/Rootəd 2013

Sistema de localización geográfica de un terminal móvil

Taddong

www.taddong.com
@taddong

David Pérez
david@taddong.com

José Picó
jose@taddong.com

PRÓLOGO

Localización de terminales móviles

- Servicios de localización GSM – LCS:
  - basados en la red
  - basados en el móvil
  - asistidos por el móvil

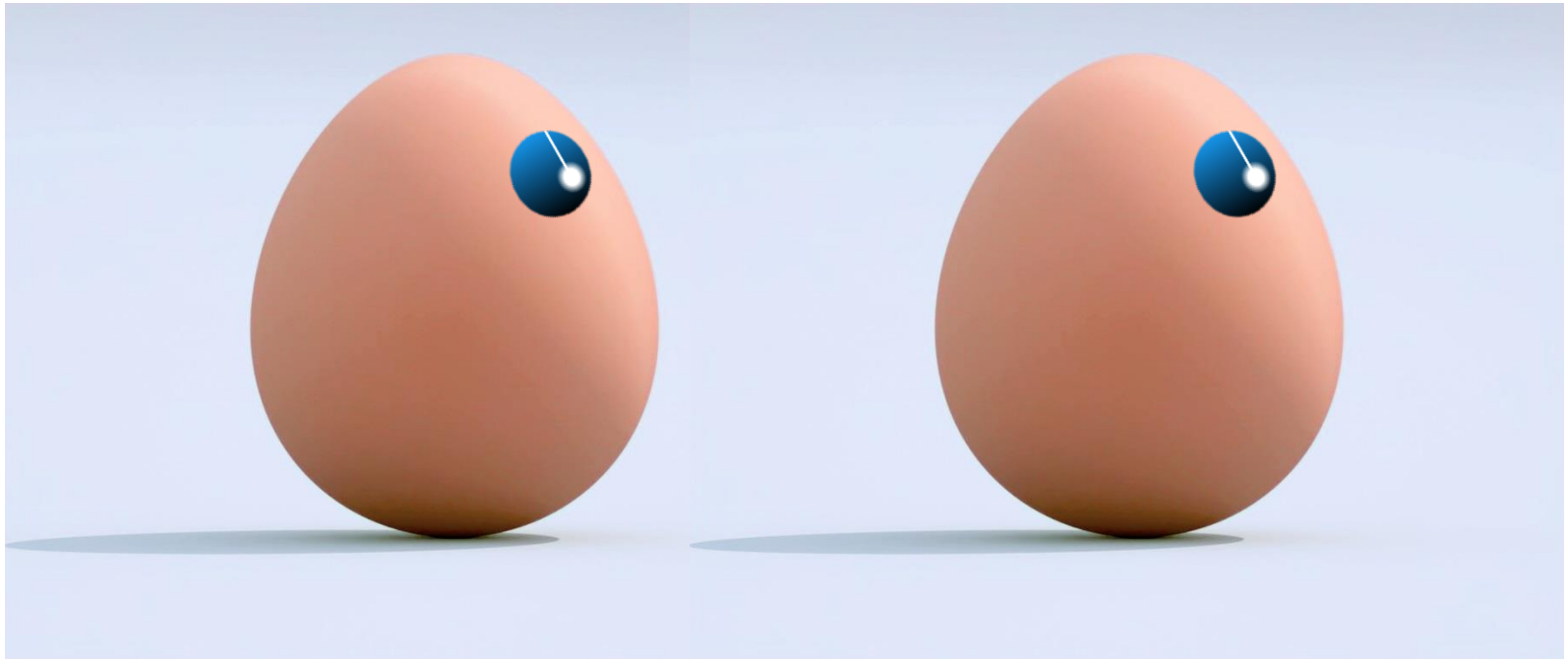
  } RRLP

- Software de localización instalado en el móvil

¿Y si el terminal no quiere ser localizado y no tenemos acceso a la red?

Y entonces alguien dijo la frase mágica:

"¡A que no hay…"



OBJETIVOS

Objetivos de esta charla

- Responder a la siguiente pregunta:

¿Cómo podríamos localizar un terminal móvil *que no quiere ser localizado sin tener acceso a la red*?

- Ilustrar el proceso de este proyecto de investigación

CONDICIONES DE PARTIDA

Condiciones de partida

- No se tiene acceso al operador
- El terminal tiene deshabilitado cualquier servicio de localización
- Datos conocidos:
  - Ubicación aproximada ("área")
  - IMEI o IMSI
- Otras restricciones al problema:
  - El *target* está en una ubicación fija (o casi)
  - Un único sistema que pueda operarse desde un vehículo convencional

Objetivo del Sistema

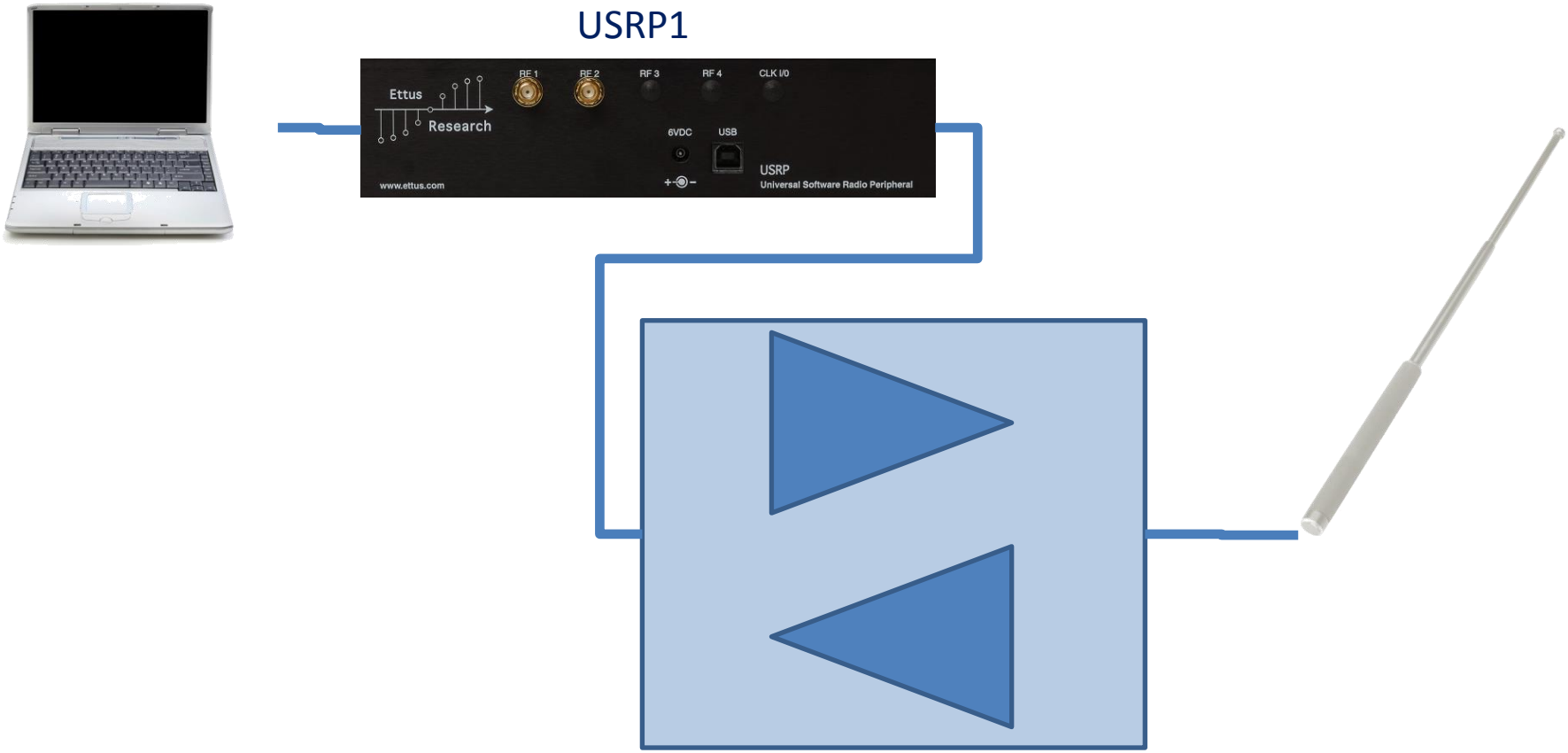
"Vamos a hacerlo bien: diseñando desde el principio y definiendo el ciclo de vida del software"

