

Enl@ce: Revista Venezolana de Información,  
Tecnología y Conocimiento  
ISSN: 1690-7515  
Depósito legal pp 200402ZU1624  
Año 12: No. 1, Enero-Abril 2015, pp. 11-22

Cómo citar el artículo (Normas APA):  
Portillo, M., Pirela, G. y Rincón, C. (2014). Algoritmo para geolocalización de dispositivos móviles a partir de emisores de WIFI. *Enl@ce Revista Venezolana de Información, Tecnología y Conocimiento*, 12 (1), 11-22

# Algoritmo para geolocalización de dispositivos móviles a partir de emisores de WIFI

*María E. Portillo Montiel*<sup>1</sup>  
*Gerardo A. Pirela Morillo*<sup>2</sup>  
*Carlos A. Rincón*<sup>3</sup>

## Resumen

Esta investigación propone un método para la geolocalización de dispositivos móviles a partir de señales WiFi predeterminadas, prescindiendo del uso del GPS para evitar potenciales problemas de seguridad y malware. El método propuesto, se basa en la técnica conocida como Punto de Triangulación Aproximado (APIT) y parte de una discretización del espacio de acción a partir de un conjunto base de emisores de señal WiFi de coordenadas y radios de acción máximos conocidos, para luego construir una rejilla que incluye las zonas de acción conjunta de todos los emisores al momento de activar la aplicación, es posible estimar con gran precisión la ubicación del dispositivo móvil determinando el área de intersección de las señales visibles en el momento. La implementación del algoritmo propuesto exhibe una complejidad temporal cuadrática respecto al tamaño de la rejilla y lineal sobre la cantidad de emisores iniciales.

**Palabras clave:** dispositivos móviles, geolocalización, WiFi, punto de triangulación aproximado.

Recibido: 27/10/14 Devuelto para revisión: 9/3/15 Aceptado: 10/3/15.

---

<sup>1</sup> Magíster Scientiarum en Computación. Licenciada en Computación. Docente Agregado. Departamento de Computación, Facultad Experimental de Ciencias, Universidad del Zulia. Correo e-: mariaeportillo@fec.luz.edu.ve

<sup>2</sup> M.Sc. en Ciencias e Ingeniería de la Computación. Licenciado en Computación. Coordinador Académico de la Licenciatura en Computación Facultad Experimental de Ciencias LUZ. Docente Asociado de la Licenciatura en Computación de LUZ. Correo e-: gepirela@fec.luz.edu.ve

<sup>3</sup> Magíster en Telemática (URBE). Licenciado en Computación. Coordinador de la Red Académica de Ciencias de la Facultad Experimental de Ciencias LUZ. Coordinador del Laboratorio de Computación de LICOM. Docente Asociado del Departamento de Computación de LUZ. Correo e-: crincon@fec.luz.edu.ve

# Geolocation Algorithm for mobile devices from issuers of WIFI

## Abstract

This research proposes a method for geolocation of mobile devices from predetermined WiFi signals, regardless of the use of GPS to avoid potential safety problems and malware. The proposed method is based on the technique known as triangulation point Approx (TIPS) and part of a space discretization action from a base set of WiFi signal emitters coordinate and maximum ranges of known and then build a grid that includes the areas of joint action by all emitters when activating the application, can be estimated with high accuracy mobile location determining the area of intersection of the visible signs at the time. The implementation of the proposed algorithm exhibits a quadratic time complexity to the size of the grid and on the amount of linear initial emitters.

**Key words:** Mobile Device, Geolocating, WiFi, Approximate Point-In-Triangulation.

## Introducción

El auge de los dispositivos móviles tipo smartphones es cada día más evidente. Las diversas opciones de conexión provistas en estos han dado paso a la utilización de mayor número de aplicaciones nativas que demandan la accesibilidad a la Internet, en especial aquellas que requieren información acerca de la ubicación geográfica del dispositivo en tiempo real, sin embargo la activación de la conexión GPS de cualquier equipo móvil conlleva serios problemas de seguridad, ante el creciente número de ataques a través de aplicaciones conocidas como “mobile malware” (troyanos, gusanos, spam, spyware, entre otros).

