Mobile Wireless Security

A short overview of security mechanisms in mobile communication

Kjetil Frigstad

Introduction

Mobile communication is a big part of daily life.

Besides voice communication we are able to access the internet, conduct transactions , send text messages etc.

However the wireless medium is limited, such as open access , bandwidth and system complexity.

Limits the max amount of overhead, and complexity we can add with the security features.

There is also restrictions due to battery life time in the user equipment. This limits the amount on processing available

Introduction

-The radio link is an open medium. This means that there is a possibility of someone intercepting the transmission.

-Lots of sensitive data that needs to be kept from third parties.

-Need to authenticate users to protect operators against billing fraud.

-The identity of the users needs to be kept safe.

The security mechanism must not increase overhead on call setup, increase the bandwidth of the channel, increase error rate or add expensive complexity to the system.

GSM

-Mobile Station (MS)

-Physical mobile device identified by IMSI.

-Subscriber Identity Module (SIM)

-Smart card containing keys, identifiers and algorithms.

Ki: unique key

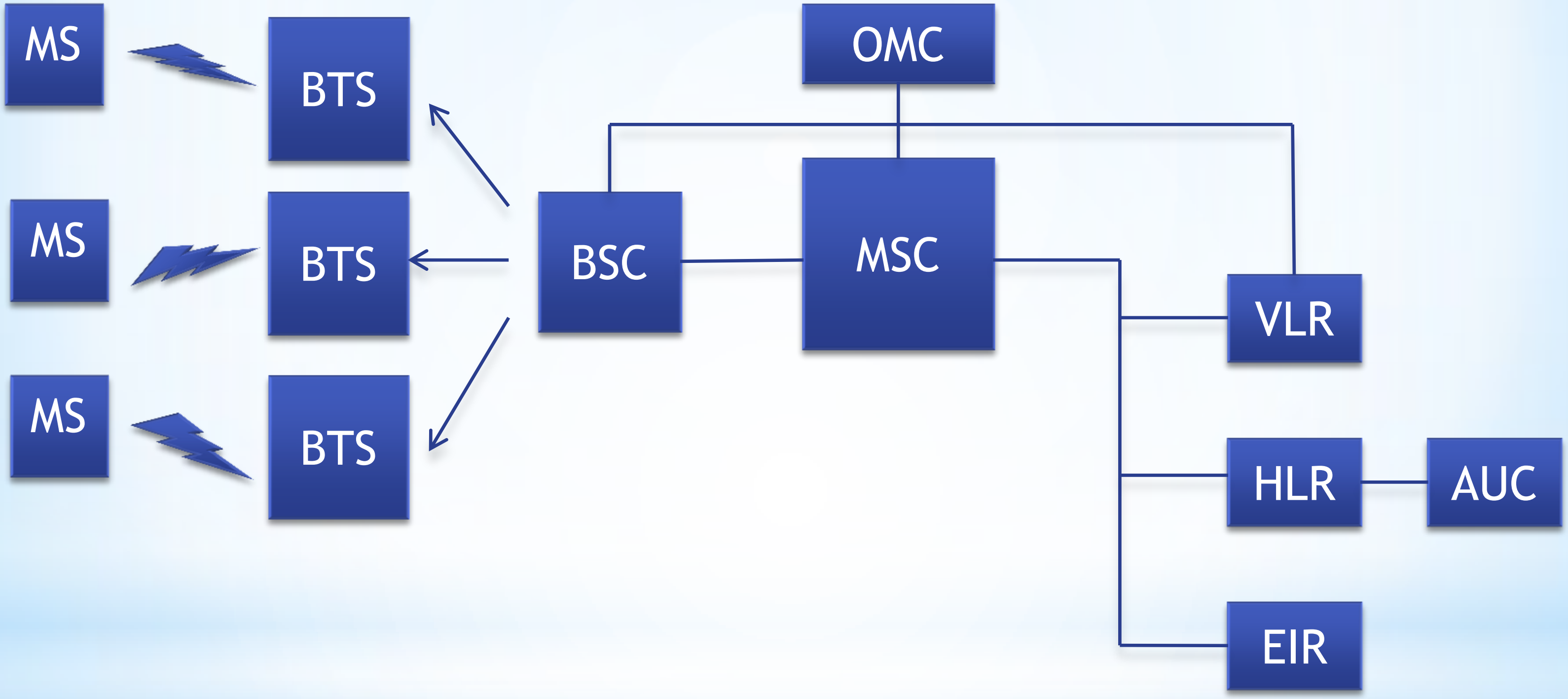
IMSI, TMSI : identifiers

MSISDN: phone number, used for routing calls to the subscriber.