DISEÑO INICIAL

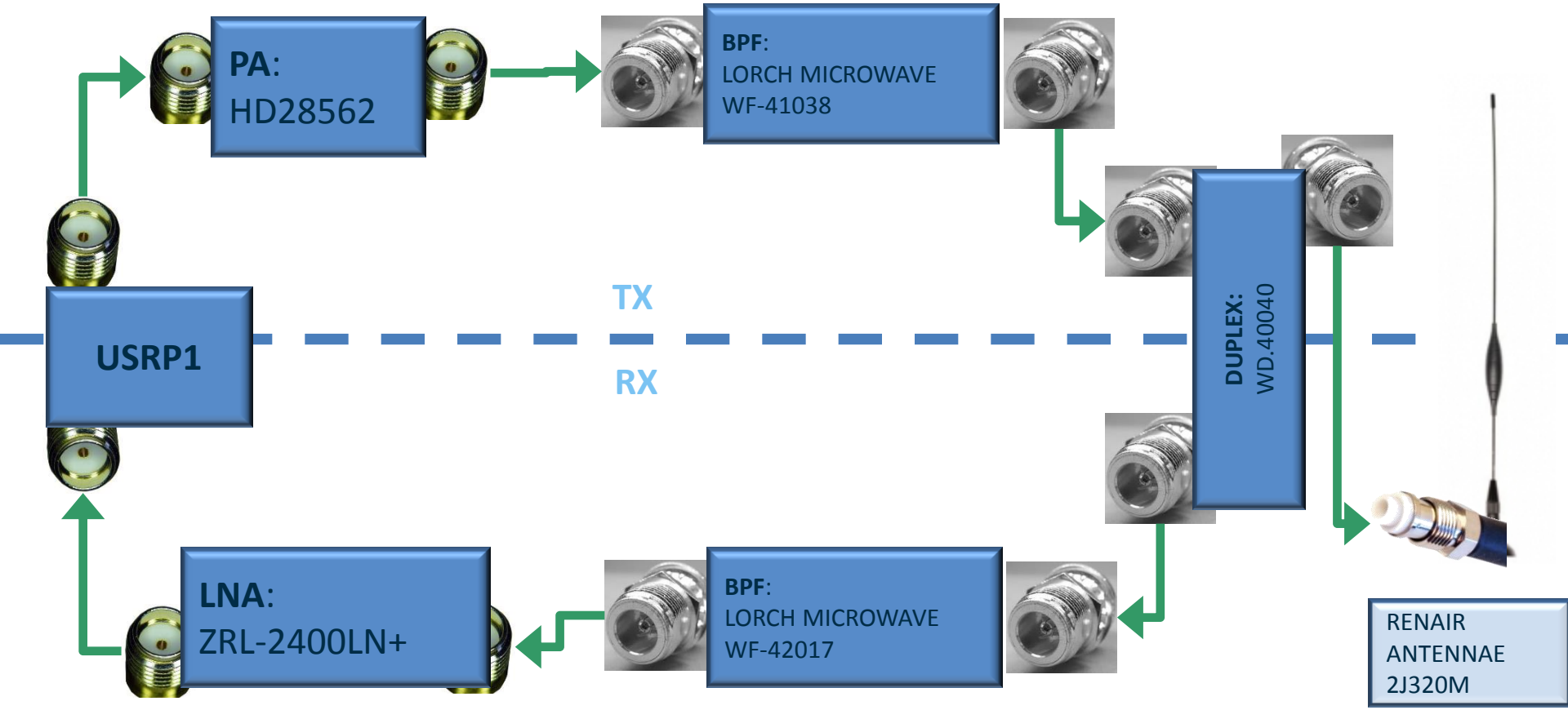
JA JA JA

Hardware

Esquema general



Hardware: etapa de amplificación (*)



(*) Nos basamos en un esquema de Dburguess creado para el Burning Man

Hardware: antenas seleccionadas *inicialmente*

Modo direccional y modo omnidireccional

- Modo omnidireccional para localizar el objetivo

- Modo direccional para "apuntar" al objetivo y realizar una localización fina (ventana del edificio)

Software

- Desarrollo sobre el software OpenBTS(*) 2.6, al que se deben añadir las siguientes funcionalidades:
  - Adquisición e integración en el sistema de datos GPS
  - Cálculos de triangulación en base a datos de potencia y retardo en tiempo proporcionados por la estación base GSM
  - Consola de usuario en modo texto

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

Investigación de las fuentes de datos útiles para triangular proporcionados por la estación OpenBTS+USRP

DATOS DISPONIBLES PARA LA TRIANGULACIÓN

Fuentes de datos

Desde una estación base pueden obtenerse datos útiles

- Potencia (absoluta) que el móvil percibe de la estación base
  - Utilizados por GSM para la planificación de los procedimientos de *handover*
- Potencia (relativa) que la estación base percibe del móvil
  - Utilizados por GSM para el control dinámico de potencia del móvil
- Retardos en tiempo
  - Utilizados por GSM para el control del *timing advance*

Fuentes de datos

Elección inicial de la fuente de datos

- Tomar como dato de partida el retardo de tiempo de la llegada de la señal nos parecía a priori un dato poco preciso.
- Por ello, nos decantamos por:
  - Utilizar datos de potencia percibida por la estación, correlados con los datos de potencia percibida por el móvil
  - Utilizar los datos de retardo en tiempo para realizar correcciones únicamente

TRIANGULACIÓN BASADA EN POTENCIA

Triangulación en base a potencia

"Esto está chupado"

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

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

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

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

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

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

NOTA: a debe ser distinto de 0

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

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

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

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

Triangulación en base a potencia

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

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

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

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

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

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

NOTA: a debe ser distinto de 0

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

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

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

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

"Esto está chupado"

