3G Security

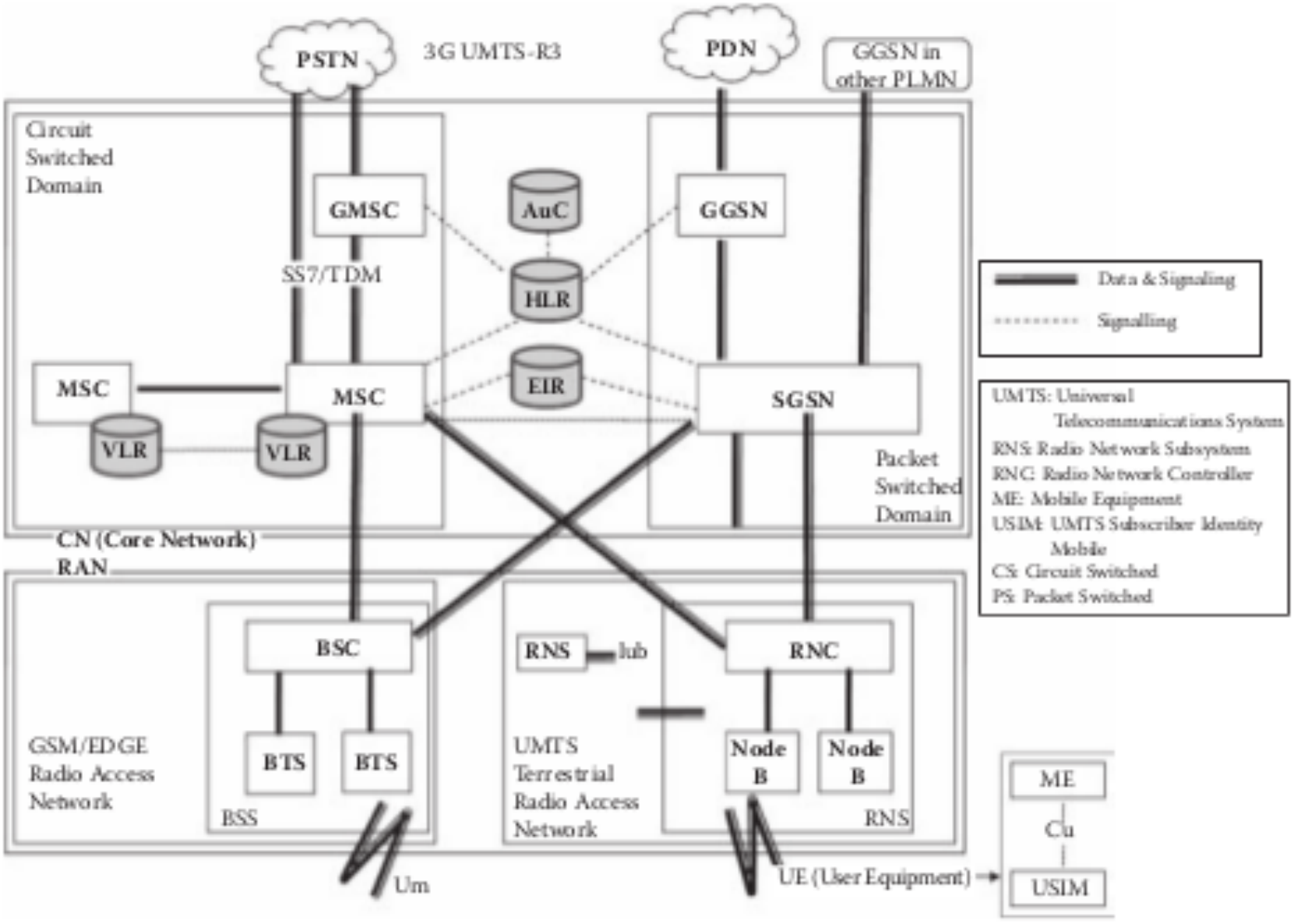
Retention of 2G Security Features [1]

- SIM-based authentication
- Confidentiality of user traffic
- Confidentiality of user identity (anonymity)
  - retain the concept of TMSI

Universal Mobile Telecommunications System (UMTS)

- Developed by thd 3rd Generation Partnership Project (3GPP).
- Main difference between UMTS and GSM/GPRS is higher access rates.
  - Achieved through Wideband Code Division Multiple Access (W-CDMA).
- UMTS network can be logically divided into two parts [1]
  - Core Network (CN)
    - carries out switching functions and interfaces to external networks
  - Radio Access Network (GRAN)
    - manages the air interface and radio resources.

