Geolocation of GSM mobile devices, even if they do not want to be found

www.taddong.com
@taddong

José Picó
jose@taddong.com
David Pérez
david@taddong.com

Intro

Taddong

Geolocation of mobile devices (MS)

- GSM Location Services – LCS:
  - Network based
  - MS based
  - MS assisted

  } RRLP

- Geolocation application, installed in the MS

OK, but could we...?

...locate any GSM mobile device,

even if we didn't have access to the network,

and the device did not want to be found?

Goals of this talk

Goals of this talk

1) Answer the following question:

¿How could we locate a mobile device that does not want to be found, without having acces to the network?

2) Illustrate the process of this research project

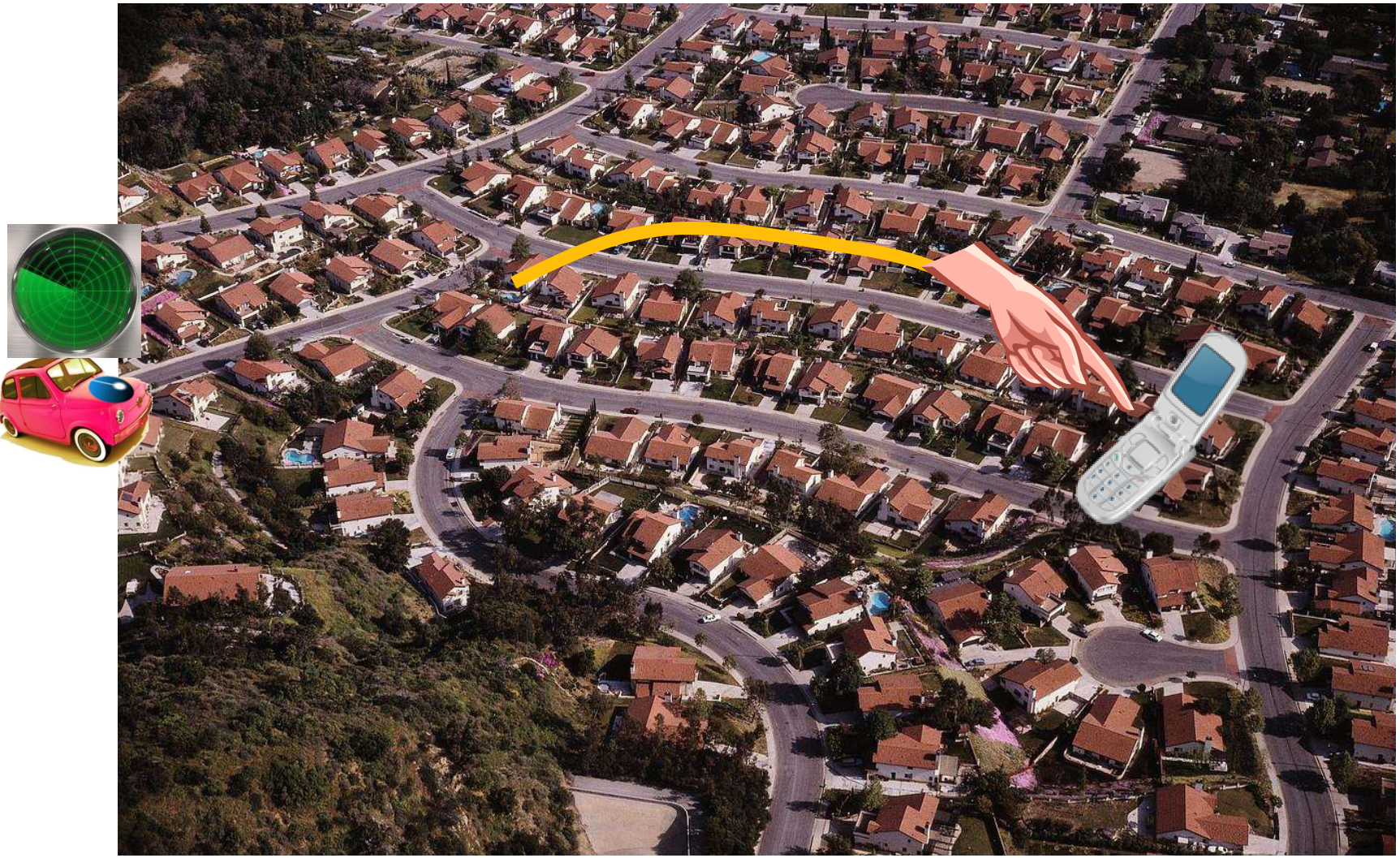
Design Constraints

Taddong

Design constraints

- No access to the network (PLMN)
- All location services disabled in the target MS
- Known data about target MS:
  - approximate location (e.g. neighborhood)
  - IMEI or IMSI
- Target is static (or quasi-static)
- Solution must consist of a single system that can be operated in a standard vehicle

Goal of the system



Taddong

Initial Design

"We will do it right: we will design the system with the whole software life cycle in mind from the very begining"

HA HA HA

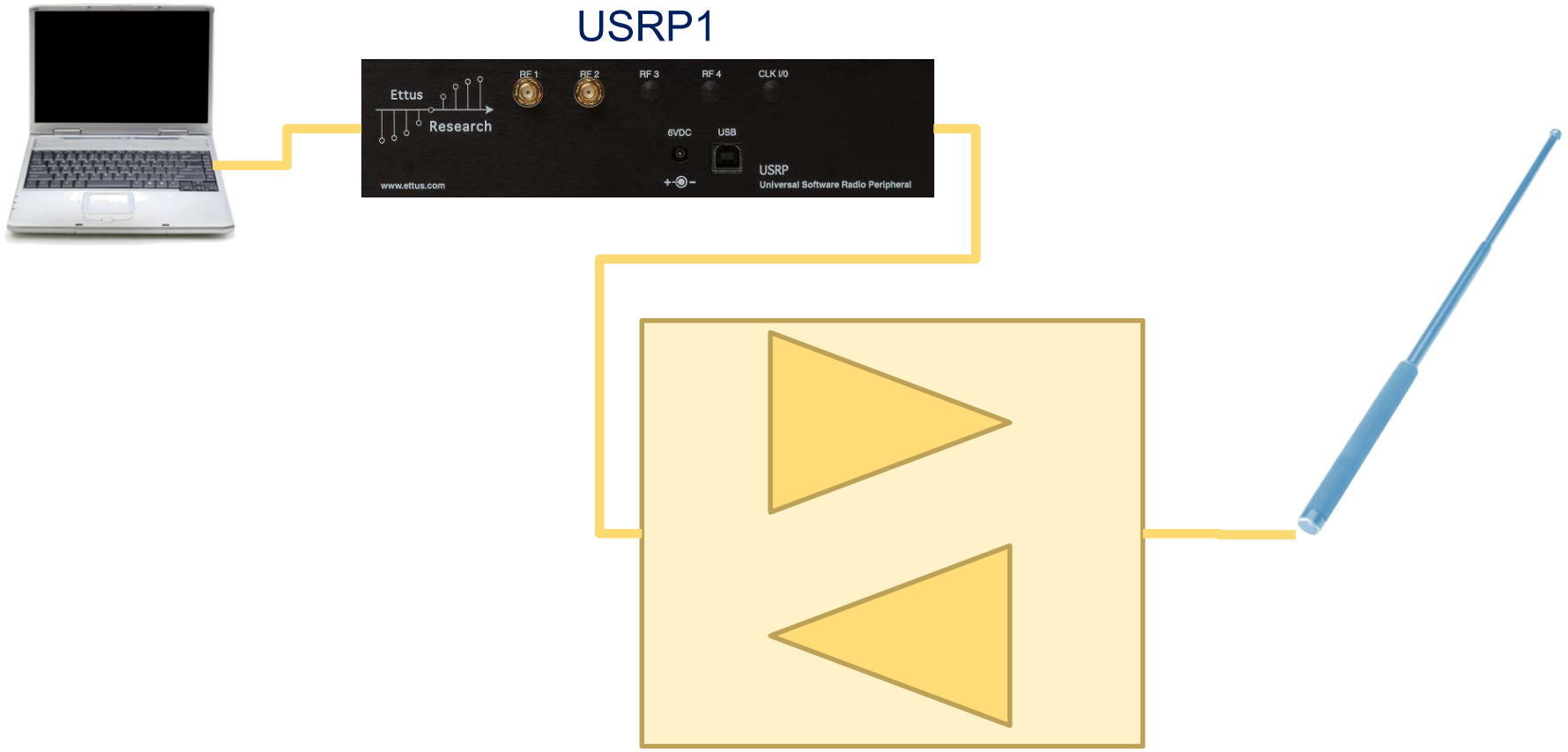
Taddong

System

- Portable fake GSM base station, capable of geolocating any GSM device within its reach.