Diseñando un modelo a partir de datos de potencia

Diferentes modelos empírico-matemáticos

Path Loss between isotropic antennas in direct sight

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

Path Loss exponent models

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

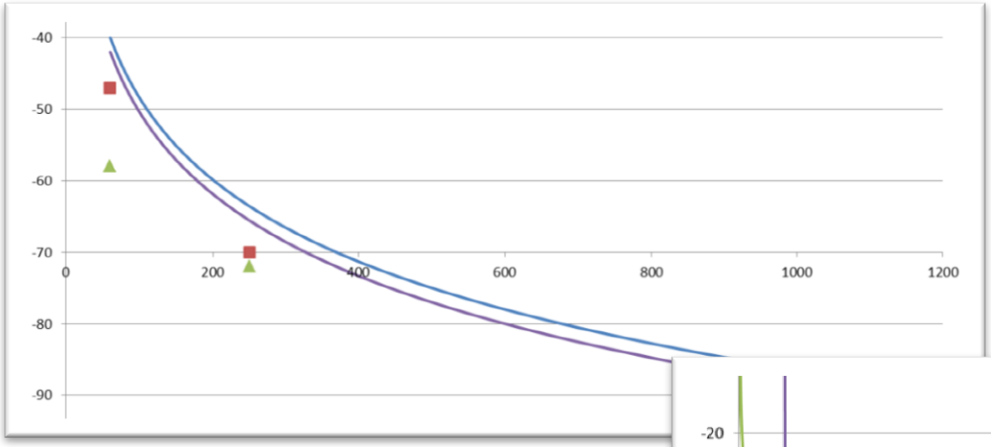
$$\mathbf{L} = 10\,n\ \log_{10}(d) + C$$

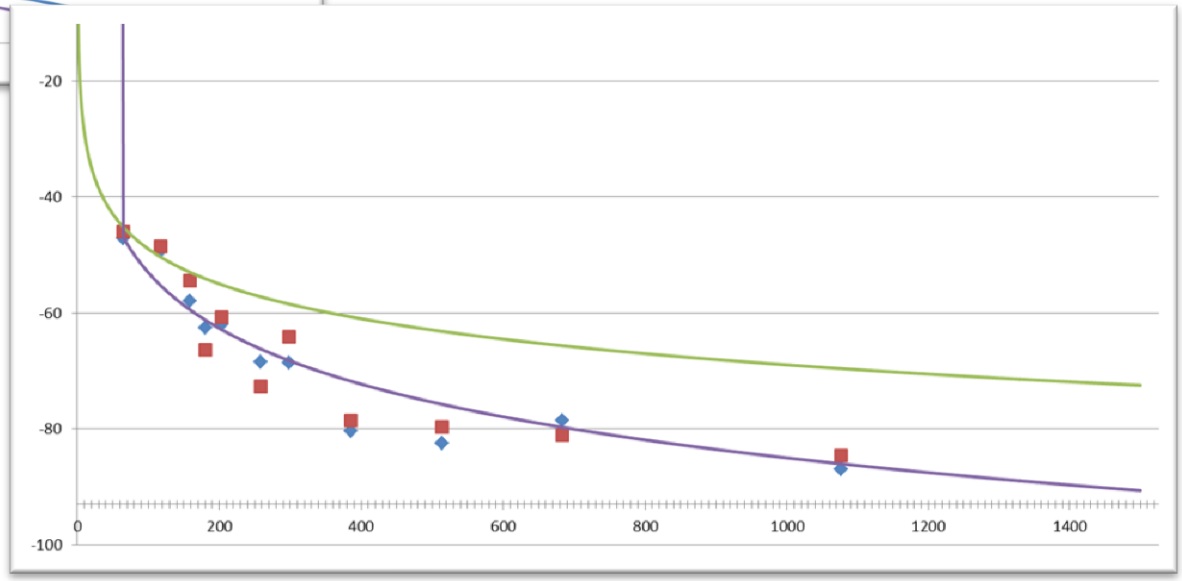
Okumura-Hatta model

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

Diseñando un modelo a partir de datos de potencia

Ajuste de los modelos a las pruebas empíricas





Diseñando un modelo a partir de datos de potencia

Ajuste de los modelos a las pruebas empíricas

- Los modelos son totalmente dependientes del entorno
- La predicción del tipo de entorno a partir de los modelos no ha sido posible (o no hemos sido capaces)
- Los datos de potencia n
  - La potencia percibida en
    puede ser muy distinta debido a
    obstáculos

DESCARTAMOS EL USO DE LOS DATOS DE POTENCIA (para triangular)

TRIANGULACIÓN BASADA EN RETARDOS DE TIEMPO

Diseñando un modelo a partir de datos de retardo en tiempo

Datos de retardo en tiempo

- El retardo en tiempo de la señal que llega del móvil se mide en símbolos de modulación (1 símbolo = 3,69 µs).
- La distancia entre móvil y BTS que corresponde a un retardo de 1 símbolo es de:

¡¡ 553,5 metros !!

Afortunadamente…

- OpenBTS mide y almacena el retardo como un *float*, la resolución téorica es:

¡¡ < 1 metro !!

Triangulación en base a tiempo

"Esto sí que está chupado"

Diseñando un modelo a partir de datos de retardo en tiempo

Características de los datos

- El error de las medidas es *bastante grande* (entre 0,25 y 0,75 símbolos).
- Descubrimos empíricamente que existe un **retardo adicional** al causado por la distancia, que es diferente para cada dispositivo.
  - Este retardo adicional no afecta al mecanismo de *timing advance*, pero sí desvirtúa los resultados de los cálculos de triangulación.

OBTENER UNA PRECISIÓN ACEPTABLE DEL SISTEMA EN FASE OMNIDIRECIONAL

~~Diseñando~~ un modelo a partir de datos de retardo en tiempo

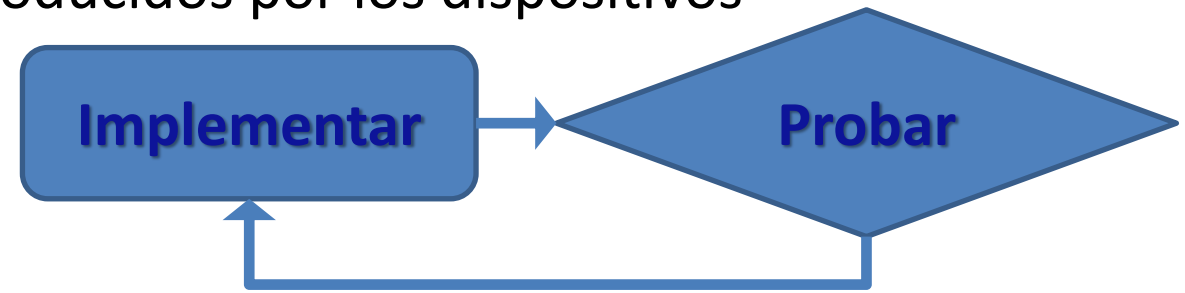
Ajustando el modelo

- Ha sido necesario diseñar algoritmos que:
  - intenten predecir/corregir las imprecisiones en las medidas para conseguir una precisión del sistema aceptable
  - intenten predecir/estimar los retardos adicionales introducidos por los dispositivos

