficulty of discovering the secret key through a brute-force attack
- Uses stream cipher RC4 for encryption and CRC32 for integrity

802.11 and cellular security.

WEP Details

▸ RC4 is a stream cipher: based on key k and initialization vector (IV) v, generates a keystream RC4(v,k)

▸ To send a message M from A to B

▸ Compute integrity checksum (CRC32): c(M)

▸ plaintext P = {M, c(M)}

▸ Encrypt P using RC4: ciphertext $C = P \oplus RC4(v,k)$

▸ Transmit $C' = v, (P \oplus RC4(v,k))$

▸ To decipher an encrypted message C', the encryption process is reversed

Some Observations

▸ The integrity check does not depend on a key, but just on the message M, so anybody can create a pair M and CRC32(M)

▸ The WEP standard specifies 64-bit key = 40 bit key and 24 IV. For 128-bit keys (24 IV and 104 bit key).

▸ The IV is sent in clear, so is available to the attacker as well.

Risk of Keystream Reuse

- $C1 = P1 \oplus RC4(v, k)$
- $C2 = P2 \oplus RC4(v, k)$
- $C1 \oplus C2 = P1 \oplus P2$

- If P1 or P2 is also known by the attacker, the other plaintext is easy to compute
- If n ciphertexts using the same keystream are available makes reading traffic easier (frequency analysis, etc)
- Find plaintext P and the encryption C with keystream k, then it is easy to decipher any ciphertext C' encrypted with the same keystream k.

Is Keystream Reused?

▸ The pseudorandom keystream is based on the shared key k and the initialization vector IV. Since the key k is secret and is difficult to be changed for every packet, changing the IV is important to prevent keystream reuse.

▸ The IV is sent in clear, so is available to the attacker as well.

▸ The WEP standard recommends, but does not require that the IV be changed every packet, also does not say anything about how to select the IV.

▸ An implementation can reuse the same IV for all packets without risking non-compliance !

24-bit IV Space

▸ Busy access point sending 1500 byte packets, at an average of 2 Mbps, exhausts the IV space in half a day.

▸ Random generation of IV can produce collisions every 5000 packets (due to the birthday paradox).

▸ Many implementations use for IV a counter that is incremented for each packet sent and reset every time the card is inserted in the computer.

802.11 and cellular security.

Exploiting Keystream Reuse

▸ **Methods to obtain pairs (plaintext, ciphertext):**

  ▸ IP fields predictable: login sequences, recognize shared libraries transfer

  ▸ Send email and wait for the user to check it via wireless links

  ▸ Send data to access-points that have access control disables and observe the encrypted data

Dictionary Attack

- Goal: Decrypt traffic
- How: Store keystream in a table, indexed by IV.
- Remember the IV is sent it clear
- When the attacker sees a packet with an IV stored already in the table, look up the corresponding keystream, XOR it against the packet, and read the data!
- Table is at most $1500 * 2^{24}$ bytes = 24 GB

Packet Modification

▸ CRC32 is linear: $c(M \oplus D) = c(M) \oplus c(D)$

▸ Message M was transmitted, and the ciphertext was C and the IV was IV, C and IV are known to the adversary.

▸ Attacker can find C' s. t. it decrypts to M', M' = M $\oplus$ D
D = arbitrarily chosen by the attacker

▸ C' = C $\oplus$ <D,c(D)>
$\quad$ = RC4(v,k) $\oplus$ <M,c(M)> $\oplus$ <D,c(D)>
$\quad$ = RC4(v,k) $\oplus$ <M $\oplus$ D, c(M) $\oplus$ c(D)>
$\quad$ = RC4(v,k) $\oplus$ <M', c(M $\oplus$ D)>
$\quad$ = RC4(v,k) $\oplus$ <M', c(M')>

802.11 and cellular security.

Packet Injection

▶ The attacker knows the keystream, he can select any message and compute CRC of the message without knowing the key.

▶ The base station will accept the packet as valid

WEP Authentication

▸ Base station verifies that a client joining the network really knows the shared secret key k.

▸ The base station sends a challenge string to the client, and the client sends back the encrypted challenge

▸ The base station checks if the challenge is correctly encrypted, and if so, accepts the client.

▸ If adversary sees a challenge/response pair for a given key k; he can perform the packet injection attack previously describe, and trick the base station.

Fluher, Mantin, and Shamir Attack

▸ This is an known-plaintext attack against RC4, that allows attackers to eventually recover a key.

▸ Attack is based on an assumption that the attacker is able to guess the first byte of plaintext used by the victim.

▸ Stubblefield, Ionnandis, and Rubin showed that the attack is possible in practice

RC4

- A proprietary cipher owned by RSA DSI, designed by Ron Rivest.

- Simple and effective design.

- Variable key size, byte-oriented stream cipher.

- Widely used (web SSL/TLS, wireless WEP).

- Key forms random permutation of all 8-bit values.

- Uses that permutation to scramble input info processed a byte at a time.

802.11 and cellular security.

RC4 Key Schedule

▸ Walks each entry in an array S of numbers: 0..255 turn, using its current value plus the next byte of key to pick another entry in the array, and swaps their values over.

▸ Total number of possible states is 256!, very big number

▸ S forms internal state of the cipher, L is the size of the key k

  ▸ for i = 0 to 255 do

    ▸ S[i] = i

  ▸ j = 0

  ▸ for i = 0 to 255 do

    ▸ j = (j + S[i] + k[i mod L])(mod 256)

    ▸ swap (S[i], S[j])

RC4 Encryption

‣ Encryption continues shuffling array values

‣ Sum of shuffled pair selects the "stream key" byte value

‣ XOR with next byte of message to en/decrypt

  ‣ i = j = 0

  ‣ for each message byte mi

    ‣ i = (i + 1) (mod 256)

    ‣ j = (j + S[i]) (mod 256)

    ‣ swap(S[i], S[j])

    ‣ t = (S[i] + S[j]) (mod 256)

    ‣ Ci = mi ⊕ S[t]

RC4 Cryptanalysis

- The algorithm was kept secret however…

- In 1994 the source code was leaked on the to cyberpunks mailing list.

- The external analysis of RC4 was done on the source code that leaked in 1994.

- Fluhrer showed two weaknesses:
  - the first byte generated by RC4 leaks information about individual key bytes.
  - found a large number of weak keys, in which knowledge of a small number of key bits suffices to determine many state and output bits with non-negligible probability.

The Attack

▸ The first bits of the output are always going to be based on the first values of Sbox since x and y are initialized to zero.

▸ $x = (x+1) \bmod 256$

▸ $y = (y+Sx) \bmod 256$

▸ swap Sx and Sy

▸ $t = (Sx + Sy) \bmod 256$

▸ $K = St$

▸ Statistical attack that allows an attacker to recover the key after 60 different IVs and the same key: they estimate 4,000,000 pkts.

Stubblefield, Ionnandis, and Rubin

▸ **Implemented the attack using inexpensive hardware.**

▸ **Identified other weaknesses in WEP**

> ▸ the keys are ascii, and therefore it limited the possible key space since numbers were based on ascii equivalents to letters.

▸ **WEP is a link layer protocol: it encrypts the network layer data.**

> ▸ First byte is going to be the IP packet.
>
> ▸ Worse, 802.11, in order to be compatible with IP as well as IPX and other network protocols, uses the 802.2 logical link layer encapsulation.
>
> ▸ This just means that all packets always start with the same 802.2 header.
>
> ▸ Guessing the first byte is trivial.

Countermeasures

▸ Improve key management: every host should have its own key and key should be changed frequently. Note that this will not solve the attacks on message authentication.

▸ Use higher-level security mechanisms such as IPSec, SSH, and VPN for security, instead of relying on WEP.

▸ Treat all systems that are connected via 802.11 as external. Place all access points outside the firewall.

802.11 and cellular security.

Lessons Learnt

- Engineering network protocols vs. security:
  - CRC-32 and RC4 are fast and simple, but they have problems
  - Being stateless and liberal are good for networking, but dangerous for security because they give an attacker more freedom

- Learn from previous works: see IPSEC, TLS.

- Public review is important: international standards should be examined by the cryptographic community

802.11 and cellular security.

WPA

- Encryption method: RC4, TKIP

- Key size: 128 bits (varies)

- Hash method: ICV, Michael

- 802.11x authentication: can be required

- Key distribution:

  - TKIP which changes the key for each packet

  - PSK, pre-shared key based on some passphrase

WPA Details

▸ **Michael generates MIC (Message Integrity Code)**

  ▸ 8 bits

  ▸ Placed between data and ICV

▸ **TKIP (Temporal Key Integral Protocol)**

  ▸ Resolves keys to be used, looks at client's configuration

  ▸ Changes encryption key every frame

  ▸ Sets unique default key for each client

▸ **TSC sequence counter to prevent replay attacks, packets have to arrive in order at the receiver**

WPA Vulnerabilities

▶ **Birthday attack**

  ▶ Get a pair D,M where D1 = MIC(M1)

  ▶ When Di = D1 where Di != 1, attack is successful

  ▶ Probability for success: 2^{32}

  ▶ If keys change during attack, forgery is garbage

WPA Vulnerabilities

▸ **Temporal Key**

  ▸ Lost RC4 Keys

  ▸ Can discover TK and MIC for example by capturing ARP messages (plaintext is known)

  ▸ Can forge messages, for example can forge ARP messages to reroute the traffic

  ▸ Injection has to be done on other channels

802.11 and cellular security.

WPA Vulnerabilities

▸ **DOS**

   ▸ Access point shuts down for 60 seconds if forged unauthorized data detected

   ▸ Possible to shut access points with little network activity

▸ **PSK**

   ▸ Used in absence of 802.1x, 1 per ESS (usually).

   ▸ Internal person can use this, and a captured MAC address/ nonce to imitate another client

   ▸ Vulnerable to external dictionary attacks, if short

802.11 and cellular security.

802.11 Services

▸ Station Services – similar to those in a wired network.

  ▸ Data Delivery

  ▸ Authentication

  ▸ Privacy

▸ Distribution Services – enables a node to roam between several base stations

  ▸ Association

  ▸ Reassociation

  ▸ Disassociation

  ▸ Integration

▸

802.11 Type of Frames

▶ **Management frame:**

  ▶ authentication of a wireless client to a base station (authentication/deauthentication)

  ▶ when more than one base station present the station authenticates itself to all of them, bit only one base station will forward packets to/from wired network (association/ disassociation)

▶ **Control frames:**

  ▶ power save: TIM, Poll

  ▶ RTS/CTS (reserve the channel)

▶ **Data frames**

Authentication/Deauthentication Association/Dissociation

▶ Clients can explicitly ask for deauthentication from a base station

▶ Base station can send an deauthentication message to a client

▶ Similarly a client can ask for dissociation from a base station

▶ All these messages are not authenticated, so anybody can inject packets

▶ Question: How easy is to do that?

Deauthentication Attack

Association Request

Association Response

Deauthentication

Data

- An attacker can deny access to individual clients, or rate limit their access

802.11 and cellular security.
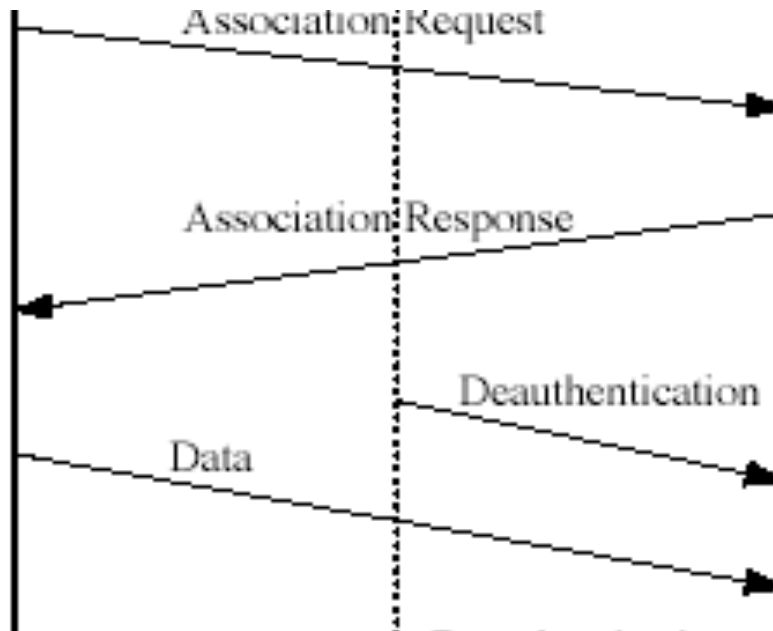
Association/Dissociation Attacks

▸ Similar with deauthentication, an attacker can pretend that he is a base station and send a disassociation message.

▸ Less impact than the deauthentication attack because for a client is less costly to associate again with a base station as opposed to authenticate again

Countermeasures?

