



PFC ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA

***DESARROLLO DE APLICACIONES
BASADAS EN WSN***

Autor: **Sebastián Román Maroto Cantillo**

Director: **Juan Vicente Capella Hernández**

Valencia, Septiembre 2010

Índice

1. Introducción-----	8
1.1 Motivación y finalidad-----	8
1.2 Breve introducción-----	8
1.3 Estructuración del proyecto-----	9
1.4 Objetivos-----	9
2. Redes Inalámbricas de Sensores WSN-----	10
2.1 Orígenes de las Redes de Sensores-----	10
2.2 Redes Inalámbricas de Sensores-----	12
2.2.1 Hardware de un Nodo Sensor-----	16
2.2.2 Software de un Nodo Sensor-----	23
2.2.2.1 PalOS-----	24
2.2.2.2 SOS-----	24
2.2.2.3 TinyOS-----	25
2.2.2.4 Linux-----	27
2.2.2.5 .NET Micro Framework-----	28
2.2.2.6 eCos-----	29
2.2.2.7 uC/OS-----	30
2.2.2.8 Contiki-----	30
2.2.2.9 MANTIS-----	31
2.2.2.10 BTnut-----	31
2.2.3 Lenguajes de Programación-----	32
2.2.3.1 Nesc-----	32
2.2.4 Diseño de Red-----	33
2.2.5 Aplicaciones-----	39
2.2.5.1 Militar-----	39
2.2.5.2 Medio Ambiente-----	40
2.2.5.3 Salud-----	42
2.2.5.4 Estructuras-----	45
2.2.5.5 Agricultura-----	57
2.2.5.6 Automoción-----	50
2.2.5.7 Domótica-----	51
2.3 Alternativas de Consumo-----	54
3. Estándares de Comunicación Orientados a Redes WSN-----	57
3.1 Tecnología Inalámbrica-----	57
3.2 Pila de Protocolos ZIGBEE-----	59
3.3 Protocolo de Comunicación IEEE 802.15.4-----	61
3.3.1 Capa de Red-----	64
3.3.2 Capa de Enlace de Datos-----	64
3.3.2.1 Formato General de Tramas MAC-----	65
3.3.2.2 La estructura de las super-tramas-----	68
3.3.2.2.1 Intercambio de tramas entre dispositivos-----	71
3.3.2.3 Mecanismo GTS (Guaranteed Time Slot)-----	74
3.3.2.4 Escaneo pasivo del medio-----	74
3.3.2.5 Mecanismo de orfandad-----	74
3.3.3 Capa Física-----	75
3.3.3.1 Canalización-----	75
3.3.3.2 Estructura de trama a nivel físico-----	77
3.3.3.3 Frecuencias y modulación-----	77
3.3.3.4 Sensitividad y Rango-----	79
3.3.3.5 Interferencia de y para otros dispositivos-----	80

3.4	Compatibilidad entre WIFI y ZIGBEE-----	81
3.4.1	Regulación europea para la banda 2400 Mhz-----	83
3.4.2	Comparativa estándares Wireless-----	83
3.5	Protocolos de Encaminamiento-----	85
4.	Mercado de las WSN-----	89
4.1	Introducción-----	89
4.2	Mercado de actualidad-----	90
4.2.1	Comparativa de Nodos Inalámbricos-----	93
4.3	Empresas destacadas-----	94
4.3.1	Libelium-----	94
4.3.2	Jennic-----	96
4.4	Actualidad y líneas futuras-----	97
5.	Conclusiones-----	102
	Acrónimos-----	104
	Bibliografía-----	107

Índice de figuras

2.1. Utilización del sonar en los barcos-----	10
2.2. Estructura de una red ad-hoc-----	13
2.3. Partes de un nodo sensor-----	16
2.4. Estructura interna de un sensor inalámbrico inteligente-----	16
2.5. Ejemplo de hardware de sensores-----	17
2.6. Fuentes de energía para los motes-----	20
2.7. Características de dispositivos inalámbricos I-----	21
2.8. Características de dispositivos inalámbricos II-----	21
2.9. Diferentes tipos de sensores-----	22
2.10. Tamaño de los sensores-----	23
2.11. Diagrama de topología cluster-tree de una red ad-hoc-----	23
2.12. Modelo de ejecución-----	24
2.13. Capas funcionales de SOS-----	25
2.14. Planificador Kernel TinyOS-----	26
2.15. Modelo de componentes de TinyOS y interacción de componentes-----	27
2.16. Principales variables a considerar-----	27
2.17. Ejemplo código NesC-----	33
2.18. Distribución de una red de sensores-----	35
2.19. Topología en estrella-----	36
2.20. Topología en malla-----	37
2.21. Topología híbrida-----	38
2.22. Ejemplo monitorización de una selva tropical-----	38
2.23. Diferentes aplicaciones de las redes sensores-----	39
2.24. Imagen de la dispersión del gas en el área-----	40
2.25. Vista aérea de la isla-----	41
2.26. Petrels-----	41
2.27. Distribución de los sensores-----	42
2.28. Investigadores tomando datos del glaciar-----	42
2.29. Ojo humano con chip integrado-----	43
2.30. Monitorización de un paciente-----	44
2.31. Ejemplo de seguimiento de un paciente-----	45
2.32. Placa del sensor-----	46
2.33. Arquitectura geográfica-----	46
2.34. Monitoreo de estructuras-----	47
2.35. Puntos en los que se colocan los sensores en los puentes-----	47
2.36. Sensor agrícola del proyecto LOFAR de la lucha contra el hongo Fitóftora-----	48
2.37. Control de viñedos-----	49
2.38. Sistema de riego-----	49
2.39. Control del tráfico-----	51
2.40. Clasificación de tecnología de redes domésticas-----	52
2.41. Sistema de iluminación inteligente en oficinas-----	54
2.42. Modelo energía renovable-----	54
2.43. Sistema de renovación de energía-----	55
2.44. Dispositivos EnOcean-----	56
3.1. Diferentes tecnologías inalámbricas-----	58
3.2. Principales tecnologías inalámbricas-----	58
3.3. Pila protocolos-----	59
3.4. Robustez tecnologías inalámbricas-----	60
3.5. Pila OSI-----	61
3.6. Arquitectura de capas orientadas a WSN-----	62
3.7. Propiedades del IEEE 802.15.4-----	62
3.8. MAC Data Service-----	63

