/Rooted® 2014

Attacking 3G

@layakk
www.layakk.com

Jose Pico
jose.pico@layakk.com

David Perez
david.perez@layakk.com

RootedCON in Valencia

Introduction

- Attacks known to work against 2G, based on a rogue base station:
  - IMSI Catching
  - Geolocation of mobile devices
  - Denial of Service
  - Eavesdropping
  - Selective downgrade to 2G
- There are devices on the market that offer part of that functionality for 3G
- Some "*renowned*" researches claim that those attacks cannot be performed in 3G
- In this talk we tell you that most of the above can be done…
- … and we tell you how.

Note: The theoretical information presented in the following slides is actually a summary of information already public, though not widely publicized.

V

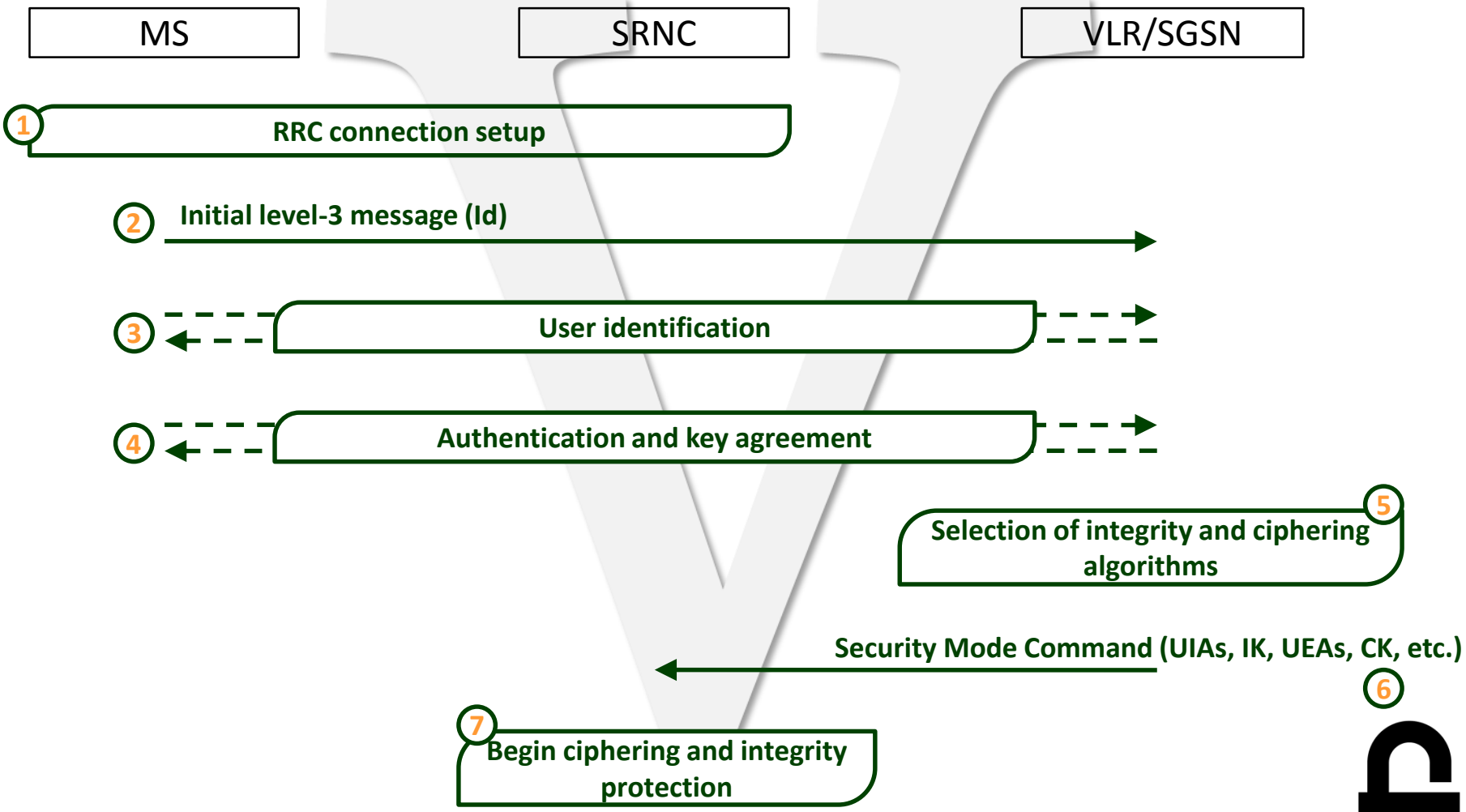
THEORETICAL BACKGROUND

¿How is that possible?

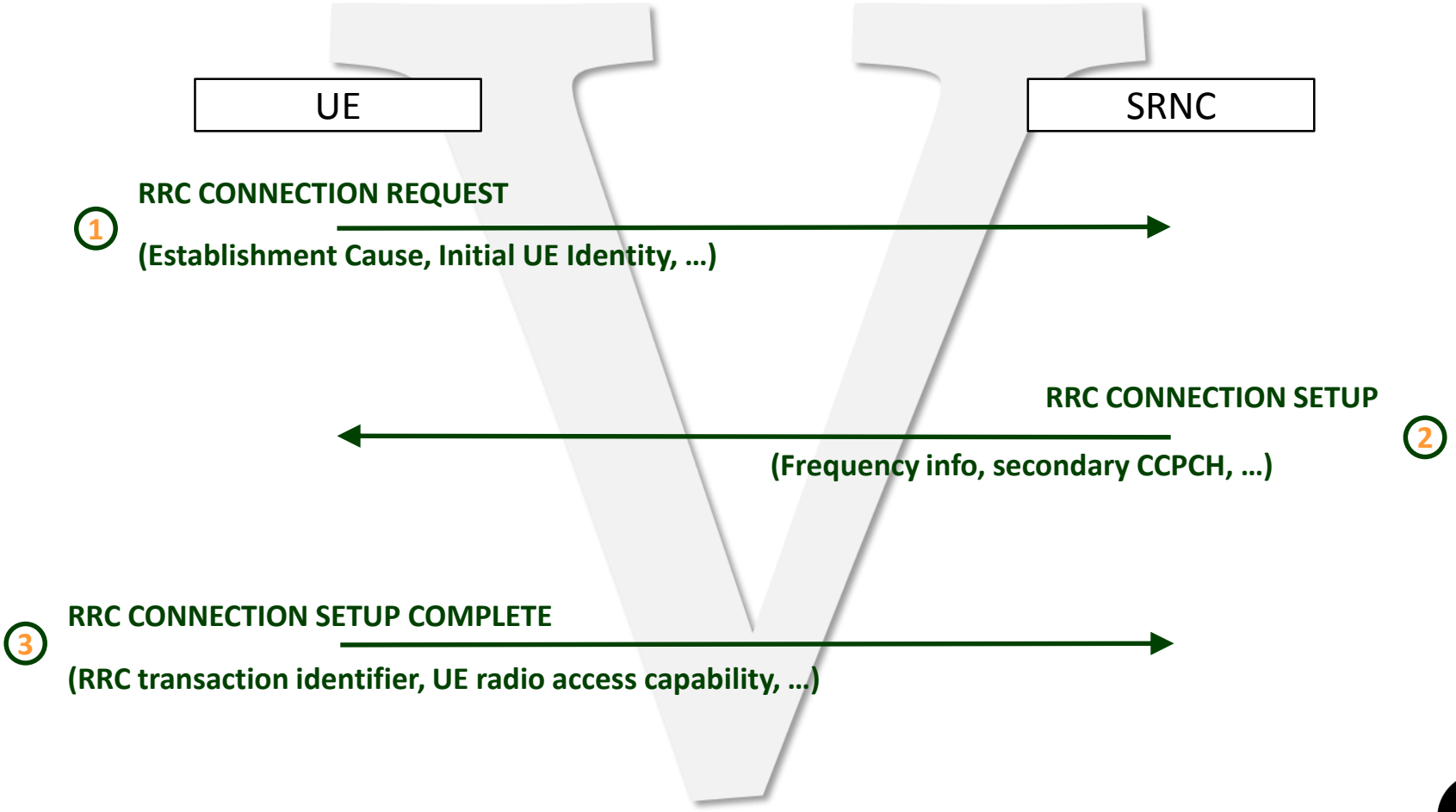
- Signaling messages are integrity protected in 3G, thanks to the *security mode command* and the structure of the protocol
- The cryptography behind the integrity protection hasn't been broken yet (at least publicly)

All signaling messages?