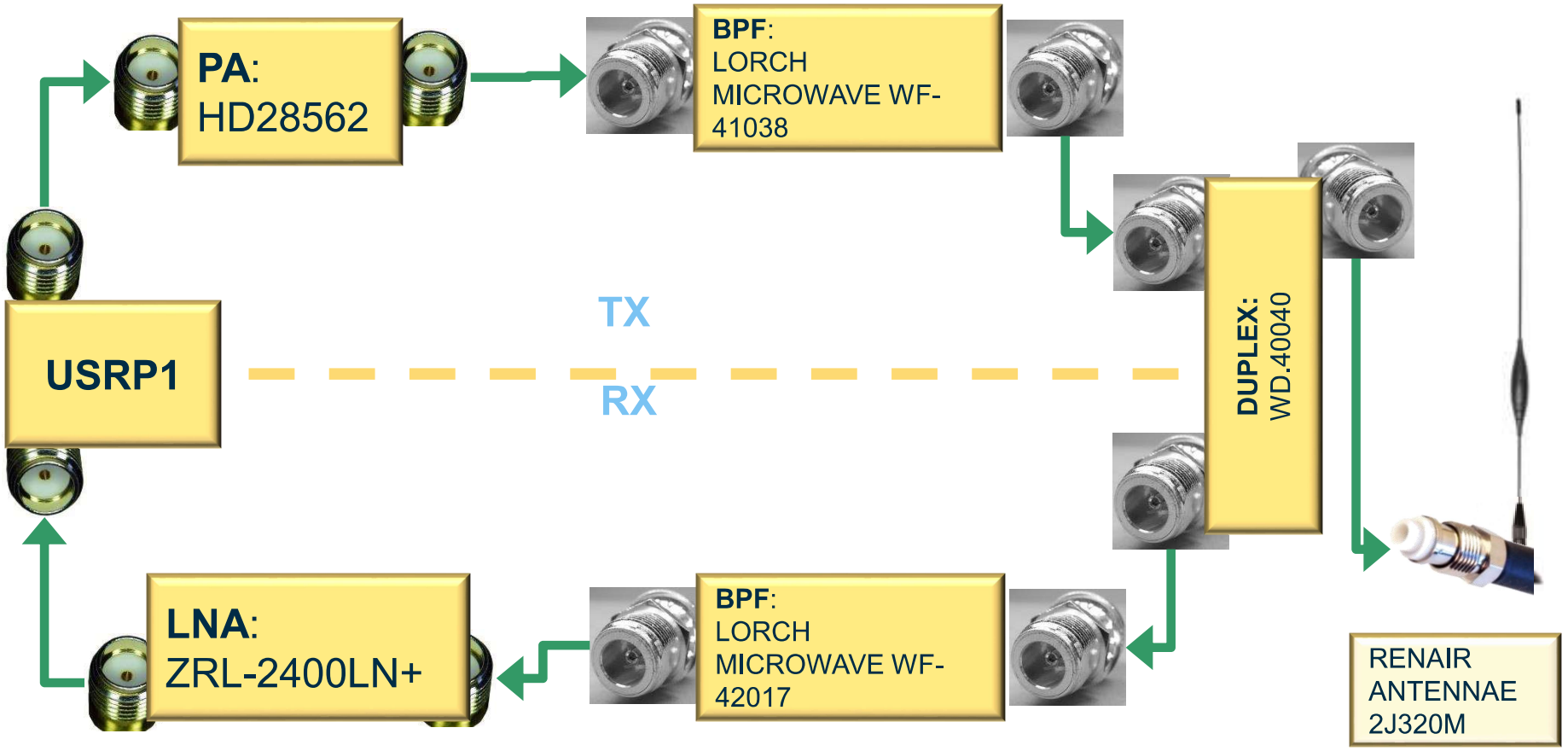
Hardware

General schematics



Taddong

Hardware: Power amplification



Taddong

Hardware: antennas

2 Modes: Omnidirectional & Directional

- Omnidirectional mode
  - Locate the target, with some error margin (e.g. building)

- Directional mode
  - Pinpoint the exact location of the target (e.g. window)

Taddong

Software

- OpenBTS(*) 2.6, adding the following functionality:
  - GPS data acquisition
  - Triangulation based on power and timing data
  - Text-based (ncurses) user console

(*) http://wush.net/trac/rangepublic

Researching the Data Available for Triangulation

Investigation of the data sources provided by the OpenBTS+USRP base station that could be used to triangulate the position of the target MS

Taddong

Data sources for triangulation

A GSM base station (BTS) provides useful data

- Power (absolute value) that the MS receives from the BTS
  - Used in GSM for *handover* procedures
- Power (relative) that the BTS receives from the MS
  - Used in GSM for dynamic control of MS power consumption
- Time delays
  - Used in GSM for the *timing advance* synchronization mechanism

Data sources for triangulation

Data source initial choice

- We figured time delays would probably be too imprecise:
  - A small error in the time measurement would translate into a huge error in distance estimation
- Thus, we opted for:
  - Use power measurements, mainly, and then,
  - Use time delay measurements only to make small adjustments (if needed and possible)

Power-based Triangulation

Taddong

Power-based Triangulation

$$(x_1 - cx_1)^2 + (y_1 - cy_1)^2 = {r_1}^2 \xrightarrow{\text{en la interseccion}} (x - cx_1)^2 + (y - cy_1)^2 = {r_1}^2$$
$$(x_2 - cx_2)^2 + (y_2 - cy_2)^2 = {r_2}^2 \qquad\qquad (x - cx_2)^2 + (y - cy_2)^2 = {r_2}^2$$

$$x^2 \overbrace{-2cx_1}^{A} x + y^2 \overbrace{-2cy_1}^{B} y + \overbrace{({cx_1}^2 + {cy_1}^2 - {r_1}^2)}^{C} = 0$$
$$x^2 \underbrace{-2cx_2}_{A'} x + y^2 \underbrace{-2cy_2}_{B'} y + \underbrace{({cx_2}^2 + {cy_2}^2 - {r_2}^2)}_{C'} = 0$$

$$\begin{matrix} x^2 + y^2 + Ax + By + C = 0 \\ (A - A')x + (B - B')y + (C - C') = 0 \end{matrix} \quad \overrightarrow{x = -\left(\frac{B - B'}{A - A'}\right)y - \left(\frac{C - C'}{A - A'}\right) = \left(\frac{B' - B}{A - A'}\right)y + \left(\frac{C' - C}{A - A'}\right)}$$

$$\left(\frac{B' - B}{A - A'}\right)^2 y^2 + \left(\frac{C' - C}{A - A'}\right)^2 + 2\left(\frac{B' - B}{A - A'}\right)\left(\frac{C' - C}{A - A'}\right)y + y^2 + A\left(\frac{B' - B}{A - A'}\right)y + A\left(\frac{C' - C}{A - A'}\right) + By + C = 0$$

$$\overbrace{\left[1 + \left(\frac{B' - B}{A - A'}\right)^2\right]}^{a} y^2 + \overbrace{\left[2\left(\frac{B' - B}{A - A'}\right)\left(\frac{C' - C}{A - A'}\right) + A\left(\frac{B' - B}{A - A'}\right) + B\right]}^{b} y + \overbrace{\left[\left(\frac{C' - C}{A - A'}\right)^2 + A\left(\frac{C' - C}{A - A'}\right) + C\right]}^{c}$$

$$y(sol1) = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \qquad y(sol2) = \frac{-b - \sqrt{b^2 - 4ac}}{2a}$$

NOTA: a debe ser distinto de 0

NOTA: en el caso especial que A-Ap=0, entonces:

$$y = \left(\frac{-C + C'}{B - B'}\right) \xrightarrow{\text{yields}} x^2 + \left(\frac{-C + C'}{B - B'}\right)^2 + Ax + B\left(\frac{-C + C'}{B - B'}\right) + C = 0$$

$$x^2 + Ax + \left(\frac{-C + C'}{B - B'}\right)^2 + B\left(\frac{-C + C'}{B - B'}\right) + C = 0 \xrightarrow{\text{yields}} \begin{matrix} a = 1 \\ b = A \\ c = y^2 + By + C \end{matrix}$$

$$x(sol1) = \frac{-A + \sqrt{A^2 - 4c}}{2} \qquad x(sol2) = \frac{-A - \sqrt{A^2 - 4c}}{2}$$

"This will be a piece of cake!"

