Sistemas & Telemática
ISSN: 1692-5238
EditorSyT@icesi.edu.co
Universidad ICESI
Colombia

Morales Rodriguez, Madelayne; Acosta Escobar, Juan Camilo; Díaz Ramírez, Juan David; Cortés Tobar, Darío Fernando

Sistema de localización agresor-victima en ambientes indoor y outdoor

Sistemas & Telemática, vol. 10, núm. 23, octubre-diciembre, 2012, pp. 51-63
Universidad ICESI
Cali, Colombia

Disponible en: http://www.redalyc.org/articulo.oa?id=411534391002

Citación: Morales, M., Acosta, J., Díaz, J. & Cortés, D. (2012). Sistema de localización agresor-victima en ambientes indoor y outdoor. *Revista S&T, 10*(23), 51-63

Artículo original

Sistema de localización agresor-victima en ambientes indoor y outdoor

Victim-Attacker monitoring system at indoor and outdoor environments

Madelayne Morales Rodriguez
mmorales@ieee.org

Juan Camilo Acosta Escobar
Jcamilo16@hotmail.com

Juan David Díaz Ramírez
juandaviddelavega@gmail.com
Universidad Icesi, Cali (Colombia)

Darío Fernando Cortés Tobar
dacortes00@hotmail.com
Universidad de Sevilla (España)

Fecha de recepción: Septiembre 30 de 2012
Fecha de aceptación: Octubre 15 de 2012

Palabras clave
Monitoreo de prisioneros; plataforma de monitoreo; vigilancia electrónica.

Keywords
Monitoring prisoners; monitoring platform; electronic surveillance

Colciencias tipo 1

Resumen

Los métodos de vigilancia electrónica de los condenados que gozan de detención domiciliaria o movilidad restringida están diseñados para permitir una rápida localización del reo. En algunos casos, como el de la agresión física, esto no es suficiente. El sistema debería garantizar a la victima que su agresor se mantiene a una distancia prudente y así ofrecerle tranquilidad. Este proyecto reconoce las limitaciones propias de los actuales sistemas de monitoreo basados en GPS (al igual que sus bondades) y diseña una plataforma de monitoreo y comunicaciones que, a partir de la combinación de tecnologías de comunicación, es capaz de interactuar con dispositivos móviles comerciales en entornos cerrados y abiertos, e informar a las víctimas –y a las autoridades– sobre eventuales violaciones a los acuerdos de distancia agresor-víctima. Las pruebas del sistema muestran que la solución es factible. Sin embargo, su aplicación en la vida real pasa por un cambio en el paradigma en el sistema judicial, para que el monitoreo no se centre en evitar la fuga, sino en proteger a la víctima, y en la mejora del tiempo de retardo en la transmisión de SMS en Colombia.

Abstract

The actual methods of electronic surveillance of the convicted in home detention (or with restricted mobility) are designed for allowing his/her fast localization. Some cases, as physical aggression, this is not enough. The system should be able to provide calm and avoid concerns to the victim, assuring that him/her attacker keeps in a safe distance. This project recognizes advantages and limitations on actual surveillance systems based on GPS; it designs a platform of surveillance and communications combining communication's technologies in a way where the platform is able to interact with commercial mobile devices at indoor and outdoor scenarios and, the key issue, it's able to inform the victim and relevant authorities about violations to agreements about distance aggressor-victim. The tests of the system show is a feasible solutions. However, its application requires both, changes in the judicial system about surveillance of the sentenced in home detention (recognizing the main objective is not prevent the fuge, but keep safe the victims), and improving the delay time in SMS traffic in Colombia.

I. Introducción

Los métodos de vigilancia electrónica son una alternativa a la prisión y a la detención domiciliaria. Ofrecen ventajas tanto para el reo como para el sistema judicial. Las del primero son sociales: la no exposición del reo a un ambiente carcelario y la posibilidad de continuar con sus actividades cotidianas, deberían aportar a su resocialización, el fin último del sistema. Las del segundo, son de orden práctico: las personas que cumplen su condena bajo esta modalidad representan menores costos de manutención y no profundizan los problemas de hacinamiento carcelario.