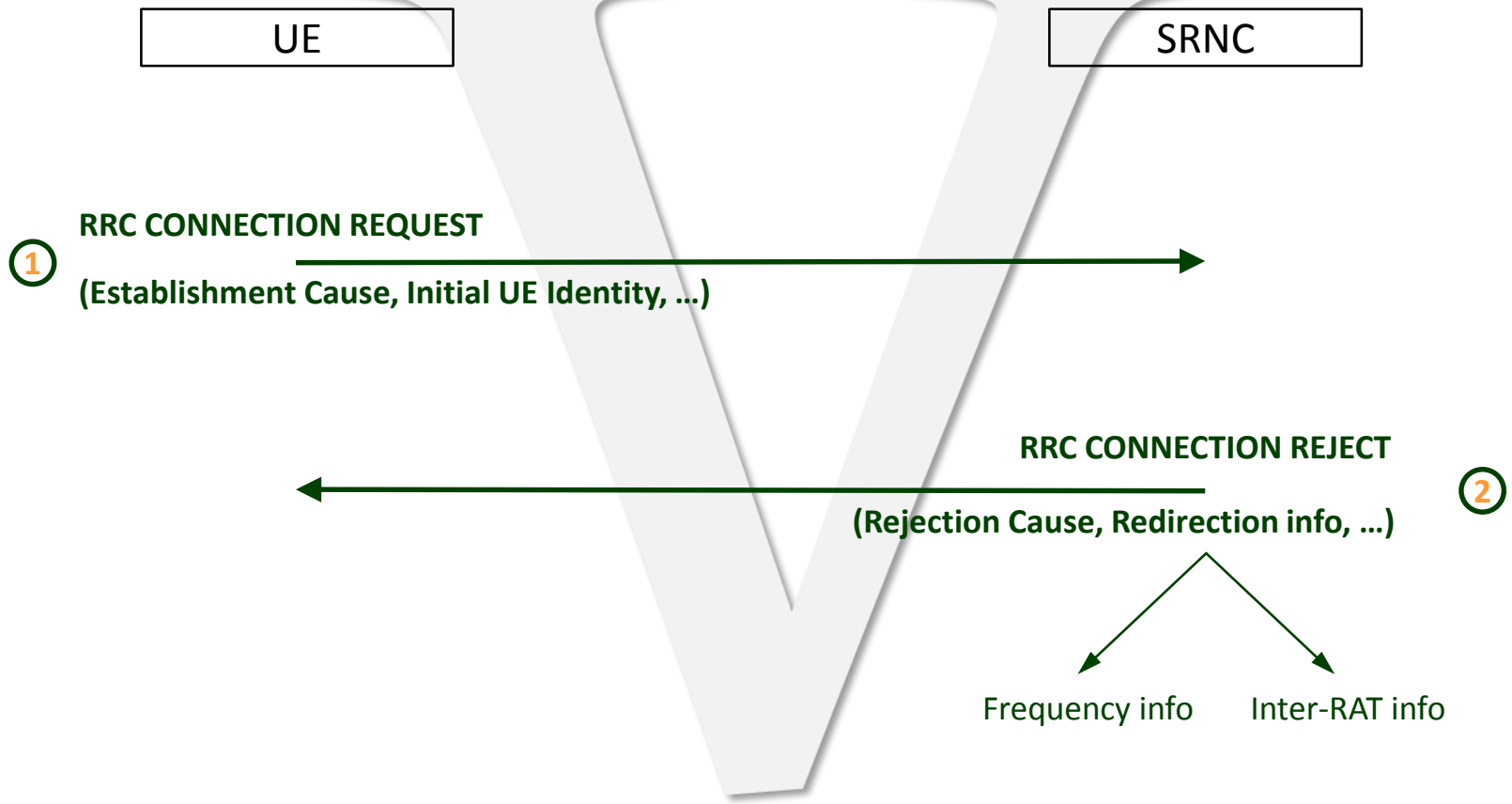
Security mode set-up procedure



Establishment of a radio channel (RRC protocol)



Rejection of a request to set up a radio channel (RRC)



RRC signaling messages NOT integrity protected

- HANDOVER TO UTRAN COMPLETE
- PAGING TYPE 1
- PUSCH CAPACITY REQUEST
- PHYSICAL SHARED CHANNEL ALLOCATION
- SYSTEM INFORMATION
- SYSTEM INFORMATION CHANGE INDICATION
- TRANSPORT FORMAT COMBINATION CONTROL (TM DCCH only)
- RRC CONNECTION REQUEST
- RRC CONNECTION SETUP
- RRC CONNECTION SETUP COMPLETE
- RRC CONNECTION REJECT
- RRC CONNECTION RELEASE (CCCH only)

MM (DL) messages allowed *before* the security mode command

- AUTHENTICATION REQUEST
- AUTHENTICATION REJECT
- IDENTITY REQUEST
- LOCATION UPDATING REJECT
- LOCATION UPDATING ACCEPT (at periodic location update with no change of location area or temporary identity)
- CM SERVICE ACCEPT, if the following two conditions apply:
  - no other MM connection is established; and
  - the CM SERVICE ACCEPT is the response to a CM SERVICE REQUEST with CM SERVICE TYPE IE set to ‘emergency call establishment’
- CM SERVICE REJECT
- ABORT