3.9. Relación del IEEE 802.15.4 con el sistema OSI-----	64
3.10. Formato de una trama <i>beacon</i> según el estándar IEEE 802.15.4-----	66
3.11. Formato de una trama de <i>datos</i> según el estándar IEEE 802.15.4-----	66
3.12. Formato de una trama <i>acknowledgment</i> según el estándar IEEE 802.15.4-----	67
3.13. Tramas de control-----	67
3.14. Formato de una trama de <i>control</i> según el estándar IEEE802.15.4-----	68
3.15. Estructura super-trama-----	69
3.16. Slotted CSMA/CA-----	69
3.17. UnSlotted CSMA/CA-----	70
3.18. Comunicación destinada a un coordinador en redes balizadas-----	71
3.19. Comunicación destinada a un coordinador en redes no balizadas-----	71
3.20. Comunicación originada en un coordinador en redes balizadas-----	72
3.21. Comunicación originada en un coordinador en redes no balizadas-----	72
3.22. Estructura de canales del IEEE 802.15.4-----	75
3.23. Frecuencia de los canales IEEE 802.15.4-----	75
3.24. Estructura de una trama PPDU según el estándar IEEE 802.15.4-----	76
3.25. Paquete PHY-----	76
3.26. Frecuencias, modulaciones y parámetros de ensachado del estándar IEEE 802.15.4-----	77
3.27. Funciones de modulación y ensanchado-----	77
3.28. Señales I/Q moduladas en banda base de la secuencia correspondiente al símbolo 0. -----	78
3.29. Interferencia con Wifi, regulación americana-----	81
3.30. Interferencia con Wifi, regulación europea. Canales 2, 7 y 12-----	81
3.31. Regulación europea para la banda de 2400 Mhz-----	82
3.32. Estándares Wireless-----	82
3.33. Comparativa de características entre diversas tecnologías inalámbricas-----	83
3.34. Protocolos de encaminamiento en redes de sensores inalámbricos.-----	84
4.1. Evolución del mercado-----	88
4.2. Barreras de adopción de WSN-----	89
4.3. Comparativa de nodos inalámbricos-----	92
4.4. Dispositivo JN5121-----	95
4.5. Sensores en el organismo-----	96
4.6. Esquema de SenseWeb-----	97
4.7. Sensado emocional de anuncios-----	98
4.8. Representación visual a través de paredes-----	99
4.9. Pulsioximetría con Wii-----	99
4.10. Servicios de Pachube-----	100

1. Introducción

1.1 Motivación y finalidad

Las redes de sensores inalámbricas son una tecnología en plena evolución que requiere grandes investigaciones para su desarrollo y aplicación. Esto es lo que nos ha motivado a la hora de realizar nuestro proyecto final de carrera, ya que teníamos gran interés en los temas relacionados con la domótica y éste se ciñe a lo que estábamos buscando. Ésta es una tecnología novedosa y de gran futuro, debido a que gracias a ella conseguiremos tener unas mejores prestaciones y adoptar una mejor calidad de vida.

Con éste proyecto pretendemos recopilar gran cantidad de información que pueda ser consultada por otras personas interesadas en la investigación de esta tecnología y les pueda servir como apoyo en aspectos de hardware, software, protocolos y aplicaciones.

1.2 Breve introducción

Durante la última década han aparecido infinidad de dispositivos que utilizan sensores para el monitoreo y control. Gracias a la evolución en prestaciones y tamaño que nos ofrece la electrónica actual, disponemos de sensores capaces de comunicarse de manera inalámbrica, capacidad de procesamiento y autonomía propia. Este tipo de dispositivos nos abre un nuevo abanico de oportunidades para diseñar y crear todo tipo de aplicaciones, protocolos y sistemas capaces de facilitar el trabajo a los seres humanos a la vez que reducen sus costes.

Las Redes Inalámbricas de Sensores o RIS (también llamadas WSN por sus siglas en inglés) pueden estar compuestos por decenas, cientos o incluso miles de pequeños computadores que operan con baterías, llamados motes y que son distribuidos a lo largo de un ambiente de interés particular. Cada nodo en una red ad-hoc recolecta datos de su ambiente, como la cantidad de luz, temperatura, humedad, vibraciones y otros factores ambientales. Cada nodo sensor, puede enviar los datos recolectados a sus vecinos, éstos a su vez a sus propios vecinos y así sucesivamente, hasta que la información alcance un destino específico, donde será procesada por computadores más “tradicionales”, brindando una buena imagen del ambiente circundante en tiempo real.

Las aplicaciones de las redes sensoriales son numerosas, desde la monitorización de un campo de cultivo, el control de presión de los neumáticos de un automóvil, el seguimiento de animales en su hábitat, verificar las propiedades físicas de piezas críticas, hasta el seguimiento médico de un paciente. Pero la idea dominante radica en las restricciones que imponen las RIS, las tecnologías que la implementan y las necesidades específicas de las aplicaciones, que requieren protocolos de encaminamiento más eficientes que incluyan criterios como maximizar el tiempo de vida de la red, garantizar la conectividad entre los nodos, lograr una alta tasa de recepción, manejar cambios dinámicos de la topología, etc. Estos protocolos son diseñados con premisas muy diferentes en cuanto a la composición o capas de la red, por lo que protocolos tradicionales basados en IP no pueden ser aplicados a las RIS. Todo esto ha potenciado la investigación en esta área, para buscar nuevas técnicas que eliminen las ineficiencias en el consumo de energía que acortan la vida de la red.

