UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

REDES INALÁMBRICAS DE SENSORES: APLICACIONES, PROTOCOLOS DE ENRUTAMIENTO Y SEGURIDAD.

TRABAJO MONOGRÁFICO
PARA OBTENER EL GRADO DE

INGENIERO EN REDES.

PRESENTA
FREDDY JOSUÉ ESCALANTE UICAB

SUPERVISORES
DR. HOMERO TORAL CRUZ.
DR. FREDDY IGNACIO CHAN PUC.
DR. JOSÉ ANTONIO LEÓN BORGES.

SUPERVISORES SUPLENTES
MT. MARTÍN ANTONIO SANTOS ROMERO.
M.S.I. LUIS FERNANDO MIS RAMÍREZ.

CHETUMAL QUINTANA ROO, MÉXICO, NOVIEMBRE DE 2019

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO MONOGRÁFICO TITULADO

"REDES INALÁMBRICAS DE SENSORES: APLICACIONES, PROTOCOLOS DE ENRUTAMIENTO Y SEGURIDAD."

ELABORADO POR

FREDDY JOSUÉ ESCALANTE UICAB

BAJO SUPERVISIÓN DEL COMITÉ DEL PROGRAMA DE LICENCIATURA Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:

INGENIERO EN REDES

COMITÉ SUPERVISOR

SUPERVISOR:

DR. JOSÉ ANTONIO LEÓN BORGES.

SUPERVISOR:

DR. HOMERO TORAL CRUZ.

SUPERVISOR:

Dr. FREDDY IGNACIO CHAN PUC.

SUPLENTE:

M.T. MARTÍN ANTONIO SANTOS ROMERO.

SUPLENTE:

M.S.I. LUIS FERNANDO MIS RAMÍREZ.

CHETUMAL QUINTANA ROO, MÉXICO, NOVIEMBRE DE 2019

RESUMEN

Las redes inalámbricas de sensores (WSNs) se han convertido en una de las áreas de investigación más atractivas en diversos campos científicos en los últimos años.

WSN se compone de varios nodos sensores que recopilan datos en áreas de difícil acceso y los envían a la estación base (BS). Al mismo tiempo las redes de sensores tienen algunas características especiales en comparación con las redes tradicionales que hacen que sea difícil competir con ellas.

La arquitectura de la pila de protocolos usado por la estación base y los nodos, integran energía y enrutamiento consciente (es decir, se está consciente de la energía de enrutamiento), integra los datos con protocolos de red (es decir, agregación de datos), se comunica haciendo uso eficiente de la energía a través del medio inalámbrico y promueve esfuerzos cooperativos de los nodos sensores (es decir, el plano de gestión de tareas).

CONTENIDO

Introducción

Las redes de sensores inalámbricas (WSN) se han convertido en una de las áreas de investigación más atractiva en muchos ámbitos científicos en los últimos años. WSN se compone de varios nodos sensores que recopilan datos en áreas de difícil acceso y los envían a la estación base (BS) o sumidero (Akyildiz, Su, Sankarasubramaniam, y Cayirci, 2002a). Al mismo tiempo las redes de sensores tienen algunas características especiales en comparación con las redes tradicionales, que hacen que sea difícil competir contra este tipo de redes.

La arquitectura del protocolo usado por la estación base y los sensores nodos (Akyildiz, Su, Sankarasubramaniam, y Cayirci, 2002b), integran la energía y la conciencia del enrutamiento (es decir, consciente de la energía de enrutamiento), integra los datos con protocolos de red (es decir, la agregación de datos), se comunica a través de la energía de manera eficiente a través del medio inalámbrico, y promueve los esfuerzos de cooperación de los nodos sensores (es decir, del plano de gestión de tareas). La pila de protocolos de red de sensores es muy similar a la pila de protocolos tradicionales (Maraiya, Kant, y Gupta, 2011), con las siguientes capas: la capa física, la capa de enlace de datos, la capa de red, capa de transporte, la capa de aplicación, del plano de gestión de energía, la gestión de la movilidad avión, y el plano de gestión de tareas. WSNs tienen diversas aplicaciones; ejemplos incluyen aplicaciones militares, monitoreo ambiental, aplicación médica, uso casero, aplicación industrial y comercial.

WSN está desplegado en entornos físicos difíciles y hostiles donde los nodos están siempre expuestos a riesgos de daños físicos (Alrajeh, Khan, y Shams, 2013). En redes inalámbricas de sensores, una de las limitaciones más importantes es el requisito de bajo consumo de energía. Los nodos de sensores llevan fuentes de energía limitadas, por lo general irremplazables. Por lo tanto, deben tener mecanismos de trade-off incorporados que le dan al usuario final la opción de prolongar la vida de la red a costa de rendimiento menor o mayor retardo de transmisión (Akyildiz, Su, Sankarasubramaniam, y Cayirci, 2002a). Con el fin de adquirir la eficiencia energética, diversos métodos de enrutamiento jerárquicos o basadas en clusters, propuesta originalmente en las redes de cable, son técnicas bien conocidas con ventajas especiales relacionadas con la escalabilidad y la comunicación eficiente. En una arquitectura jerárquica, los nodos más altos de energía se pueden usar para procesar y enviar la información, mientras que los nodos de baja energía se puede utilizar para realizar la detección en las proximidades del objetivo. La creación de grupos y asignación de tareas especiales puede contribuir en gran medida a la escalabilidad del sistema en general, toda la vida, y la eficiencia energética. El objetivo principal de enrutamiento jerárquico es mantener de manera eficiente el consumo de energía de los nodos de

sensores mediante su participación en la comunicación de múltiples saltos. la formación de agrupaciones se basa típicamente en la reserva de energía de los sensores y la proximidad del sensor a la cabeza del racimo. Varios protocolos de enrutamiento basadas en clusters se proponen en la literatura como Leach (Heinzelman, Chandrakasan, y Balakrishnan, 2002), TEEN (Lee, Noh, y Kim, 2013), APTEEN (Manjeshwar y Agrawal, 2002), HEED (Younis y Fahmy, 2004), Pegasis (Lindsey, y Raghavendra, 2002) y Heep (Boubiche, y Bilami, 2011). Cuando LEACH es uno de los primeros enfoques jerárquicos para las redes de sensores.

La organización de los nodos de la red de cadenas evita la mala disipación de energía en el protocolo de LEACH y reduce el retraso de enrutamiento generada por el protocolo Pegasis (Boubiche, y Bilami, 2011). Con base en el enfoque de la agrupación de las cadenas, en cada clúster nodo de cadenas adyacentes se forman y el nodo más potente es seleccionado para ser la cabeza de clúster (CH). Todos los nodos transmiten sus datos recogidos a su CH usando cadenas vecinas de los nodos. A continuación, la CHS transmiten los datos recibidos directamente a la estación base, o indirectamente a través de los vecinos CHS. La transmisión de los datos recogidos a través de las cadenas de los nodos vecinos puede reducir las distancias de transmisión y optimizar el consumo de energía. La agregación de datos se aplica por cada nodo en una cadena para reducir la cantidad de datos que se intercambian entre los nodos y su CH, que se reserva la energía (Boubiche, y Bilami, 2011).

Los investigadores recientemente han comenzado a estudiar el movimiento del sensor y atributos únicos de las redes de sensores móviles ya que se asumió que las redes de sensores originalmente sólo ingresen con nodos estáticos. Se ha sugerido que la movilidad de los sensores nodo mejora la cobertura de detección. Las pulgas de proyectos robóticos en Berkeley; Robocontrolmote y Movilidad parasita eran intentos para permitir la movilidad en redes de sensores. En Leach (Heinzelman, Chandrakasan, y Balakrishnan, 2002), la movilidad no es compatible de forma directa. En una ocasión, si un nodo se aleja del clúster en cabeza tiene que gastar más energía para mantenerse en contacto con el clúster a cabeza. Para mitigar este problema se ha propuesto M-Leach (Nguyen, Defago, Beuran, y Shinoda, 2008). Adicional a M-Leach, hay algunos protocolos de red de sensores móviles (MSN) como Leach-Mobile (Kim y Chung, 2006), Leach-ME (Kumar, Vinu, y Jacob, 2008), Energy Efficient Mobile Wireless Sensor Network Routing Protocol… Protocolo de enrutamiento de red de sensor inalámbrico de energía eficiente (E2 MWSNRP) (Sara, Kalaiarasi, Pari, y Sridharan, 2010) y Grid Based Energy Efficient Routing el Grid basado Energía Eficiente de enrutamiento (GBEER) (Kweon, Ghim, Hong, y Yoon, 2009) que

fue propuesto para la comunicación de múltiples fuentes a múltiples sinks móviles en la red de sensores inalámbricos.

Adicional a las restricciones de energía y movilidad, la mayoría de redes inalámbricas de sensores son vulnerables a muchos tipos de ataques a la seguridad debido a abrir medios inalámbricos, comunicación multi-hop descentralizado, y el despliegue en zonas hostiles y físicamente no protegidas (Alrajeh, Khan, y Shams, 2013).

Basado en (Karlof, y Wagner, 2003) la investigación, podemos clasificar los ataques de enrutamiento en seis Categorías: ataque agujero, agujero negro de ataque, ataque de un desvío selectivo, ataque Sybil, ataque de inundación "ola" y Redirección.

Además de la eficiencia energética, la movilidad y la seguridad todavía existen algunos otros temas de investigación abiertas, tales como: integración de las redes de sensores e Internet, redes inalámbricas de sensores en entornos difíciles (redes de sensores inalámbricas subterráneas (WUSNs) y redes de sensores inalámbricos bajo el agua UWSNs) y redes de sensores inalámbricos multimedia.

Capítulo 1. Introducción a las Redes de Sensores Inalámbricos (Wireless Sensor Networks WSN´s)

1.1. Conceptos Básicos

Las redes de sensores representan una mejora significativa sobre los sensores tradicionales, que se despliega en las dos formas siguientes (Akyildiz, Su, Sankarasubramaniam, Y Cayirci, 2002a): 1) Los sensores pueden ser colocados lejos del fenómeno real. Por lo tanto, grandes sensores que utilizan algunas técnicas complejas para distinguir los objetivos del ruido ambiental son obligatorios. 2) Solo se pueden implementar varios sensores que sólo realizan la detección. Las posiciones de los sensores y las comunicaciones son topología cuidadosamente diseñado.

Las primeras redes de sensores involucraban transductores simples que convierten una medida variable en una señal que puede ser transmitida a un sistema central de procesamiento para su análisis. Estas redes de sensores se basan en una topología en estrella, con un solo salto punto a punto de enlace entre el sensor y la estación base central. Los requisitos de alimentación de enlaces de un solo salto limitan el alcance de la red, a menos que una fuente de alimentación importante está disponible en cada nodo (Loo, C. E., Yong, M., Leckie, C., y Palaniswami).

A fin de que las redes de sensores se pueden utilizar para varias áreas de aplicación, se requieren técnicas de redes inalámbricas ad hoc. Aunque se han propuesto muchos protocolos y algoritmos para redes ad hoc inalámbricas tradicionales que no se adaptan bien a las características únicas y requisitos de las aplicaciones de las redes de sensores. Muchos investigadores están actualmente involucrados en el desarrollo de esquemas que cumplan estos requisitos. Las principales diferencias entre las redes de sensores y redes ad hoc son (Akyildiz, Su, Sankarasubramaniam, y Cayirci, 2002b):

- El número de nodos de sensores en una red de sensores puede ser varios órdenes de magnitud mayor que los nodos en una red ad hoc.
- Los nodos de sensores están densamente desplegados.
- Los nodos sensores son propensos a fallas.
- La topología de una red de sensores cambia con mucha frecuencia.

- Los nodos de sensores frecuentemente utilizan un paradigma de comunicación de difusión, mientras que la mayoría de las redes ad hoc se basan en comunicaciones punto a punto.
- Los nodos de sensores están limitados en potencia, capacidades computacionales y de memoria.
- Los nodos de sensores pueden no tener identificación global (ID) a causa de la gran cantidad de gastos generales y número grande de sensores.

Las redes de sensores inalámbricos se componen de varios sensores nodos, donde el objetivo principal de un sensor nodo es recoger información de su entorno y transmitirla a uno o más puntos de estaciones de control centralizados llamados estaciones base (Akyildiz, Su, Sankarasubramaniam, y Cayirci, 2002a; Karlof, y Wagner, 2003; Alrajeh, Khan, y Shams, 2013). Una estación base es típicamente muchas órdenes de magnitud más potente que un sensor nodo, con enlaces de banda ancha para la comunicación entre ellos. Puede ser una puerta de entrada a otra red, un potente procesamiento de datos, un centro de almacenamiento, o un punto de acceso para la interfaz humana y puede ser utilizado como un nexo para difundir la información de control en la red o extraer datos de ella (Karlof, y Wagner, 2003). Por otra parte, los sensores nodos se ven obligados a utilizar menor potencia, de menor ancho de banda, radios de corto alcance, también tienen la capacidad de auto-curación y auto-organización. Son descentralizados y distribuidos en la naturaleza y forman una red inalámbrica de saltos múltiples para permitir que se comuniquen a la estación base más cercana (Karlof, y Wagner, 2003; Alrajeh, Khan, y Shams, 2013).

Una de las ventajas de las redes inalámbricas de sensores es su capacidad para operar sin supervisión en ambientes hostiles, donde los esquemas de monitoreo son riesgosos, ineficientes y algunas veces no factibles. Por lo tanto, se espera que los sensores sean desplegados de forma aleatoria en el área de interés por un medio relativamente no controlado. Dada la vasta área a cubrir, la corta vida de los sensores que funcionan con baterías y la posibilidad de tener nodos dañados durante el despliegue, se espera una gran población de sensores en la mayoría de las aplicaciones WSNs. El diseño y la operación de una red de gran tamaño requerirían estrategias arquitectónicas y de gestión escalables. Además, los sensores en este tipo de entornos son de energía finita y sus baterías no se pueden recargar. Por lo tanto, el diseño de algoritmos de energía se convierte en un factor importante para extender la vida útil de los sensores. La agrupación de sensores nodos ha sido ampliamente perseguida por la comunidad de investigación con el fin de alcanzar el objetivo de escalabilidad de la red (Abbasi y Younis, 2007).