De acuerdo con el informe de la compañía McAfee, correspondiente al segundo trimestre del año 2012, el número de este tipo de ataques

se multiplica a un ritmo cada vez más rápido. La compañía británica Gamma Group, especializada en intrusión de sistemas, durante el año 2012 desarrolló un malware conocido como FinFisher, un troyano que permite el control remoto de dispositivos iOS, Android, Windows Phone, Blackberry y Symbian. Este es instalado al dispositivo, bien sea a través de la web o a través de una falsa notificación de actualización del sistema vía SMS. Una vez instalado, este malware puede controlar y monitorear los dispositivos infectados en forma remota sin importar dónde estén localizados. Entre otras cosas, es capaz de grabar llamadas de voz, mensajes SMS/MMS y correos electrónicos, así como datos de geolocalización (GPS) Marquis, Marczak y Gauenieru, 2012.

A pesar de que para ese momento, las estadísticas de ataques se inclinan considerablemente hacia

el sistema operativo Android, la empresa de seguridad rusa Kaspersky Lab durante el mes de junio de 2012 descubrió un malware disponible en el Apple App Store llamado “Find & Call”. Esta app corresponde a un troyano que carga la libreta de direcciones del dispositivo infectado a un servidor remoto, posteriormente el servidor envía spam a las direcciones de correo electrónico y números de teléfono pertenecientes a los contactos de la víctima para enviarles mensajes SMS contándoles acerca de esta aplicación.

Además, esta app toma las coordenadas GPS desde el dispositivo infectado y la carga en el servidor remoto, con lo cual almacena un historial de su ubicación. Ante tal evidencia, la compañía Apple procedió a la eliminación de la mencionada app del App Store, sin embargo, queda demostrado que ningún sistema operativo está exento de este tipo de ataques.

Por otro lado, a pesar de que la geolocalización basada en GPS resulta confiable y exacta en ambientes externos, esta no ofrece buen desempeño en zonas urbanas y en espacios interiores (Kaushik, 2012). Se requiere, entonces, la implementación de técnicas alternativas al GPS para lograr la geolocalización de dispositivos móviles para el correcto comportamiento del creciente número de aplicaciones dependientes del contexto, de manera segura, confiable y exacta. La ingeniería de software, propone para tales casos varias metodologías adecuadas para satisfacer tal fin. En particular, la metodología de desarrollo en cascada descrita por Pressman (2002), se perfila como adecuada y suficiente con

el fin de llevar a cabo el desarrollo de un algoritmo para la geolocalización de dispositivos móviles a partir de señales WiFi predeterminadas. La metodología indicada, contempla la ejecución ordenada de cuatro fases: análisis, diseño, codificación y pruebas, enmarcados en el alcance de la presente investigación, se realizaron las dos primeras fases, análisis de requisitos y diseño de las estructuras de datos y el algoritmo, las fases de implementación y pruebas han de ser consideradas en el alcance de próximas investigaciones.

### **Definiciones básicas**

Wireless Fidelity (WiFi, por su abreviatura en ingles), es una tecnología de redes de área local tipo wireless que permite la conexión entre computadoras y otros dispositivos a través de una conexión inalámbrica. Está basada en el estándar IEEE 802.11.

Los estándares definidos en la norma IEEE 802.11, son: IEEE 802.11a (5GHz), IEEE 802.11b (2.4GHz), IEEE 802.11n (2.4 y 5GHz). Estos estándares ofrecen velocidades teóricas en el rango de 11 Mbps a 300 Mbps. La banda de los 2.4GHz ofrece un mejor rendimiento pero al ser compartida por otras aplicaciones basadas en radio frecuencia tiende a sufrir de mayor interferencia, mientras que la banda de los 5GHz ofrece un menor rendimiento (considerando la distancia de la señal), pero es menos susceptible a interferencias. Los protocolos de seguridad en redes inalámbricas son consecuencia natural del uso de radiofrecuencia como mecanismos para

transmitir la información. Existen diferentes protocolos como WEP, WPA (PSK – AES), WPA2, entre otros.

## Arquitectura de redes WiFi

Las aplicaciones más comunes de WiFi incluyen conexión a Internet, acceso telefónico de voz sobre IP (VoIP, por sus siglas en inglés), juegos, transferencia de datos entre dispositivos, así como otros beneficios. La arquitectura de las redes WiFi, consiste en un conjunto de puntos para acceder (APs, por sus siglas en inglés) y uno o más clientes. Un cliente es conectado en forma directa a un AP. Un AP, se comunica con el cliente enviando mensajes de difusión a su Identificador de Servicio (SSID, por sus siglas en inglés) o nombre de red enviando paquetes, conocidos como beacons.