UMTS Network



Source: [1].

UMTS Components

- Mobile Station (MS)
  - Contains a Universal Subscriber Identity Module (USIM).
- UMTS Terrestrial Radio Access Network (UTRAN)
  - Two types of components
    - Node-Bs - roughly corresponds to a BTS in GSM
    - Radio network controller (RNC) - roughly corresponds to BSC in GSM.
- Core Network
  - MSC, HLR, VLR, AuC
  - Serving GPRS Support Node (SGSN) [1]
    - Management of mobility
    - handling of IP packet sessions
    - routes packet traffic to the ad hoc Gateway GPRS Support Node (GGSN) - gateway between cell network and packet data networks such as the Internet.

Network Access Security [1]

- User identity confidentiality
- Authentication and key agreement
- Data confidentiality
- Integrity protection of signaling messages

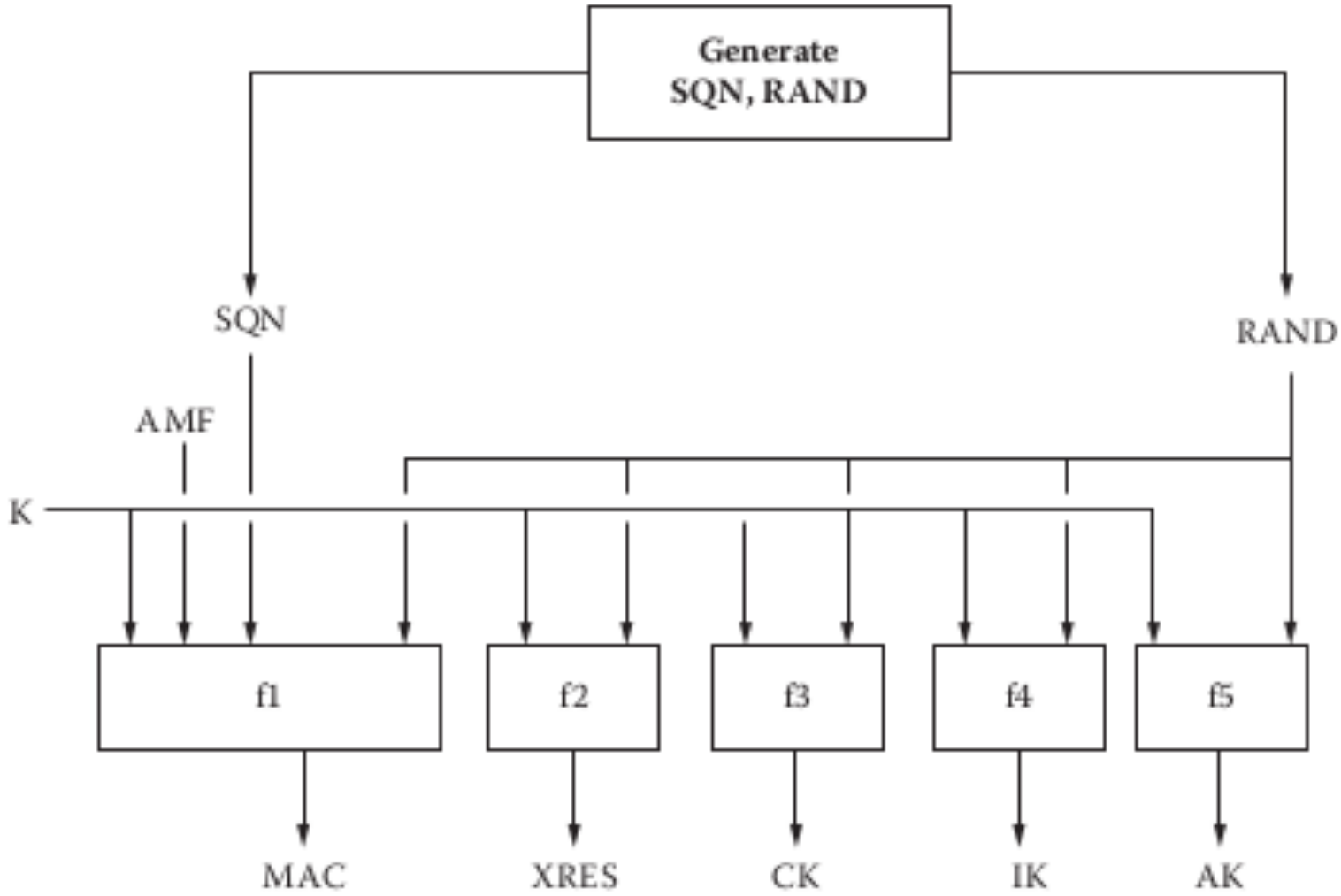
User Identity Confidentiality [1]

