R. Roman, J. Lopez, and J. Zhou, "Análisis de Seguridad en Redes Inalámbricas de Sensores", *V Jornadas de Ingenería Telemática (JITEL05)*, pp. 335-343, 2005.
NICS Lab. Publications: `https://www.nics.uma.es/publications`

Análisis de Seguridad en Redes Inalámbricas de Sensores

Rodrigo Román Castro[1], Javier López Muñoz[1], Jianying Zhou[2]
[1] E.T.S. Ingeniería Informática, Universidad de Málaga, 29071 - Málaga
[2] Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore 119613
roman@lcc.uma.es, jlm@lcc.uma.es, jyzhou@i2r.a-star.edu.sg

Abstract *The design and development of security infrastructures and protocols for Wireless Sensor Networks is a difficult task, due to several factors like the constraints of the sensor nodes and the public nature of the communication channels. The intrinsic features of these networks create numerous security problems. In this paper, we analyze and put into perspective those problems.*

1. Introducción

Las redes inalámbricas de sensores (Wireless Sensor Networks) [1] están compuestas por cientos o miles de dispositivos (nodos) equipados con sensores (temperatura, sonido, movimiento,...) y con una capacidad limitada de comunicación y cálculo. Estas redes permiten a los sistemas informáticos acceder y procesar a distancia información procedente del mundo real.

Los campos de aplicación de las redes de sensores son muy variados (Salud, Entornos Inteligentes,...), y están creciendo día a día. Actualmente, los usos más comunes de este tipo de redes incluyen la monitorización de espacios naturales, la seguridad en la construcción y mantenimiento de edificios, la vigilancia de espacios protegidos, y el control de maquinaria industrial.

Sin embargo, las redes de sensores son extremadamente vulnerables ante cualquier tipo de ataque, tanto interno como externo. Esto es debido a factores tales como las limitaciones de los nodos, su falta de protección ante ataques físicos, y la facilidad de acceso al canal de comunicaciones. En este contexto, todo protocolo, arquitectura, o aplicación que no tome en cuenta la seguridad desde las primeras fases de su desarrollo difícilmente podrá ser utilizado en la vida real.

El objetivo de este artículo es el de analizar los problemas de seguridad en redes de sensores, dando además una perspectiva de algunas de las soluciones que actualmente se pueden aplicar, pero que en muchas ocasiones no son las óptimas. La estructura del artículo es la siguiente: En la sección 2, se muestra la infraestructura y los elementos que componen una red de sensores inalámbrica. La sección 3, que es el núcleo de este trabajo, analiza los distintos problemas de seguridad asociados con este tipo de redes, tales como el uso de primitivas de seguridad, la infraestructura de claves, el encaminamiento de información, etc. Finalmente, la sección 4 finaliza el artículo discutiendo los principales retos de seguridad actuales.

2. Infraestructura de Redes de Sensores

La infraestructura de una red de sensores se divide en dos partes, la *red de adquisición de datos* y *la red de diseminación de datos.*

- La red de adquisición de datos es la Red de Sensores propiamente dicha. Esta formada por un conjunto de nodos cuya tarea es la de medir, procesar y reenviar los datos físicos de sus alrededores, y por una o más estaciones base (Base Station) a cargo de recoger los datos procedentes de los nodos y de enviarles información de control procedente de los usuarios.

- La red de diseminación de datos es un conjunto de redes, tanto inalámbricas como basadas en cables, que proporcionan a cualquier usuario una interfaz con la que interactuar con la red de sensores. La seguridad de esta red esta fuera del alcance de este artículo.

Los nodos están densamente distribuidos o muy cerca o en el interior del objeto u entorno que desea observarse, y las medidas realizadas deben enviarse hacia la estación base donde los usuarios puedan acceder a ellas. Todos estos nodos son dispositivos con unos recursos (memoria, capacidad computacional, batería) muy limitados. Por otro lado, las estaciones base no poseen tantas restricciones como los nodos, y suelen tener un suministro continuado de energía.

Actualmente, el modelo de nodo más popular es el MICA2 [2]. Éste utiliza un procesador de 8 Mhz con 128Kb de memoria de instrucciones, 4Kb de RAM, y 512Kb de memoria flash para almacenamiento de datos. Su transmisor de radio le permite enviar 19.2Kb/s en un canal compartido, y su batería le permite trabajar de forma ininterrumpida hasta 2 semanas, aunque es posible mantenerlo en funcionamiento durante 1 año.