Taddong

Distance estimation based on power measurements

Different models exist

Path Loss between isotropic antennas in direct sight

$$\mathrm{L} = 20\ \log_{10}\left(\frac{4\pi d}{\lambda}\right)$$

Path Loss exponent models

$$\mathrm{PL} = PL_0 + 10\,\gamma\ \log_{10}\left(\frac{d}{d_0}\right) + X_G$$

$$\mathrm{L} = 10\,n\ \log_{10}(d) + C$$

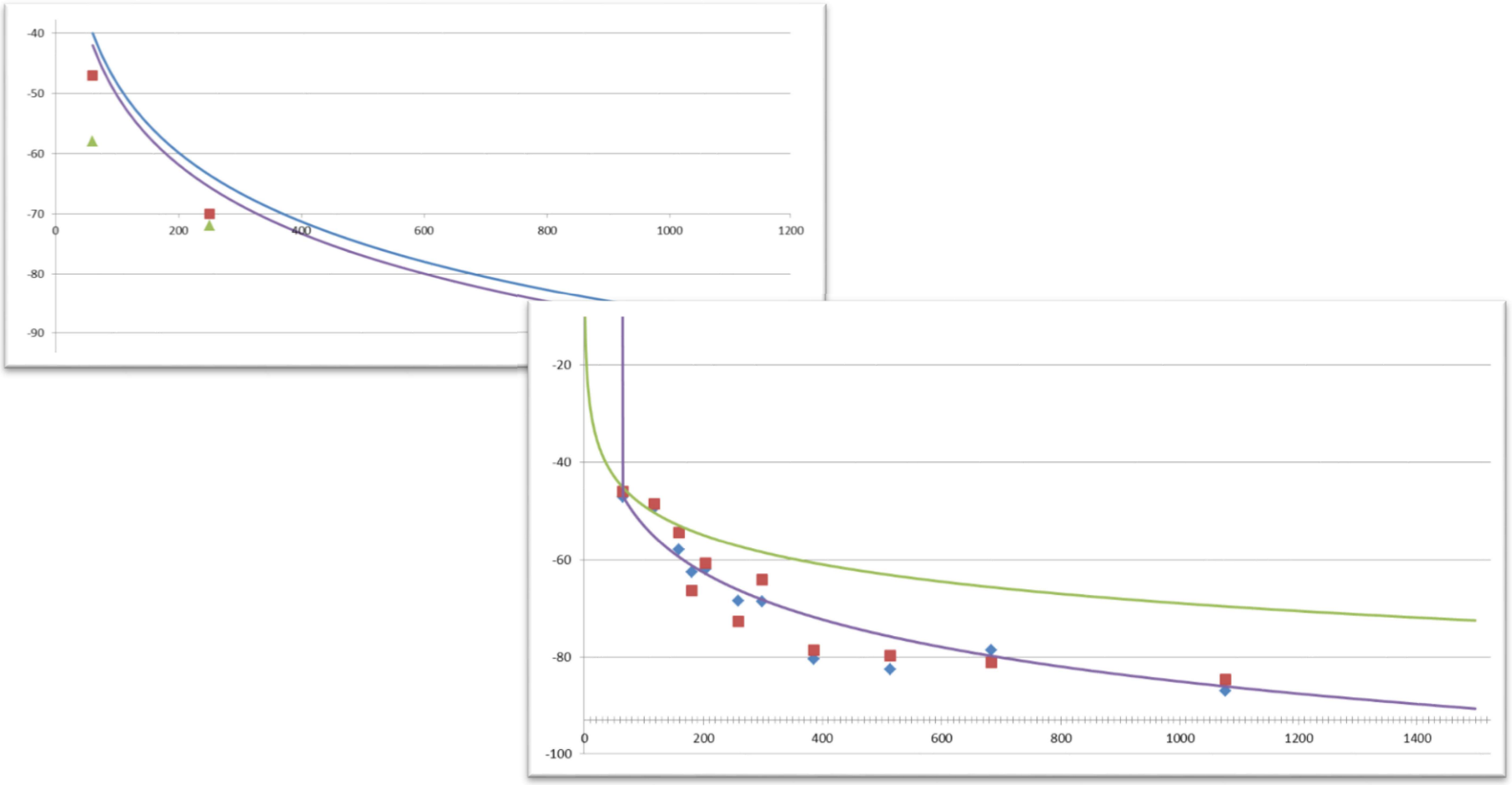
Okumura-Hatta model

$$L_U = 69.55 + 26.16\ \log f - 13.82 \log h_B - C_H + (44.9 - 6.55 \log h_B) \log d$$

Taddong

Distance estimation based on power measurements

Trying to adjust the models to our empirical data



Taddong

Distance estimation based on power measurements

Trying to adjust the models to our empirical data

- Models depend heavily on the environment
- We could not find or build a model that would automatically adapt to any environment
- Power measurements [illegible]reliable:
  - The effect of different [illegible] transmission path can have dra[illegible]

WE DISCARDED POWER FOR TRIANGULATION

Time-based Triangulation

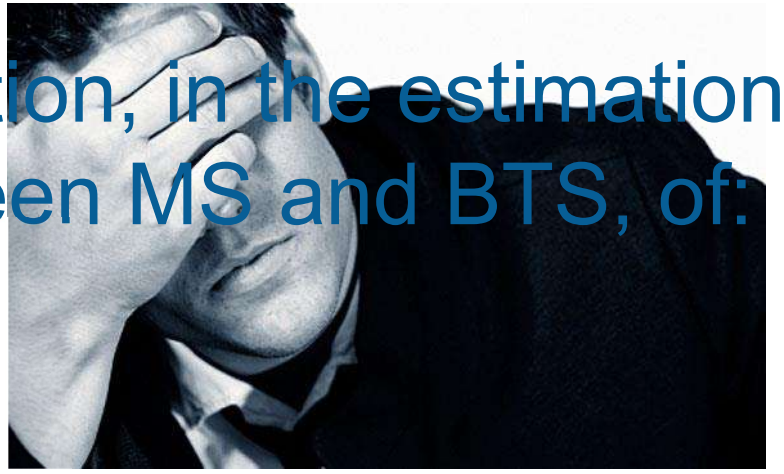
Taddong

Distance estimation based on time delay measurements

Time delay measurements

- In GSM, the delay of the signal that arrives to a BTS, as used in the *timing advance* mechanism, is measured in *modulation symbols*
- 1 symbol = 3,69 µs
- That means a resolution, in the estimation of the distance between MS and BTS, of:

¡¡ 553,5 meters !!



Fortunately, we heard a voice…

- OpenBTS measures and stores that time delay as a *float*, which would give a theoretical resolution of:

¡¡ < 1 meter !!

Taddong

Time-based Triangulation

Taddong

Distance estimation based on time delay measurements

Data properties

- Measurement errors are *quite big* (between 0,25 and 0,75 symbols).
- We found, empirically, that on top of that caused by the distance between MS and BTS, there is an **additional delay,** different for each device.
  - This delay is not big enough to affect GSM's *timing advance* mechanism, but it did render our triangulation calculations pretty much useless.

Obtaining an Acceptable Precission

Taddong

~~Designing~~ a distance estimation model based on time measurements

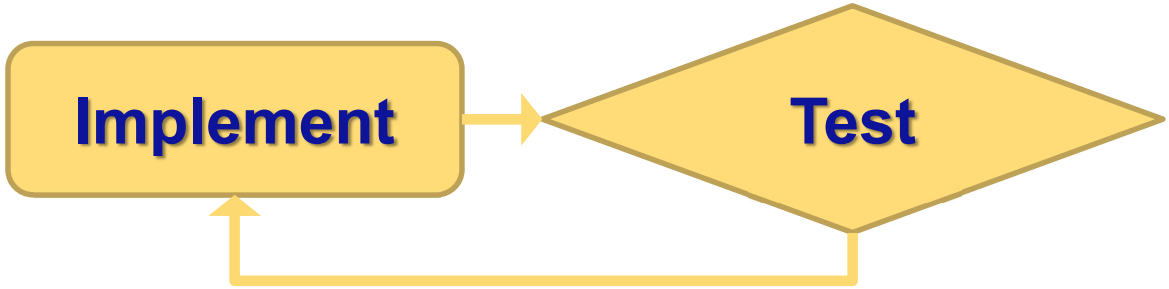
Adjusting the model

- We were forced to design algorithms to:
  - Predict/correct the errors in the time delay measurements
  - Predict/estimate the additional delays introduced by the different devices