PIN: local security code (only on MS).

LAI: location area identity, used for location update

GSM architecture



Network Databases

HLR: Contains all administrative info about each user, as well as current location

VLR: Tracks mobile user that are out of the home network

EIR: Contains white list, grey list and blacklist

AUC: IMSI - International mobile subscriber identity

TMSI - Temporary mobile subscriber identity

LAI - Location Area Identity

Ki - Authentication Key (128 bit)

Identity Protection

-TMSI is used instead of IMSI over the air interface

-TMSI prevents a potential eavesdropper from identifying the subscriber

-TMSI is assigned when IMSI is transmitted to AUC on the first phone switch on

-For every location update (new MSC) the network provides a new TMSI

-TMSI is used by MS to report to the network during a call initialization.

-The network uses TMSI to communicate with MS

-On MS switch off, TMSI is stored in the SIM card for reuse.

-The VLR performs assignment, administration and update of the TMSI.

Authentication

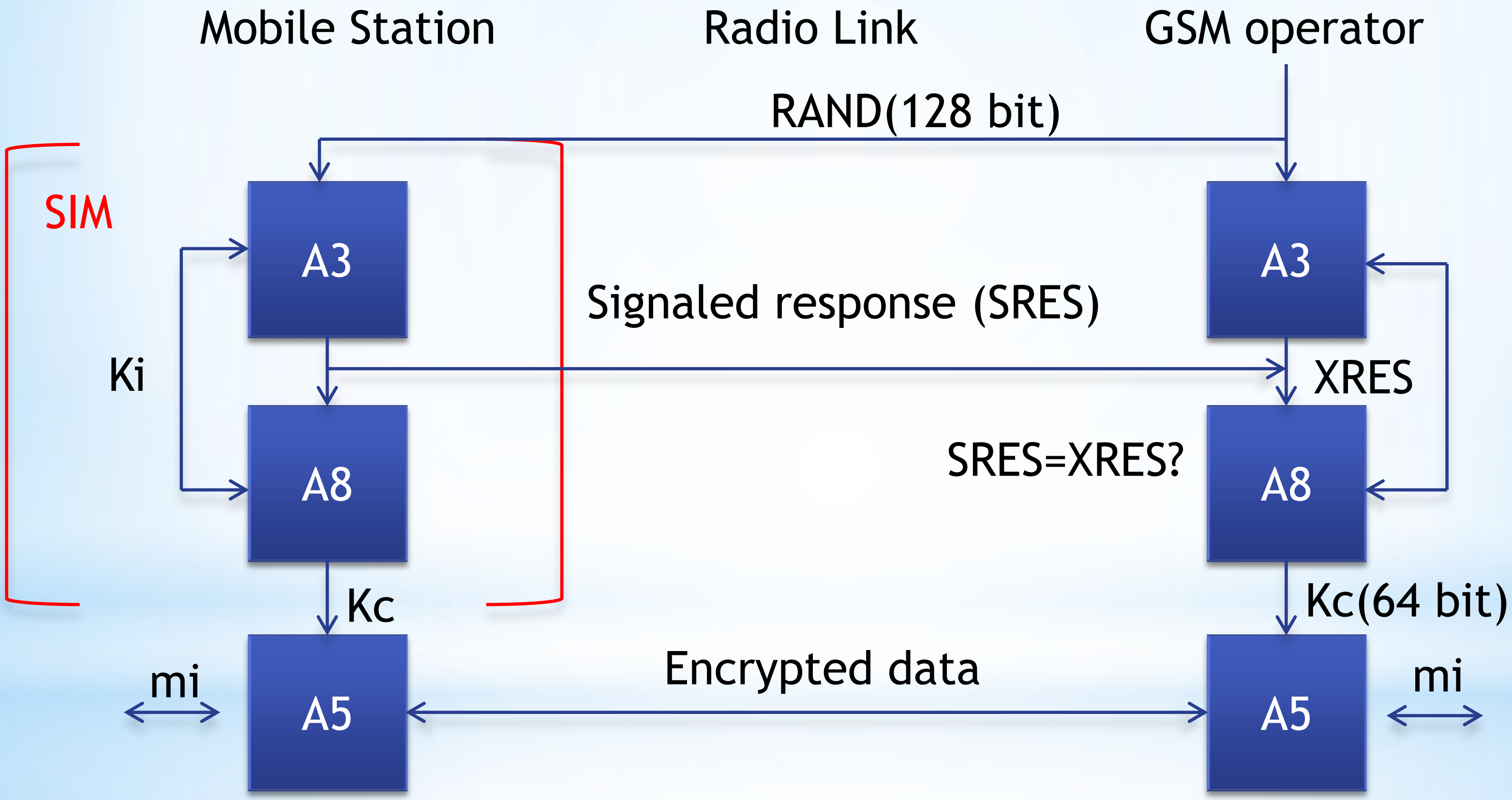
Authentication goals:

- -Authenticate the subscriber (SIM)
- -Protect the network against unauthorized use
- -Create a session key

Authentication scheme:

- -Subscriber identification (IMSI or TMSI)
- -Challenge-response authentication of the subscriber by the operator

Authentication and encryption



-The Authentication Center (AUC) provides parameters for RAND, XRES, Kc.

-The Home location register(HLR) provides the MSC with the information

-The Visitor location register (VLR) stores the generated information when the the MS is not in the home network

(one operator does not know the Ki of another operator)

GSM summary

-TMSI is used rather then IMSI to protect identity. Prevents tracing of the user and mapping the transmitted signal to the user.

-The MS is authenticated by the network with use of a unique key (Ki) stored only in SIM and AUC. Ki is NEVER sent over the air interface.

-For each call a ciphering key (Kc) is generated in MS and in the network, using Ki and algorithms A3, A8. This key is used in algorithm A5 to encrypt the data.

Observations

-The algorithms A1,A8 and A5 were never made public. Access to the algorithms could compromise the security.

-Ki is relatively easily extracted from the SIM *(physically)* . Knowledge of Ki allows cloning of sim cards.

-Only the air interface is encrypted

-Kc is only 64 *(54)* bits long.

-MS is authenticated to BS, but not the other way around.

Attack history

1991

First GSM implementation.

April 1998

The Smartcard Developer Association (SDA) together with U.C. Berkeley researches cracked the COMP128 algorithm stored in SIM and succeeded to get K_i within several hours. They discovered that Kc uses only 54 bits.

August 1999

The weak A5/2 was cracked using a single PC within seconds.

December 1999

Alex Biryukov, Adi Shamir and David Wagner have published the scheme breaking the strong A5/1 algorithm. Within two minutes of intercepted call the attack time was only 1 second.

May 2002

The IBM Research group discovered a new way to quickly extract the COMP128 keys using side channels.

*COMP128 is a common implementation of A3 and A8

Security in 3G

Principles:

-Build on GSM security

-Correct problems with GSM security

-Add new security features

Problems in GSM

-No mutual authentication, allows active attacks (false BTS).

-Key transmission, the IMSI, RAND,XRES and Kc are transmitted in clear within the network.

-No integrity algorithm provided

-Weak encryption algorithms, key lengths are too short. High computation speed resulted in that COMP128 has been broken.

+++

New security features

-Protection against active attacks on the radio interface. A new integrity mechanism added to protect the critical signaling information on the radio interface.

-Enhanced authentication protocol provides mutual authentication and freshness of cipher/integrity keys.

-Enhance encryption, stronger algorithm and longer keys.

-Encryption terminates in the network rather then the base station.