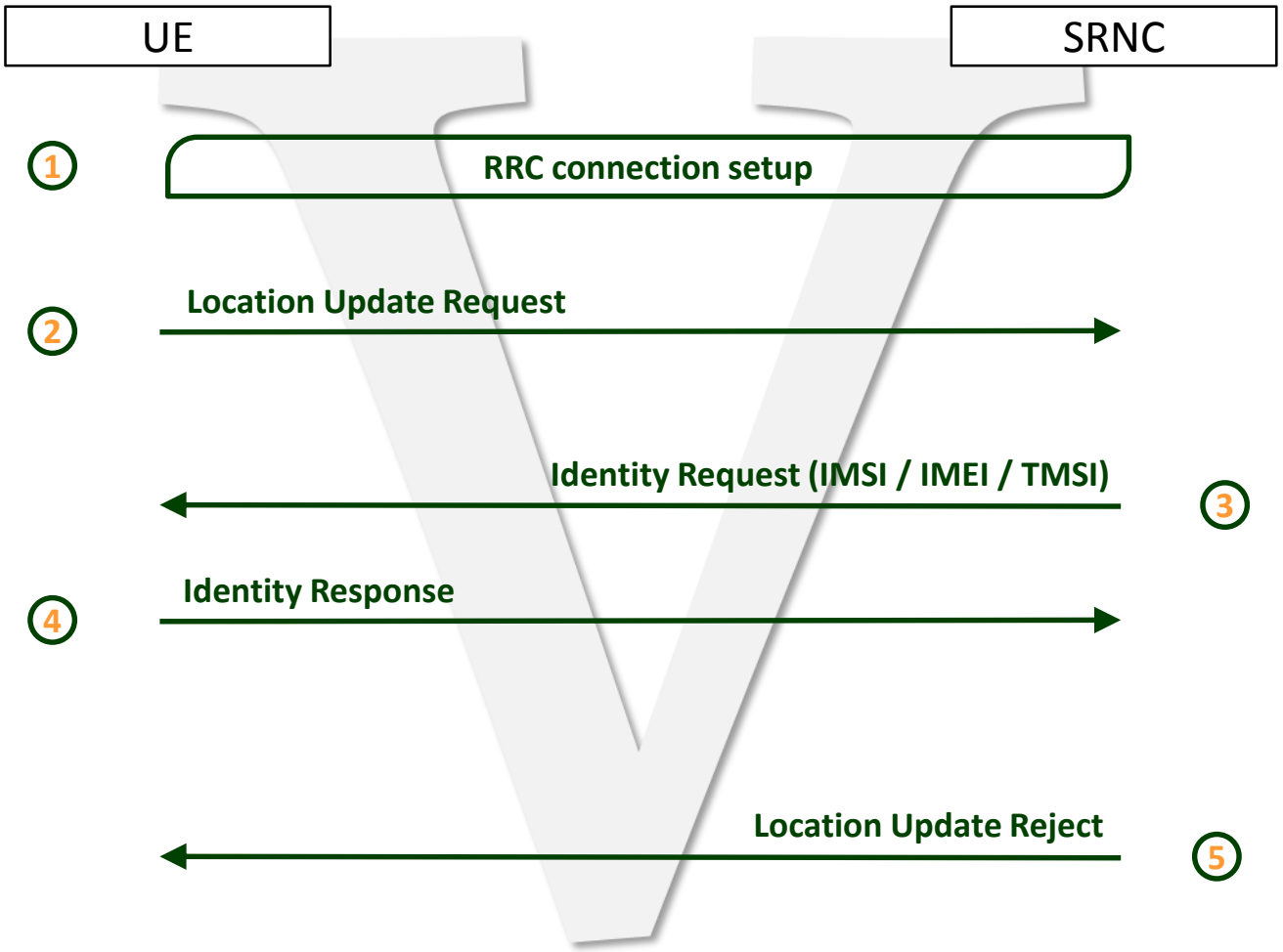
Attack infrastructure: 3G base station (node B)

- HW
  - Radio receiver&transmitter with 5 MHz bandwidth
  - Sampling rate >= 3,84 Msps
  - Clock with proper rate and precission
- SW
  - 3G modem (SW based in order to control the baseband)
  - Emulation of certain parts of the protocols

ATTACKS

- IMSI / IMEI Catching
- Geolocation of mobile devices
- Denial of Service
- Selective downgrade to 2G

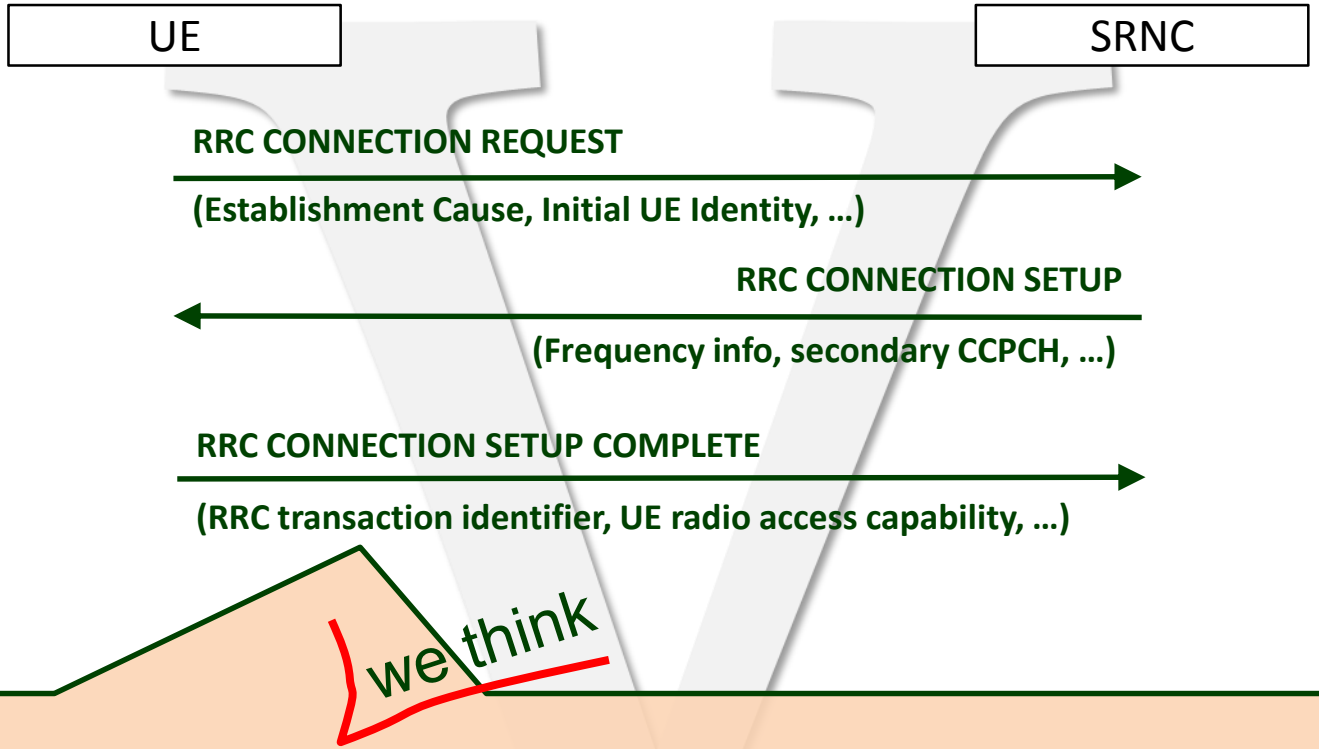
IMSI / IMEI *Catching*



Geolocation of mobile devices

- All data needed for geolocation is available on signaling channels
- Once established an RRC connection with a device, the rest is identical to 2G.
- ¿Is it necessary to complete the registration of the device in the network?

