REVISIÓN DEL ESTADO DEL ARTE DE REDES DE SENSORES INALÁMBRICOS

Catalina Aranzazu Suescún[1], Gustavo Alberto Moreno López [2]

[1]Catalina Aranzazu Suescún, Ing. Electrónica, Especialista en Telecomunicaciones, MSc(c) en Ingeniería con énfasis en Telecomunicaciones Universidad Pontificia Bolivariana, Integrante del Grupo de investigación de Aplicaciones en Telecomunicaciones GIAT. catazazu@gmail.com
[2]Gustavo Alberto Moreno López, Ing. Electrónico, Especialista en Telecomunicaciones, MSc(c) en Ingeniería con énfasis en Telecomunicaciones Universidad Pontificia Bolivariana, Docente Politécnico Jaime Isaza Cadavid, Coordinador del Grupo de investigación de Aplicaciones en Telecomunicaciones GIAT. Carrera 48 N° 7-151, gamoreno@elpoli.edu.co

RESUMEN

Este artículo presenta un estudio del estado del arte de las redes de sensores inalámbricas, las cuales siguen un desarrollo creciente y presentan una gran variedad de aplicaciones. Estas redes constituyen un campo actual y emergente de estudio donde se combina el desarrollo de computadores, comunicaciones inalámbricas y dispositivos móviles e integración con otras disciplinas como agricultura, biología, medicina, etc. Se presenta el concepto principal, los componentes, topologías, estándares, aplicaciones, problemas y desafíos, luego se profundiza en soluciones de seguridad y se concluye con herramientas básicas de simulación.

Palabras clave: Nodos de sensores, Seguridad, Aplicaciones, Inalámbricos

Recibido: 17 de abril de 2009. Aceptado: 30 de Junio de 2009
Received: April 17, 2009 Accepted: June 30, 2009

SURVEY ON THE STATE OF THE ART OF WIRELESS SENSOR NETWORKS

ABSTRACT

This article presents a survey of the state of the art of wireless sensor networks, which follows a growing development and a wide variety of applications. These networks provide a current and emerging field of study where combines the development of computers, wireless communications and mobile devices and integration with other disciplines such as agriculture, biology, medicine, etc. Presents the main concept, components, topologies, standards, applications, problems and challenges, deepens security solutions and conclude with basic tools of simulation.

Keywords: *Sensor Node, Security, Applications, Wireless*

1. INTRODUCCIÓN

Los sensores han sido tradicionalmente elementos indispensables en los procesos industriales debido a la capacidad que proporcionaban de monitorizar y manipular las magnitudes físicas involucradas en los diferentes procesos productivos. La conectividad entre los sensores se realizaba mediante el uso de redes cableadas tradicionales. Actualmente los continuos avances tecnológicos han incentivado el desarrollo de dispositivos con capacidades de comunicación inalámbrica, dispuestos en cualquier localización, cada vez más pequeños, autónomos, más potentes y con un consumo de batería más eficiente; de ahí surge las redes de sensores inalámbricos (WSN, Wireless Sensor Network), que están compuestas por una serie de miles, incluso millones de sensores, llamados nodos, los cuales poseen capacidad de almacenamiento, procesamiento y energía limitada.

El continuo desarrollo de estas particulares redes ha provocado su incorporación y uso en ámbitos muy dispares. Desde la monitorización ambiental (humedad, temperatura, luz, etc.) fundamental para el desarrollo de la domótica, pasando por las aplicaciones militares, industriales, médicas o comerciales [1].

En este artículo, se presenta un estudio de los conceptos fundamentales de las redes de sensores inalámbricas, las aplicaciones, estándares principales, desafíos, problemas básicos, las últimas soluciones planteadas en el tema de seguridad, herramientas de simulación, y otros temas de investigación.

2. FUNDAMENTOS DE REDES DE SENSORES

2.1 Definición

Una red de sensores inalámbrica es una red de pequeños sistemas informáticos embebidos colocados en el mundo físico, y capaces de interactuar con este [2].
Gómez, [3], presenta otra definición como un conjunto de elementos autónomos (nodos) interconectados de manera inalámbrica, que miden variables como movimiento, presión, temperatura y humedad, etc.
Si los sensores utilizados son de tamaño que se mide en milímetros o micrómetros, la tecnología necesaria ya es de tipo nanotecnología. En vez de redes de sensores, se suele utilizar el nombre *polvo inteligente* (*smart dust*). Si son robots, se habla de *niebla de utilidad* (*utility fog*).

Las redes de sensores están distribuidas en un área específica y los nodos pueden ser estacionarios o móviles.

Una red de nodos móviles, forman una red *ad hoc* capaz de realizar ruteo entre ellos. Su formación es por *auto-configuración* sobre una topología física arbitraria, bajo modificación frecuente por los movimientos, salidas, llegadas y fallas de los nodos participantes.

Las redes de sensores tienen las siguientes tareas típicas [4]:

- Determinar un parámetro ambiental: calor, presión, luz, radiación, presencia de humo, humedad, ruido, fricción
- Detectar eventos: presencia, llegada, movimiento, vibración, flujo
- Estimar parámetros: velocidad, dirección
- Clasificar los objetos detectados
- Seguir la trayectoria de un objeto detectado

La red en sí no tiene valor, sino las salidas.

2.2 Características

Entre las características que poseen las redes de sensores se encuentran las siguientes [1], [3], [5]:

Topología y mantenimiento: En general los nodos que forman las redes de sensores se caracterizan por estar aleatoriamente distribuidos sin seguir ninguna topología regular. Debido a ello se recomienda que el mantenimiento y configuración sea completamente autónomo (no requiera de la intervención humana) mediante el uso de algoritmos distribuidos.

Limitaciones energéticas: Uno de los principales cuellos de botella que encontramos en las operaciones realizadas por los sensores es, la disponibilidad energética de los nodos. Los sensores en la mayoría de los casos poseen baterías que se caracterizan por no poder ser recargadas, lo cual convierte este problema en la principal restricción a la hora de desarrollar nuevos protocolos. Aumentar el tiempo de vida de un sensor implicará, por tanto, disminuir los niveles de tolerancia o limitar la precisión de los resultados obtenidos.

Hardware y software específico: El microcontrolador, el sistema operativo y las aplicaciones desarrolladas para las WSN's deben tener muy en cuenta las limitaciones energéticas antes expuestas. El sistema operativo más empleado como base para la construcción de aplicaciones en redes inalámbricas de sensores, es TinyOS [6], desarrollado en la Universidad de Berkeley [7].

Sincronización de los dispositivos: Para que el tratamiento de la información que se propaga por una red de sensores se realice de forma correcta, los nodos deben sincronizarse. Por ello en las WSN's deben imponerse procesos de acceso al medio por división múltiple en el tiempo (*Time Division Multiple Access*, TDMA) y ordenación temporal para que la detección de los eventos se produzca sin ambigüedades.

Enrutamiento dinámico: Las redes de sensores deben ser capaces de adaptarse a los cambios de conectividad de los nodos. Por ello, los protocolos de enrutamiento utilizados deben estar preparados para incluir o excluir a nodos de sus rutas.

Restricciones temporales: Si bien las WSN's deben soportar comunicaciones en tiempo real entre los diferentes nodos, esto no debe perjudicar a las características de retardos, ancho de banda u otros parámetros de calidad de servicio de las redes (*Quality of Service*, QoS).

Seguridad: Atendiendo al uso final para el cual esté desarrollada la red de sensores, la seguridad en las comunicaciones puede ser un factor muy importante a la hora de determinar los protocolos que se desarrollaran en las diferentes capas de los nodos. Este es el claro ejemplo de las redes de sensores utilizadas en el ámbito militar.

Otras características:

- No se utiliza infraestructura de red: encaminamiento entre nodos sin visión directa con comunicaciones multisalto.
- Topología dinámica: nodos autoconfigurables, tolerancia a fallos.
- Facilidad de despliegue.
- De bajo consumo.
- Muy bajo coste.
- Pequeño tamaño.
- Operación sin mantenimiento durante varios meses o años.

2.3 Elementos

Los elementos principales se ilustran en la figura 1:

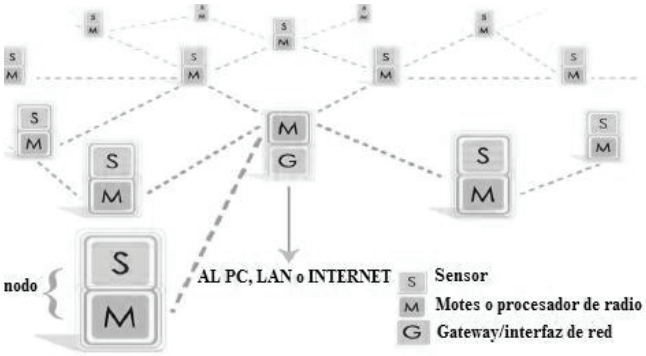

Figura1. Componentes de una Red de sensores inalámbricos

Sensores: De distinta naturaleza y tecnología toman del medio la información y la convierten en señales eléctricas.
Motes: O procesadores de radio, toman los datos del sensor a través de sus puertas de datos, y envían la información a la estación base.
Nodo: Es un sensor/motes
Gateway: Elementos para la interconexión entre la red de sensores y una red TCP/IP.
Estación Base: Recolector de datos basado en un ordenador común o sistema embebido.
Red Inalámbrica: Típicamente basada en el estándar 802.15.4, *ZigBee.*

2.4 Topología

En las redes de sensores inalámbricas se tienen los siguientes tipos de dispositivos [8], como se muestra en la figura 2:

Full-Function Devices (FFD):
– Cualquier topología
– Capaz de hacer de coordinador de red (en red de área personal, PAN)
– Habla con cualquier otro dispositivo.