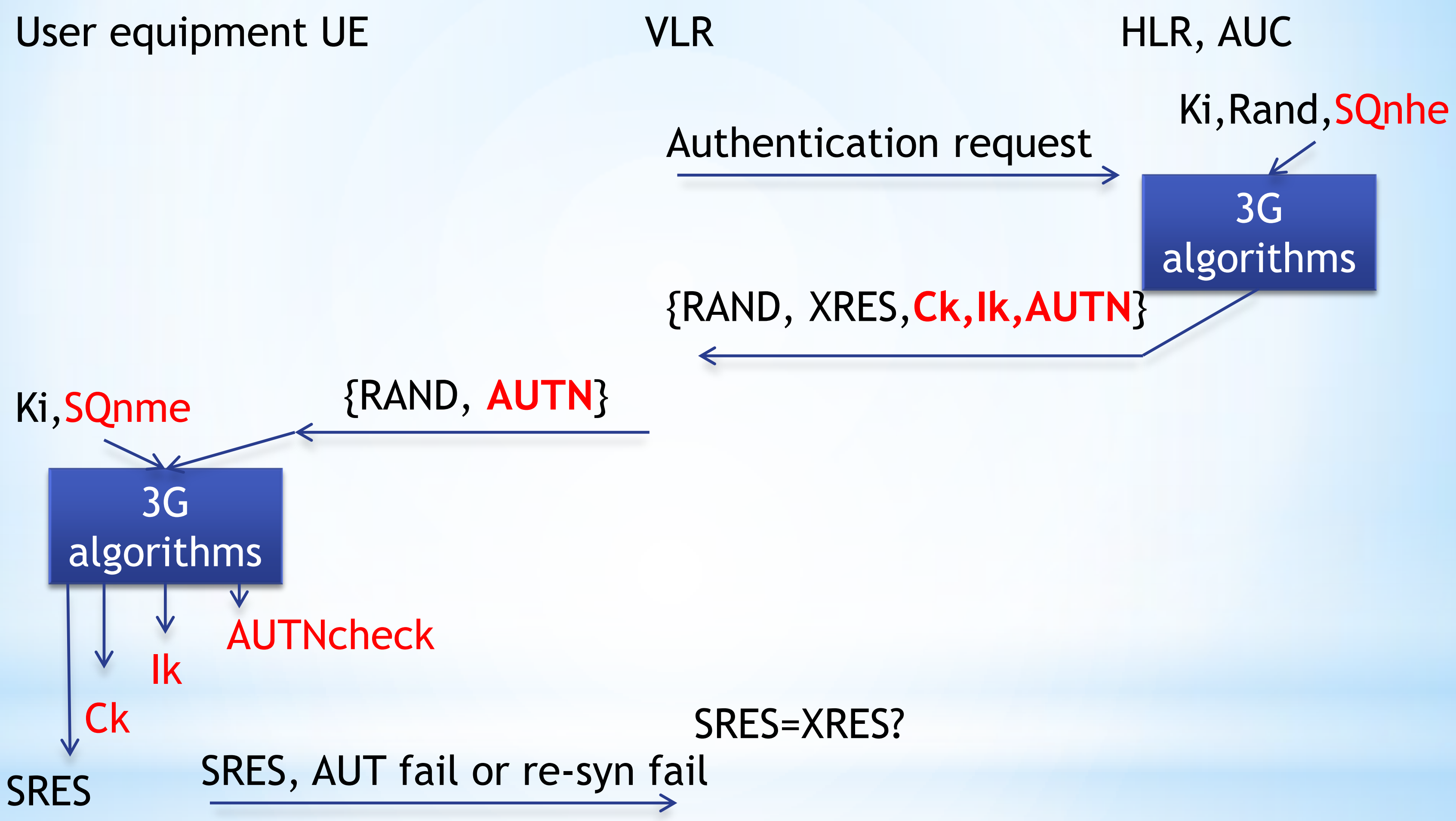
-Core network security. Some protection of signaling between network nodes.

-The user is notified whether security is on, and what level of security that is available. Meaning that users can configure security features for different services and needs.

-And more, amongst enhanced roaming security etc.

-TMSI is used same as in 2G to protect user identity.

Enhanced Authentication



User equipment UE

VLR

HLR, AUC

Ki,Rand,SQnhe

Authentication request

3G algorithms

{RAND, XRES,**Ck,Ik,AUTN**}

{RAND, **AUTN**}

Ki,SQnme

3G algorithms

AUTNcheck

Ik

Ck

SRES

SRES=XRES?

SRES, AUT fail or re-syn fail

Ki: subscriber key

SQNms: Sequence number information MS/UE

SQNhe: Sequence number information home network

AUTN: authentication token for the network

Ck: Cipher key *(new Kc)*

Ik: Integrity key

XRES: expected response

SRES: signaled response

The sequence number is to ensure key freshness and support in authentication (synchronization). If the SQN is not accepted the UE computes a re-sync token and responds to the network which uses this token to resynchronize the sequence numbers.