Debido a las limitaciones de su infraestructura, una red de sensores es extremadamente vulnerable ante cualquier tipo de ataque, tanto procedente del exterior (inyección de paquetes) como del interior (un nodo controlado por un adversario). Por lo tanto, es necesario que tanto la infraestructura como los protocolos de la red estén preparados para afrontar este tipo de situaciones adversas. Proteger la información no solo requiere de un conjunto de algoritmos eficientes de cifrado, sino de una política óptima de manejo de claves en términos de distribución, almacenamiento y mantenimiento. Además, es necesario proteger la agregación de datos dentro un grupo (estático o dinámico) de nodos y su encaminamiento hacia la estación base. Finalmente, entre otras cosas, la red debería ser capaz de monitorizar errores o brechas de seguridad en cualquiera de sus miembros y responder ante estas circunstancias de forma automática.

3. Seguridad y Redes de Sensores

3.1. Primitivas de Seguridad

Los nodos que forman parte de una red de sensores utilizan transmisores de radio para sus comunicaciones. Todos los nodos existentes en el mercado operan en bandas de frecuencia que no necesitan de licencia, sean los 433 Mhz (el espectro más bajo de las bandas ISM en Europa) o las bandas utilizadas en el estándar IEEE 802.15.4 para redes de área personal (PAN) [3]. La capacidad máxima del canal de comunicación oscila entre 19.2 Kbps y 250 Kbps.

Cualquier adversario puede acceder a la información procedente de una red de sensores, debido a que los nodos están (normalmente) distribuidos en un entorno de fácil acceso, y los canales de comunicación inalámbricos son inherentemente inseguros. En consecuencia, cualquier dispositivo puede escuchar o inyectar paquetes en la red de sensores.

Es por lo tanto indispensable incluir unas primitivas de seguridad dentro de los nodos para así proporcionar tanto una mínima protección al flujo de información como una base para la creación de protocolos seguros. Esas primitivas de seguridad son la *criptografía de clave simétrica* (SKE), los *códigos de autenticación de mensajes* (MAC), y la *criptografía de clave pública* (PKC). Debido a la escasez de recursos disponibles en los nodos, implementar estas primitivas de seguridad de una forma eficiente (usando menos energía, memoria y ciclos de CPU) sin sacrificar sus propiedades de seguridad es todo un reto.

Los nodos comerciales disponibles actualmente son capaces de implementar SKE a nivel software de una forma eficiente en términos de CPU, memoria y energía. Un ejemplo es el proyecto TinySec [4], librería criptográfica incluida dentro del sistema operativo TinyOS. TinySec es capaz tanto de autenticar y verificar la integridad de un mensaje como de proteger su confidencialidad, o ambas, utilizando cifrados de bloque como Skipjack o RC5 en modo CBC. En todos los casos el gasto de energía, ancho de banda y CPU es menor del 10 %.

En nodos cuya radio funcione de acuerdo al estándar 802.15.4 [3] la SKE la proporciona el hardware, quitando carga a la CPU y disminuyendo el uso de energía del nodo. En éste estándar, una aplicación puede elegir entre varias "suites" de seguridad que proporcionan (juntas o por separado) cifrado, autenticación y protección contra el reenvío utilizando el algoritmo AES. No obstante, no todos estos modos de funcionamiento son seguros [5], por lo que los diseñadores de aplicaciones deben tener cuidado al usar el estándar.

Respecto al MAC, éste se suele calcular utilizando algoritmos de cifrado en bloque, en un modo especial denominado CBC-MAC. Este modo es eficiente y rápido, y además permite reducir la cantidad de memoria requerida para implementar el MAC al compartir el algoritmo de cifrado en bloque con los demás módulos criptográficos del nodo, sean éstos software [4] o hardware [3].

En el contexto de las redes de sensores, la inclusión de PKC en un nodo utilizando software se consideraba imposible, pero no existían experimentos que demostraran esa presunción. Algunos estudios apuntaron a la criptografía de curva elíptica (ECC) como una posible solución aplicable a las redes de sensores, debido al reducido tamaño de sus claves, la rapidez de cálculo de sus primitivas, y los ahorros en energía y memoria en comparación con otros algoritmos como RSA.

Finalmente, un trabajo reciente en este área [6] desarrolló una implementación de PKC en TinyOS. Ésta utiliza ECC sobre $\mathbb{F}_{2^p}$ con una longitud de clave de 163 bits, con un gasto de memoria de 1Kb de RAM y 34Kb de ROM, y con un tiempo de ejecución de 34 segundos tanto para la generación de claves como para la generación de una clave secreta compartida.