Reduced function device (RFD):
– Solo en topología en estrella
– No puede ser coordinador de red
– Sólo habla a los coordinadores de red
– Implementación muy simple.

Coordinador *Personal area network* (PAN): es el nodo coordinador principal de la red.

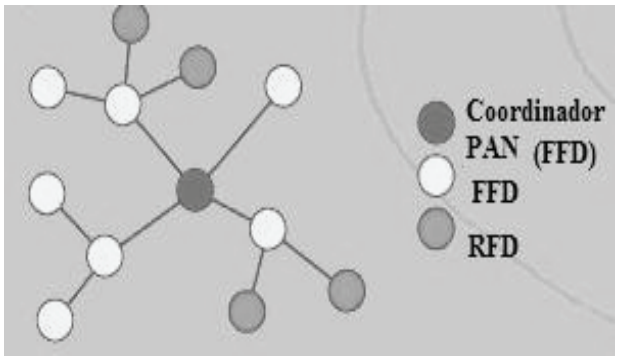

Figura 2. Tipos de dispositivos

La topología puede ser en malla, estrella, clúster de estrellas, ilustradas en la figura 3 respectivamente.


Figura 3. Topologías de malla (izquierda), estrella (centro) y clúster de estrella (derecha).

En las topologías entonces, existe un coordinador o una comunicación directa entre nodos (peer-to-peer) [1].

2.5 Estándares

La red esta basada en algunos de los estándares inalámbricos, indicada en la tabla 1, donde habrá que alcanzar un compromiso entre [2]:

- Velocidad de transmisión
- Cobertura
- Coste energético por paquete enviado.

Actualmente el estándar elegido para este tipo de redes, es el IEEE 802.15.4, que es soportado y promovido por ZigBee [9]:

- 20-250 Kbs
- 1-100 Metros
- Hasta 2 años de batería

Zigbee: Tecnología dirigida a las necesidades de mercado de redes inalámbricas de bajo coste basadas en la norma IEEE 802.15.4, [3]. Se inicio como un consorcio industrial sin ánimo de lucro para definir especificaciones globales de aplicaciones inalámbricas fiables, económicas y de baja potencia basadas en la norma IEEE 802.15.4.

Se debe tener en cuenta que una implementación compatible con el estándar 802.15.4 puede no ser estándar ZigBee.

ZigBee define más niveles además de capa física y capa MAC (PHY/MAC), como se observa en la figura 4:

– Encaminamiento
– Seguridad a nivel superior
– Aplicación/perfiles

La tabla 1 presenta un resumen de las principales características de las tecnologías Wifi, Bluetooth y Zigbee.

Estándar	Wifi 802.11g	Bluetooth 802.15.1	Zigbee 802.15.4
Aplicación principal	Wlan	Wpan	Control y monitorización
Memoria necesaria	1 MB+	250 KB+	4-32 KB
Vida batería (días)	0.5- 5	1-7	100-1000+
Tamaño red	32 nodos	7	255/65000
Velocidad (Kbps)	54 Mbps	720 Kbps	20-250 Kbps
Cobertura (metros)	100	10	1-100
Parámetros importantes	Velocidad, flexibilidad	Coste y perfiles de aplicación	Fiabilidad, bajo consumo y bajo costo

Tabla 1. Comparación Estándares Inalámbricos

Por ejemplo, para perfiles *lighting*, garantizará que los interruptores de la compañía A, hablarán con las luces fabricadas por B.

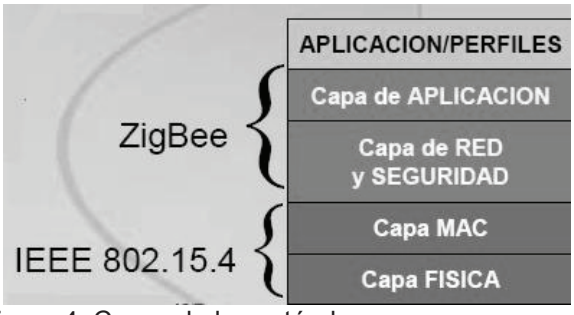

Figura 4. Capas de los estándares

2.6 Enrutamiento

Los protocolos convencionales de distribución de datos o enrutamiento no son eficientes en este tipo

de redes con restricciones tan elevadas en el consumo de energía [8]. En su lugar se han desarrollado otros protocolos más específicos que resuelven en parte ese problema. De forma muy sencilla se citan los protocolos basados en negociación que usan descriptores antes de transmitir la información, evitando así parte de la redundancia; *la difusión directa* basada en enrutamiento reactivo originado en destino; *el de ahorro de energía* también del tipo reactivo pero basado exclusivamente en probabilidades de consumo energético; *el multicamino* basado en incrementar la disponibilidad de la red cuando el camino óptimo no esta disponible; y finalmente Control de acceso al medio pero específico para redes de sensores y denominado: *S-MAC*. [5]

Encaminamiento en Redes Ad-hoc Inalámbricas: [10] Una red Ad Hoc Inalámbrica se entiende como un conjunto de nodos distribuidos de forma aleatoria en un espacio D-dimensional. En la misma, la comunicación puede ser generada por cualquier nodo de la red, que actúa por tanto como fuente, hacia cualquier otro nodo, que asume el papel de destino. Dicha comunicación se produce mediante un esquema multisalto en el que los datos son retransmitidos por una serie de nodos intermedios hasta alcanzar este último. Los protocolos de encaminamiento más representativos, se clasifican según si es uniforme o no-uniforme.

Clasificación Uniforme o de estructura plana, figura 5, indica que todos los nodos de la red desempeñan iguales funciones y poseen las mismas características. En este caso, no se incurre en ningún coste de mantenimiento de la estructura de la red; sin embargo, se adaptan en muy poca medida a ampliaciones conservando sus mismas prestaciones.

Clasificación No uniforme, figura 6, es propio de estructuras jerárquicas en las que algunos nodos desarrollan papeles especiales e incluso pueden dotarse de capacidades particulares en términos de cómputo, energía o almacenamiento entre otros. Esto les permite soportar algoritmos más complejos, reducir la sobrecarga debida a la comunicación y ofrecer la posibilidad de balanceo de carga mientras mantienen sus características incluso ante incrementos del número de nodos en la red; por el contrario, generan cierto coste de mantenimiento de la estructura y necesitan en muchos casos la disponibilidad de nodos heterogéneos

Figura 5. Protocolos de encaminamiento Uniforme

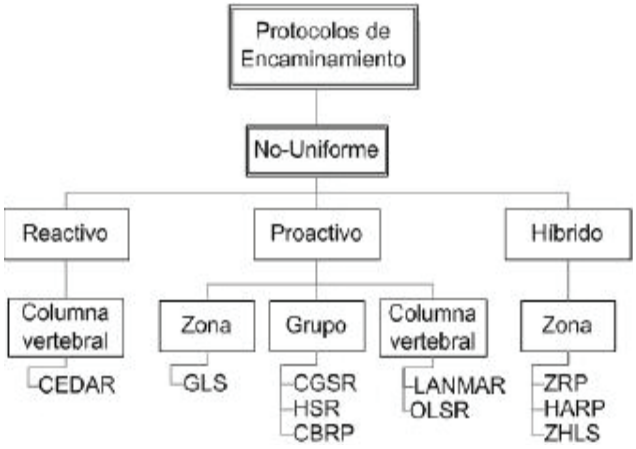

Figura 6. Protocolos de encaminamiento No-uniforme

En cada una de las clasificaciones, de uniforme y no-uniforme, los protocolos presentan una nueva peculiaridad relativa al procedimiento adoptado para el descubrimiento del camino a establecer y su mantenimiento. Bajo este punto de vista, puede diferenciarse entre:

Proactivo: su funcionamiento se basa en tablas, creadas a partir de una fase original de descubrimiento de ruta, que albergan la información referente a los caminos en la red con base en distintos criterios. Esta información es de ámbito global y por tanto, todos los nodos conservan caminos posibles hacia el resto. Para la diseminación de la misma, los nodos intercambian estos datos bien periódicamente o bien ante la aparición de un cambio en ella. Los protocolos activos logran que el envío de datos se produzca

con un retardo despreciable debido a que la información sobre la ruta a seguir está disponible previamente; no obstante, consumen recursos de la red, energía, cómputo, almacenamiento, etc., Independientemente del grado de utilización de la ruta.

