P. Najera, R. Roman and J. Lopez, "Acceso seguro a nodos RFID en una arquitectura de red personal", *XI Jornadas de Ingeniería Telemática (JITEL 2011)*, pp. 104-111, 2011.
NICS Lab. Publications: https://www.nics.uma.es/publications

Acceso seguro a nodos RFID en una arquitectura de red personal

Pablo Najera, Rodrigo Roman, Javier Lopez
Departamento de Lenguajes y Ciencias de la Computación
Universidad de Málaga
Edificio Institutos Universitarios de Investigación (4.0.8), Parque Tecnologico de Andalucía. CP 29590
{najera | roman | jlm}@lcc.uma.es

***Resumen*-El paradigma de red personal (PN) permitirá la interacción y colaboración del creciente abanico de dispositivos personales. Con tal fin, la PN ha de integrar en su seno de forma segura múltiples tecnologías heterogéneas con diversas capacidades computacionales y de comunicación. En particular, la incorporación de la tecnología RFID en objetos personales conlleva múltiples riesgos de seguridad y privacidad que han suscitado un elevado interés de la comunidad investigadora en los últimos años. Más allá de su seguridad de forma aislada, su integración en la PN y la interacción de ésta con redes de área extensa como Internet of Things requieren una arquitectura de red personal adecuada para tal contexto. Este artículo proporciona los fundamentos de tal arquitectura segura incluyendo el análisis de aspectos como la incorporación e inicialización de las restringidas etiquetas RFID en la PN, la autenticación tanto de miembros de la PN como de usuarios y servicios remotos en su acceso a las tecnologías de contexto, el control de las políticas de privacidad y el establecimiento de canales seguros de comunicación supervisados.**

***Palabras Clave*-** Seguridad RFID, red personal, arquitectura software

I. INTRODUCCIÓN

El emergente paradigma de red personal habilita la comunicación de todos los dispositivos y servicios del usuario de forma flexible, segura y auto-organizada. Dicha topología de red ha de proporcionar las bases para la provisión de servicios relativos al contexto del usuario así como permitir la comunicación con redes de área extensa (ej. Internet of Things) con objeto de interactuar con dispositivos y redes remotas, así como facilitar la complementación y agregación de los servicios personales.

Dentro de las tecnologías clave en la realización de este modelo de red se encuentran las redes de sensores corporales (body sensor networks, BSNs) que permiten desde el control de los parámetros fisiológicos del usuario al reconocimiento de sus actividades personales o profesionales lo que está llevando a su adopción en múltiples áreas, desde el cuidado de la tercera edad y monitorización de pacientes a aplicaciones nóveles en áreas militares y de consumo.

Si bien no analizada usualmente como miembro de la PN, otra tecnología clave en la integración de capacidades computacionales y de comunicación en objetos cotidianos es la tecnología RFID (*Radio Frequency IDentification*, identificación por radiofrecuencia), la cual permite la identificación única de un objeto y la obtención de datos relacionados (ej. características o historial), gracias a la incorporación de un circuito miniaturizado (etiqueta RFID) en el objeto a controlar. De hecho, la tecnología RFID puede considerarse como un sensor adicional, donde en lugar de parámetros como temperatura o humedad, la red siente los objetos que se encuentran presentes y sus metadatos. Desde esta perspectiva, el lector RFID actúa como otro nodo sensor, que obtiene este tipo particular de datos sobre el contexto basado en el soporte de las etiquetas RFID.

La ITU describe la tecnología RFID como uno de los pivotes que habilitarán la venidera Internet of Things, convirtiendo los objetos cotidianos en objetos inteligentes [1], mientras la Comisión Europea espera que el uso de esta tecnología se multiplique por cinco durante la próxima década. Sin embargo, hay que tener en cuenta las amenazas potenciales a la privacidad y seguridad que puede generar su integración en objetos personales y documentación de los usuarios. Debido a esto, la comunidad investigadora ha dedicado notables esfuerzos a minimizar los riesgos de seguridad proporcionando un amplio rango de protocolos de autenticación mutua [2,3], esquemas de protección de la privacidad [4,5] y primitivas criptográficas ligeras [6,7] para esta tecnología con objeto de evitar accesos no autorizados a las etiquetas RFID personales, así como el seguimiento y perfilado del usuario.

Tal y como se presenta más tarde en este artículo, la integración segura de la tecnología RFID en la PN como tecnología de percepción del contexto complementa a las BSNs y proporciona notable beneficios al conocimiento y servicios potenciales de la PN. La seguridad de RFID como tecnología independiente está alcanzado un adecuado nivel de madurez gracias a los avances de investigación en los últimos años; sin embargo, su integración en el modelo de PN, interacción con otros recursos de la red, usuarios remotos y proveedores de servicio requiere un análisis de seguridad específico y una arquitectura de PN preparada para tales tecnologías heterogéneas. Aunque un creciente volumen de investigación se está enfocando a los paradigmas de PN con la propuesta de diversas arquitecturas de red [8,9,10], y los beneficios de la integración de redes de sensores y RFID ha motivado ya la propuesta de diversas arquitecturas en diferentes escenarios [11,12,13], ninguna de ellas ha introducido la integración segura de RFID y redes de sensores inalámbricas en PNs.

Este artículo expone los beneficios de la colaboración de RFID y tecnologías de sensores en redes PN, analiza como esta integración podría lograrse y define los fundamentos de una arquitectura de PN segura. Tal arquitectura permitiría

proporcionar diversas funcionalidades como registrar y mantener de forma segura las etiquetas personales como miembros de la PN, autenticar y autorizar tanto nodos PN como dispositivos remotos en sus solicitudes para acceder a estas tecnologías sensibles al contexto, proporcionar un túnel de comunicación segura con las entidades sin capacidad IP y asegurar el cumplimiento de las políticas de seguridad y privacidad en estas comunicaciones.

Este artículo está organizado de la siguiente forma. La Sección 2 muestra las ventajas y limitaciones de la integración de RFID y BSNs en las PNs. La Sección 3 presenta nuestro concepto de red personal y los tipos de nodos contemplados. La Sección 4 introduce los módulos de nuestra propuesta de arquitectura de PN segura. La Sección 5 analiza la gestión segura de nodos PN y comunicación con las tecnologías de contexto en la arquitectura. Finalmente, la Sección 6 concluye el artículo.