Evitar la fuga es el concepto que rige el diseño de los dispositivos electrónicos de monitoreo actuales. Por tanto, está basado en el uso de una manilla permanente, no removible, que permite la localización precisa del individuo a partir de tecnología GPS, una tecnología que, a pesar de sus limitaciones para operar en ambientes *indoor*, cumple con su propósito fundamental: permitir la ubicación del individuo en cualquier momento.

El maltrato y el abuso entran en la categoría de crímenes excarcelables, por lo que es usual que la condena o parte de ella se cumpla bajo esta modalidad, es decir por fuera de un establecimiento carcelario pero con el compromiso del agresor de no abandonar determinado perímetro y guardar cierta distancia con el agredido. El sistema de manilla actual, si bien permite el monitoreo y la ubicación inmediata del reo mediante la utilización de un GPS, no puede garantizar que las restricciones de distancia se cumplen ni monitorear la movilidad del reo en ambientes *indoor*. Estas limitaciones crean una paradoja tremenda: mientras el agresor goza de libertad y una vida relativamente normal, la víctima vive intranquila, pues queda desprotegida, con motivos para sentirse amenazada, vulnerable. Independiente del comportamiento del agresor, la vida de la víctima no es normal, pues no sabe a ciencia cierta, si su agresor cumplirá con sus compromisos de distancia o si por el contrario, aprovechará la situación para repetir la agresión.

Este proyecto no pretende ahondar en las cuestiones sociológicas de la situación planteada sino aportar a la seguridad y, sobre todo, a la percepción de seguridad de las personas que han sido víctimas de algún tipo de maltrato o abuso, a través de un instrumento tecnológico que les permita, primero, conocer, con absoluta precisión si su agresor respeta la distancia pactada, y segundo, de no ser así, les ofrece la posibilidad de activar una alerta que evite su agresión. Técnicamente hablando el proyecto propone diseñar y desarrollar una plataforma de monitorización y comunicaciones capaz de interactuar con dispositivos móviles comerciales en entornos *indoor* y *outdoor*, capaz de informar a las victimas sobre la presencia de su agresor.

La plataforma desarrollada combina tecnologías de comunicación (i.e gps, gprs, bluetooth). Su diseño parte de un cambio en el paradigma del sistema judicial: en lugar

de centrarse en la ubicación física del agresor, para evitar su fuga, usar la ubicación del agresor y su víctima, para garantizar que la distancia entre ellos se mantiene y que, en consecuencia, la agresión no se repite.

II. Método

El objetivo general del proyecto fue diseñar y desarrollar una plataforma de monitorización y comunicaciones que le informe a la victima la proximidad su agresor. Como objetivos intermedios se plantearon: investigar los protocolos de comunicación más apropiados para usar en ambientes *indoor* y *outdoor*; programar un dispositivo que permita la identificación de las víctimas y agresores que pasan por un determinado punto; desarrollar una aplicación móvil para dispositivos comerciales que reporte información necesaria para la plataforma de localización; y diseñar un sistema de seguimiento y control de los dispositivos de la víctima y agresor que guarde registro de las víctimas con su respectivo agresor y su posición actual.

Como se muestra en la Figura 1, el sistema de localización cuenta con tres tipos de dispositivos móviles, el de la víctima, el del agresor y el faro, y dos servidores, un servidor web y un servidor encargado de la recepción de la información de los faros y de los dispositivos móviles. Para la garantía de funcionamiento del sistema el dispositivo del agresor cuenta con tecnología Bluetooth, GPS y acceso a la red de datos GPRS, y no es removible, el dispositivo de la víctima es un celular que cuenta con tecnología Bluetooth, GPS y acceso a redes de datos GPRS; y el faro cuenta con un módulo Bluetooth y conexión Ethernet.