▸ Non-cryptographic, non-invasive methods

▸ For a successful attack, deauthentication message must be sent after authentication was established (monitor for authentication message)

▸ Delay the effects of deauthentication/dissociation requests (queuing), then observe traffic from the client; if data comes, then the request must have been spoofed

802.11 and cellular security.

Power Management

▸ Allow idle station to go to sleep (save battery)

▸ Wireless station announces when it goes to sleep

▸ Base station starts buffering packets for the sleeping node

▸ Periodically the base station broadcasts (traffic indication map) TIM indicating that there are buffered packets

▸ Wireless station can also wake up an poll the base station to see if there are buffered packets

▸ Relies on time synchronization mechanisms between the base station and the wireless stations (TIM period and timestamp also sent in clear)

802.11 and cellular security.

Power Management (cont.)

▸ Broadcast/multicast frames are also buffered at the base station and sent at a different time calls DTIM (delivery traffic indication map) also periodically broadcast

▸ Power Saving stations wake up prior to expected DTIM

▸ If TIM indicates frame buffered the wireless station sends PS-Poll and stays awake to receive data else the station sleeps again

Power Saving Attacks

▶ An attacker impersonates a wireless station that is asleep and pretends that is awake

▶ The base station will send all the buffered frames, that will be lost

▶ An attacker impersonates a base station and sends spoofed TIM making it believe that there are no packets buffered for it

▶ An attacker can send corrupted TIM period to the wireless station making it keep sleeping or desynchronized.

802.11 Medium Access

▶ Two mechanisms for channel access

  ▶ Distributed Coordination Function (DCF), mandatory

  ▶ Point Coordination Function (PCF), optional, used only in infrastructure mode

▶ DCF is a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol

▶ Why "collision avoidance" ?

Collision Detection

▸ Every node listens, if channel free, then send

▸ If "collide", they retransmit at random times (exponential back-off)

▸ Collisions may still exist, since two stations may sense the channel idle at the same time

▸ In case of collision, the entire packet transmission time is wasted

▸ Random access MAC protocols: ALOHA, SLOTTED ALOHA, CSMA and CSMA/CD (used by Ethernet)

Collision Avoidance

▸ Collision detection is very difficult (in some cases impossible) in wireless. Transmitters don't reliably know if there is a collision at the receiver.

▸ Collision detection does not work well for wireless

    ▸ multipath fading of a radio signal: small time delays can occur in radio signals, as results the quality of the signal at the receiver will be degraded (weaker).

    ▸ Hidden terminal: Two or more senders might not receive from each other.

    ▸ COLLISION AVOIDANCE !

Hidden Terminal

Hidden Terminal:

Metal partition

Access
Point

Sender 1

Sender 2

Signal strength
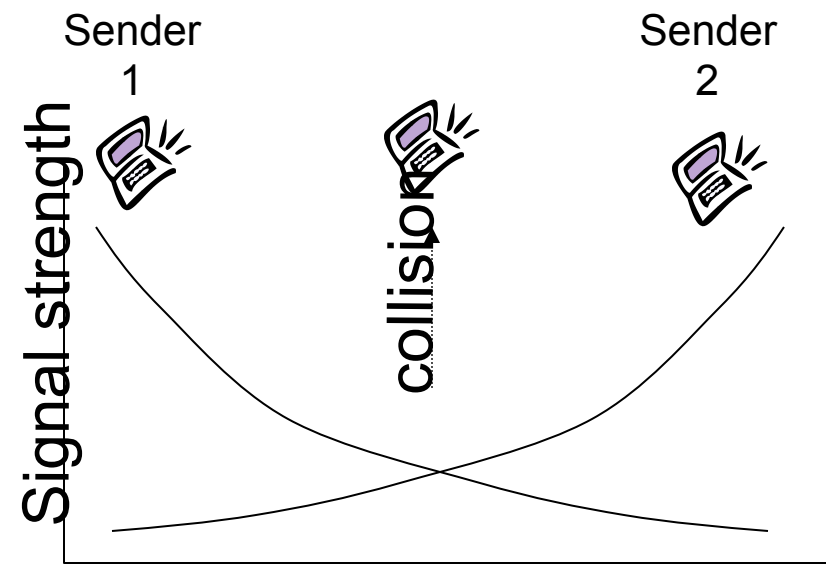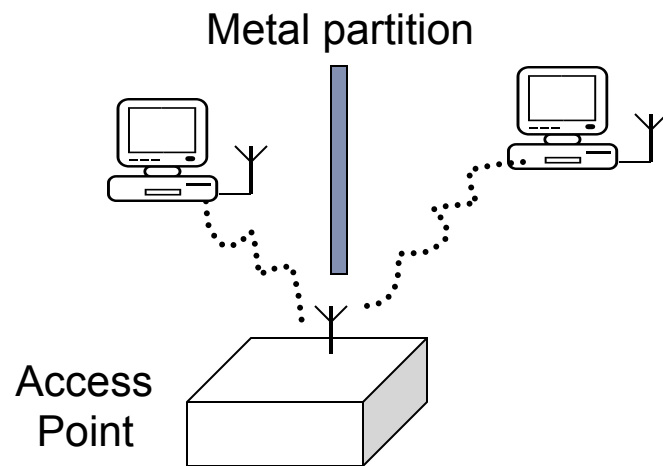
collision

CSMA/CA: Collision Avoidance

▸ Listens to see if medium is idle ("carrier sense").

▸ If idle, wait an additional random backoff time.

▸ If line is still idle, transmit.

▸ Wait for receiver acknowledgement.

▸ Retransmit if necessary.

▸ Additional RTS/CTS to reserve the channel, and the size of the data to let other know how long the channel will be busy

RTS/CTS Mechanism
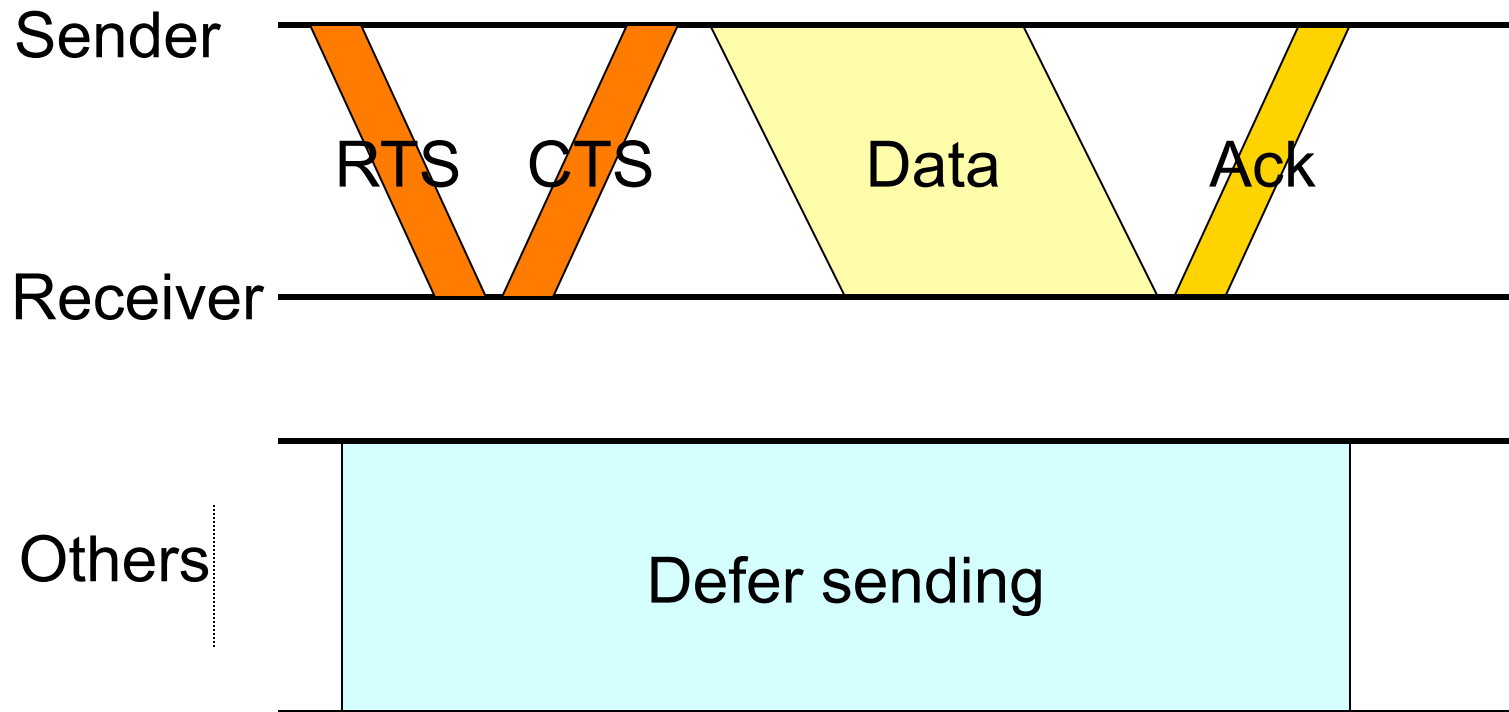
RTS/CTS is optional in 802.11b

Virtual Carrier Sensing

▸ RTS/CTS contain duration of data transfer + Ack

▸ Virtual Carrier Sensing: Nodes overhearing RTS/CTS stay silent for specified duration (stored in Network Allocation Vector NAV)

▸ Interframe intervals used as a priority mechanism: four types SIFS, PIFS, DIFS, EIFS; Attack can exploit SIFS/DIFS

| DIFS | RTS | SIFS | CTS | SIFS | DATA | SIFS | ACK | DIFS |

Media Access Attacks

▸ Packet sending to the media is not authenticated in 802.11.

▸ Sending packet within each SIFS (20 microseconds) to compete for the media; requires the attacker to "work hard" to block the channel: sending 50,000 packets/second,

▸ Virtual Carrier-Sense attack: Sending out packets with large NAV, since maximum value for NAV is 32 milliseconds, attacker needs to send 30 times/second to block the channel

Practicality of the Attacks

▸ A wide variety of 802.11 cards do not typically allow the generation of any control frames, permit other key fields (such as NAV) to be specified by the host, or allow reserved or illegal field values to be transmitted.

▸ Software-based method to modify headers of frames by exploiting a debugging feature (auxiliary port)

Defense to Virtual Carrier-Sense Attack

▸ For four key frame types contains NAV:

  ▸ ACK and Data frame: ignore NAV since there is no fragmentation.

  ▸ RTS frame NAV: respected until such time as a data frame should be sent.

  ▸ CTS frame NAV: specify some threshold (30%) if such time is used by CTS frame then ignore NAV.

Summary

- ▶ Authentication/Deauthentication and association/ disassociation packets not authenticated, anybody can inject

- ▶ Software-based attack was successfully conducted

- ▶ Exploit the RTS/CTS mechanism to conduct carrier sense attack

- ▶ Low-overhead, non-cryptographic

- ▶ countermeasures are suggested
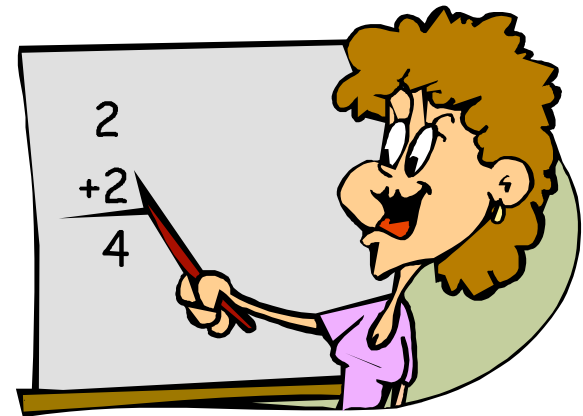
Cristina Nita-Rotaru

Security Issues in Cellular Networks

Cellular Networks

▸ Wired infrastructure

▸ Uses licensed spectrum

▸ Base stations consisting of transmitter, receiver, and control unit, each serving a cell

▸ Each cell is allocated a band of frequencies

▸ Cells are set up such that antennas of all neighbors are equidistant (hexagonal pattern)
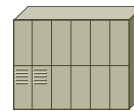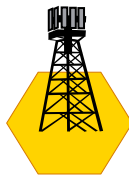
Radio Controller

Core Network

Cell

Key concept: frequency reused by dividing the area covered by a cellular network in cells, avoid co-channel and adjacent interference
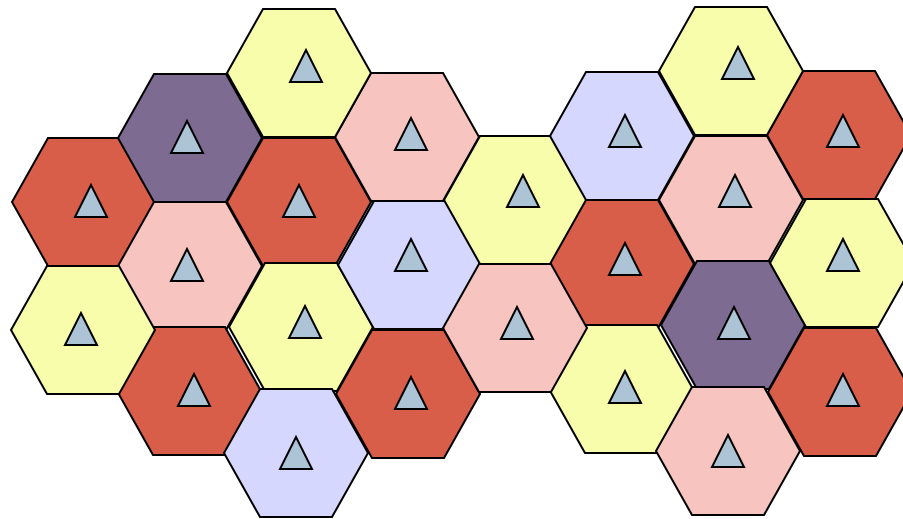
Clustering

A cluster is a group of cells which use the entire spectrum

▸ Clustering ensures that cells which use the same frequency are separated by a minimum distance called the reuse distance D

▸ R is the radius of a cell

▸ N is the size of cluster

$$\frac{D}{R} = \sqrt{3N}$$

802.11 and cellular security.