1.2. ¿Qué es una Red de Sensores Inalámbricos?

Es una infraestructura compuesta por varios nodos de sensores, donde el objetivo principal de un nodo sensor es recopilar información de su entorno y transmitirlo a uno o más puntos de control centralizado; llamadas estaciones base.

1.3. Importancia de una Red de Sensores Inalámbricos.

Las redes inalámbricas de sensores (WSNs) se han convertido en una de las áreas de investigación más atractivas en diversos campos científicos en los últimos años.

WSN se compone de varios nodos sensores que recopilan datos en áreas de difícil acceso y los envían a la estación base (BS). Al mismo tiempo las redes de sensores tienen algunas características especiales en comparación con las redes tradicionales que hacen que sea difícil competir con ellas.

La arquitectura de la pila de protocolos usado por la estación base y los nodos, integran energía y enrutamiento consciente (es decir, se está consciente de la energía de enrutamiento), integra los datos con protocolos de red (es decir, agregación de datos), se comunica haciendo uso eficiente de la energía a través del medio inalámbrico y promueve esfuerzos cooperativos de los nodos sensores (es decir, el plano de gestión de tareas).

Capítulo 2. Arquitectura de Protocolo

2.1. Arquitectura de Protocolo de Pila

Los protocolos de pila son una combinación de diferentes capas y se compone de la capa física, capa de enlace de datos, capa de red, capa de transporte, capa de aplicación, el plano de gestión de energía, el plano de gestión de movilidad y el plano de gestión de tareas. Cada capa tiene un conjunto de protocolos con diferentes operaciones e integrados con otras capas. El protocolo de pila utilizado por los nodos del fregadero y los sensores se muestra en la Figura 1.

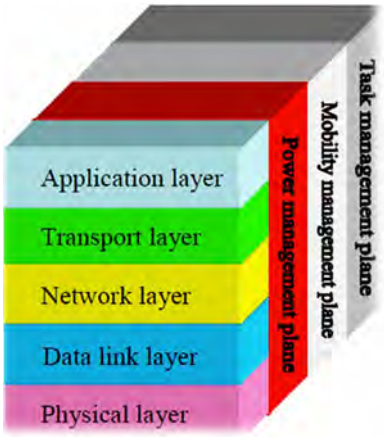

Figura 1

2.1.1. Capa Física

La capa física es responsable de la selección de frecuencia, la generación de frecuencia portadora, la detección de señales, modulación y codificación de datos. La generación de frecuencia y detección de señal tienen más que ver con el diseño del hardware y el transceptor subyacente. La capa física presenta muchas cuestiones de investigación abiertas que son en gran parte inexploradas. Los temas de investigación incluyen esquemas de modulación, las estrategias para superar los efectos de propagación de señal y diseño de hardware (Kifayat, Merabti, Shi, y Llewellyn, 2010).

2.1.2. Capa de Enlace de Datos

La capa de enlace de datos es responsable de la multiplexación de flujos de datos, la detección de tramas de datos, y de acceso al medio y de control de errores. Se asegura de que la conexión punto a punto y conexiones punto a multipunto sean fiables en una red de comunicación. La capa de enlace de datos es una combinación de diferentes protocolos, incluye: control de acceso al medio (MAC) y el control de errores.

- Protocolos MAC: Organiza miles de sensores nodos y establece el enlace de comunicación usando salto a salto (hop by hop) para transferir datos de manera eficiente y de manera justa y compartir recursos de comunicación entre los sensores nodos.
- Esquemas de Control de Errores: Dos tipos importantes de control de errores en las redes de comunicación son la corrección de errores hacia adelante (FEC) y técnicas de petición de repetición automática (ARQ). Los trabajos de investigación en todas estas áreas continúan brindando mejoras.

2.1.3. Capa de Red

La capa de red es proporcionar la interconexión con las redes externas como otras redes de sensores, en un escenario, los nodos de hundimiento se pueden usar como una puerta de enlace a otras redes. La capa de red en una WSN debe ser diseñado con las siguientes consideraciones: La eficiencia energética, las redes inalámbricas de sensores se centran en datos de redes WSN que se han basado en atributos de direccionamiento y los sensores nodos son conscientes de la ubicación. La capa de enlace se encarga de cómo dos nodos se comunican entre sí, la capa de red es responsable de decidir qué nodo con quien hablar.

2.1.4. Capa de Transporte

La capa de transporte entra en juego cuando el sistema necesita comunicarse con el mundo exterior. La transmisión de datos desde dentro hasta el usuario externo es un problema porque las redes inalámbricas de sensores no usan una identificación global y atributos basados en nombramiento se utiliza para enviar los datos. Muy poca investigación se ha hecho en la capa de transporte.

2.1.5. Capa de Aplicación

La capa de aplicación contiene la lógica necesaria para la adquisición y procesamiento de datos. Una sencilla aplicación podría medir cantidades, tales como la temperatura, la humedad o la luminosidad en intervalos regulares y reenviar los datos a un nodo receptor. Otras aplicaciones también pueden procesar los datos medidos, servir peticiones de datos o enviar mensajes en respuesta a eventos externos. Además, las aplicaciones también necesitan decidir qué nodos envíen sus datos. Estos pueden ser nodos específicos o un destino de alto nivel tales como sumideros de datos.

2.1.6. Plano de Gestión de Movilidad

El plano de gestión de la movilidad detecta y registra el movimiento de los sensores nodo, por lo que una ruta de vuelta al usuario siempre se mantiene, puede realizar un seguimiento de sus sensores nodo que son vecinos. Al saber quiénes son los vecinos, los nodos sensores pueden equilibrar su poder y uso de tareas.

2.1.7. Plano de Gestión de Energía

El plano de gestión de energía administra la forma en que un sensor nodo utiliza su poder y gestiona el consumo de energía entre las tres operaciones (detección, cómputo y comunicaciones inalámbricas). Por ejemplo, para evitar recibir mensajes duplicados, un sensor nodo puede apagar su receptor después de recibir un mensaje de uno de sus vecinos. Además, un sensor nodo transmite a sus vecinos una baja en el poder y no puede participar en mensajes de enrutamiento. La energía restante se reserva para la detección de tareas.

2.1.8. Plano de Gestión de Tareas

El plano de gestión de tareas (es decir, los esfuerzos de cooperación de los sensores nodo) programa saldos y horarios de detección de los eventos y de las tareas de un área específica. Por lo tanto; no todos los nodos de sensores en esa área específica se requieren para llevar a cabo las tareas de detección al mismo

tiempo. Dependiendo de su nivel de potencia, algunos nodos realizan la tarea de detección más que otros.

Capítulo 3. Protocolos de Enrutamiento

3.1. Desafíos de los Protocolos de Enrutamiento

Wireless Sensor Networks presentan grandes desafíos en términos de aplicación. Hay varios atributos clave que los diseñadores deben considerar con cuidado, que son de particular importancia en las redes de sensores inalámbricas. (Joshi y Priya, 2011) describen estos retos como los siguientes:

- El costo de Clustering;
- Selección de Cluster-cabezas y Clusters;
- Funcionamiento en tiempo real;
- Sincronización;
- La agregación de datos;
- Los mecanismos de reparación;
- Calidad de Servicio (QoS).

3.2. Protocolos de Enrutamiento Basados en Clúster para WSN

Hay diferentes maneras en que podemos clasificar los protocolos de enrutamiento de redes de sensores. De acuerdo con la estructura de la red, estos protocolos de enrutamiento se pueden clasificar como plana, jerárquica, y los protocolos basados en la localización. Con el fin de adquirir la eficiencia energética, diversos métodos de enrutamiento jerárquicos o basadas en clusters, propuesta originalmente en las redes de cable, son técnicas bien conocidas con ventajas especiales relacionadas con la escalabilidad y la comunicación eficiente. En el enrutamiento basado en clúster, los nodos desempeñan diferentes funciones o funcionalidades, con el objetivo de formar técnicas de enrutamiento de agrupamiento de los nodos con diferentes roles para que las cabezas del clúster pueden hacer algo de agregación de datos o confusión con el fin de ahorrar energía, en el siguiente artículo se describe algunos de los retos de la agrupación.

3.2.1. LEACH

Leach (Low Energy Adaptive Clustering Hierarchy) es una auto-organización y Protocolo de agrupamiento adaptable propuesto por (Heinzelman,

Chandrakasan, y Balakrishnan, 2002) que utiliza la aleatorización para distribuir la carga de energía de manera uniforme entre los nodos sensores. En el esquema de filtración, los nodos se organizan en un grupo local y un nodo se comporta como una cabeza de clúster local. LEACH incluye una rotación aleatoria de la posición de la cabeza clúster de alta energía, que rota entre los sensores. Esta característica conduce a una distribución equilibrada del consumo de energía a todos los nodos y hace que sea posible tener una mayor vida útil para toda la red.

3.2.2. TEEN

TEEN (Threshold sensitive Energy Efficient sensor Network) es un protocolo de enrutamiento básico de múltiples saltos en clúster jerárquico (Lee, Noh, y Kim, 2013). En el protocolo Teen, en cada fase de configuración de clúster, el clúster de cabeza transmite a sus miembros de clúster los siguientes valores de umbral: a) umbral duro: es un valor absoluto para el atributo detectado. Si el nodo detecta este valor, se convierte en su transmisor e informa de los datos a la CH. b) umbral suave: es una pequeña variación en el valor del atributo detectado, lo que hace que el nodo gire sobre su transmisor. La primera vez que un parámetro del conjunto de atributo alcanza su valor umbral de fuerza, el nodo transmite los datos detectados. El valor detectado se almacena en una variable llamada valor detectado. El nodo transmitirá los datos en el periodo del brote actual sólo cuando se cumplen las dos condiciones siguientes: 1) el atributo detectado es mayor que el umbral de fuerza; 2) el atributo detectado difiere del valor detectado por una cantidad igual o mayor que el umbral suave. De este modo, el umbral de fuerza trata de reducir el número de transmisiones enviando sólo cuando el atributo detectado está en el rango de interés. El umbral suave reduce el número de transmisión mediante la eliminación de todas las transmisiones, que tienen poco o ningún cambio en el atributo detectado (Lee, Noh, y Kim, 2013).

3.2.3. APTEEN

APTEEN (Adaptive Threshold sensitive Energy Efficient sensor Network protocol) (Manjeshwar y Agrawal, 2002) es una extensión de Teen y tiene por objeto tanto la captura de las colecciones de datos periódicos y reaccionar a los eventos de tiempo crítico. La arquitectura es la misma que en Teen. Cuando la estación base forma las agrupaciones, las cabezas de racimo transmiten los atributos, los valores umbral y el horario de transmisión a todos los nodos. Las

cabezas también llevan a cabo la agregación de datos con el fin de ahorrar energía. APTEEN soporta tres tipos de consulta diferentes: histórico, para analizar los valores de los datos pasados; de una sola vez, a tener una visión instantánea de la red; y persistente para monitorear un evento para un período de tiempo.

3.2.4. HEED

HEED (Hybrid Energy-Efficient Distributed Clustering) es un algoritmo de agrupamiento de saltos múltiples para redes de sensores inalámbricas, con un enfoque en la agrupación eficiente mediante la selección apropiada de bolitas de cabezas en función de la distancia física entre los nodos. Los principales objetivos de HEED son (Younis y Fahmy, 2004):

- Distribuir el consumo de energía para prolongar la vida de la red
- Reducir al mínimo la energía durante la fase de selección de racimos de cabeza
- Reducir al mínimo la sobrecarga de control de la red

El aspecto más importante deHEED es el método de selección de racimos cabezas. Los Cluster-Heads se determinan en base a dos parámetros importantes (Younis y Fahmy, 2004):

1. La energía residual de cada nodo se utiliza para elegir probabilísticamente el conjunto inicial de cluster-heads. Este parámetro se utiliza comúnmente en muchos otros esquemas de agrupamiento.

2. Costo Intra-Cluster de Comunicación es utilizado por los nodos para determinar el clúster ha unirse. Esto es especialmente útil si un nodo dado cae dentro del intervalo de más de un grupo de cluster. En Heed es importante identificar cuál es el rango de un nodo en términos de sus niveles de energía que tendrá varios niveles de potencia de transmisión discretos.

El nivel de potencia utilizado por un nodo de anuncios dentro de un clúster y durante la agrupación se denomina nivel de potencia de clúster (Younis y Fahmy, 2004). Los bajos niveles de energía de clúster promueven un aumento de la reutilización espacial (Younis y Fahmy, 2004), mientras que se requieren altos niveles de potencia de clúster para la comunicación entre los grupos sectoriales, ya que abarcan dos o más áreas de cluster.

Por lo tanto, al elegir un clúster, un nodo se comunicará con el grupo de clusters que produce el menor coste de comunicación dentro del clúster. El coste de la comunicación interna del clúster se mide utilizando la medición Promedio Mínimo de alimentación de Alcanzabilidad (AMRP) (Younis y Fahmy, 2004). El AMRP es el promedio de todos los niveles mínimos de potencia requeridos para cada nodo dentro de un rango de clúster R para comunicarse de manera

efectiva con el grupo de clúster i. El AMRP de un nodo i se convierte en una medida de la energía de espera de la comunicación interna del clúster si este nodo es elevado a clúster-head. Utilizando AMRP como segundo parámetro de selección de cluster-head es más eficiente que la selección de un nodo cluster-head más cercano (Younis Y Fahmy, 2004).

3.2.5. PEGASIS

Pegasis (Power-Efficient GAthering in Sensor Information Systems) es un protocolo basado en cadena que es casi óptimo para la aplicación de recogida de datos en redes de sensores (Lindsey, y raghavendra, 2002). En el protocolo Pegasis, la idea principal es formar una cadena entre los nodos de sensores de manera que cada nodo se comunica sólo con un vecino cercano, los datos recogidos se mueven de nodo a nodo, quedan fusionadas, y, finalmente, un nodo designado transmite a la BS. Los nodos se turnan para transmitir a la BS de manera que la energía promedio gast

mjada por cada nodo por cada ronda se reduce. Los nodos sensores se organizan para formar una cadena; sin embargo, la construcción de una cadena para reducir al mínimo la longitud total es similar al problema del viajante de comercio, que se sabe que es intratable. Sin embargo, con los parámetros de radio comunicación de energía se puede construir una cadena simple con un enfoque codicioso.