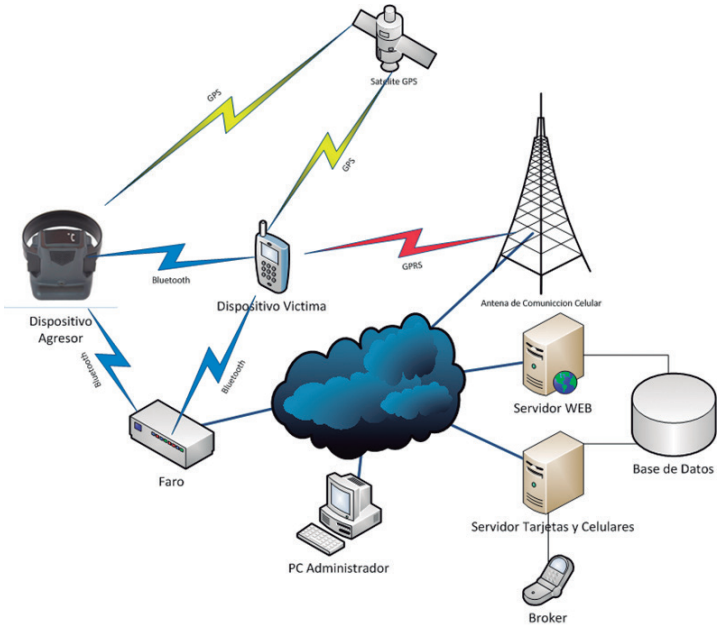

Figura 1. Esquema General del sistema

Se seleccionaron dispositivos móviles con tecnología Android porque: por su precio, son de fácil acceso; permiten el desarrollo de aplicaciones gracias a las librerías y soporte con el que cuenta; su tecnología viene en crecimiento, y está presente en la mayoría de teléfonos inteligentes (Lyons, 2012).

Para el faro se utilizó una tarjeta Beagleboard XM, escogida básicamente por su tamaño y capacidad de procesamiento, además de su facilidad para la integración con accesorios que permiten la conexión Bluetooth, Wi-fi y Ethernet (BeagleBoard.org, 2011). Para la configuración del embebido se tuvieron en cuenta los siguientes puntos:

A. Boot de la Beagle Board XM

Se presentaron inconvenientes con el inicio de la Beagle (booting de la tarjeta) que hicieron además evidente la poca disponibilidad de información disponible al respecto (por tratarse de un embebido nuevo en el mercado). Se optó por conseguir el conector DC que no viene incluido en la tarjeta, con lo que se solucionó el problema (Acosta, Díaz, & Morales, 2011).

B. Instalación del SO

Para la elección del Sistema Operativo se optó por de las distribuciones de Linux, por su GNU GPL, que permite libertad en la modificación y distribución del software. El SO Maverick 10.10 cuenta con una interfaz grafica muy intuitiva y fácil de programar, además de que los requerimientos de hardware que exige se adaptaban a la perfección con las características de la técnicas de la tarjeta (Ubuntu, 2011).

C. Script

La configuración de los módulos Bluetooth (plug and play) fue muy sencilla. Para su detección por parte del embebido, se uso un Bash Script, que hace un *script* en Linux que escanea los dispositivos Bluetooth y manda la información por un flujo de datos al servidor. A continuación se muestra el código del *script* (Usemos Linux, 2010):

```
while[1]
do
echo dispositivo>log.txt
echo 3.341638, -76.528852 >>log.txt
hcitool scan|grep :>>log.txt
echo exit>> log.txt
nc 192.168.0.2 12345 < log.txt
sleep 30
done
```

Como se mencionó, el sistema cuenta con dos servidores. Un servidor WEB que se encarga de la gestión de los usuarios y las relaciones; y el servidor de la tarjeta-celular que recibe la información de ellos y la persiste en la base de datos. Ambos servidores apuntan a una misma base de datos hecha en MySQL.

La interfaz WEB se hace a través de unas nuevas librerías Ajax llamadas ICEfaces. La persistencia se hace con ayuda de Hibernate que es una tecnología que utiliza Java para lograr mapeo objeto/relacional. Este tema se trata con mayor profundidad en la tesis, a la cual se puede referir (Acosta et al., 2011).

El sistema permite la identificación de la posición en todo momento de los dispositivos involucrados, en este caso los del agresor y la víctima.