Interference

- **Co-channel interference**:
  - Addressed by deciding how many cells must be in between before reusing a frequency

- **Adjacent channel interference**:
  - Channel assignment to different cells within a cluster done to minimize adjacent channel interference by not assigning neighboring frequencies to the same cell

Supporting Many Users Simultaneously

n is the number of users supported simultaneously

N is the cluster size

k is the number of cells required to cover a given area

W is the bandwidth needed per user

S is the total available spectrum

$$n = \frac{k(S/N)}{W}$$

Capacity Enhancements

▸ **Frequency borrowing:** frequencies are taken from adjacent cells by congested cells

▸ **Cell-splitting**: increase the number of available number of channels in hot-spots

▸ **Cell sectorization**: reuse more channels on short distance by using SDMA

▸ **Power control**: to ensure that BS receives a constant equal power from all users, users at farther distance should transmit at higher power, and users at closer distance should transmit at lower power

Cellular Networks: Handoff (or Handover)

Handoff: user transitions from one coverage area to another coverage area
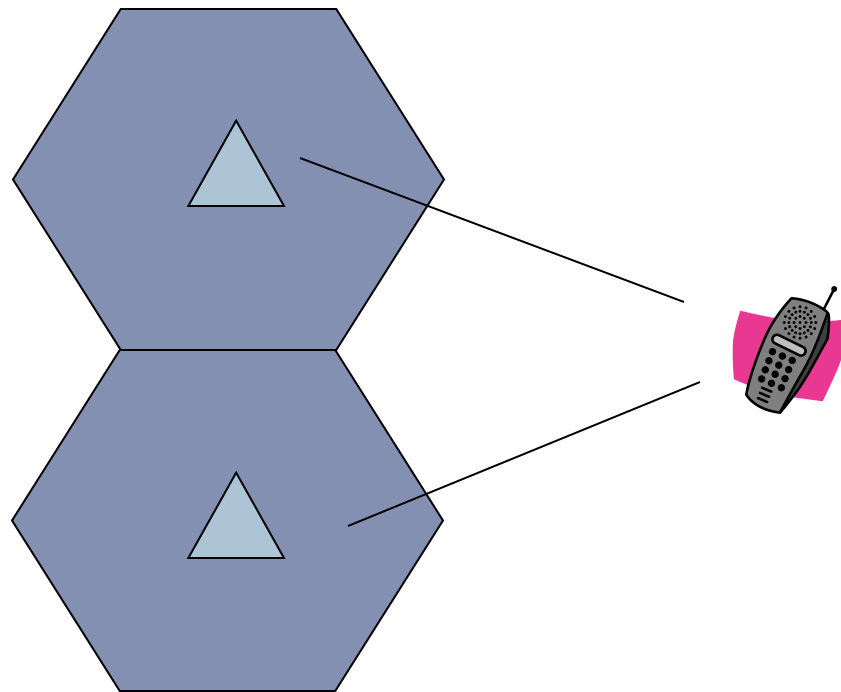
Issues Related to Handoffs

▸ **Optimal BS selection**: in general on the boundaries between cells, difficult to decide what BS is best

▸ **Ping-pong effect**: call gets bounced back and forth between two BS when the call is on the boundary

▸ **Data loss**: interruption due to handoff may cause loss of data

▸ **Detection of handoff requirement**: who and when initiates handoff, based on what criteria

Handoff Performance Metrics

▶ **Cell blocking probability**: probability of a new call being blocked

▶ **Call dropping probability**: probability that a call is terminated due to a handoff

▶ **Call completion probability**: probability that an admitted call is not dropped before it terminates

▶ **Probability of unsuccessful handoff**: probability that a handoff is executed while the reception conditions are inadequate

More Handoff Performance Metrics

- **Handoff blocking probability**: probability that a handoff cannot be successfully completed
- **Handoff probability**: probability that a handoff occurs before call termination
- **Rate of handoff**: number of handoffs per unit time
- **Interruption duration**: duration of time during a handoff in which a mobile is not connected to either base station
- **Handoff delay**: distance the mobile moves from the point at which the handoff should occur to the point at which it does occur

802.11 and cellular security.

1G: First-Generation Analog

▸ **Advanced Mobile Phone Service (AMPS)**

▸ Created in 1978, remained in operations till 2008

▸ In North America, two 25-MHz bands allocated to AMPS

▸ One for transmission from base to mobile unit

▸ One for transmission from mobile unit to base

▸ Each band split in two to encourage competition (12.5MHz per operator)

▸ Channels of 30 KHz: 21 control channels (FSK), 395 traffic channels (FM voice) per operator

▸ Frequency reuse exploited (R = 7)

▸ Maximum data transmission rate of 10kbps

AMPS: Channels Categories

▸ **Downlink control channel** for system management

▸ **Downlink paging channel** for locating a client in the network and alerting it when it receives a call

▸ **Bidirectional access channels** for call setup and channel assignment

▸ **Bidirectional data channels** to carry user voice/data.

AMPS: How Does It Work?

▶ Client scans for most powerful control channel and broadcasts a 32-bit serial number and a 10-digit telephone number

▶ The base station hearing the client, registers with a mobile switching office (MSO) and informs the home location register (HLR) of the present location

▶ Client updates its position every 15 minutes

AMPS: Making a Call

▸ Client sends the number through the access channel

▸ Base station sends request to the MSO which assigns a duplex channel for the call on the data/voice channel

▸ Both parties are informed through the paging channel

▸ Once the callee is located, it will take the call on the allotted voice channel

From 1G to 2G

▶ **From analog to digital**: first-generation systems are almost purely analog (use analog modulation techniques); second-generation systems are digital

▶ **From non-encrypted to encryption** – 2G systems provide encryption to prevent eavesdropping unlike 1G

▶ **Improved channel access** – 2G provide support for channels to be dynamically shared by a number of users

802.11 and cellular security.

2G Standards

- GSM in Europe
- Digital-AMPS (DAMPS) in US
- Personal Digital Cellular (PDC) in Japan

GSM

- Most popular cellular network
- Commercial operation began in 1991 with Radiolinja in Finland
- Four variants:
  - Most GSM networks operate in the 900 MHz or 1800 MHz bands.
  - United States and Canada use the 850 MHz and 1900 MHz bands because the 900 and 1800 MHz frequency bands were already allocated.
- Channel access mechanism is TDMA
- Several data services offered besides voice

GSM Control Channels

▸ **Broadcast control channel (BCCH)**: downlink channels that contains the BS's identity and channel status; All clients monitor the BCCH to see if they entered a new cell

▸ **Dedicated control channel (DDCH)**: used for call setup, location updates and call-management related information; each call has its own alloted DDCH

▸ **Common control channel (CCCH)**: downlink paging channel to alert a client about a call, random access channel, and access grant channel in which BS inform the client of the alloted full-duplex channel for the call

GSM Data Rate and SIM

▸ Maximum speed for data services is 34Kbps, but forward-error correction and encryption reduce the data rate to 9.6 Kbps

▸ **Subscriber Identity Module (SIM) card**:

▸ pluggable, stores information such as the subscriber's identification number, networks and countries where it can get service;

▸ SIM can be moved to another phone

802.11 and cellular security.

Data over Voice Channel

▶ **Cellular networks were primarily designed to support voice only**

▶ **Issues when sending data over voice channels:**

  ▶ **Signal distortion**: data receivers can not interpolate data the way a human can, even with degradation of quality

  ▶ **Handoff error**: the delay in transfer of the call can result in data loss

  ▶ **Interfacing with the fix network**: cell networks should be able to differentiate between data and voice

Strategies to Address "Data over Voice"

▸ Send a control message to indicate a data call and disable the voice coding

▸ Use a two-stage dial-up, first to the cellular carrier, then the subscriber, carrier has different numbers for each service is offers

▸ Assign different numbers to a subscriber for each service

GSM Data Services: SMS

▸ One of the most popular, stands for Short Messaging Systems

▸ Connectionless transfer of 160-alphanumeric characters

▸ Can be point-to-point or broadcast

▸ **Send over the control channel**

Other Data Services

▸ High-Speed Circuit-Switched Data (HSCSD): allows large file transfers; 57.6 kbps

▸ General Packet Radio Service (GPRS): more appropriate for burst traffic as e-mail and fax, 171.2Kbps

802.11 and cellular security.

Security and Privacy

▸ Authentication, billing

▸ Privacy, even a bigger issue given that modern phones have GPS

▸ Attacks on infrastructure: control channel used for data, cellular and Internet connected

▸ Attacks on the devices themselves

802.11 and cellular security.

Billing

▸ Cellular service is a high cost service (infrastructure + licensed spectrum)

▸ Authentication for billing purposes is main focus

▸ Communication between base stations and mobile phones is wireless so encryption is needed

Authentication Architecture

▸ **User is permanently associated with a home location register (HLR) in his subscribed network;**

  ▸ contains user profile, billing and location information

▸ **Visitor location register (VLR)**

  ▸ maintains information about the roaming users; information is downloaded from the user's HLRs.

▸ **Authentication Center**

  ▸ validates a user by verifying their identity with the Equipment Identity Register

Home Location Register

Visitor Location Register

Mobile Switching Center

Equipment Identity Register

Authentication Center
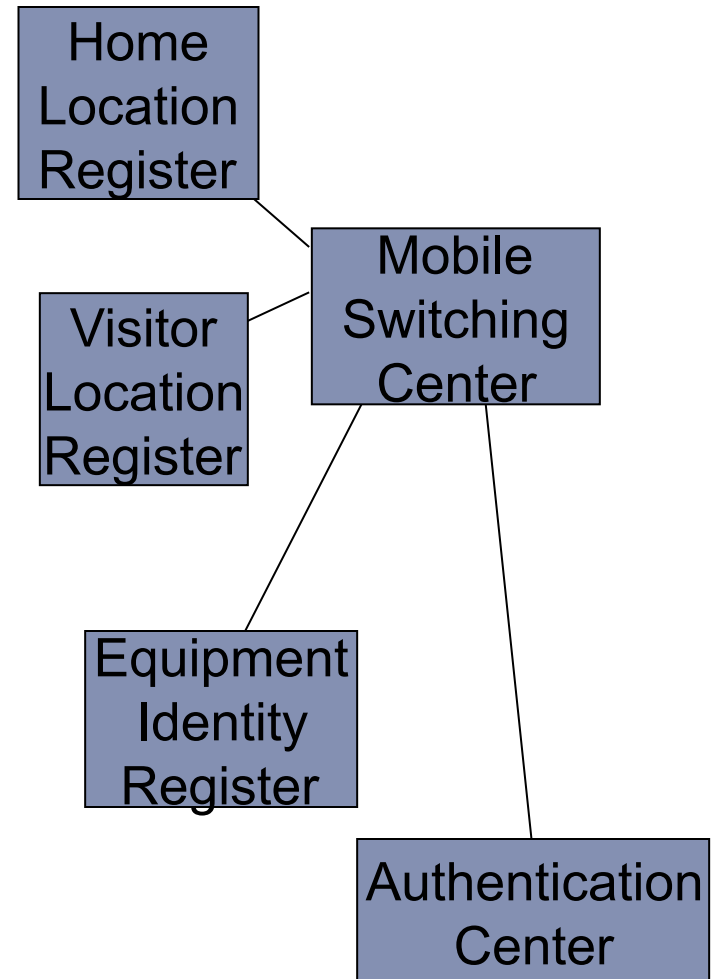
GSM Main Security Focus

▸ Focus:
  ▸ Make sure the client is billed for the service
  ▸ **Provide authentication, confidentiality and anonymity of the communication**

▸ Assumptions
  ▸ There is a long-term relationship between the client and the network operator (home network) in the form of a contract
  ▸ The long-term relationship is represented by a long-term secret key shared by the client and network and serving as basis for identification

GSM Security Goals

▶ **Authentication**: Subscriber authentication
- ▶ challenge-response protocol
- ▶ long-term secret key between subscriber and HLR
- ▶ roaming without revealing long-term key to the VLR

▶ **Confidentiality**: Confidentiality of communications and signaling over wireless
- ▶ key shared between the subscriber and VLR established with the help of HLR

▶ **Privacy**: Protection of the subscriber's identity from eavesdroppers
- ▶ usage of short-term temporary identifiers

Subscriber Identity Module (SIM)

▶ **Protected by a PIN code**

▶ **Removable from the terminal**

▶ **Contains all data specific to the end user which have to reside in the Mobile Station:**

  ▶ IMSI: International Mobile Subscriber Identity (permanent user's identity)

  ▶ PIN

  ▶ TMSI (Temporary Mobile Subscriber Identity)

  ▶ K : User's secret key

  ▶ K_c : Ciphering key

  ▶ List of the last call attempts

  ▶ List of preferred operators

  ▶ Supplementary service data (abbreviated dialing, last short messages received,...)