3.2. Infraestructura de Claves

Los canales de comunicación entre dos nodos cualesquiera de la red de sensores deben estar protegidos para evitar ataques procedentes de agentes externos a la red. Esta protección la proporcionan las primitivas de seguridad introducidas en la sección anterior, pero para su uso es necesario que cada nodo pueda disponer de una serie de claves. Es por tanto necesario desarrollar una infraestructura de claves.

Existen tres factores básicos en el diseño de una infraestructura de claves para redes de sensores: almacenamiento, distribución, y mantenimiento de claves.

- Las políticas de almacenamiento indican el número de claves que un nodo necesita almacenar para abrir un canal de comunicación seguro con otros miembros de la red. Influye sobre la solidez de la red (network resilience), que define el porcentaje de la red que puede ser controlado por un adversario después de que éste obtenga las claves de un subconjunto de los nodos, y también influye sobre la cantidad de memoria disponible para el nodo.

- Los protocolos de distribución definen como se distribuyen las claves a los diversos nodos. Un nodo puede recibir sus claves antes de incorporarse en la red de sensores, o crear sus claves después (dentro de la red) utilizando información previamente almacenada.

- Los protocolos de mantenimiento especifican como un nodo puede incluirse o eliminarse de la red de sensores, recibiendo una serie de claves o anulando el uso de las que ya disponía. Este área de la infraestructura de claves no se encuentra muy desarrollada.

Respecto al almacenamiento de claves, existen dos casos extremos de diseño: *modo de clave global* (global keying) y *modo de clave por parejas* (pairwise keying). En el modo de clave global, existe una sola clave que todos los nodos poseen e utilizan para cifrar sus canales de comunicación. En el otro modo, clave por parejas, un nodo debe almacenar una clave por cada uno de los otros nodos existentes en la red, de tal forma que cada par de nodos compartirá un canal seguro específico.

Ninguno de los casos anteriores es viable en la mayoría de los escenarios posibles. El modo de clave global no proporciona solidez a la red, ya que si un solo nodo revela su clave a un adversario, todas las comunicaciones de la red se verán comprometidas. Y el modo de clave por parejas no es una solución escalable, debido a las restricciones de memoria de los nodos. Por esta razón se han estado buscando soluciones más óptimas, tales como compartir claves únicamente entre vecinos, o el paradigma de los conjuntos de claves (key pools).

El paradigma de los conjuntos de claves, introducido en [7], busca obtener un equilibrio entre el número de claves distribuidas en cada nodo y la solidez de la red. En este paradigma todos los nodos recogen un número determinado de claves de un conjunto global, creando conjuntos locales, antes de ser incluidos en la red de sensores. Después, solo los nodos que compartan una clave (o un número determinado de claves) de sus propios conjuntos pueden abrir un canal seguro de comunicación. El tamaño del conjunto global y de cada conjunto local son factores que influyen en la memoria disponible de los nodos y en la conectividad y la solidez de la red.

Este paradigma ha sido mejorado posteriormente, buscando optimizar o la construcción del conjunto global o la distribución de las claves hacia los conjuntos locales, de tal forma que la conectividad de la red sea cercana al 100 % (cada nodo pueda comunicarse con su vecino directo) mientras se disminuye el tamaño de los conjuntos locales y se aumenta la solidez de la red. Existen varias soluciones que logran este objetivo, sean basadas en principios matemáticos (como el esquema de Bloom [8] o la teoría combinatoria [9]), o aprovechando información obtenida "a priori" respecto a la distribución física de los nodos en la red de sensores [10].

Otros protocolos son capaces de negociar las claves de un nodo una vez que éste se haya sido incorporado a la red de sensores. En una de las soluciones un nodo negocia las claves que compartirá con sus vecinos más directos a través de la estación base [11], aunque este método puede no ser escalable. En otro modelo más simple, cada nodo contacta con sus vecinos y negocia las claves justo después de la construcción de la red [12]. En este modelo no se protege el intercambio de información, ya que en la mayoría de los escenarios no existe ninguna amenaza en el momento de la creación de la red de sensores.

Un área que aún esta inexplorada es el uso de criptografía de clave pública para la negociación de claves entre pares de nodos. Ya que es posible utilizar PKC en redes de sensores [6], queda por investigar como aplicarla en la creación e intercambio de claves y en los protocolos de mantenimiento de claves.