- Identification of a user on the radio access link by a temporary identifier - Temporary Mobile Subscriber Identity (TMSI).
- Protects against passive eavesdroppers. Protects against tracking of users.
- Temporary identity cannot be used on initial registration, permanent identity (IMSI) is sent instead.
- Association between TMSI and IMSI is stored in the VLR.
- TMSI is sent to the user in encrypted form.

Authentication and Key Agreement [1]

- AuC provides serving network's VLR with Authentication Vecors (AVs).
- Each AV consists of
  - random number RAND
  - expected response XRES
  - cipher key CK
  - integrity key IK
  - authentication token AUTN

Generation of Authentication Vector



Source: [1].

Generation of Authentication Vector

- The AuC maintains a sequence number SQN. It generates a fresh random number RAND.
- Using the secret key K, it computes a MAC with the function $f1$

$$\text{MAC} = f1(K, \text{SQN}, \text{RAND}, \text{AMF})$$

where AMF (Authentication Management Field) is used for operator-specific options in the authentication process e.g: limitation of the lifetime of a key [2].

Generation of Authentication Vector [1]

- The next component is the expected response XRES given by

$$\text{XRES} = f2(K, \text{RAND})$$

where $f2$ is a message authentication function that is possibly truncated.

- The following component is the cipher key CK given by

$$\text{CK} = f3(K, \text{RAND}).$$

.

- The next component is the integrity key IK given by

$$\text{IK} = f4(K, \text{RAND}).$$

- The next component is the anonymity key AK given by

$$\text{AK} = f5(K, \text{RAND}).$$

- Note that $f3, f4$ and $f5$ are key generating functions.