Building a distance estimation model based on time measurements

Adjusting the model

- We were forced to design algorithms to:
  - Predict/correct the errors in the time delay measurements
  - Predict/estimate the additional delays introduced by the different devices



Taddong

Building a distance estimation model based on time measurements

Field testing

Taddong

Building a distance estimation model based on time measurements

Field testing = testing in fields of oranges ;-)

Taddong

Building a distance estimation model based on time measurements

Field testing = testing in fields of oranges

Taddong

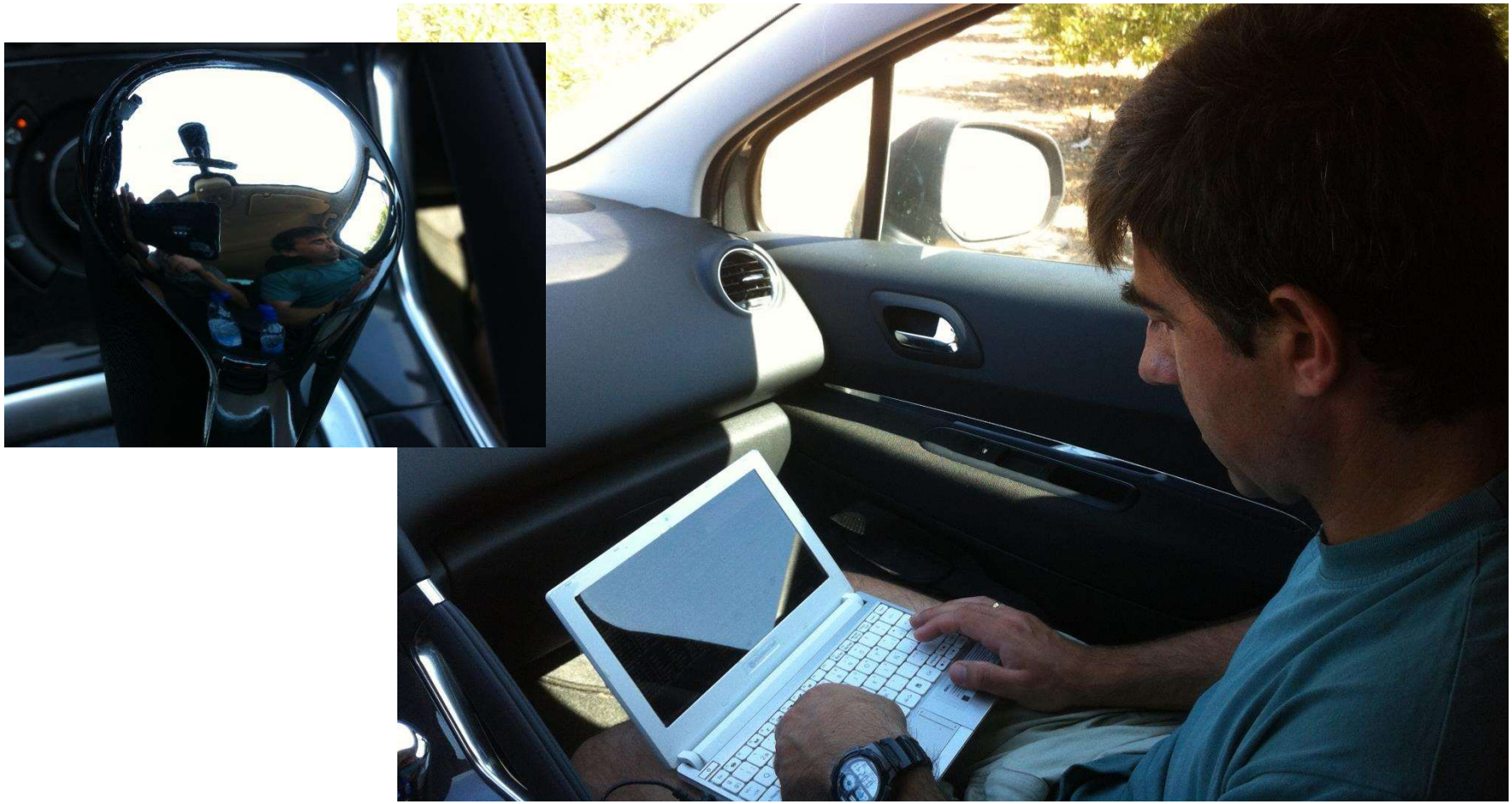
Building a distance estimation model based on time measurements