3.2.6. HEEP

HEEP (Hybrid Energy Efficiency Protocol) combina dos algoritmos, Leach y Pegasis. HEEP sugiere un enfoque de auto-organización de la nueva red, que se unen a grupos y los enfoques basados en la cadena. Este nuevo enfoque se denomina enfoque de agrupación de cadenas. La organización de los nodos de la red de cadenas de clúster evita la mala disipación de energía en el protocolo de lixiviación y reduce el retraso de enrutamiento generado por el protocolo Pegasis (Boubiche, y Bilami, 2011). Con base en el enfoque de la agrupación de las cadenas, en cada nodo de clúster de cadenas adyacentes se forman y selecciona el nodo más potente para ser la cabeza de clúster. Todos los nodos transmiten sus datos recogidos a su CH usando cadenas vecinas de los nodos. A continuación, la CHS transmiten los datos recibidos directamente a la estación base, o indirectamente a través de los vecinos CHS. La transmisión de los datos recogidos a través de los nodos de las cadenas vecinas puede reducir las distancias de transmisión y optimizar el consumo de energía. La agregación de

datos se aplica por cada nodo en una cadena, para reducir la cantidad de datos intercambiados entre los nodos y su CH, que preserva las reservas de energía (Boubiche, y Bilami, 2011).

3.3. Protocolos de Enrutamiento Basados en Clúster para MSN

La mayoría de los protocolos de enrutamiento en redes inalámbricas de sensores tienen en cuenta que todos los nodos son homogéneos con respecto a la energía lo cual no es el enfoque realista. En particular nodos irregulares están asociados a múltiples Cluster-head; en este caso el clúster-head con gran número de oda drenará su energía para comparar al grupo de cabeza con menor número de nodos miembros asociados. Además, el soporte de movilidad es otro problema con el protocolo de enrutamiento, para mitigar estos problemas, se han propuesto algunos protocolos.

3.3.1. M-LEACH

(Nguyen, Defago, Beuran, y Shinoda, 2008) propuso M-Leach (Mobile Leach); M-Leach permite la movilidad de los nodos no-cluster-head y cluster-head durante la configuración y la fase de estado estacionario. MLEACH también considera la energía del nodo restante en la selección de los cluster-head. Algunos supuestos también se asumen en M-Leach al igual que otros protocolos de enrutamiento de la agrupación. Inicialmente todos los nodos son homogéneos en sentido de la ganancia de la antena, todos los nodos tienen su información de ubicación a través de GPS y la estación base se considera fijo en la M-Leach. La fase de instalación distribuida de lixiviación se modifica por M-Leach con el fin de seleccionar el cluster-head adecuado. En M-Leach los cluster-heads se seleccionan sobre la base del modelo de atenuación (Heinzelman, Chandrakasan, y Balakrishnan, 2002).

Cluster-heads óptimos se seleccionan para disminuir el poder de atenuación. Otros criterios de selección de cluster-heads son la velocidad de la movilidad. Un nodo con la movilidad mas baja y el mínimo de energía de atenuación es seleccionado como cluster-head en M-Leach. No-Cluster-heads a continuación transmiten su estado a todos los nodos en el rango de transmisión. Los nodos no-Cluster-head calculan su disposición a partir de múltiples cluster-heads y seleccionan el grupo de cluster-head con la máxima energía residual. En la fase de estado estacionario, si los nodos del clúster se alejan del cluster-head o el cluster-head se aleja de sus nodos miembros a continuación, otro grupo de cluster-head se adecua para los nodos miembros. Es el resultado en

la formación de la agrupación ineficiente. Para hacer frente a este problema MLEACH proporciona mecanismo de traspaso de nodos para cambiar al nuevo grupo de cluster-head. Cuando los nodos deciden hacer el traspaso, envía un mensaje DIS de incorporación a la corriente del cluster-head y también envía JOIN-REQ al nuevo grupo de cluster-head. Después del traspaso que se produce en el cluster-head se reprograma el patrón de transmisión.

3.3.2. LEACH-ME

LEACH-ME (LEACH Mobile Enhanced) Se propuso para mejorar Leach-M (Kumar, Vinu, y Jacob, 2008) mediante la selección de los nodos menos móviles con relación a sus vecinos para ser CHS. Cada nodo contiene las transiciones de cluster-head que ha hecho durante la fase de estado estacionario durante la transmisión de datos. Los nodos transmiten un recuento de transición a su CH durante la ranura TDMA. El CH calcula el recuento medio de la transición de sus miembros para los últimos pocos ciclos. Como resultado, una ranura activa aumentará cuando el número de recuento de transición está más allá del valor umbral. Durante la ranura activa, los nodos transmiten sus identificadores y cada nodo calcula la distancia a todos los nodos y calcular el factor de movilidad de acuerdo con (1)

$$M_i(t) = \frac{1}{n-1} * \sum_{j=0}^{n-1} d_{ij}(t) \quad (1)$$

donde $M_i(t)$ es el factor móvil basado en la lejanía del nodo i al resto de los nodos N es el número de vecinos de nodo i, y $d_{ij}(t)$ es la distancia de nodo i de sus vecinos j. Después de calcular el factor móvil, los nodos con menos valor del factor de movilidad ij se seleccionan para ser CHS, tomando en consideración el nivel de energía de ese nodo no está por debajo de un cierto umbral. La fase de estado estacionario es el mismo para Leach-M y Leach-ME.

3.3.3. LEACH-Mobile

(Kim y Chung, 2006) propuso un Protocolo de enrutamiento de autoorganización de apoyo para nodos móviles para la red de sensores inalámbrica. En el esquema propuesto, como lixiviación se divide en rondas, donde cada ronda comienza con una fase de puesta a punto cuando se organizan los grupos, seguida de una fase de estado estacionario cuando se producen transferencias de datos a la estación base. Con el fin de minimizar la sobrecarga, la fase de

estado estacionario es mucho mas en comparación con la fase de puesta a punto. Una de las ideas básicas en Leach-Mobile es confirmar la inclusión de nodos de sensores en un clúster específico en la fase de estado estacionario como el nodo principal del clúster y la cabeza sin clúster recibe mensaje en particular en un intervalo de tiempo determinado de acuerdo al horario de tiempo TDMA que cada conjunto de sensores tiene, y después de reorganizar el grupo con un mínimo consumo de energía.

Leach-Mobile asume que todos los nodos CH de red de sensores tiene que tener datos para enviar al CH necesariamente en su asignación de intervalos de tiempo en el horario de TDMA.

Mientras que el grupo de cabeza en el protocolo LEACH espera para recibir datos detectados de acuerdo al programa de TDMA durante la fase de estado estacionario, la cabeza de clúster en Leach-móvil transmite el mensaje de solicitud de transmisión de datos al nodo de cabecera no agrupado para la recopilación de datos detectados de acuerdo con el horario TDMA en cada intervalo de tiempo. Como la transferencia de datos se lleva a cabo, la cabeza de clúster confirma con una lista de ranura de tiempo de nodos si los datos detectados se reciben en consecuencia en una ranura de tiempo TDMA asignado en cada momento en el que termina un marco, a continuación, marca el nodo en la lista de no-receptora. Si los datos detectados no se reciben de nuevo desde el nodo marcado previamente, cuando termina el siguiente fotograma, se elimina el nodo y también puede asignar este intervalo de tiempo al nodo que recién se unió en horario de TDMA. Supone para la cabeza de clúster que los nodos que no responden al mensaje de solicitud de datos se mueven y se encuentran fuera de su región de clúster. A continuación, el calendario TDMA creado por reprogramación se transmite a todos los miembros del clúster de nodos.

Mientras el CH declara el número de miembros del nodo dentro de su propio grupo región por el mensaje de petición de datos, cada nodo móvil confirma la agrupación a la que pertenecerá. Después de que los grupos están organizados y los CH son seleccionados, los nodos CH no transmiten datos al CH después de recibir el mensaje de petición de datos. Si el mensaje de solicitud de datos no se recibe hasta que el marco termina con intervalo de tiempo asignado por el horario TDMA, el procedimiento de funcionamiento del protocolo va al siguiente fotograma. Si el nodo móvil no recibe el mensaje de petición de datos incluso cuando termina el próximo marco, difunde el mensaje de petición clúster-join. A continuación, el grupo CH al recibir clúster-join transmite el mensaje de solicitud del CH de agrupación como una fase de puesta a punto para ese nodo.

Después de que se ha completado esta fase, el nodo móvil decide el nuevo clúster al que pertenecerá para esta ronda como el nodo móvil se mueve. Esta decisión se basa en la intensidad de señal recibida del mensaje de anuncio.

3.3.4. E² MWSNRP

(Energy Efficient Mobile Wireless Sensor Network Routing Protocol) propuesto por (Sara, Kalaiarasi, Pari, y Sridharan, 2010) y se espera que garantizará una vida útil más larga de la red y una mejor relación de entrega de paquetes con menos consumo de energía. MWSNRP es un protocolo de enrutamiento de trayectos múltiples híbrido que puede ser diseñado principalmente para la red móvil deficiente de energía altamente dinámico del sensor inalámbrico donde la reducción de la disipación de la energía y la transmisión fiable de datos es una necesidad. A pesar de la forma real del campo del sensor, se supone que toda el área a ser circunscrito se integra en un cuadrado grande y luego se divide en diferentes zonas cuadradas después de que los nodos sensores se implementan en el campo.

- Enrutamiento dentro de la zona se llama IntrA Precinct Routing (IAPR).
- El hecho de enrutamiento fuera de una zona se llama IntEr Precinct Routing (IEPR).
- IntrA Precinct Routing (IAPR):): Cada nodo en un recinto se supone está dentro del alcance de comunicación de todos los demás nodos en el recinto. Así que cada nodo sensor puede comunicarse con el nodo de fusión usando la comunicación de salto. Cuando se detecta un evento, el nodo sensor primero se comunica con el nodo de fusión. Los controles de nodo de fusión si el destino se encuentra dentro de su recinto. Si es así, de forma proactiva el evento se envía al destino. Para reenviar los datos a otros recintos, se emplea el IntEr Precinct Routing.
- IntEr Precinct Routing: Es una técnica de múltiples rutas de enrutamiento reactivo empleado para la comunicación entre los nodos de fusión. Cuando se utiliza un único camino en el protocolo de enrutamiento de la demanda en este tipo de redes, es necesario un redescubrimiento de ruta en respuesta a cada corte de ruta (Sara, Kalaiarasi, Pari, y Sridharan, 2010). El EMWSNRP permite la selección de los mejores caminos de la computación de la energía sobrante nodal máxima. El mensaje RREQ contiene los siguientes campos:
  < Source address, source precinct id, sequence no., broadcast
  id, hop count, destination address, maximum surplus energy >.

El identificador de emisión se incrementa cada vez que la fuente emite un nuevo RREQ. El número de secuencia indica la información de frescura sobre una ruta. A medida que el RREQ se desplaza desde una fuente a varios destinos, se establece automáticamente por el camino inverso de todos los nodos a la fuente. Estas entradas de ruta inversa se mantienen durante al menos el tiempo suficiente para que el RREQ pueda atravesar la red y producir una respuesta al remitente. Si un nodo de fusión intermedia tiene una ruta actual hasta el destino y si el RREQ no se ha procesado previamente, entonces el nodo unicasts (RREP) da vuelta a su vecino del que haya recibido la RREQ. El mensaje RREP contiene los campos siguientes:

<Source address, destination address, destination precinct id, sequence number, hop count, readiness factor, maximum surplus energy, lifetime>.

Si el factor de disposición denota «desprenderse», un mensaje de error de ruta (ERR) se propaga en el camino inverso en lugar de RREP. Cuatro pasos importantes están involucrados:

- Mecanismo de selección de Energía Consciente;
- Encontrar la energía sobrante nodal máxima a lo largo de los mejores caminos;
- Clasificación de los trayectos múltiples en orden descendente utilizando el excedente de energía nodal;
- Reenvío de los paquetes de datos a través de la ruta de acceso con la energía sobrante nodal máxima.

3.3.5. GBEER

Varios investigadores se han concentrado para proporcionar protocolos de enrutamiento muy eficientes de energía para la red de sensores inalámbrica con lavabos móviles. (Kweon, Ghim, Hong, y Yoon, 2009) han propuesto Grid Based Energy Efficient Routing (GBEER) para la comunicación de múltiples fuentes a múltiples lavabos móviles en redes de sensores inalámbricos. Una estructura permanente de red está construida con la información de ubicación mundial. Las solicitudes de datos se encaminan a la fuente a lo largo de la red y los datos se envían de nuevo a los sumideros. La solución de rejilla quórum se adopta para promocionar de manera efectiva y solicitar los datos para lavabos móviles. La sobrecarga de comunicación causada por la movilidad del fregadero se limita a la celda de la cuadrícula. No hay consumo de energía adicional debido a múltiples eventos porque sólo una estructura de rejilla se construye de forma independiente del evento.

Capítulo 4. Seguridad en WSN

WSN es una tecnología emergente y tienen un gran potencial para ser empleado en situaciones críticas como campos de batalla y las aplicaciones comerciales tales como la construcción, uno de los principales retos en las redes de sensores inalámbricas a enfrentarse hoy en día es la seguridad. Mientras que el despliegue de nodos de sensores en un entorno sin vigilancia hace que las redes sean vulnerables a una variedad de ataques potenciales, la potencia inherente y las limitaciones de memoria de los nodos de sensores hace que las soluciones de seguridad convencionales inviable. En las siguientes secciones vamos a discutir los requisitos de seguridad en WSN, los ataques a WSN también el mecanismo de seguridad en red de sensores inalámbricos.