Reactivo: también denominado "bajo demanda". Las rutas se construyen únicamente en el momento en que un nodo necesita establecer una comunicación. Es en ese preciso instante cuando se desencadena una fase de descubrimiento de ruta que concluye una vez que la fuente recibe la respuesta del destino que incluye el camino elegido para el envío de datos. El coste de mantenimiento de rutas disminuye en gran medida, a costa de introducir una latencia producida por la generación inicial del camino y un posible problema de saturación de la red fruto de la inundación de la misma con mensajes de petición de ruta.

Híbrido: generalmente utilizado para protocolos no uniformes. Incluye ambos procedimientos anteriores en distintos niveles del encaminamiento. Así, se consigue reducir la sobrecarga de la red con mensajes de control presentada por los protocolos activos, mientras que se disminuye la latencia de las operaciones de búsqueda mostrada entre los reactivos.

En el caso de los protocolos uniformes, ya sea si es reactivo o activo, hay una clasificación que obedece al tipo de información del estado de la red que manejan los nodos para proceder al encaminamiento. Según este criterio, un protocolo uniforme se basa en:

Topología: los nodos mantienen información referida al conjunto global de la red. Un grupo importante de estos protocolos son los basados en el estado del enlace, en los que la información sobre las conexiones establecidas por cada nodo con sus vecinos es diseminada a lo largo de la red de tal forma que cualquier nodo conozca el esquema de enlaces de la misma. Esta aproximación no se adapta de forma óptima al carácter dinámico de este tipo de redes; sin embargo, una información de tal calibre incide muy positivamente en la selección de la mejor ruta, el balanceo de carga o la gestión de la calidad del servicio.

Destino: el conocimiento en este caso se restringe al ámbito local. El grupo más numeroso de entre esta clase de protocolos son los llamados "distancia-vector" dado que, en lugar de rutas completas, mantienen cierta medida de la distancia hasta distintos destinos (generalmente el número de saltos mínimo) y el vector de dirección hacia ellos (el identificador del nodo del salto siguiente).

Posición: el conocimiento de cada nodo se basa en las coordenadas geográficas de sí mismo y del resto. El principio del encaminamiento consiste en la aproximación secuencial hacia el destino mediante la implementación de saltos al vecino que esté más próximo a éste. En redes de topología homogénea resulta una técnica muy eficiente; sin embargo, en presencia de discontinuidades u obstáculos debe apoyarse en algoritmos específicos para mejorar su rendimiento; al mismo tiempo, esta aproximación requiere un sistema de posicionamiento absoluto o relativo, lo cual limita considerablemente su aplicación.

Por su parte, los protocolos no uniformes pueden catalogarse en función del tipo de organización que presentan, diferenciándolos según su base en:

Zona: los nodos son agrupados según la zona geográfica que ocupan. Así, se reduce la sobrecarga de mantenimiento de ruta al ámbito local de la misma. Una vez más, es necesario el conocimiento de la posición de los nodos y el consiguiente sistema que lo provea.

Grupo: la asociación de nodos se realiza en torno a uno de ellos (clusterhead) que actúa como líder del grupo, responsabilizándose del alta y la baja de nodos en el grupo y de ciertas funciones jerarquizadas del encaminamiento. Esta jerarquía reduce la sobrecarga de control de la red a partir de nodos que, en la mayoría de los casos, requieren capacidades más amplias que las del resto.

Columna vertebral: un conjunto de nodos son seleccionados dinámicamente para conformar una columna vertebral (backbone) de la red. A dichos nodos se les asignan funciones especiales como la construcción de caminos y la propagación de paquetes de control y datos. El resto de nodos se apoya en estos para realizar su establecimiento de ruta para la comunicación deseada. Una vez más, se logra una alta capacidad de adaptación a las ampliaciones de la red y un control del encaminamiento a un menor coste; por el contrario, sigue incurriéndose en cierto gasto de mantenimiento de la estructura.

2.7 Aplicaciones

Existe una gran diversidad de aplicaciones actuales y en desarrollo para usar las redes de sensores inalámbricas, entre ellas las siguientes [3], [4], [6], [11], [12], [13]:

Seguridad: en nuestro entorno hay muchos elementos que pueden llegar a ser muy peligrosos: escapes de gas, instalaciones eléctricas en mal estado, contaminación de agua o aire, etc. Que un sensor perciba esto suele ser sencillo, el factor determinante es poder comunicarlo de forma adecuada en el sitio adecuado y con un coste adecuado. Muchos sistemas de seguridad han demostrado ser poco eficaces, bien por ser demasiado complicados y caros como para aplicarse masivamente, bien por estar muy limitados por la dependencia de las baterías, por emplear diferentes tecnologías propietarias no compatibles, o por no estar bien preparados para entrar en una red de comunicaciones.

Domótica: una de las aplicaciones más atractivas para este tipo de redes. Dispositivos heterogéneos de diferentes fabricantes podrían comunicarse entre sí, librando al usuario de tareas triviales. Las luces pueden atenuar su intensidad cuando se encienda el televisor o el televisor reducir el volumen cuando suene el teléfono. Cada persona puede tener su propio perfil, al que se adapte de forma automática la temperatura, la luz, la música, la televisión o el ordenador, tanto en casa como en la oficina.

Defensa: uno de los ámbitos donde se ve mayor posibilidad de uso de las redes Ad-Hoc en general y de las redes de sensores en particular, es el militar. En 2005 se presentó un prototipo que empleaba motas MICA2 con sensores de sonido de bajo precio para la detección de francotiradores. El sistema es capaz de localizar el origen de un disparo, con precisión de 1 metro y latencia de 2 segundos, con tal de que esté separado 0,4 segundos de un segundo disparo [14]. Podemos encontrar otro ejemplo en la industria del armamento, actualmente en fase de desarrollo avanzado: un campo minado auto-regenerable [15]. Se trata de una red Ad-Hoc donde cada nodo es una mina anti-tanque. Si el enemigo abre una brecha en el campo, las minas lo perciben y tienen la capacidad de desplazarse para volver a cerrar el campo.

Aunque se espera que las redes de sensores puedan reemplazar a este tipo de armas: las minas se usan mucho porque es una forma eficaz de evitar el movimiento del enemigo en un área remota. Desplegarlas resulta muy barato, pero desmantelarlas es muy caro, además son especialmente crueles porque siguen activas durante décadas, sin distinguir entre amigos, enemigos y población civil. Como alternativa, una red de sensores puede desplegarse sobre el terreno para detectar de forma precisa al enemigo, lo que permitirá su destrucción por diversos medios (misiles, aviación, control remoto, etc.).

Monitorización de instalaciones: la lectura de los contadores de agua y electricidad puede hacerse mediante una red de sensores, habrá un nodo por vivienda de un edificio o un barrio sin necesidad de tender nuevos cables. Un nodo principal recopilará la información para enviarla a la compañía suministradora. De esta misma forma se pueden monitorizar cableado eléctrico o cañerías de agua o gas, estructuras (figura 7), sin necesidad de un cableado paralelo.

Figura 7. Monitoreo de Estructuras

Podemos encontrar muchas otras aplicaciones, como:

El control de inventarios, de animales silvestres (figura 8), y monitorización del tiempo (lo que es especialmente útil en agricultura). [6]

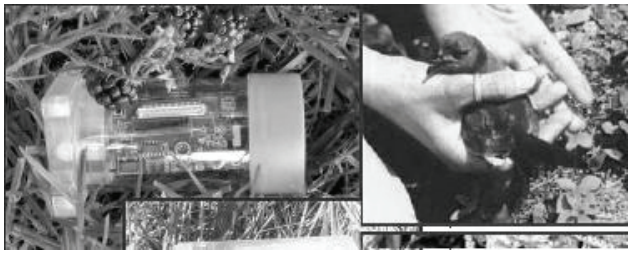
Figura 8. Seguimiento a animales

Monitorización del entorno (Figura 9), lecturas de un entorno inaccesible y hostil en un período de tiempo para detectar cambios, tendencias, incendios, etc. [3]


Figura 9. Monitoreo del entorno

Estudios Medioambientales, medida de luz, velocidad del viento, precipitación, temperatura, humedad, presión barométrica, actividad sísmica.

Mejora en cultivos y procesos industriales, para control de la cantidad de agua, fertilizantes, pesticidas, etc. que las plantas necesitan. Gestión de alarmas, como daños por heladas o intrusiones de animales. Para telemetría, control de calidad en procesos industriales, diagnóstico de maquinaria.

Logística y control de recursos, asignación de nodos inteligentes a los contenedores de productos, como se presenta en la figura 10.

