R. Rios, I. Agudo, and J. L. Gonzalez, "Implementación de un esquema de localización privada y segura para interiores", *IX Jornadas de Ingeniería Telemática (JITEL10)*, pp. 237 - 244, 2010.
NICS Lab. Publications: https://www.nics.uma.es/publications

Implementación de un esquema de localización privada y segura para interiores

Rubén Ríos del Pozo, Isaac Agudo Ruiz
Dpto. de Lenguajes y Ciencias de la Computación
Universidad de Málaga
Email: {ruben,isaac}@lcc.uma.es

José Luis Gonzalez
Telefónica I+D
Madrid
Email: jluis@tid.es

Resumen

Las aplicaciones basadas en localización proporcionan a los usuarios servicios personalizados dependiendo de su ubicación. Las estimaciones prevén que estos servicios se extenderán enormemente en los próximos años reportando grandes beneficios tanto a la industria como a los usuarios finales. Sin embargo, para que estos avances sean posibles se hace necesario analizar en profundidad las distintas implicaciones de seguridad y privacidad que la utilización de tales servicios pueden traer consigo a los usuarios.

En este trabajo proponemos un sistema de localización que da soporte a la provisión de servicios basados en localización para entornos *indoor* y que se fundamenta en la tecnología de redes de sensores inalámbricos. En este esquema hemos tenido en cuenta diversos aspectos de seguridad y privacidad, prestando especial atención a la limitación extrema de recursos característica de las redes de sensores. Finalmente hemos desarrollado una prueba de concepto para comprobar la viabilidad de nuestro esquema dentro del ámbito del proyecto OSAmI.

1. Introducción

Los servicios basados en localización (*Location-Based Services*, LBS) han ido ganando popularidad en los últimos años gracias al auge de las comunicaciones móviles y a los avances en los sistemas de localización. Los LBS tienen como objetivo proporcionar un servicio personalizado a los usuarios basándose en la ubicación en la que estos se encuentran. Para ello se hace necesaria la existencia de dos componentes fundamentales en estos sistemas, en primer lugar la utilización de alguna tecnología de posicionamiento, ya sea obtenida por el propio cliente (e.g. mediante GPS) o suministrada por un servidor de localización externo (e.g. la propia infraestructura de red GSM), y por otra parte, una tecnología de comunicación que permita al cliente interactuar con el proveedor del servicio.

Las aplicaciones típicas basadas en localización ofrecen servicios de navegación (indicación de direcciones, búsqueda de aparcamiento), emergencias (asistencia en carretera, llamadas de emergencia), ocio (búsqueda de amigos, redes sociales), información (páginas amarillas geográficas, guías turísticas), etcétera.

Si bien GPS es el estándar de facto, a la espera de que Galileo entre en acción [1], esta tecnología no permite localizar en espacios cerrados. Es precisamente en este ámbito, el de la localización en interiores (*indoor*), donde se están presentando más avances en los últimos años. Por poner un ejemplo, los populares servicios de audio guías de museos actualmente requieren de una interacción del usuario para seleccionar la zona en la que se encuentran, sin embargo ya son varias las iniciativas para hacer que estas guías sean sensibles a la posición [2].

Compañías como Cisco proporcionan soluciones de localización *indoor* [3] aunque por lo general están orientadas a entornos empresariales donde la privacidad no se considera un requisito fundamental. Por otra parte, Nokia está implementando en fase de pruebas un servicio de localización en interiores

para móviles en el centro comercial Kamppi en Helsinki, Finlandia. Este sistema permite que cualquier persona dentro del centro comercial pueda localizar los comercios más cercanos, compartir su localización con otros y buscar amigos que se encuentren cerca.

La localización en interiores presenta nuevos retos técnicos en la determinación y representación de la información de localización [4]. Las tecnologías utilizadas para el posicionamiento en exteriores presentan ciertas limitaciones que imposibilitan su utilización en entornos *indoor*. Los principales obstáculos que encuentran son, por un lado la atenuación o pérdida de la señal dentro de edificios y, por otro lado, la imposibilidad de ofrecer una información de localización exacta o una representación adecuada de la misma dependiendo de las necesidades del servicio. La capacidad de proporcionar coordenadas lógicas o relativas, en lugar de coordinadas físicas, simplifica en gran medida la provisión de servicios de localización dentro de edificios, donde los espacios se encuentran claramente diferenciados por zonas, como son diferentes plantas y habitaciones.

La mayoría de LBS para interiores se basan en la provisión de servicios por proximidad. En este caso el sistema de localización se basa en tecnologías de comunicaciones de medio o corto alcance como Wi-Fi, Bluetooth (BT), infrarrojos (IR) o una combinación de las anteriores [3, 5, 6]. El aprovechamiento de una infraestructura preexistente hace de Wi-Fi y Bluetooth las tecnologías a considerar en el momento de desarrollar un sistema de localización con una inversión inicial reducida. Dado que éstas no son tecnologías específicas de posicionamiento los aspectos de seguridad se suelen relegar a un segundo plano.

En este trabajo se plantean dos esquemas de localización segura para interiores. Por un lado se describe un esquema inicial junto a su implementación, cuyo objetivo principal es comprobar la viabilidad de la propuesta. Además se analizan los retos de seguridad y privacidad a cubrir y se proporcionan soluciones a éstos en un segundo esquema con características avanzadas. Este último esquema permite autenticar a las partes involucradas en el proceso de localización al mismo tiempo que es capaz de preservar la privacidad de los usuarios.

El articulo se organiza de la siguiente manera. La sección 2 analizan diferentes aspectos a considerar en el diseño de un esquema de localización *indoor* seguro utilizando la tecnología de redes de sensores. En la siguiente sección se presenta el esquema propuesto, y se dan detalles sobre la plataforma utilizada, la arquitectura del sistema, la implementación de la prueba de concepto y su aplicación con éxito dentro del ámbito de un proyecto. La sección 4 analiza posibles mejoras de nuestro esquema para implementaciones futuras. Finalmente, en la sección 5 se exponen las conclusiones del trabajo.