1.3 Estructuración del proyecto

La estructura en que hemos enfocado el proyecto profundiza sobre las redes de sensores inalámbricas. Comenzamos hablando de la historia de las redes de sensores inalámbricas pasando por su hardware, software y sus múltiples aplicaciones hoy en día utilizadas. Después pasamos a conocer los diferentes protocolos para el funcionamiento eficiente de estas redes, como es el protocolo ZigBee y el estandar IEEE 802.15.4, detallando las diferentes capas y mecanismos de funcionamiento, además de la compatibilidad entre diferentes tecnologías inalámbricas y los diferentes protocolos de encaminamiento.

Finalizamos hablando del comercio actual de las WSN, las diferentes empresas que encabezan esta tecnología, haciendo hincapié en Libelium, que es una empresa española lider en el país, y acabamos dando a conocer algunas ideas futuras que se quieren llevar a cabo con este tipo de redes y que aún pareciendo algo futuristas formarán parte de nuestras vidas en poco tiempo.

1.4 Objetivo

El objetivo principal de éste proyecto es llevar a cabo un estudio sobre las redes de sensores inalámbricas mostrando un amplio abanico de aplicaciones de ésta tecnología, el porqué de su creación y adaptación en función de las necesidades de cada situación, resaltando la importancia de los protocolos para su comunicación y profundizando más en los diferentes sistemas operativos y los múltiples lenguajes de programación.

2. Redes Inalámbricas de Sensores WSN

2.1. Orígenes de las Redes de Sensores

Las redes de sensores provienen de la utilización de sensores durante las guerras con la detección de los atacantes por mar. Es por esto que empezaron a utilizar el “SONAR” (del inglés SONAR, acrónimo de Sound Navigation And Ranging, ‘navegación y alcance por sonido’) que es una técnica que usa la propagación del sonido bajo el agua (principalmente) para navegar, comunicarse o detectar otros buques.

El sonar puede usarse como medio de localización acústica, funcionando de forma similar al radar, con la diferencia de que en lugar de emitir señales de radiofrecuencia se emplean impulsos sonoros. De hecho, la localización acústica se usó en aire antes que el radar, siendo aún de aplicación el SODAR (la exploración vertical aérea con sonar) para la investigación atmosférica.

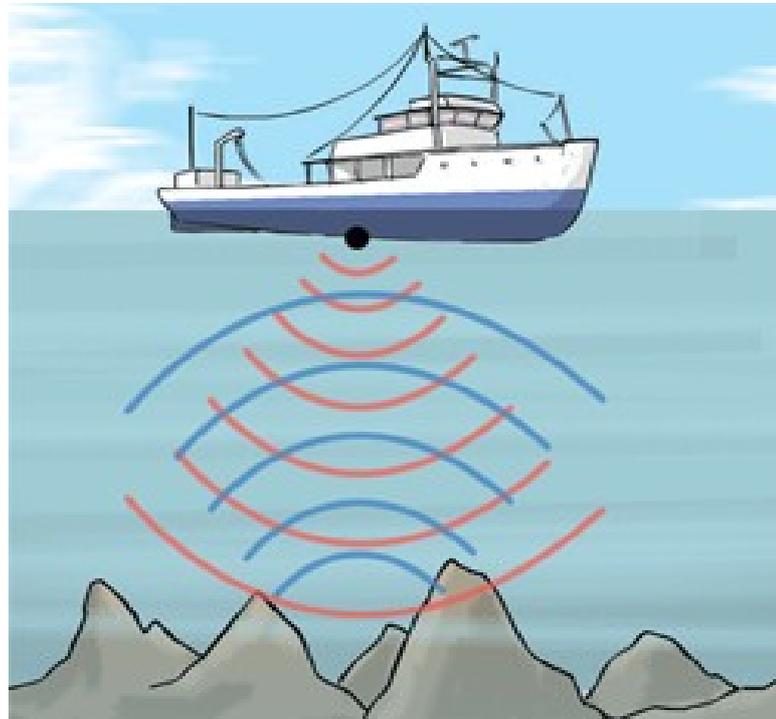


Figura 2.1: Utilización del sonar en los barcos

El término «sonar» se usa también para aludir al equipo empleado para generar y recibir el sonido. Las frecuencias usadas en los sistemas de sonar van desde las infrasónicas a las ultrasónicas. Aunque algunos animales (como delfines y murciélagos) han usado probablemente el sonido para la detección de objetos durante millones de años, el uso por parte de humanos fue registrado por vez primera por Leonardo Da Vinci en 1490. Se decía que se usaba un tubo metido en el agua para detectar barcos, poniendo un oído en su extremo.

En el siglo XIX se usaron campanas subacuáticas como complemento a los faros para avisar del peligro a los marineros.

El uso de sonido para la «ecolocalización» submarina parece haber sido impulsado por el desastre del Titanic en 1912. La primera patente del mundo sobre un dispositivo de este tipo fue concedida por la Oficina Británica de Patentes al meteorólogo inglés Lewis Richardson un mes después del hundimiento del Titanic, y el físico alemán Alexander Behm obtuvo otra por un resonador en 1913. El canadiense Reginald Fessenden construyó un sistema experimental en 1914 que podía detectar un iceberg a dos millas de distancia, si bien era incapaz de determinar en qué dirección se hallaba.

Durante la Primera Guerra Mundial, y debido a la necesidad de detectar submarinos, se realizaron más investigaciones sobre el uso del sonido. Los británicos emplearon pronto micrófonos subacuáticos, mientras el físico francés Paul Langevin, junto con el ingeniero eléctrico ruso emigrado Constantin Chilowski, trabajó en el desarrollo de dispositivos activos de sonido para detectar submarinos en 1915. Aunque los transductores piezoeléctricos y magnetostrictivos superaron más tarde a los electrostáticos que usaron, este trabajo influyó sobre el futuro de los diseños detectores. Si bien los transductores modernos suelen usar un material compuesto como parte activa entre la cabeza ligera y la cola pesada, se han desarrollado muchos otros diseños. Por ejemplo, se han usado películas plásticas ligeras sensibles al sonido y fibra óptica en hidrófonos (transductores acústico-eléctricos para uso acuático), mientras se han desarrollado el Terfenol-D y el PMN para los proyectores. Los materiales compuestos piezoeléctricos son fabricados por varias empresas, incluyendo Morgan Electro Ceramics.