Cryptographic Algorithms of GSM

R — Random number

K — User's secret key

A3

A8

R   S   K_c — Triplet

Authentication

A5 — Ciphering algorithm
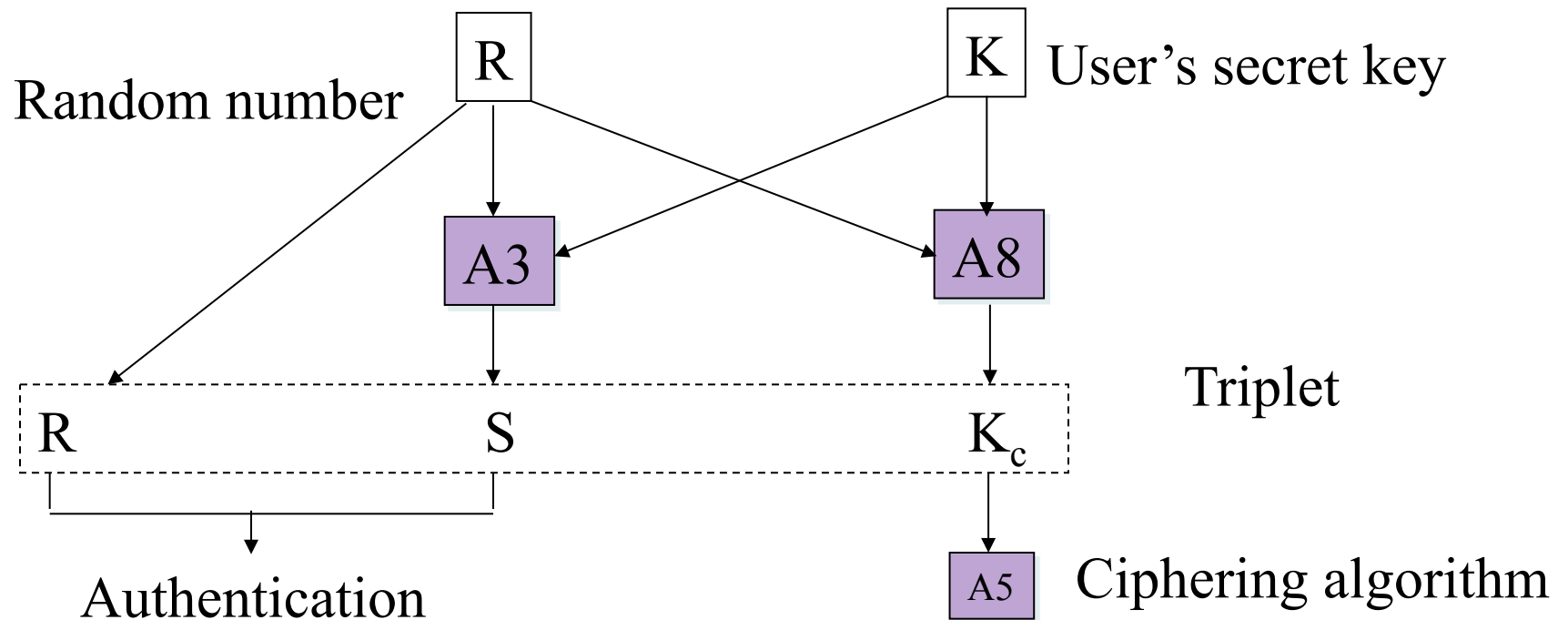
K_c: ciphering key
S : signed result
A3: subscriber authentication (operator-dependent algorithm)
A5: ciphering/deciphering (standardized algorithm)
A8: cipher generation (operator-dependent algorithm)

802.11 and cellular security.

Authentication Protocols of GSM

Mobile Station   Visited network   Home network

IMSI/TMSI

K R

A8   A3

IMSI (or TMSI)

IMSI

K_c S

Triplets (K_c, R, S)

Triplets

Authenticate (R)

K_i R

A8   A3

K_c S' Auth-ack(S')

S=S'?
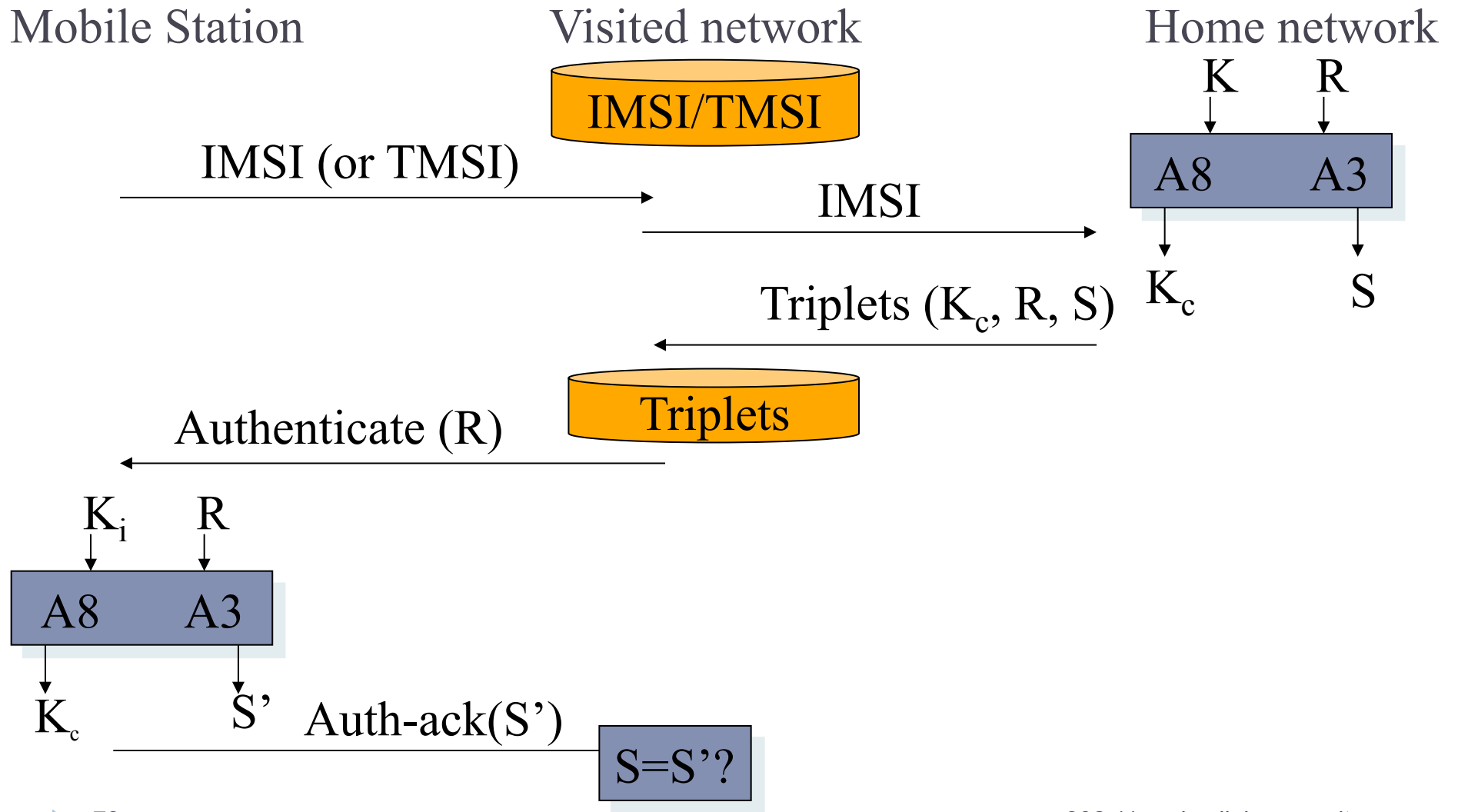
GSM Authentication

▸ Phone reads IMSI (International Mobile Subscriber Identity) from SIM and sends it to BS (network)

▸ The 'network' determines the identity of the client

▸ If this is not the home network, the identity is sent to the home network

▸ **Home network, looks up the secret K and sends (R, S, K_c) to the visited network,** where R is a challenge, S is the correct response to the challenge and K_c is a key for encryption

GSM Authentication

▸ R is a random number

▸ S is computed based on R and K using an algorithm known as A3

▸ K_c is computed based on R and K using an algorithm known as A8

▸ Visited network sends R to client

▸ Client computes S' and K_c' and sends them to visiting network

▸ Visiting network compares S' to S and K_c' to K_c and decides if the client was correctly authenticated

GSM Confidentiality

▶ Once the client is authenticated, encryption provided using A5 a stream cipher and the new key K_c

Encryption in GSM

K_c FRAME NUMBER

K_c FRAME NUMBER

A5

A5

CIPHERING
SEQUENCE

CIPHERING
SEQUENCE

PLAINTEXT
SEQUENCE

$\oplus$

CIPHERTEXT
SEQUENCE

$\oplus$

PLAINTEXT
SEQUENCE

Sender
(Mobile Station or Network)

Receiver
(Network or Mobile Station)
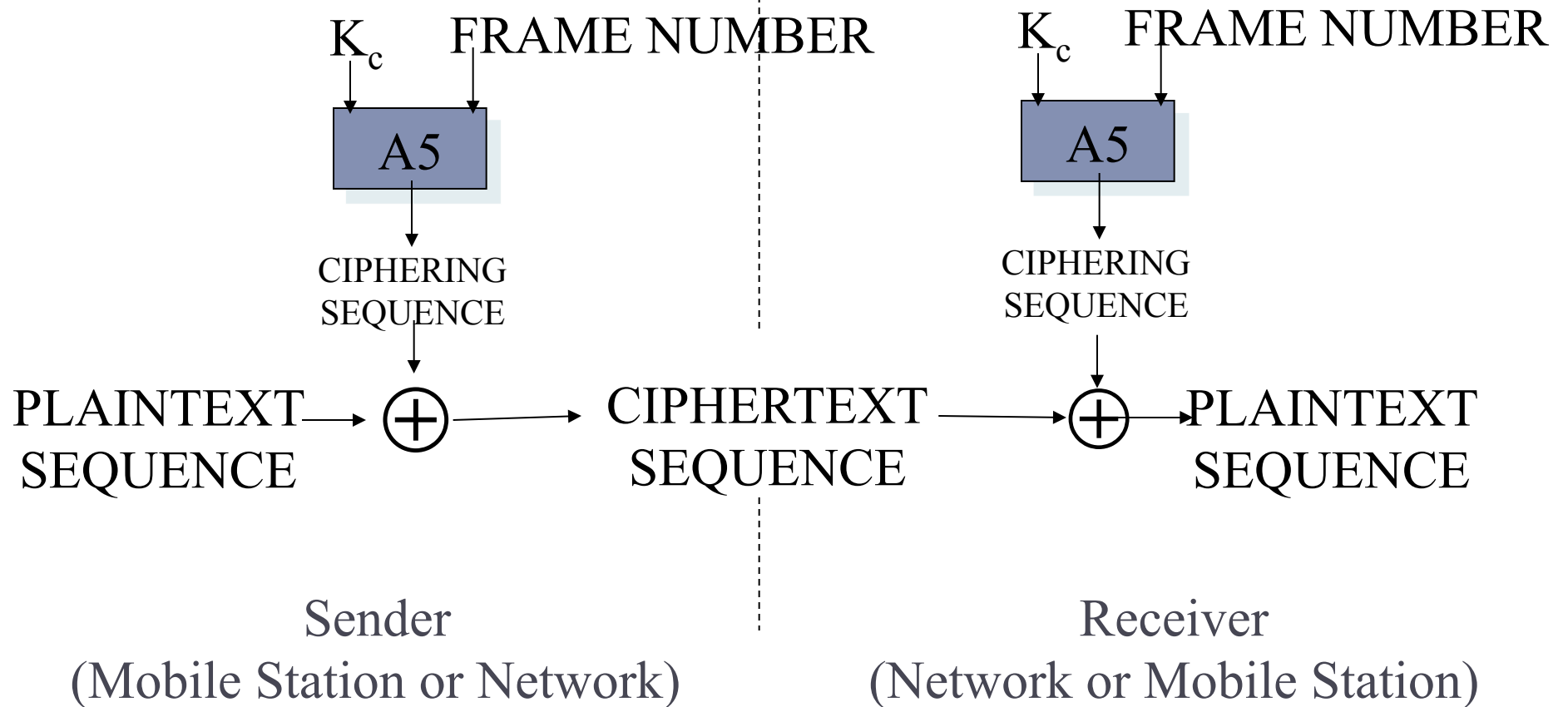
GSM Anonymity

▸ Client receives a temporary identification TMSI, encrypted with K_c

▸ In next authentication, the client can use the TMSI for authentication

▸ If the client moves into another visiting network, new one contacts previous one to obtain TMSI

▸ If data context (the authentication triple) is no longer available, client needs to send the IMSI (start over)

- What's wrong with the authentication protocol?
- Can you spot any problems?