Se ha hablado un poco del papel de cada actor del sistema por separado, sin embargo no se ha mencionado en detalle los requerimiento de conexión del sistema que permiten su interacción. El enfoque del proyecto está en la capa de aplicación. Siempre estuvo enfocado en buscar la forma correcta para que interactuaran las diferentes tecnologías, debido a que se encontraba en una capa del modelo OSI superior, nunca hubo que entrar en la parte baja del código, e interpretación de las tramas de las mismas, e identificación de cabeceras, todo resulto muy natural e intuitivo, gracias a la utilización de las tecnologías que fueron escogidas como solución a la propuesta de sistema planteada en el proyecto.

Por ejemplo, para conectar el faro con el servidor, se envía por un puerto al servidor un archivo plano que se va escribiendo a medida que el faro hace lecturas; este archivo plano es interpretado por el servidor, de acuerdo a unas especificaciones y pruebas que se hicieron para observar cómo obtiene el faro la Dir. MAC del dispositivo móvil. Después de esto, es sencillo manejar la información. De igual manera con lectura de coordenadas que se hace por parte del servidor y del dispositivo móvil, cuando recibe la información dada por el GPS. La Tabla 1 resume la elección de aspectos técnicos para el funcionamiento del sistema.

Tabla 1. Especificaciones de SO y Lenguaje de Programación

Dispositivo	**SO**	**Lenguaje de Programación**
Faro	Ubuntu Maverick 10.10	Bash script
Servidor WEB	Windows 7	JSF
Servidor Aplicación	Windows 7	Java
Aplicación Móvil	Android	Java Android

III. Descripción de la aplicación

El funcionamiento interno del sistema se explica a partir de un ejemplo que supone la existencia de una orden de caución que prohíbe al agresor acercarse a menos de 500 metros a la víctima.

Al agresor se le asigna un dispositivo no removible y a la victima un teléfono celular con el software del sistema. Se ingresan los datos de las dos personas al sistema a través de la página WEB del sistema de localización. Crear individuos y relaciones requiere privilegios de administrador del sistema, con usuario y contraseña. Después de crear a

los dos individuos se establece la relación agresor-víctima, su distancia máxima legal y se asigna un administrador de caso, quien puede tener o no permiso para editar relaciones y crear de personas, nivel de acceso que se establece dependiendo del rol de la persona. Un policía normal, por ejemplo, no debería poder agregar personas al sistema, pero si podría ser responsable de actuar en el caso que haya violación de términos, en su caso asignado. En todo momento se tiene un registro en la base de datos de la última localización disponible de cualquiera de los dos individuos. En el caso que esté al aire libre, el celular o dispositivo del agresor envía un mensaje por internet celular cada minuto dando su posición, la cual obtiene del modulo GPS en su dispositivo, este mensaje TCP llega al servidor celular-tarjeta que se encarga de actualizar su posición en la base de datos. Para el caso de ambientes indoor existen dos posibilidades, dependiendo de la presencia en el sitio de un faro del sistema.

» Si el lugar al que entra, por ejemplo un centro comercial, cuenta con un faro, éste escanea por Bluetooth los dispositivos cercanos cada 20 segundos – el intervalo mínimo de tiempo en el que realiza el escaneo sin sacar los datos de su memoria caché– y envía su ubicación mediante un mensaje TCP al *Servidor tarjetas – celulares*, donde se actualiza también su posición. Pruebas de campo desarrolladas por el grupo investigador determinaron que en estos 20 segundos se puede detectar hasta una persona moviéndose a una velocidad de 2.6 m/s, a una distancia máxima de 20 metros a través de un muro de 60 cm. de espesor.

» Si el lugar al que entra no cuenta con un faro, el mecanismo de alerta en vigía sería el Bluetooth, él escanearía los dispositivos a su alrededor y enviaría los datos por GPRS al *Servidor celular-tarjeta* que procesaría la información. Según pruebas realizadas por el equipo investigador, estos dispositivos se identifican *entre ellos* hasta a sesenta metros de distancia en ambientes indoor sin obstáculos entre ellos.