4.1. Requisito de Seguridad en WSN

Las redes de sensores inalámbricos comparten muchas características con las redes tradicionales, los requisitos de seguridad de una red inalámbrica de sensores se pueden clasificar de la siguiente manera:

- Confidencialidad de los datos: Las aplicaciones como la vigilancia de la información, secretos industriales y la distribución de claves necesita confiar en la confidencialidad. El enfoque estándar para mantener la confidencialidad es a través del uso de la encriptación.
- Autenticación de datos: La autenticación garantiza la fiabilidad del mensaje mediante la identificación de su origen. Los ataques en redes de sensores no sólo implican la alteración de paquetes; adversarios también pueden inyectar falsos paquetes adicionales (Padmavathi y Shanmugapriya, 2009). Los datos de autenticación verifican la identidad de los remitentes y receptores. La autentificación de datos se consigue a través de mecanismos simétricos o asimétricos, donde los nodos que se envían y reciben comparten claves secretas. Debido a la naturaleza inalámbrica de los medios de comunicación y la naturaleza de las redes de sensores sin vigilancia, es un gran reto garantizar la autenticación.
- Integridad de los datos: La integridad de datos es un requisito básico para datos de sensores seguros en WSN. Es para asegurar que la información no se cambia en tránsito, ya sea debido a la mala intención o por accidente.
- Frescura de Datos: Incluso si la confidencialidad y la integridad de los datos está garantizada, hay una necesidad de garantizar la frescura de cada mensaje. La actualidad de los datos sugiere que los datos son

recientes y asegura que no hay mensajes antiguos que se hayan reproducido. Para asegurarse de que no hay mensajes antiguos para reproducirse, una marca de tiempo puede ser añadida al paquete.

- Disponibilidad: Esto asegura que los servicios de red deseados están disponibles incluso en presencia de ataques de denegación de servicio.
- Autorización: Asegura que sólo los sensores autorizados pueden estar implicados en el suministro de información a los servicios de red.
- No repudio: que denota que un nodo no puede denegar el envío de un mensaje que ha enviado previamente.
- Auto organización: Una red de sensores inalámbricos es típicamente una red Ad Hoc que requiere que cada nodo sensor sea independiente y lo suficientemente flexible como para ser auto organizado y auto sanado de acuerdo a diferentes situaciones. Debido al despliegue de nodos al azar ninguna infraestructura fija está disponible para la gestión de redes WSN. Las redes de sensores distribuidos deben auto organizarse para apoyar el enrutamiento de múltiples saltos. Deben también auto organizarse para llevar a cabo la gestión de claves y construir la relación de confianza entre los sensores.
- Localización de Seguridad: A menudo, la utilidad de una red de sensores se basa en su capacidad de localizar con precisión y de forma automática cada sensor en la red. Una red de sensores para localización de fallos necesitará información de ubicación precisa con el fin de determinar la ubicación de un fallo. Por desgracia, un atacante puede manipular fácilmente información de una ubicación no segura por fuertes señales falsas de reporte, reproducir señales.

Después de discutir los requisitos de seguridad en WSN, en la siguiente sección vamos a clasificar y describir algunos ataques que pueden afectar a la red.

4.2. Ataques a WSN

Basado en la investigación de (Karloff, y Wagner, 2003), podemos clasificar los ataques de enrutamiento en seis categorías:

- Ataque caer en el agujero: En el ataque pozo negro, el objetivo del atacante es atraer a todo el tráfico de un área en particular a un nodo de compromiso. Este ataque puede crear también el reenvío selectivo y ataques de los agujeros negros.
- Ataque agujero negro: Un nodo atacante puede crear un agujero negro, mediante la atracción y drop-ping todo el tráfico en una zona específica.

- Desvío selectivo: En este tipo de ataques, el atacante puede negar el envío de paquetes o dejarlos caer y actuar como un agujero negro.
- Sybil Ataque: En un ataque de Sybil, un nodo malicioso puede representar varias identidades a la red. Este tipo de ataques está amenazando al fallo esquemas tolerantes como el almacenamiento distribuido, enrutamiento de trayectos múltiples y el mantenimiento de topología.
- Ataque Sybil: En un ataque Sybil, un nodo malicioso puede representar varias identidades a la red. Este tipo de ataques amenaza al esquema de fallos tolerantes como el almacenamiento distribuido, enrutamiento de trayectos múltiples y el mantenimiento de topología.
- Ataque Hello Flood: En un ataque de inundación, el atacante transmite paquetes de saludo para convencer a los nodos que el atacante es un vecino.
- Redirección: Este tipo de ataques se puede hacer por reenviar el mensaje junto con el camino equivocado o mediante el envío de actualizaciones de enrutamiento falsas.

4.2.1. Mecanismo de Seguridad en WSM

Para proteger WSNs contra diferentes tipos de vulnerabilidades, los mecanismos de prevención como la criptografía y autenticación se pueden aplicar para prevenir algunos tipos de ataques. Este tipo de mecanismos de prevención forman la primera línea de defensa para redes inalámbricas de sensores. Sin embargo, algunos ataques como los agujeros de gusano, sumidero, no podrían ser detectado mediante este tipo de mecanismos de prevención. Además, estos mecanismos sólo son eficaces para prevenir ataques externos y su incapacidad de garantizar la prevención de intrusos desde el interior de la red (Silva et al, 2005). Debido a esto, es necesario el uso de algunos mecanismos de detección de intrusiones.

- Criptografía: Las técnicas de cifrado-descifrado ideados para las redes cableadas tradicionales no son factibles de ser aplicadas directamente a las redes inalámbricas y en particular para las redes de sensores inalámbricas. WSNs consisten en pequeños sensores que realmente sufren de la falta de procesamiento, memoria y potencia de la batería
  (Pathan, Dai, y Hong, 2006). La aplicación de cualquier sistema de cifrado requiere la transmisión de bits adicionales, por lo tanto, el

procesamiento adicional, la memoria y energía de la batería, que son recursos muy importantes para la longevidad de los sensores. La aplicación de los mecanismos de seguridad tales como el cifrado también podría aumentar el retardo, jitter y pérdida de paquetes en redes de sensores inalámbricos (Pathan, Dai, y Hong, 2006).

- Sistemas de Detección de Intrusos (IDS): Se consideran para actuar como la segunda línea de defensa contra los ataques de red que los mecanismos de prevención no tienen en cuenta (Silva et al, 2005). Un sistema de detección de intrusiones se define en (Debar, Dacier, y Wespi, 1999) como "un sistema que monitoriza dinámicamente los eventos que tienen lugar en un sistema y decide si estos eventos son síntomas de un ataque o constituye a un uso legítimo del sistema". Sin embargo, hay muchos desafíos planteados en contra de la aplicación de la DS para redes inalámbricas de sensores. Estos retos se deben a la falta de recursos como, la energía, el procesamiento y el almacenamiento.

En general, los sistemas de IDS se clasifican en IDS de mal uso y la anomalía IDS. El primero coincide con las nuevas observaciones con las firmas almacenadas en la base de datos del IDS. Detecta las actividades anormales del perfil normal predefinido con el fin de identificar posibles ataques.

Añadir a la criptografía y la intrusión en el sistema de detección. Hay una amplia variedad de sistemas de seguridad que pueden ser inventados para contrarrestar los ataques maliciosos y éstos se pueden clasificar como de alto nivel y de bajo nivel. La figura 2 (Padmavathi y Shanmugapriya, 2009) muestra el orden de los mecanismos de seguridad.

4.3. Esquema de seguridad de agregación de datos en Redes heterogéneas de sensores inalámbricos.

La agregación de datos es un concepto básico importante en redes de sensores inalámbricos (WSN), que se ha propuesto para optimizar el proceso de recolección de datos y las reservas de energía de los nodos sensores. De hecho, y debido a la densidad de red, el proceso de recolección de datos sufre de redundancia e interrelación de datos que puede drenar las baterías del nodo sensor y afectar el rendimiento de la red (sobrecarga, ancho de banda de transmisión, latencia ...). Por lo tanto, es necesario utilizar métodos para fusionar datos en los nodos intermedios con el fin de reducir el número de paquetes transmitidos a la estación base, permitiendo así ahorro de energía y ancho de banda. Esto se puede lograr a través de un mecanismo de agregación de datos.

A pesar de las ventajas de la agregación de datos puede conducir a algunas fallas de seguridad: Usurpación de identidad, eliminación deliberada de los paquetes, alteración de lecturas sensoriales y resultados de agregación. Se han propuesto muchas soluciones de seguridad para asegurar el proceso de agregación de datos. Estas soluciones se proponen principalmente para WSN homogéneo donde los nodos son idénticos en capacidad, consumo de energía y complejidad del hardware. Las soluciones propuestas tienen como objetivo garantizar la agregación segura de datos y una difusión autenticada basada en una variedad de mecanismos de seguridad como el cifrado simétrico y el mensaje de autenticación MAC. La mayoría de estos mecanismos son sencillos y sólo pueden garantizar un nivel mínimo de seguridad. Además, no pueden tolerar el uso de niveles de alta seguridad y algoritmos más complejos, como el cifrado asimétrico y el homomorfismo de privacidad, que requieren mayor poder de cálculo, reservas de energía y memoria. De hecho, los nodos sensores simples no pueden soportar mecanismos complejos y potentes.

Las WSNs heterogéneas representan una nueva clase de tecnología y un área de investigación reciente que Supera los límites de las WSN, especialmente en el campo de la seguridad. El progreso continuado en Redes de sensores, especialmente en la miniaturización de los procesadores ha permitido el desarrollo de Varias variedades de nodos. Cuando se utiliza más de un tipo de nodos en un WSN, se llama Heterogéneo. Una red típica heterogénea de sensores inalámbricos está compuesta por un gran número de nodos homogéneos y un número reducido de nodos heterogéneos como se muestra en la Figura 1. Los nodos idénticos, que principalmente recogen datos, son baratos (recursos limitados) mientras que los Los nodos heterogéneos son más caros, disponen de alta capacidad de computación y de recursos (Memoria y reservas energéticas). De hecho, el despliegue de nodos heterogéneos de sensores de alta capacidad en una Red contribuye a la distribución eficiente de la carga de trabajo entre los nodos de la red. De este modo, los nodos sensores de alta capacidad de recursos están cargados con el logro de tareas complejas y de alto consumo de energía, mientras que las tareas sencillas y de bajo consumo de energía se delegan a Nodos de sensores de recursos limitados.

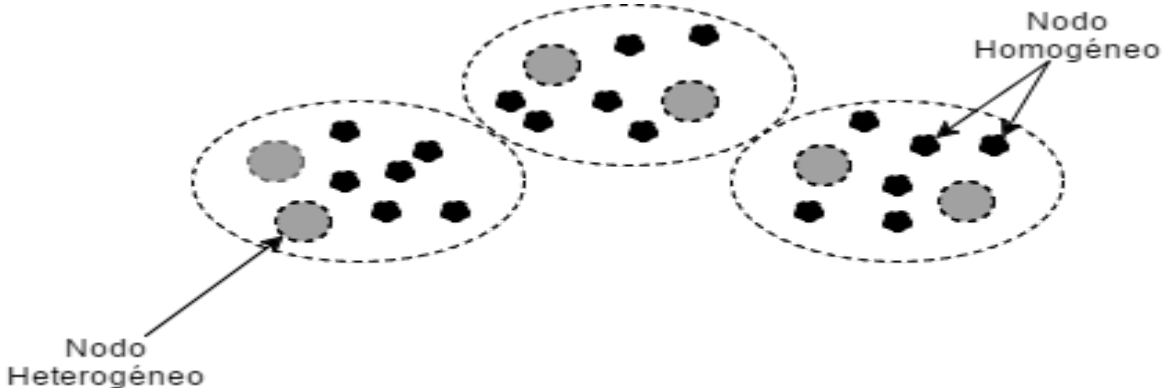

Figura 2 Red de sensores inalámbricos heterogéneos.

Las capacidades de recurso de los nodos sensores heterogéneos han abierto nuevas direcciones de investigación de seguridad ya que se pueden usar algoritmos complejos y de alto nivel de seguridad para asegurar el proceso de agregación de datos. Se utilizan varias técnicas de seguridad para asegurar el proceso de agregación de datos en WSN heterogéneo, cuya

base está representada por el algoritmo de privacidad homomorfismo. La idea principal es aplicar las funciones de agregación directamente a los datos cifrados, protegiendo así la integridad de los datos mientras los transmiten desde los nodos de agregación a la estación base. El problema de seguridad de agregación de datos en las WSN heterogéneas es relativamente nuevo y los protocolos de seguridad propuestos son innumerables en comparación con los homogéneos. Además de los principales problemas de seguridad, un protocolo heterogéneo de seguridad de agregación de datos debe garantizar los siguientes puntos:

- Explotación de las altas capacidades de los nodos sensores heterogéneos.
- Respeto de las limitaciones de recursos de los nodos sensores homogéneos simples.
- Optimización del proceso de agregación de datos al tiempo que garantiza una alta precisión de los datos.

La principal contribución de este trabajo es el estudio de los protocolos de agregación de seguridad existentes dedicados a las WSNs heterogéneas. En nuestra opinión, los protocolos de seguridad de agregación de datos heterogéneos deben identificarse y diferenciarse de los dedicados a las WSN homogéneas, ya que no pueden aplicarse a este tipo clásico de redes. Por otro lado, la adopción de protocolos homogéneos de seguridad de agregación de datos en redes WSN heterogéneas puede explotar de manera insuficiente las capacidades de los recursos de la red. Hasta donde sabemos, sólo se han propuesto ocho protocolos y creemos que es interesante arrojar luz sobre estos protocolos y discutir sus estrategias de seguridad. El resto del trabajo se organiza de la siguiente manera: La Sección 2 presenta una clasificación y una encuesta de los diferentes protocolos de seguridad de agregación de datos heterogéneos publicados. En la Sección 3, evaluamos y discutimos los protocolos de seguridad de agregación de datos heterogéneos encuestados basados en el enfoque de seguridad adoptado. Finalmente, concluimos el artículo en la Sección 4.