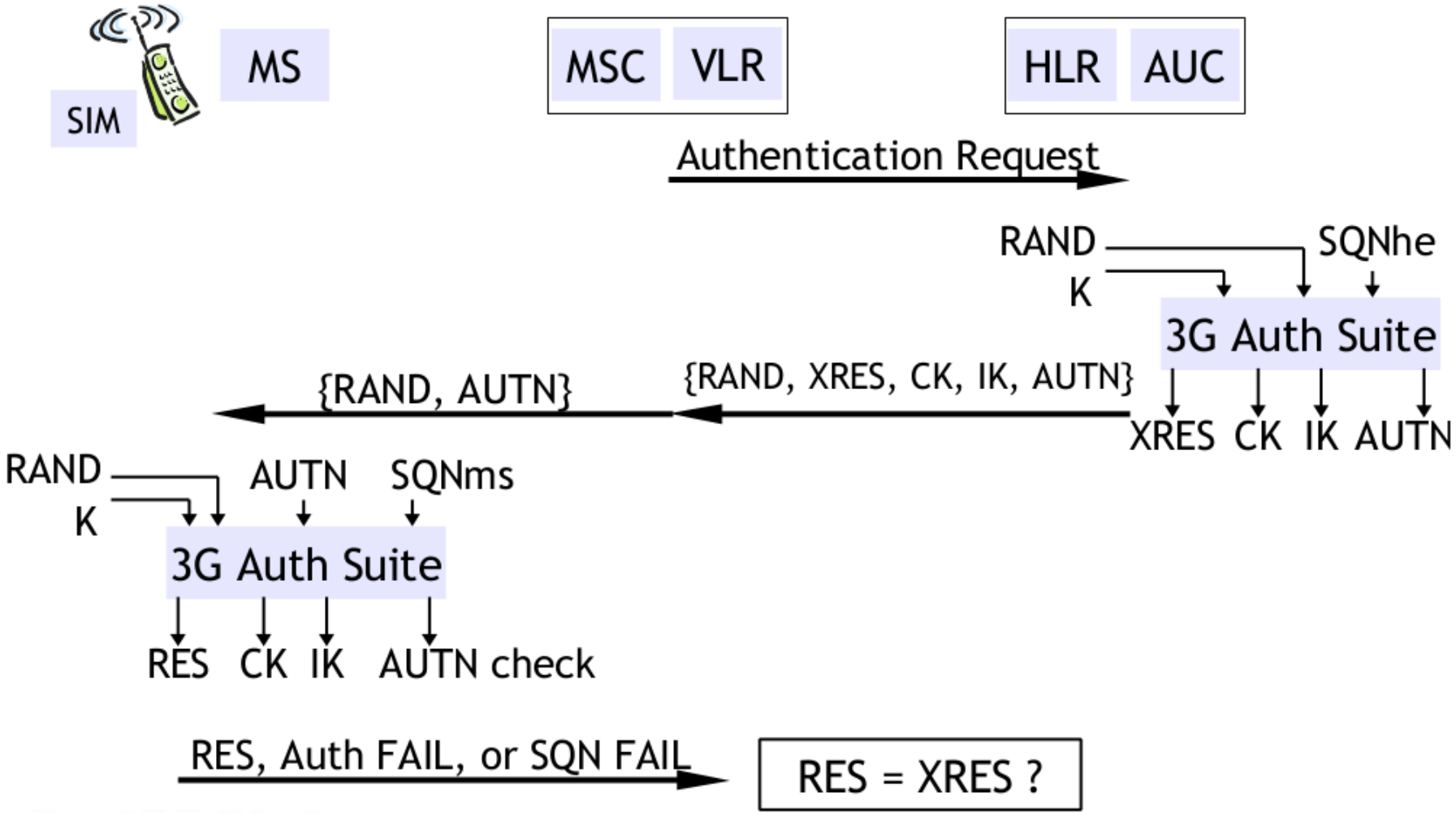
Generation of Authentication Vector [1]

- The final component is the authentication token AUTN computed by

$$\mathrm{AUTN} = (S := \mathrm{SQN} \oplus \mathrm{AK}, \mathrm{AMF}, \mathrm{MAC}).$$

- When the VLR/SGSN begins an authentication and key agreement process:
  - it selects the next AV from the vector of AVs.
  - sends the parameters RAND and AUTN to the MS.
- Using the secret key K, the USIM runs the following steps:
  1. compute the key AK as $\mathrm{AK} = f5(K, \mathrm{RAND})$.
  2. recover SQN by computing $\mathrm{SQN} = S \oplus \mathrm{AK}$.
  3. If SQN is less than the MS's current sequence number, send back ther response "synchronization failure".
  4. compute $\mathrm{XMAC} = f1(K, \mathrm{SQN}, \mathrm{RAND}, \mathrm{AMF})$.
  5. if XMAC does not match MAC, send back the response "MAC failure".
  6. compute $\mathrm{RES} = f2(K, \mathrm{RAND})$.
  7. Send back RES as authentication response.
  8. Compute keys $\mathrm{CK} = f3(K, \mathrm{RAND})$ and $\mathrm{IK} = f4(K, \mathrm{RAND})$.

Authentication and Key Agreement



Source: [3].

Encryption (Stream Cipher $f8$)

- UMTS uses the stream cipher function $f8$ for encryption.
- $f8$ takes as input:
  - 128-bit secret key CK.
  - 32-bit value called COUNT.
  - 5-bit value called BEARER.
  - 1-bit value called DIRECTION.
- The keystream of a given length ℓ is generated with

$$\text{keystream} = f8(\text{CK}, \text{BEARER}, \text{DIRECTION}, \ell).$$

- The ciphertext is obtained by computing $\text{ciphertext} = \text{plaintext} \oplus \text{keystream}$ where plaintext is the frame's data.
- The KASUMI algorithm is used to implement $f8$.