Conocer la posición de los dispositivos en todo momento, garantiza poder calcular de manera permanente la distancia entre ellos y permite que al ser esta distancia menor a la determinada en la configuración del caso, se disparen las alertas en el sistema. Ellas se manifiestan inicialmente con el envío de un mensaje de texto a la victima indicándole la presencia de su agresor y, en el caso de que esta situación se repita un número determinado de veces o que la proximidad aumente a un nivel considerado excesivo (e.g. 60 metros o menos), se envía un mensaje de texto al administración del caso quien se encargará de tomar las acciones que considera adecuadas (i.e. contactar a la víctima, al agresor o a la policía local o ir directamente al lugar de los hechos).

a) Requerimientos

Para el desarrollo del sistema se plantearon como requerimientos funcionales que el sistema debe: permitir gestionar personas, entendiendo esto como la posibilidad de ingresar personas al sistema, eliminarlas, editarlas; permitir gestionar relaciones de personas, dándole al administrador de la relación la posibilidad de realizar los ajustes y monitorear las relaciones registradas en el sistema; permitir a la victima saber

cuando este cerca su agresor, que es uno de sus principales focos y objetivos; y debe permitir enviar una notificación a la policía y a la victima de la violación de los términos establecidos, siempre que sea necesario y cuando así lo determine el administrador de la relación.

Como requerimientos no funcionales, el sistema: requiere el uso de un sistema embebido de 10cm x 12 cm; debe manejar un tiempo de latencia pequeño, debido a la actualidad de sus datos es un factor determinante de la confiabilidad de la aplicación; debe permitir la persistencia de los datos en el sistema; y debe estar en funcionamiento permanente (7x 24).

b) Programación del Servidor WEB

Tomando en consideración que para el desarrollo del servidor se usaron tecnologías ICEFaces (Icesoft, 2012) e Hibernate (King, Bauer, Bernard, & Ebersole, 2012), para la programación del servidor se usó como IDE de programación *MyEclipse*, debido a que brinda soporte para ambas. Adicionalmente como servidor de aplicaciones se utilizo JBoss porque su acoplamiento con el lenguaje de programación Java permite la interoperabilidad en cualquier SO. Además, es confiable porque ese trata de un producto de licencia de código abierto sin costo adicional, cumple con los estándares de calidad, es confiable a nivel de empresa, es incrustable y orientado a arquitectura de servicios, tiene flexibilidad consistente, ofrece servicios del middleware para cualquier objeto Java y brinda un soporte completo para JMX.

Como se mencionó, para el desarrollo del servidor se usó Hibernate, una tecnología de vital importancia en el proyecto, debido al volumen de la información, Hibernate permite garantizar la persistencia de los objetos, realizando el mapeo de las clases de Java en tablas de BD. Otro aspecto importante en el desarrollo del servidor fue el uso de la tecnología ICEfaces, que hereda la simplicidad de desarrollo y el alcance del conjunto de características de los JSF y proporciona al programador la eficiencia y expansión del espectro de las capacidades de RIA que pueden ser incluidas en cualquier aplicación WEB basada en JSF.

c) Programación del Servidor de la aplicación

Servidor de la aplicación se refiere al que se encarga de toda la parte de gestión de la información que proviene de la tarjeta y del dispositivo móvil. Adicionalmente es el que tiene mayor relación con la base de datos. A pesar de que el servidor Web también realiza operaciones en la base de datos, no lo hace de manera directa, como es el caso de este servidor.

La Figura 2 presenta el modelo de relación de la base de datos e incluye las tablas presentes en ella.