4.4. Mecanismos de seguridad de agregación de datos para redes de sensores inalámbricos heterogéneos

La aseguración de los protocolos de agregación de datos para WSN heterogéneo se pueden clasificar en dos tipos: de extremo a extremo y protocolos de agregación de datos hop por hop [5,6]. En protocolos de agregación de datos de extremo a extremo, la seguridad se garantiza aplicando la función de agregación directamente a los datos cifrados. En el segundo tipo de protocolos, los datos deben descifrarse en cada nodo de agregación, perdiendo así la privacidad de extremo a extremo entre el transmisor y el receptor. Recientemente se ha introducido un tercer tipo de protocolo de seguridad de agregación de datos, que divide la red en dos etapas: nodos heterogéneos de capacidad de recursos elevados y nodos de sensores de capacidad de recursos limitados y sencillos. Este nuevo tipo de protocolo introduce una estrategia de seguridad de dos niveles donde cada etapa de la red aplica distintos enfoques de seguridad. La clasificación heterogénea del protocolo de seguridad de agregación de datos se presenta en la Figura 2.

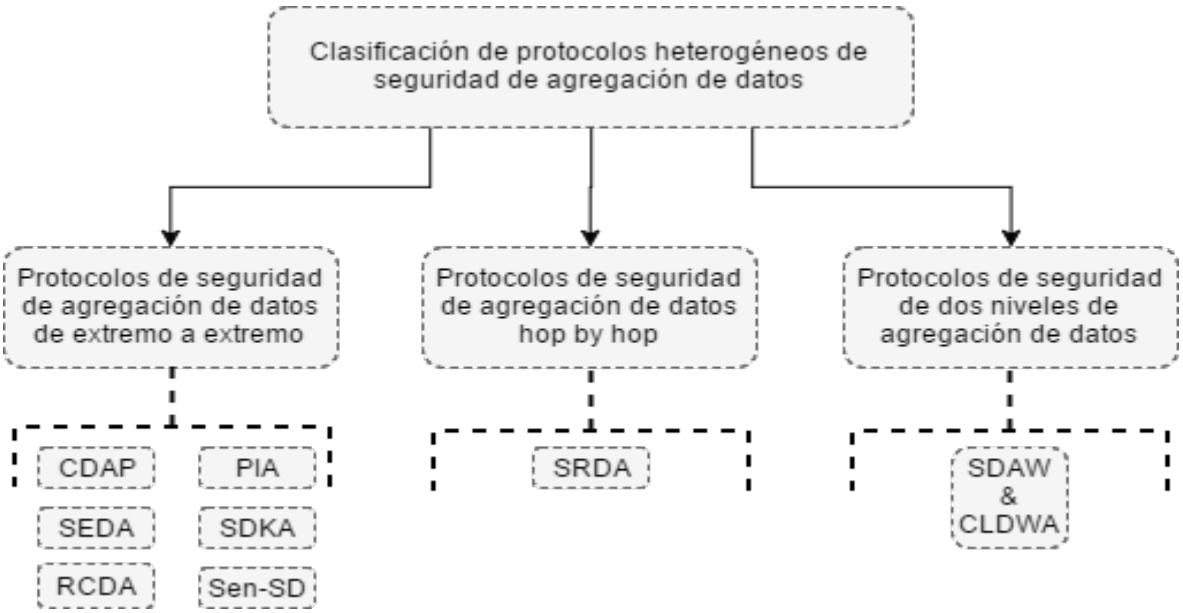

Figura 3 Clasificación de Protocolos Heterogéneos de Seguridad de Agregación de Datos.

4.5. Protocolos de agregación de datos seguros de extremo a extremo

Los protocolos de agregación de datos seguros de extremo a extremo apuntan a asegurar la privacidad y confidencialidad de los datos de los nodos sensores a la estación base (Figura 3). Para ofrecer más seguridad, los datos detectados se ocultan y los nodos realizan las funciones de agregación directamente en los datos cifrados. La mayoría de los protocolos de agregación de datos seguros de extremo a extremo utilizan homomorfismo de privacidad, lo que asegura este tipo de seguridad.

4.5.1. Agregación de datos ocultos en redes de sensores heterogéneos usando homomorfismo de privacidad (CDAP)

Ozdemir [7] ha propuesto el protocolo CDAP para facilitar el proceso de agregación y para obtener una transmisión de extremo a extremo segura entre la estación base y los nodos de la red. Por lo tanto, propuso el uso del homomorfismo de privacidad para proporcionar ocultamiento de datos de extremo a extremo y también para operar directamente en textos de cifrado mientras proporciona un proceso seguro de agregación de datos. El protocolo se aplica a una WSN heterogénea donde se utilizan nodos potentes llamados AGGNODE.

4.5.2. Privacidad y preservación de la integridad de datos (PIA)

Taban et al. [9] han abordado el problema de la agregación de datos, con la garantía de la integridad de los datos y la eficiencia y protección de la información privada como

objetivo común. En su modelo, el nodo de agregación se utiliza como intermediario entre el usuario y los nodos de sensor. El problema es que el usuario quiere comprobar la integridad de los datos agregados recibidos mientras que el propietario de la red prefiere mantenerlos secretos del usuario. En este contexto, los autores proponen cuatro soluciones.

Capítulo 5. Aplicación de Redes de Sensores Inalámbricas

Las redes de sensores tienen una variedad de aplicaciones. Los ejemplos incluyen aplicaciones militares, vigilancia del medio ambiente (que implica el monitoreo del aire, suelo y agua), aplicaciones médicas, aplicaciones del hogar, aplicación industrial y comercial.

5.1. Aplicaciones Militares

La mayor parte del conocimiento elemental de las redes de sensores se basaba al principio en la defensa, especialmente dos programas importantes las Redes de Sensor Distribuidas (DSN) y la tecnología de la información del sensor forman la Agencia de Investigación Avanzada de Defensa de Proyectos (DARPA), las redes de sensores se aplican con éxito en la detección militar.

De hecho, es muy difícil decir con certeza si las motas se desarrollaron debido a las necesidades militares y de defensa de aire o si se inventaron de forma independiente y se aplicaron posteriormente a los servicios del ejército. En cuanto a las aplicaciones militares, el área de interés se extiende a partir de la recopilación de información, por lo general, Vigilancia y Seguimiento del campo de batalla y el sistema de detección de disparos.

La vigilancia del campo de batalla y seguimiento: En territorio critico de campo de batalla, vías de acceso y caminos estrechos se pueden cubrir rápidamente con redes de sensores y ser seguidos de cerca por las actividades de las fuerzas opuestas. A medida que las operaciones se desarrollan y se preparan nuevos planes operativos, nuevas redes de sensores pueden ser desplegadas en cualquier momento para la vigilancia del campo de batalla.

Sistema de detección de Disparo: El sistema de detección de francotiradores Boomerang (Raytheon BBN Technologies, 2013) ha sido desarrollado para la detección de la ubicación exacta de francotiradores con una definición de disparos de armas pequeñas desde el tirador. Se ha utilizado por los militares, las fuerzas del orden, y los municipios.

El sistema funciona cuando el vehículo está parado o en movimiento, utilizando un solo mástil montado, un conjunto compacto de micrófonos. Boomerang detecta disparos de armas pequeñas que viajan hacia el vehículo, la trayectoria de las balas que pasan dentro de aproximadamente 30 metros del mástil y los tiradores que disparan a distancias máximas de armas eficaces. La detección del ataque entrante se determina en menos de un segundo. Mucho esfuerzo se

ha implementado para evitar que el sistema produzca falsas alarmas causadas por eventos no balísticos tales como baches en la carretera, cierre de puertas, el ruido del viento, las transmisiones de radio tácticos y eventos de ruido extraños (tráfico de vehículos, petardos, y la actividad urbana). El sistema no alerta cuando se dispara desde el vehículo.

Boomerang se integra fácilmente con otras opciones de productos Boomerang, tales como el Sistema de la conciencia de la situación, así como otros sistemas de terceros. A través de su intuitivo Kit de integración de sistemas y sencilla interfaz Ethernet, la salida de Boomerang se puede utilizar para girar dispositivos de cámara, alimentar a las estaciones de armas a distancia, o reportar la posición del tirador a un Centro de Operaciones Tácticas existente. Ya sea independiente o en combinación con otros sistemas, Boomerang aumenta la detección de objetivos y la supervivencia.

5.2. Aplicaciones Medioambientales

Existen varias aplicaciones de redes de sensores ambientales incluyendo el seguimiento de los movimientos de las aves, pequeños animales e insectos; monitoreo de las condiciones ambientales que afectan a los cultivos y el ganado; irrigación; instrumentos macro de Vigilancia de la Tierra a gran escala y la exploración planetaria; Detección biológica/química; Agricultura de precisión; biológica, la Tierra y la vigilancia del medio ambiente marino, el suelo y la atmósfera; detección de incendios forestales; la investigación meteorología o geofísica; la detección de inundaciones; mapeo de biocomplejidad del entorno; y el estudio de la contaminación (Zhang, Sadler, Lyon, y Martonosi, 2004). Ilustraremos a continuación algunos proyectos relacionados con las aplicaciones ambientales.

- Monitoreo Volcanico: WSNs se han utilizado en ambientes extremos, donde el acceso humano continua imposible. El monitoreo de volcanes es un ejemplo de estas aplicaciones extremas, donde una red de sensores puede ser fácilmente desplegada cerca de los volcanes activos a supervisar continuamente sus actividades y proporcionar datos a una escala y resolución, antes no era posible con las herramientas existentes.

Dos redes inalámbricas de sensores se desplegaron en volcanes activos por este proyecto (Kifayat, Merabti, Shi, y Llewellyn, 2010). Su despliegue inicial en el volcán Tungurahua, Ecuador, en julio de 2004 sirvió como una prueba de concepto y consistía en un pequeño conjunto de nodos inalámbricos que capturaban datos de infrasonido continuas. Su segundo despliegue en el volcán

Reventador, Ecuador, en julio / agosto de 2005 constaba de 16 nodos desplegados sobre una abertura de 3 km a los flancos superiores del volcán para medir tanto las señales sísmicas y de infrasonidos con una alta resolución (24 bits por canal a 100 Hz) (Kifayat, Merabti, Shi, y Lewellyn, 2010).

- ZebraNet: ZebraNet (Zhang, Sadler, Lyon, y Martonosi, 2004) es una red inalámbrica de sensores desplegados en Kenia para realizar un seguimiento de dos especies de cebras. Fue diseñada para la vigilancia y el seguimiento de la vida silvestre. ZebraNet utiliza nodos significativamente más grandes y más pesados que las motas. La arquitectura está diseñada para que una red inalámbrica siempre esté en movimiento, multisalto. En muchos aspectos, este diseño no encaja con la supervisión de la tormenta Petrel en las posiciones estáticas (madrigueras). ZebraNet, en el momento de escribir estas líneas, todavía no ha tenido un despliegue completo a largo plazo por lo que actualmente no existe un análisis exhaustivo de la fiabilidad de sus algoritmos de redes de sensores y de diseño.

5.3. Aplicaciones Médicas

WSNs también puede ser útil en el sector de la salud a través de la televigilancia de los datos fisiológicos humanos, el seguimiento y la supervisión de médicos y pacientes en un hospital (Gao, Greenspan, Welsh, Juang, y Alm, 2005) hay varios proyectos en curso para utilizar redes inalámbricas de sensores en el sector médico. Se describen algunos de ellos aquí:

- Proyecto UbiMon: UbiMon (entorno de monitorización ubicua de sensores portátiles e imi88plantables) es la arquitectura para la vigilancia móvil distribuida, desarrollado en el Imperial College de Londres. El objetivo de este sistema es proporcionar una gestión continua de pacientes en sus estados fisiológicos naturales, de manera que las anormalidades transitorias, sino que amenazan la vida pueden ser detectados y predijeron (Ng et al, 2004).
- Proyecto Alarma-Net: Alarma-Net es una red de sensores inalámbricos para la vida asistida y monitoreo residencial, está siendo desarrollado en la Universidad de Virginia. El sistema de alarma Net integra dispositivos heterogéneos, algunos usables en el paciente y algunos colocados dentro de la vivienda. Juntos realizan una misión de salud especificado por un profesional de la salud. Los datos se recogen, agregan, pre-tratan,

almacenan, y se actua en consecuencia, de acuerdo con un conjunto de requisitos del sistema identificados (Wood et al, 2006).

5.4. Aplicaciones en el Hogar

Junto con el desarrollo militar, la aplicación del medio ambiente y el médico de la red de sensores no es tan difícil imaginar que la aplicación entre en nuestra vida normal en el futuro. Muchos de los conceptos que ya han sido diseñados por los investigadores y arquitectos, como "Smart Medio Ambiente: Algunos incluso se realizan. Veamos el concepto de "hogar inteligente": Después de un trabajo duro se vuelve a casa. En la puerta principal el sensor detecta que está abriendo la puerta, entonces se le dirá al hervidor de agua que ponga a hervir un poco de agua y el aire acondicionado se encienda.

- Entorno Inteligente: Los nodos de sensores pueden ser empotrados en muebles y electrodomésticos, y pueden comunicarse entre sí y una sala de servidores. El servidor de habitación también se puede comunicar con otros servidores de habitaciones para aprender acerca de los servicios que ofrecen como la impresión, escaneo y fax.

5.5. Aplicación Industrial y Comercial

En consecuencia, muchas aplicaciones industriales y comerciales diferentes se han desarrollado sobre la base de las redes de sensores inalámbricas. Las aplicaciones específicas para los espacios industriales y comerciales incluyen (Adams, 2004):

- Almacenes, gestión de flotas, fábricas, supermercados, complejos de oficinas.
- El gas, el agua y los medidores eléctricos.
- Detectores de Humo, CO, H_2O.
- Cajas o dispositivos de refrigeración.
- Equipo de servicios de gestión y mantenimiento preventivo.
- Servicios de seguridad (incluidos los sensores de seguridad peel-n'-stick).
- Control de iluminación.
- línea de montaje y flujo de trabajo e inventario.

- Los sistemas de tratamiento de materiales (calor, flujo de gas, refrigeración, químicos).
- Los sistemas de tratamiento de materiales (calor, flujo de gas, refrigeración, químicos).
- La monitorización remota de la sede corporativa de los activos, facturación y gestión de la energía.