II. ADECUACIÓN DE LA INTEGRACIÓN DE RFID EN PNS

A pesar de que las BSNs proporcionan a la PN cierta consciencia sobre el contexto del usuario a través de los parámetros fisiológicos del propietario, sus actividades y entorno, la representación lograda de la realidad que le rodea no es completa y el conocimiento manejado por el sistema de información para monitorizar y dar soporte al usuario está abierto a otras contribuciones. La tecnología RFID complementa adecuadamente a la BSN. En particular, RFID mejora las características de la red en los siguientes aspectos:

- *Mayor alcance*: la extrema miniaturización de las etiquetas RFID, su habilidad para obtener energía durante el propio proceso de lectura y su bajo coste permite llevar las capacidades de computación y comunicación a un rango mayor de productos de consumo, mobiliario, elementos de infraestructura y objetos personales, incrementando sustancialmente la calidad y cantidad de datos manejados por la PN. Sin embargo, al mismo tiempo, tales objetos personales RFID sólo disponen de recursos altamente restringidos y criptografía ligera, incrementando los riesgos de seguridad y privacidad en la PN.
- *Detectar presencia*: la tecnología RFID permite reconocer la presencia de objetos individuales portados por el usuario o en su contexto, denotando información sobre las herramientas que el usuario tiene disponibles, su actividad actual y rango de acciones potenciales. Basado en esta información, la PN puede proporcionar información específica para apoyar al usuario, habilitar servicios de red, o lograr privilegios especiales en el entorno gracias a la posesión de llaves, equipamiento profesional, tarjetas de identificación u otros objetos distinguidos.
- *Características de los objetos personales*: las etiquetas RFID pueden proporcionar además del reconocimiento del objeto, metadatos sobre sus características. De esta forma, la PN puede incrementar su conocimiento sobre la situación donde el usuario está inmerso, así como capacidades y propiedades de los objetos accesibles, utilizando estos datos para mejorar sus servicios.
- *Registro de actividad en objeto*: la información mantenida en las etiquetas puede incluir también un registro sobre interacciones previas de los objetos personales con otros dispositivos y PNs, lugares donde el objeto ha estado, propietarios previos o hechos relevantes relacionados con el objeto. Este tipo de información histórica del objeto, definida y adaptada a las características específicas y propósito de cada tipo de objeto personal, incrementaría la calidad de los datos gestionados por la PN, así como la información forense recopilada para detectar nodos comprometidos, intrusiones o ataques.
- *Gestión transparente y segura de información personal*: una parte significativa de la información personal (incluyendo certificados de eventos personales, calificaciones académicas, documentos médicos o económicos, informes y estudios) se mantiene actualmente como documentación en papel. La integración de la tecnología RFID en la documentación personal proporcionará un enlace transparente con el mundo digital para un procesado ágil y automatizado de sus contenidos. Además, habilitará el uso de mecanismos de seguridad avanzados que han sido tratados extensamente tanto en documentación electrónica como en los primeros pioneros en documentación híbrida (ej. la extensa suite de mecanismos de seguridad en ePassport), sin sacrificar la fiabilidad y conveniencia del soporte físico.
- *Autenticación de usuario*: como beneficio adicional de la integración de RFID en documentación personal, la integración de esta tecnología en las tarjetas de identificación y documentación habilita la identificación segura y autenticación del usuario en su PN, en el contexto que rodea al usuario o incluso el acceso a redes y servicios remotos con mínima interacción del usuario.

Por lo tanto, la integración segura de RFID en la PN puede mejorar de forma sustancial los servicios relativos al contexto. Aunque la integración de las tecnologías de RFID y sensores aporta múltiples beneficios a la PN, la mayoría de etiquetas RFID sólo implementan criptografía ligera y muestran capacidades computacionales y de comunicación muy limitadas elevando potenciales riesgos de seguridad en la PN. Además, la heterogeneidad de recursos entre RFID, sensores y otros dispositivos personales muestran la necesidad de un modelo de comunicaciones seguro adecuado para la integración de las etiquetas personales en la arquitectura PN.

III. ARQUITECTURA HARDWARE DE RED PERSONAL

Nuestra visión del paradigma de red personal se centra en la definición de una arquitectura segura de red para la integración de la tecnología RFID en la esfera de nodos que rodea al usuario, el corazón de la PN, y la comunicación de este núcleo avanzado con dispositivos remotos (ej. clusters de dispositivos personales en localizaciones remotas, otras PNs o servicios centrales de monitorización). Al igual que en la literatura relacionada [9,10], consideramos una arquitectura de red centralizada donde el dispositivo maestro da soporte a las comunicaciones y gestión de la red, mientras proporcionamos un especial énfasis a la integración de dos tecnologías base para el reconocimiento del contexto: redes de sensores inalámbricas y RFID. En particular, consideramos los siguientes tipos de nodos (véase Fig. 1):

- *Dispositivo maestro*: sin restricciones computacionales y de memoria. El usuario interactúa con él

frecuentemente garantizando la recarga de su batería o incorpora técnicas de recolección de energía de forma que es posible asumir su estado operativo. Integra interfaces de comunicación para interactuar con redes de área extensa (ej. 3G/UMTS, LTE o WiMax) y es portado normalmente por el usuario. Aunque podrían surgir dispositivos concretos para desempeñar tal rol, los omnipresentes teléfonos inteligentes ya satisfacen este perfil.