Control de tráfico en carreteras para la detección de accidentes o atascos, el monitoreo de flujos de tráfico, y para estacionamiento donde los sensores detectan si o no está ocupado para contar la disponibilidad actual e indicar dónde se puede estacionar.

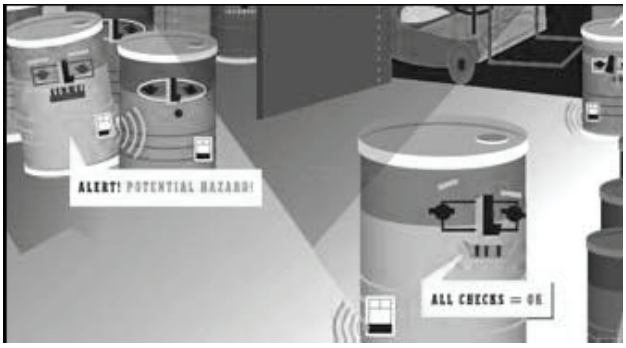

Figura 10. Control de recursos

En el ámbito de la salud pueden emplearse para monitorizar pacientes o para asistir a personas con discapacidad.

Sistemas de entretenimiento como juguetes o vídeo-juegos.

Localización de objetos y personas

Redes In-Home

Situaciones de Emergencia

2.8 Problemas y Desafíos

Sin embargo a pesar de los grandes desarrollos que se están produciendo en este campo de investigación, son muchos los problemas que quedan hoy en día por solucionar, problemas derivados directamente de las condiciones distribuidas e inalámbricas de los dispositivos que forman las redes de sensores.

Entre los problemas que comentábamos anteriormente podemos destacar principalmente dos [1]. En primer lugar los sensores se encuentran directamente ligados con el entorno que los rodea, a diferencia de las redes de datos tradicionales. Esto provoca que a la hora de diseñar el buen funcionamiento de una red de sensores, los parámetros a considerar sean muy elevados, acrecentados por la característica inalámbrica del medio de transmisión utilizado.

A continuación se presentan algunos de los problemas y desafíos en las WSN, [13], [4], [16]:

Problemas:
Optimización del consumo de energía en los nodos para lograr el máximo tiempo de vida de la red.
Ancho de banda y cobertura de la red limitados
Recursos de computación limitados
Soluciones ad-hoc para redes ad-hoc
Topología muy dinámica de la red:
- – Elementos móviles
- – Nodos con alta probabilidad de fallo
- – Nodos que entran en el sistema
- – Cuantos más nodos en la red mayor será el rendimiento.

La cobertura de red es limitada.
Heterogeneidad de hardware, interoperabilidad, incompatibilidad, sistemas operativos diferentes, por ejemplo una mote mica2 es incapaz de comunicarse con una mote micaZ.
Inexistencia de protocolos estándares que permitan a las aplicaciones interoperar.
Inexistencia de APIs estándar (para la portabilidad de las aplicaciones)

Desafíos:
Maximizar el tiempo de vida de la red al mismo tiempo que la aplicación cumple con sus requisitos de QoS:
Redes WSN fácilmente reprogramables
Redes WSN fácilmente repobladas:
Requisitos de adaptabilidad / flexibilidad
Capacidad de manejar recursos limitados de los nodos sensor.
Capacidad de comunicación con ancho de banda limitada.
Algoritmos distribuidos donde todos los nodos sean capaces de cooperar para elaborar una respuesta, tomando en cuenta las capacidades de los nodos (p.e. energía).
Heterogeneidad.

Temas para seguir investigando:
Algunos de los tópicos que han sido de interés para continuar investigando son [4], [16]**:**
Arquitectura WSN
Middleware WSN.
Optimización de redes de sensores (minimizar el tiempo de reacción, maximizar la cobertura, etc).
Técnicas para minimizar la disipación de energía de un nodo
Protocolos de enrutamiento óptimo
Seguridad en WSN
Abstracción de la WSN: WWW, BBDD, Sistema de ficheros, semántica de sensores.
Mecanismos de asignación de roles dinámicamente a nodos en una WSN para algoritmos distribuidos.
Mecanismos de localización de nodos
Extender el conjunto de funciones de TinyOS tomando como ejemplo otros S.O. embebidos como QNX, RT-Linux, etc.
Middleware que tenga en cuenta los desafíos WSN.
Mecanismos de direccionamiento
Aplicación de agentes
Aplicación de actuadores
Arquitectura común para obtener aplicaciones distribuidas en WSN

2.9 Problemas y soluciones de Seguridad

Generalmente las redes de sensores se despliegan en ambientes hostiles para la recolección de diferentes tipos de datos, por lo cual se ven expuestos a severos ataques físicos y de software. El desarrollo de métodos que aumenten la seguridad, se convierte entonces en un punto esencial en el estudio de las redes de sensores.

Tipos de Ataques
Las redes de sensores están predispuestas a múltiples ataques debido a que su despliegue se realiza en áreas abiertas. Dentro de los principales ataques se encuentran [17], [18]:

- Negación del Servicio (*Denial of Service* DoS): este tipo de ataque es a nivel físico, donde un nodo malicioso, envía indiscriminadamente mensajes que consumen el ancho de banda disponible de la red, consiguiendo la indisponibilidad temporal de un servicio o inclusive degenerando todo el sistema.
- Nodos comprometidos y suplantación de fuentes: en este caso el atacante introduce, ya sea física o por software, un nodo corrupto a la red para transmitir información corrupta.
- Recolección pasiva de información o
- *Eavesdropping*: el atacante “escucha” y recolecta la información de la red, sin realizar ningún daño al sistema.
- Ataques Físicos: son sustracción física de los nodos de la red para hurtar la información y claves de criptografía.
- SinkHole: se introduce un nodo malicioso cerca a la estación base para atraer información confidencial.
- Ataque Sybil: el atacante introduce múltiples nodos con identidades ilegítimas o con identidades hurtadas de la red.

- Ataque gusano: en este caso se genera un túnel entre dos nodos, por el cual el atacante recolecta la información y la reenvía con cierto retraso.

La figura 11 presenta las principales amenazas en las redes de sensores.

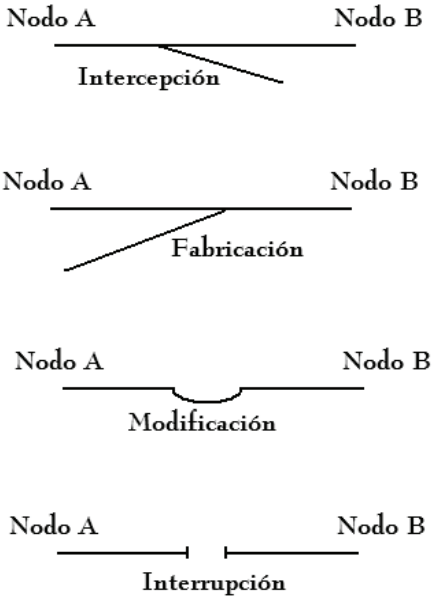

Figura 11. Amenazas de las redes WSN

A continuación se presenta un estudio de los principales problemas y las últimas soluciones planteadas en el tema de seguridad en redes de sensores inalámbricos, el manejo de claves y cifrado, el análisis de los mecanismos de manejo de claves, la autenticación y la detección.

a. Manejo de claves y cifrado

Gran parte de las implementaciones de seguridad en los WSN, utilizan cifrado y esquemas de manejo de claves. El principal problema a solucionar, es lograr que el esquema de manejo sea suficientemente eficiente de tal forma que si un intruso logra capturar un nodo, no le sea posible acceder a todas las claves de la red y por tanto a la información confidencial del sistema.

Los diferentes autores que investigan soluciones para la seguridad de las WSN, realizan suposiciones referentes a la capacidad de los diferentes nodos. Como se expresa anteriormente, los sensores poseen capacidades de procesamiento, almacenamiento y una fuente de energía limitada, sin embargo, es posible encontrar un pequeño grupo de nodos, cuyos recursos no sean tan limitados, denominados superiores o cabeza de *cluster* (celda). Para estos casos, la red es heterogénea [19], [20].

Redes Homogéneas

- Piscina de claves: Un concepto ampliamente utilizado en los mecanismos de manejo de claves es el de piscina de claves. El primer trabajo que usa el concepto de piscina es el de [21].

A diferencia de [21] donde solo se utiliza una piscina de claves, en [22], se manejan dos piscinas, una de transmisión y otra de retorno. Antes del despliegue, a cada nodo se le entregan, aleatoriamente, dos anillos de *m/2* claves de cada piscina (donde m es el número total de claves por nodo). Las piscinas se actualizan mediante una función *Hash* [23], luego de un período de tiempo o generación. Cada piscina posee P/2 claves, donde *P* es el número total de claves del sistema. Las claves de retorno se generan usando la cadena de *Lamport* basada en *Hash* [24], comenzando por las claves que corresponden a la última generación. Luego del despliegue, cada nodo inicia el reconocimiento de sus vecinos enviando un mensaje con su ID y el número de generación en el cual fue desplegado. Si un vecino encuentra claves comunes, envía un mensaje de respuesta con su ID y su generación. Se calculan entonces las generaciones en el ciclo de vida de cada nodo que se superponen, como se observa en la figura 12, pues solo en estas generaciones pueden establecer comunicación.