Capítulo 6. Redes de Sensores Inalámbricas en Ambientes Desafiantes

6.1. Redes Inalámbricas de Sensores Subterráneos

Las redes de sensores inalámbricos subterráneos (WUSN) son una extensión importante de las redes terrestres de sensores inalámbricos, donde los nodos de los sensores están enterrados bajo tierra y se comunican de forma inalámbrica a través del suelo. Como un campo prometedor, las WUSNs permiten una amplia variedad de aplicaciones novedosas, tales como riego inteligente, mantenimiento de campos deportivos, patrullas fronterizas, monitoreo de infraestructura, detección de intrusos, entre otros (Akyildiz, Melodia, & Chowdhury, Vuran, 2009).

Aunque su despliegue se basa principalmente en nodos de sensores subterráneos, un WUSN todavía requiere dispositivos sobre el terreno para la recuperación de datos, la gestión y las funcionalidades de retransmisión. En consecuencia, existen tres enlaces de comunicación diferentes en WUSNs basados en las ubicaciones del transmisor y del receptor (Silva, & Vuran, 2010):

- Enlace subterráneo a subterráneo (UG2UG): Tanto el emisor como el receptor están enterrados bajo tierra y se comunican a través del suelo. Este tipo de comunicación se emplea para la entrega de información de salto múltiple.
- Enlace tierra subterránea a tierra (UG2AG): El emisor está enterrado y el receptor está sobre el suelo. Los datos de monitoreo se transfieren a relés o sumideros por encima de estos enlaces.
- Enlace por encima de tierra a subterráneo (AG2UG): Nodo remitente sobre tierra envía mensajes a nodos subterráneos. Este enlace se utiliza para la entrega de información de gestión a los sensores subterráneos.

6.2. Redes Inalámbricas de Sensores Submarinos

Las redes inalámbricas de sensores submarinos (UWSN) están previstas para permitir aplicaciones para una amplia variedad de propósitos tales como,

monitoreo de la contaminación, recolección de datos oceanográficos, navegación asistida, prevención de desastres y vigilancia táctica (Akyildiz, Pompili & Melodia, 2005).

En las subsecciones siguientes ilustraremos la diferencia entre WSN terrestre y UWSN; También discutiremos la arquitectura UWSN y finalmente la comparación entre los tipos de arquitectura UWSN.

6.3. Diferencias entre WSN Terrestre y UWSN

Aunque WSN y UWSN son diferentes, principalmente debido a las características únicas del agua, ciertos aspectos de la investigación de WSN se pueden aplicar a UWSN. Las principales diferencias entre redes de sensores terrestres y submarinos son las siguientes:

- Método de comunicación: UWSN utiliza señal acústica mientras que WSN utiliza ondas de radio.
- Costo: Aunque se espera que los sensores terrestres se vuelvan cada vez más baratos, los sensores subacuáticos son dispositivos costosos. Esto se debe a la complejidad de los transceptores de la UWSN y a la mayor protección requerida por el hardware.
- Potencia: UWSN necesita más potencia porque utiliza señal acústica y cubre una distancia más larga. En comparación con la señal acústica, RF necesita menos potencia, ya que el procesamiento en los receptores no es tan complejo.
- Memoria: La conexión de una señal acústica puede ser desactivada por situaciones especiales bajo el agua, como zonas de sombra. Debido a este hecho, los sensores submarinos necesitan adquirir más datos para evitar la pérdida de datos. Sin embargo, esto no es un problema para los sensores terrestres.
- Densidad: En la aplicación de sensores terrestres, como el sistema de seguimiento, los sensores se pueden desplegar densamente. Mientras que un sensor subacuático es más caro que el sensor terrestre, costará más dinero desplegar densamente. Incluso si el dinero no es un problema, todavía no es fácil desplegarlos.
- Movilidad: La mayoría de los nodos sensores en redes de sensores basadas en tierra son típicamente estáticos, aunque es posible implementar interacciones entre estos nodos estáticos y una cantidad límite de nodos móviles (por ejemplo, entidades móviles de recolección de datos como "mulas" que pueden o no ser Nodos de sensores). Por el contrario, la mayoría de los nodos de sensores submarinos, excepto algunos nodos fijos equipados

con boyas de superficie, tienen movilidad baja o media debido a la corriente de agua y otras actividades submarinas. A partir de observaciones empíricas, los objetos subacuáticos pueden moverse a la velocidad de 2-3 nudos (o 3-6 kilómetros por hora) en una condición subacuática típica. Por lo tanto, si un protocolo de red propuesto para redes de sensores basadas en tierra no considera la movilidad para la mayoría de los nodos sensores, probablemente fallaría cuando se clonara directamente para aplicaciones acuáticas (Cui, Kong, Gerla, & Zhou, 2006).

Hoy en día, muchos protocolos diferentes para WSN terrenal han sido desarrollados. Sin embargo, no son aptos para UWSN. No sólo las arquitecturas de UWSN impactan el desarrollo de un nuevo protocolo, sino también las características del submarino. Es otro lugar diferente con la red de sensores terrestres. Por lo tanto, podemos desarrollar diferentes tipos de protocolo de acuerdo con las arquitecturas de UWSN. A continuación, se discutirá la idea de que los protocolos deben ser diseñados de acuerdo al tipo de arquitectura.

Capítulo 7. Redes de Sensores Multimedia Inalámbricos (WSN)

La integración de tecnologías de redes inalámbricas de bajo consumo de energía con hardware de bajo costo, como cámaras y micrófonos de semiconductores de óxidos metálicos complementarios (CMOS, por sus siglas en inglés), ahora está permitiendo el desarrollo de sistemas de redes distribuidas a las que nos referimos como redes inalámbricas de sensores multimedia (Akyildiz, Melodia , Y Chowdhury, 2006) (Akyildiz, Melodia, & Chowdury, 2007), es decir, redes de dispositivos inteligentes inalámbricos interconectados que permiten recuperar corrientes de vídeo y audio, imágenes fijas y datos de sensores escalares. En las siguientes secciones vamos a describir / ilustrar / discutir / escribir los factores importantes que influyen en el diseño de redes de sensores multimedia, la arquitectura de referencia de WMSN y la seguridad de WMSN.

7.1. Arquitecturas UWSN

De acuerdo con (Cui, Kong, Gerla, & Zhou, 2006), UWSN puede clasificarse aproximadamente en dos grandes categorías:

- Vigilancia acuática a largo plazo no crónica: Este tipo de UWSN puede funcionar durante mucho tiempo y los datos recolectados por los sensores no son datos en tiempo real. Para el monitoreo a largo plazo, el ahorro de energía es un tema central a considerar en el diseño del protocolo. Es evidente que en las UWSN para el monitoreo acuático a largo plazo, la localización es una tarea imprescindible para localizar sensores móviles, ya que usualmente sólo los datos de localización son útiles en el monitoreo acuático. Además, la información de localización de sensor puede ser utilizada para ayudar al reenvío de datos, ya que el enrutamiento geográfico resulta ser más eficiente que una inundación pura. Además, la ubicación puede ayudar a determinar si los sensores flotan hasta el límite del área interesada. Si esto ocurre, los sensores deben tener algunos mecanismos para reubicarse (autopropulsados) o pop hasta la superficie del agua para la redistribución manual. Por último, se requiere una transferencia de datos confiable, resistente y segura para asegurar un sistema de observación robusto en la arquitectura UWSN presentada.

En este tipo de red, los nodos sensores están densamente desplegados para cubrir grandes y espaciales áreas de monitoreo continuo. Los datos son

recogidos por sensores locales, relacionados con sensores intermedios, y finalmente alcanzan los nodos de superficie (equipados con módems acústicos y RF (radiofrecuencia)), que pueden transmitir datos al centro de comando terrestre por radio.

Exploración Acuática Crítica de Tiempo Corto: Comparada a UWSN a largo plazo y no crítico en el tiempo, este tipo de UWSN se enfoca en datos en tiempo real. Por lo tanto, para hacer la transferencia de datos de manera eficiente deben ser más preocupantes al diseñar el protocolo de red. Además, este tipo UWSN sólo funciona para un corto plazo que significa que el ahorro de energía no es tan importante como a largo plazo. Sin embargo, la transferencia de datos confiable, resistente y segura es una característica avanzada siempre deseada para ambos tipos de UWSN.

En (Cui, Kong, Gerla, & Zhou, 2006) asumen que un equipo de investigación quiere identificar el lugar de destino de un barco accidentado y destruido naufrago.

7.2. Comparación de las dos clasificaciones

La diferencia entre las dos clasificaciones es estática y móvil. En (Cui, Kong, Gerla, & Zhou, 2006), las UWSN a largo plazo no críticos en el tiempo y de corta duración se basan en la capacidad móvil. Es por eso que se refieren a la ubicación consciente de cualquier manera. Por otra parte, a largo plazo y a corto plazo no distingue 2D o 3D. Obviamente, hay algunas diferencias en el diseño del protocolo.

El próximo año, las redes de sensores inalámbricos submarinas (WSNS) serán cada vez más importantes en la investigación del mundo submarino.

7.3. Factores Importantes Que Influyen En El Diseño De WMSN

- Requisito de QoS: Uno de los primeros y más importantes desafíos en el diseño de WMSNs es cumplir con los requisitos de QoS específicos de la aplicación. Los WMSNs están diseñados para abordar una gama de escenarios de aplicaciones que van desde la simple aplicación escalar hasta soporte multi-nivel que involucra sensores heterogéneos que incluye

soporte de sensores multimedia además del uso de sensores escalares. La transmisión de contenido multimedia se genera durante períodos de tiempo más largos y requiere una entrega de información sostenida. Por lo tanto, una base sólida es necesaria en términos de hardware y soportar algoritmos de alto nivel para ofrecer QoS para considerar los requisitos específicos de la aplicación.

- Restricciones de recursos: Los dispositivos sensores están restringidos en términos de batería, capacidad de procesamiento, memoria y velocidad de datos alcanzable.
- Demanda de ancho de banda alto: En los WMSN, el requisito de ancho de banda para la comunicación de datos multimedia es un orden de magnitud mayor que el ancho de banda requerido para las WSN existentes. Por ejemplo, la arquitectura escalar WSN que involucra átomos como TelosB o Micaz etc. soporta el estándar de radio Zigbee / 802.15.4 que soporta la velocidad de datos de hasta 250Kbps.
- Consumo de energía: El consumo de energía es una preocupación fundamental en los WMSN, incluso más que en las redes de sensores inalámbricos tradicionales. En Gürses y Akan, 2005 se introduce un enfoque específico para la conservación de la energía que puede utilizarse en la detección del cambio de estado de un punto caliente.
- Integración con la Arquitectura de Internet (IP): El diseño de WMSNs debe soportar varios otros estándares de comunicación inalámbrica como Bluetooth, WiFi, etc. y el paquete de Protocolo de Internet (IP). Esto puede permitir al usuario extraer la información de la red desde cualquier lugar en cualquier momento.

Añádase a estos factores (requisito de QoS, limitación de recursos ... etc.), existen otros factores que influyen en el diseño de WMSN:

- Capacidad variable del canal.
- Acoplamiento entre capas de funcionalidad.
- Técnicas de codificación de fuentes multimedia.

7.4. Arquitectura de Referencia de WSN

En (Akyildiz, Melodia, & Chowdhury, 2007) introducen una arquitectura de referencia para WMSNs, donde se muestran tres redes de sensores con diferentes características:

1. Sensores uniformes de un solo nivel, homogéneos, procesamiento distribuido, almacenamiento centralizado.

2. Sensores heterogéneos agrupados, de un solo nivel, procesamiento centralizado, almacenamiento centralizado.
3. Multier, sensores heterogéneos, procesamiento distribuido, almacenamiento distribuido.

7.5. Seguridad de redes inalámbricas de sensores multimedia

A medida que las redes inalámbricas de sensores multimedia se vuelven más ampliamente utilizadas, la seguridad en las redes de sensores multimedia también se convierte en un problema. Mientras que el uso de códigos más fuertes, técnicas de marca de agua, algoritmos de encriptación, entre otros, han resultado en una comunicación inalámbrica segura, hay consideraciones completamente diferentes en las redes WMSN (Akyildiz, Melodia y Chowdhury, 2006). Para mejorar la seguridad, se han utilizado técnicas de marca de agua (Wang, Peng, Wang, Sharif, & Chen, 2008). Sin embargo, por lo general, la seguridad mejorada obtenida por las técnicas de marca de agua es a costa del consumo de energía porque el cálculo de en las técnicas de marca de agua cuesta energía (Luo, 2013), que es un recurso precioso para los sensores. Para abordar este problema, se propuso un esquema adaptativo de marca de agua consciente de la energía en (Wang, Peng, Wang, Sharif, & Chen, 2008). Los detalles se pueden encontrar en (Wang, Peng, Wang, Sharif, & Chen, 2008). Otro trabajo sobre la seguridad en redes de sensores multimedia se puede encontrar en (Wang, Peng, Wang, Sharif, & Chen, 2008).

Capítulo 8. Cuestiones Abiertas En Redes De Sensores Inalámbricas

Extremadamente se requieren soluciones de eficiencia energética para cada aspecto del diseño WSN para ofrecer las ventajas potenciales del fenómeno WSN. Todavía existen varios otros grandes desafíos. En las subsecciones siguientes, se discuten estos retos y se ponen a relieve los problemas de investigación abiertos para abordarlos.

8.1. Integración de redes de sensores e Internet

Con el fin de ampliar la aplicabilidad de WSN y proporcionar información útil en cualquier momento y en cualquier lugar, su integración con Internet es muy importante. WSN intercomunicadas con Internet es de gran importancia, el método de interconexión IP es actualmente la forma más cómoda y eficaz. Teniendo en cuenta que la instancia completa convencional de la pila de protocolos TCP / IP no es apropiado para el sensor nodo (Zhou, y Zhang, 2013), esquemas de diseño de la pila de protocolos para todo IP WSN han sido propuestos por muchas instituciones y académicos.