3.3. Infraestructura de Clave Local - Grupos Seguros

A lo largo de la vida útil de una red de sensores, existen ciertas situaciones en las que uno o más subconjuntos de nodos deben agruparse para cooperar en una tarea determinada. Un ejemplo de esta cooperación es cuando un grupo de nodos recoge los datos medidos por sus vecinos y los procesa, obteniendo como resultado un informe de un tamaño más reducido que las medidas iniciales. Otro ejemplo es cuando la red de sensores debe informar de la posición de un vehículo que la atraviesa, utilizando nodos que no se pueden mover de su posición actual.

Estos grupos deben disponer de una infraestructura de clave local, que les permita abrir canales de comunicación seguros entre uno o varios miembros del grupo. Proteger la seguridad de un grupo dentro de una red de sensores que ya se encuentra protegida no es redundante, ya que hay situaciones en las que el grupo necesita de esa protección.

La autenticación del origen es un factor importante dentro de los grupos seguros. Un mensaje dirigido a algunos o todos los miembros del grupo

debe estar debidamente autenticado, o cualquier mensaje que proceda del interior o exterior de la red de sensores puede considerarse, intencionadamente o no, como procedente del grupo. La confidencialidad es también importante, ya que en ciertos escenarios, como la medición de datos dentro de una central nuclear, el grupo puede querer ocultar el intercambio de información y sus resultados finales al resto de la red. Finalmente, la integridad de los mensajes es también esencial, porque sin ella tanto los mensajes de control como las medidas internas del grupo podrían ser atacadas.

Como en la infraestructura de claves vista en el apartado anterior, existen tres factores básicos a resolver a la hora de diseñar la infraestructura de claves de un grupo seguro: almacenamiento, distribución, y mantenimiento de claves. No obstante, proteger a un grupo de nodos es muy distinto a proteger toda la red. Primero, los grupos se crean en la mayoría de los casos de forma dinámica, cuando la estación base lo ordena o cuando ciertas lecturas (ejemplo: un vehículo aproximándose) fuerzan a la red a organizarse a sí misma. En estos casos, las claves del grupo deben ser negociadas y distribuidas automáticamente a todos los (futuros) miembros.

Segundo, los nodos que pertenezcan a un grupo deben ser capaces de guardar todas las claves necesarias para establecer los canales de comunicación seguros, teniendo en cuenta que en casos extremos puede que no haya espacio en memoria para estas claves. Tercero, debido a que los nodos entrarán y saldrán de su grupo local frecuentemente (ejemplo: cuando se está siguiendo un vehículo en el interior de la red de sensores), las operaciones de mantenimiento deben ser seguras para los grupos, en el sentido que un nodo externo no puede entrar en el grupo cuando no esta invitado y un nodo interno no puede abandonar el grupo demasiado pronto. Finalmente, los grupos deben satisfacer dos requerimientos más: "forward security", es decir, que un nodo que abandone el grupo no pueda acceder a las comunicaciones actuales de éste, y túnel seguro (secure tunnel), donde las medidas realizadas por el grupo deben ser leídas única y exclusivamente por la estación base en ciertos escenarios (como por ejemplo plantas nucleares).

Las infraestructuras de clave local no han sido demasiado investigadas en los últimos años, y existen pocas soluciones, la mayoría de ellas costosas en términos de recursos [13]. Una excepción ha sido la protección de grupos creados estáticamente, o clústers, que se configuran antes de la creación de la red, y donde nodos con mayores recursos (denominados "cluster heads") están a cargo de manejar y proteger la seguridad del grupo [14]. Aun así, es necesario desarrollar nuevos esquemas que permitan la creación y mantenimiento de grupos seguros de una forma óptima.

3.4. Routing

Los nodos son capaces de enviar un bit de información, en condiciones óptimas (línea de visión sin obstáculos, máximo gasto de energía, sin interferencias), a un distancia máxima de entre 100 y 300 metros. Esto hace necesario el utilizar algoritmos de encaminamiento, ya que en la mayoría de los casos no es posible enviar un paquete de datos directamente hacia su destino dentro de la red.

El diseño de algoritmos de encaminamiento es una tarea compleja [15]. Es necesario que los paquetes sean capaces de alcanzar cualquiera de los nodos (conectividad) mientras éstos cubren la mayor área posible utilizando sus sensores (cobertura), incluso cuando empiecen a fallar debido a problemas energéticos o de otro calibre (tolerancia a fallos). El algoritmo debería ser también capaz de funcionar con cualquier número de nodos o densidad de la red (escalabilidad) y proveer una calidad de servicio. Al mismo tiempo, los diseñadores deben tratar de reducir al máximo posible los requisitos de memoria, energía y CPU.