Geolocation of mobile devices



This radio channel can be kept open long enough to carry out all needed measurements, before the device finally desists in its attempt to register with the fake cell

Denial of Service

- Since the “Location Update Reject” message may be sent before ciphering and integrity protection are established, the DoS attack based on LU Reject Cause Codes is totally posible in 3G

Selective downgrade to 2G

- A selective downgrade to 2G may be carried out in at least two different ways:
  - If the TMSI of the target device is known (it may be obtained via some other technique), the connection establishment attempts may be redirected to a 2G cell using Inter-RAT info
  - Knowing any ID of the target device, a cell could be configured with the LAC of the real cells (if there are 2 LACs in the environment, 2 fake base stations could be used), and this cell could reject the registration attemtps with “Location Area not allowed”

we think

Attack infrastructure: 3G base station (node B)

- HW
  - Radio receiver&transmitter with 5MHz bandwidth
  - Sampling rate >= 3,84 Msps
  - Clock with proper rate and precission
- SW
  - 3G modem (SW based in order to control the baseband)
  - Emulation of certain parts of the protocols

V

To receive a downlink signal

DEVELOPMENT OF A SOFTWARE-BASED 3G MODEM

HW

SAMPLING

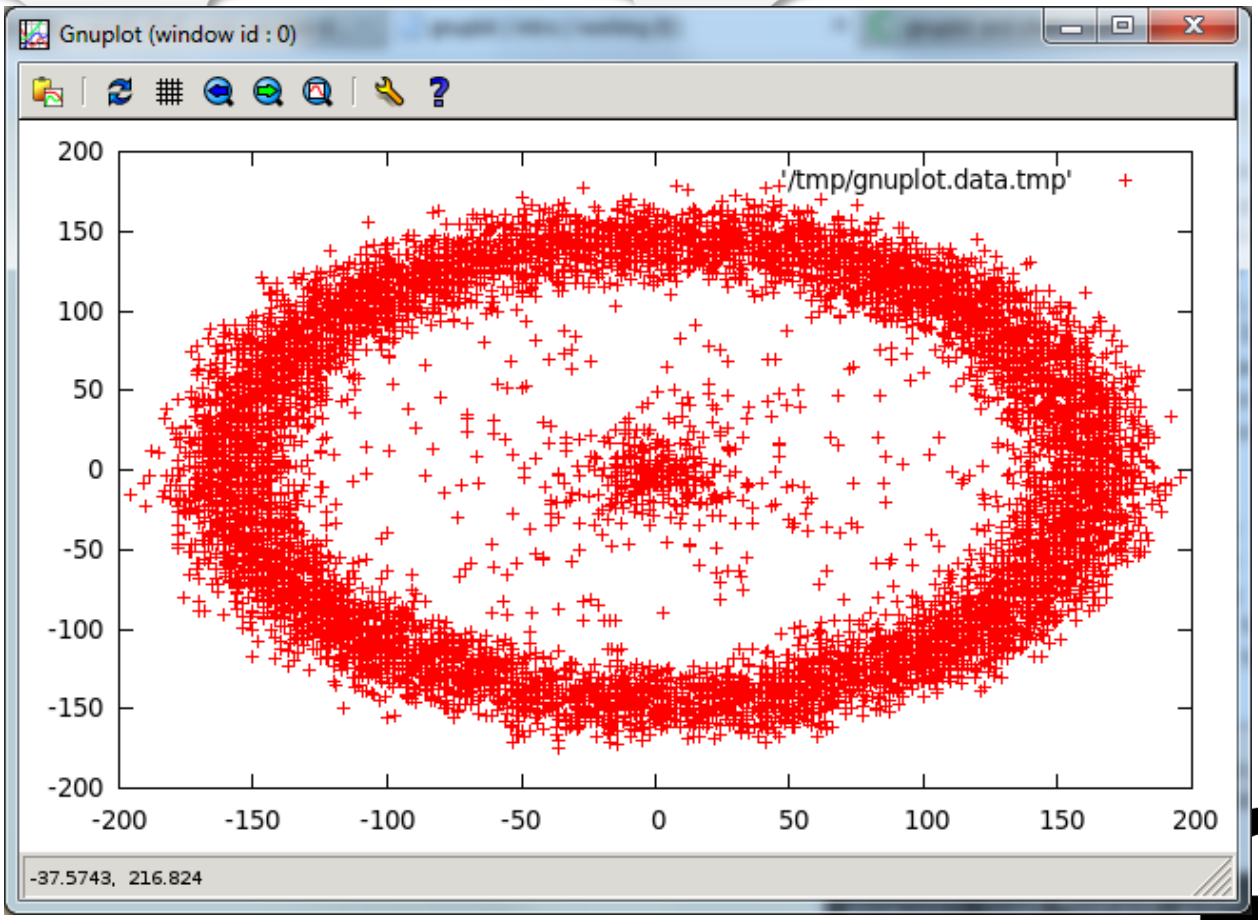
UmTRX

GigE

https://code.google.com/p/umtrx/

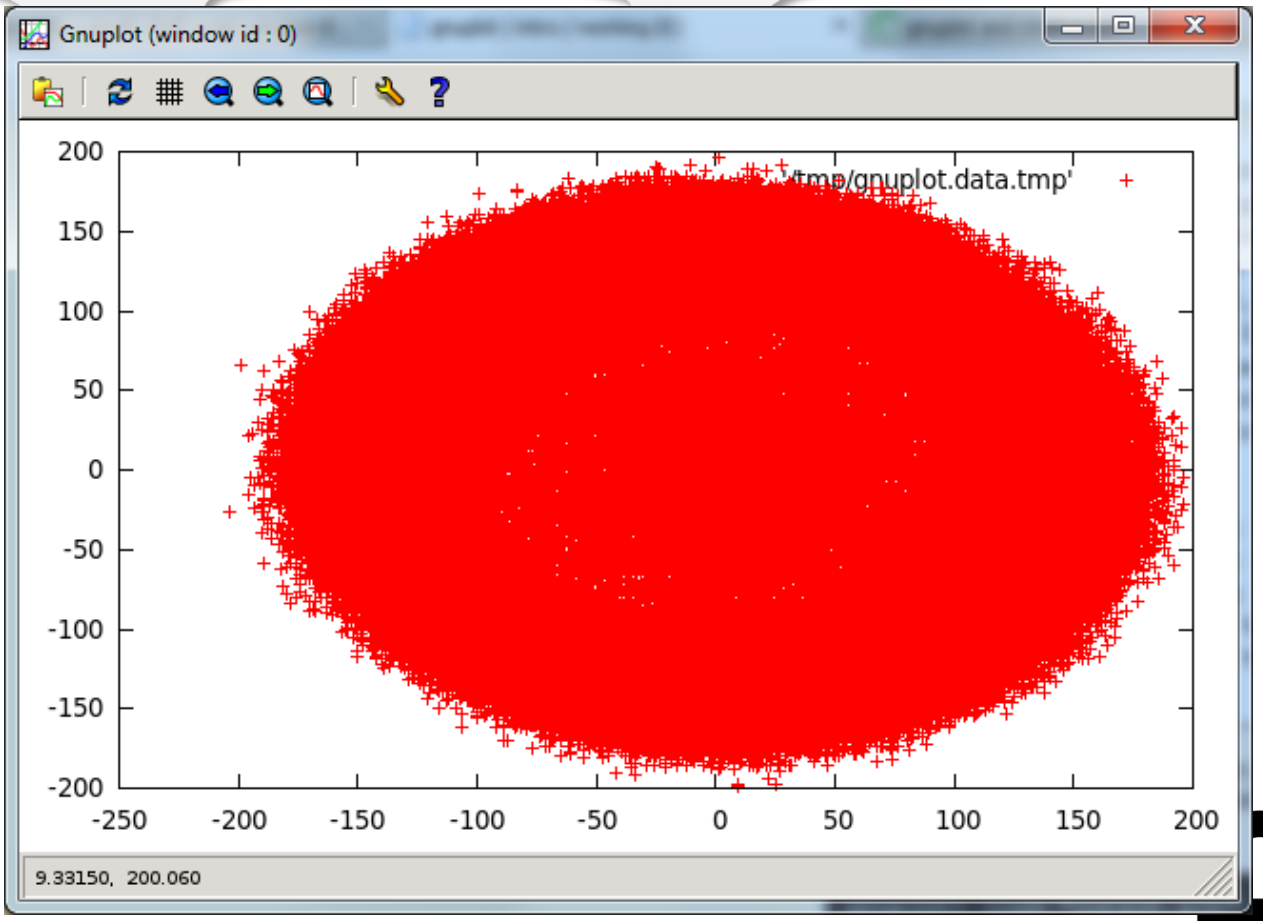
A 2G signal in the IQ plane

SAMPLING



A 3G signal in the IQ plane

SAMPLING



Downlink reception

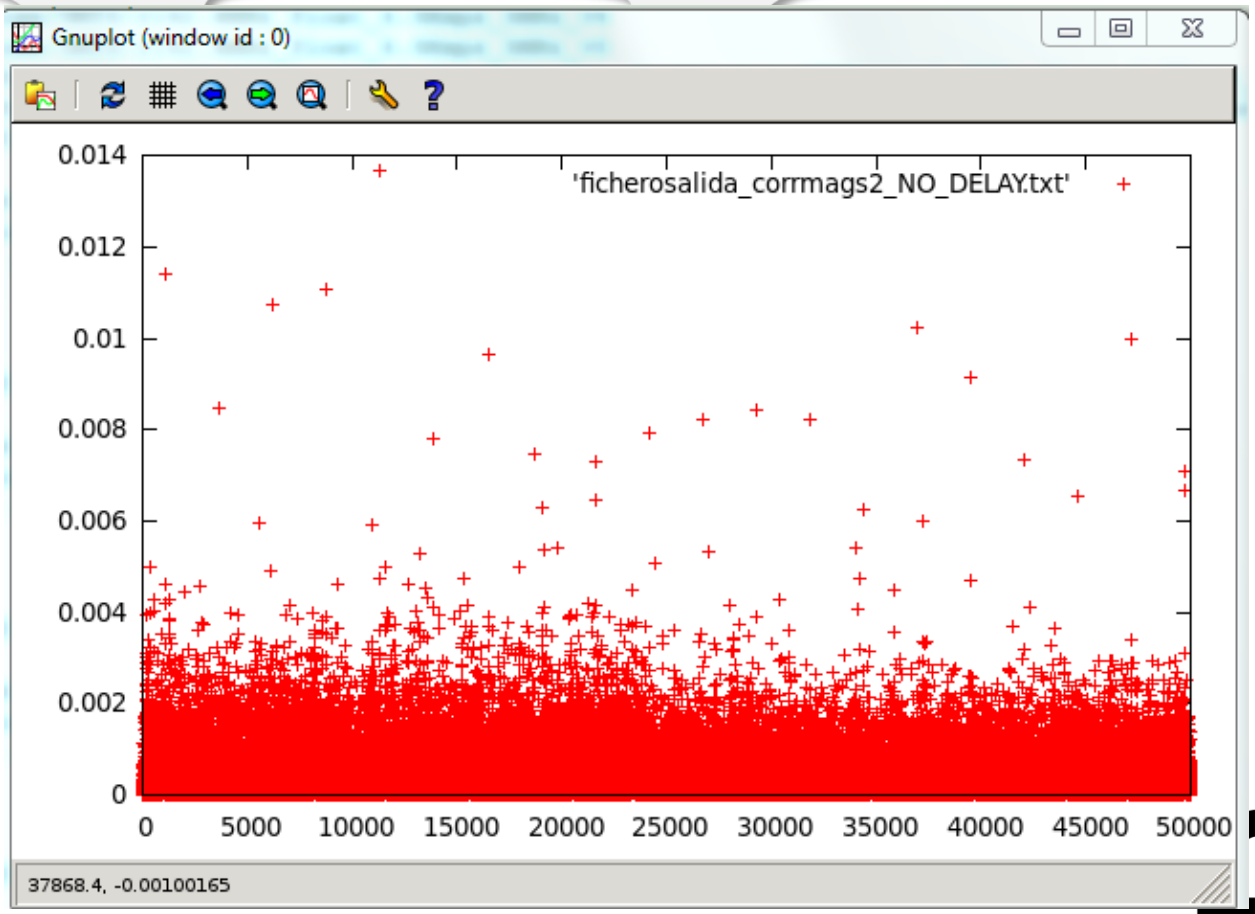
SAMPLING

RESAMPLING

- The sampling rate must be a multiple of the modulation symbol rate
- In UMTS the symbol rate is 3,84 Msps (1 symbol = 1 chip)
- 13 Msps → 3,84 Msps