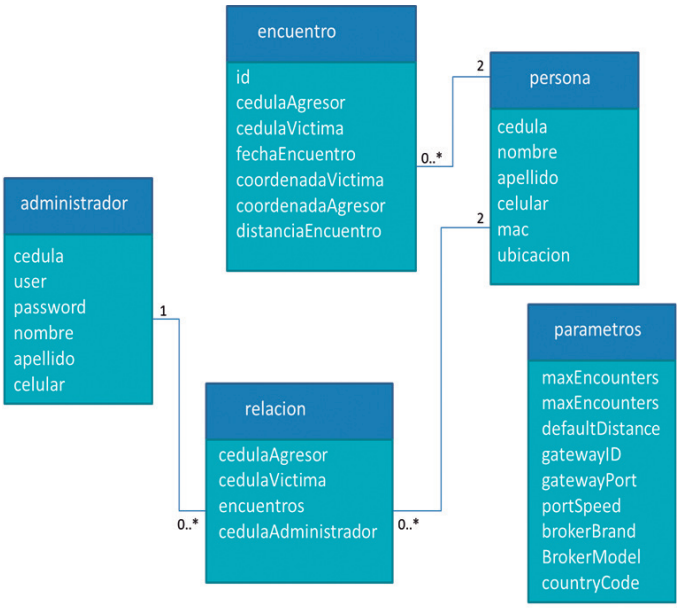

Figura 2. Modelo entidad relación de la base de datos

IV. Resultados experimentales

Para comprobar el funcionamiento de la aplicación se desarrollaron una serie de pruebas que buscaban determinar la confiabilidad de la aplicación, entre ellas se encuentran: prueba de distancia máxima de reconocimiento entre dos celulares haciendo uso del Bluetooth, prueba de distancia máxima de reconocimiento entre el faro y el celular, prueba de velocidad máxima que se puede alcanzar por una persona sin ser detectada por el faro, prueba de duración de la batería del celular con la aplicación corriendo, prueba del aumento en el número de encuentros cuando ocurre un evento, prueba de actualización de la posición por celular y por el faro en la base de datos y prueba de recepción de mensajes por detección del agresor por la tarjeta, el GPS y Bluetooth.

La tabla 2 resume los resultados alcanzados en las pruebas realizadas.

Tabla 2. Resumen de pruebas experimentales del sistema

Prueba	Detalle	Observaciones
Reconocimiento entre dos celulares Bluetooth	Descripción	Prueba para determinar la distancia máxima de reconocimiento Bluetooth entre dos celulares. La prueba se realizo en un ambiente cerrado, sin obstáculos.
	Resultados Esperados	Reconocimiento a una distancia máxima de treinta metros.
	Resultados Obtenidos	La distancia de reconocimiento Bluetooth es bastante grande, comparada con lo que se esperaba de 65 metros.
	Conclusiones	La distancia máxima a la que el dispositivo celular de la víctima y el brazalete agresor podrían identificarse en un ambiente cerrado, sin obstáculos entre ellos, estaría alrededor de 60 metros.
Distancia Máxima de reconocimiento Faro – Celular	Descripción	Prueba para determinar la distancia máxima en la que el faro identifica la dirección MAC del dispositivo Bluetooth.
	Resultados Esperados	Detección a no menos de cinco metros.
	Resultados Obtenidos	La distancia de reconocimiento a alrededor de veinticinco metros, muy superior a lo esperado.
	Conclusiones	La distancia máxima en la que el faro alcanza a detectar un dispositivo Bluetooth y registrar su MAC es veinticinco metros en un ambiente cerrado con una pared de 60 cm de espesor entre el faro y el dispositivo. Esto indica que en un lugar sin obstáculos, como la entrada de un centro comercial, esta distancia aumentaría notablemente.
Velocidad para caminar sin ser detectado por el Faro	Descripción	Prueba para determinar la velocidad máxima a la que se puede caminar sin ser detectado por el faro.
	Resultados Esperados	Que una persona caminando a una velocidad promedio alta pudiera ser detectada por el faro.
	Resultados Obtenidos	La velocidad a la que no se detecta una persona que pasa por el faro es a unos 2,5 m/s (9km/h).
	Conclusiones	El agresor o la victima tendrían que pasar corriendo muy rápido por el faro para no ser detectadas por este, lo que despertaría sospechas y sería contraproducente para el agresor en caso que busque acceder a su víctima.
Duración de la batería del celular con la aplicación ejecutándose	Descripción	Prueba para determinar el tiempo que demora la aplicación en consumir la batería del teléfono, al estar un 100% del tiempo activa, sin otras funciones activadas.
	Resultados Esperados	Consumo de la total de la batería en aproximadamente 18 horas.

Tabla 2. Resumen de pruebas experimentales del sistema (cont.)