En 1916, bajo el patrocinio del Consejo Británico de Invenciones e Investigaciones, el físico canadiense Robert Boyle se encargó del proyecto del sonar activo con Albert Beaumont Wood, construyendo un prototipo para pruebas a mediados de 1917. Este trabajo, para la División Antisubmarina, fue realizado en el más absoluto secreto, y usaba cristales de cuarzo piezoeléctricos para producir el primero aparato de detección subacuática de sonido activo factible del mundo.

Para 1918 tanto Estados Unidos como el Reino Unido habían construido sistemas activos, si bien los británicos estaban considerablemente más avanzados. Probaron su ASDIC (Allied Submarine Detection Investigation Committee, así eran conocidos los equipos de detección activa) en el HMS Antrim en 1920 y empezaron la producción de unidades en 1922. La 6ª Flotilla Destructoras tuvo buques equipados con ASDIC en 1923. Un buque-escuela antisubmarino, el HMS Osprey, y una flotilla de entrenamiento compuesta por cuatro buques se estableció en Isla de Pórtland en 1924. El Sonar QB estadounidense no llegó hasta 1931.

Con el inicio de la Segunda Guerra Mundial, la Marina Real Británica tenía cinco equipos para diferentes clases de buques de superficie y otros para submarinos, incorporados en un sistema de ataque antisubmarino completo. La efectividad de los primeros ASDIC estaba limitada por el uso de las cargas de profundidad como arma antisubmarina. Esto exigía que el buque atacante pasase sobre el contacto sumergido antes de lanzar las cargas, lo que hacía perder el contacto sonar en los momentos previos al ataque. El ataque exigía, pues, disparar a ciegas, periodo en el que el comandante del submarino podía adoptar con éxito medidas evasivas. Esta situación se remediaba usando varios buques cooperando juntos y con la adopción de «armas de lanzamiento delantero», como el Hedgehog y más tarde el Squid, que lanzaban las cargas a un blanco situado delante del atacante y por tanto aún en contacto ASDIC. Los desarrollos durante la guerra desembocaron en unos equipos ASDIC que usaban diferentes formas de onda, permitiendo que los puntos ciegos fueran cubiertos continuamente. Más tarde se emplearon torpedos acústicos.

Al inicio de la Segunda Guerra Mundial la tecnología británica de sonar fue transferida a los Estados Unidos. La investigación sobre el sonar y el sonido submarino se amplió enormemente, particularmente en este país. Se desarrollaron muchos nuevos tipos de sonar militar, entre ellos las sonoboyas, el sonar sumergible y el de detección de minas. Este trabajo formó la base de los desarrollos de posguerra destinados a contrarrestar los submarinos nucleares. El sonar siguió desarrollándose en muchos países para usos tanto militares como civiles. En los últimos años la mayoría de los desarrollos militares han estado centrados en los sistemas activos de baja frecuencia.

En la Segunda Guerra Mundial Estados Unidos usó el término SONAR para sus sistemas, acrónimo acuñado como equivalente de RADAR. En 1948, con la formación de la OTAN, la estandarización de señales llevó al abandono del término ASDIC en favor de SONAR. También puede utilizarse como RADAR.

El radar (término derivado del acrónimo inglés RAdio Detection And Ranging, “detección y medición de distancias por radio”) es un sistema que usa ondas electromagnéticas para medir distancias, altitudes, direcciones y velocidades de objetos estáticos o móviles como aeronaves, barcos, vehículos motorizados, formaciones meteorológicas y el propio terreno. Su funcionamiento se basa en emitir un impulso de radio, que se refleja en el objetivo y se recibe típicamente en la misma posición del emisor. A partir de este "eco" se puede extraer gran cantidad de información. El uso de ondas electromagnéticas permite detectar objetos más allá del rango de otro tipo de emisiones (luz visible, sonido, etc.)

Entre sus ámbitos de aplicación se incluyen la meteorología, el control del tráfico aéreo y terrestre y gran variedad de usos militares.

A partir de ahí se ha ido investigando sobre las diferentes formas de obtener información en los diferentes ámbitos, lo que ha llevado a que los sensores evolucionen hasta el momento con las redes de sensores inalámbricas, las cuales son capaces de obtener información periódica en las diferentes facetas sin tener que estar una persona presente en el medio físico y exentas de mantenimiento, ya que se crean redes de sensores que constan de una cantidad importante de nodos autónomos capaces de autoconfigurarse en el caso de que alguno de ellos deje de funcionar y elegir un camino alternativo a la hora de propagar la información hasta el sumidero para su posterior envío por Internet hasta los equipos de monitorización.

2.2 Redes Inalámbricas de Sensores (Ad-hoc)

La expresión ad-hoc hace referencia a una red en la que no hay un nodo central, sino que todos los dispositivos están en igualdad de condiciones. Ad-hoc es el modo más sencillo para crear una red, un tipo de red formada por un grupo de nodos móviles que forman una red temporal sin la ayuda de ninguna infraestructura externa. Para que esto se pueda llevar a la práctica es necesario que los nodos se puedan ayudar mutuamente para conseguir un objetivo común: que cualquier paquete llegue a su destino aunque el destinatario no sea accesible directamente desde el origen. El protocolo de encaminamiento es el responsable de descubrir las rutas entre los nodos para hacer posible la comunicación.

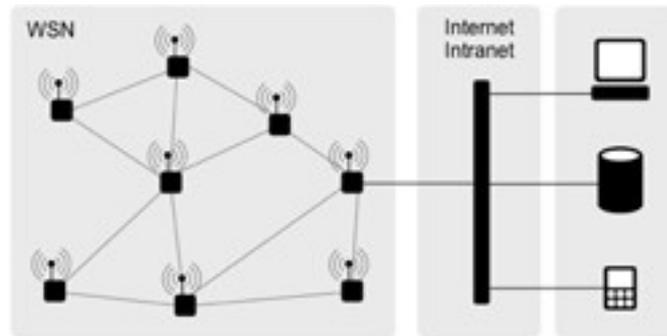


Figura 2.2: Estructura de una red ad-hoc

Las redes de sensores son un concepto relativamente nuevo en adquisición y tratamiento de datos con múltiples aplicaciones en distintos campos, tales como entornos industriales, domótica, entornos militares, detección ambiental, etc.