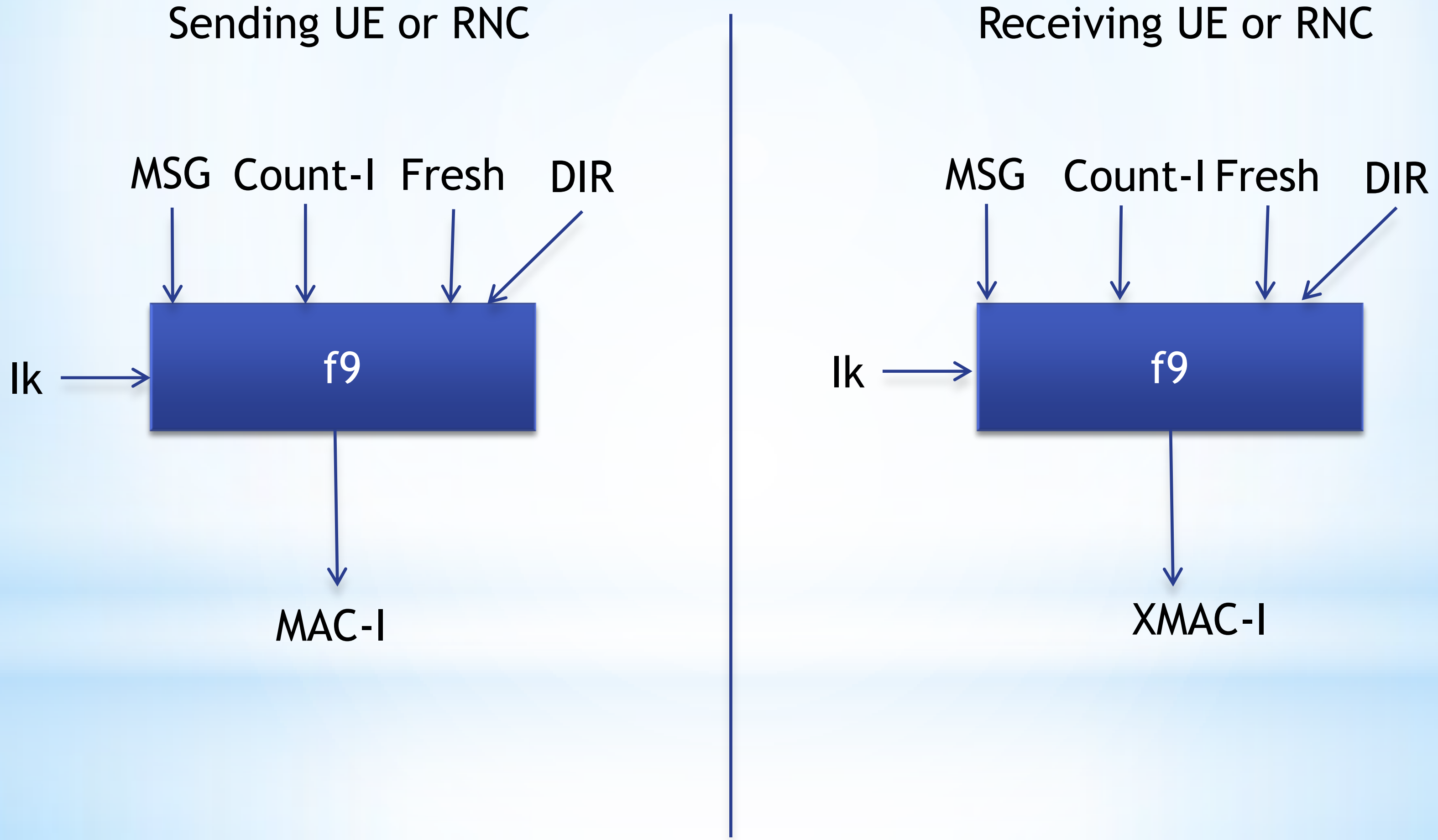
Integrity protection

-To protect against false base station attacks e.g.