Field testing = testing in fields of oranges

Taddong

Building a distance estimation model based on time measurements

Field testing = testing in fields of oranges

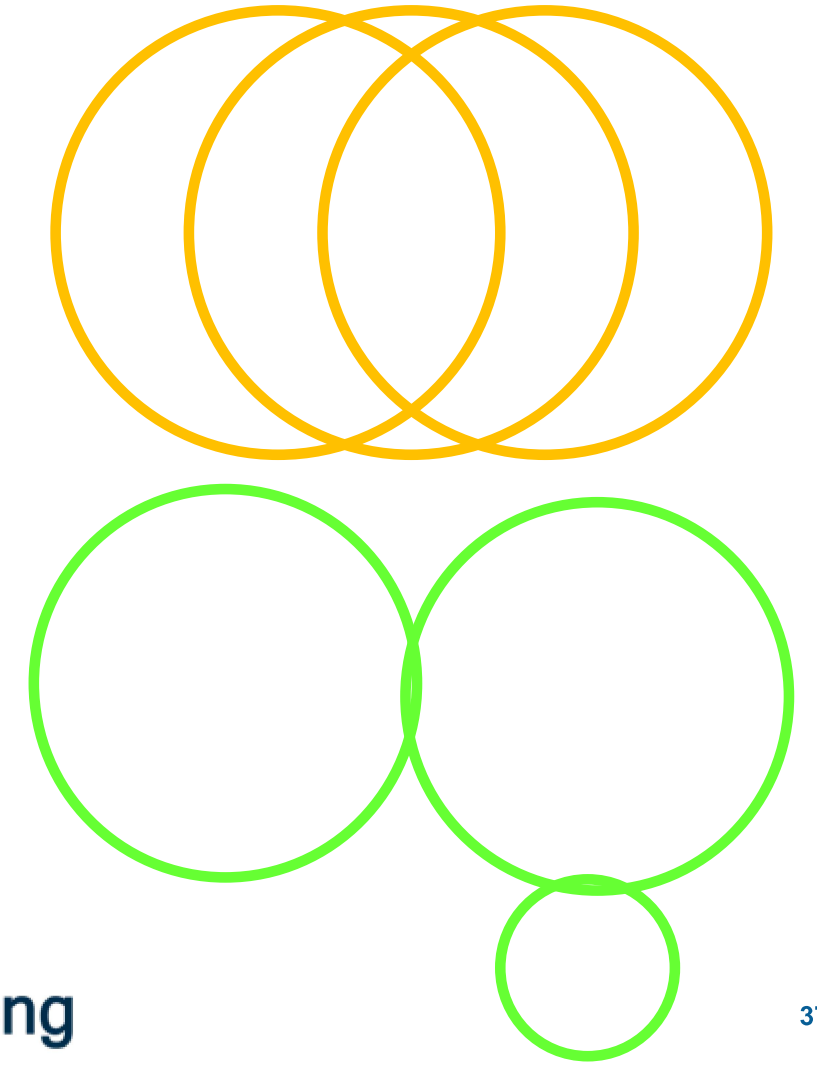


Taddong

Building a distance estimation model based on time measurements

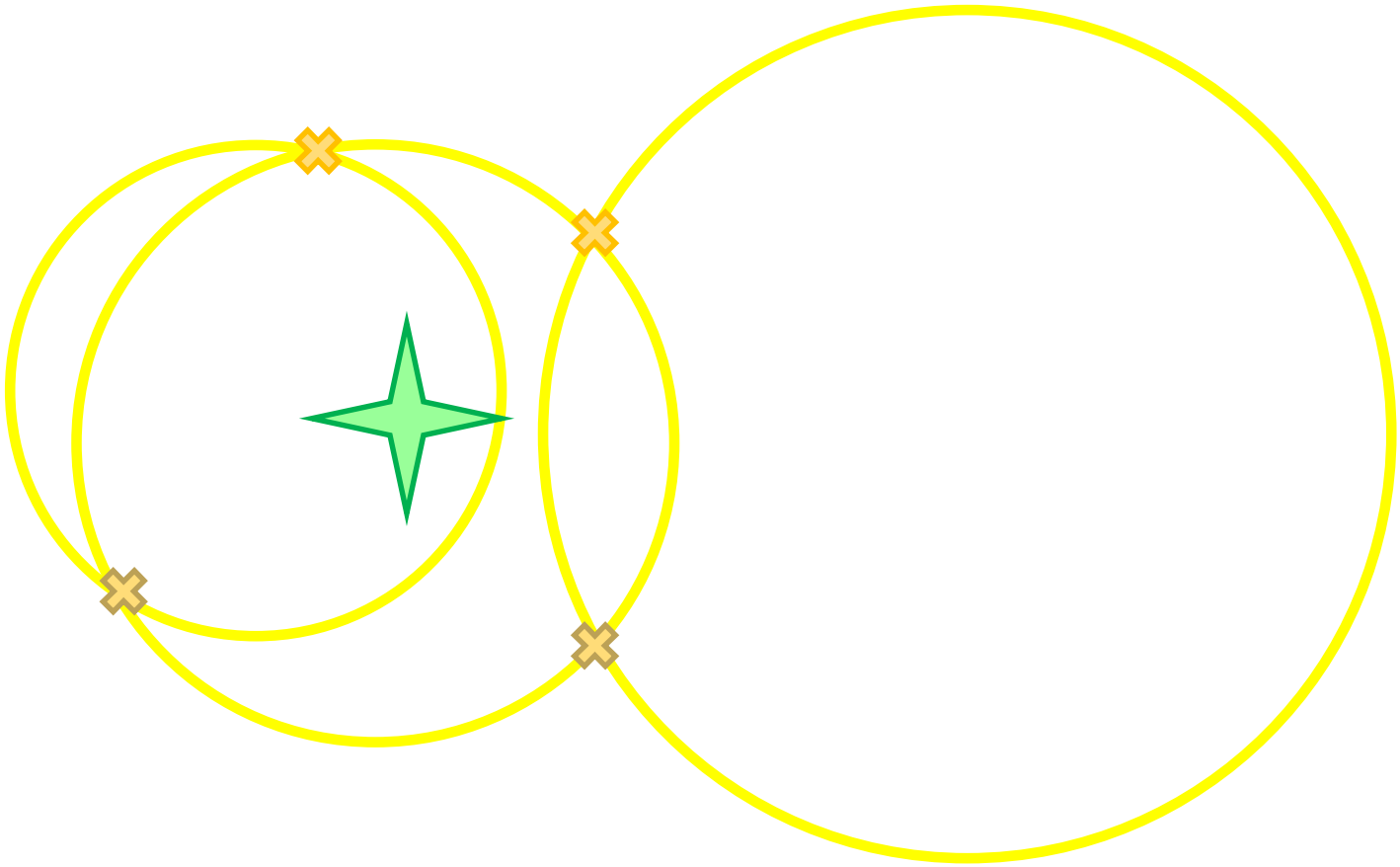
Example of adjustment #1

- From:
  - triangulating every time we got 3 triangulation points
- To:
  - choose the **best 3** triangulation points among the last 200 acquired



Building a distance estimation model based on time measurements

Example of adjustment #2

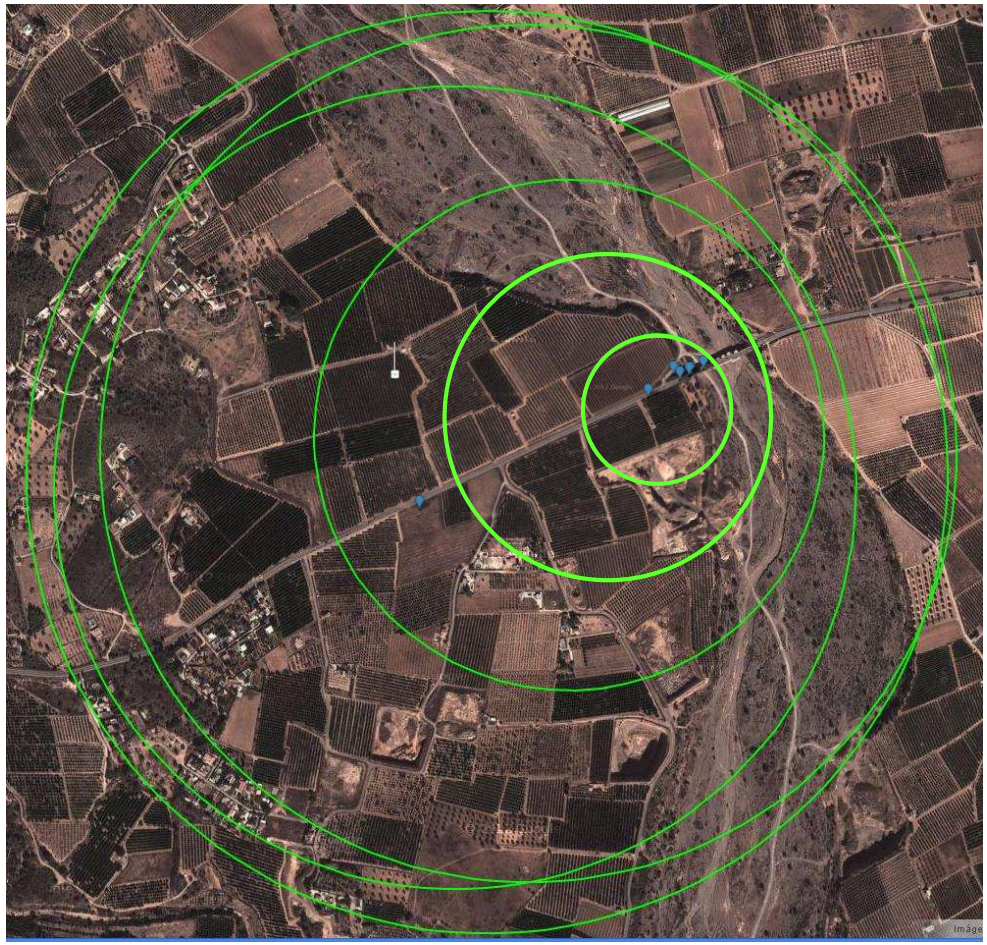


Taddong

Building a distance estimation model based on time measurements

After Phase 1 of adjustments

- Precission was not enough yet ☹
- Figure: where do these circles intersect?



Taddong

Building a distance estimation model based on time measurements

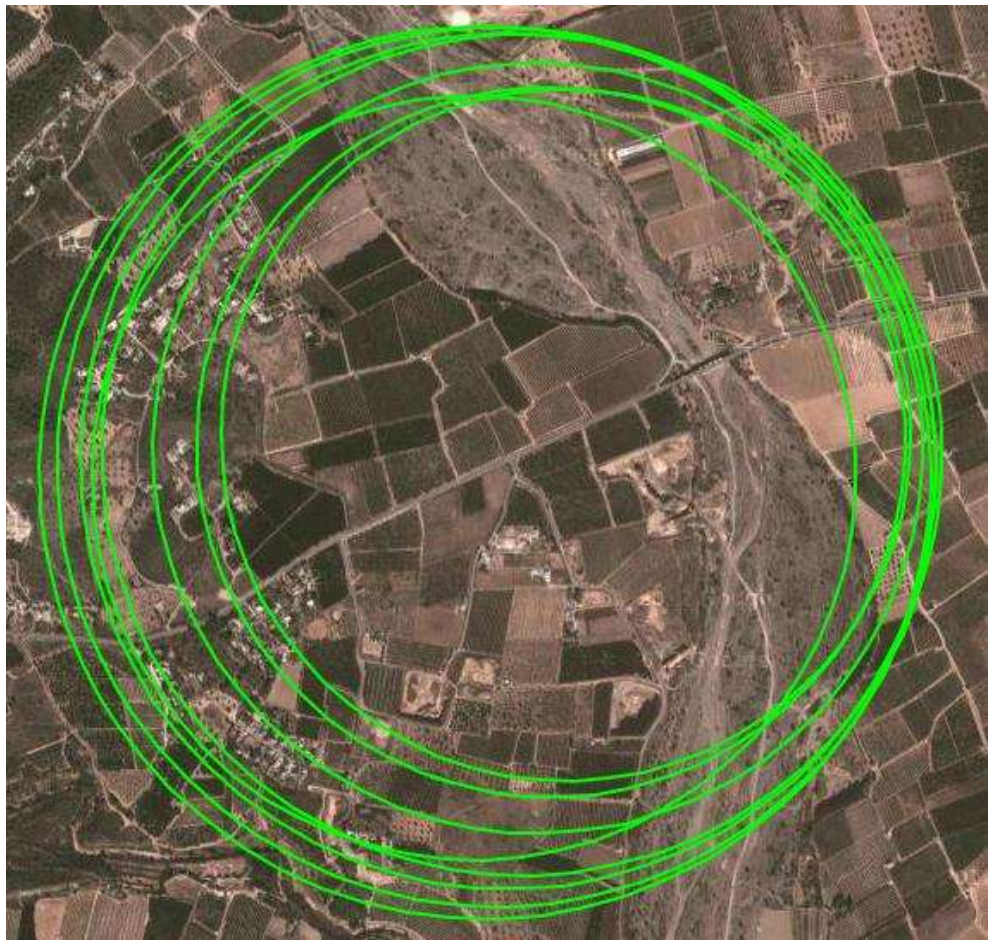
Phase 2 of adjustments. Example.