Esta clase de redes se caracterizan por su facilidad de despliegue y por ser autoconfigurables, pudiendo convertirse en todo momento en emisor, receptor, ofrecer servicios de encaminamiento entre nodos sin visión directa, así como registrar datos referentes a los sensores locales de cada nodo. Otra de sus características es su gestión eficiente de la energía, que les permite obtener una alta tasa de autonomía que las hacen plenamente operativas.

Las redes de sensores dependen fundamentalmente de las técnicas ad-hoc en las redes wireless. Aunque muchos protocolos y algoritmos han sido diseñados para las redes tradicionales wireless ad-hoc, estas no son convenientes para las características únicas que tienen las redes de sensores.

Para resaltar este punto se muestran diferencias entre redes de sensores y redes ad-hoc:

- El número de nodos sensores en una red de sensores puede estar varios órdenes de magnitud por encima de los nodos en las redes ad-hoc.
- Los nodos sensores pueden ser densamente desplegados.
- Los nodos sensores son más propensos a los fallos.
- La topología de la red de sensores cambia frecuentemente.
- Los nodos sensores utilizan principalmente la comunicación por difusión mientras que la mayoría de las redes ad-hoc están basadas en la comunicación punto a punto.
- Los nodos sensores están limitados en cuanto a potencia, capacidad computacional y memoria.

Desde que un gran número de nodos sensores pueden desplegarse densamente, los nodos vecinos pueden estar muy cerca unos de otros. De ahí, que la comunicación multiton en redes de sensores exige un menor consumo de energía que las tradicionales comunicaciones. Además, las transmisiones a bajos niveles de energía pueden mantenerse así, lo cual es deseable en operaciones secretas.

Las redes de sensores ad-hoc consideradas altamente distribuidas, están constituidas por nodos pequeños (inalámbricos) y de peso ligero que se despliegan en un área específica. Son redes sin infraestructura, flexibles en las cuales todas las estaciones ofrecen servicios de encaminamiento para permitir la comunicación de estaciones que no tienen conexión

inalámbrica directa. La principal característica de las redes móviles ad-hoc es que todos los dispositivos que forman parte de la red, además de funcionar como terminales finales, realizan también funciones de retransmisión de paquetes típicamente asociadas a routers. Su función es proveer una infraestructura de comunicación inalámbrica que puede servir para poder monitorear algo en específico (temperatura, presión, movimiento de objetos, etc.).

La construcción de estos nodos sensores con los cuales se conforma la red ha sido posible debido a los avances en el área de sistemas micro electromecánicos (MEMS). Los MEMS son dispositivos miniatura fabricados con capacidad de sensado, comunicación y procesamiento.

Cada uno de estos nodos, se divide en tres subsistemas:

- El subsistema del sensor: sensa (mide un parámetro) el medio ambiente.
- El subsistema de procesado: lleva a cabo el cómputo de la información recabada por el sensado.
- El subsistema de comunicación: es el responsable del intercambio de mensajes con los nodos sensores vecinos.

Por otra parte, mientras que un nodo individual tiene una región de sensado, una potencia de procesamiento y una cantidad de energía limitada, teniendo un gran número sensores se da un aumento en la robustez, confiabilidad y precisión en el área de cobertura de dicha red. Esto se da, ya que al tener más nodos sensores que cooperan y colaboran entre sí en una región determinada, la adquisición de la información es múltiple. Brindándonos así, más seguridad en el sensado y reafirma el buen desempeño de la red.

Los retos que involucra una Red Inalámbrica de Sensores son el tipo de arquitectura, la disseminación y recolección de la información, las técnicas adoptadas por los nodos sensores para localización y aumentar la eficiencia en el consumo de energía. Este último es factor primario que limita la vida útil de la red.

La actividad de medir parámetros o sensar, se da de manera periódica o esporádica. Un ejemplo de tipo periódico es el sensar factores ambientales para medir la temperatura, humedad o la radiación nuclear. El detectar la entrada de un intruso, el medir el estrés crítico de estructuras o maquinaria, son claros ejemplos de actividades esporádicas de sensado.

Áreas que hacen de las redes de sensores una categoría distinta dentro de las redes inalámbricas ad-hoc son:

φ Movilidad de los nodos:

La movilidad no es algo que se deba cumplir. El despliegue de nodos para monitorear las propiedades del suelo no lo requiere.

φ Tamaño de la red:

El número de sensores en la red puede ser mucho más grande que una típica red inalámbrica ad-hoc.

φ Densidad de la red:

Esto varía de acuerdo al tipo de aplicación. En el ámbito militar, se requiere que la red siempre esté disponible y con alto grado de seguridad y redundancia de información.

φ Limitación de Energía:

En el caso de las redes de sensores, se espera que funcionen en ambientes agresivos en cuanto a condiciones ambientales, con el mínimo o nula supervisión humana posible.

Emplear este tipo de redes, donde la única fuente de alimentación para el nodo sensor es la batería, nos limita la vida útil de la red, exigiendo de esta manera un conjunto de protocolos de red muy eficientes a nivel capa de red, capa de enlace de datos y hasta física para brindar un control óptimo de energía.

Las fuentes de alimentación en redes de sensores se pueden clasificar de la siguiente manera:

- o Recargables
- o No recargables
- o Regenerativas (capacidad de regenerar energía a partir del parámetro físico de estudio).

φ Fusión de los datos e información:

Las limitaciones del ancho de banda y la energía demandan el aumento de bits y de información en los nodos intermedios. Para la fusión de los datos, se necesita el aumento de múltiples paquetes dentro de uno solo antes de su transmisión. Lo que se busca es reducir el ancho de banda a utilizar mediante encabezados redundantes en los paquetes y minimizando el retardo al acceder al medio para transmitir los múltiples paquetes. La fusión de la información busca retransmitir la salida del procesamiento del sensado a un nodo de monitoreo.