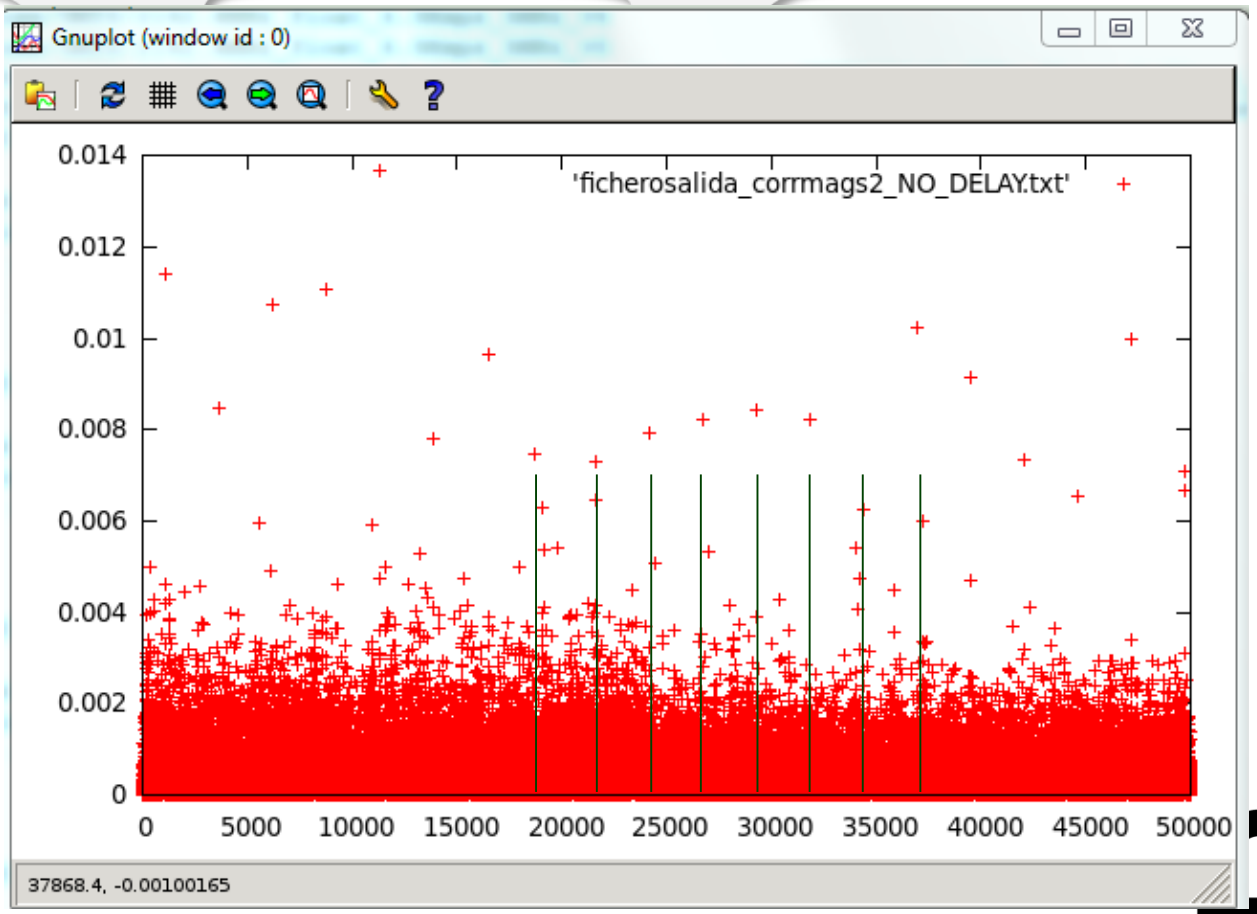
Downlink reception

- SAMPLING
- RESAMPLING
- PSCH IDENTIFICATION



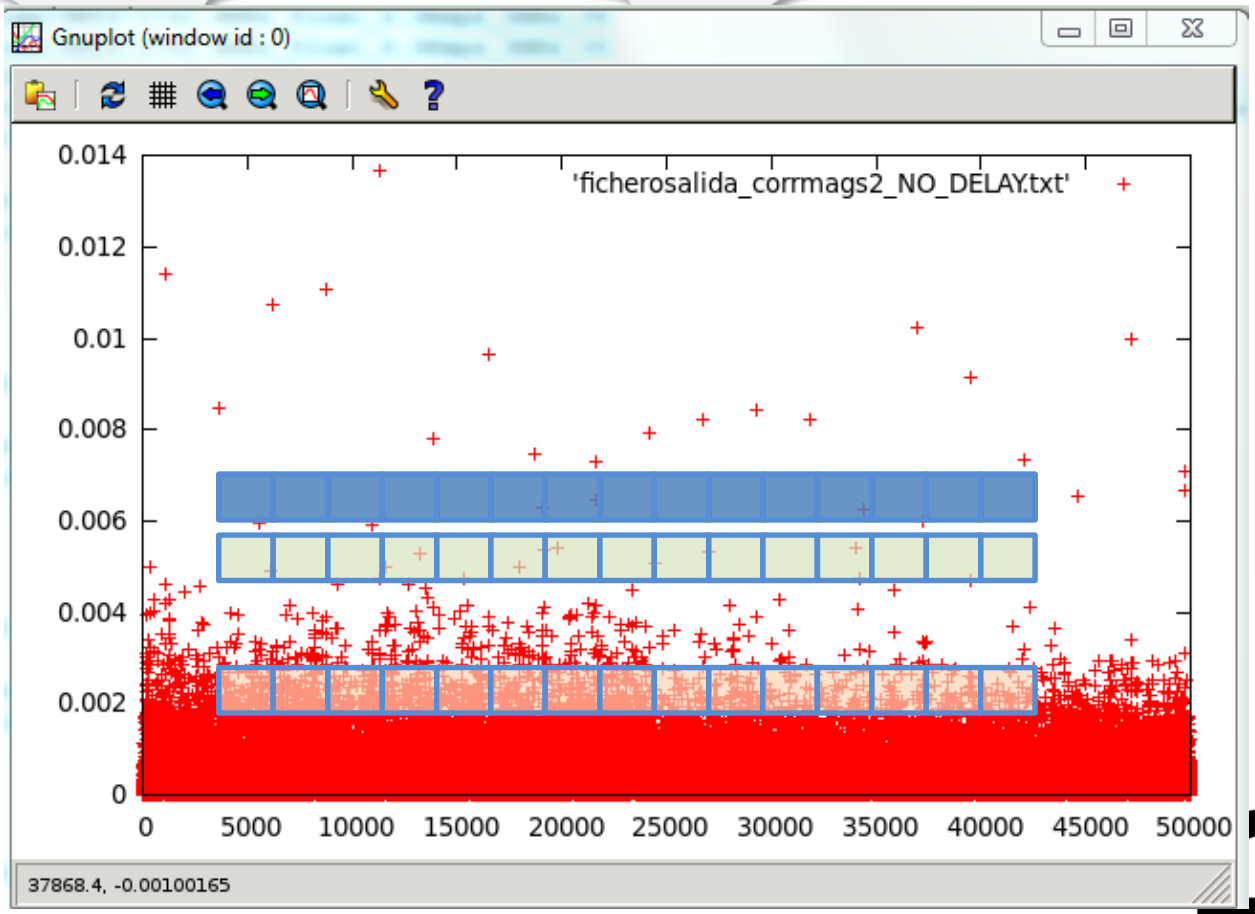
Downlink reception

- CAPTURA
- RESAMPLING
- PSCH IDENTIFICATION
- TIMESLOT SYNCRONIZATION



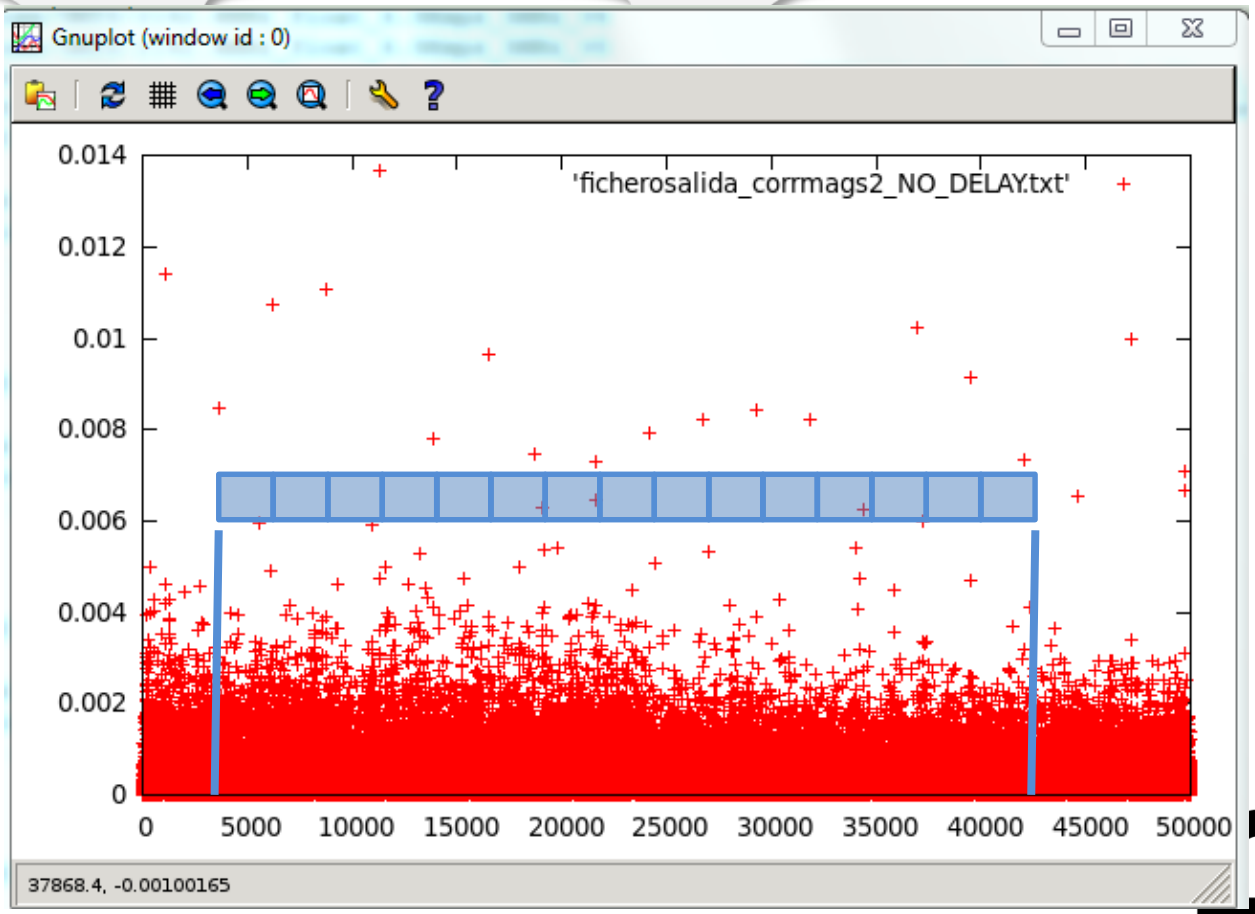
Downlink reception

- SAMPLING
- RESAMPLING