2. Localización Indoor usando Redes de Sensores

Las redes de sensores (*Wireless Sensor Network*, WSN) se componen de pequeños dispositivos de bajo coste (sensores) con capacidad para monitorizar los fenómenos físicos que tienen lugar en su entorno y comunicarlos a un dispositivo con mayor capacidad para procesar y analizar tal información (estación base). El elenco de sensores que pueden ir acoplados a los nodos que conforman la red es amplísimo, entre los cuales es posible encontrar sensores de temperatura, humedad, luminosidad, presión, radiación, etcétera [7]. Esto los convierte en dispositivos muy versátiles capaces de desempeñar tareas muy diversas, lo cual unido a su reducido coste y tamaño hace de las WSNs una tecnología ideal para la monitorización de diversos entornos y recursos.

Por ello, las WSNs han aparecido en diversos ámbitos, tanto en exteriores como en interiores [8]. Entre las aplicaciones más características que pueden desempeñar en exteriores se encuentra la monitorización de los niveles de contaminación atmosférica y recolección de datos climáticos, gestión eficiente de cultivos, detección y prevención de incendios forestales, etcétera. En interiores, las WSNs pueden ser utilizadas como medio para la vigilancia del hogar frente a intrusiones, detección de fugas de aguas o gases y monitorización de personas en situación de dependencia, entre otros.

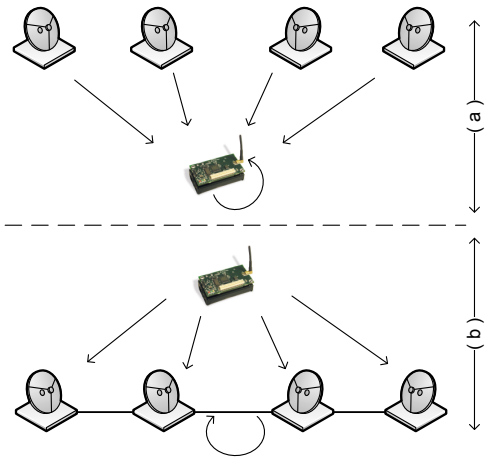

Figura 1: Esquemas de localización

Otra de las posibilidades que las WSNs son capaces de ofrecer es la localización de recursos o individuos. Por un lado se pueden localizar elementos externos a la red gracias a los diferentes sensores que llevan acoplados los nodos, por ejemplo, un sensor de presencia o una cámara. Por otro lado, también es posible localizar elementos pertenecientes a la red a través la medición de ciertas características de las señales de radio intercambiadas entre los dispositivos.

Es de suponer que en un futuro cercano, cuando todos los objetos de nuestro entorno formen parte de una única red, la Red de Objetos o *Internet of Things* [9] esta última forma de localización prevalezca sobre la anterior. Existen principalmente tres métodos dependiendo de la característica observada [10]: basados en la potencia de la señal recibida (*Received Signal Strength*, RSS), basados en el ángulo de llegada de la señal (*Angle of Arrival*, AoA) y basados en el tiempo de llegada (*Time of Arrival*, ToA). Este proceso se conoce como fase de observación.

De forma general podemos distinguir cuatro grandes grupos en los que englobar las soluciones de localización dependiendo de la entidad que realiza la observación y el cálculo de la posición del dispositivo [11]. Así pues, podemos identificar soluciones en las que ambos procesos son llevados a cabo por el dispositivo o por la infraestructura de red, y otras soluciones en las que el proceso de observación es realizado por el dispositivo, que comunica tal información a la red para que realice el cálculo, y viceversa. En la Figura 1 se muestran dos esquemas básicos de sistemas de localización, en los que se presentan de manera simplificada los elementos que conforman el sistema y las partes involucradas en cada proceso. En el caso (a), el dispositivo sensor es el encargado de recoger la información recibida del sistema así como de procesar su propia localización a partir de ésta. Mientras que en el otro caso, (b), es el sistema de posicionamiento el que realiza las observaciones y calcula la ubicación del dispositivo. Esta información puede ser simplemente almacenada en el punto del sistema que realiza el cálculo o puede ser enviada a la otra parte (o una tercera) para que tenga constancia de la localización del dispositivo.

Esta clasificación es interesante por las implicaciones que tiene desde el punto de vista de la seguridad y la privacidad de los (portadores de los) dispositivos. Dependiendo de la entidad o entidades involucradas en la observación y el cálculo posterior de la posición, el sistema puede verse vulnerado desde diferentes ángulos. Así por ejemplo, si la infraestructura se limita a informar ciertos datos que permiten a los dispositivo determinar su posición, como es el caso de GPS, el dispositivo tiene pleno control sobre su información de localización quedando la privacidad de localización del usuario asegurada frente a posibles infracciones del sistema de posicionamiento.

Existen diferentes tipos de ataques que pueden afectar a la correcta localización del dispositivo. De manera general podemos encontrar dos tipos de ataques, aquellos realizados por atacantes externos y los realizados por atacantes internos [12]. Los atacantes externos son aquellos que no forman parte de la

infraestructura y por tanto no pueden autenticarse con el resto de la red; su intención es convencer a un nodo o a la infraestructura de posicionamiento de que tal nodo se encuentra en una posición diferente de su posición real. Por otra parte, son atacantes internos aquellos que forman parte del sistema pero que se comportan de forma maliciosa, tratando de convencer al sistema de localización de que se encuentra en una posición diferente de la que realmente se encuentra. Asimismo, ambos tipos de atacantes pueden tratar de suplantar a otros nodos para que el sistema de posicionamiento crea que está localizando a un nodo cuando en realidad es otro nodo el que se encuentra en esa posición. Este tipo de ataques suele tener como finalidad obtener acceso a los recursos que el nodo suplantado está autorizado o inculpar a otro dispositivo en la realización de determinadas acciones. Del mismo modo, un atacante podría hacerse pasar por el sistema de posicionamiento para intentar conseguir información confidencial de los nodos de la red. Desde el punto de vista de la privacidad, los atacantes tratan de determinar la posición de un dispositivo o hacer un seguimiento (*tracking*) del mismo sin estar autorizados para ello. La posibilidad de realizar un seguimiento de individuos abre las puertas a que se puedan llevar a cabo acciones indeseadas, desde el envío de publicidad personalizada hasta incluso acciones criminales como robos y secuestros.