El AP, emite su señal en intervalos de duración de 100ms a una velocidad de datos de 1Mbps. La conectividad entre el cliente y el AP, depende básicamente de las características de su SSID, si la configuración de esta no es la correcta la comunicación no será posible. Si existen varios AP con el mismo SSID, el cliente se conectará al AP con mayor potencia de señal. La red WiFi, utiliza radio señales para proveer conectividad a Internet o hacia el operador de red de un dispositivo móvil para tener acceso a los servicios de Internet (Kaushik, 2012).

Las redes inalámbricas locales WLAN, utilizan dispositivos de distribución o de red como enrutadores (Routers), puntos de acceso (Access

Points) y extensores de red (Extenders). Estos dispositivos se encuentran definidos dentro de las tres primeras capas de modelo OSI (Red, Enlace de Datos y Física, respectivamente).

## Ventajas y desventajas de las red WiFi

La principal ventaja de la red WiFi, es que hace posible la interconexión de diversos dispositivos en forma inalámbrica, además permite el acceder a la Internet desde cualquier dispositivo móvil que disponga del servicio de red.

Otra ventaja es que este tipo de redes están estandarizadas, lo cual hace posible conectarse a cualquier punto cuya accesibilidad este disponible en cualquier lugar del mundo, basta con configurar la información de conexión en el dispositivo utilizado para tal fin (laptops, smartphones, tablets, consolas de videojuegos, entre otros). Finalmente, a través de las redes WiFi es posible desplegar una red LAN sin cablear, especialmente en aquellos lugares donde, por condiciones de la edificación o normas establecidas, no es posible la instalación de cables de red.

A pesar de sus múltiples ventajas, existen algunos aspectos negativos en torno a este tipo de redes: su alcance está restringido a un área determinada, entre 10 y 300 metros, ello dependerá, principalmente, de la potencia del *router* utilizado, en algunos casos se precisa la instalación de amplificadores de señal con el fin de obtener mayor cobertura, los puntos para acceder, disponibles en forma gratuita pueden

ser utilizados para robar información personal por parte de usuarios maliciosos de la red WiFi, ello por carecer de configuraciones de seguridad que protejan la información que viaja por la red; dependiendo del tipo de ambiente en el cual opere la red, la intensidad de la señal emitida puede verse afectada, ocasionando problemas de conectividad, finalmente, el consumo de electricidad es bastante alto lo que provoca descarga frecuente de la batería del dispositivo utilizado.

### **Técnicas de geolocalización en redes WiFi**

Roxin y colaboradores, describen en Roxin, Gaber y Wack, 2007, una revisión de las técnicas actuales para la geolocalización de dispositivos conectados a redes inalámbricas. Estas técnicas se clasifican, según su uso de infraestructura (hardware) especializada, en dedicadas y no dedicadas. Las técnicas dedicadas incurren en costos elevados para la adquisición, instalación y mantenimiento del hardware especializado que requieren para su correcto funcionamiento, mientras que las no dedicadas, evaden tales costos, sacrificando marginalmente precisión y exactitud que el hardware especializado ofrecería.

Por su parte, las técnicas no dedicadas se clasifican en 1) probabilísticas y 2) determinísticas. Las primeras técnicas, son más flexibles y resistentes a situaciones de deterioro o pérdida de la señal, ya que se basan en estimaciones de distribuciones estadísticas de dichas señales calculadas en ubicaciones predefinidas, estas no llevan a resultados exactos ni actualizados en tiempo real.

Finalmente, las técnicas no dedicadas, determinísticas se basan en el cálculo preciso de valores escalares denominados fuerza de señal recibida (RSS – según sus siglas en inglés) desde los AP; estos valores se promedian y se asocia con la ubicación del dispositivo que se desea localizar.

Cuatro de estas técnicas son: vecino más cercano en espacio de señal, simple o promediado (NNSS o NNSS-AVG, por sus siglas en inglés), polígono más pequeño y punto de triangulación aproximado (APIT, por sus siglas en inglés). Los primeros tres, requieren cálculos geométricos que involucran distancia euclidiana y centroide de polígonos potencialmente irregulares, los cuales pueden incrementar la complejidad computacional, tanto en la representación en memoria como en tiempo de ejecución. La técnica APIT, evita tal costo discretizando el espacio de acción de todos los AP conocidos, lo cual conlleva a un mejor aprovechamiento de los recursos de los dispositivos móviles donde correría.