- Dynamic correction of the *additional delay*, based on certain specific conditions. E.g.:
  - Negative radius
  - Particular combinations of circle intersections

Building a distance estimation model based on time measurements

After Phase 2 of adjustments.

- Figure: same test as before



Taddong

Impersonating the real network

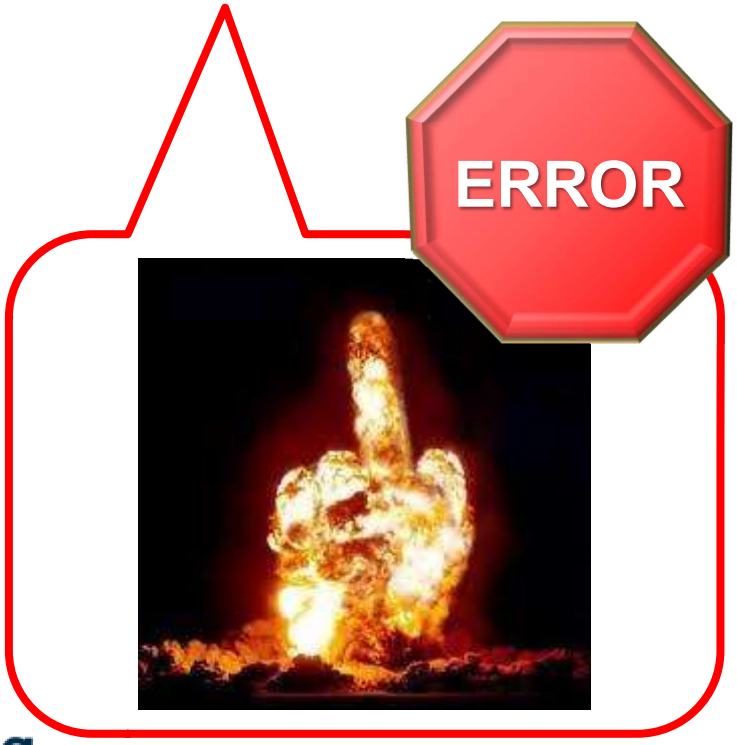
Taddong

Impersonating the real network

- We needed to configure the system to work in a real scenario, and for that:

- We needed to impersonate the real network of the target device

"This is going be a walk in the park, because we have already done this a hundred times!"



Impersonating the real network

Symptoms

- No device attempted to register with our fake cell.
- The terminals didn’t even see our fake cell as a neighbour cell.
- If we repeated the tests using a commercial BTS, terminals registered normally.

Impersonating the real network

Why, why, why???!!!

- Hypothesis #1: Not enough power
  - Discarded: when really close, we were frying the terminal
- Hipothesis #2: Something wrong with the information in our beacon?
  - We captured beacon signals from the c[illegible] BTS
  - We modified OpenBTS so that our be[illegible]by-bit equal to that of the commercial BT[illegible]
  - Yet, the problem remained! ☹

Taddong

Impersonating the real network

Hypothesis #3: precission of the clock

- Check:
  - We measured the frequency deviation of our USRP, and it turned out to be 900 Hz, while GSM allows only 45 Hz
- Workaround:
  - We modified OpenBTS to include an *offset* in syntonization
- Result:
  - Terminals registered correctly!!!

"Finally, solved!"

Taddong

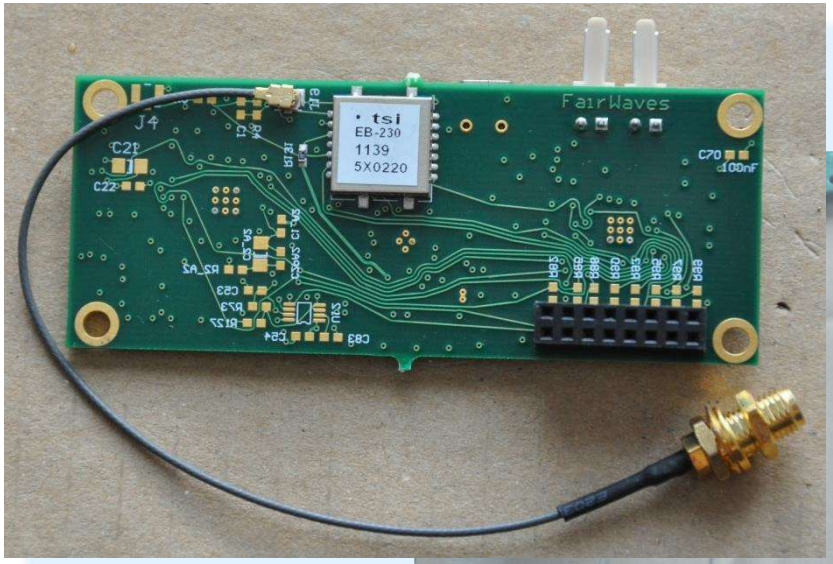
Impersonating the real network

The workaround was not good enough

- Terminals got registered, but...
- Time delay measurements got totally distorted, and made the system diverge ☹

Impersonating the real network

Final solution: replace clock with another more precise (clocktammer)



Taddong

Range

Taddong

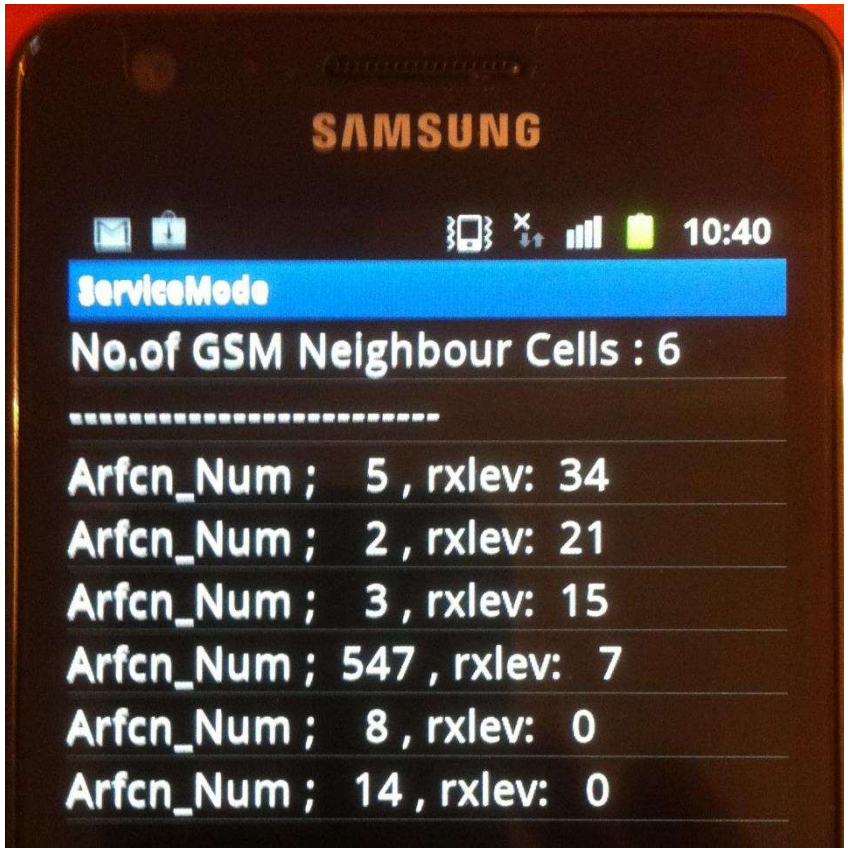
Range: first tests

- Once registered with our BTS, the MS remained in it up to a distance of 1,8 km in open field. Not bad.
- However, the maximum distance at which an MS registered with us, turned out to be…

¡¡ 15 meters !!