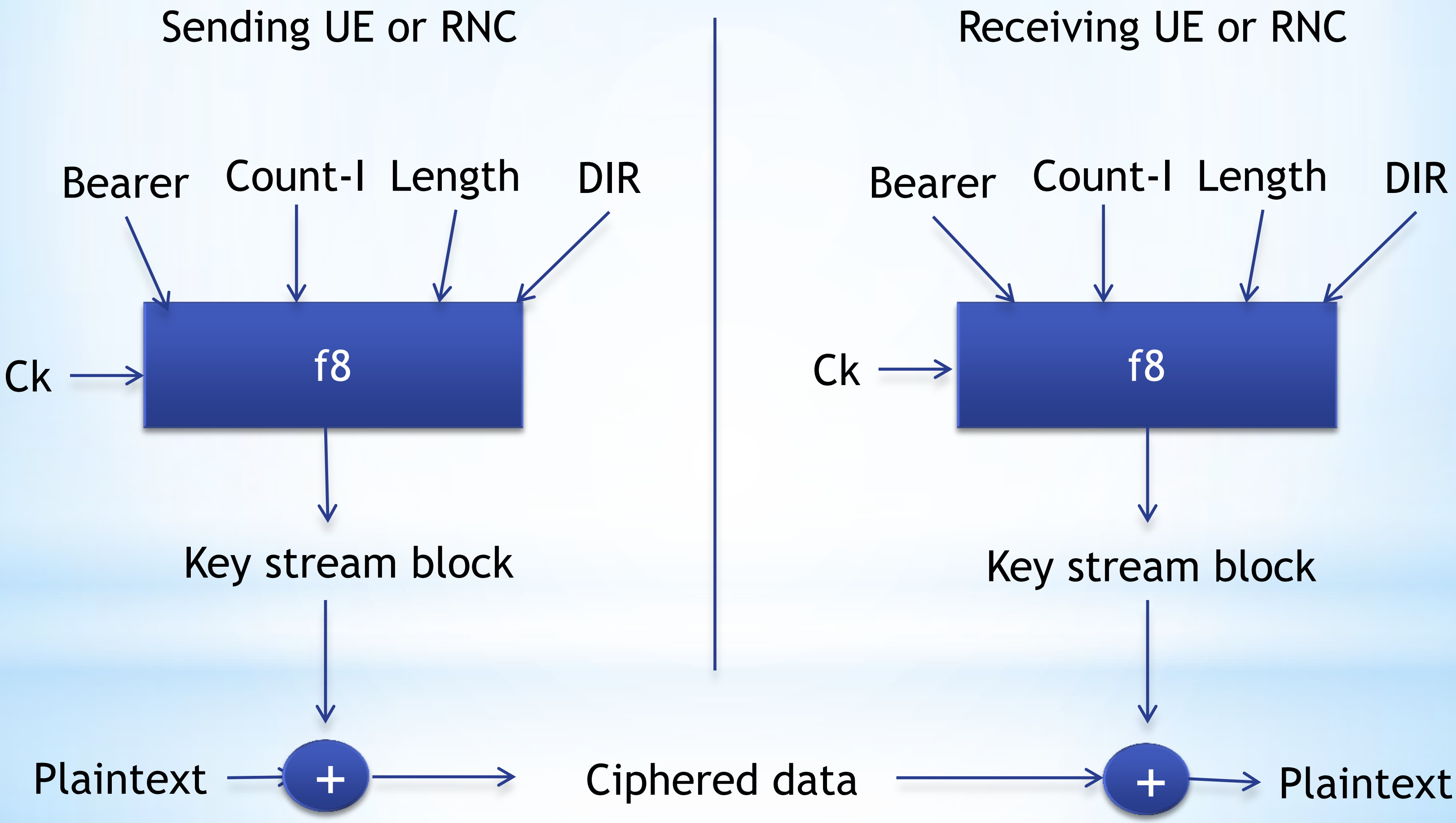
the UE must be able to verify that the signaling data has not been modified. It must also be able to identify that that the origin of the data is indeed the one claimed.

-To achieve this the Message Authentication Code (MAC) f9 is used.

Integrity protection



Data confidentiality



Summary 3G

-Improved weaknesses from 2G.

- -Two way AUT.
- -Network security
- -Enhanced encryption
- -Encrypt terminates in network rather then at base station
- -Integrity mechanism to protect signaling

-Backward capability

- - GSM parameters can be derived from 3G parameters.

-User awareness of security

Problems in 3G

-All that can happen to a fixed host attached to the internet, could happen to a 3G terminal

-IMSI still sent in clear text when user is registering for the first time

-Still possible with false BTS

-Hijack of incoming/outgoing calls still possible when encryption is off

A brief look at 4G

-Layer based network structure

-IPv6 address scheme

-In 2G and 3G the security issue is solved by multiple layers of encryption on the protocol stack.

-Disadvantage: wasted power, energy transmission delay and low flexibility

-In 4G, a concept of interlayer security allowing dynamic replacing/switching mobility management protocols and reconfiguring network services in a secure way.