La seguridad es otro factor que no puede ignorarse en el diseño de algoritmos de encaminamiento. Cualquier adversario tiene a su disposición una gran variedad de ataques [16] que le permiten manipular a su antojo los caminos de la red, provocando pérdidas, alteraciones o falsificaciones de paquetes. Como ejemplo, es posible redirigir el tráfico de la red hacia un conjunto de nodos anunciándolos como nodos con mejores características, reales o no, de velocidad o conectividad. Es posible también modificar los mensajes de control, o utilizar múltiples identidades en un ataque "sybil".

La infraestructura de claves es útil en la protección de los algoritmos de encaminamiento, ya que permite autenticar a los nodos y proteger la confidencialidad e integridad de los paquetes. Sin embargo, no es suficiente. Tomando el control de un grupo de nodos de la red, un adversario puede modificar cualquier mensaje de control en su propio beneficio. Además, la red puede recibir un ataque de denegación de servicio (DoS) en cualquiera de sus secciones. Es por tanto necesario diseñar algoritmos de encaminamiento que sean robustos ante todos estos tipo de ataques.

Hasta ahora, las investigaciones se han enfocado principalmente en dos áreas: la protección de algoritmos de encaminamiento previamente existentes, tales como la difusión dirigida (directed diffusion [17]), y el descubrimiento de nuevas técnicas para proteger los algoritmos, como por ejemplo los caminos redundantes entre nodos [18] o el descubrimiento y marcado de zonas sin cobertura [19]. Pero la mayoría de los protocolos existentes no tienen en cuenta la seguridad en ninguno de los pasos de su diseño.

Como conclusión, el mayor reto en este área es el de descubrir nuevas técnicas de protección y aplicarlas a nuevos algoritmos, que a la vez que in-

corporan la seguridad como un requisito en todas las fases de su diseño tengan en cuenta los factores esenciales previamente mencionados (conectividad, escalabilidad, etc).

3.5. Agregación de Datos

Dentro de una red de sensores, los nodos generan una inmensa cantidad de datos producto de las mediciones realizadas al entorno. En la mayoría de los casos estos datos deben ser enviados a la estación base, por lo que hay un gran costo, en términos de consumo de energía y ancho de banda, en transportar todos estos datos a través de la red. Sin embargo, ya que los nodos suelen estar densamente distribuidos, los datos procedentes de nodos pertenecientes a una misma zona serán redundantes. El rol de la agregación es el de aprovechar esta situación y resumir todos los datos redundantes en un solo informe, por lo que se reduciría el envío de información hacia la estación base.

Este proceso de agregación es presa fácil de cualquier adversario, incluso aunque la red esté protegida contra ataques hacia la integridad de sus datos. Si un nodo agregador es controlado por un adversario, puede fácilmente ignorar los datos procedentes de sus vecinos y crear un informe falso. Y aún en el caso de que un nodo agregador sea de confianza, éste puede recibir datos manipulados o erróneos.

Utilizando funciones matemáticas que sean resistentes ante ataques internos, es posible defender al nodo agregador ante datos que provengan de nodos manipulados o en mal estado. Utilizando ideas de la teoría estadística, el autor en [20] analizó la robustez de un conjunto de funciones (por ejemplo, demostrando que el mínimo, el máximo, la suma, y la media son funciones inseguras) y propuso algunas herramientas (ej. ignorar valores extremos) para mejorar la robustez de las funciones de agregación.

Existen también soluciones orientadas a descubrir cuando los informes enviados por un nodo agregador están falsificados o no. Una posibilidad consiste en entablar una negociación entre la estación base y el agregador sobre los datos empleados en la creación del informe. Por ejemplo, en [21] la prueba que el agregador debe crear sobre los datos procedentes de sus vecinos se construye sobre un Árbol Hash Merkle.

Existe otra solución que utiliza la densidad de las redes como herramienta, haciendo que los nodos vecinos funcionen como testigos de la agregación. Ellos realizarán los mismos cálculos que el agregador, obteniendo un resultado parecido al estar en la misma zona física. Como ejemplo, en [22] los nodos crean una prueba de sus cálculos utilizando para ello un MAC y una clave secreta compartida con la estación base, de tal forma que el agregador debe enviar a la estación base tanto el informe como las pruebas de los testigos.

Finalmente, es también posible filtrar los paquetes que contienen el informe y las pruebas cuando ambos se encaminan a la estación base, disminuyendo el tráfico generado por informes falsos. En [23], las pruebas creadas por los testigos utilizan una clave procedente de un "key pool", y el agregador las comprime utilizando un filtro de Bloom. En el camino, los nodos que posean una clave del "key pool" pueden comprobar si una prueba está en el interior del filtro de Bloom.