Construyendo un modelo a partir de datos de retardo en tiempo

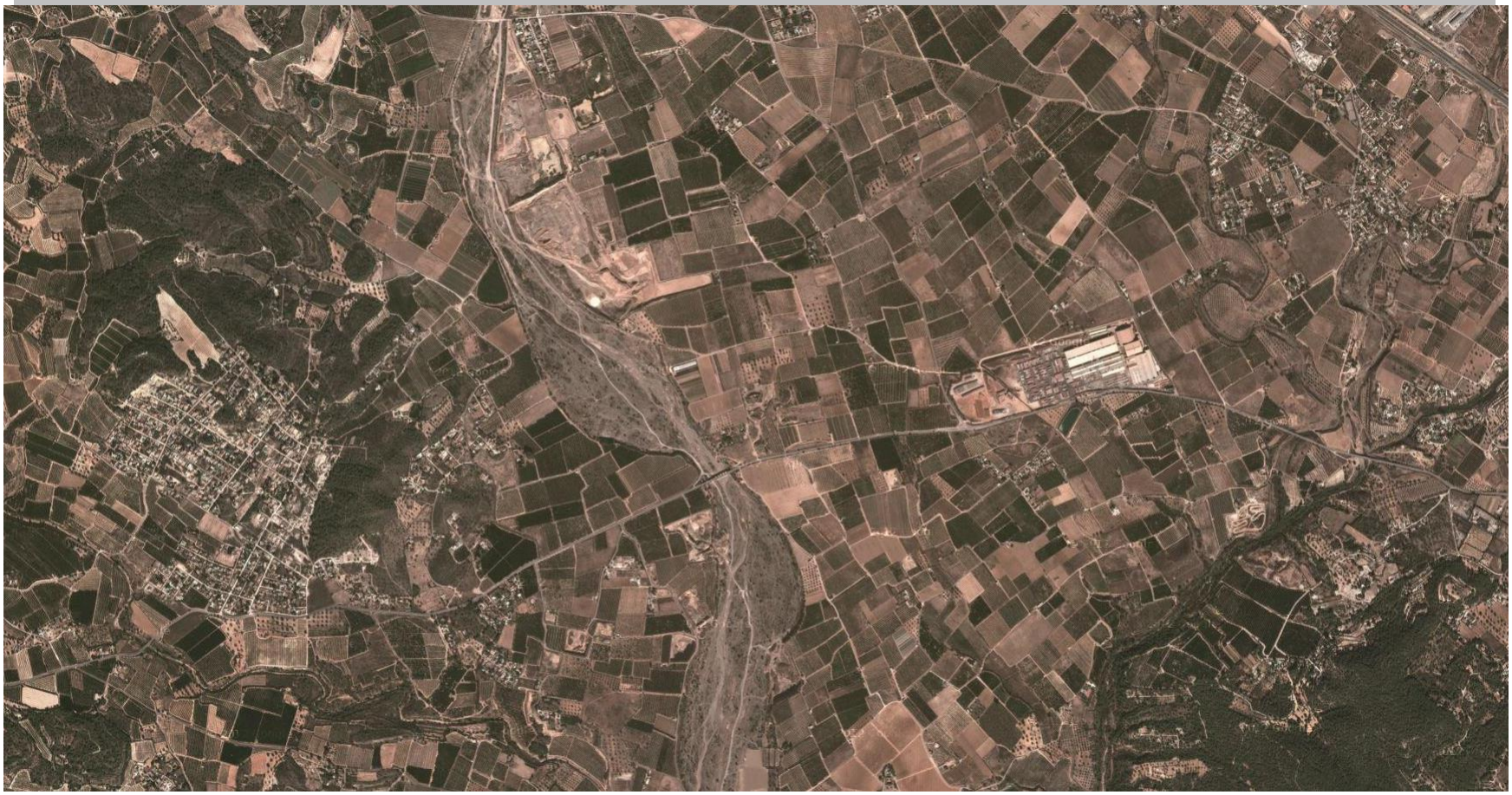
Ajustando el modelo

- Ha sido necesario diseñar algoritmos que:
  - intenten predecir/corregir las imprecisiones en las medidas para conseguir una precisión del sistema aceptable
  - intenten predecir/estimar los retardos adicionales introducidos por los dispositivos



Construyendo un modelo a partir de datos de retardo en tiempo

Inicio de las pruebas de campo



Construyendo un modelo a partir de datos de retardo en tiempo

Inicio de las pruebas de campo… de naranjos.

Construyendo un modelo a partir de datos de retardo en tiempo

Inicio de las pruebas de campo… de naranjos.

Construyendo un modelo a partir de datos de retardo en tiempo

Inicio de las pruebas de campo… de naranjos.

Construyendo un modelo a partir de datos de retardo en tiempo

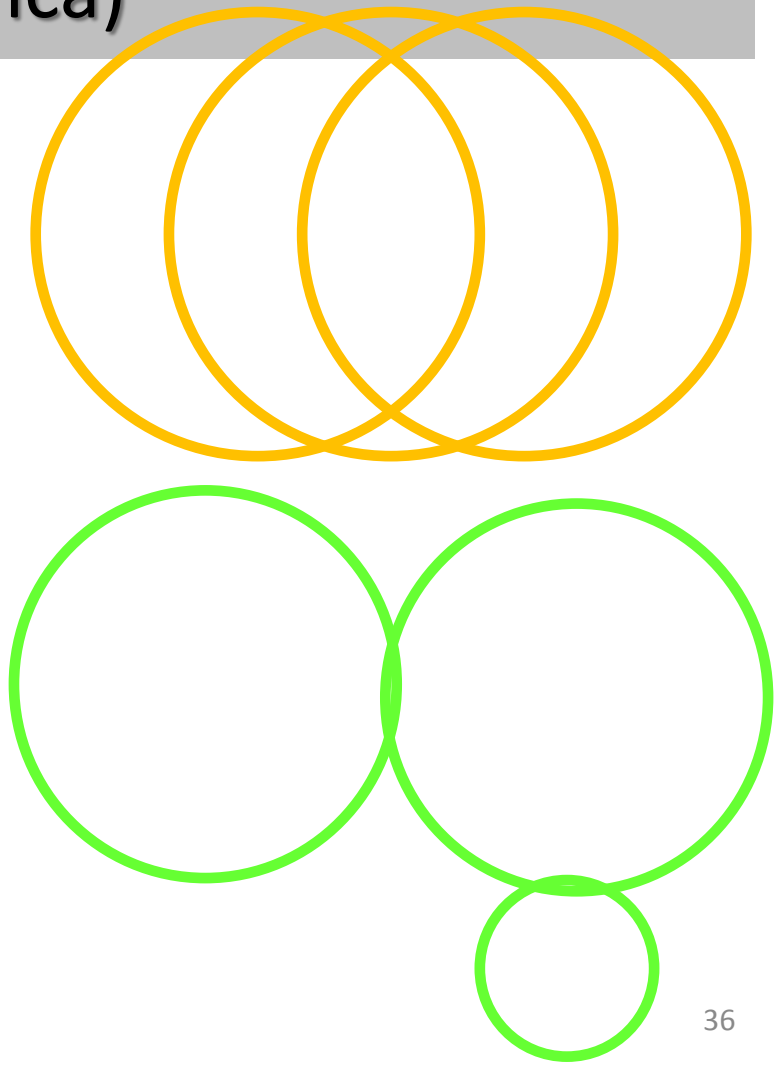
Inicio de las pruebas de campo… de naranjos.