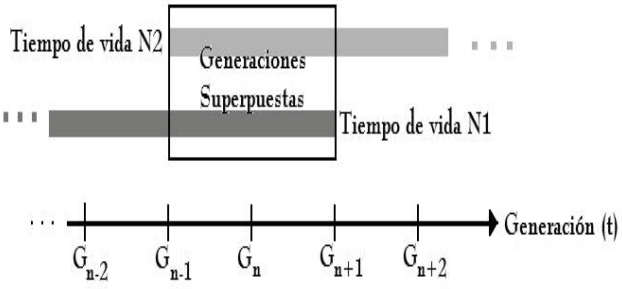

Figura 12. Ventana de generación.

Siguiendo la línea, en [25] se presentan dos esquemas donde emplean diversas piscinas. El primer esquema se denomina ABAB, debido a la utilización de dos piscinas de claves, A y B, y un tercer conjunto (S) que está compuesto por las

claves que comparten A y B. Se escogen *m* claves de A y se almacenan en un nodo y *m* claves de B y se almacenan en otro nodo. Se continúa el mismo proceso hasta completar todos los sensores de la red. Finalmente, se despliegan los nodos como se presenta en la figura 13.

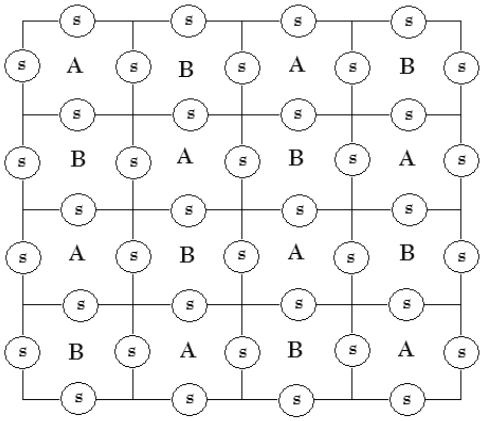

Fig. 13. Esquema ABAB

El esquema ABCD, por su parte, usa *2r* piscinas, donde *r* es el número de filas de nodos a desplegar. En este caso, el conjunto S, comprende las claves que comparten las *2r* piscinas. El despliegue se muestra en la figura 14. Una vez efectuado el despliegue, se usan los protocolos de [21], [26] para establecer claves pares entre nodos.

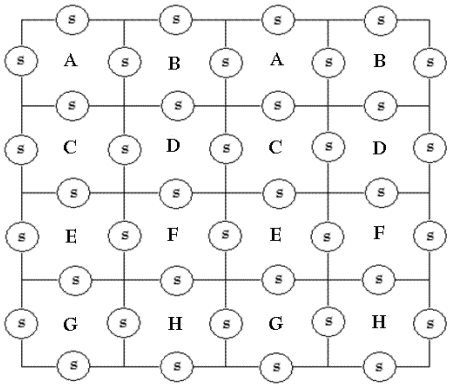

Figura 14. Esquema ABCD

En [27], se retoma la idea básica de [21], con una sola piscina de la cual se seleccionan *P* claves aleatoriamente. Se almacena un número *m* de claves en cada nodo antes de ser ubicado en el campo de sensado.

- Nodos conscientes de su localización: Existen aplicaciones en las que, debido a la hostilidad del campo de sensado, es imposible acceder vía terrestre al lugar de interés y es necesario desplegar los nodos aleatoriamente desde el aire, lo que hace muy difícil determinar su ubicación exacta en el campo. Sin embargo, existen ocasiones donde los sensores están conscientes de su localización en la red.

En [28], los autores, sugieren un nuevo esquema de generación de claves aleatorias cuando los nodos son conscientes de su localización. El campo de sensado se divide en pequeñas áreas y los N sensores desplegados, son distribuidos uniformemente en el área formando celdas, como se observa en la figura 15. Un servidor distribuye las claves en los nodos, que han sido generadas con una clave maestra y una función pseudoaleatoria.

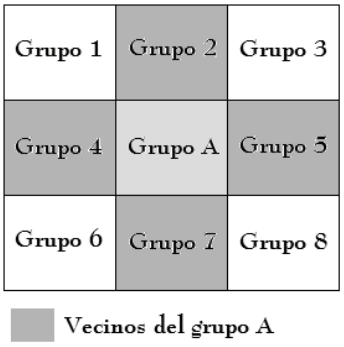

Figura15. División del área de sensado

En [29] los nodos también conocen su localización en la red. La diferencia con el anterior esquema es la introducción de un hardware reprogramable, para la generación o actualización de claves, que utiliza DES (*Data Encryption Standard*) [30].

- Otros esquemas: Algunos autores han decidido no basarse en trabajos anteriores y disminuir las consideraciones en la red de casos especiales o puntuales, como el conocimiento previo de la localización de cada nodo.

Para el cifrado, en [31] se supone que los nodos comparten una clave simétrica con la estación base y conocen la clave pública de la BS, además poseen claves pares simétricas con los vecinos.

Otra consideración simple, se encuentra en el esquema de [32], donde antes del despliegue, se selecciona una clave maestra y se decide el tamaño máximo de cada celda. A cada sensor se le

asigna una clave, encriptada en la clave maestra. La BS, entrega a los nodos una clave de grupo y computa una función polinomial f(x) de un campo finito o de Galois GF [33], que se obtienen a través de m+1 puntos (x,y) aleatorios (los puntos corresponden a localizaciones de nodos). Las funciones f(1), f(2)…f(m), junto al valor del tiempo actual *t*, encriptado en la clave de grupo y sin encriptar, son enviadas como *broadcast* a los nodos. Cada sensor, según el esquema *Shamir* [34], determina la clave con las funciones recibidas. Luego verifica si la clave encontrada es autentica, desencriptando el tiempo actual *t* y comparándolo con el recibido. Si es necesario enviar o renovar las claves, se encriptan con la clave anterior. Si se encuentra un nodo corrupto, se vuelve a calcular la función polinomial excluyendo las localizaciones de los nodos afectados.

Redes Heterogéneas

Enlaces solo con sus superiores

En las redes heterogéneas existe una jerarquización de los *clusters*, pues se tienen nodos denominados superiores. Con esta característica algunos autores han decidido que la comunicación se establezca siempre entre nodos y sus superiores y de ser necesaria una sesión entre nodos se utilice como intermedio el jefe de *cluster*. Con esto se logra reducir el número de claves almacenadas o generadas por los nodos.

En [35], se enseñan dos protocolos, donde solo trabajan con claves de grupo, claves públicas de superiores y claves de sesión con jefes de celda. Organizan la red en celdas mediante el algoritmo HEED (*Hybrid, Energy-Efficient, Distributed Clustering*) [36], de esta manera existe una jerarquización de los nodos.

Por otro lado, los autores de [37], se enfocan en el tipo de cifrado a utilizar. Está basada en LCG (generador lineal congruente, *Linear Congruential Generator*) [38], [39] y rotación ortogonal de matrices [40]. Para la primera cifrado, se genera una secuencia de números aleatorios *Sn*, de acuerdo a una semilla *So*. Estos números de secuencia, se escogen de tal manera que el flujo de números, provea un ciclo o periodo de tiempo largo y tenga buenas propiedades estadísticas. Cuando es posible trabajar con sensores que posean una considerable capacidad de almacenamiento o procesamiento, se pueden establecer sesiones entre nodos, lo que permite funciones de agregación de datos [41], protección contra intrusos, entre otros.

Para los autores en [42], los nodos poseen un par de claves pública/privada, una clave de grupo que se actualiza constantemente y un certificado de autenticidad de la clave pública, pero solo los superiores o *Gateways* pueden usar la clave pública para computar firmas digitales. Los nodos comparten la clave pública con el superior. Una autoridad de certificación, firma las claves públicas de los *gateways.*

Una función pseudo aleatoria (PRF, *Pseudo-Random Function*) es usada en [43] para crear una piscina de claves con las cuales establecer comunicación entre nodos vecinos. Suponen que los nodos son estáticos y conocen su localización en la red. Los superiores son denominados H y los nodos comunes, son llamados L.

Por otro lado en [44], se forman los *clusters* y los superiores envían un mensaje *Hello* que concatena su ID con su clave privada. Los nodos L recolectan los *Hello* y envían su propia concatenación para certificarse. Luego los nodos L generan una pseudo celda con los nodos vecinos según el diagrama de Voroni [45], con el fin, de crear sus propias claves de sesión.