φ Distribución del Tráfico:

El patrón de tráfico varía en base al tipo de aplicación de la red. El sensado de un factor ambiental, genera de manera periódica pequeños paquetes con datos que indica el estado del parámetro de estudio a una estación central de monitoreo. Esto demanda un bajo ancho de banda.

Sin embargo, cuando se trata de detectar a un intruso en el ámbito militar, se genera un tráfico de detección en eventos con limitantes en la transmisión en tiempo real. A diferencia, las redes ad-hoc, generalmente en cuanto al tráfico, utilizan digitalización y empaquetado de comunicación de voz o de datos .

φ Escalabilidad:

En algunos tipos de redes, el número de nodos puede crecer hasta llegar a varios miles. Como no existe un access point concreto, la incorporación y descarte de nodos es un proceso sencillo y transparente.

φ Seguridad:

Las redes inalámbricas son vulnerables a ataques, y las redes ad-hoc lo son especialmente. Pueden padecer tanto ataques activos como pasivos y el atacante puede emular a un nodo legítimo y capturar paquetes de datos y control, destruir tablas de encaminamiento, etc. Es por ello que se utilizan técnicas de encriptación como AES.

2.2.1 *Hardware* de un Nodo Sensor

Los nodos inalámbricos se llaman motas, del inglés ‘mote’, por su ligereza y reducido tamaño. Son dispositivos electrónicos capaces de captar información proveniente del entorno en el que se encuentran, procesarla y transmitirla inalámbricamente hacia otro destinatario.

Diseñar un mota no se reduce a miniaturizar un ordenador personal. Hay que tener en cuenta que queremos un espacio reducido, un consumo muy bajo de energía y un coste de los dispositivos reducido. Y en contraposición a esto una potencia de ejecución de programas elevadas y una transmisión de datos eficaz y con amplia longitud de emisión.

Un **nodo sensor** es un elemento computacional con capacidad de procesamiento, memoria, interfaz de comunicación y puede formar conjuntos de sensores. El Hardware básico de un nodo sensor se compone de un transceptor (transmisor/receptor), procesador, uno o más sensores, memoria y batería. Los componentes brindan la opción de comunicación (enviar/recibir información), ejecutar tareas que requieren procesamiento más allá de efectuar funciones de sensado.

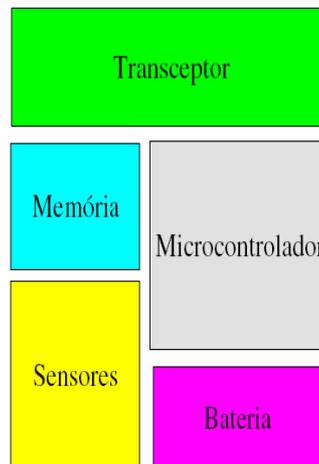


Figura 2.3: Partes de un nodo sensor

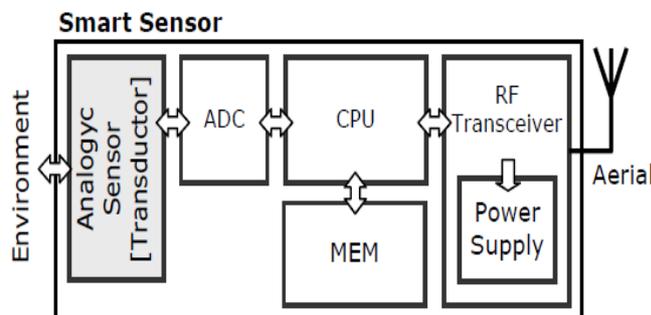


Figura 2.4: Estructura interna de un sensor inalámbrico inteligente

La capacidad de procesamiento depende del tipo de microprocesador que se emplee. Así mismo, posee una memoria interna en el microcontrolador. La comunicación se realiza mediante un transceptor (transmisor/receptor). Además, se tiene la fuente de alimentación que varía dependiendo el tipo de tecnología con la cual la batería esté fabricada. En cuanto al sensor, éste es el responsable de monitorear el parámetro de interés e informar del mismo. La figura 2.5 presenta ejemplos de hardware de sensores, tomando como referencia algunas características de la familia MOTES y su evolución. Estos *motes* o partículas, son pequeños dispositivos inalámbricos basados en tecnología MEMS, que detectan factores físicos.

Mote Type Year	WeC 1998	René 1999	René 2 2000	Dot 2000	Mica 2001	Mica2Dot 2002	Mica 2 2002	Telos 2004	
									
Microcontroller									
Type	AT90LS8535		ATmega163		ATmega128			TI MSP430	
Program memory (KB)	8		16		128			48	
RAM (KB)	0.5		1		4			10	
Active Power (mW)	15		15		15		60	0.5	
Sleep Power (W)	45		45		75		75	2	
Wakeup Time (s)	1000		36		180		180	6	
Nonvolatile storage									
Chip	24LC256			AT45DB041B			ST M24M01S		
Connection type	I ² C			SPI			I ² C		
Size (KB)	32			512			128		
Communication									
Radio	TR1000			TR1000	CC1000		CC2420		
Data rate (kbps)	10			40	38.4		250		
Modulation type	OOK			ASK	FSK		O-QPSK		
Receive Power (mW)	9			12	29		38		
Transmit Power at 0dBm (mW)	36			36	42		35		
Power Consumption									
Minimum Operation (V)	2.7		2.7		2.7			1.8	
Total Active Power (mW)	24		27		44		89		
Programming and Sensor Interface									
Expansion	none	51-pin	51-pin	none	51-pin	19-pin	51-pin	10-pin	
Communication	IEEE 1284 (programming) and RS232 (requires additional hardware)							USB	
Integrated Sensors	no	no	no	yes	no	no	no	yes	

Figura 2.5: Ejemplo de hardware de sensores

Familia Motes

Diferentes partes que comportan un nodo sensor:

PROCESADOR

Es el componente que interpreta y procesa los datos para transmitirlos a otra estación. También gestiona el almacenamiento de datos en la memoria.