Diseñando un modelo a partir de datos de retardo en tiempo

Ejemplo de ajuste (rep. gráfica)

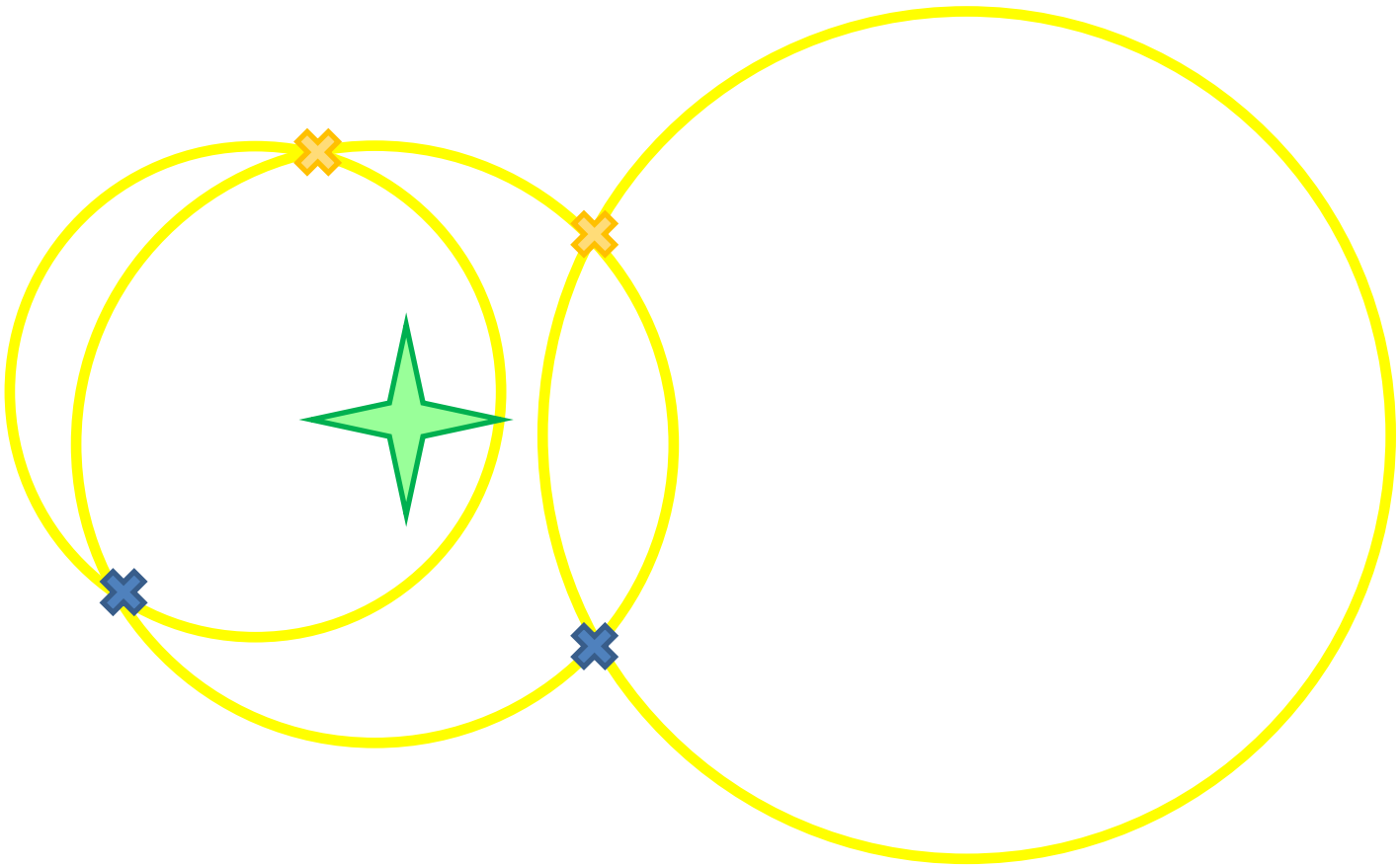
- De triangular cada 3 puntos de triangulación adquiridos

- A elegir los 3 **mejores** entre todos los puntos adquiridos con una profundidad histórica de 200



Diseñando un modelo a partir de datos de retardo en tiempo

Ejemplo de ajuste (rep. gráfica)



Diseñando un modelo a partir de datos de retardo en tiempo

Fase 1 de ajustes en funcionamiento

- En el ejemplo se muestra un caso muy desfavorable: desplazamiento en linea recta con un error significativo

Diseñando un modelo a partir de datos de retardo en tiempo

Fase 2 de ajustes

- Corrección dinámica del retardo adicional en base a situaciones identificadas que nos aseguren una corrección correcta, como por ejemplo:
  - Radios negativos
  - Casos especiales en la combinación de intersecciones

Diseñando un modelo a partir de datos de retardo en tiempo

Ejemplo 3 de ajuste implementado (en funcionamiento)

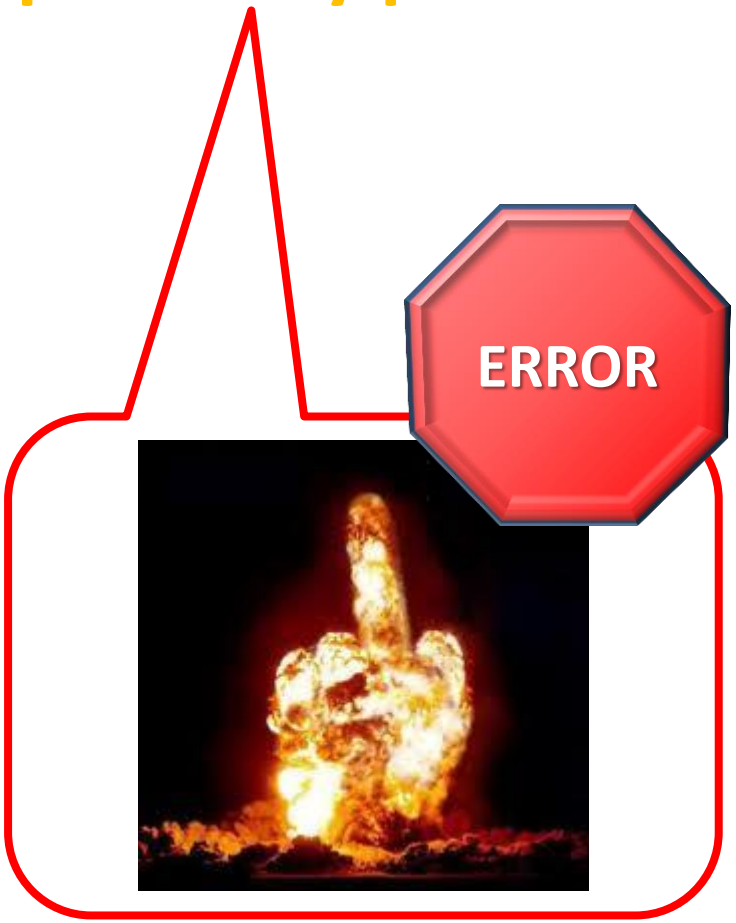
- Misma prueba anterior con la corrección dinámica del retardo adicional