Es importante en este punto recalcar que son las características físicas de la señal las que en última instancia permiten determinar la localización de los dispositivos, ubicando la fuente de la señal. Sin embargo, para identificar al dispositivo necesitamos intercambiar información adicional a nivel lógico que describa de forma única al dispositivo. Esta información en el caso de tecnologías como Bluetooth y Wi-Fi se encuentra en la forma de una dirección MAC, que no es más que un identificador que corresponde de manera única a un interfaz de red. Este identificador permanece constante a lo largo del tiempo [1], por tanto, se utiliza generalmente como medio para autenticar el origen de los paquetes de información. El uso de la MAC en las comunicaciones hace que sea posible averiguar que elementos se están comunicando en la red sin que los nodos tengan conocimiento de este hecho.

Este trabajo no pretende ofrecer una solución global a los problemas de seguridad y privacidad en sistemas de posicionamiento. Podemos afirmar que no existe tal solución, de hecho, cualquier sistema puede ser vulnerado aunque en muchas ocasiones el coste puede superar los beneficios. Incluso podemos encontrar trabajos como [13] en el que mediante el análisis de ciertas características de las señales de radio durante su etapa transitoria es posible reconocer a los dispositivos que generan tales señales de forma unívoca. Sin embargo, este tipo de análisis es bastante costoso y requiere la utilización de equipos altamente sofisticados. Por ello, en este trabajo proponemos un primer acercamiento que permita dificultar la labor de un posible atacante, resolviendo algunas de las amenazas que impedirían el buen funcionamiento de un servicio basado en localización. A continuación se describen los principales retos que nos encontramos:

- Autenticación del cliente: tenemos que evitar que un atacante puede hacerse pasar por un usuario legítimo del sistema y por tanto pueda acceder a los servicios a los que de otra forma no estaría autorizado a acceder

- Autenticación del sensor de referencia (rastreador): tenemos que evitar que un atacante pueda impersonar a los elementos del sistema de posicionamiento haciendo pensar al usuario que está comunicándose con un elemento legítimo y consiga así hacer un seguimiento de la posición del usuario.

- Privacidad de la localización: tenemos que evitar que un atacante externo con acceso a todas las comunicaciones sea incapaz de inferir los clientes que se encuentran encuentran en una determinada posición por la observación de los mensajes intercambiados entre el cliente y el sistema de posicionamiento.

[1] Aunque existe la forma de modificar la dirección MAC de algunos interfaces de red, no es un proceso que se realice de manera automática sin necesidad de que intervenga el usuario. Además, el cambio de la dirección MAC es posible únicamente en determinados dispositivos, siendo una tarea vetada en la mayoría de dispositivos móviles.

Además de los retos de seguridad y privacidad propuestos hemos de tener en cuenta la usabilidad de las soluciones. Esto también supone un reto en el momento de la implantación del sistema. No es deseable que los usuarios tengan que participar constantemente y de manera activa en el proceso de localización o que se introduzca una sobrecarga excesiva en el sistema como consecuencia de querer mantener ciertos niveles de seguridad y privacidad. Es necesario encontrar un equilibrio entre los niveles de seguridad y usabilidad. En la Cuadro 1 se muestra una comparativa entre las tecnologías más utilizadas para localización *indoor* en la que se hace referencia tanto a aspectos de seguridad como de usabilidad.

	Wi-Fi	BT	RFID
Autenticación Cliente	Si	Si	Si
Autenticación Rastreador	Si	Si	Si
Privacidad Localización	No	No	Si
Sin Interacción Usuario	Si	Si	No

Cuadro 1: Comparación de Tecnologías

En lo relativo a la autenticación, tanto del cliente como del rastreador, las tres tecnologías consideradas en Cuadro 1 pueden proporcionar esta característica. Sin embargo, en el caso de optar por Wi-Fi y Bluetooth, que suelen utilizar como mecanismo para la localización la transmisión de beacons (o balizas), éstas no ofrecen los mecanismos pertinentes para facilitar la autenticación. Si bien es cierto que de manera opcional puede optarse por realizar la autenticación entre las partes comunicantes, ésta sólo se considera en el momento de realizar una conexión entre dispositivos. El problema de requerir el establecimiento de una conexión entre ambos dispositivos es su excesivo coste tanto en tiempo como en recursos (batería). Por su parte, las tecnologías utilizadas en las tarjetas sin contacto fueron diseñadas para mecanismos de control de acceso, por tanto pueden proporcionar autenticación mutua.

Debido a que los dispositivos dotados de tarjetas Wi-Fi y/o Bluetooth suelen utilizar su dirección física en el proceso de localización y que esta dirección es por lo general estática, un atacante que se encuentre a la escucha de las comunicaciones sería capaz de hacer un seguimiento de los dispositivos involucrados. Estas tecnologías no ofrecen ningún mecanismo que evite esta seria amenaza. Si bien hay algunos protocolos de autenticación para tarjetas inteligentes que proporcionan privacidad de localización, se presupone que dado que las comunicaciones por inducción electromagnética se realizan a muy corta distancia, es difícil que se puedan interceptar las comunicaciones incluso cuando el protocolo no proporcione privacidad de localización.