MAC ($f9$ Function) [1]

- The function $f9$ is used for checking authenticity and integrity of signaling messages between the MS and RNC.
- $f9$ computes a 32-bit MAC, which is appended to the frame.
- The algorithm takes as input:
  - 128-bit secret integrity key IK
  - variable length message, denoted by MESSAGE
  - 32-bit value called COUNT
  - 32-bit value called FRESH
  - 1-bit value called DIRECTION
- A MAC is computated as

$$\text{MAC} = f9(\text{IK}, \text{COUNT}, \text{MESSAGE}, \text{DIRECTION}, \text{FRESH}).$$

- $f9$ is applied only to the signaling data (not the user data).
- The implementation of $f9$ is based on the KASUMI algorithm.

KASUMI Block Cipher

- Derived from MISTY1 designed by Mitsubishi
- Key size is 128 bits
- Block size is 64 bits
- 8 rounds (uses a Feistel network)
- Broken by Dunkelman, Keller and Shamir using a related key attack - January 2010 (MISTY1 isn't affected by their technique).

Mitigating Weakesses in 2G [1]

The following are weaknesses in 2G which have been mitigated by 3G.

- Active attacks with a rogue BTS
- Cipher keys and authentication data are sent in the clear between/within networks
- Encryption is used on the wireless link. Communication of user and signaling data such as between BTS and BSC is not encrypted.
- Data integrity is not provided. Data integrity prevents certain rogue BTS attacks and protects against channel hijack.
- The IMEI is unsecured.
- the home enviornment operator doesn't know or can't control how a serving network uses authentication parameters for subscribers roaming in that serving network.
- 2G systems lack the flexibility to upgrade and improve security over time.

Protection Against Some Types of Attack

- DoS attacks using request spoofing have been made infeasible in 3G by providing integrity and non-replay of signaling requests.
- Active attacks such as impersonation of a network or impersonation of a user in 2G are made infeasible in 3G by providing integrity of signaling messages.
- Identity catching: counteracted in UMTS by integrity of signaling data and by using an encryption key shared by a group of users to protect the IMSI [4].

Note a modified femotocell can be used to build an IMSI catcher for 3G [5].

Attacks on 3G

- DoS Attacks
- IMSI Catcher with a modified femotocell [5].
- GSM attacks due to interoperability between 3G and GSM: forcing an MS to use GSM by for example jamming the 3G bands.
- Redirection of traffic from one network to another via a false base station [6].
- Authentication and Key Agreement (AKA) linkability attack: tracking users by distinguishing between MAC failures and synchronization failures [7].

Denial of Service [1]

- Suppose a false base station is set up with a strong signal signal such that an MS camps to it. The MS is then out of reach of paging signals of the serving network - deprived of service.
- If the false BS also contains a modified MS, the attacker can connect to the serving network and selectively relay messages to the user.
- Radio jamming: attacker can jam the UMTS bands; MS can't connect to the network.

Redirection Attack [6]