- *Sensores inalámbricos*: recaban información sobre los parámetros fisiológicos del usuario y estado del contexto. Son posibles diversas características y localizaciones en el usuario y deben ser adaptadas al propósito y aplicaciones de la PN. La red podría incluir una estación base que gestione los nodos sensores y agregue la información, aunque dicha función podría integrarse en otro nodo de la red como el dispositivo maestro.
- *Etiquetas RFID*: múltiples tipos de tecnología RFID pueden coexistir en la PN. Por ejemplo, las etiquetas pasivas UHF EPC Gen2 son más adecuadas para objetos personales (ej. ropa, gafas o herramientas profesionales) cubriendo requisitos básicos de identificación y gestión de información, con un bajo coste por etiqueta y largas distancias de lectura. Por otra parte, la documentación personal requiere mecanismos criptográficos avanzados tales como los disponibles en las etiquetas pasivas HF basadas en ISO/IEC 14443. La tecnología RFID activa proporciona capacidades más avanzadas de computación y medición de características físicas, si bien, en la mayoría de escenarios consideramos que ésta puede ser sustituida por nodos sensores (ej. la familia Mica [14]) a medida que su coste se reduzca en el futuro.
- *Lector(es) RFID*: encargados de identificar y recuperar la información almacenada en los objetos personales. Pueden ser necesarios lectores multi-estándar para comunicarse con los diferentes tipos de tecnologías RFID. Los lectores UHF portables son capaces de acceder a los objetos personales en la esfera del usuario (radio aproximado de 2m) mientras los lectores pasivos HF (tales como los integrados en algunos modelos de teléfonos inteligentes [15,16]) requieren alta proximidad a las etiquetas durante el proceso de comunicación. En caso de que se requiera lectura a corta distancia, podría ser necesaria la notificación al usuario (a través de dispositivos de entrada/salida) para su interacción explícita en el proceso de comunicación.
- *Dispositivos de entrada/salida*: además de los omnipresentes *smartphone*, se prevé que emerjan otras tecnologías para PNs con objeto de proporcionar métodos no intrusivos para la entrada de datos (ej. paneles táctiles en ropa, brazaletes equipados con sensores) y presentación de la información (ej. gafas de realidad aumentada).
- *'Gadgets' o dispositivos avanzados*: diseñados para tareas específicas (ej. GPS, reproductores de música, cámaras digitales y dispositivos de juego). Pueden participar de forma no continua en la red habilitando servicios adicionales. Presentan recursos computacionales y de comunicación menos restringidos que las tecnologías ubicuas.

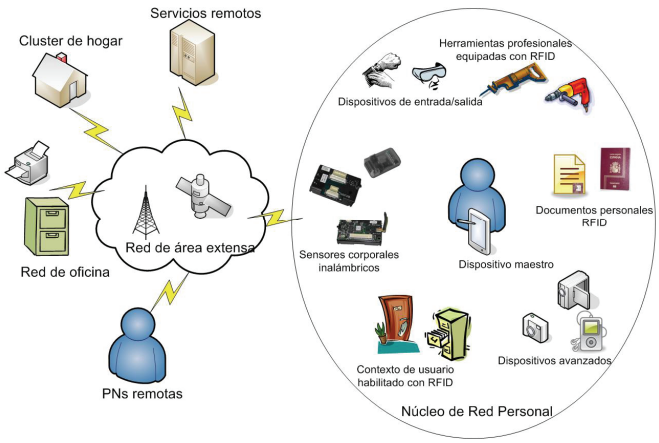

Fig. 1. Esquema de comunicaciones en la red personal

IV. COMPONENTES SOFTWARE EN LA ARQUITECTURA DE RED PERSONAL

Nuestra propuesta no es la primera contribución de una arquitectura software para PNs. En la literatura existente se ha trabajado ya en este área [8,9,10] proporcionando una arquitectura general para este novel paradigma de red que ya considera un amplio rango de aspectos de la gestión de red para dispositivos personales genéricos. Mientras estos trabajos previos proporcionan un adecuado soporte para el desarrollo de PNs, tales enfoques genéricos no analizan cómo lograr la integración segura de la tecnología RFID en la PN.

Las entidades remotas que requieran comunicarse con las etiquetas no pueden acceder a ellas directamente (las etiquetas RFID no poseen dirección IP y las entidades remotas requerirían localizar su ubicación actual en la PN y lectores RFID al alcance). Además, dada la potencial pérdida de información personal, debe poder garantizarse el cumplimiento de las políticas de privacidad del usuario en cualquier comunicación con dichos dispositivos. Debido a esto, la PN debería gestionar el direccionamiento y acceso seguro a etiquetas personales, asegurando el cumplimiento de los requisitos de seguridad en tales comunicaciones.

En la materialización de nuestra visión, la PN debe proporcionar soporte a la colaboración segura de los nodos heterogéneos que coexisten en la red, así como su interacción con entidades externas. Para lograr dicho objetivo, los dispositivos personales deben ser reconocidos como miembros de la PN, proporcionando mecanismos seguros para inicializar nuevos nodos o transferir la propiedad desde otras entidades. Los miembros de la PN y las entidades externas autorizadas deben disponer de las claves y credenciales actualizadas de la red, así como ser capaces de establecer comunicaciones seguras con otros nodos (incluyendo nodos basados en tecnologías de red incompatibles). Durante las comunicaciones, las entidades deben ser autenticadas y se debe asegurar el cumplimiento de las políticas de privacidad. Con objeto de lograr estos objetivos, proponemos una arquitectura de PN basada en los siguientes módulos y comportamiento (véase Fig. 2):

• *PN Members Database* (Base de datos de miembros): encargada de mantener una base de datos de los nodos que se reconocen como entidades de la PN. La base de datos debería mantener metadatos relativos a cada nodo único durante el tiempo que pertenezcan a la red, incluyendo direccionamiento (ej. IP, MAC, dirección PN), materiales criptográficos (ej. certificados digitales y claves), roles, niveles de reputación y privilegios.

• *Member Discovery and Maintenance Module* (Modulo de descubrimiento y mantenimiento de miembros): PN es un paradigma de red dinámico donde se necesita incorporar bajo demanda nuevos dispositivos personales, mientras los antiguos miembros de PN pueden cambiar de propietario, ser comprometidos o desechados. Este módulo gestiona del ciclo de vida seguro de los dispositivos asociados a PN, ya sea con una relación permanente o temporal en la red, incluyendo la incorporación a PN (es decir, proceso de inicialización, intercambio de claves y material criptográfico), actualización de claves y recursos, así como protocolos de desasociación.