- PSCH IDENTIFICATION
- TIMESLOT SYNCRONIZATION
- SSC GROUP IDENTIFICATION



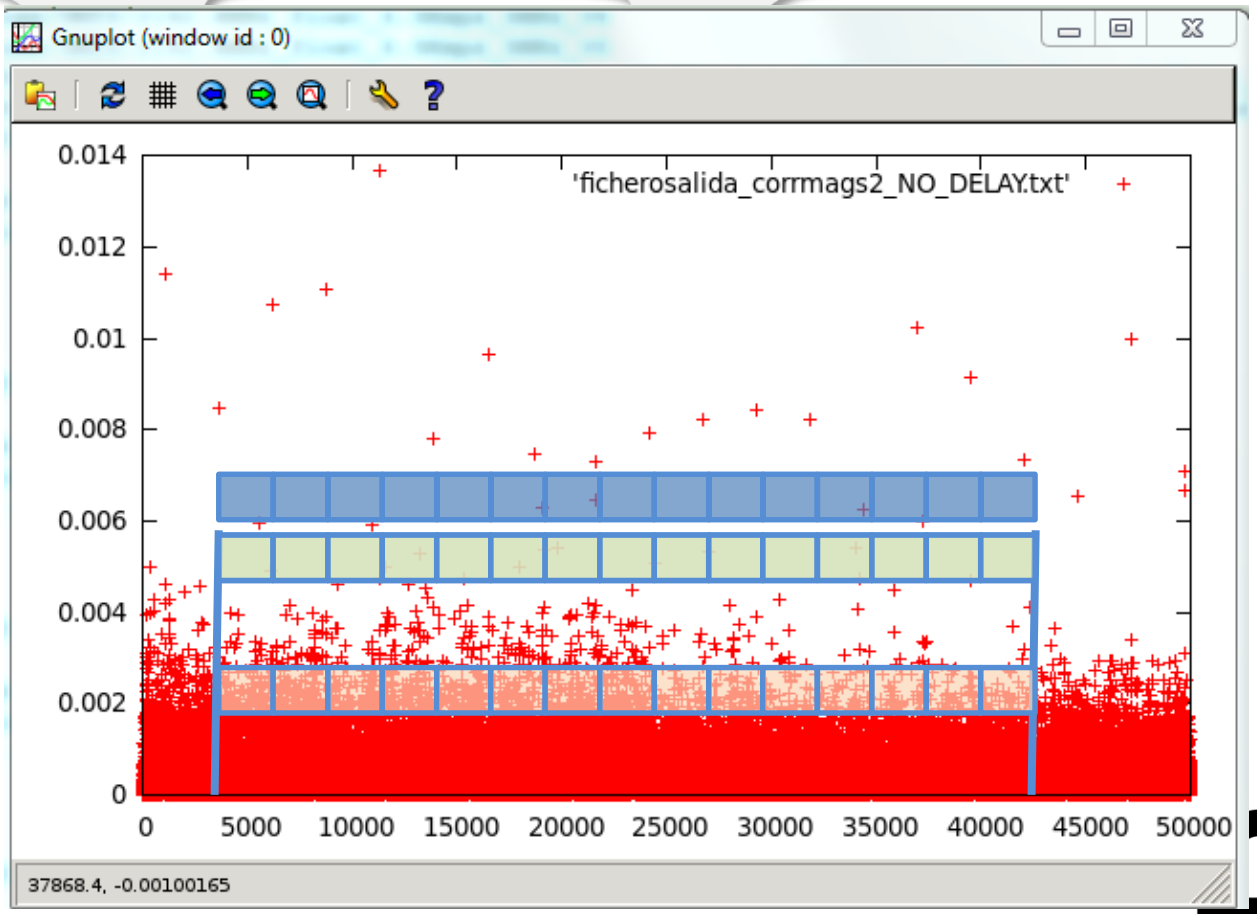
Downlink reception

- SAMPLING
- RESAMPLING
- PSCH IDENTIFICATION
- TIMESLOT SYNCRONIZATION
- SSC GROUP IDENTIFICATION
- FRAME SYNCRONIZATION

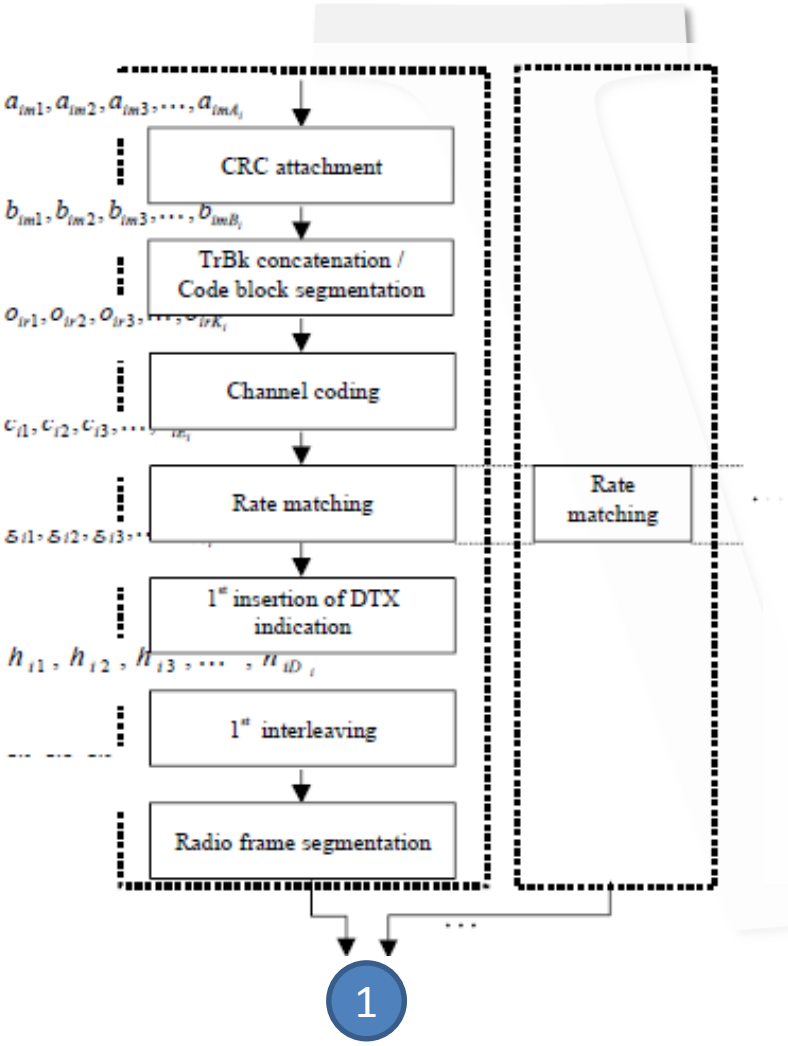


Downlink reception (I)