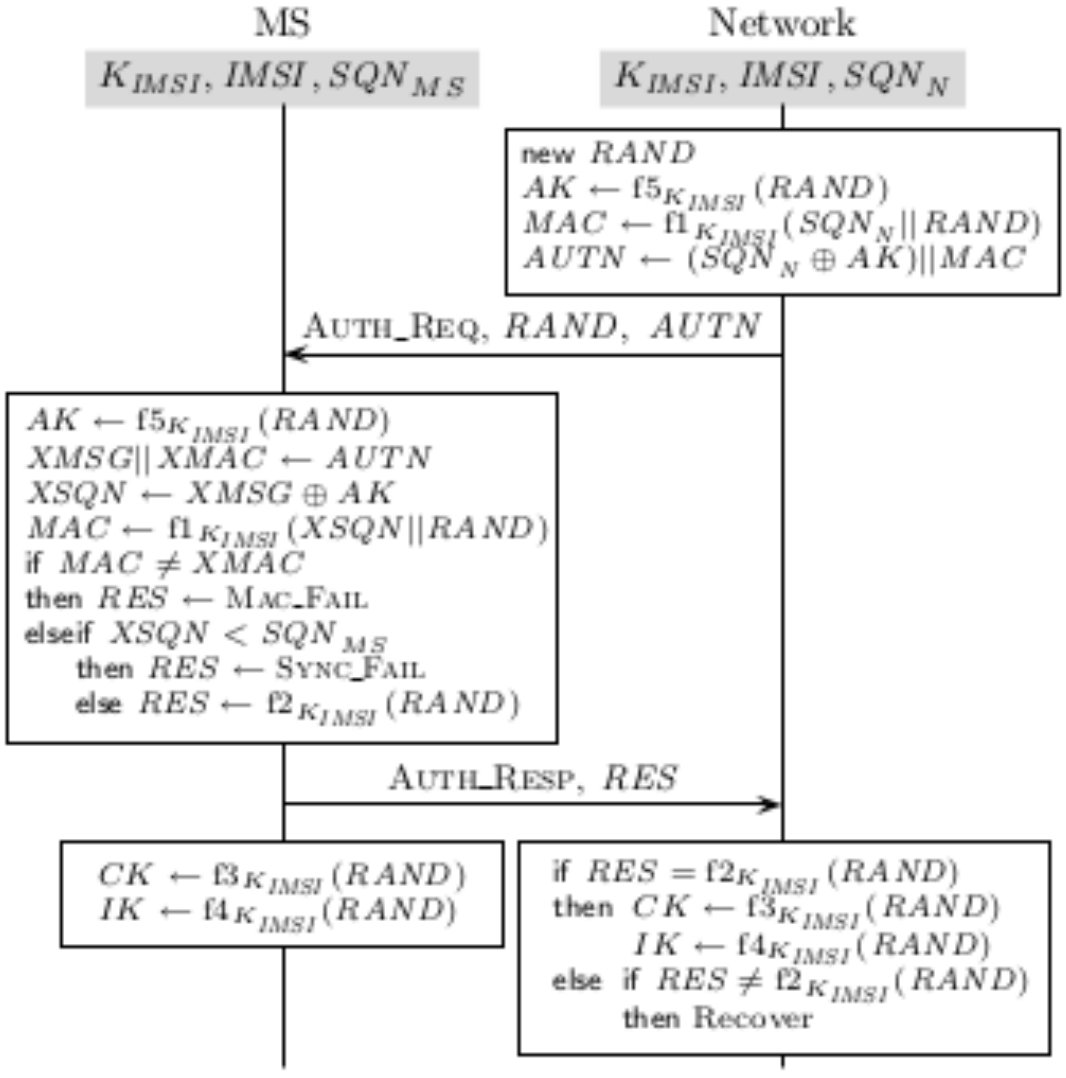
Assume the user is in the area of his home network HN. The attacker uses a fake BS/MS. The attacker does the following

- Set up a false base station and attract the victim to camp on it. The victim is then out of reach of the paging signals sent by HN.
- Through a modified MS in the false base station, the attacker connect to a foreign network SN on behalf of the victim's MS.
- Relay messages between MS and the foreign network SN.

Note authentication will be successful on the MS and in SN. Suppose SN charges higher prices for services, then the attacker causes the victim to be charged more. Furthermore, suppose SN does not enable encryption (unlike say HN), then the attacker can eavesdrop on the victim's data.

AKA Linkability Attack [7]

Let's recap on the AKA protocol, which consists of two messages: an authentication request and an authentication response.