Asimismo, en este trabajo consideramos la usabilidad como un factor fundamental y por tanto requerir al usuario que intervenga en el proceso de localización supone una traba en el diseño del sistema de localización. En el caso de las tecnologías Wi-Fi y Bluetooth, no se requiere la interacción por parte del usuario, basta con que éste lleve consigo su dispositivo con el interfaz de red correspondiente activado para que el sistema de localización pueda ubicarlo. Sin embargo, esto no es así en el caso de las tarjetas sin contacto, que debido a su corto alcance requiere que el usuario acerque su etiqueta al lector para que éste sea capaz de detectar su presencia.

La utilización de nodos sensores para localización de los usuarios puede resultar por si mismo utópico e intrusivo puesto que el usuario tendría que llevar consigo un dispositivo cuyo único cometido es interactuar con el sistema de localización. Sin embargo, se prevé que en un futuro próximo los sensores serán elementos de uso generalizado en la sociedad al igual que lo son ahora los teléfonos móviles [14][9]. Bajo estas previsiones todos llevaremos con nosotros algún dispositivo con capacidad computacional y para comunicarse basado en estándares como IEEE 802.15.4 [15], ya sea en forma de una red de área corporal (*Body Sensor Network*, BSN) o como dispositivos independientes (p.ej.: un llavero o un reloj), que puedan desempeñar las funciones que se presentan en este trabajo.

Por tanto, nuestro objetivo es proporcionar una solución de localización segura que proporcione

privacidad de localización y que además no requiera de interacción por parte del usuario.

3. Esquema de Localización Privada y Segura con WSN

La funcionalidad básica que se espera de un servicio de localización es el posicionamiento de los usuarios dentro de un mapa del edificio. De esta forma los usuarios pueden compartir su localización con otros usuarios que se encuentren en el mismo edificio o incluso en otro edificio. Para ello, una solución es que la posición de cada individuo se reporte directamente a un servidor de localización que mantiene una base de datos con la posición de todos los usuarios registrados del sistema.

Idealmente cuando un usuario se aproxima a un edificio su dispositivo de localización *indoor* inicia una negociación con el edificio de forma que se establece una relación de confianza entre ambos, lo cual permite que el usuario pueda acceder a los servicios basados en localización prestados por el edificio. Para ello se le puede requerir al usuario que presente ciertas credenciales que lo identifiquen como un usuario autorizado a hacer uso los servicios disponibles en el edificio. Cuando un usuario es desconocido por el edificio se le puede permitir un acceso limitado a los servicios de localización ofertados.

La pieza básica para que este esquema funcione es la localización de los nodos sensores por parte de los nodos que forman parte del sistema de referencia. Esta localización se tiene que llevar a cabo de forma segura tanto para el sistema como para sus usuarios. Ahí es donde entra nuestro desarrollo.

3.1. Plataforma de Programación

Para demostrar la viabilidad de nuestro esquema de localización hemos diseñado una prueba de concepto utilizando la plataforma de sensores MICAz [16] de la compañía Crossbow Technology. Este tipo de dispositivos permite la creación de redes de sensores de bajo consumo gracias principalmente al transceptor de radio y al microcontrolador que incorporan. El transceptor se trata del CC2420 de Texas Instruments [17], el cual es compatible con IEEE 802.15.4 y Zigbee. Por tanto, es capaz de trabajar en la banda de frecuencia de 2.4 GHz y de ofrecer una tasa de transferencia de datos que puede llegar a alcanzar los 250 Kbps, con potencias de transmisión que oscilan entre los -25 dBm y 0 dBm. El microcontrolador es el ATmega128L fabricado por Atmel [18]. Se trata de una arquitectura RISC de 8 bits con capacidad para trabajar a una velocidad de hasta 8MHz. Es interesante notar que, aunque la especificación establece una frecuencia máxima de procesamiento de 8 MHz, al estar alimentados por dos baterías del tipo AA (3 voltios), la frecuencia de funcionamiento suele reducirse a 4 MHz[2]. Además, ofrece una memoria flash programable de 128 KB, una memoria RAM de 4 KB y finalmente una memoria externa de 512 KB dedicada principalmente al almacenamiento de mediciones.

Los nodos sensores utilizan el sistema operativo TinyOS [19]. TinyOS es un sistema operativo de código abierto diseñado específicamente para su utilización en redes de sensores inalámbricas. Presenta una arquitectura basada en componentes lo cual posibilita la fácil integración y eliminación de funcionalidades al tiempo que se minimiza el tamaño del código, lo cual es un factor determinante en las plataformas para las que está diseñado. Entre las funcionalidades ofrecidas de forma nativa se encuentran protocolos de red, componentes para el acceso a los sensores, mecanismos para la comunicación a través del puerto serie con un PC y así hacer las veces de estación base, herramientas para la lectura y escritura en memoria, etcétera. El lenguaje de programación utilizado para el desarrollo de aplicaciones es NesC [20], que es básicamente una extensión del lenguaje C diseñado para incorporar los conceptos de estructuración y el modelo de ejecución de TinyOS.

[2]Este valor es establecido por defecto en el sistema operativo TinyOS para reducir así el consumo energético

3.2. Arquitectura del Sistema

El sistema desplegado para la realización de la prueba de concepto se compone principalmente de dos tipos de nodos, los primeros son aquellos que los usuarios llevan consigo y en el segundo tipo se encuentran los nodos que forman parte del sistema de localización, que en adelante llamaremos indistintamente *anchors* o rastreadores. Ambos tipos de nodos son idénticos en cuanto a las capacidades que ofrecen, salvo que los integrantes del sistema de posicionamiento se encuentran conectados a través del puerto serie del ordenador para la comunicación de los datos de localización al servidor central que mantiene una base de datos sobre la ubicación de los diferentes usuarios del sistema.

3.3. Implementación de la Prueba de Concepto

La implementación de nuestro esquema se ha basado principalmente en la utilización de cuatro elementos que han posibilitado la localización de los usuarios de manera no intrusiva al mismo tiempo que se preserva la privacidad de localización de los usuarios, evitando que puedan ser rastreados por agentes externos, y se autentica a las partes comunicantes:

- Compartición de una clave simétrica: tanto los sensores legítimos del sistema como los elementos del sistema de localización comparten una clave que en la implementación actual es cargada durante el despliegue del sistema. Esta clave puede ser actualizada de manera ocasional mediante un mecanismo de refresco de claves.