En [46], se divide el campo de sensado en áreas iguales, (basado en la trabajo de [47]) como se muestra en la figura 15, los sensores conforman grupos uniformes y cada grupo selecciona un superior. Antes del despliegue se genera una clave para cada grupo de nodos y se almacena en cada integrante.

Al igual que en la investigación de [29], el trabajo en [48] introduce un componente de hardware llamado LFSR (*Linear Feedback Shift Register*). El cual es el responsable de la generación de claves. Para la arquitectura, todos los nodos deben poseer LFSR y formar celdas con superiores o cabeza de *cluster*.

b. Análisis de los mecanismos de manejo de claves

Los mecanismos de manejo de claves que utilizan el concepto de piscina de claves, deben poseer nodos con grandes capacidades de almacenamiento, lo cual, se imposibilita en la medida en que los sensores tengan limitaciones en

la memoria. Sin embargo, cuando las claves se renuevan cada cierto periodo y los nodos que fallecen son reemplazados, el número de nodos comprometidos disminuye considerablemente, como ocurre en [22]. Si además, como en [25], se trabajan con más de una piscina, las cuales pueden ser reutilizadas en diferentes zonas, los anillos de claves de cada nodo puede aumentar consiguiéndose mayor seguridad y mejor conectividad. Los mecanismos que necesitan que los nodos posean conocimiento previo de su localización, solo pueden ser usados en aplicaciones donde la red se despliegue de manera manual y premeditada. No obstante, poseen una ventaja frente a otros mecanismos cuando se usan claves maestras que el atacante no conoce y por tanto no se pueden generar claves de cifrado y descifrado [28].

El algoritmo [32], puede forzar la salida de un nodo comprometido, al aislarlo del sistema cuando genera daños en la red, pero su efectividad depende de los recursos del nodo.

Algunos esquemas, aunque son novedosos, poseen gran complejidad computacional [37] o comprometen el tamaño del chip y aumentan el consumo de potencia del nodo, disminuyendo su tiempo de vida [48]
Los mecanismos que poseen redes heterogéneas, disfrutan la ventaja frente a los sistemas homogéneos, de la posibilidad de descargar la seguridad a los nodos que tiene mayores recursos de procesamiento y almacenamiento, logrando aliviar el funcionamiento de los nodos comunes y en general de la red.

Dentro de los temas abiertos para trabajos futuros, se encuentran los siguientes aspectos:

- Mejorar la capacidad de adicionar y retirar nodos de la red sin comprometer la seguridad del sistema.
- Reducir el consumo de energía, disminuir el encabezado u *overead* de los mensajes que generan los diferentes algoritmos.
- Comprobar la efectividad de los mecanismos en diversas redes y topologías.
- Mejorar las políticas para renovar las claves de que permitan reducir el tiempo de operación.
- Concretar la arquitectura de hardware del sensor embebido [48].

c. Autenticación

La autenticación es un punto fundamental en la seguridad de las redes de sensores. Esto se debe a que un atacante puede clonar un nodo o sustraer la información de las claves de la red y enviar información maliciosa a la red. Es necesario entonces generar mecanismos que permitan a los nodos reconocer que la información recibida es auténtica, mediante la validación de la identidad del nodo transmisor. El mensaje de autenticación más utilizado es el MAC, el cual contiene diferente información que justifica la legitimidad de un nodo.

Autenticación de múltiples saltos

La autenticación por múltiples saltos se utiliza, generalmente, en la verificación de las ID de los nodos nuevos que se despliegan en la red, para generar sesiones entre nodos o simplemente en las ocasiones donde no es necesario que toda la red, solo un grupo o un nodo, conozca la validez de un sensor.

Autenticación por Broadcast

La autenticación por *broadcast* es el esquema más utilizado en las redes de sensores inalámbricos, donde su herramienta básica es la función *Hash*.

Análisis de los algoritmos de Autenticación

La base de los algoritmos de autenticación es el código de mensaje de autenticación MAC. Como adición o diferenciación, algunos utilizan dos anillos de claves aleatorios que teóricamente tiene un tiempo de vida infinito [49]. Otros manejan esquemas básicos de ID que de forma muy simple, con pocos encabezados y bajos recursos, logran que los atacantes no puedan capturar la información de la red de los datos entregados a los nodos [50].

Como beneficios agregados de la autenticación, en [51] se reducen los saltos de transmisión de los reportes, mejorando la eficiencia del filtrado de mensajes. En [52], se controlan los ataques Sybil utilizando solo criptografía simétrica, pero se debe limitar el número de nodos por grupo a 40 para que tener un grado de seguridad aceptable. Y gracias a que no se necesita de un servidor de autenticación, en [53], se reduce el tráfico y consumo de energía, pero se requieren grandes recursos computacionales para los PIV's.

Por otro lado, los atacantes pueden identificar la solución del rompecabezas, mediante la fuerza bruta [54], pero al demorar largo tiempo su ejecución, es posible renovar el rompecabezas y aumentar el grado de seguridad de la red. Como limitación del algoritmo, se encuentra la longitud del rompecabezas, pues debe ser tal que sea posible su resolución en poco tiempo por parte del transmisor, pero lo suficientemente grande para obtener mayor seguridad.

Como temas abiertos para trabajos futuros, se encuentran los siguientes aspectos:

Mayor investigación de los sistemas de detección de intrusos, IDS.
Lograr esquemas que soporten grades redes.
Reducir los recursos necesarios para el manejo de PIV's.
Al igual que en la sección anterior, mejorar la capacidad de adicionar y retirar nodos.
Reducir el costo computacional de la resolución del rompecabezas por parte del transmisor y el retraso generado [54].

d. Detección de intrusos

Debido al despliegue de los sensores en áreas abiertas, donde es posible que un atacante capture un nodo y acceda a toda su información, fácilmente se presentan ataques por clonación, por intrusos o DoS. A los nodos comprometidos se les suele denominar *Moles* [55].

Monitoreo de Nodos

Para el monitoreo de la red, varios autores, postulan el concepto de que los mejores candidatos para proteger el sistema y por ende a los sensores, son los mismos nodos.

Basados en el anterior supuesto, los autores de [56], desarrollan dos algoritmos de auto protección, donde una serie de nodos se activan para monitorear un área específica de la red. En el primero, denominado Activación Independiente Preprogramada, PIA (*Prescheduled independient activation*), cada sensor tiene una lista predefinida de activación, a la cual se acogen sin tener ningún conocimiento del comportamiento de otros sensores. De esta forma, cuando expira el reloj de un nodo, se activa el sensor con una probabilidad *P* y reinicia su reloj. Al activarse, busca nodos activos para enlazarse y compartir información de posibles eventos sospechosos, pero si no encuentra, vuelve a un estado de reposo o de sueño. Sin embargo, si ha conformado de manera premeditada, un par de comunicación con otro nodo, ambos se activan en el mismo instante. En el segundo algoritmo, llamado Cooperación de Vecinos, NC (*Neighborhood cooperative*), los nodos poseen una lista de activación distribuida, es decir los nodos se activan teniendo en cuenta el comportamiento de sus vecinos. El nodo pasa por cuatro estados, como se muestra en la figura 16. Duerme durante un periodo establecido, al terminar el periodo pasa a estado de descubrir, en el cual envía mensajes a sus vecinos para tratar de establecer conexión. Si no encuentra enlace, pasa a un estado de espera, donde sigue enviando mensajes. Cuando recibe un mensaje de aprobación pasa a estado activo y se conecta.

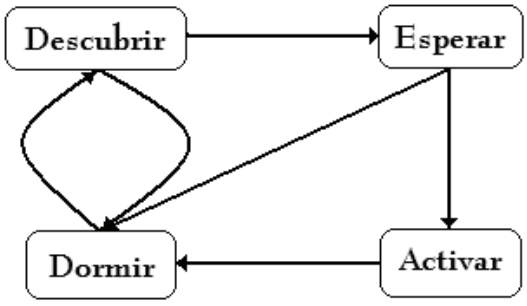

Figura 16. Diagrama de Estados del sensor

En [57], presentan el protocolo Aleatorio, eficiente y distribuido RED (*Randomized, Efficient and Distribuited*), para detección de ataques. Se fundamenta, en el conocimiento que posee cada nodo sobre su localización en la red, y su objetivo es asignar, de manera aleatoria, el rol de testigo entre los nodos para que monitoreen la red

Sistema de Detección de Intrusos

Cuando los recursos de los nodos no son tan limitados, es posible utilizar un software especial para la detección de intrusos, denominado IDS (*Intrusion Detection System).*

Los autores de [58], utilizan el Sistema de Detección de Intrusos, instalado en pequeños grupos de sensores. Estos nodos, monitorean la red buscando intrusos, manteniendo, durante un período, su área de cobertura en modo promiscuo, es decir, recolectando toda clase de información, para luego enviarla al superior de *cluster*.