Impersonating the Visiting Network

- The visiting network is never authenticated, some entity can impersonate the visiting network
  - faked base stations attacks, IMSI Catchers
  - technology to create these fake base stations is available

What if Crypto Algs Are Broken?

▸ If A5 is broken – anybody can decipher communication

▸ If A3 is broken – compute K based on S and R (which are sent on the air)

▸ If A8 is broken – secret key can be recovered based on R and K_c

R Random number

K User's secret key

A3

A8

Triplet

R   S K_c

Authentication

A5 Ciphering algorithm
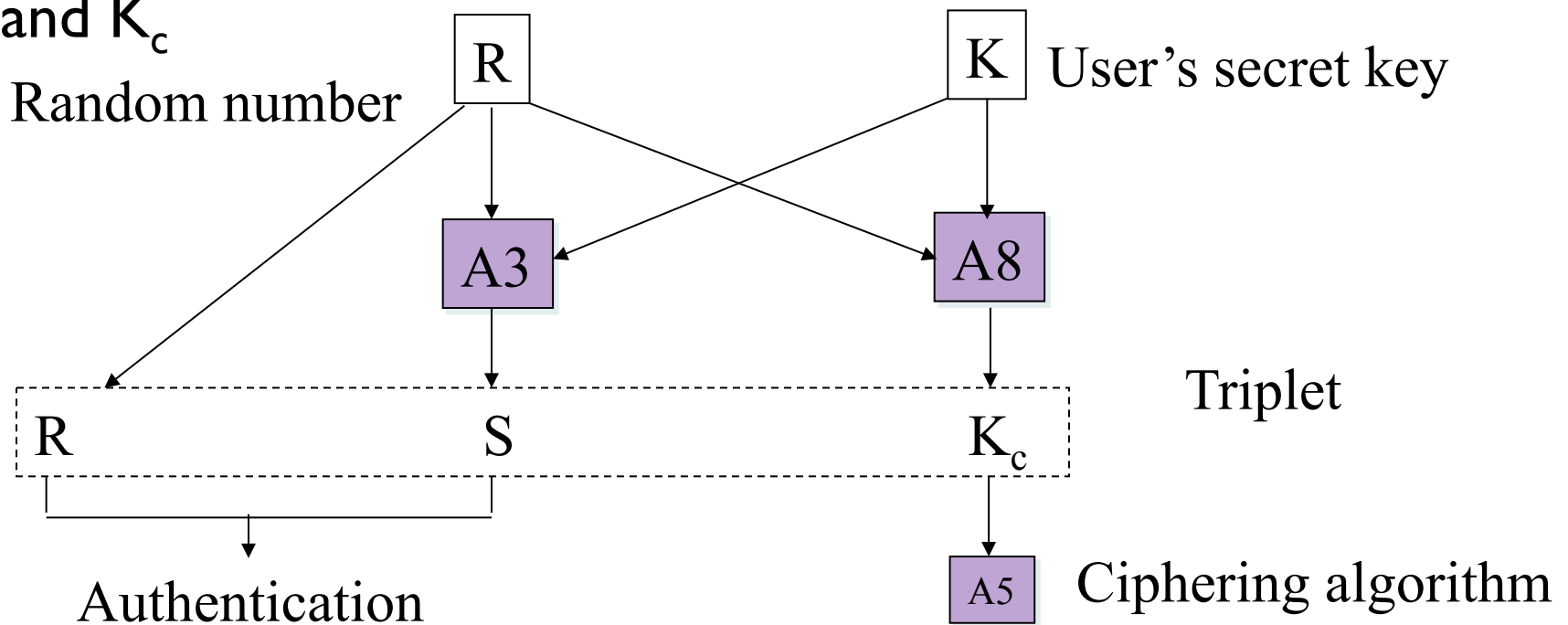
Attacks against A5/1

- ▶ Passive attacks A number of attacks on A5/1 using known plaintext attacks.

- ▶ 2003 Active attacks using ciphertext-only, 2003

- ▶ 2006 Real-time decryption attacks demonstrated

- ▶ 2009 German computer engineer Karsten Nohl announced that he had cracked the A5/1 cipher.

What about A3 and A8

▸ One implementation was COMP128 and variants

▸ Proprietary, closed designed

▸ Attacks were showed against COMP128 and some of the follow up variant, leading to phone cloning

▸ More about GSM cloning

  ▸ http://www.isaac.cs.berkeley.edu/isaac/gsm.html

802.11 and cellular security.

Summary on GSM security

- Focused on the protection of the air interface

- Visited network has access to all data (except the secret key of the end user)

- Successful attacks have been reported:
  - faked base stations
  - cloning of the SIM card
  - confidentiality broken

3G

- Was supposed to solve all problems and provide high-speed wireless communication, up to 2 Mbps
- Uses CDMA as channel access mechanism
- Many standards
  - UMTS, same as W-CDMA
  - Cdma2000
- Services available in Europe and Japan

3G Architecture
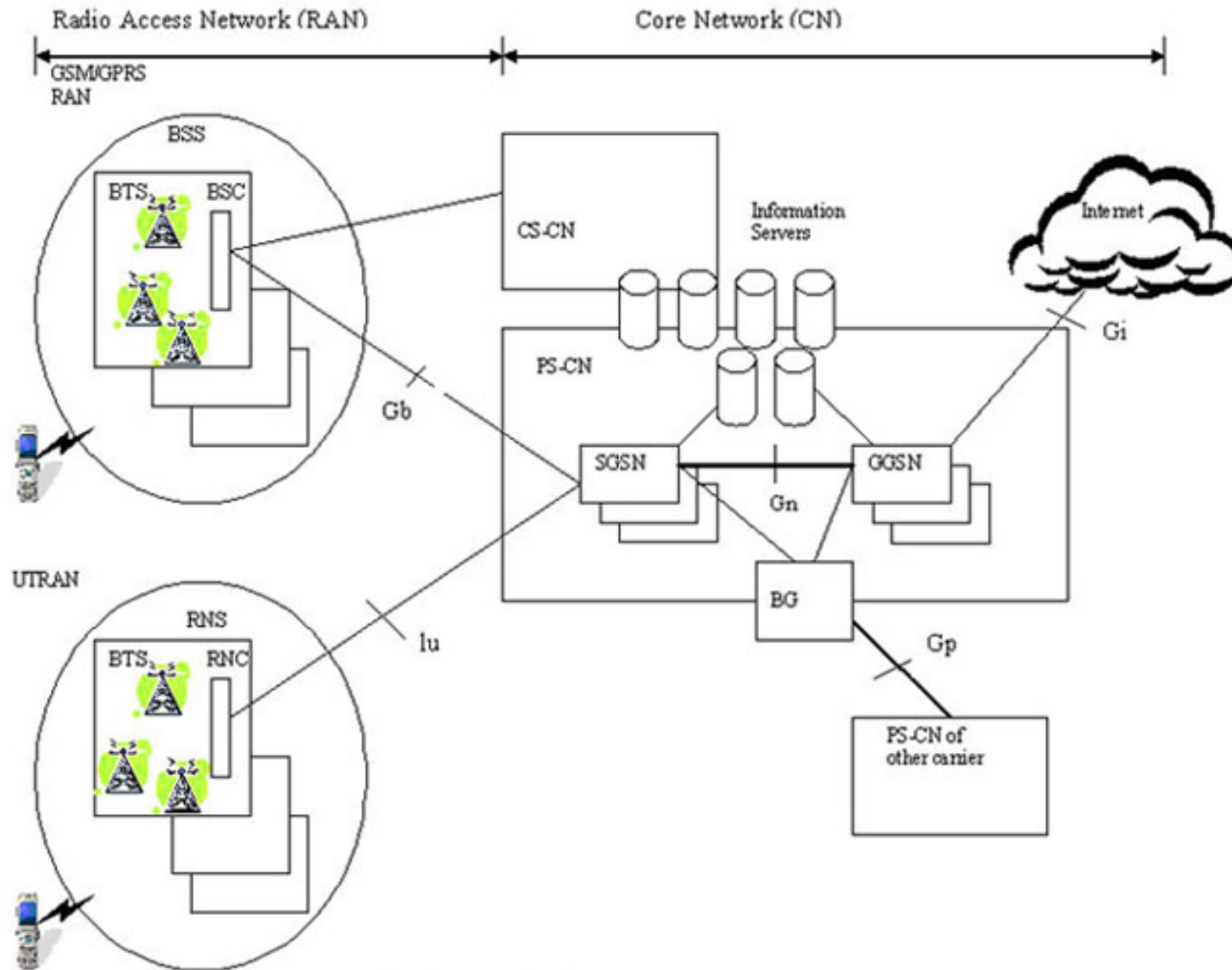
Fig 2. 3G Network Architecture

802.11 and cellular security.

Radio Access Network

- **GPRS/GSM RAN system which is connected to**
    - the Packet Switched Network (PS-CN) and
    - the Circuit Switched Network (CS-CN).
- **UTRAN (3G) consists of subsystems, with each subsystem consisting of one Radio Network Controller (RNC) which is connected to several Base Transceiver Stations (BTS).**

Core Network (PS-CN)

▸ SGSN connects one or more RSC and BSC with the PS-CN: provides access control, mobility management, paging and route management

▸ GGSN is the logical gateway to the Internet: can be used to connect to another PS-CN or carrier

▸ Information servers:

  ▸ (HLR) maintains subscriber information

  ▸ Authentication Center (AuC) maintains authentication information.

  ▸ IP based servers such as DNS, DHCP and RADIUS servers which interact with the SGSN/GGSN and provide control and management functions.

Issues with 3G

▸ CDMA was not as successful as thought in terms of:

  ▸ Solving interference

  ▸ Dropped calls

  ▸ Capacity

  ▸ Quality of speech

802.11 and cellular security.

3GPP Security

▸ Reuse of 2nd generation security principles (GSM):

  ▸ USIM (User Services Identity Module)

  ▸ Radio interface encryption

  ▸ Limited trust in the Visited Network

  ▸ Protection of the identity of the end user

▸ Correction of the following weaknesses of the previous generation:

  ▸ Possible attacks from a faked base station

  ▸ Cipher keys and authentication data transmitted in clear between and within networks

  ▸ Encryption not used in some networks

  ▸ Data integrity not provided

802.11 and cellular security.