- Eliminación de identificador: los mensajes transmitidos por los nodos de una red de sensores son, por norma general, encapsulados en tramas compatibles con el estándar IEEE 802.15.4. Éstas contienen una serie de campos que sirven para identificar a los nodos que componen la red. Para evitar que un atacante que se encuentre escuchando las comunicaciones pueda tracear a un individuo es necesario eliminar esta información.

- Ajuste de la potencia de transmisión: limitar la potencia en la que los rastreadores emiten las señales de beaconing permite a los sensores responder únicamente a aquellas señales emitidas por dispositivos que se encuentran en un rango de acción reducido.

- Frescura de los datos: es necesario garantizar que los datos generados son frescos, es decir, que ningún adversario sea capaz de reproducir un mensaje de respuesta a una baliza antigua y así conseguir suplantar a un usuario. Este tipo de ataque se conoce como ataque por repetición.

Las limitaciones en términos computacionales, energéticos y de almacenamiento inherentes a los nodos de una red de sensores dificultan la utilización de primitivas criptográficas complejas. Por este motivo, en los primeros trabajos de seguridad en WSNs se consideraba que la criptografía de clave pública era excesivamente exhaustiva para poder ser utilizada en este ámbito [21][22], al requerir unos tiempos para la generación de la claves y verificación de firmas de varias decenas de segundos. Aunque esta visión ha ido cambiando en los últimos años gracias a la evolución de la criptografía de curva elíptica, que ha conseguido reducir los tiempos a pocos segundos, desde el punto de vista del rendimiento aún sigue siendo más aconsejable utilizar criptografía de clave simétrica al ser capaz de ofrecer tiempos del orden de micro segundos [23]. El principal inconveniente de los algoritmos de clave simétrica es la gestión de claves.

Esto ha motivado la elección del algoritmo de clave simétrica AES con un tamaño de bloque de 128 bits y por tanto con el mismo tamaño de clave. Esta implementación fue desarrollada en el ámbito del proyecto europeo SMEPP [24] y ha sido adaptada para nuestros propósitos actuales. Además, para reducir el problema de la distribución de claves se ha optado por precargar a los sensores involucrados en el proceso de localización con la clave AES antes del despliegue del sistema.

Por otra parte se hace necesario eliminar de los paquetes de datos cualquier información que pudiera identificar a los nodos. Esto se convierte en un requisito indispensable ya que en caso de mantener un identificador constante por cada usuario del sistema, un agente externo tendría la posibilidad de hacer un seguimiento de sus movimientos. Este es uno de los problemas principales de tecnologías como Wi-Fi y Bluetooth, que en las capas más bajas de la pila de protocolos proporcionan direcciones de enlace (MAC) que son únicas para cada dispositivo. Existen principalmente dos formas de solventar este problema, la primera es utilizar pseudónimos y la segunda es utilizar un mismo identificador para todos los dispositivos. En caso de optar por la utilización de pseudónimos, es decir, un identificador que se utiliza en lugar del verdadero identificador, éste no puede ser estático ya que sería cuestión de tiempo que un atacante pudiera rastrearlo. Por tanto, es necesario que los pseudónimos vayan cambiando de manera ocasional, lo que requiere de un mecanismo de sincronización entre dispositivos para que la comunicación sea posible. El segundo caso es utilizar un identificador común para todos los dispositivos, lo cual los hace indistinguibles entre sí. Esto no permite la identificación a nivel de enlace y por tanto el encaminamiento de paquetes se ve imposibilitado. Sin embargo, nuestro esquema al no requerir de mecanismos de encaminamiento, la identificación se puede realizar a nivel de aplicación, información que se encuentra debidamente protegida mediante AES.

Asimismo en nuestra implementación hemos utilizado un mecanismo basado en el ajuste de la potencia de transmisión con el fin de limitar el radio de acción de los nodos que forman parte del sistema de posicionamiento. Al reducir el alcance de las señales emitidas por los rastreadores, sólo aquellos usuarios que se encuentran en sus proximidades tendrán acceso a las balizas y serán capaces de responder. El tiempo de respuesta debe encontrarse debidamente limitado, lo cual se deja a la elección del administrador del sistema. De manera obvia, el tiempo de espera para la llegada de balizas no debe ser excesivamente elevado por una razón principal: un tiempo elevado permite que un nodo que se encuentra en las proximidades del *anchor*, y que tiene acceso a las balizas, pueda repetir esta información a otro nodo que se encuentra fuera del alcance de éste. El nodo remoto, a su vez, respondería al nodo que hace de puente en la comunicación para hacer pensar al *anchor* que el nodo remoto también se encuentra en las inmediaciones del *anchor*. Del mismo modo, la potencia de transmisión es también un parámetro que se deja a la elección del administrador del sistema, dependiendo de las necesidades de cada instalación. En concreto, los nodos que se han utilizado para la prueba de concepto, los cuales integran el chip de radio CC2420, permiten utilizar diferentes potencias de transmisión. TinyOS ofrece una función (`CC2420Packet.setPower`) que permite modificar el registro que controla el nivel de transmisión para cada mensaje de manera individual. En nuestro caso hemos utilizado un valor que ofrece un rango de transmisión que se encuentra en torno a los 30 centímetros.