• *Naming Resolution and Communication Management* (Resolución de nombres y gestión de comunicaciones): recibe las peticiones de miembros de PN o dispositivos remotos que desean comunicarse con un nodo de PN identificado por una convención de nombres reconocible. El módulo gestiona la solicitud resolviendo la identidad del nodo final, comprobando los privilegios del nodo solicitante (a través del módulo Authentication and Authorization Module), y transfiriendo la conexión al módulo de red apropiado (es decir, PN Routing o Secure Context Management).

• *Authentication and Authorization Module* (Módulo de autenticación y autorización): para (re)conectar a la PN y establecer conexiones a dispositivos de la red, tanto los miembros de PN como nodos remotos necesitan autenticarse en la red. Este módulo gestiona tal proceso y, en base a los privilegios de los nodos, proporciona autorización para futuras interacciones con los miembros de PN.

• *PN Routing* (Enrutamiento en PN): determina la ruta más adecuada para interconectar al solicitante (local o remoto) con la entidad solicitada de PN. La ruta tiene en cuenta la movilidad de los nodos en la red, así como la heterogeneidad en tecnologías de comunicación y capacidades computacionales con objeto de determinar la posición actual del nodo final e incluir los nodos proxy necesarios en la ruta.

• *Secure tunnel Manager* (Gestor de túnel seguro): se encarga de habilitar tales comunicaciones seguras entre los nodos finales, incluyendo el uso de proxies y pasarelas en PN que actúen como puente entre diferentes tecnologías de red, adaptando los mecanismos de seguridad empleados en cada conexión salto a salto con objeto de maximizar el nivel de seguridad de acuerdo a las capacidades de cada par de nodos.

• *Privacy policies and profile DB* (Base de datos de políticas de privacidad y perfiles): gestiona la información relativa al perfil del usuario, así como las políticas de privacidad que definen cómo se debe tratar su información personal y datos almacenados o generados por la PN.

• *Secure Context Management* (Gestión segura del contexto): encargado de gestionar la información generada por las tecnologías sensibles al contexto (es decir, redes de sensores y RFID). Esta información debe ser procesada de acuerdo a las restricciones de privacidad y seguridad deseadas por el usuario. Basado en esta entrada, se filtra, anonimiza y agrega la información de contexto en función de la entidad solicitante y sus privilegios de acceso.

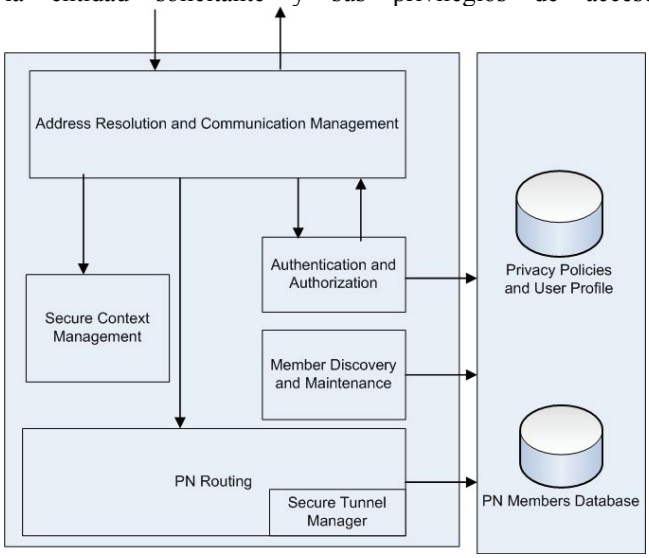

Fig. 2. Componentes software de la arquitectura de PN

En nuestro modelo de PN centralizado, el dispositivo maestro mantiene una posición distinguida disponiendo de una visión global de la red de dispositivos personales, y proporcionando interfaces externos a las redes de área extensa, así como una presencia previsiblemente continua en la red. Como resultado, la arquitectura completa de PN podría desplegarse en el dispositivo maestro que estaría encargado de las funciones de gestión de las comunicaciones en la red. Sin embargo, parte de los módulos de la arquitectura y sus funciones relacionadas podrían delegarse a otros dispositivos de la PN con capacidades computacionales y de comunicación adecuadas, así como una apropiada disponibilidad en la red. Por ejemplo, una estación base inalámbrica podría encargarse del módulo Secure Context Management o un dispositivo avanzado podría mantener PN Members Database o el repositorio de Privacy Policies and User Profile. Tal arquitectura de red distribuida podría definirse de forma estática, aunque nuevas propuestas podrían proporcionar mecanismos seguros para delegación dinámica de las funciones de PN en la red.

V. GESTIÓN SEGURA DE RFID Y NODOS SENSORES

La integración de la tecnología RFID en la PN requiere que se tengan en cuenta consideraciones específicas en cuanto a las funciones llevadas a cabo por los diferentes módulos de la arquitectura. A continuación, discutiremos cómo se puede lograr dicha integración, y los aspectos que han de ser contemplados en la arquitectura. En particular, analizaremos el descubrimiento y gestión de los objetos personales etiquetados, la comunicación segura con las tecnologías pervasivas y el cumplimiento de las políticas de seguridad y privacidad.

A. Descubrimiento y gestión de objetos RFID en la arquitectura

Como miembros de la PN, las etiquetas RFID personales deberían ser incluidas en la PN Members Database para saber qué etiquetas del contexto del usuario pertenecen a la red, y cómo autenticar y acceder a dichas etiquetas. La base de datos debe almacenar información de identificación como el código único de identificación (UID), esquemas de nombrado propios de PN, dirección IPv6 móvil como se propone en [18] o pseudónimos para esquemas de protección de la privacidad. De forma adicional, la base de datos debe mantener el material criptográfico de forma que los nodos autorizados puedan realizar con éxito los protocolos de autenticación mutua, acceder y actualizar sectores específicos de memoria o incluso desactivar las etiquetas.