SUPLANTACIÓN DEL OPERADOR REAL

Suplantación del operador real

"Esto lo hemos probado miles de veces: aquí no hay problema"

- En esta fase queríamos parametrizar y configurar el sistema para funcionar en un entorno de operación real



Suplantación del operador real

Síntomas

- El sistema “en real” no registraba ningún terminal.
- Los terminales ni siquiera veían la celda falsa como celda vecina
- Al hacer las pruebas con la nanobts los terminales sí se registraban

Suplantación del operador real

Hipótesis iniciales

- Hipótesis 1: Potencia
  - Descartada, porque estábamos friendo al terminal

- Hipótesis 2: emisión errónea en los bits de beacon de nuestra estación
  - Escuchamos las señales de beacon de un operador celda openbts+usrp
  - Modificamos el código de openbts para que emita exactamente igual (bit a bit) que el del operador
  - Aún así, el problema no se resolvía

Suplantación del operador real

Hipótesis 3 y solución: precisión del reloj

- Medimos la desviación en la sintonización de frecuencias de nuestra USRP y se desviaba 900 Hz (GSM permite 45 Hz)
- Solución implantada: modificamos el código para poderle configurar manualmente on *offset* en la sintonización

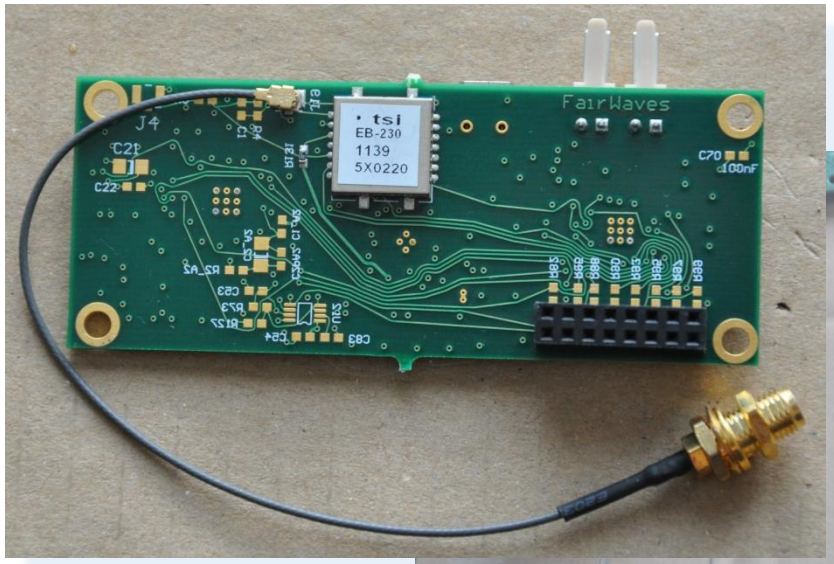
Suplantación del operador real

La solución no era buena

- La modificación en el código solucionaba el problema del registro del terminal
- Sin embargo, las medidas de retardo se distorsionaban y hacían que el sistema se transformase en divergente

Suplantación del operador real

Solución final: poner un reloj de mayor precisión (clocktammer)



ALCANCE DEL SISTEMA

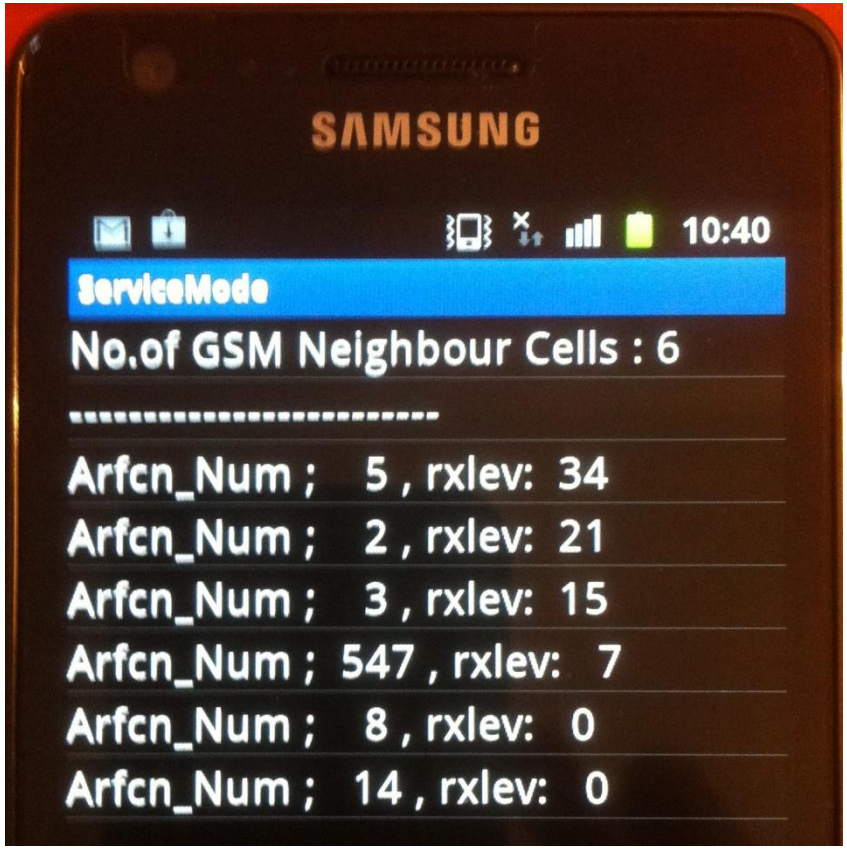
Primeras pruebas de alcance

- Una vez registrado en nuestro sistema, el móvil permanecía en él con un alcance aprox. de 1,8 km. en el campo
- Un móvil se conseguía registrar en nuestro sistema a la distancia máxima de…

¡¡ 15 metros !!