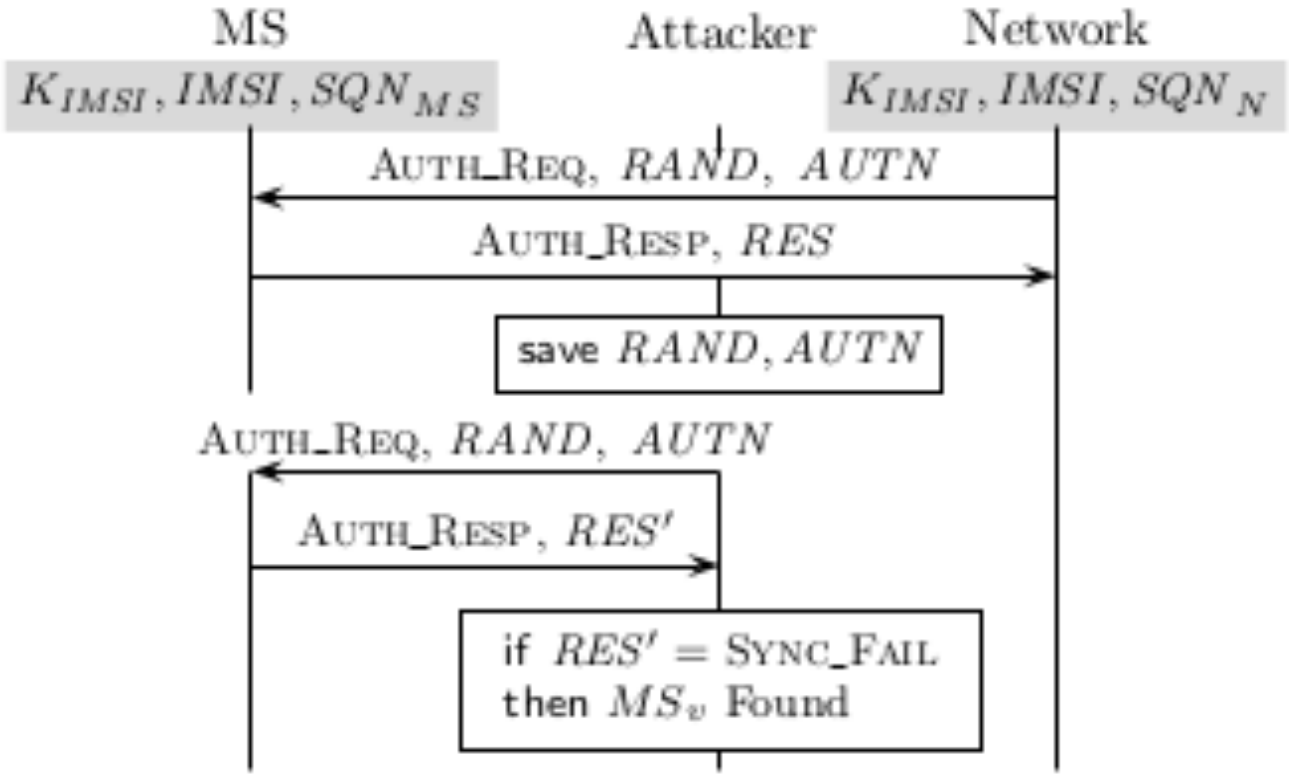


Source: [7].

AKA Linkability Attack [7]

- Suppose the attacker wishes to target an MS M.
- He captures an authentication request message $(\mathrm{RAND}, \mathrm{AUTN})$ that is sent to M.
- Later he sets up a fake base station and replays the captured authentication request to all MSs in the area.
- MSs other than M respond with a MAC failure because the authentication request was not constructed with the secret key of M.
- M responds instead with a synchronization failure
  - the sequence number M recovers from the authentication request is less than its current sequence number.
- The attacker can distinguish between the two responses and therefore can find M.

AKA Linkability Attack [7]



Source: [7].

References I


Boudriga, N.:
Security of Mobile Communications. 1st edn.
Auerbach Publications, Boston, MA, USA (2009)


Pütz, S., Schmitz, R., Martin, T.:
Security mechanisms in UMTS.
Datenschutz und Datensicherheit **25** (2001)


Tague, P.:
Mobile security: Telecom security from 1g to 4g.
`http://wnss.sv.cmu.edu/courses/14829/f13/files/14829f13_03.pdf` (2013)


Vinck, B., Horn, G., Muller, K.:
A viable security architecture for umts.
ACTS Mobile Submmit, Sorrento, Italy (1999)

References II


Golde, N., Redon, K., Borgaonkar, R.:
Weaponizing femtocells: The effect of rogue devices on mobile telecommunications.
In: NDSS, The Internet Society (2012)


Zhang, M., Fang, Y.:
Security analysis and enhancements of 3gpp authentication and key agreement protocol.
Trans. Wireless. Comm. **4** (2005) 734–742


Arapinis, M., Mancini, L.I., Ritter, E., Ryan, M., Golde, N., Redon, K., Borgaonkar, R.:
New privacy issues in mobile telephony: fix and verification.
In Yu, T., Danezis, G., Gligor, V.D., eds.: ACM Conference on Computer and Communications Security, ACM (2012) 205–216