3GPP Security

▶ **New security features**

- ▶ New kind of service providers (content providers, HLR only service providers,…)

- ▶ Increased control for the user over their service profile

- ▶ Enhanced resistance to active attacks

- ▶ Increased importance of non-voice services

Authentication in 3GPP

Mobile Station   **Visited Network**   **Home Environment**

Sequence number (SQN) $RAND(i)$

K: User's secret key → Generation of cryptographic material

Authentication vectors

IMSI/TMSI

K

User authentication request
$RAND(i) \| AUTN(i)$

Verify $AUTN(i)$
Compute $RES(i)$

User authentication response $RES(i)$

Compare $RES(i)$
and $XRES(i)$

K

Compute $CK(i)$
and $IK(i)$

Select $CK(i)$
and $IK(i)$

▶ 97
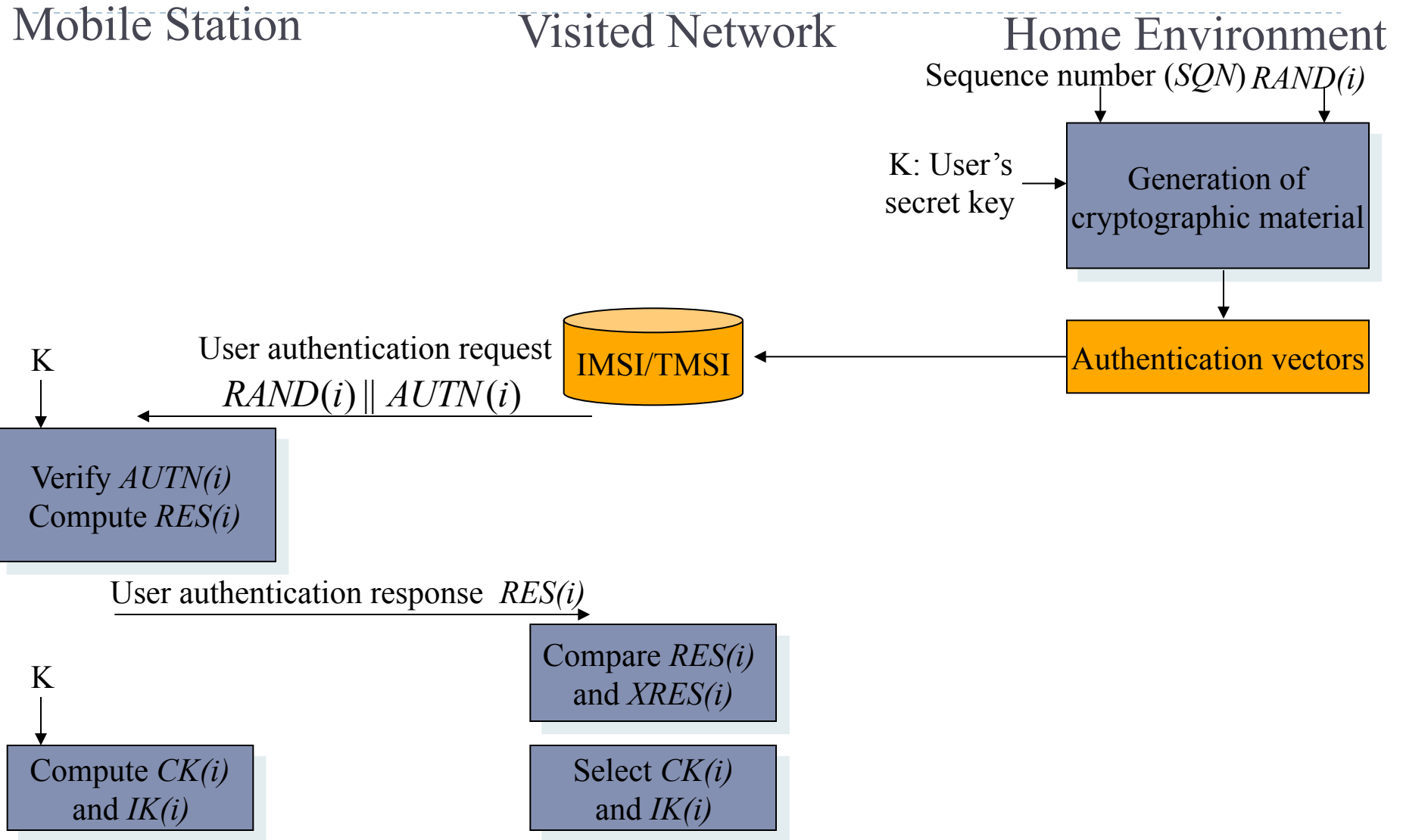
Generation of Authentication Vectors
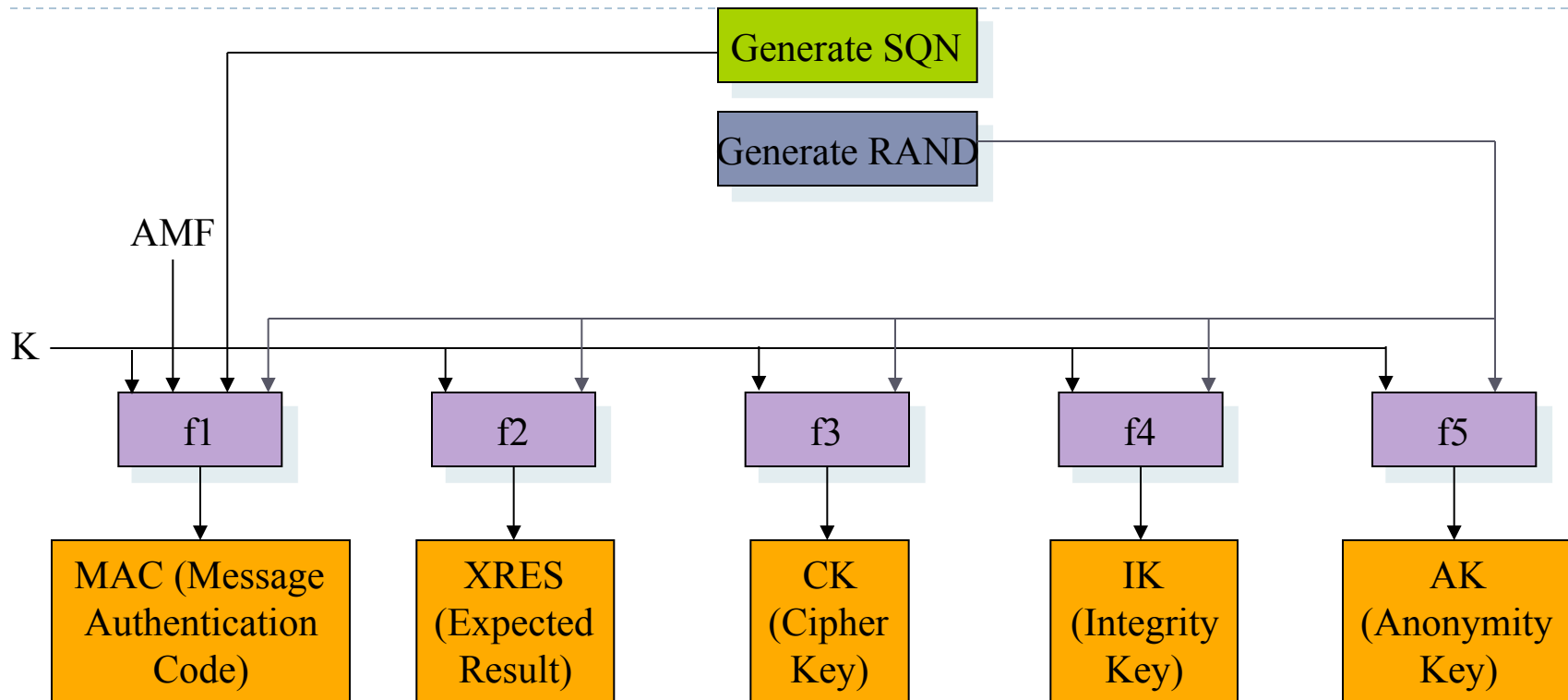
$$AUTN := (SQN \oplus ACK) \| AMF \| MAC$$

$$AV := RAND \| XRES \| CK \| IK \| AUTN$$

AMF: Authentication and Key Management Field
AUTN: Authentication Token
AV: Authentication Vector

User Authentication Function in the USIM

- Verify MAC = XMAC
- Verify that SQN is in the correct range

USIM: User Services Identity Module
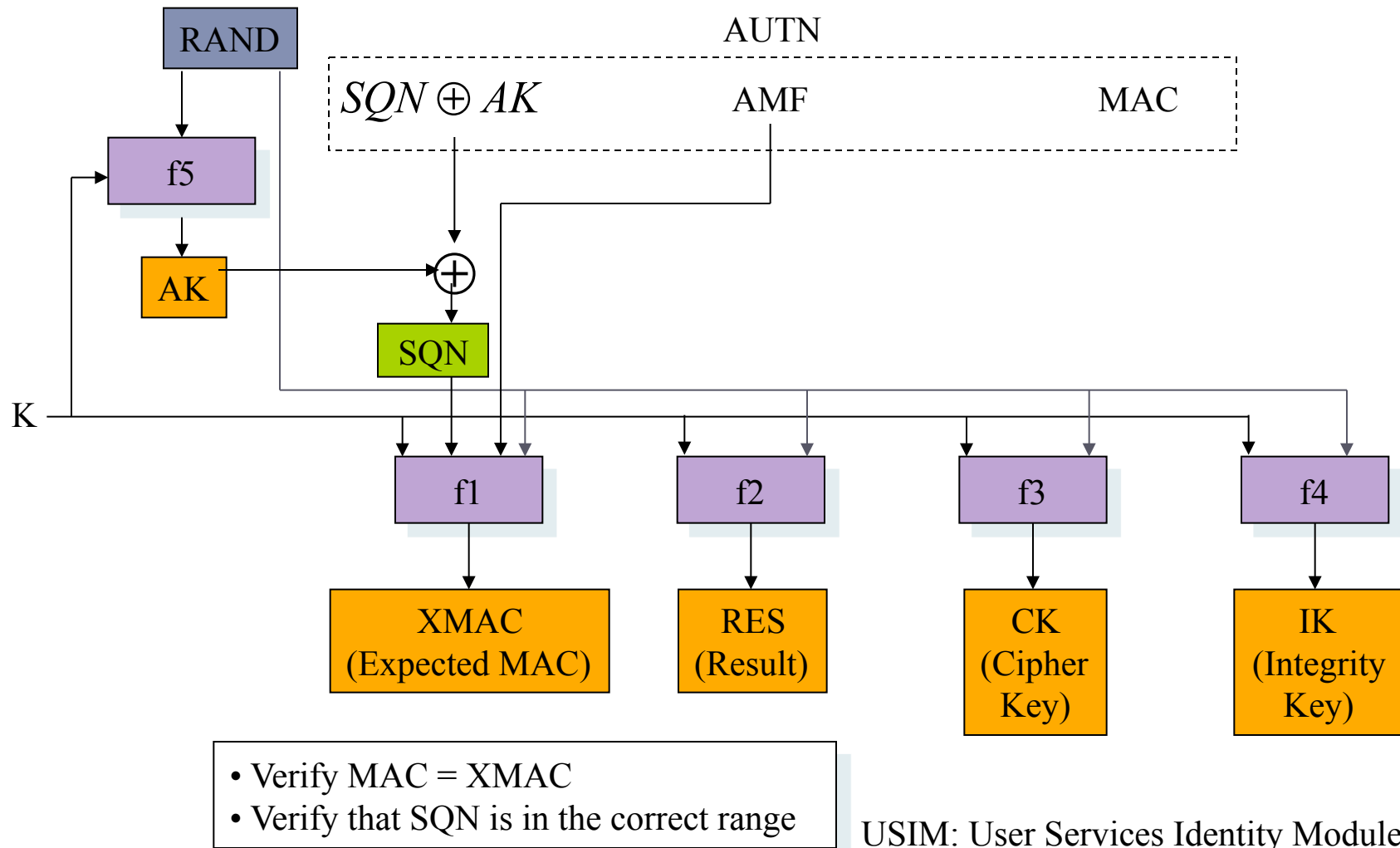
Authentication and Key Generation

▸ In addition to f1, f2, f3, f4 and f5, two more functions are defined: f1* and f5*, used in case the authentication procedure gets desynchronized (detected by the range of SQN).

▸ f1, f1*, f2, f3, f4, f5 and f5* are operator-specific

▸ However, 3GPP provides a detailed example of algorithm set, called *MILENAGE*

▸ MILENAGE is based on the *Rijndael* block cipher

▸ In MILENAGE, the generation of all seven functions f1…f5* is based on the Rijndael algorithm