En una situación ideal, el despliegue de una PN permitiría la selección de mecanismos de seguridad y protocolos de autenticación comunes para todas las etiquetas RFID empleadas en objetos personales. Sin embargo, las características hardware de las etiquetas RFID varían ampliamente de etiquetas básicas que se comportan como máquinas de estado a etiquetas avanzadas capaces de realizar criptografía de clave pública, coexistiendo así etiquetas basadas en diferentes ramas de RFID y protocolos de autenticación. Por lo tanto, la arquitectura PN (incluyendo la PN Members Database, o los módulos de Secure túnel manager y Authentication and Authorization) deberá estar preparada para gestionar los materiales criptográficos y protocolos requeridos por la etiquetas RFID adoptadas en la PN.

A medida que el usuario obtiene o despliega nuevos objetos equipados con RFID, las etiquetas han de ser reconocidas e incluidas en la esfera personal de forma segura. El proceso de incorporar una etiqueta RFID en la PN es gestionado por el módulo Member Discovery and Maintenance. En el caso de etiquetas RFID vírgenes, desplegadas específicamente para aplicaciones de la PN, deberá emplearse un protocolo de inicialización para intercambiar los materiales criptográficos adecuados con la etiqueta (ej. claves, pseudónimos, y/o certificados) y registrar la etiqueta en la PN Members Database. El mecanismo específico para identificar de forma segura la etiqueta y grabar los materiales criptográficos adecuados dependerá de los protocolos de autenticación seleccionados del amplio rango disponible en la literatura. El proceso de incorporación podría requerir interacción explícita del propietario de la PN con el nodo maestro (o algún otro miembro de la PN con capacidades de entrada/salida) con objeto de confirmar qué objetos etiquetados deberían ser aceptados como miembros de la red (ej. mediante selección por pantalla, o acercando físicamente el lector a la etiqueta) y participar en el establecimiento o generación de claves con un alto nivel de entropía (ej. moviendo un dispositivo equipado con acelerómetro o proporcionando una entrada por teclado).

Si la etiqueta es adoptada en la PN, podría requerirse el empleo de un protocolo de transferencia de propietario para obtener los permisos para gestionar de forma segura la etiqueta y regenerar su material criptográfico, pudiéndose adoptar y adaptar esquemas tales como [19][20] en el contexto de la PN. Sin embargo, nuevas propuestas de protocolos podrían tomar en consideración los servicios y recursos disponibles en la PN, la integración de ésta en redes de área extensa y la potencial interacción explícita del usuario con el fin de obtener la transferencia segura de etiquetas entre entidades distantes. En aquellos escenarios donde la etiqueta es necesaria aún en la aplicación original (ej. productos en garantía, o documentos de identificación privados o públicos), el objetivo del proceso de incorporación podría derivar en la compartición de la propiedad de forma segura [21].

B. Acceso seguro a sensores y nodos RFID

El módulo de Naming and Connection Management tiene una particular importancia en el acceso a las etiquetas RFID dado que permite emplear un pseudónimo o esquema de nombrado de la PN en lugar del identificador físico reconocido directamente por la etiqueta. Más aún, el módulo PN Routing libera al nodo solicitante de la necesidad de conocer el camino hasta el lector RFID en cuyo rango de lectura se encuentre la etiqueta. En nuestra visión, un miembro de la PN o un dispositivo remoto podría estar interesado en la información provista por una etiqueta RFID de dos formas posibles:

- *Acceso directo*: el dispositivo desea establecer una comunicación directa con la etiqueta con objeto de identificar el objeto, autenticarlo, actualizar su memoria o extraer información específica.
- *Conocimiento agregado*: el dispositivo requiere obtener consciencia sobre el contexto en el que el usuario se encuentra inmerso. Para su conveniencia, dicho conocimiento puede representarse mejor mediante la agregación de la información provista por los diferentes objetos personales etiquetados y sensores, en lugar de acceder directamente a cada nodo y componer el contexto por si mismo.

Nuestra arquitectura se encuentra preparada para gestionar ambos tipos de requisitos de interacción. En el caso de peticiones de acceso directo, el solicitante es requerido en primer lugar a autenticarse en la PN y obtener autorización para dicho acceso, tras esto, los módulos de nombrado y direccionamiento son responsables de resolver la identidad de la etiqueta, así como su ubicación actual en el seno de la PN y proporcionar una ruta adecuada para alcanzarlo. Si se requiere llevar a cabo una comunicación segura, el submódulo Secure Tunnel Manager participa en el establecimiento de un túnel desde el punto de acceso de la PN hasta el lector RFID próximo a la etiqueta solicitada o, en caso de que los nodos intermedios no sean capaces de participar en dicho túnel, crear enlaces seguros salto a salto dentro de la PN con objeto de maximizar la seguridad del canal extremo-a-extremo de acuerdo a los recursos computacionales y de comunicación de cada nodo en la ruta.

Por otra parte, si se desea hacer uso del conocimiento agregado, tras la autenticación y autorización inicial se emplea el módulo Secure Context Management para proporcionar la información de contexto requerida sobre los parámetros físicos del entorno y objetos personales cercanos. La información relativa al contexto es recopilada y procesada por el módulo como procedimientos en segundo plano que a su vez hacen uso de los servicios de nombrado y direccionamiento seguros proporcionados por la PN. Estos

procedimientos pueden ser iniciados directamente por una petición al módulo o tener lugar periódicamente, desacoplando las consultas de las comunicaciones seguras que realmente tienen lugar con los nodos sensores y RFIDs.

El mecanismo de acceso directo permite al nodo solicitante controlar la comunicación con la etiqueta final a bajo nivel, con objeto de leer o actualizar información específica. Este enfoque es muy adecuado, por ejemplo, en la interacción de entidades remotas con documentación personal RFID para autenticar al propietario de la PN e incluso obtener pruebas no repudiables de interacción con la PN.

Sin embargo, en este caso el control del cumplimiento de los requisitos de seguridad y las políticas de privacidad proporciona un bajo grado de granularidad. Las peticiones y comandos enviados a la etiqueta pueden ser bloqueados o enviados, pero, sin mayor filtrado y procesado de la información directa intercambiada, no es posible ajustar adecuadamente la granularidad de la información personal transmitida. En este caso, los mecanismos de autorización podrían ser reforzados incrementando los requisitos a cumplir por el nodo solicitante antes de que se le otorguen privilegios de acceso directo, dado que la información transmitida a bajo nivel podría potencialmente contener información sensible. La Sección 5.C proporciona una discusión más detallada sobre las alternativas posibles en el acceso directo.