Una visión general de cómo WSN se interconectan con las redes IPv6

De acuerdo con el autor en (Zhou, y Zhang, 2013), hay tres enfoques principales para conectar redes de sensores con redes TCP / IP, son las siguientes:

- Arquitectura de proxy: De esta manera, toda la interacción entre los clientes y los sensores nodo es a través de la representación mediante la conversión de protocolo y la superposición de protocolo. El inconveniente del enfoque de extrapolación es que puede crear un único punto de fallo.
- Retardo de tolerancia a Redes: El método de DTN (otoño de 2003) es muy similar a la arquitectura proxy, pero consiste en una capa de paquete que se encuentra por encima de la capa de transporte, lo que ayuda a evitar un punto único de fallo en el nodo receptor. Este enfoque está diseñado para entornos con problemas donde la partición de la red es frecuente.

- Arquitectura All-IP: En todo IP WSN, se requieren todos los sensores nodo para implementar el protocolo TCP / IPv6 para ser una terminal de red, realizando así una perfecta integración de WSN e Internet TCP / IP a través de la comunicación directa.

El 6LoWPAN (IPv6 Over, Low Power WPAN) (Grupo de trabajo IETF, 2013) estándar ha sido desarrollado para integrar el IPv6, estándar con sensores nodos de baja potencia. Esto marca que la combinación de IPv6 y WSN está en el camino hacia la normalización (Zhou, y Zhang, 2013). La capa física y la capa MAC del 6LoWPAN adaptan el estándar IEEE 802.15.4 (Hui, y Culler, 2008), mientras que la capa de red es compatible con IPv6 (Yibo et al, 2011). Una capa de adaptación entre la capa de red y la capa MAC está diseñado para lograr la conectividad sin fisuras de IPv6 y MAC con el estándar IEEE 802.15.4 (Zhou, y Zhang, 2013).

8.2. Direcciones Futuras De La Investigación

Las discusiones anteriores muestran claramente que, aunque hay mucha investigación de WSN, todavía existen muchos problemas abiertos. En esta sección, presentamos algunas de las direcciones de investigación futuras, resumidas como sigue:

8.2.1. WSNs heterogéneas:

Han surgido WSNs heterogéneas para resolver los problemas relacionados con las WSNs homogéneas, como las limitadas capacidades de energía. Una WSN heterogénea generalmente está formada por más de un tipo de nodos (Yu, Wang, Zhang, & Zheng, 2007) en su mayoría homogéneos con limitadas capacidades de cálculo y memoria, y pocos nodos heterogéneos con mayores capacidades que dan un equilibrio a las tareas (Kumar, Tsiatsis, & Srivastava, 2003) (Rhee, Seetharam, & Liu, 2004), y representa una manera efectiva de aumentar la vida útil de la red. La integración de la heterogeneidad en la red tiene muchas ventajas. De hecho, la heterogeneidad puede mejorar la escalabilidad de las redes de sensores, reducir las necesidades energéticas sin sacrificar el rendimiento, dar un equilibrio entre el costo de las redes y la funcionalidad, fomentar nuevas aplicaciones de banda ancha y mejorar los mecanismos de seguridad con protocolos más complejos y consumidores de energía. Los WSNs heterogéneos también presentan

desventajas como el problema de despliegue de nodos heterogéneos que consiste en definir el número y el emplazamiento de los nodos heterogéneos. Además, la introducción de nodos heterogéneos en la red puede presentar nuevas preocupaciones de seguridad. De hecho, las WSN heterogéneas tienen que considerar diversas capacidades de seguridad. En WSNs heterogéneos, los nodos homogéneos son económicos y de energía limitada. Sus tareas principales consisten en recolectar y reportar datos. Los nodos heterogéneos tienen tareas más complejas y computacionales, poder y memoria. Se consideran tres tipos de heterogeneidad en redes de sensores inalámbricos (Yu, Wang, Zhang, Zheng, 2007; Katiyar, Chand, & Soni, 2010):

- Heterogeneidad Computacional: En la heterogeneidad computacional, los nodos del sensor tienen un procesador más potente y más memoria, lo que lleva a cálculos complejos adicionales y almacenamiento de datos a más largo plazo.
- Heterogeneidad de enlaces: En la heterogeneidad de enlaces, los nodos de sensores están formados por el rango de radio más potente que permite transmisiones más confiables.
- Heterogeneidad energética: Los nodos contienen baterías de alimentación reemplazables o alimentadas directamente, lo que permite una mayor vida útil de la red.

8.2.2. Redes de Nano sensores (NSNs):

Debido al notable progreso en nanotecnología, se realiza una nueva clase de redes de sensores inalámbricos denominados nano-escala de redes de sensores (NSNs) y se utilizan cada vez más. Los NSNs se componen generalmente de dispositivos de escala nanométrica que realizan tareas básicas como la computación, la detección y la comunicación. Estos dispositivos no se comercializan, pero muchos proyectos están trabajando en producirlos a granel. Algunos tipos de nano sensores son reportados y sobrevivieron como sensores de hidrógeno en miniatura (Villatoro y Monzon-Herńandez, 2005), nano sensores para detección química y biológica (Yonzon, Stuart, Zhang, & McFarland, 2005), nano sensores químicos y biológicos para Molecular (Akyildiz, & Jornet, 2010) (Falconi, Damico, & Wang, 2007). Además, se exploran las posibilidades de comunicación a nanoescala para conectar los nano sensores para formar un NSN. El trabajo propuesto en (Akyildiz, Brunetti, Blazquez, 2008) confirma la posibilidad de comunicación a nanoescala, ya sea mediante electromagnetismo o algún tipo de transceptor de base molecular. En los últimos años se han realizado nuevas actividades de investigación para comprender las propiedades únicas de los nano materiales que

podrían utilizarse para la comunicación entre dispositivos nano (Akyildiz y Jornet, 2010), (Atakan, & Akan, 2010) (CHOU, 2013).

Debido a su posible uso en los niveles atómicos, un NSN puede ser explotado para nuevo tipo de aplicaciones de nanotecnología, donde se prevé la comunicación distribuida entre los nano sensores para lograr el objetivo de aplicación, que no se puede realizar con redes de sensores convencionales. Un ejemplo de las aplicaciones propuestas para los NSN es la aplicación biomédica (monitorización de la salud y suministro de fármacos), las aplicaciones medioambientales (monitorización de plantas y la lucha contra la plaga de insectos), industriales (interfaces táctiles ultra sensibles) y las aplicaciones militares (defensa biológica y química) (Akyildiz, & Jornet, 2010).

8.2.3. Biosensor Network:

Los investigadores se han centrado recientemente en la simulación de comportamiento de los animales, especialmente el comportamiento de las ratas. De hecho, han demostrado que, mediante la estimulación de las regiones del cerebro, los animales pueden ser guiados a través de entornos hostiles (S. K. Talwar et al, 2002). También pueden ser entrenados para realizar algunas tareas como encontrar objetivos tales como explosivos estimulando regiones del cerebro para producir o reforzar estímulos para varios movimientos comandados. De acuerdo con la simulación cerebral, los animales permiten al controlador guiarlos conduciendo así a una comunicación inalámbrica.

Recientemente, las operaciones de búsqueda y rescate involucran a animales que son expertos en la negociación de terrenos 3D difíciles tanto en la luz como en la oscuridad y que combinan sus funciones naturales como olfato, visual, auditivo y sensaciones táctiles para encontrar sustancias químicas o personas. Esto los hace más eficaces que los robots mecánicos. Recientemente, y debido a los avances en neurofisiología, es posible entrenar a un gran número de ratas que son guiadas a distancia a coste moderado. Además, los avances en la integración a gran escala de baja potencia (VLSI) y los sistemas microelectrónicos (MEMS) permiten diseñar dispositivos inalámbricos de comunicación y conexión en red que podrían caber en una mochila transportada por una rata.

En las aplicaciones dedicadas a las misiones de rescate, el grupo de ratas puede ser guiado y coordinado de forma autónoma para formar una red cooperativa de sensores inalámbricos de múltiples saltos y completar una misión crítica (Li, Panwar, Mao, Burugupalli y Lee, 2005). La red de biosensores está

dedicada principalmente a aplicaciones de recuperación de desastres naturales (búsqueda de personas atrapadas y peligros), aplicaciones de seguridad nacional (búsqueda de explosivos, bioagentes, etc., en contenedores o buques de carga), operaciones militares (por ejemplo, reconocimiento y búsqueda de minas), Y aplicaciones de aplicación de la ley (por ejemplo, recolectando evidencia de regiones inaccesibles) donde es importante desarrollar tecnologías de comunicación inalámbrica y de red que permitan la configuración y operación de la red de sensores que está compuesta por un conjunto coordinado de animales entrenados y algunos robots mecánicos. Guiado por un centro de mando. En el futuro los animales pueden ser reemplazados por robots.

Las redes de biosensores presentan algunos problemas que deben abordarse. De hecho, en este tipo de redes, las ratas deben trabajar en tres tipos diferentes de roles: buscadores, seguidores y relés. Es importante investigar más las técnicas de control cooperativo para guiar y recompensar de forma autónoma a un gran conjunto de animales que realizan diferentes tareas y generalizar estas técnicas para incluir un equipo de buscadores. La búsqueda puede apuntar a minimizar el tiempo total de búsqueda minimizando la distancia recorrida por cada buscador. En este tipo de redes, el sistema de transmisión por radio tiene que satisfacer las necesidades de los sensores, el sistema de gestión de red para la información de enrutamiento y el sistema de control de información de estado y de orientación remota que tiene sus propios requisitos de calidad de transmisión y señal. Las características de propagación de radio deben ser exploradas en la capa física.

8.2.4. Red de Sensores de Cuerpo Inalámbrico (WBSN):

Una red de sensores de cuerpo inalámbricos (WBSN) es un tipo de WSN basado en radiofrecuencia (rf). Una característica principal de WBSN es que permite la interconexión de nodos minúsculos con capacidades del sensor o del actuador en, sobre, o alrededor de un cuerpo humano en un corto alcance de cerca de 2m. La red sin hilos del sensor del cuerpo se desarrolla especialmente para supervisar, manejar y comunicar diversos signos vitales del cuerpo humano como temperatura y presión arterial. Para ello, se instalan diferentes sensores en la ropa o directamente en el cuerpo o bajo la piel humana. Los actuadores instalados en el cuerpo humano se utilizan para inyectar drogas controladoras o medicamentos que salvan vidas. La comunicación entre sensores, actuadores y teléfono celular se establece a través de una unidad central. La función del teléfono celular consiste en transmitir la información a y desde el cuerpo humano al mundo externo (médico,

emergencia). En WBSNs, las direcciones IP se asignan a cada cuerpo. El estándar IEEE 802.15 Task Group 6 se utiliza para desarrollar dispositivos de bajo consumo energético y para desarrollar aplicaciones para WBAN.

Muchos estudios sobre la propagación de ondas electromagnéticas en el cuerpo han sido conducidos por investigaciones que han propuesto algunos modelos para la capa física. Incluso si los movimientos del cuerpo pueden influir directamente en la intensidad de la señal recibida, los modelos propuestos no los consideran. Recientemente, se realizan investigaciones basadas en el acoplamiento galvánico y la transformación de información a través de los huesos y que pueden ofrecer resultados prometedores y más investigados. A nivel de la capa de enlace de datos y de la capa de red, se han propuesto algunos protocolos. Este nivel todavía tiene un montón de temas de investigación abierta. En el nivel de la capa de enlace de datos, los investigadores deben tener en cuenta en el desarrollo de protocolos específicos MAC las características del cuerpo, tales como los movimientos, la fisiología humana, como el latido del corazón. También deben tener en cuenta la movilidad de los nodos. La combinación de enrutamiento térmico con mecanismos más eficientes energéticamente representa un interesante tema de investigación en este campo. Además, los frameworks de Qos son esenciales y deben ser usados. El apoyo a la movilidad incorporado en el protocolo, la seguridad, la interoperabilidad y otras cuestiones representan problemas de investigación prometedores que deben ser investigados. Muchos de estos mecanismos podrían unirse en un protocolo de capas cruzadas para realizar un sistema óptimo.

Referencias

Adams, J. (2004). Designing with 802.15.4 and ZigBee. Paper presented at the Industrial Wireless Applications Summit, San Diego, CA.

Akyildiz, I. F., Brunetti, F., & Blazquez, C. (2008). Nano networks: A new communication paradigm. Computer Networks, 52(12), 2260–2279. doi:10.1016/j.comnet.2008.04.001

Akyildiz, I. F., & Jornet, J. M. (2010). Electromagnetic wireless nanosensor networks. Nano Communication Networks, 1(1), 3–19. doi:10.1016/j.nancom.2010.04.001

Akyildiz, I. F., Melodia, T., & Chowdhury, K. R. (2006). A survey on wireless multimedia sensor networks. Computer Networks, 51(4), 921–960. doi:10.1016/j.comnet.2006.10.002

Akyildiz, I. F., Melodia, T., & Chowdury, K. R. (2007). Wireless multimedia sensor networks: A survey. IEEE Wireless Communications, 14(6), 32–39. doi:10.1109/MWC.2007.4407225

Akyildiz, I. F., Pompili, D., & Melodia, T. (2005). Underwater acoustic sensor networks: Research challenges. Ad Hoc Networks, 3(3), 257–279. doi:10.1016/j.adhoc.2005.01.004

Akyildiz, I. F., & Stuntebeck, E. P. (2006). Wireless underground sensor networks: Research challenges. Ad Hoc Networks Journal, 4(6), 669–686. doi:10.1016/j.adhoc.2006.04.003

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002, March). (2002-1). Wireless sensor networks: A survey. Computer Networks, 38(4), 393–422. doi:10.1016/S1389-1286(01)00302-4

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002, August). (2002-2). A Survey on Sensor Networks. IEEE Communications Magazine, 40(8), 102–114. doi:10.1109/MCOM.2002.1024422

Akyildiz, I. F., Sun, Z., & Vuran, M. C. (2009). Signal Propagation Techniques for Wireless nderground Communication Networks. Physical Communication Journal, 2(3), 167–183. doi:10.1016/j.phycom.2009.03.004

Alrajeh, N. A., Khan, S., & Shams, B. (2013). Intrusion Detection Systems in Wireless Sensor Networks: A Review. International Journal of Distributed Sensor Networks, 1–7.