Functions f1...f5*
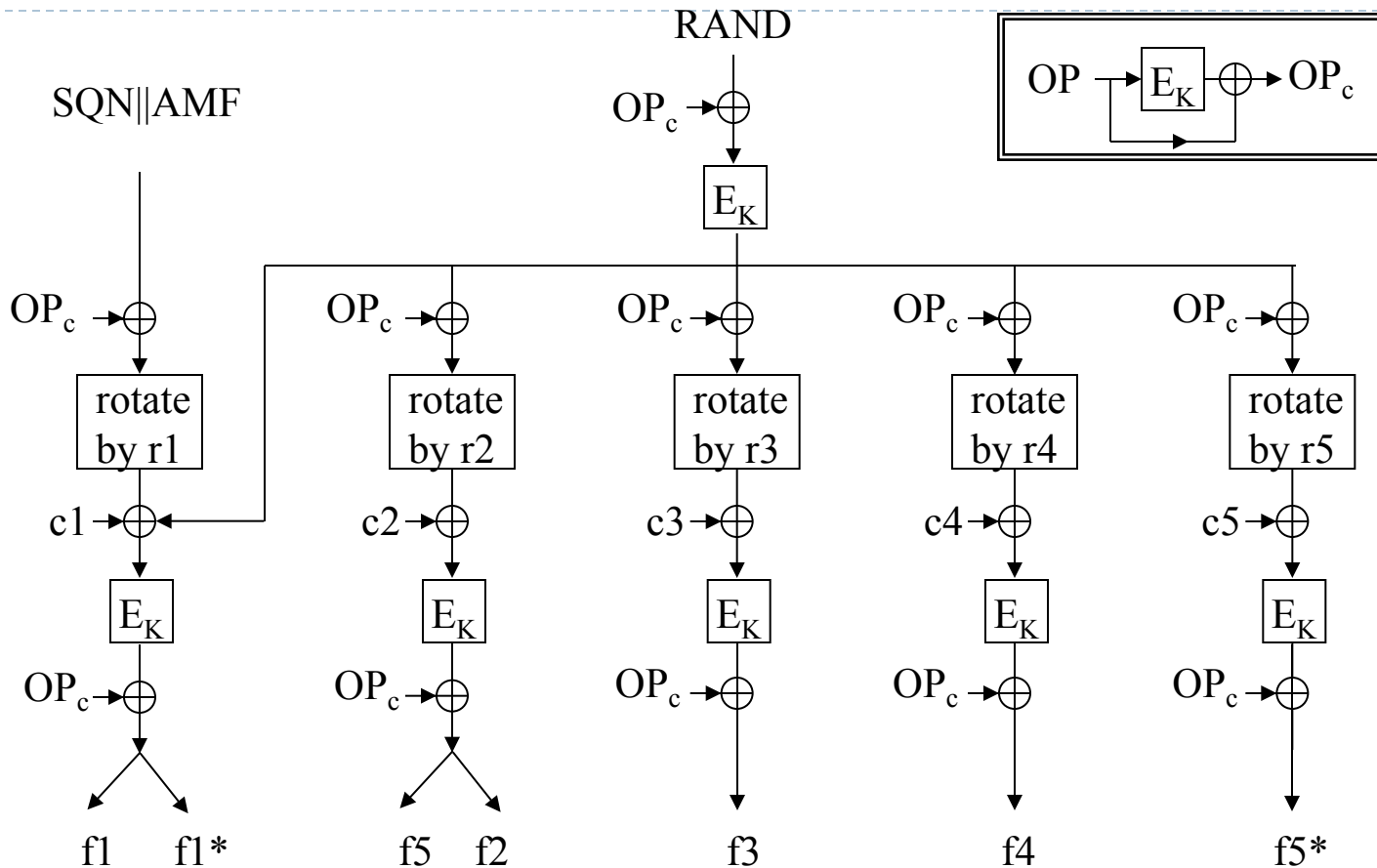
OP: operator-specific parameter
r1,…, r5: fixed rotation constants
c1,…, c5: fixed addition constants

E_K : Rijndael block cipher with 128 bits text input and 128 bits key

What About Crypto Algs?

▸ 2010, reports of a new attack that had "broken Kasumi" (also known as A5/3), the standard encryption algorithm used to secure traffic on 3G GSM wireless networks, by means of a sandwich attack (a type of related-key attack), allowing them to identify a full key

Summary on 3GPP security

- Some improvement with respect to 2nd generation
  - Cryptographic algorithms are published
  - Integrity of the signalling messages is protected
- Privacy/anonymity of the user not completely protected
- 2nd/3rd generation interoperation might open security breaches
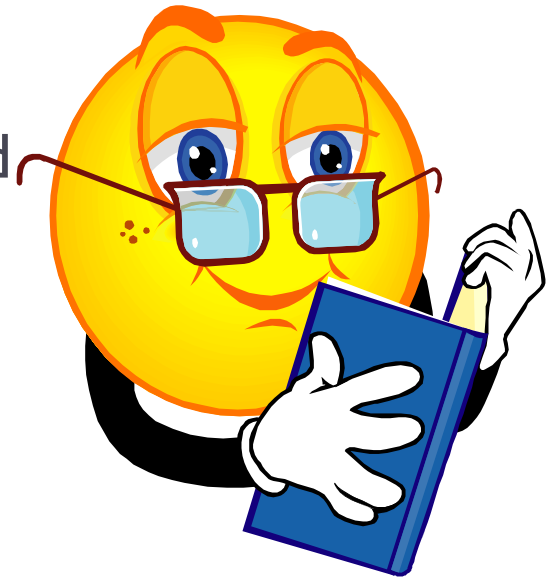
Attacks against Infrastructure

▸ Cellular protocols and infrastructure are more complex

▸ What happens with the wired infrastructure

▸ Are there ways in which attackers can exploit one service to attack other services?

SMS Architecture
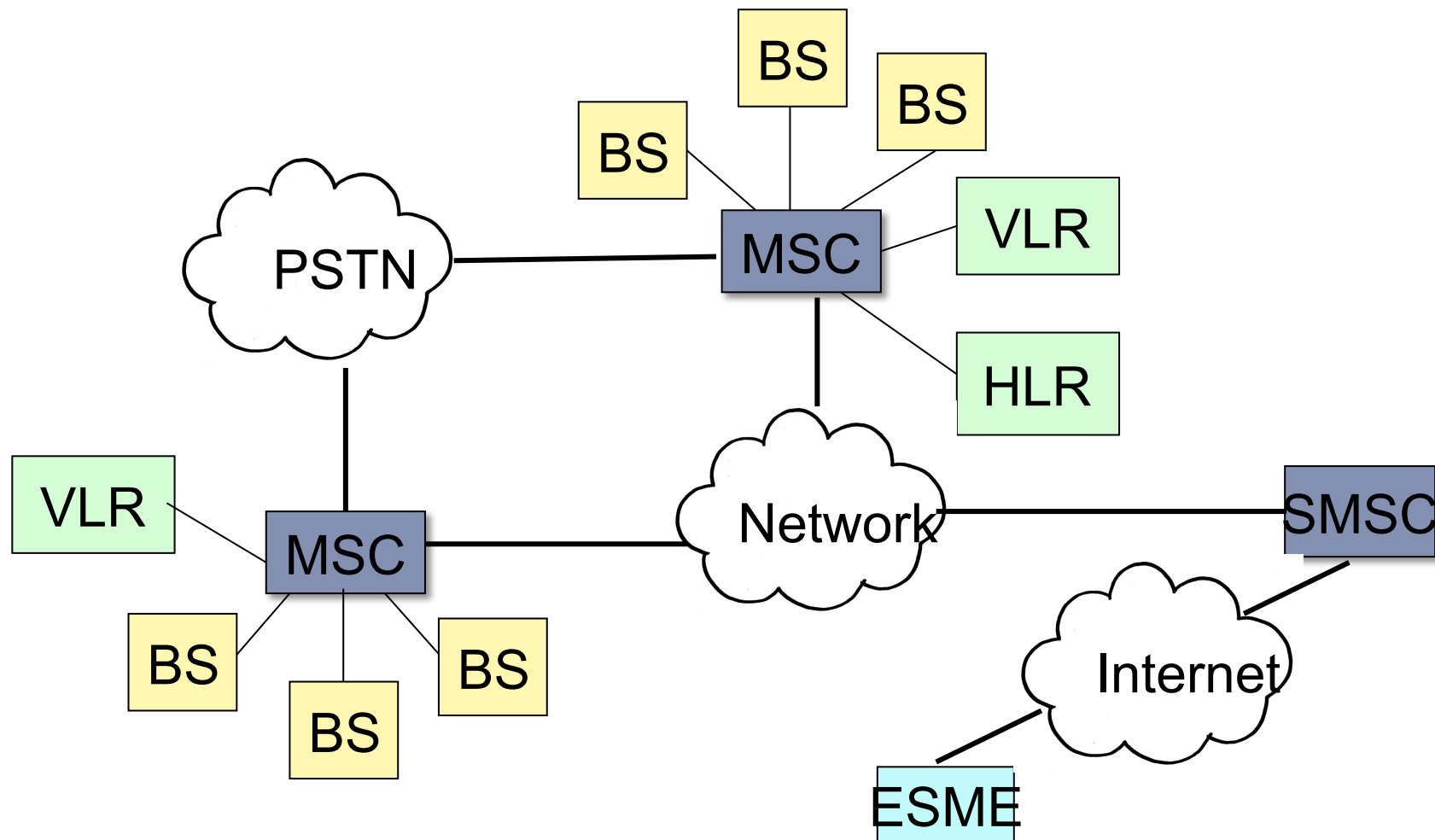
SMS Communication

- Control channel (CCH)
  - Paging channel PCH
  - Random access channel RACH
  - Standalone dedicated control channel SDCCH

- Traffic channel (TCH)
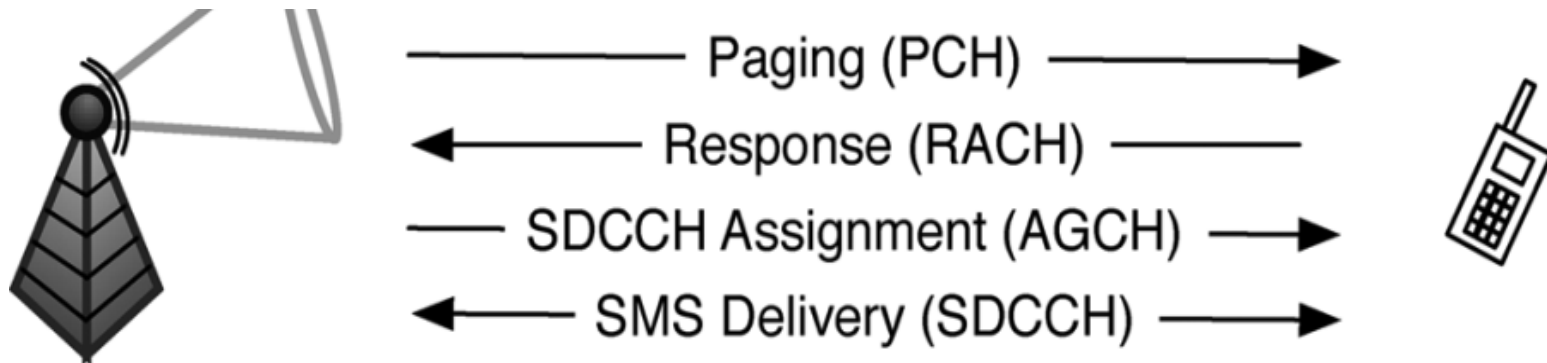
Exploiting ESME to Block Calls

▸ All messages pass through SMSC

▸ SMSC have buffer and eviction policies that did not take into account denial of service from ESME

▸ Creating a hit-list

  ▸ Internet search for NPA/NXX DB

  ▸ Web Scraping

  ▸ Worm, for example device recently call lists

Solutions

▶ Eliminating Internet-originated SMS

▶ Separation of voice and data

▶ Resource provisioning

▶ Rate limitation

4G Architecture

http://burgami.com/4g
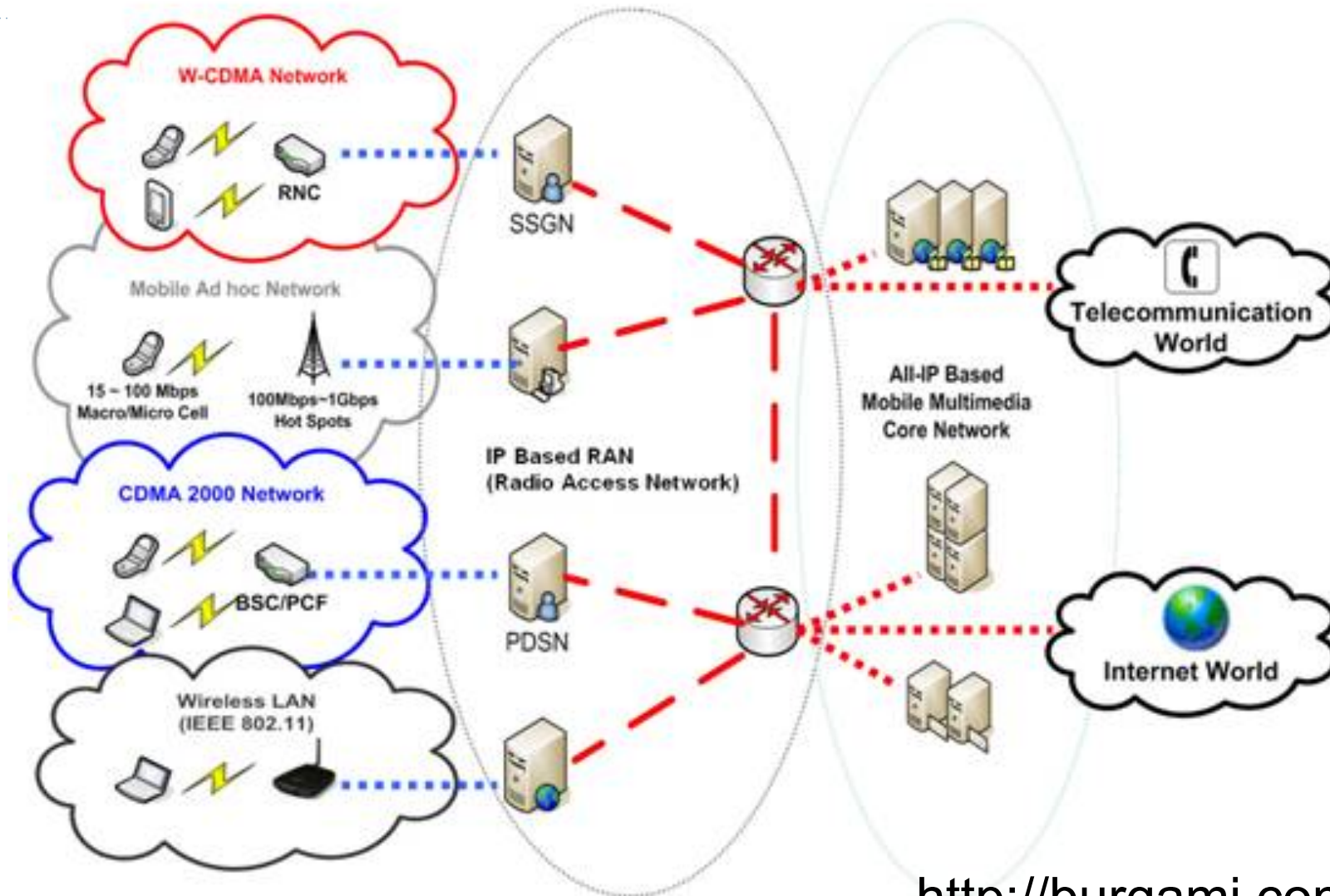
802.11 and cellular security.