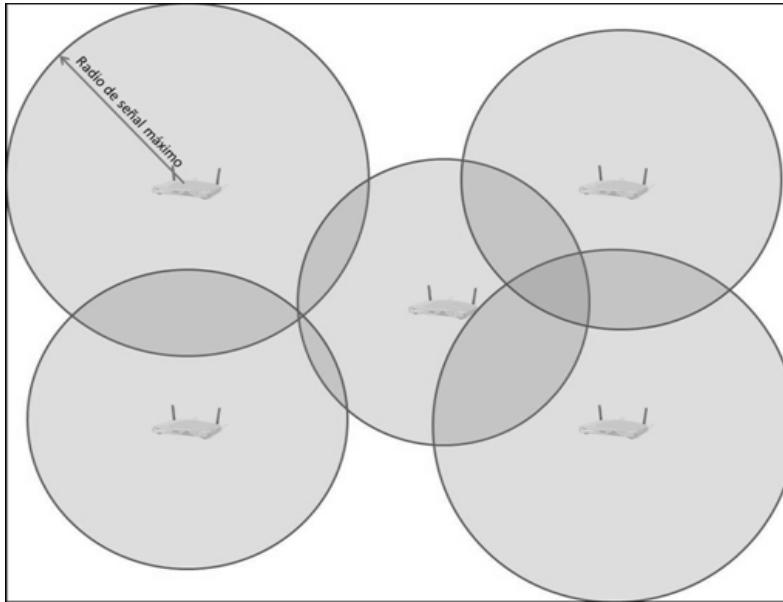
### **Método propuesto**

Para lograr estimar la geolocalización de un dispositivo móvil, se propone un método que adapta la técnica de Punto en Triangulación Aproximado (APIT – por sus siglas en inglés), descrita en Roxin, Gaber y Wack, 2007. Esta técnica inicia con una discretización del espacio de acción a partir de un conjunto base de emisores de señal WiFi (e.g., routers), denominados “anclas”. Conociendo las coordenadas de las N anclas iniciales, así como del radio máximo de acción de estas anclas, se puede construir una

teselación (o rejilla) que incluya por completo las zonas de acción conjunta de todas las  $N$  anclas. La figura 1, muestra cinco AP ubicadas en un espacio continuo, las cuales usadas como anclas, pueden

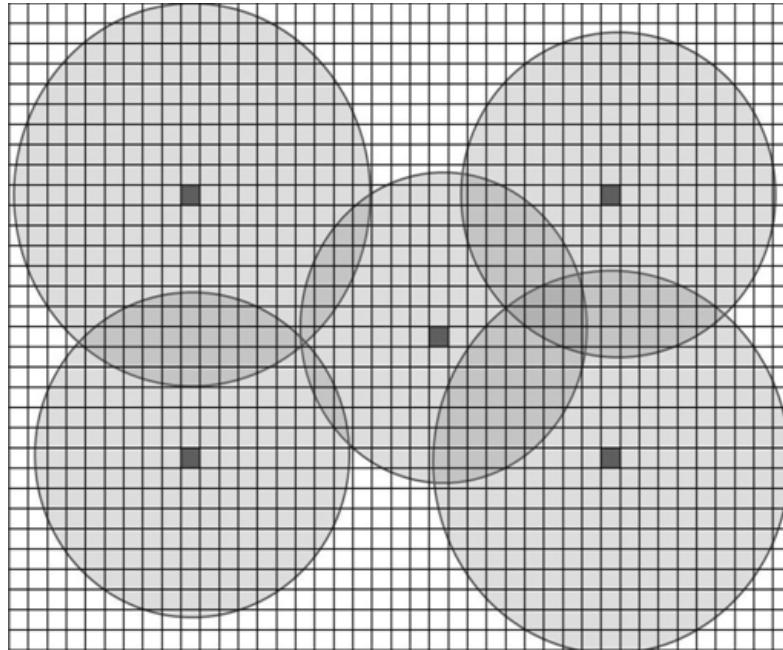
resultar en la rejilla que se muestra en la figura 2. Esta rejilla, representará una discretización en celdas del espacio total a ser considerado por el método propuesto.

**Figura 1**  
**Ejemplo de cinco AP usados como anclas**



Fuente: elaboración propia, (2014).