La agregación segura es un campo con muchos interrogantes por resolver. Los protocolos interactivos entre los agregadores y la estación base consumen muchos recursos, y no son escalables sin la presencia de una jerarquía de comprobación de informes. Los sistemas basados en pruebas requieren en la mayoría de los casos de una negociación entre el agregador y los testigos, además de incrementar el tamaño de los informes a enviar. En definitiva, sería necesario disponer de nuevas soluciones que minimicen tanto el número de negociaciones necesarias como el tamaño de los informes, y que introduzcan nuevas técnicas para detectar y eliminar informes falsos más eficazmente.

3.6. Auditoría

Dentro de una red de sensores un usuario solo podrá acceder a la red de adquisición de datos, en la mayoría de los casos, a través de la estación base. Como resultado, cualquier cambio en el estado interno de los nodos (bajo nivel de batería, fallos en el hardware) o de la red pasaría inadvertido. Sería por lo tanto indispensable proporcionar un subsistema de auditoría dentro de la red que permitiera a los usuarios preguntar o recibir informes periódicos acerca de su estado.

Una posible aplicación de ese subsistema de auditoría sería un *Sistema de Detección de Intrusiones* (IDS). Éstos sistemas monitorizan las actividades de la red, recogiendo y analizando datos sobre su comportamiento, con el objetivo de detectar intrusos y alertar al usuario de este hecho. Estos sistemas pueden considerarse, en cierta forma, como una "Segunda Línea de Defensa", que se activa una vez un adversario haya tomado control de ciertas partes de la red.

Un IDS para redes de sensores podría aprovecharse de los conceptos y las técnicas de los IDS desarrollados para redes "Ad Hoc" [24]. Sin embargo, éstas técnicas no pueden aplicarse directamente a las redes de sensores, debido a sus características únicas. Cada nodo de la red no puede realizar de forma completa todas las tareas de detección debido a sus limitaciones de energía y CPU. Además, dado que la densidad de las redes de sensores suele ser alta, sería redundante obligar a todos los nodos a vigilar los paquetes enviados en su vecindario. Por lo tanto, el problema más básico a la hora de desarrollar un IDS es la distribución de las tareas de detección entre los nodos de la red, problema

que actualmente cuenta con algunas soluciones en entornos basados en clusters [25].

Existen también otros problemas aún no resueltos o discutidos en este área. Un IDS debe ser simple y altamente especializado, capaz de analizar y reaccionar ante los problemas que se den en los protocolos de la red. El conjunto de reglas utilizado por los algoritmos de detección debe ser simple y fácil de interpretar, produciendo resultados que consuman poca memoria. Los nodos con tareas de detección deben ser capaces de intercambiar información entre ellos para alcanzar un mejor porcentaje de detección, y las alertas generadas por la arquitectura deben llegar a la estación base lo antes posible.

Cabe mencionar aquí que existen soluciones parciales que son capaces de comprobar la integridad de los nodos de la red, y que podrían ser incorporadas en un IDS. Una de estas soluciones (health monitoring [26]) permite al usuario comprobar si un grupo de nodos se encuentra activo o no. Otro algoritmo, utilizado en [27], analiza fluctuaciones en las mediciones de los nodos utilizando el "Hidden Markov Model" (HMM) para descubrir variaciones inesperadas. Finalmente, es también posible comprobar la integridad del "firmware" de un nodo utilizando técnicas de atestación de código (Code Attestation Techniques [28]).

3.7. Otros Problemas

Una red de sensores necesita de una infraestructura de seguridad que le permita protegerse tanto de los ataques internos como de los ataques externos a la confidencialidad, integridad, y autenticación de los elementos de la red. Sin embargo, esto no es suficiente para resolver determinados problemas que no han sido suficientemente desarrollados en la literatura, tales como la privacidad y la seguridad de agentes móviles.

La privacidad, en determinadas situaciones, es una propiedad esencial. Por ejemplo, en un campo de batalla, sería importante ocultar la localización y las identidades de la estación base y de los nodos que generan información. En contraste, en un escenario de rescate (ej: terremoto), localizar a los nodos (ej: perros) es algo absolutamente necesario.