- SAMPLING
- RESAMPLING
- PSCH IDENTIFICATION
- TIMESLOT SYNCRONIZATION
- SSC GROUP IDENTIFICATION
- FRAME SYNCRONIZATION
- **SCRAMBLING CODE IDENTIFICATION**



Downlink reception (II)



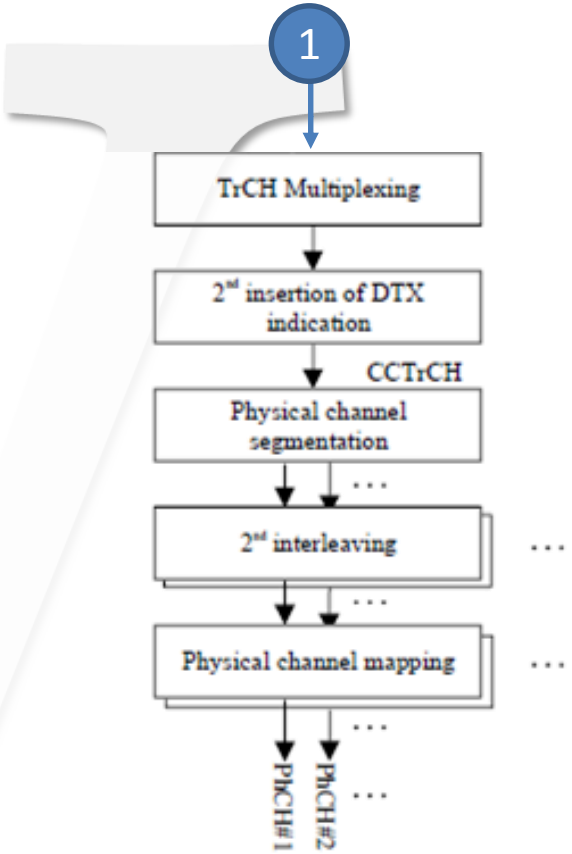
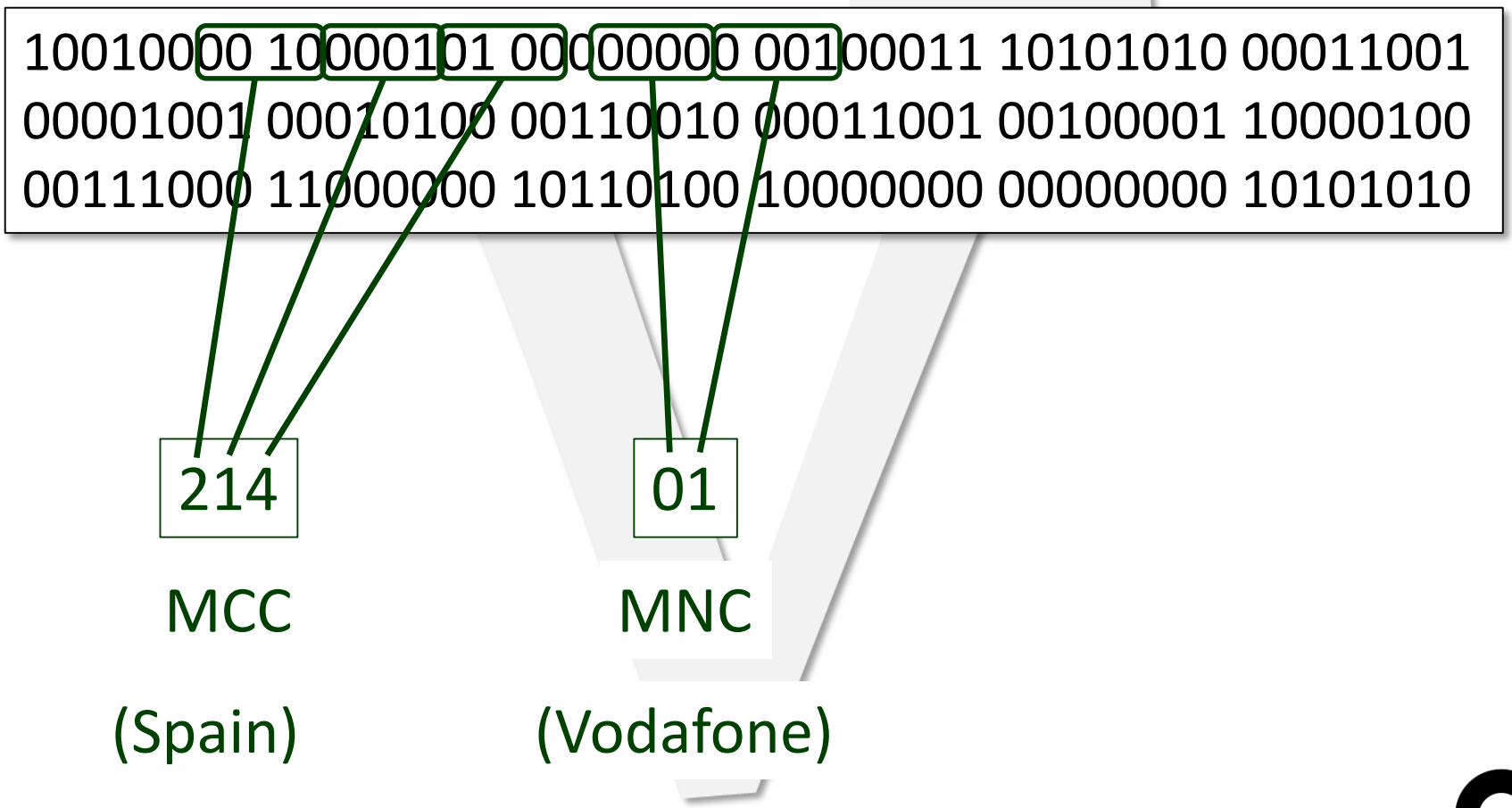


Figure 2: Transport channel multiplexing structure for downlink

DEMO

Master Information Block

90850023aa1909143219218438c0b48000aa



Attack infrastructure: 3G base station (node B)

- HW
  - Radio receiver&transmitter with 5MHz bandwidth
  - Sampling rate >= 3,84 Msps
  - Clock with proper rate and precission
- SW
  - 3G modem (SW based in order to control the baseband)
  - Emulation of certain parts of the protocols

Introduction

we think

- Attacks known to work against **3G**, based on a rogue base station:
  - IMSI Catching
  - Geolocation of mobile devices
  - Denial of Service
  - Eavesdropping
  - Selective downgrade to 2G
- There are devices on the market that offer part of that functionality for 3G
- Some "*renowned*" researches claim that those attacks **can** be performed in 3G

we think

- In this talk we tell you that most of the above can be done…
- … and we tell you how.

TO PROBE FURTHER...

QUESTIONS

@layakk
www.layakk.com

Attacking 3G

Jose Pico
jose.pico@layakk.com

David Perez
david.perez@layakk.com

/Rooted® 2014