Para garantizar la frescura de los datos enviados, evitando así ataques por repetición, se ha optado por que las balizas enviados por los sensores que componen el sistema de localización contengan datos generados a partir de una función pseudoaleatoria. En particular, los balizas contienen un número pseudoaleatorio con una longitud de 32 bits, lo cual ofrece un espacio de direccionamiento lo suficientemente grande como para evitar que se produzcan colisiones en un largo espacio de tiempo. Los nodos llevados por los usuarios, al recibir las balizas, extraerán su contenido y lo anexionarán con su número de serie, el cual es único para cada dispositivo y que es precargado en la fase previa al despliegue del sistema. Finalmente, se aplicará el algoritmo de cifrado sobre esta información y se enviará de vuelta al *anchor*, el cual utilizará la clave compartida entre ambos para descifrar tal información. En caso de tratarse de un usuario legítimo del sistema, el número aleatorio corresponderá con el enviado por el *anchor* instantes previos y éste podrá extraer el número de serie del dispositivo, identificando así al usuario.

En la Figura 2 se muestra un ejemplo reducido de un posible intercambio de mensajes realizado entre los participantes del sistema de localización y los usuarios del sistema. En concreto se muestra una secuencia completa de localización en la que un *anchor* envía una baliza con un número aleatorio, el cual es recibido por Sensor1 y Sensor2. Estos generan el mensaje de respuesta e inmediatamente después lo envían a el *anchor*, que los procesa y comprueba su autenticidad. En caso afirmativo, los

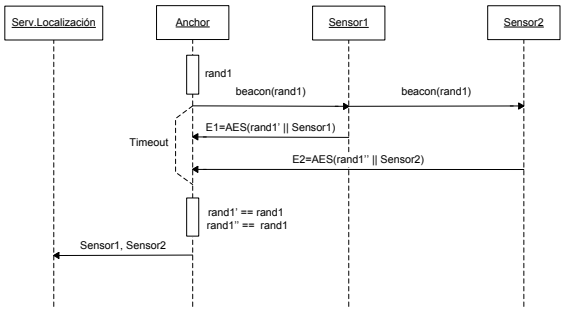

Figura 2: Diagrama de secuencia de la prueba de concepto

números de serie de los sensores se envían al Servidor de Localización, que almacena la información sobre la ubicación de tales sensores.

Además, es interesante notar que cualquier usuario puede decidir en un momento determinado deshabilitar su dispositivo sensor para evitar ser localizado por el sistema o por otros usuarios que compartan la misma clave. Esto supone un valor añadido a la privacidad de los usuarios, que tienen el control sobre cuándo pueden ser localizados.

3.4. Aplicación dentro del proyecto OSAmI

El proyecto OSAmI-Commons [25] es un proyecto avalado por el programa Eureka-ITEA2 y financiado por el Plan Avanza a nivel nacional, en el que participan empresas líderes europeas, institutos de investigación y universidades, y que tiene como objetivo el desarrollo de la plataforma base para aplicaciones de *Inteligencia Ambiental*. La Inteligencia Ambiental se puede ver como el espacio de interacción de las personas y las tecnologías en su vida cotidiana. Estas tecnologías identifican nuestra presencia y son capaces de dar respuesta a nuestras necesidades y hábitos de una forma invisible y anticipatoria. Por otra parte, las necesidades de privacidad de los usuarios tienen que verse salvaguardadas de igual forma.

Uno de los escenarios de aplicación del proyecto, proporcionado por Telefónica, se centra en servicios multimedia que sean sensibles a la localización, de forma que el contenido multimedia vaya siguiendo al usuario mientras de mueve por el edificio. El desarrollo proporcionado no depende de la tecnología de posicionamiento utilizada. Para ello se ha desacoplado el servidor de localización, que mantiene información de la posición de los usuarios, de los sistemas de referencia que captan la posición del usuario. De esta forma se puede localizar a un mismo usuario usando varias tecnologías de forma simultánea.

Uno de los problemas que quedaban abiertos y que se pretenden resolver dentro de OSAmI en el campo de servicios basados en la localización es el de proporcionar otros mecanismos de localización que permitieran un alto grado de seguridad para el usuario y que a su vez se acoplaran con los desarrollos existentes dentro del proyecto. Podemos considerar este trabajo como un primer acercamiento en esa dirección.

4. Mejoras sobre el esquema inicial

Uno de los mayores problemas de seguridad que presenta nuestra prueba de concepto es que todos los usuarios comparten la misma clave con el sensor del sistema de localización. Esto implica que un usuario legítimo del sistema puede descifrar el mensaje de respuesta enviado por otro usuario y obtener su número de serie, que podrá utilizar para suplantarlo. Una posible solución, que está actualmente en fase de desarrollo, es utilizar, de manera adicional a la clave compartida (K_A), una clave simétrica

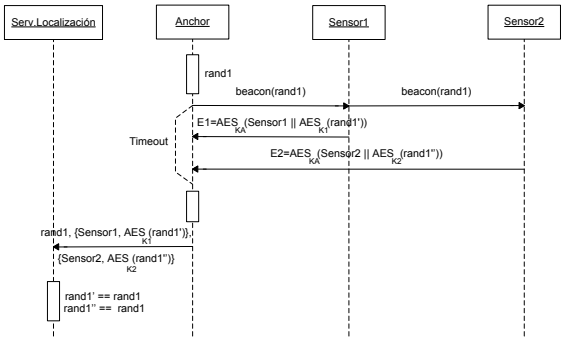

Figura 3: Diagrama de secuencia esquema avanzado

(K_i) diferente por cada nodo, que sería compartida entre cada nodo y el servidor de localización, de manera análoga al servicio de autenticación de la identidad del subscriptor en GSM [26]. De esta forma, en la respuesta de los sensores, en lugar de cifrar únicamente con la clave compartida por todos los nodos legítimos el número de serie junto al número aleatorio enviado por los sensores de referencia, se utilizaría la clave K_i de cada nodo para cifrar dicho número aleatorio, que junto con el número de serie del nodo, sería nuevamente cifrado con la clave del grupo K_A. De esta forma, los nodos legítimos no son capaces de impersonar a otros nodos, ya que no serían capaces de cifrar el número aleatorio con la clave correspondiente. Como contrapartida necesitamos que el servidor de localización se involucre de forma activa en el proceso de localización, dejando de ser una mera base de datos y liberando de carga computacional a los *anchors* de la red que pasarían a comportarse como proxies del proceso de localización. La Figura 3 muestra el diagrama de secuencia que describe este proceso.