Existen tres tipos de amenazas contra la privacidad [29]. Si un adversario es capaz de determinar el sentido de un mensaje sólo por su existencia y por el contexto del entorno que rodea a la red, existe una *amenaza contra la privacidad de contenido* (content privacy threat). Si un adversario es capaz de deducir las identidades de los nodos que se están comunicando, existe una *amenaza contra la privacidad de identidad* (identity privacy threat). Y si el adversario es capaz de deducir o aproximar la localización de uno de los nodos que participan en una comunicación existe una *amenaza contra la privacidad de localización* (location privacy threat).

Existen algunos estudios sobre las amenazas de privacidad de localización y contenido [29] que exploran la privacidad de algunos protocolos de encaminamiento. Pero en general, la privacidad en un entorno de redes de sensores es un campo inexplorado, en el que sería importante descubrir e investigar los escenarios en los que existe una amenaza contra la privacidad.

Dado que las redes de sensores están dando sus primeros pasos, existen algunas aplicaciones cuyos requerimientos de seguridad no están aún investigados. Un ejemplo es el área de los agentes móviles [30], que proporciona una interesante herramienta para procesos de computación distribuida. No obstante, cualquier adversario puede ser capaz tanto de incluir en la red un agente malicioso como de modificar los resultados almacenados dentro del agente. Por lo tanto, sería necesario tanto investigar como proveer integridad de código e integridad de resultados dentro de un entorno tan limitado como una red de sensores.

4. Conclusión

La seguridad en redes de sensores es un campo de investigación que está creciendo rápidamente y alcanzando resultados que pueden aplicarse en escenarios la vida real. Durante este crecimiento se ha pasado de un entorno completamente inseguro a disponer de algoritmos básicos, arquitecturas, y herramientas de seguridad.

No obstante, este campo de investigación esta lejos de considerarse maduro. La criptografía de clave pública y los sistemas de detección de intrusiones son técnicas aplicadas recientemente en las redes de sensores. Es también necesario desarrollar algoritmos seguros de encaminamiento que proporcionen conectividad, cobertura y tolerancia a fallos. Finalmente, los algoritmos de agregación de datos deberían ser mas óptimos y seguros, y la privacidad de los flujos de datos debería tomarse en cuenta.

Otras áreas de seguridad en desarrollo en el campo de las redes de sensores [31] son la capacidad de los nodos de aguantar ataques físicos, la optimización de las infraestructuras de seguridad en términos de recursos (energía, tiempo de computación), la detección y reacción ante ataques de denegación de servicio, y la discusión sobre los problemas de privacidad social en las redes de sensores. Finalmente, existen áreas mínimamente desarrolladas que requieren de especial atención, como la protección de redes de sensores con nodos móviles o con múltiples estaciones base, o la medición de la confianza (trust) existente entre nodos.

Referencias

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. *Wireless sensor networks:*

a survey. Computer Networks, 38(4), Marzo 2002.

[2] Crossbow Technology, Inc. *MICA2 and MICAz, Wireless Measurement Systems*. http://www.xbow.com.

[3] IEEE Standard, 802.15.4-2003. *Wireless medium access control and physical layer specifications for low-rate wireless personal area networks*. Mayo 2003, ISBN 0-7381-3677-5.

[4] C. Karlof, N. Sastry, D. Wagner. *TinySec: a link layer security architecture for wireless sensor networks*. Proceedings of 2nd International Conference on Embedded Networked Sensor Systems (SensSys'04), Noviembre 2004.

[5] N. Sastry, D. Wagner. *Security considerations for IEEE 802.15.4 networks*. Proceedings of 2004 ACM Workshop on Wireless security (Wise'04), Octubre 2004.

[6] D. J. Malan, M. Welsh, M. D. Smith. *A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography*. Proceedings of 1st IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (Secon'04), Octubre 2004.

[7] L. Eschenauer, V. D. Gligor. *A key-management scheme for distributed sensor networks*. Proceedings of 9th ACM Conference on Computer and Communications Security (CCS'02), Noviembre 2002.

[8] J. Lee, D. R. Stinson. *Deterministic key predistribution schemes for distributed sensor networks*. Proceedings of 11th Annual Workshop on Selected Areas in Cryptography (SAC'04), Agosto 2004.

[9] B. Yener, S. A. Camtepe. *Combinatorial design of key distribution mechanisms for wireless sensor networks*. Proceedings of 9th European Symposium On Research in Computer Security (ESORICS'04), Septiembre 2004.

[10] W. Du, J. Deng, Y. S. Han, S. Chen, P. K. Varshney. *A key management scheme for wireless sensor networks using deployment knowledge*. Proceedings of IEEE INFOCOM'04, Marzo 2004.