Conditions for registration

$P_{Attacker} > P_{ServingCell}$



Taddong

How much power did we need?

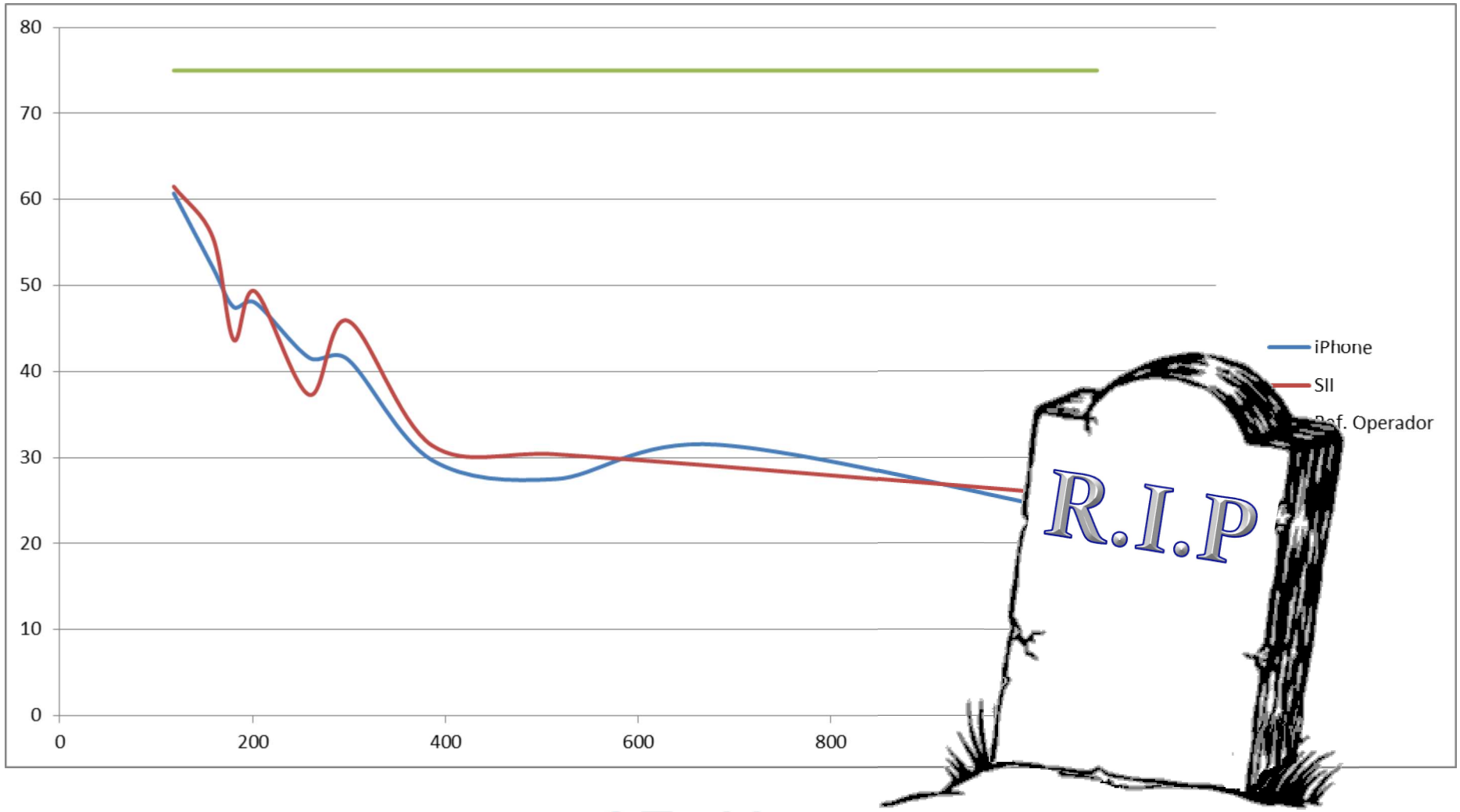
Measuring the power of a real network

The terminals reported the maximum measurable power (saturation level) even at a distance of 2 Km

Taddong

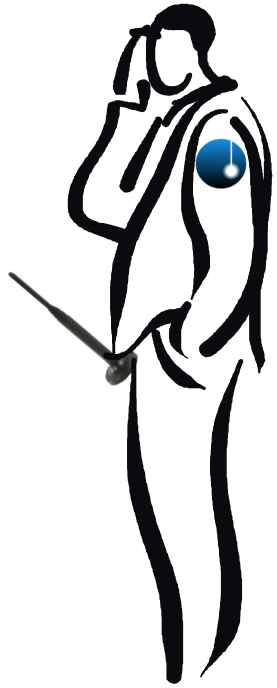
How much power did we need?

Real network vs. our fake BTS



Taddong

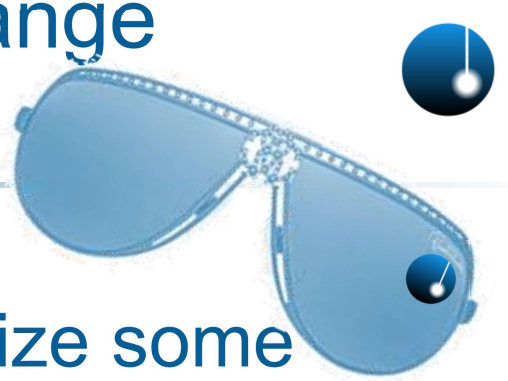
Problem



Taddong

Solution

Solution to the registration range problem



Technical explanation

- GSM defines a mechanism to prioritize some cells over others (CRO - *Cell Reselection Offset*)
- Using that mechanism in our beacon, if we got in the list of the 6 most powerful neighbour cells, we won.
- It was not implemented in OpenBTS 2.6. We had to add emision of SI3 Rest Octets.

Solution to the registration range problem

Example of our new registration range

Taddong

Directional Mode

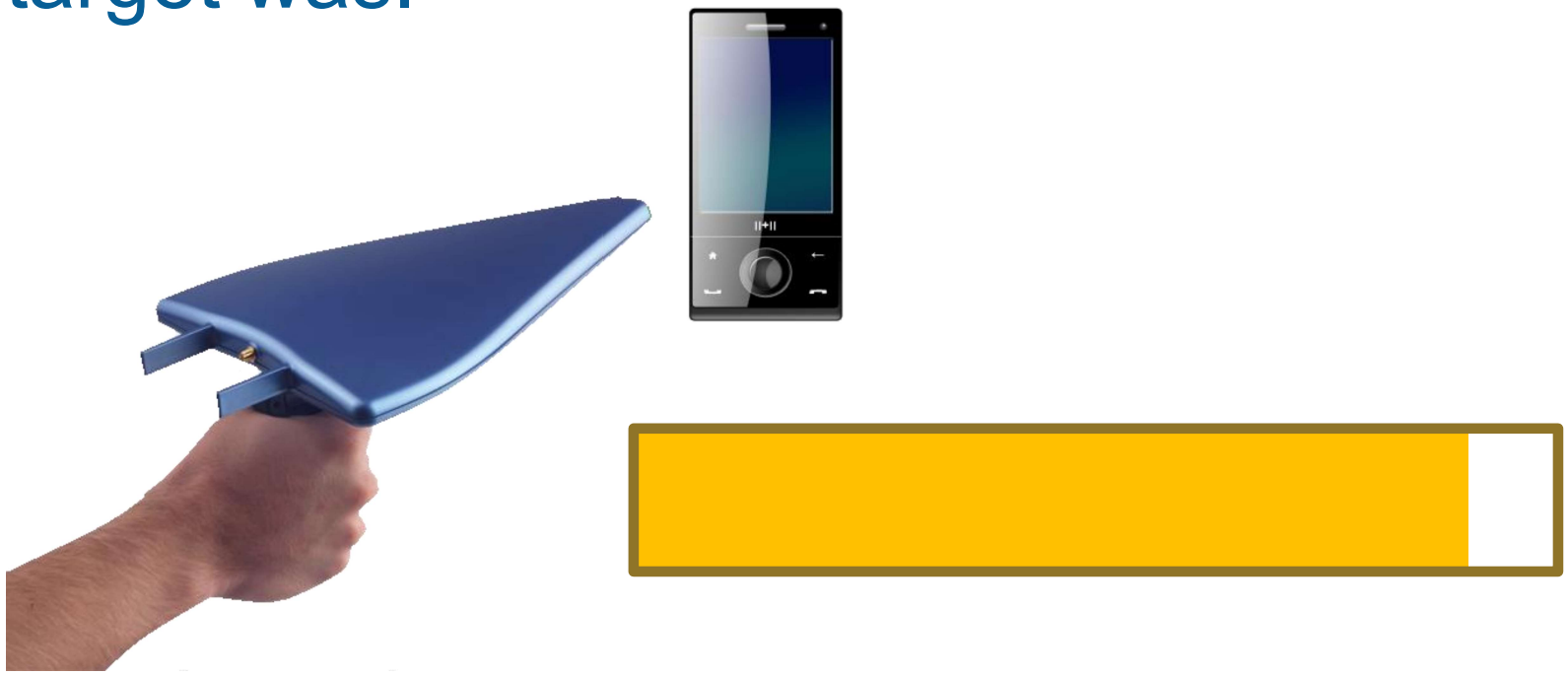
Taddong

Directional Mode

- The idea was to have a pointer that could, at close range, tell us where exactly the target was.