Condiciones de potencia para el registro

$$P_{Atacante} > P_{ServingCell}$$



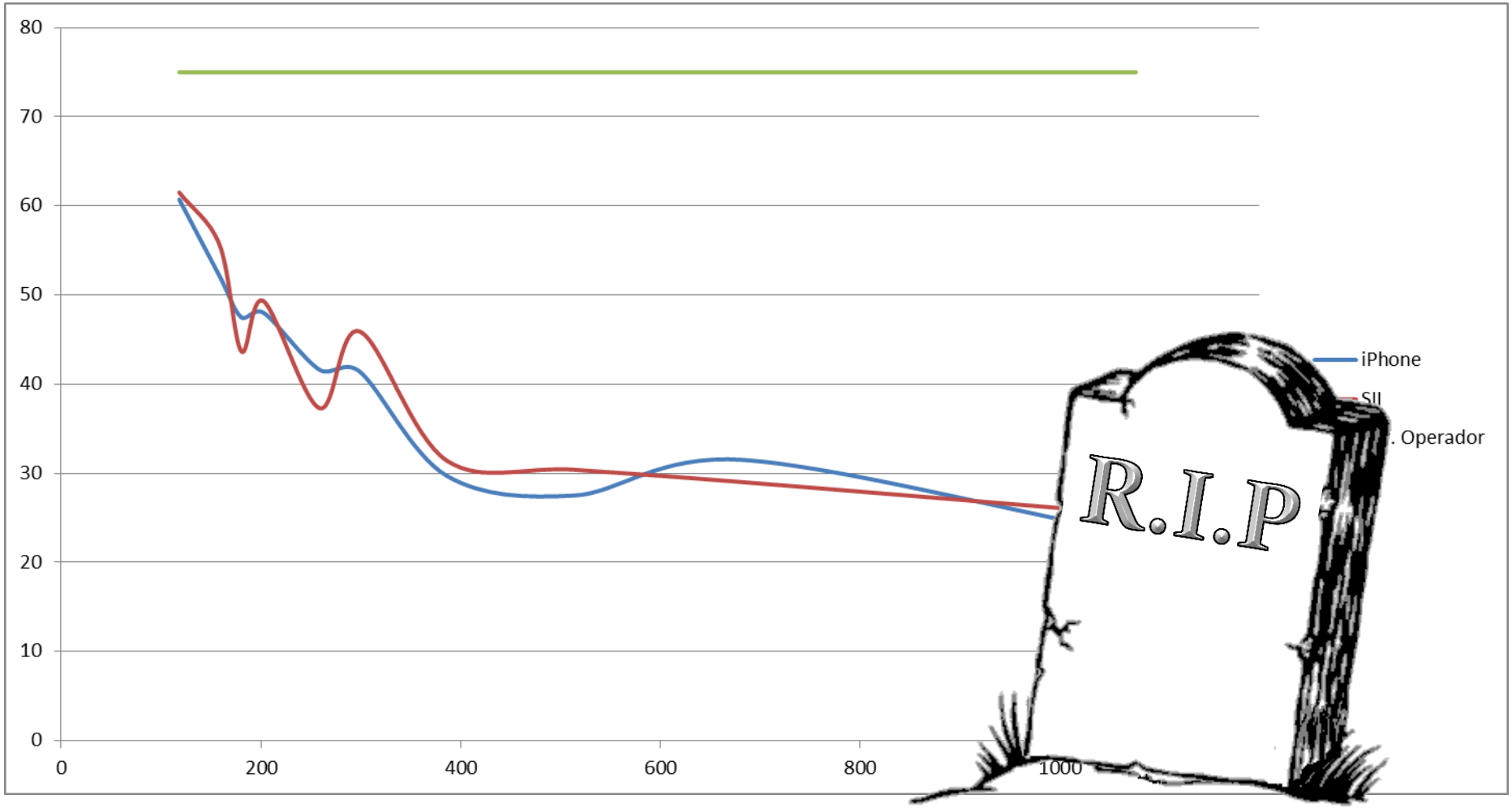
¿A qué potencia deberíamos emitir?

Medidas del operador real

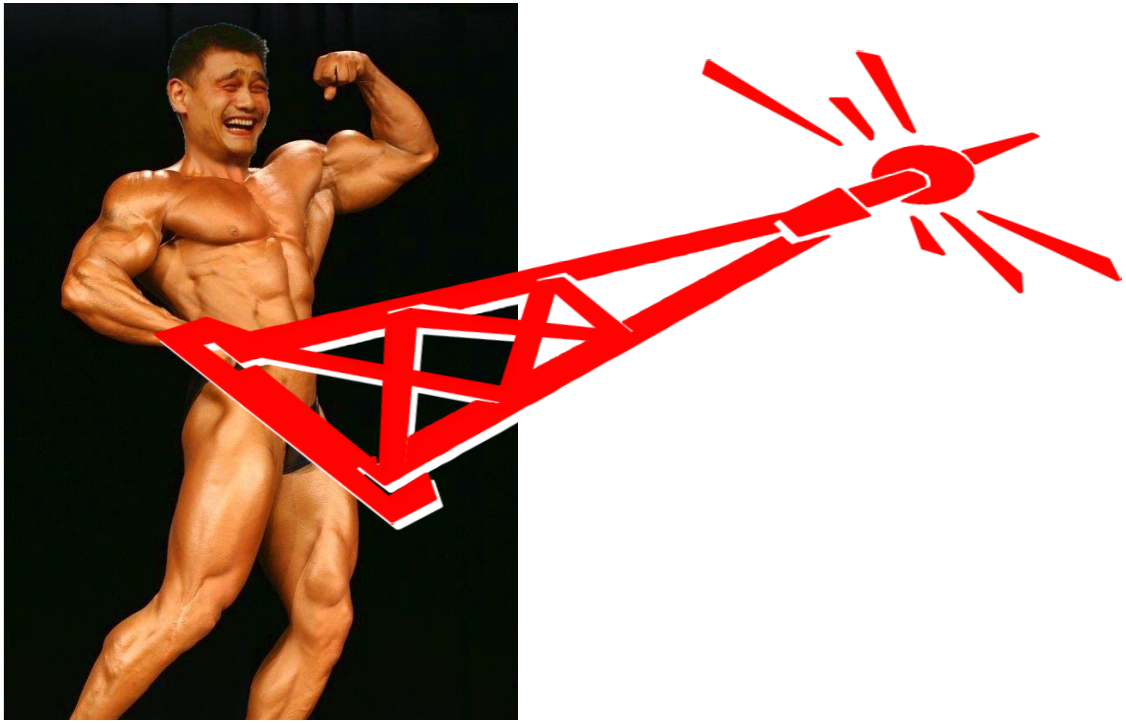
Los terminales percibían la máxima potencia "medible" en GSM a más de 2 km.

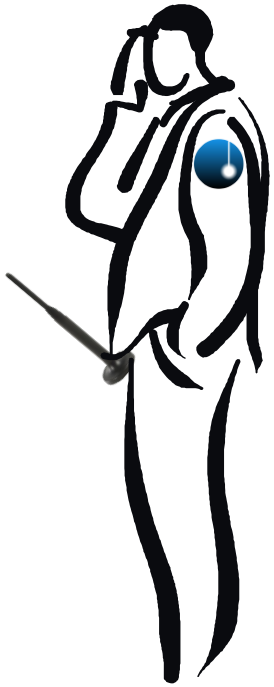
¿A qué potencia deberíamos emitir?

Medidas del operador real vs estación base



La situación era esta





Solución

Solución al problema de la distancia de registro

Explicación técnica

- GSM define un mecanismo para priorizar unas celdas sobre otras (CRO - *Cell Reselection Offset*), de forma que basta con estar entre las 6 celdas que el móvil percibe como más potentes
- No está implementado en OpenBTS 2.6 (se implementa en la emisión en el beacon de los SI3 Rest Octects)

Solución al problema de la distancia de registro

Distancia conseguida

PRECISIÓN CON LA ANTENA DIRECTIVA

La parte directiva del proyecto

- La idea es disponer de un “puntero” que nos indique dónde está el target

La parte directiva del proyecto

- La idea es disponer de un “puntero” que nos indique dónde está el target

Parte directiva del proyecto

"¡Esto lo implemento yo en un par de horas!"