What's New in 4G

▸ Layered Protocols

▸ IP plays a significant role, through the use of IMS architecture

▸ More complex, interface with other protocols will make it more vulnerable

Evolving Security Architecture
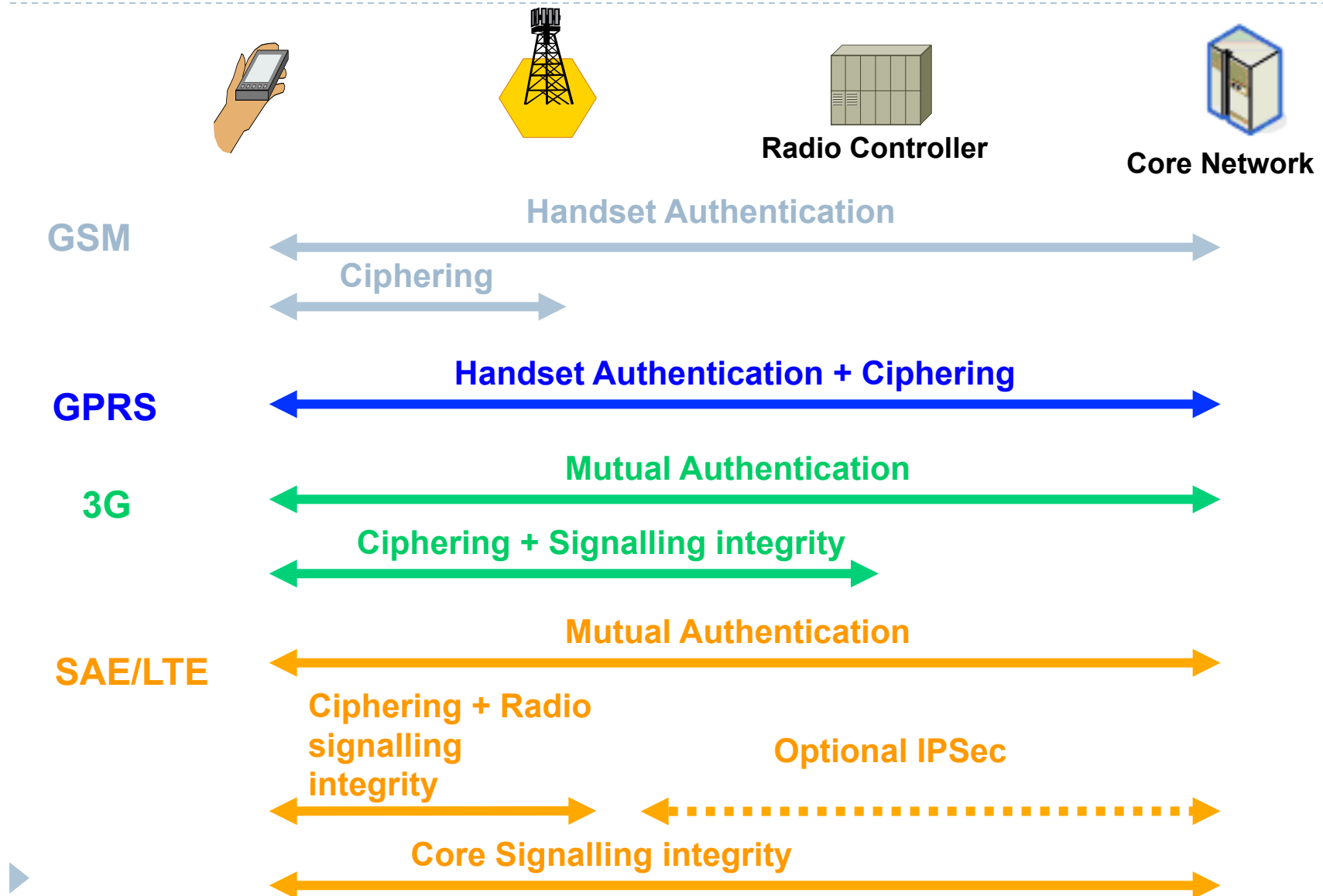
Attacks against Smartphones

▸ They are running operating systems

▸ Attacks on such devices started to appear

▸ Vulnerabilities in OS

▸ Applications get more rights than they should

Security Issues Related to Smartphones

▸ **Smartphones contain private data**

  ▸ from sensors: location, microphone, camera, accelerometer

  ▸ database: address book, SMS storages

  ▸ phone identifiers: IMEI, phone #, SIM card ID

  ▸ indirectly: files shared w/ other app, msgs from other app

▸ **Opportunities to leak private data**

  ▸ transmits out the network interface

  ▸ indirectly: files shared and msgs sent to other app

Android

- Open software platform for mobile development

- A complete stack – OS, Middleware, Applications

- An Open Handset Alliance (OHA) project

- Powered by Linux operating system

- Fast application development in Java

- Open source under the Apache 2 license

802.11 and cellular security.
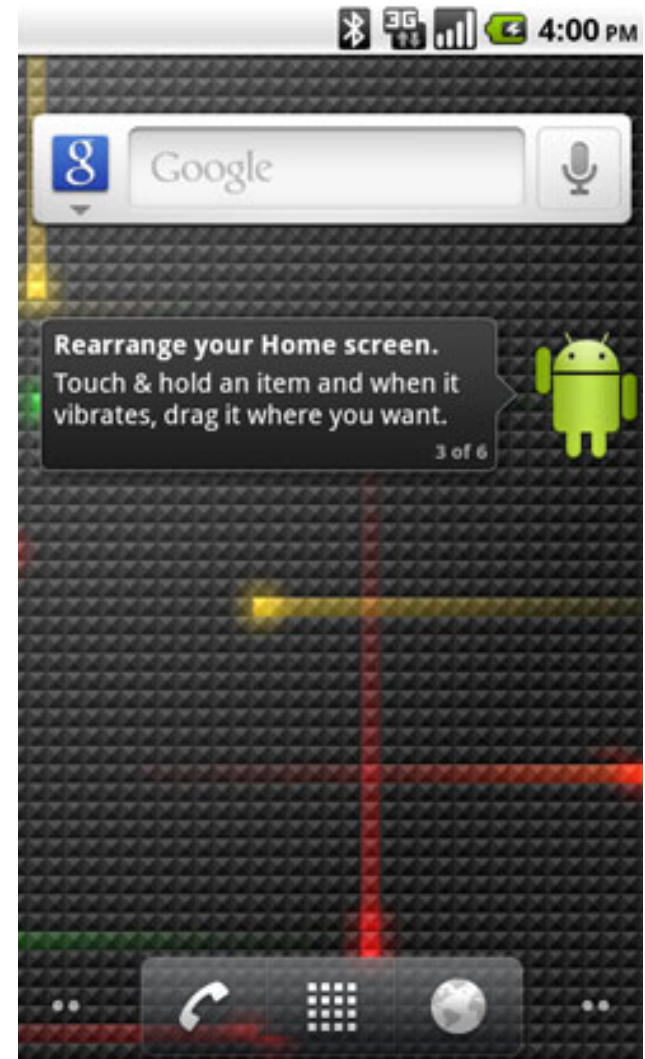
TaintDroid

▸ Used taint analysis to evaluate what applications are leaking information

  ▸ gives up instructional level tracking

  ▸ tracks data flow only, not control flows

  ▸ coarse granularity

    ▸ use one tag for array/file/msg

    ▸ higher false positive rate

▸ Implemented on Android

▸ Examined a representative set of applications

Performance

CaffeineMark 3.0 benchmark
(higher is better)
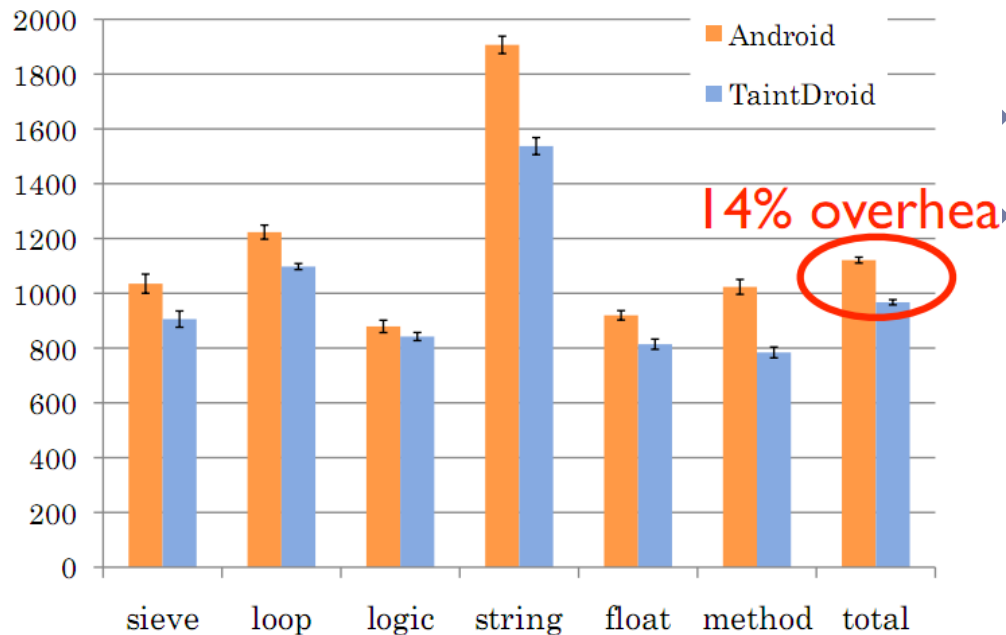
14% overhead

- Memory overhead: 4.4%
- IPC overhead: 27%
- Macro-benchmark:
  - App load: 3% (2ms)
  - Address book: (< 20 ms) 5.5% create, 18% read
  - Phone call: 10% (10ms)
  - Take picture: 29% (0.5s)

116

Application Study

▸ Selected 30 applications with bias on popularity and access to location, camera, microphone and phone IDs

applications	#	permissions
The Weather Channel, Cetos, Solitarie, Movies, Babble, Manga Browser	6	📡
Bump, Wertago, Antivirus, ABC --- Animals, Traffic Jam, Hearts, Blackjack, Horoscope, 3001 Wisdom Quotes Lite, Yellow Pages, Datelefonbuch, Astrid, BBC News Live Stream, Ringtones	14	📡 📞
Layer, Knocking, Coupons, Trapster, Spongebot Slide, ProBasketBall	6	📡 📷 📞
MySpace, Barcode Scanner, ixMAT	3	📷
Evernote	1	📡 📷 🎤

802.11 and cellular security.

Findings – Location Info Leak

- **Of 105 flagged connections, only 37 clearly legitimate**

- **15 of the 30 applications shared physical location with an ad server**
  - admob.com, ad.qwapi.com, ads.mobclix.com, data.flurry.com

- **Frequency**
  - one application transmits the phone information every time the phone boots
  - In some cases, periodic and occurred without app use

Findings – Phone Identifiers

- 7 applications sent device (IMEI) and 2 apps sent phone info (Ph. #, SIM ID) to a remote server without informing the user
  - One app's EULA indicated the IMEI was sent
  - Another app sent the hash of the IMEI
- Appeared to be sent to app developers ...
- Most traffic was plaintext (e.g., AdMob HTTP GET)

```
...&s=a14a4a93f1e4c68&..&t=062A1CB1D476DE85
B717D9195A6722A9&d%5Bcoord%5D=47.6612278900
00006%2C-122.31589477&...
```

Iphone Location Storage Findings

▶ **Iphone and Android have both previously transmitted their locations back to Google and Apple.**

▶ **It was shown that iPhone is collecting and storing location information <u>even when location services are turned off</u>**

  ▶ Location data appear to be collected using cellphone towers and Wi-Fi access points

  ▶ Location is stored on an unencrypted location file on the iPhone

Summary Cellular Networks Security

- GSM encryption broken

- 3G encryption attacks reported

- With more complex services and interface with IP, more attacks on the core

- Expect more security issues in upcoming 4G

- Recent security and privacy problems related to smartphones