Puesto que de un nodo sensor se espera una comunicación y una recogida de datos mediante sensores, debe existir una unidad de procesado, que se encargue de gestionar todas

estas operaciones.

Hay muchos tipos diferentes de productos disponibles en el mercado para ser integrados en un nodo, como microcontroladores, microprocesadores y FPGA.

-FPGA: Actualmente éstas presentan varias desventajas, la mayor de ellas es el consumo. A pesar de que en el mercado podemos encontrar FPGAs de bajo consumo, este consumo no es lo suficientemente bajo como debería ser para este tipo de nodos. Esto no significa que en un futuro cercano, éstas sean una buena opción si se consigue que reduzcan el consumo.

-Microprocesadores: Han sido sustituidos por los microcontroladores, ya que éstos integran dentro de un mismo dispositivo, un microprocesador y memoria.

-Microcontroladores: Como se ha dicho, incluyen un microprocesador y memoria, pero además tienen una interfaz para ADCs, UART, SPI, temporizadores y contadores. Hay muchos tipos de microcontroladores que van desde los 4 bits hasta 64 bits, con una variación del número de temporizadores, con diferentes consumos de energía, etc.

Actualmente los más utilizados son los siguientes procesadores de bajo consumo:

- **ARM7:** Se denomina ARM a una familia de microprocesadores RISC diseñados por la empresa Acorn Computers y desarrollados por Advanced RISC Machines Ltd., una empresa derivada de la anterior. <http://www.arm.com/>

- **Atmel AVR:** Los AVR son una familia de microcontroladores RISC de Atmel. La arquitectura de los AVR fue concebida por dos estudiantes en el Norwegian Institute of Technology, y posteriormente refinada y desarrollada en Atmel Norway, la empresa subsidiaria de Atmel, fundada por los dos arquitectos del chip.

El AVR es una CPU de arquitectura Harvard. Tiene 32 registros de 8 bits. Algunas instrucciones sólo operan en un subconjunto de estos registros.

<http://www.atmel.com/products/avr/>

- **Intel XScale:** El Intel XScale es un núcleo de microprocesador, la implementación de Intel de la quinta generación de la arquitectura ARM. La tecnología fue vendida a Marvell Technology Group en junio de 2006. Está basado en el ISA v5TE sin las instrucciones de coma flotante. El XScale usa un entero de 7 niveles y 8 niveles de memoria Superpipeline de arquitectura RISC. Es el sucesor de la línea de microprocesadores y microcontroladores Intel StrongARM, que Intel adquirió de la división de Semiconductores Digitales de DEC como efecto colateral de un pleito entre las dos compañías. <http://www.marvell.com/>

- **Intel 8051:** El Intel 8051 es un microcontrolador (μ C) desarrollado por Intel en 1980 para uso en productos embebidos. Es un microcontrolador muy popular. Los núcleos 8051 se usan en más de 100 microcontroladores de más de 20 fabricantes independientes como Atmel, Dallas Semiconductor, Philips, Winbond, entre otros. La denominación oficial de Intel para familia de μ Cs 8051 es MCS 51. Este microcontrolador está basado en una Arquitectura Harvard (es decir, existen espacios de direcciones separados para código y datos). Aunque originariamente fue diseñado para aplicaciones simples, se permite direccionar 64 KB de ROM externa y 64 KB de RAM por medio de líneas separadas chip select para programa y datos. <http://www.intel.com/design/mcs51/>

- **PIC:** Los 'PIC' son una familia de microcontroladores tipo RISC fabricados por Microchip Technology Inc. y derivados del PIC1650, originalmente desarrollado por la división de microelectrónica de General Instruments. El nombre actual no es un acrónimo. En realidad, el nombre completo es PICmicro, aunque generalmente se utiliza como Peripheral Interface Controller (Controlador de Interfaz Periférico). El PIC original se diseñó para ser usado con la nueva UCP de 16 bits CP16000. Siendo en general una buena UCP, ésta tenía

malas prestaciones de E/S, y el PIC de 8 bits se desarrolló en 1975 para mejorar el rendimiento del sistema quitando peso de E/S a la UCP. El PIC utilizaba microcódigo simple almacenado en ROM para realizar estas tareas; y aunque el término no se usaba por aquel entonces, se trata de un diseño RISC que ejecuta una instrucción cada 4 ciclos del oscilador. <http://www.microchip.com/>

• **TI MSP430:** El MSP430 es una familia de microcontroladores producidos por Texas Instruments. Construido con una CPU de 16 bits, el MSP430 está diseñado para aplicaciones empotradas de bajo costo y bajo consumo de energía. La arquitectura tiene reminiscencias del DEC PDP-11. Desafortunadamente, el MSP430 carece de una característica muy importante del PDP11, la cual era la memoria para indexar memoria. Esta característica permitía que las rutinas de interrupción se escribieran sin utilizar registros, por lo que no requería apilamientos. El MSP430 es muy útil para aplicaciones inalámbricas o para aplicaciones de bajo consumo.

<http://www.ti.com/msp430>

ALIMENTACION

Normalmente la fuente de alimentación son baterías difícilmente sustituibles o transformadores con salida adecuada para el nodo si se dispone de toma de corriente. Para las situaciones en donde no se dispone de red eléctrica y la posibilidad de sustituir las baterías es muy complicada, se están estudiando diferentes técnicas para alimentar el sensor, como puede ser mediante placas solares.

Ante la limitación de la vida útil del dispositivo hay que realizar una gestión eficiente del consumo energético.

El consumo de energía viene dado por lo que consumen los sensores, la comunicación y el procesado. La mayor cantidad de energía es consumida en la transmisión de información, siendo menor en el procesado y uso de los sensores. Por ejemplo el coste de transmisión de 1 Kb. a una distancia de 100 metros es aproximadamente el mismo que ejecutar 3 millones de instrucciones por un procesador de 100 millones de instrucciones por segundo.

Las baterías son la principal fuente de energía de estos motes, pudiendo ser recargables o no recargables.

Están clasificados según el material electroquímico usado para el electrodo como pueden ser NiCd (níquel-cadmio), NiZn (níquel -zinc), Nimh (níquel metal hidruro), y Litio-Ion.