**Figura 2**  
**Teselación resultante.**

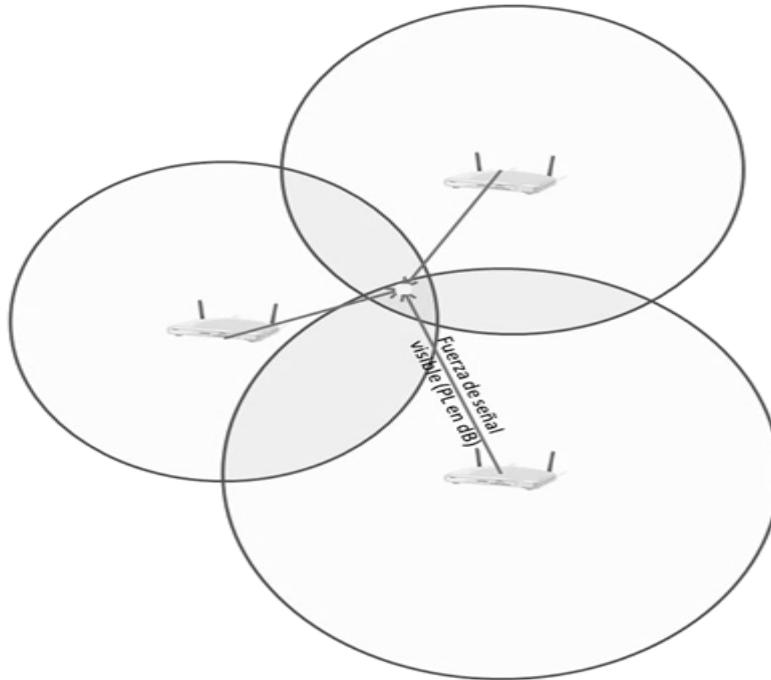


Fuente: elaboración propia, (2014).

La aplicación del método propuesto tomará del dispositivo móvil donde se ejecutará la lista de redes (o anclas) visibles y la fuerza de la señal de cada red visible en el momento de activación de la aplicación. De esta lista, se identificará el subconjunto de  $k$  anclas visibles y sus respectivas fuerzas de señal en el momento, medidas en  $dB$ . Dado que se conoce la celda exacta en la rejilla

desde donde se emite la señal de cada ancla, se puede calcular, a partir de la fuerza de la señal en  $dB$ , el radio de acción, en  $mts.$ , de cada ancla visible. La figura 3, muestra un ejemplo en el que el dispositivo móvil (señalado en amarillo) sólo visualiza tres de las cinco anclas originales, con sus respectivas fuerzas atenuadas (medidas en  $dB$ ).

**Figura 3**  
**Un dispositivo móvil detecta sólo tres de las anclas originales y sus respectivas señales atenuadas**



Fuente: elaboración propia, (2014).

Con esta información se etiquetan las celdas que sean cubiertas por cada radio de acción visible, de tal manera que cada celda quedará etiquetada con un número entre cero y el número de anclas visibles, dependiendo de la cantidad de estas, en el momento cuyos radios de acción se intersequen

en la prenombrada celda. El área probable de ubicación del dispositivo al momento de activar la aplicación corresponderá al conjunto de celdas de la rejilla con el mayor valor de etiqueta, como lo muestra la figura 4.



granularidad y exactitud en los resultados del método propuesto, a costa de un aumento polinomial de la complejidad computacional del mismo, tal como se describe en la sección siguiente.

## Descripción del algoritmo

Sea  $A$  el conjunto de anclas iniciales, con  $|A|=N$ . Conociendo la ubicación y el radio de acción máximo de cada ancla, se calcula la rejilla de  $f$  (filas)  $\times$   $c$  (columnas) celdas, de geometría cuadrada, con lado constante. Esta rejilla se calcula sobre un área rectangular ajustada para que incluya todos los círculos de acción de las anclas iniciales, asumiendo potencia máxima de señal en cada una.

Ahora, sea  $VIA$  el subconjunto de anclas visibles al momento de activar la aplicación; con  $|V|=k$ . “ $n_i \in V$ , denominemos  $l_i$ =fuerza de señal de  $n_i$  (en dB) y  $s_i$ =radio de acción de  $n_i$  (en mts.). Con cada  $s_i$  es posible calcular el conjunto de celdas  $C_i$  cubiertas por la señal emitida por el  $n_i$  respectivo, dada la celda donde este se encuentra.