- Usamos los datos de potencia percibida por la estación base para esta funcionalidad: a más potencia, mejor estamos apuntando

Parte directiva del proyecto

Problema y solución

- Problema:
  - Las medidas eran extremadamente inestables y oscilantes
- Explicación
  - GSM regula constantemente la potencia del móvil para que gaste la mínima batería necesaria para llegar a la estación base.
- Solución
  - Implementamos que este mecanismo se detuviese cuando el sistema está en modo direccional

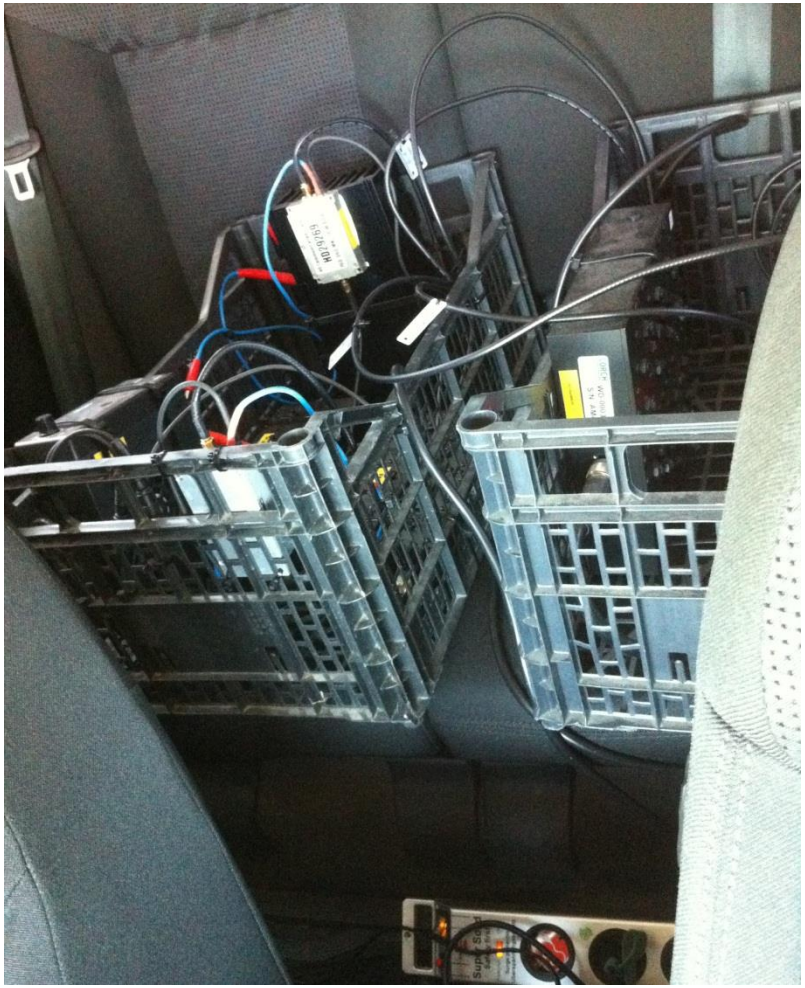
RESULTADO FINAL

Resultado final

El setup HW

Resultado final

El setup HW

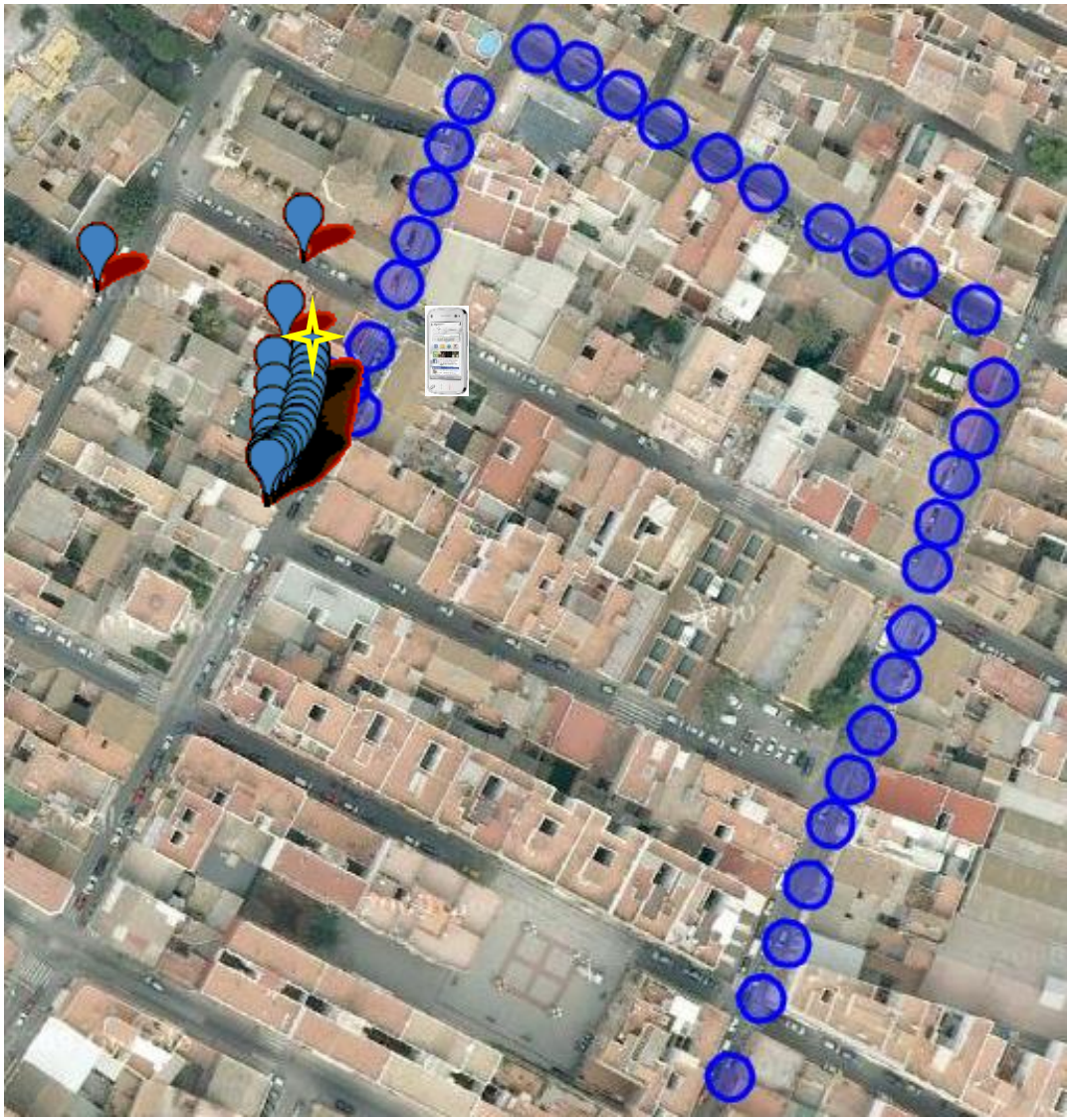


Resultado final

Precisión del sistema omnidireccional en campo abierto

Resultado final

Precisión del sistema omnidireccional en entorno urbano



Resultado final

Demos de funcionamiento de la consola

Videos modo omnidireccional

Video modo direccional

Consola ncurses

Consola iPad

Consola ncurses

Muchas gracias

Taddong

www.taddong.com

@taddong