Mecanismos Contra ataques DoS
Uno de los ataques más recurrentes es la Negación de Servicio, DoS, pues logra bloquear un servicio o inclusive, la red completa. Esto debido a que cada nodo del sistema coopera en diferentes actividades y su mal funcionamiento genera una cadena de deterioro en el comportamiento de toda la WSN. Para evitar este tipo de ataque, varios mecanismos se han desarrollado, basados en criptografía, autenticación, rejuvenecimiento o reinicio del sistema, entre otros.

Algunos temas para trabajos futuros

Corregir el problema de los falsos positivos.
Diferenciar el tráfico malicioso adicionado del legítimo.
Realizar simulaciones en ambientes reales [59, 60].
Realizar avances en la investigación de los nodos móviles.
Reducir el consumo de energía y costo computacional cuando se utilizan IDS [59].
Implementar la identificación de la huella dactilar en cada nodo [61].
Buscar nuevas propiedades para encontrar la huella social y extenderlas a otras redes [62].
Mejorar la tasa de uso de los mecanismos para optimizar el consumo de energía y costo del sensor [63].

2.10 Herramientas de simulación

En la mayoría de los casos los dispositivos usados para la implementación de redes de sensores inalámbricos se caracterizan por ser pequeños, autónomos, muy numerosos y con importantes limitaciones energéticas. Todos estos factores originan que los estudios analíticos a realizar sean muy complejos y los estudios experimentales muy costosos. Por ello vemos la necesidad que existe por parte de los investigadores y desarrolladores de realizar simulaciones [1] previas antes de la implantación física de estas redes.

La realización de simulaciones previas es esencial antes de la implantación de las WSN's, sobre todo si ello conlleva nuevos protocolos y funcionalidades de red. Este hecho ha provocado un auge en las herramientas de simulación disponibles. Sin embargo, la obtención de resultados fiables y representativos mediante simulaciones no es una tarea sencilla.

Hay dos aspectos claves que se deben evaluar antes de la realización de las simulaciones pertinentes:
- La utilización del modelo correcto.
- La elección de la mejor herramienta para el modelo en cuestión.

Existen simuladores que permiten realizar comparaciones de protocolos, algoritmos, pruebas de rendimiento, etc. y es posible simular una red de miles de nodos de sensores ejecutando una aplicación, o un protocolo.

Los dos simuladores más extensamente utilizados en WSN son TOSSIM [6], y NS-2 [64]. NS-2 se centra en la simulación de nodos y redes a nivel de paquete, orientado más a la simulación de protocolos y comportamientos. TOSSIM's proporciona una simulación completa de redes TinyOS a nivel de bit, Centrado a la simulación a nivel de aplicación real, no tanto a nivel de protocolos. Pero hay más simuladores, como Omnet ++ [65] y otros indicados en la figura 17.

Simulador	Disponibilidad	Escalabilidad	Lenguaje programación	Módulos sensores	Modelos Wireless	Eventos/Tiempo
S2	v	v	C++	x	v	Evento
Glomosim	v	v	C++	x	v	Evento
Opnet	x	v	C++	x	v	Evento
SensorSim	v	v	C++	v	v	Evento
Tossim	v	x	nesC	v	v	Evento
EmStar	v	v	nesC/C++	v	v	Evento/tiempo
Sens	v	v	C++	v	v	Evento
Mantis	v	x	C	v	x	Tiempo
Siesta	v	v	Java	v	x	Tiempo
Prowler	v	v	Matlab	x	v	Evento
JProwler	v	v	Java	x	v	Evento

Figura 17. Herramientas de simulación.

3. CONCLUSION

Con este trabajo, se logra una aproximación al tema de Redes de sensores inalámbricos (WSN), que encuentran multitud de aplicaciones en la sociedad actual y en ellas convergen un buen número de tecnologías de la información y las comunicaciones.
Se profundiza en la seguridad como uno de los temas de estudio más importante en las redes de sensores inalámbricos, debido a la incapacidad de utilizar los mecanismos convencionales contra ataques, pues los sensores cuentan con recursos

de procesamiento y almacenamiento limitados. Para obtener un buen grado de seguridad en las WSN, es necesario ejecutar en conjunto los mecanismos de autenticación, manejo de claves y detección de intrusos en la red.

Es un campo que esta creciendo y evolucionando y donde hay amplio material, tanto para la investigación, como para el desarrollo de productos y aplicaciones. Cómo trabajo futuro se estudiará más sobre optimización, diseño, desplegamiento, soluciones distribuidas y seguridad en las redes de sensores inalámbricas, y realizar pruebas experimentales de un modelo en una herramienta de simulación.

4. REFERENCIAS BIBLIOGRÁFICAS

[1] Corral I., Ana Belén. Diseño e implementación de un entorno de simulación para redes de sensores inalámbricos [Ingeniería de Telecomunicación]. Universidad Politécnica de Cartagena, 2005.

[2] RAAP. Redes de Sensores Inalámbricos. Disponible en: http://www.dsi.uclm.es/asignaturas/42650/ [consultado el 19 de marzo de 2009].

[3] GOMEZ M., Francisco. Departamento de Arquitectura y Tecnología de Computadores. Redes de Sensores Inalámbricas. Disponible en: http://atc.ugr.es/~aprieto/TIC_socio_sanitario/A11_4_05_Redes_sensores.pdf [consultado el 29 Diciembre 2008].

[4] Schaeffer Elisa. Un Vistazo a los fundamentos de optimización de redes sensoras. Disponible en: http://it.ciidit.uanl.mx/~elisa/presentations/optsensora.pdf [consultado el 2 de enero 2009].

[5] FRANCO B., Carlos. Tendencias: Wireless Sensor Networks. Disponible en: http://www.coit.es/publicaciones/bit/bit165/61-64.pdf [consultado el 27 Diciembre 2008].

[6] TOSSIM. Disponible en: http://www.tinyos.net/ [consultado el 2 de enero 2009].

[7] UNIVERSIDAD DE BERKELEY. Computer Science. Disponible en: http://www.cs.berkeley.edu/ [consultado el 3 enero 2009].

[8] RUIZ M., Pedro. Introducción a las redes de sensores. Disponible en: http://ants.dif.um.es/rm/ [consultado el 29 diciembre 2008].

[9] ZIGBEE ALLIANCE. Disponible en: http://www.zigbee.org/ [consultado el 2 abril de 2009]

[10] VINAGRE D., Juan José. Teoría del encaminamiento en redes Ad hoc inalámbricas. [Tesis Doctoral]. Universidad Carlos III de Madrid, 2007.

[11] Ortuño P., Miguel Angel. Protocolo de encaminamiento en origen con identificadores no únicos para redes Ad-Hoc de dispositivos con recursos limitados. [Tesis Doctoral]. Universidad Rey Juan Carlos, 2006.

[12] CEI. Metodología de despliegue para redes de sensores y estrategias de actuación. Disponible en: http://www.cei.upm.es/Seminario_CEI/2008/Presentaciones/5_Jorge_Portilla_MTP_Seminario_CEI-2.pdf [consultado el 27 de diciembre 2008].

[13] OLIVARES M., Teresa. Universidad de Castilla La Mancha. Redes de sensores inalámbricos. Disponible en: http://www.info-ab.uclm.es [consultado el 3 de enero 2009].

[14] Lédeczi, A., Nádas, A., P.V¨olgyesi, y otros. System for urban warfare. ACM Transactions on Sensor Networks 1, 2, 153–177, 2005.

[15] Self-healing minefield.Disponible en: http://www.darpa.mil/sto/smallunitops/SHM/proginfo.html [Consultado el 2 de abril de 2009].

[16] ESCOLAR D., Soledad. Estado del arte e investigación. Disponible en: http://rderuben.googlepages.com/wsn.pdf/ [consultado el 2 de enero 2009].

[17] K. Papadopoulos, T. Zahariadis, N. Leligou y S. Voliotis, Sensor Networks Security Issues In Augmented Home Environment. IEEE International Symposium on Consumer Electronics,ISCE 2008. Abril de 2008.

[18] T. Zia y A. Zomaya, Security Issues in Wireless Sensor Networks. International Conference on Systems and Networks Communications,ICSNC. Octubre de 2006.

[19] V. Mhatre, C. P. Rosenberg, y D. Kofman, et al., A Minimum Cost Heterogeneous Sensor Network with a Lifetime Constraint, IEEE Transactions on Mobile Computing. Vol. 4. Enero de 2005,

[20] M. Yarvis, N. Kushalnagar, y H. Singh, et al., Exploiting Heterogeneity in Sensor Networks, Proc. of IEEE INFOCOM 2005.

[21] L. Eschenauer y V. D. Gligor, A key-management scheme for distributed sensor networks. Proceedings of the 9th ACM conference on Computer and communications security, pp. 41-47, Noviembre de 2002.

[22] C. Castelluccia y Angelo Spognardi, RoK: A Robust Key Pre-distribution Protocol for Multi-Phase Wireless Sensor Networks. Third International Conference on

Security and Privacy in Communications Networks and the Workshops, SecureComm 2007.