Del dispositivo móvil se obtendrá cada  $l_i$  (en dB), que corresponde a la Pérdida de Camino (PL – por sus siglas en inglés) referida en Netgate, 2013, donde se describe un modelo común para relacionar PL con la distancia,  $D$  ( $s_i$ , en mts.), del dispositivo receptor a la fuente, para emisores de señal WiFi a 2.4GHz. Dicha fórmula se describe debajo:

$$PL = 41dB + n*10*\log(D)$$

Con valores para  $n=2$ , para espacios abiertos;  $n=3.3$ , para espacios abiertos de oficinas; y  $n=4.5$  para espacios domésticos (e.g., casas). La relación entre  $s_i$  y  $l_i$  se calcula, entonces, como sigue:

$$s_i = 10^{(l_i - 41dB)/10n}$$

El seudocódigo del método propuesto, sería como se muestra a continuación:

```
01 Inicializar todas las celdas de la rejilla en 0
02 "n, V
03 { C_i = Conjunto de celdas dentro de s_i
04 "t, C_i
05 t.etiqueta++
06 }
07 P = Conjunto de celdas con mayor etiqueta
08 Return P
```

La complejidad computacional del método propuesto dependerá directamente del radio de acción máximo de las anclas iniciales, la cantidad total de estas anclas iniciales y el tamaño de las celdas de la rejilla, otros factores que influirán en esta complejidad serán los métodos usados para obtener el conjunto de celdas dentro de  $s_i$ . En cualquier caso, se puede construir un algoritmo de complejidad temporal polinomial, con grado máximo cuadrático respecto al tamaño de la rejilla y lineal sobre la cantidad de anclas iniciales.

Finalmente, se presumirá que los dispositivos que emitirán la señal tendrán una zona de acción esférica, la cual será proyectada en 2D (es decir, se considerará regiones de acción circulares) y se despreciará momentáneamente aspectos de geometría y construcción física del espacio

real (i.e., muros, paredes y otros elementos que afecten la fuerza de la señal). Se escoge una geometría de celdas cuadradas para simplificar la aproximación. Debido a que del tamaño de estas celdas depende el tamaño final de la rejilla y, por ende, la complejidad temporal del algoritmo, dicho valor de tamaño será determinado durante la fase de pruebas del método una vez implementado. Durante esta fase de prueba también se determinará el mejor valor de  $n$  para el cálculo de los  $s_i$ . Se espera que, una vez implementado el método propuesto, las pruebas de rigor determinen exactamente el impacto de estos elementos en la efectividad y eficiencia de la aplicación.

## Conclusiones

La información de geolocalización de un dispositivo móvil basada en GPS, trae como consecuencia el aumento del riesgo informático del usuario, así como el incremento en el consumo de energía. En este documento se describió un algoritmo de complejidad computacional baja a moderada (polinomial, cuadrática) para la geolocalización de dispositivos móviles, usando solamente las señales WiFi disponibles, prescindiendo del uso de GPS, el cual no ofrece suficiente confiabilidad y precisión en zonas urbanas y espacios interiores.

La implementación del algoritmo propuesto permitirá conocer de manera segura, confiable y exacta la ubicación de un dispositivo móvil en espacios interiores y dentro del rango cubierto por las señales de emisores de WiFi configurables

en el sistema, de tal manera que se satisfacen las necesidades de ubicación que presentan las crecientes aplicaciones ubicuas, dependientes del contexto, orientadas a dispositivos móviles inteligentes. El uso de la técnica particular en la que se basa el algoritmo (APIT) ofrece mayor precisión que otras técnicas de geolocalización sin GPS, además de que evita la necesidad de instalar hardware dedicado.

En próximas investigaciones se implementará el método propuesto en dispositivos basados en sistema Android, con la finalidad de probar su efectividad para el proceso de geolocalización. De obtener resultados positivos, se desarrollarán sistemas para plataforma Android que, utilizando la geolocalización, permitan un mayor grado de automatización de los procesos.

## Referencias bibliográficas

- Kaushik, S. (2012) An overview of technical aspect for wifi networks technology. *Ijcesc*, 28-34.
- Marquis-Boire, M., Marczak, B. y Gauenieru, C. (2012) The smartphone who loved me: finfisher goes mobile?" [en línea], research brief number, the citizen lab, university of Toronto. Recuperado el 9 de febrero del 2013 de <https://citizenlab.org/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile>
- Netgate (2013). Primer on wifi range. *Rubicon communications* Recuperado el 15 enero

2013 de [http://www.netgate.com/info/antennas/tutorial\\_on%20link\\_budgets.pdf](http://www.netgate.com/info/antennas/tutorial_on%20link_budgets.pdf)

Pressman, R. S. (2002) *Ingeniería del software: un enfoque práctico*. España: McGraw-Hill.

Roxin, A., Gaber, J. y Wack, M. (2007). Survey of wireless geolocation techniques, globecom workshops, 1-9, 26-30.