Prueba	Detalle	Observaciones
Duración de la batería del celular con la aplicación ejecutándose	Resultados Obtenidos	La batería se consumió totalmente en aproximadamente 24 horas.
	Conclusiones	El consumo de batería del celular no es un impedimento para la implementación de la plataforma, se puede notar
Aumento de encuentros cuando sucede un evento	Descripción	Prueba para determinar si al tener encuentros casuales victima- agresor, el contador de encuentros se incrementa.
	Resultados Esperados	Que se aumente en cada uno de los casos el contador de encuentros.
	Resultados Obtenidos	Los esperados.
	Conclusiones	Cada vez que ocurre un encuentro efectivamente aumenta el contador de encuentros de la relación.
Actualización de la posición por el celular en la base de datos	Descripción	Prueba para determinar si al cambiar de posición el celular por GPS, el cambio se actualiza en la base de datos.
	Resultados Esperados	Que se actualice la posición en la base de datos cuando este al aire libre pero no en espacios cerrados.
	Resultados Obtenidos	En una ocasión se actualizo la posición dentro de un ambiente cerrado. Una vez no se actualizo en ambiente cerrado. Las otras dos veces si se actualizó al aire libre.
	Conclusiones	El GPS en ciertas ocasiones y dependiendo de las características del ambiente cerrado, puede funcionar correctamente. La aplicación funciona correctamente en este aspecto.
Actualización de la posición por la tarjeta en la BD	Descripción	Prueba para determinar si al detectar la posición del celular por el faro, esta se actualiza en la BD.
	Resultados Esperados	Que se actualice correctamente en todo intento la posición al ser detectado el dispositivo por el faro.
	Resultados Obtenidos	Los esperados.
	Conclusiones	Esta parte de la plataforma funciona de acuerdo a lo proyectado.
Recepción de mensaje por detección del agresor por GPS	Descripción	Prueba para determinar si al detectar al agresor por GPS se le está enviando la notificación a la victima
	Resultados Esperados	Que el mensaje de texto llegue inmediatamente se del encuentro.
	Resultados Obtenidos	Por el tipo de dispositivos que se utiliza (bróker) el mensaje de texto tiene un retraso de hasta treinta segundos..

Tabla 2. Resumen de pruebas experimentales del sistema (cont.)

Prueba	Detalle	Observaciones
Recepción de mensaje por detección del agresor por GPS	Conclusiones	Este tiempo de retardo podría ser mejorado con un dispositivo diseñado especialmente para el envío de mensajes de texto.
Recepción de mensaje por detección del agresor por la tarjeta	Descripción	Prueba para determinar si al detectar al agresor por el faro, se le envía notificación a la víctima.
	Resultados Esperados	Que al detectarlo se envié la notificación inmediatamente.
	Resultados Obtenidos	El retardo mencionado
	Conclusiones	Esta parte de la plataforma funciona de acuerdo a lo proyectado.
Recepción del mensaje por detección del agresor por Bluetooth	Descripción	Prueba para determinar si al detectar al agresor por Bluetooth, se le envía notificación a la víctima
	Resultados Esperados	Que se envíe la notificación con un máximo de retardo de un minuto al colocar los dispositivos en un mismo espacio.
	Resultados Obtenidos	Aparte del minuto como máximo que se demora en detectarlo hay que sumarle el retardo del bróker.
		Esta parte de la plataforma funciona de acuerdo a lo proyectado.

Conclusiones y trabajo futuro

Las pruebas de cobertura, detección de dispositivos y velocidad de respuesta comprueban que el diseño y la tecnología empleada en el sistema, son adecuadas para asegurar a la víctima de maltrato que tanto ella como las autoridades respectivas serán oportunamente informadas de la inminencia de un encuentro con el agresor.

Como tareas pendientes queda la creación del brazalete del agresor, un dispositivo que integre las tecnologías empleadas aquí. También es una tarea pendiente la creación de súper administradores que se encargaran exclusivamente de crear los administradores y modificar los parámetros del sistema y un módulo de gestión de las tarjetas para manejar el inventario y alarmas de falta de notificación de una víctima o un agresor en un tiempo determinado, la obtención del certificado de seguridad del servidor Web HTTPS, el cifrado de los datos enviados por los celulares y las tarjetas, y el acceso remoto a las tarjetas.