Por otro lado, el acceso mediante conocimiento agregado proporciona un mayor control del cumplimiento de los requisitos de seguridad y privacidad deseados realizando un filtrado de los datos generados por las tecnologías sensibles al contexto, anonimizando los nodos origen de la información antes de que la información sea presentada a la entidad solicitante. Por lo tanto, este mecanismo permitiría reducir los requisitos sobre el nodo solicitante (ej. niveles de reputación o privilegios explícitos otorgados al usuario) para autorizar la interacción del solicitante con el módulo de Secure Context Management, responsabilizando a este último de asegurar la privacidad de los datos personales finalmente mostrados, a costa de reducir la flexibilidad del nodo solicitante en su interacción con las entidades finales de la red y requerir a la PN tareas adicionales de procesado. La Sección 5.D proporciona discusión adicional sobre el uso de las políticas de privacidad en la arquitectura de PN.

C. Alternativas en el acceso directo seguro a nodos RFID

En el enfoque de acceso directo, una entidad remota o local solicita establecer una comunicación con un nodo específico de la PN (estación base, nodo sensor, nodo RFID o dispositivo avanzado). Mientras el módulo de enrutamiento podría proporcionar una ruta directa a nodos PN que incorporen conectividad IP (incluyendo nodos sensores [22]), uno o más nodos proxy serán necesarios en caso de dispositivos basados en tecnologías de comunicación incompatibles o recursos computacionales y criptográficos extremadamente restringidos.

En particular, en el caso de etiquetas RFID personales que carecen de pila TCP/IP e incorporan recursos de comunicación, computación y memoria muy reducidos, el modo de acceso directo (para lectores RFID no locales) requiere del uso de nodos proxy que establezcan un puente entre las diferentes tecnologías de comunicación y reenvíen las consultas y comandos del nodo solicitante a la etiqueta final. Estos nodos pasarela deberían tener también un rol predominante para asegurar el cumplimiento de las políticas de seguridad y privacidad durante la comunicación con las etiquetas RFID.

En el enrutamiento seguro de las comunicaciones de acceso directo a las etiquetas RFID personales, se podrían adoptar las siguientes alternativas (véase Fig. 3):

• *Nodo proxy como repetidor de comandos*: tras la autenticación del nodo solicitante, resolución y localización de la etiqueta a acceder, se establece un túnel seguro desde el nodo remoto al lector RFID en rango de lectura. Uno o más nodos proxy participan en la ruta, sin embargo, los enlaces de comunicación seguros entre las entidades son empleados únicamente para retransmitir la comunicación entre las entidades extremo.

En este caso, la entidad remota debe conocer la tecnología RFID concreta de la etiqueta y enviar comandos que sean compatibles con dicha entidad final. El lector RFID o nodo inteligente más próximo a la etiqueta extrae los comandos recibidos a través del canal seguro y los envía a la etiqueta personal. Tras su respuesta, se encapsula el mensaje proveniente de la etiqueta RFID y se envía de vuelta al dispositivo remoto a través del túnel.

En este esquema, el nodo solicitante es además responsable de completar el protocolo de autenticación (mutua) con la etiqueta, debiendo conocer o ser capaz de obtener el material criptográfico necesario (ej. claves o certificados digitales). En caso de que la etiqueta adoptada en la PN pertenezca a una aplicación exterior (ej. etiquetas

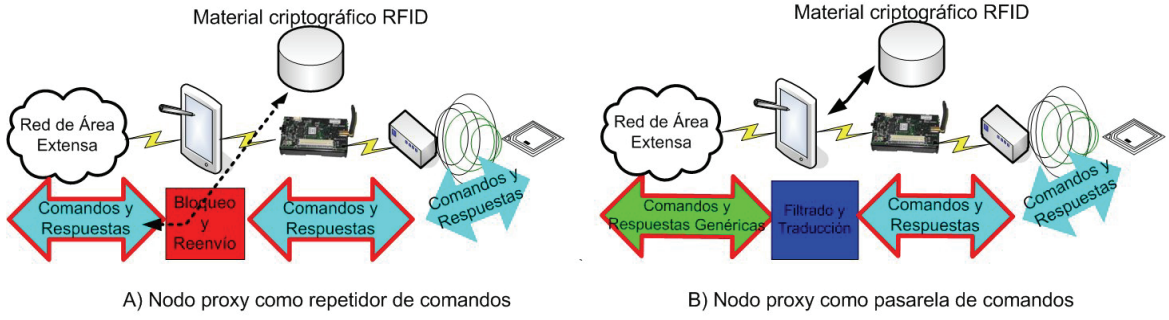

Fig. 3. Alternativas en el acceso directo seguro a nodos RFID

RFID en documentación personal privada o gubernamental), el solicitante podría obtener los materiales criptográficos de terceras partes (ej. un servidor de gestión de claves RFID [23]). En caso contrario, la PN podría directamente proporcionar tales materiales a la entidad solicitante una vez autenticado en la PN. En el último caso, la PN sería responsable de refrescar las claves involucradas por medio del módulo Member Discovery and Maintenance (ej. una vez la comunicación ha finalizado o de forma periódica) con objeto de prevenir futuras comunicaciones no autorizadas.

Dado que los comandos directos se envían a la etiqueta, la PN tiene un bajo control sobre la información personal o privada recuperada o modificada por el solicitante; sin embargo, podría otorgarse un rol adicional a un nodo proxy en la ruta (ej. el dispositivo maestro o el lector RFID) con objeto de analizar el flujo de tráfico y bloquear aquellos mensajes que no se ajusten a las políticas de seguridad.