Si bien es cierto que un atacante externo podría enviar balizas haciéndose pasar por un rastreador, ya que no se ofrece información que autentique que una baliza ha sido generada de manera legítima por un rastreador, el atacante no podría obtener la identidad del usuario puesto que desconoce la clave de descifrado. No obstante, esto puede suponer un ataque de denegación de servicio específico en el ámbito de las redes de sensores, el ataque por agotamiento de baterías. Aunque en la presente propuesta no se proporcionan los mecanismos adecuados para hacer frente a este tipo de amenaza, en la actualidad nos encontramos desarrollando una nueva versión del prototipo que tiene en cuenta esta forma de ataque.

En nuestro esquema, tanto los usuarios que quieren acceder a los servicios basados en localización como los equipos de localización o rastradores comparten un clave simétrica de cifrado. Esta clave puede ser la misma para todos los edificios o puede ser una diferente para cada zona *indoor*. En nuestra implementación de referencia solo hemos trabajado con una zona de localización *indoor* y por tanto solo se comparte una clave. En caso de que quisiéramos usar una clave distinta por cada edificio se podría que definir un conector con GPS para que al acercarse a cada edificio se estableciera la clave apropiada. Otra posibilidad sería enviar junto al número aleatorio un identificador de zona que podría servir para indicar la clave a utilizar. Por último, podríamos establecer un protocolo de intercambio de claves entre la zona y el sensor, basado en criptografía de clave pública, que nos permita negociar la clave de zona apropiada cada vez que cambiemos de zona. Trabajos recientes en criptografía de clave pública basada en curvas elípticas para WSNs, en concreto basada en la misma plataforma que hemos utilizado para nuestra prueba de concepto, dan tiempos inferiores a los 500 ms [27] por operación de firma o cifrado.

Al utilizar todos los usuarios la misma clave dentro de la misma zona *indoor* se permite que los usuarios puedan localizar de forma autónoma a sus compañeros, a la vez que se impide que usuarios externos al sistema, es decir que no conozcan la clave, puedan inferir nada de nuestra localización. Si utilizamos el esquema de autenticación avanzado donde cada nodo usa una clave diferente para cifrar el número aleatorio tenemos el inconveniente de que los otros nodos no podrán verificar la identidad de sus compañeros al desconocer la clave que cada nodo comparte con el servidor de localización. De hecho los

vecinos, aunque son capaces de obtener el número de serie del nodo, no son capaces de saber a ciencia cierta si se trata de un nodo legítimo el que crea el mensaje ya que sólo el servidor de localización puede comprobar que el número aleatorio cifrado es legítimo.

Por último, en el desarrollo inicial se considera que la comunicación entre los *anchors* y el servidores de localización se realiza por un canal seguro. En la práctica esto se traduce en la necesidad de utilizar algún mecanismo criptográfico para proteger las comunicaciones entres los anchos y el servidor. Dado que los *anchors* tiene suficiente poder computacional, para este fin se podrían utilizar protocolos estándar como WS-Security o incluso TLS.

Actualmente estamos trabajando en una nueva versión del sistema que tenga en cuenta todos estos aspectos.

5. Conclusiones y Trabajo Futuro

En este trabajo hemos presentado el desarrollo de un sistema de localización para entornos *indoor* capaz de resolver algunos de los problemas de seguridad y privacidad que pueden acontecer a lo hora de proporcionar servicios basados en localización. En concreto nos hemos centrado en resolver principalmente dos de los problemas que consideramos de mayor relevancia para este tipo de servicios, es decir, evitar la suplantación de los usuario que hacen uso del sistema y evitar que un atacante externo sea capaz de obtener información privada sobre los usuarios, p.ej. qué usuarios acceden a qué servicios o dónde se encuentra un usuario en un momento determinado. Al mismo tiempo, al encontrarse basada en el uso de redes de sensores inalámbricas, nuestra propuesta trata de ser lo menos intrusiva y lo más liviana posible. Por ello, en lugar de centrarse en la utilización de innumerables intercambios de mensajes entre el dispositivo del usuario y el sistema de localización o operaciones criptográficas con un elevado nivel de complejidad, la propuesta se centra principalmente en el uso de un cifrado AES de 128 bits para la generación de pseudónimos dinámicos para cada nueva transacción.

Un aspecto que queremos hacer notar es que el esquema que se presenta en este trabajo no trata de ser la solución definitiva a los problemas planteados a lo largo del artículo. Nuestro objetivo con este trabajo es hacer notar la necesidad de estudiar la problemática de seguridad que aparece en este tipo de entornos así como la necesidad de proporcionar la implantación de mecanismos de identificación privada en futuros desarrollos, de manera que sea posible acceder a diferentes servicios sin que entidades externas sean capaces de identificar al usuario que hace uso de estos. Además, es interesante recalcar que los problemas de privacidad siguen existiendo ya que este problema puede aparecer a distintos niveles. En nuestro caso nos hemos centrado en el nivel más bajo, el de las comunicaciones físicas. Sin embargo, si consideramos que un servicio determinado al que estamos accediendo puede seguirnos a medida que nos movemos, por ejemplo un flujo multimedia, a pesar de utilizar pseudónimos en los niveles más bajos, un observador podría relacionar un flujo determinado con un dispositivo.