Una debilidad del modelo es la dependencia en el bróker –y sus estándares de servicio– para el envío-recepción de SMS. Como se indicó en la Tabla 2, el tiempo entre la generación y la recepción del mensaje puede ser de hasta 30 segundos,

tiempo suficiente, a una velocidad de 2,5m/segundo (velocidad de carrera) para avanzar 75 metros. Esto, en la práctica, hace que mensajes como *agresor a 60 metros* sean inútiles. Por lo tanto, si al momento de la implementación de un sistema de este tipo no es factible resolver el tema con el proveedor, es necesario hacerlo a través de configuración, para garantizar que las alertas se generan cuando el agresor esté, al menos a treinta segundos de poder llegar al límite previsto en la ley.

Referencias bibliográficas

Acosta, J., Díaz, J, & Morales, M. (2011). *Sistema de localización agresor-victima en ambientes indoor y outdoor* [tesis de grado], Universidad Icesi, Cali, Colombia

BeagleBoard.org (2011, junio 1). *BeagleBoard-xM Product Details* [en línea]. Recuperado de http://beagleboard.org/hardware-xM/

Icesoft Tech. (2012). *Icefaces overview* [En línea]. Recuperado de http://www.icesoft.org/java/projects/ICEfaces/overview.jsf

JBoss Community (2011, abril). *The JBoss way* [en línea]. Recuperado de www.jboss.org.

King, G., Bauer, C., Bernard, E., & Ebersole, S. (2012, febrero 8). *Hibernate getting started guide* [en línea]. Recuperado de http://docs.jboss.org/hibernate/core/3.6/quickstart/en-us/html_single/

Lyons, G (2012, febrero 2). *2012 Mobile Market Share infographic* [en línea]. Recuperado de http://connect.icrossing.co.uk/2012-mobile-market-share-infographic_7962.

Ubuntu. (2011). *Ubuntu 10.10 (Maverick Meerkat) Beta* [en línea]. Disponible en http://old-releases.ubuntu.com/releases/10.10/

Usemos Linux (2010, julio 30). *Qué novedades podemos esperar en Ubuntu 10.10 Meerkat* [en línea]. Recuperado de http://usemoslinux.blogspot.com/2010/07/que-novedades-podemos-esperar-en-ubuntu.html

Currículum vitae

Madelayne Morales Rodriguez

IEEE Graduated Student Member. Ingeniera Telemática de la Universidad Icesi (2012) con interés en las áreas de planeación y gerencia de proyectos en Tecnologías de la Información y las Comunicaciones (TIC) y servicios interactivos. Desde su último año de carrera es miembro del grupo de investigación en Informática y Telecomunicaciones [i2T] de Icesi donde actualmente hace parte del equipo de investigadores del Proyecto *Servicio universal en cooperación Colombia-España para sistemas satélite de televisión* [Success TV], financiado por Colciencias.

Juan Camilo Acosta Escobar

Ingeniero Telemático egresado de la Universidad Icesi en 2012, con interés y experiencia en las áreas de diseño y desarrollo de aplicaciones Web y móviles, gestión y administración de redes y telecomunicaciones y seguridad informática. Actualmente trabaja en el Banco de Occidente (Cali, Colombia), en el proyecto *Core Bancario de Comercio Exterior*.

Juan David Díaz Ramírez

Ingeniero Telemático con cinco años de formación en la Universidad Icesi y uno en el Institut National des Sciences Appliquées de Lyon (Francia), con experiencia y especial interés en el diseño, la gestión y la administración de redes de comunicación y servidores y el desarrollo de proyectos de redes y sistemas.

Darío Fernando Cortés Tobar

Ingeniero Electrónico de la Universidad Autónoma de Occidente, Msc. De la Universidad de Sevilla, con experiencia e interés en el área de electrónica señales y comunicaciones inalámbricas. Actualmente se encuentra desempeñándose como investigador de la Universidad de Sevilla (España).