[11] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, J. D. Tygar. *SPINS: Security protocols for sensor networks*. Proceedings of 7th International Conference on Mobile Computing and Networking (MOBICOM'01), Julio 2001.

[12] R. Anderson, H. Chan, A. Perrig. *Key infection: smart trust for smart dust*. Proceedings of 12th IEEE International Conference on Network Protocols (ICNP'04), Octubre 2004.

[13] J. Zachari. *A decentralized approach to secure group membership testing in distributed sensor networks*. Proceedings of 2003 Military Communications Conference (MILCOM 2003), Octubre 2003.

[14] Y. W. Law, R. Corin, S. Etalle, P. H. Hartel. *A formally verified decentralized key management architecture for wireless sensor networks*. Proceedings of 2003 Personal Wireless Communications (PWC'03), IFIP WG 6.8 - Mobile and Wireless Communications. Septiembre 2003.

[15] J. N. Al-Karaki, A. E. Kamal. *Routing techniques in wireless sensor networks: a Survey*. IEEE Wireless Communications, Vol 11(6), pag 6-28, Diciembre 2004.

[16] C. Karlof, D. Wagner. *Secure routing in wireless sensor networks: attacks and countermeasures*. Proceedings of 1st IEEE International Workshop on Sensor Network Protocols and Applications, Mayo 2003.

[17] R. Di Pietro, L. V. Mancini, Y. W. Law, S. Etalle, P. Havinga. *LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks*. Proceedings of 32nd International Conference on Parallel Processing Workshops (ICPP'03), Octubre 2003.

[18] J. Deng, R. Han, S. Mishra. *A performance evaluation of intrusion-tolerant routing in wireless sensor networks*. Proceedings of 2nd IEEE International Workshop on Information Processing in Sensor Networks (IPSN'03), Abril 2003.

[19] Q. Fang, J. Gao, L. J. Guibas. *Locating and bypassing routing holes in sensor networks*. Proceedings of IEEE INFOCOM'04, Marzo 2004.

[20] D. Wagner. *Resilient aggregation in sensor networks*. Proceedings of 2nd ACM workshop on Security of Ad Hoc and Sensor Networks (SANS'04), Octubre 2004.

[21] B. Przydatek, D. Song, A. Perrig. *SIA: Secure information aggregation in sensor networks*. Proceedings of 1st International Conference on Embedded Networked Sensor Systems (SenSys'03), Noviembre 2003.

[22] W. Du, J. Deng, Y. S. Han, P. K. Varshney. *A witness-based approach for data fusion assurance in wireless sensor networks*. Proceedings of GLOBECOM'03, Diciembre 2003.

[23] F. Ye, H. Luo, S. Lu, L. Zhang. *Statistical en-route filtering of injected false data in sensor networks*. Proceedings of IEEE INFOCOM'04), Marzo 2004.

[24] P. Brutch, C. Ko. *Challenges in intrusion detection for wireless ad hoc networks*. Proceedings of 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), Enero 2003.

[25] F. Anjum, D. Subhadrabandhu, S. Sarkar, R. Shetty. *On optimal placement of Intrusion Detection Modules in Sensor Networks*. Proceedings of the 1st International Conference on Broadband Networks, Octubre 2004.

[26] C. Hsin, M. Liu. *A Distributed monitoring mechanism for wireless sensor networks*. Proceedings of 2002 ACM Workshop on Wireless Security (WiSe'02), Septiembre 2002.

[27] S. S. Doumit, D. P. Agrawal. *Self-organized criticaly & stochastic learning based intrusion detection system for wireless sensor networks*. Proceedings of 2003 Military Communications Conference (MILCOM'03), Octubre 2003.

[28] A. Seshandri, A. Perrig, L. Van Doorn, P. Khosla. *SWATT: software-based attestation for embedded devices*. Proceedings of 2004 IEEE Symposium on Security and Privacy (S&P'04), Mayo 2004.

[29] C. Ozturk, Y. Zhang, W. Trappe, M. Ott. *Source-location privacy for networks of energy-constrained sensors*. Proceedings of 2nd IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems (WSTFEUS'04), Mayo 2004.

[30] H. Qi, Y. Xu, X. Wang. *Mobile-agent-based collaborative signal and information processing in sensor networks*. Proceedings of the IEEE, 91(8)1172-1183, Agosto 2003.

[31] E. Shi, A. Perrig. *Designing Secure Sensor Networks*. IEEE Wireless Communications, 11(6)38-43, Diciembre 2004.