Atakan, B., & Akan, O. (2010). Carbon nano tube-based nano scale ad hoc networks. IEEE Communications Magazine, 48(6), 129–135. doi:10.1109/ MCOM.2010.5473874
Boubiche, D., & Bilami, A. (2011). HEEP (Hybrid Energy Efficiency Protocol)

Based on Chain Clustering. Int. J. Sensor Networks, 10(1/2), 25–35. doi:10.1504/IJSNET.2011.040901

Chou, C. T. (2012). Molecular circuits for decoding frequency coded signals in nano-communication networks. Nano Communication Networks, 3(1), 46–56. doi:10.1016/j.nancom.2011.11.001

Chou, C. T.Chun Tung Chou. (2013). Extended Master Equation Models for Molecular Communication Networks. IEEE Transactions on Nanobioscience, 12(2), 79–92. doi:10.1109/TNB.2013.2237785 PMID:23392385

Cui, J.-H., Kong, J., Gerla, M., & Zhou, S. (2006). Challenges: Building Scalable Mobile Underwater Wireless Sensor Networks for Aquatic Applications. IEEE Network. Special Issue on Wireless Sensor Networking, 20(3), 12–18.

Debar, H., Dacier, M., & Wespi, A. (1999). Towards a taxonomy of intrusion-detection systems. Computer Networks, 31(8), 805–822. doi:10.1016/S1389-1286(98)00017-6

Falconi, C., Damico, A., & Wang, Z. (2007). Wireless Joule nano heaters. Sensors and Actuators, 127(1), 54–62. doi:10.1016/j.snb.2007.07.002

Fall, K. (2003). A delay-tolerant network architecture for challenged internets. Paper presented at the SIGCOMM'2003, Karlsruhe, Germany. doi:10.1145/863955.863960

Gao, T., Greenspan, D., Welsh, M., Juang, R., & Alm, A. (2005). Vital SignsMonitoring and Patient Tracking over a Wireless Network. Paper presented at IEEE 27th Annual International Conference of the Engineering in Medicine and Biology Society (EMBS), Shanghai, China.

Gürses, E., & Akan, Ö. B. (2005). Multimedia communication in wireless sensor networks. Annales des Télécommunications, 60(7-8), 872–900.

Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2002). An applicationspecific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications, 1(4), 660–670. doi:10.1109/TWC.2002.804190

Hui, J. W., & Culler, D. E. (2008). IP is dead, long live IP for wireless sensor networks. Paper presented at the sixth ACM conference on embedded network Sensor System (SenSys '08), Raleigh, USA. doi:10.1145/1460412.1460415

IETF Working Group. (2013). IPv6 over low power WPAN working group. Available from http://tools.ietf.org/wg/6lowpan/

Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and coun-termeasures. Ad Hoc Networks, 1(2-3), 293–315. doi:10.1016/S1570-8705(03)00008-8

Katiyar, I., Chand, N., & Soni, S. (2010). Clustering Algorithms for Heterogeneous Wireless Sensor Network: A Survey. International Journal of Applied Engineering Research, 1(2), 273–287.
Kifayat, K., Merabti, M., Shi, Q., & Llewellyn, D. (2010). Security in Wireless Sensor Networks. In Handbook of Information and Communication Security. Springer. doi:10.1007/978-3-642-04117-4_26

Kim, D. S., & Chung, Y. J. (2006). Self-organization routing protocol supporting mobile nodes for wireless sensor network. Paper presented at the First Int. Multi-Symp. on Computer and Computational Sciences, Hangzhou, China. doi:10.1109/IMSCCS.2006.265

Kumar, G. S., Vinu, P. M. V., & Jacob, K. P. (2003). Mobility Metric based LEACHMobile Protocol. Paper presented at the 16th International Conference on Advanced Computing and Communications (ADCOM'08), Chennai, India.

In-Network Processing. Paper presented at the 2nd Intl. Workshop on Wireless Networks and Applications, San Diego, CA.

Kweon, K., Ghim, H., Hong, J., & Yoon, H. (2009). Grid-Based Energy-Efficient Routing from Multiple Sources to Multiple Mobile Sinks in Wireless Sensor Networks. Paper presented at the 4th International Symposium on Wireless Pervasive Computing (ISWPC'09), Melbourne, Australia. doi:10.1109/ISWPC.2009.4800585

Lee, S., Noh, Y., & Kim, K. (2013). Key Schemes for Security Enhanced TEEN Routing Protocol in Wireless Sensor Networks. International Journal of Distributed Sensor Networks, 2013, 1–8. doi:10.1155/2013/374796

Li, Y., Panwar, S. S., Mao, S., Burugupalli, S., & Lee, J. (2005). A Mobile Ad Hoc Bio-Sensor Network. Proceedings of the IEEE, ICC, 2005.

Lindsey, S., & Raghavendra, C. (2002). PEGASIS: Power-Efficient Gathering in Sensor Information Systems. Paper presented at the IEEE Aerospace Conference, Montana, USA. doi:10.1109/AERO.2002.1035242

Loo, C. E., Yong, M., Leckie, C., & Palaniswami, M. (2006). Intrusion Detection for Routing Attacks in Sensor Networks. International Journal of Distributed Sensor Networks, 2(4), 313–332. doi:10.1080/15501320600692044

Luo, Z. (2008). Survey of Networking Techniques for Wireless Multimedia Sensor Networks. International Journal of Recent Technology and Engineering, 2(2), 182–183.

Manjeshwar, A., & Agrawal, D. P. (2002). APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks. Paper presented at the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, Ft. Lauderdale,

FL. doi:10.1109/IPDPS.2002.1016600

Maraiya, K., Kant, K., & Gupta, N. (2011). Application based Study on Wireless Sensor Network. International Journal of Computers and Applications, 21(8), 9–15. doi:10.5120/2534-3459

Ng, J. W. P., Lo, B. P. L., Wells, O., Sloman, M., Peters, N., Darzi, A., . . . Yang, G.-Z. (2004). Ubiquitous Monitoring Environment for Wearable and Implantable Sensors. Paper presented at the International Conference on Ubiquitous Computing (UbiComp), Tokyo, Japan.

Nguyen, L. T., Defago, X., Beuran, R., & Shinoda, Y. (2008). An Energy Efficient Routing Scheme for Mobile Wireless Sensor Networks. Paper presented at the IEEE International Symposium on Wireless Communication Systems (ISWCS'08), Reykjavik, Iceland.

Padmavathi, G., & Shanmugapriya, D. (2009). A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. International Journal of Computer Science and Information Security, 4(1-2), 1–9.

Pathan, A.-S. K., Dai, T. T., & Hong, C. S. (2006). A Key Management Scheme with Encoding and Improved Security for Wireless Sensor Networks. In S. Madria et al. (Ed.), International Conference on Distributed Computing and Internet Technology (ICDCIT'06) (LNCS) (Vol. 4317, pp. 102-115). Berlin, Germany: Springer. doi:10.1007/11951957_10

Rhee, S., Seetharam, D., & Liu, S. (2004). Techniques for Minimizing Power Consumption in Low Data-Rate Wireless Sensor Networks. In Proc. of IEEE Wireless Communications and Networking Conference. Atlanta, GA: IEEE.

Sara, G. S., Kalaiarasi, R., Pari, S. N., & Sridharan, D. (2010). Energy Efficient Mobile Wireless Sensor Network Routing Protocol. In N. Meghanathan et al. (Ed.), Recent Trends in Networks and Communications: Proceedings of the International Conferences, NeCoM 2010, WiMoN 2010, WeST 2010, (LNCS) (Vol. 90, pp 642- 650). Berlin, Germany: Springer. doi:10.1007/978-3-642-14493-6_65

Silva, A. P. R. D., Martins, M. H. T., Rocha, B. P. S., Loureiro, A. A. F., Ruiz, L. B., & Wong, H. C. (2005). Decentralized intrusion detection in wireless sensor networks. Paper presented at the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, Montreal, Canada. doi:10.1145/1089761.1089765

Silva, A. R., & Vuran, M. C. (2010). Communication with Aboveground Devices in Wireless Underground Sensor Networks: An Empirical Study. Paper presented at the IEEE International Conference on Communications (ICC), Cape Town, South Africa. doi:10.1109/ICC.2010.5502315

Talwar, S. K., Xu, S., Hawley, E. S., Weiss, S. A., Moxon, K. A., & Chapin, J. K.

(2002). Behavioural Neuroscience: Rat Navigation Guided by Remote Control. Nature, 417(6884), 37–38. doi:10.1038/417037a PMID:11986657

Villatoro, J., & Monzon-Herńandez, D. (2005). Fast detection of hydrogen with nano fiber tapers coated with ultra thin palladium layers. Optics Express, 13(13), 5087–5092. doi:10.1364/OPEX.13.005087 PMID:19498497

Wang, H., Peng, D., Wang, W., Sharif, H., & Chen, H. (2008). Energy-Aware Adaptive Watermarking for Real-Time Image Delivery in Wireless Sensor Networks. Paper presented at theIEEE International Conference on Communications (ICC '08), Beijing, China. doi:10.1109/ICC.2008.286

Wood, A., Virone, G., Doan, T., Cao, Q., Selavo, L., Wu, Y., . . . Stankovic, J. (2006). ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring. Technical Report CS-2006-11. University of Virginia.

Yibo, C., Hou, K.-M., Zhou, H., Shi, H.-L., Liu, X., Diao, X., . . . De Vaulx, C. (2011). 6LoWPAN stacks: a survey. Paper presented at the 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), Wuhan, China.

Yonzon, C. R., Stuart, D. A., Zhang, X., McFarland, A. D., Haynes, C., & Vanduyne, R. (2005). Towards advanced chemical and biological nano sensors-An overview. Talanta, 67(3), 438–448. doi:10.1016/j.talanta.2005.06.039 PMID:18970187

Younis, O., & Fahmy, S. (2004). HEED: A Hybrid Energy-Efficient Distributed Clustering Approach for Ad Hoc Sensor Networks. IEEE Transactions on Mobile Computing, 3(4), 366–379. doi:10.1109/TMC.2004.41

Yu, L., Wang, N., Zhang, W., & Zheng, C. (2007). Deploying a Heterogeneous Wireless Sensor Network. Paper presented at the International Conference on Wireless Communications, Networking and Mobile Computing (WiCom'07), Shanghai, China.

Zhang, P., Sadler, C., Lyon, S., & Martonosi, M. (2004). Hardware design experiences in ZebraNet. Paper presented at the ACM SenSys'04, Baltimore, MD. doi:10.1145/1031495.1031522

Zhou, Q., & Zhang, R. (2013). A Survey on All-IP Wireless Sensor Network. Paper presented at the 2nd International Conference on Logistics, Informatics and Service Science, Beijing, China. doi:10.1007/978-3-642-32054-5_105

TÉRMINOS Y DEFINICIONES CLAVE

E2MWSNRP: protocolo de enrutamiento de red de sensores inalámbricos móviles con eficiencia energética, es un protocolo de enrutamiento híbrido de múltiples rutas que puede diseñarse principalmente para red de sensores inalámbricos móviles deficientes en energía dinámica donde la disipación de energía, la reducción y la transmisión confiable de datos es imprescindible.

GBEER: El enrutamiento eficiente en energía basado en la red es un protocolo de enrutamiento muy eficiente en energía para la comunicación desde múltiples fuentes a múltiples sumideros móviles en red de sensores inalámbricos.

Sistemas de detección de intrusos: se define como un sistema que monitorea la computadora, sistema o actividades de red para detectar signos de violaciones de las políticas de seguridad. En general, los esquemas de IDS se clasifican en IDS de mal uso e IDS de anomalías.

LEACH-ME: Jerarquía de agrupación adaptativa de baja energía-Mobile Enhanced es Una versión mejorada de M-LEACH. En LEACH-ME, la selección de cluster-head es basado en los nodos menos móviles en relación con sus vecinos. La fase de estado estacionario es lo mismo para LEACH-M y LEACH-ME.

LEACH-Mobile: Jerarquía de agrupamiento adaptativo de baja energía-Mobile es una autoorganización protocolo de enrutamiento que admite nodos móviles para WSN. En el propuesto esquema, como LEACH se divide en rondas, donde cada ronda comienza con una fase de configuración cuando los grupos están organizados, seguidos de una fase de estado estable cuando se producen transferencias de datos a la estación base. Para minimizar los gastos generales, el constante
La fase de estado es larga en comparación con la fase de configuración. Una de las ideas básicas en LEACHMobile es confirmar la inclusión de nodos sensores en un grupo específico en la constante fase de estado

M-LEACH: la jerarquía de agrupación adaptativa móvil de baja energía es una agrupación protocolo de enrutamiento que permite la movilidad de nodos de cabeza de clúster y no cabeza de clúster durante la fase de configuración y estado estable. La fase de configuración de LEACH se modifica por M-LEACH para seleccionar cabezales de clúster adecuados según el modelo de atenuación

y velocidad de movilidad. En la fase de estado estable, si los nodos se alejan del clúster o
la cabeza del clúster se aleja de sus nodos miembros, MLEACH proporciona una transferencia mecanismo para que los nodos se conecten a un nuevo clúster para evitar una falta de eficiencia en agrupación de formación.

UWSN: la red inalámbrica de sensores submarinos es una extensión de la tierra redes inalámbricas de sensores, donde los nodos sensores están bajo el agua y se comunican por señales acústicas a través del agua.
Red inalámbrica de sensores: una infraestructura compuesta por varios nodos de sensores, donde el objetivo principal de un nodo sensor es recopilar información de su entorno y transmitirlo a uno o más puntos de control centralizado; llamadas estaciones base.

WMSN: la red inalámbrica de sensores multimedia se compone de varias redes inalámbricas, nodos inteligentes interconectados que están equipados con cámaras, micrófonos y otros sensores que producen contenido de datos multimedia.

WUSN: La red inalámbrica de sensores subterráneos es una extensión importante de redes de sensores inalámbricos terrestres, donde los nodos sensores están enterrados bajo tierra y se comunican de forma inalámbrica a través del suelo.