- *Nodo proxy como pasarela de comandos*: un nodo pasarela en la ruta segura entre solicitante y etiqueta permite intermediar y traducir la comunicación entre ambas entidades. En este caso, el solicitante no requiere conocer el estándar RFID en que se basa la etiqueta, sus características de memoria, comandos compatibles o materiales criptográficos para llevar a cabo la autenticación (mutua) con la etiqueta personal. El solicitante enviaría sus comandos en base a un conjunto normalizado de operaciones para etiquetas RFID genéricas, mientras el nodo pasarela sería responsable de traducir los comandos específicos que serán enviados a la etiqueta RFID, así como interpretar y traducir las respuestas proporcionadas por la etiqueta.

En esta solución, el solicitante sólo necesita mantener las credenciales para autenticarse en la PN. La pasarela se encargaría de recopilar los materiales criptográficos necesarios a través de los mecanismos provistos por la PN y de llevar a cabo la autenticación (mutua) con la etiqueta personal, liberando por tanto a la entidad solicitante del proceso de autenticación doble y de la gestión de credenciales de los nodos individuales de la PN. La gestión segura de las etiquetas personales también se beneficiaría de esta solución dado que los materiales criptográficos necesarios en las comunicaciones internas a la red no se transmiten a entidades externas. Además, es posible obtener un mayor control durante la comunicación 'directa' con la etiqueta habilitando una supervisión más adecuada de las operaciones y datos transferidos (ej. comandos enviados o zonas de memoria) con objeto de comprobar la sensibilidad de los datos, privilegios del solicitante y asegurar el cumplimiento de las políticas de seguridad.

Aunque se mejora la seguridad y privacidad en la PN con esta solución, este enfoque podría no satisfacer aquellos escenarios en los que la entidad solicitante requiera un control más detallado del proceso de comunicación con la etiqueta personal (ej. durante la autenticación y validación de documentos personales RFID).

El rol de pasarela podría ser asumido tanto por el interfaz exterior de la PN (ej. el dispositivo maestro) como por el lector RFID o nodo inteligente que envía los comandos finales. El primero permitiría analizar y filtrar solicitudes inadecuadas en el punto mismo de entrada a la red, por lo tanto controlando la propagación de mensajes no deseados y previniendo posibles ataques potenciales (ej. mensajes mal formados) así como mejorando el uso de recursos de red (ej. batería y ancho de banda); mientras que el segundo enfoque permitiría concentrar las funcionales RFID (tales como formación de mensajes correctos y conocimiento de protocolos empleados) en las entidades de red directamente relacionadas.

D. Políticas de privacidad

Las políticas de privacidad tendrán un rol clave en la integración de la tecnología RFID en la PN. Estas políticas deberían de ser suficientemente flexibles para gestionar el ecosistema de elementos personales etiquetados, dado que estos podrán pertenecer a un amplio rango de categorías y tipos de objetos, así como la potencial diversidad de dispositivos remotos personales o profesionales y proveedores de servicios que pueden requerir acceso a las etiquetas personales y su información asociada. En este contexto, las políticas de privacidad deberían de proporcionar un mecanismo para representar qué categorías o etiquetas individuales mantienen información privada, cuáles no representan un riesgo a la privacidad, en qué condiciones es posible proporcionar acceso público o restringido a los actores seleccionados, e incluso qué datos personales deberían ser filtrados y desasociados de las fuentes donde se generaron antes de ser compartidos con entidades remotas.

En el caso de acceso directo a etiquetas individuales por parte de actores externos, se podrían emplear mecanismos de control de acceso (ej. ACL o RBAC) para definir a qué actores se les permite ejecutar qué comandos sobre qué etiquetas. Se podrían emplear parámetros adicionales relativos al contexto del usuario en las políticas de acceso (ej. localización, actividad actual u otras PN en el entorno).

En el caso de solicitudes de conocimiento agregado, la solución podría estar también basada en estas técnicas, pero en este caso, los elementos a acceder serían los tipos de conocimiento agregado que la PN es capaz de generar tras procesar y filtrar la información, en lugar de las instancias particulares de sensores y etiquetas RFID.

En la literatura, una solución relevante en esta dirección es el dispositivo RFID Guardian que mantiene una política de seguridad centralizada definiendo qué lectores RFID están autorizados a acceder a qué etiquetas en qué condiciones. El dispositivo logra su propósito intercediendo en el proceso de comunicación y llevando a cabo tácticas de simulación de etiquetas para bloquear lectores no autorizados. A pesar de ser un buen punto de comienzo, dicho dispositivo es un claro ejemplo de las soluciones de seguridad existentes en la literatura sobre RFID: no se integra en una PN y únicamente considera a las etiquetas RFID como una tecnología aislada, sin tener en consideración la información generada por otras tecnologías tales como BSNs ni evaluar el contexto del usuario. Además, se centra en el acceso local a las etiquetas RFID por lectores que se encuentran físicamente próximos al usuario, y no considera la integración de los dispositivos personales en redes de área extensa y las comunicaciones con PNs o proveedores de servicio remotos.

Nuestra visión integrada de la tecnología RFID en la PN tiene en consideración ambos aspectos y proporciona la base arquitectural para acceder de forma segura a estas

tecnologías también desde Internet, dejando la puerta abierta al desarrollo de políticas de privacidad específicas para este contexto.

VI. Conclusiones

La PN podría beneficiarse de la integración de los objetos personales habilitados con RFID, sin embargo, sus especiales características (ej. pasividad, no direccionamiento IP, reducidos recursos de comunicación y computación) y los riesgos potenciales a la seguridad y privacidad hacen que sea necesaria una arquitectura de PN preparada para soportar tales tecnologías pervasivas.

En este artículo, hemos definido las bases de una arquitectura de PN adecuada para dicho propósito. En nuestro modelo, las etiquetas personales deberían ser reconocidas como nodos de la PN, manteniendo tanto los materiales criptográficos relacionados como información sobre direccionamiento y metadatos, junto con posible información sensible que habilite el acceso e interacción segura con otros miembros y entidades externas. El despliegue e integración desde sus inicios de los objetos etiquetados en la PN permitiría la selección y definición de un conjunto común de protocolos de autenticación que estandaricen la gestión de etiquetas personales. Sin embargo, desde una perspectiva más práctica, la PN debería soportar la adopción de etiquetas heterogéneas e incorporar mecanismos para la transferencia y compartición segura de propiedad.