Como trabajo futuro pretendemos ampliar nuestro esquema de manera que los dispositivos que llevan los usuarios puedan ser localizados no sólo por un único elemento del sistema de referencia, sino que los distintos *anchors* colaboren entre sí para determinar la posición de los usuarios del sistema. Esto traerá consigo nuevas oportunidades gracias a la posibilidad de incorporar a las técnicas hasta el momento propuestas, otros mecanismos de localización más avanzadas, como la triangulación. Sin embargo, esto también dará lugar a nuevos desafíos tanto desde el punto de vista de la comunicación y coordinación entre los distintos dispositivos del sistema como desde la perspectiva de la seguridad y la privacidad. En concreto, al existir más interacción entre dispositivos y la necesidad de realizar comunicaciones salto a salto hasta alcanzar a la estación base, la privacidad de localización se verá afectada.

Agradecimientos

Este trabajo ha sido parcialmente financiado a través de los siguientes proyectos: OSAmI (TSI-020400-2009-92), financiado por el Ministerio de Industria, Turismo y Comercio mediante el Plan Avanza; y SPRINT (TIN2009-09237), finaciado por el Ministerio de Ciencia e Innovación y cofinanciado por FEDER (Fondo Europeo de Desarrollo Regional).

Referencias

[1] Z. Hunaiti, A. Rahman, M. Denideni, and W. Balachandran, "The impact of galileo on pedestrians navigation systems," *Electronics, Communications, and Computers, International Conference on*, vol. 0, p. 40, 2006.

[2] G. Ghiani, F. Paterno, C. Santoro, and L. D. Spano, "UbiCicero: A location-aware, multi-device museum guide," *Interacting with Computers*, vol. 21, no. 4, pp. 288 – 303, 2009.

[3] CISCO, "Wi-Fi Location-Based Services - Design and Deployment Considerations." [Online]. Available: https://learningnetwork.cisco.com/docs/DOC-3418

[4] M. Thomson, J. Winterbottom, and A. Corporation, *Locations with Locally-Defined Coordinate Reference Systems for PIDF-LO*, IETF Network Working Group Internet draft, 2009. [Online]. Available: http://tools.ietf.org/html/draft-thomson-geopriv-indoor-location-01

[5] A. Zafeiropoulos, I. Papaioannou, E. Solidakis, N. Konstantinou, P. Stathopoulos, and N. Mitrou, "Exploiting Bluetooth for deploying indoor LBS over a localisation infrastructure independent architecture," *International Journal of Computer Aided Engineering and Technology*, vol. 2, no. 2, pp. 145–163, 2010.

[6] S. Aparicio, J. Pérez, P. Tarrío, A. M. Bernardos, and J. R. Casar, "An indoor location method based on a fusion map using bluetooth and wlan technologies," in *DCAI*, 2008, pp. 702–710.

[7] Crossbow Technology, "MTS/MDA Sensor Board Users Manual," 2007. [Online]. Available: http://www.xbow.com/support/Support_pdf_files/MTS-MDA_Series_Users_Manual.pdf

[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393 – 422, 2002.

[9] European Commission, "Internet of Things in 2020 - A Roadmap for the Future," Sept. 2008. [Online]. Available: ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/enet/internet-of-things-in-2020-ec-eposs-workshop-report-2008-v3_en.pdf

[10] M. Vossiek, L. Wiebking, P. Gulden, J. Wieghardt, C. Hoffmann, and P. Heide, "Wireless Local Positioning," *Microwave Magazine, IEEE*, vol. 4, no. 4, pp. 77 – 86, dec. 2003.

[11] A. I. G.-T. Ferreres, B. R. Álvarez, and A. R. Garnacho, "Guaranteeing the Authenticity of Location Information," *IEEE Pervasive Computing*, vol. 7, no. 3, pp. 72–80, 2008.

[12] S. Capkun and J.-P. Hubaux, "Secure Positioning in Wireless Networks," in *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, Feb. 2006, pp. 221–232.

[13] K. Bonne Rasmussen and S. Capkun, "Implications of Radio Fingerprinting on the Security of Sensor Networks," in *Proceedings of IEEE SecureComm*, sept. 2007, pp. 331 –340.

[14] M. Chui, M. Löffler, and R. Roberts, "The Internet of Things," McKinsey Quarterly, March 2010. [Online]. Available: https://www.mckinseyquarterly.com/High_Tech/Hardware/The_Internet_of_Things_2538

[15] IEEE 802.15 WPAN TG4b, *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*, IEEE Computer Society Std., 2006. [Online]. Available: http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf

[16] Crossbow Technology, "MICAz 2.4 GHz - Wireless Module." [Online]. Available: http://www.xbow.com/Products/productdetails.aspx?sid=164

[17] Texas Instruments, "CC2420 - 2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver." [Online]. Available: http://focus.ti.com/lit/ds/symlink/cc2420.pdf

[18] ATMEL, "ATmega128l Datasheet." [Online]. Available: http://www.atmel.com/dyn/resources/prod_documents/doc2467.pdf

[19] TinyOS Community Forum, "An open-source OS for the networked sensor regime." [Online]. Available: http://www.tinyos.net/

[20] P. Levis, "TinyOS Programming," June 2006. [Online]. Available: http://csl.stanford.edu/~pal/pubs/tinyos-programming.pdf

[21] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[22] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*. New York, NY, USA: ACM, 2004, pp. 162–175.

[23] R. Roman, C. Alcaraz, and J. Lopez, "A Survey of Cryptographic Primitives and Implementations for Hardware-Constrained Sensor Network Nodes," *Mobile Networks and Applications*, vol. 12, no. 4, pp. 231–244, 2007.

[24] SMEPP Project, "Secure middleware for embedded p2p systems." [Online]. Available: http://www.smepp.org/

[25] OSAMI, "Open source ambient intelligence commons for an open and sustainable internet." [Online]. Available: http://www.osami-commons.org/

[26] H. Imai, *Wireless Communications Security*, M. G. Rahman and K. Kobara, Eds. Artech House, Inc., 2006.

[27] D. Aranha, L. Oliveira, J. Lopez, and R. Dahab, "NanoPBC: Implementing Cryptographic Pairings on an 8-bit Platform," in *CHiLE 09 - Conference on Hyperelliptic curves, discrete Logarithms, Encryption, etc*, 2009.