Directional Mode

- The idea was to have a pointer that could, at close range, tell us where exactly the target was.



Directional Mode

“This won’t take us longer than 2 hours to implement!”

- For this mode, we decided to use the power received by the BTS:
  - the more power, the better we would be pointing at the target

Directional Mode

Problem & Solution

- Problem:
  - The measures were very oscillating and unstable.
- Cause:
  - GSM constantly regulates the power emitted by the terminal, so the MS always transmits at the minimum power that will allow it to reach the BTS.
- Solution:
  - We modified the code to deactivate this power control mechanism when the system was in directional mode.

Final Result

Taddong

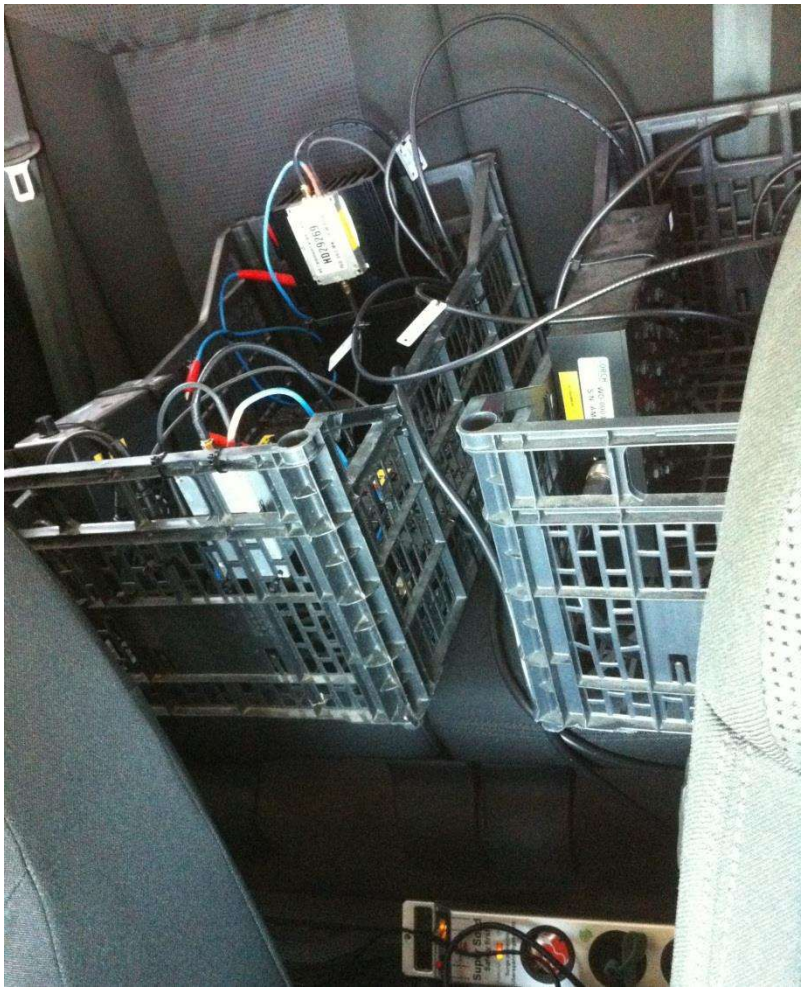
Final Result

Hardware setup

Taddong

Final Result

Hardware setup

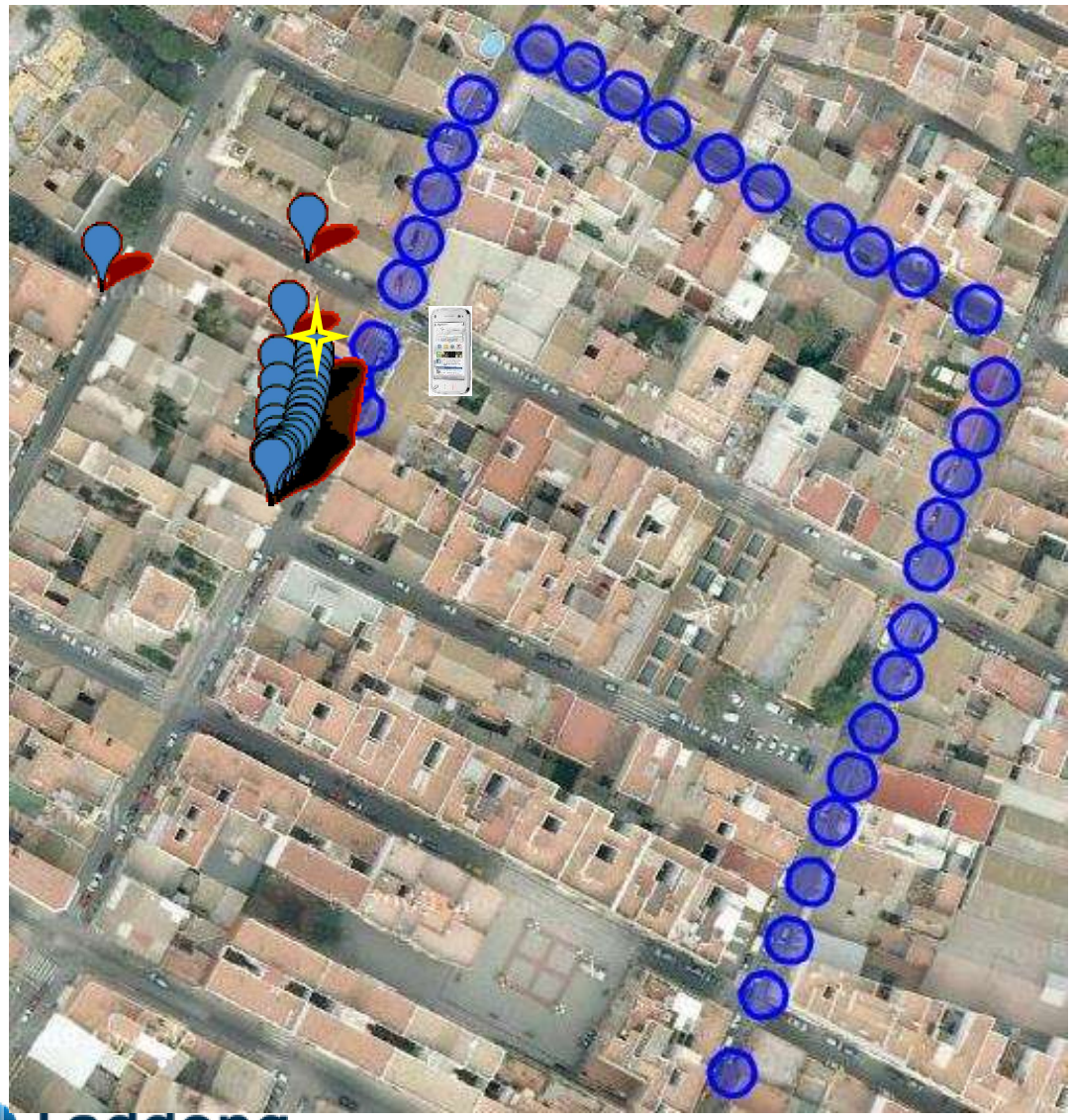


Final Result

Precission in open field environment

Final Result

Precission in urban environment



Final Result

Demo (videos)

Omnidirectional mode

ncurses console

iPad console

Directional mode

ncurses console

Taddong

Future Work

- Extend system functionality to 3G
- Improve algorithms to obtain a better position accuracy
- Add functionality to the remote (iPhone) console


Thank you!
Taddong
www.taddong.com
@taddong