La arquitectura controla asimismo la autenticación y autorización de las entidades antes de otorgar privilegios en la red y habilitar las comunicaciones. En nuestro enfoque, las peticiones relativas a las tecnologías pervasivas restringidas en recursos (ej. RFID) pueden ser provistas de dos formas: acceso directo a los nodos finales e información agregada relativa al contexto. Como se ha discutido previamente, cada enfoque presenta sus propios beneficios y dificultades y deberían ser tratados de forma independiente, mediante la gestión segura del contexto y esquemas de acceso directo.

En el acceso directo, la PN ha de resolver y establecer una ruta segura para alcanzar el nodo final, incluyendo etiquetas RFID no basadas en IP. Como se ha mostrado, el rol de los nodos proxy como retransmisores de mensajes o nodos pasarela tiene un impacto sobre los requisitos aplicables al nodo solicitante y el cumplimiento de los requisitos de seguridad. Por último, las políticas de seguridad tienen un rol crucial en la PN y deben ser capaces de representar qué miembros de la PN y entidades externas son capaces de acceder a nodos de contexto o tipos de conocimiento en determinadas situaciones.

La investigación previa en aspectos tales como la integración de RFID y sensores, seguridad en RFID, transferencia segura de propietario o esquemas de control de acceso en RFID pueden ser adoptadas a este propósito proporcionando las bases para la realización de dicha arquitectura. Sin embargo, en lugar de analizarlas como tecnologías aisladas, una visión global de tales como componentes de la heterogénea PN, centrada en el usuario, e integrada en Internet, abre una puerta a la propuesta de soluciones específicamente diseñadas para los requisitos y recursos de este emergente paradigma.

Agradecimientos

Este trabajo ha sido financiado parcialmente por la Comunidad Europea a través de NESSoS (FP7-256890) y por el Ministerio de Ciencia a través de ARES (CSD2007-00004) y SPRINT (TIN2009-09237), el último cofinanciado por fondos FEDER. El primer autor ha sido financiado por el Ministerio de Educación a través del Programa F.P.U.

Referencias

1. International Telecommunication Union, ITU Internet Reports: The Internet of Things, November 2005.
2. Yum, D. H. et al., Distance Bounding Protocol for Mutual Authentication, IEEE Transactions on Wireless Communications, pp. 592-601, 2011
3. Piramuthu, S. RFID Mutual Authentication Protocols, Decision Support Systems, Elsevier (In press), 2010.
4. Armknecht, F. et al. Impossibility Results for RFID Privacy Notions, Transaction on Computational Science XI (6480), 2010, pp. 39-63.
5. Alomair, B. and Poovendran, R. Privacy versus Scalability in Radio Frequency Identification Systems, Computer Communication, 2010.
6. Peris-Lopez, P. et al., Cryptographic Puzzles and Distance-bounding Protocols: Practical Tools for RFID Security, 'IEEE International Conference on RFID 2010', Orlando, USA, 2010, pp. 45-52.
7. Kavun, E. B. and Yalcin, T., A Lightweight Implementation of Keccak Hash Function for Radio-Frequency Identification Applications, in RFIDSec'10, Springer, Istanbul, Turkey, 2010, pp. 258-269.
8. Anggraeni, P. N., Prasad, N. R. and Prasad, R. Secure personal network, Personal, Indoor and Mobile Radio Communications, IEEE 19th International Symposium on, 2008, pp. 1-5.
9. Ibrohimovna, M., et al., Secure and Dynamic Cooperation of Personal Networks in a Fednet, 6th IEEE CCNC 2009, pp. 8 -14.
10. Project IST-FP6-IP-027396, Magnet Beyond, http://magnet.aau.dk, last accessed: March 2011
11. Anggorjati, B., et al., RFID Added Value Sensing Capabilities: European Advances in Integrated RFID-WSN Middleware, 7th IEEE Conference on SECON 2010, pp. 1 -3.
12. Xiaoguang, Z. and Wei, L. The research of network architecture in warehouse management system based on RFID and WSN integration, IEEE International Conference on ICAL 2008, pp. 2556 -2560.
13. Tolentino, R. S., et al., Next Generation RFID-Based Medical Service Management System Architecture in Wireless Sensor Network, in Communication and Networking, Springer Berlin Heidelberg, 10.1007/978-3-642-17587-9_17, 2010, pp. 147-154.
14. Memsic WSN product family, http://www.memsic.com/products/wireless-sensor-networks.html, last accessed: March 2011
15. NFC-enabled Google Nexus S, http://www.google.es/nexus/#/tech-specs, last accessed: March 2011
16. NFC-enabled Nokia smartphones, http://www.nearfieldcommunicationsworld.com/2010/06/17/33966/all-new-nokia-smartphones-to-come-with-nfc-from-2011/, last accessed: March 2011
17. Yang, H., Yang, L. and Yang, S.-H., Hybrid Zigbee RFID sensor network for humanitarian logistics centre management, Journal of Network and Computer Applications (In Press), 2010.
18. Dominikus, S. and Schmidt, J.-M. Connecting Passive RFID Tags to the Internet of Things, 'Interconnecting Smart Objects with the Internet Workshop', Prague, Czech Republic, 2011.
19. Yu Ng, C., Susilo, W., Mu, Y. and Safavi-Naini, R. Practical RFID Ownership Transfer Scheme, Journal of Computer Security - Special Issue on RFID System Security, 2010.
20. Song, B. and Mitchell, C. J. Scalable RFID Security Protocols supporting Tag Ownership Transfer, Computer Communication, Elsevier, 2010.
21. Kapoor, G. et al. Single RFID Tag Ownership Transfer Protocols, IEEE Transactions on Systems, Man, and Cybernetics, 2011, pp. 1-10.
22. Mulligan, G., The 6LoWPAN architecture, 4th workshop on Embedded networked sensors, ACM, New York, NY, USA, 2007, pp. 78-82.
23. Najera, P., Moyano, F., Lopez, J., Security Mechanisms and Access Control Infrastructure for e-Passports and General Purpose e-Documents, Journal of Universal Computer Science, 15, 2009,970-991.