[23] I. Mironov, Hash functions: Theory, attacks, and applications. Microsoft Research, Silicon Valley Campus. Noviembre de 2005. (En Línea): https://research.microsoft.com/users/mironov/papers/hash_survey.pdf

[24] L. Lamport, Password authentication with insecure communication. Commun. ACM, vol. 24, no. 11, 1981.

[25] S. Emre Taşçı, E. Bayramoğlu y A. Levi, Simple and Flexible Random Key Predistribution Schemes for Wireless Sensor Networks Using Deployment Knowledge. International Conference on Information Security and Assurance. IEEE 2008.

[26] W. Du, J. Deng, Y.S. Han, S. Chen, and P.K. Varshney, A key management scheme for wireless sensor networks using deployment knowledge, IEEE Infocom, 2004.

[27] Y. Ho Kim, H. Lee y D. Hoon Lee, A secure and efficient key management scheme for wireless sensor networks. Security and Privacy in Communications Networks and the Workshops, SecureComm 2007. Third International Conference, 17-21 Septiembre de 2007.

[28] J. Young Chun, Y. Ho Kim, J. Lim y D. Hoon Lee, Location-aware Random Pair-wise Keys Scheme for Wireless Sensor Networks. Third International Workshop on Security Privacy and Trust in Pervasive and Ubiquitous Computing. 2007.

[29] M. Meribout y A. Al-Zoubi, A Recurrent Decentralized Key Management Architecture for Wireless Sensor Network. Proceedings of the 2nd international workshop on Agent-oriented software engineering challenges for ubiquitous and pervasive computing. 2008.

[30] U.S. Department Of Commerce/National Institute Of Standards And Technology, Data Encryption Standard, (Des). Federal Information Processing Standards Publication. Octubre de 1999. (En línea): http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[31] J. Luo, P. Papadimitratos y J-P. Hubaux, GossiCrypt: Wireless Sensor Network Data Confidentiality Against Parasitic Adversaries. 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, IEEE SECON '08, 2008..

[32] X. Yi, M. Faulkner y E. Okamoto, Securing Wireless Sensor Networks. The Third International Conference on Availability, Reliability and Security. IEEE 2008.

[33] MIT open Course Aware, Chapter 7: Introduction to finite fields. Ingeniería eléctrica y ciencias de la computación. (En línea): http://ocw.mit.edu/NR/rdonlyres/ElectricalEngineering-and-Computer-Science/

[34] A. Shamir, How to share a secret, Communications of the ACM, vol. 22, no. 11, pp. 656-715. Nov 1979.

[35] J. Abraham y K. S. Ramanatha, A Complete Set of Protocols for Distributed Key Management in Clustered Wireless Sensor Networks, International Conference on Multimedia and Ubiquitous Engineering. ACM, 2007.

[36] Ossama Younis and Sonia Fahmy, HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad-hoc Sensor Networks, IEEE Transactions on Mobile Computing, volume 3. 2004.

[37] A. Hamid, M. Mahbub Alam y C. Seon Hong, Developing a Security Protocol based on LCG and Orthogonal Matrices for Wireless Sensor Networks. The 9th International Conference on Advanced Communication Technology**.** Febrero de 2007.

[38] D.E. Knuth, Deciphering a Linear Congruential Encryption. IEEE Transactions on Information Theory, Vol. IT-X, no. 1, pp.49-52, Enero de 1985,.

[39] D.E. Knuth, The Art of Computer Programming, Vol 2: Seminumerical Algorithms. Ed. Addison-Wesley, 1969.

[40] I. Ingemarsson, Commutative Group Codes for the Gaussian Channel. IEEE Transactions on Information Theory, vol. IT-19, no. 5, pp. 215-219, Marzo de 1973.

[41] K-W. Fan, S. Liu y P. Sinha, Scalable Data Aggregation for Dynamic Events in Sensor Networks. Conference On Embedded Networked Sensor Systems**.** Proceedings of the 4th international conference on Embedded networked sensor systems. Noviembre de 2006.

[42] J. Mache, C-Y. Wan y M. Yarvis, Exploiting Heterogeneity for Sensor Network Security. 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. SECON 2008.

[43] X. Du, H-H. Chen, Y. Xiao y M. Guizani, A Pseudo-Random Function based Key Management Scheme for Heterogeneous Sensor Networks. IEEE GLOBECOM 2007 proceedings.

[44] J. Brown, X. Du, y K. Nygard, An Efficient Public-Key-Based Heterogeneous Sensor Network Key Distribution Scheme. IEEE GLOBECOM 2007 proceedings.

[45] F. Aurenhammer y R. Klein, Voronoi Diagrams. (En Línea): http://www.pi6.fernuni-hagen.de/publ/tr198.pdf

[46] Y. Sun, J. Zhang, H. Ji y T. Yang, KMSGC: A Key Management Scheme for Clustered Wireless Sensor Networks Based on Group-oriented Cryptography**.** IEEE International Conference on Networking, Sensing and Control, ICNSC 2008. Abril de 2008.

[47] W. Du, J. Deng, Y. S. Han, S. Chen, y P. K. Varshney., A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge. INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies. Marzo de 2004.

[48] Kalpana Sharma, Vikash Varun y Rohit Kumar, System on Chip for Sensor Network Security: A Proposed Architecture. 10th International Conference on Advanced Communication Technology, ICACT 2008.

[49] J. Zhang, X. Liu Y H. Xu, An Efficient Scheme for Broadcast Authentication in Wireless Sensor Networks. ASIAN ACM Symposium on Information, Computer and Communications Security**.** Proceedings of the 2006 ACM Symposium on Information, computer and communications security. 2006.

[50] N. Sultana y E-N. Huh, An Efficient Scheme for Secure Group Communication in Mobile Wireless Sensor Networks. Conference on Ubiquitous Information Management And Communication. Proceedings of the 2nd international conference on Ubiquitous information management and communication. ACM, 2008.

[51] Byung Hee Kim y Tae Ho Cho, Efficient Selection Method of Message Authentication Codes for Filtering Scheme in Sensor networks. Conference on Ubiquitous Information Management And Communication. Proceedings of the 2nd international conference on Ubiquitous information management and communication. ACM, 2008

[52] J. Yin y S. Kumar Madria, Sybil Attack Detection in a Hierarchical Sensor Network. Third International Conference on Security and Privacy in Communications Networks and the Workshops, SecureComm 2007.

[53] K. Chang y K. G. Shin, Distributed Authentication of Program Integrity Verification in Wireless Sensor Networks. Securecomm and Workshops. IEEE, 2006**.**

[54] P. Ning, A. Liu y W. Du, Mitigating DoS Attacks against Broadcast Authentication in Wireless Sensor Networks. ACM Transactions on Sensor Networks, Vol. 4, No. 1, Article 1. Enero de 2008

[55] F. Ye, H. Yang, y Z. Liu. Catching "Moles in Sensor Networks. 27th International Conference on Distributed Computing Systems. 2007.

[56] D. Wang, Q. Zhang y J. Liu, The Self-Protection Problem in Wireless Sensor Networks. ACM Transactions on Sensor Networks, Vol. 3, No. 4, Article 20. Octubre de 2007.

[57] M. Conti, R. Di Pietro, L. V. Mancini y A. Mei, A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks. The ACM International Symposium on Mobile Ad Hoc Networking and Computing. 2007.

[58] M. Ketel, Applying the Mobile Agent Paradigm to Distributed Intrusion Detection in Wireless Sensor networks. 40th Southeastern Symposium on System Theory. IEEE, Marzo de 2008.

[59] I. Chatzigiannakis y A. Strikos, A Decentralized Intrusion Detection System for Increasing Security of Wireless Sensor Networks, Emerging Technologies and Factory Automation, ETFA 2007.

[60] G. Huo y X. Wang, DIDS: A Dynamic Model of Intrusion Detection System in Wireless Sensor Networks. Proceedings of the 2008 IEEE International Conference on Information and Automation. Zhangjiajie, China. Junio de 2008.

[61] K. Bonne Rasmussen y S. Capkun, Implications of Radio Fingerprinting on the Security of Sensor Networks. Third International Conference on Security and Privacy in Communications Networks and the Workshops, SecureComm 2007.

[62] K. Xing, F. Liu, X. Cheng y D. H.C. Du, Real-time Detection of Clone Attacks in Wireless Sensor Networks**.** The 28th International Conference on Distributed Computing Systems. IEEE 2008.

[63] D. Seong Kim, C. Su Yang, y J. Sou Park, Adaptation Mechanisms for Survivable Sensor Networks against Denial of Service Attack. Second International Conference on Availability, Reliability and Security. ACM. 2007.

[64] NETWORK SIMULATOR. Disponible en: http://www.isi.edu/nsnam/ns/ [consultado el 3 de enero 2009].

[65] OMNET++. Disponible en: http://www.omnetpp.org/index.php [consultado el 3 de enero 2009].