Actualmente se están estudiando sistemas basados en energía renovables para solucionar el problema de la energía en estos nodos, basados en energía solar, termo generación, energía basada en vibraciones, etc.

Fuente de energía	Densidad de energía
Baterías (Zinc Aire)	1050-1560 mWh/cm ³
Baterías (recargable Litio)	300 mWh/cm ³ (3-4 V)
Solar (exterior)	150 mWh/cm ³ (expuesto al sol) 0.15 mWh/cm ³ (día nublado)
Solar (interior)	0.006 mWh/cm ³ (nivel escritorio oficina) 0.57 mWh/cm ³ (< 60 W lámpara de escritorio)
Vibración	0.01-0.1 mWh/cm ³
Ruido acústico	3*10 ⁻⁶ mWh/cm ² a 75 Db 9.6*10 ⁻⁴ mWh/cm ² a 100 Db
Reacción nuclear	80 mW/cm ³ , 106 mWh/cm ³

Figura 2.6: Fuentes de energía para los motes

COMUNICACION INALAMBRICA

El dispositivo de comunicación se trata de un dispositivo vía radio que permite enviar y recibir datos para comunicarse con otros dispositivos dentro de su rango de transmisión.

Los nodos usan la banda ISM que son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica. El uso de estas bandas de frecuencia está abierto a todo el mundo sin necesidad de licencia, respetando las regulaciones que limitan los niveles de potencia transmitida.

Los medios a elegir para realizar una comunicación inalámbrica son varios: radio frecuencia, comunicación óptica mediante láser e infrarrojos. La comunicación por láser es la que menos energía consume pero requiere de una comunicación visual entre emisor y receptor, y además también depende de las condiciones atmosféricas. Los infrarrojos como el láser, no necesitan antena, aunque es bastante limitado en su capacidad de transmisión. La radio frecuencia, RF, es la más adecuada para usar en aplicaciones inalámbricas. Las WSN usan las frecuencias de comunicación que andan entre 433 MHz y 2.4 Ghz.

Las funcionalidades de emisión y recepción se combinan en un solo aparato que es llamado transceptor. Los estados de operación son emitir, recibir, dormir e inactividad. En los actuales modelos de transceptor, el modo inactivo consume casi igual que el modo recepción. Por lo que es mejor tener completamente apagado las comunicaciones radio, en el modo inactivo, cuando no se esta emitiendo ni recibiendo.

También es significativa la cantidad de energía consumida cuando cambia de modo durmiente a transmisión de datos.

Los sistemas más populares dentro de los sistemas de comunicación de radio para nodos de redes inalámbricos son:

- Chipcon CC1000 <http://www.chipcon.com/>
- Chipcon CC1020
- Chipcon CC2420
- Xemics XE1205 <http://www.semtech.com/>
- 802.15.4 Chipsets and SoC <http://www.jennic.com/>

Una comparativa de las principales características de estos dispositivos es:

	CC1000	CC1021	CC2420	TR1000	XE1205
Manufacturer	Chipcon	Chipcon	Chipcon	RFM	Semtech
Operating Frequency [MHz]	300 - 1000	402 - 470 / 804 - 940	2400	916	433 / 868 / 915
Bit Rate [kbps]	76.8	153.6	250	115.2	1.2 - 152.3
Power Supply Voltage [V]	2.1 - 3.6 (typ. 3.0)	2.3 - 3.6 (typ. 3.0)	2.1 - 3.6 (int. 1.8)	2.2 - 3.7 (typ. 3.0)	2.4 - 3.6

Figura 2.7: Características de dispositivos inalámbricos I

	CC1000	CC1021	CC2420	TR1000	XE1205
Sleep Mode [uA]	0.2 - 1 (osc. core off)	1.8 (core off)	1	0.7	0.2
Standby Mode [uA]			426 (Voltage and osc. running)		850
RX [mA]	9.3 (433MHz) / 11.8 (868MHz)	19.9	19.7	3.8 (115.2kbps)	14
TX Min [mA]	8.6 (-20dBm)	14.5 (-20dBm)	8.5 (-25dBm)		33 (-5dBm)
TX Max [mA]	25.4 (+5dBm)	25.1 (-5dBm)	17.4 (0dBm)	12 (+1.5dBm)	62 (+15dBm)

Figura 2.8: Características de dispositivos inalámbricos II

MEMORIA

Desde un punto de gasto de energía, las clases más relevantes de memoria son la memoria integrada en el chip de un microcontrolador y la memoria flash, la memoria RAM fuera del chip es raramente usada. Las memorias flash son usadas gracias a su bajo coste y su gran capacidad de almacenamiento.

La memoria flash es una forma desarrollada de la memoria EEPROM que permite que múltiples posiciones de memoria sean escritas o borradas en una misma operación de programación mediante impulsos eléctricos, frente a las anteriores que sólo permite escribir o borrar una única celda cada vez. Por ello, flash permite funcionar a velocidades muy superiores cuando los sistemas emplean lectura y escritura en diferentes puntos de esta memoria al mismo tiempo.

Las memorias flash son de carácter no volátil, esto es, la información que almacena no se pierde en cuanto se desconecta de la corriente, una característica muy valorada para la multitud de usos en los que se emplea este tipo de memoria.

Los requerimientos de memoria dependen mucho de la capacidad que necesite nuestra aplicación. Hay dos categorías de memorias según el propósito del almacenamiento:

- Memoria usada para almacenar los datos recogidos por la aplicación.
- Memoria usada para almacenar el programa del dispositivo.

SENSORES

Los sensores son dispositivos hardware que producen una respuesta medible ante un cambio en un estado físico, como puede ser temperatura o presión. Los sensores detectan o miden cambios físicos en el área que están monitorizando. La señal analógica continua detectada es digitalizada por un convertidor analógico-digital y enviada a un controlador para ser procesada.

Las características y requerimientos que un sensor debe tener son un pequeño tamaño, un consumo bajo de energía, operar en densidades volumétricas altas, ser autónomo y funcionar desatendidamente y tener capacidad para adaptarse al ambiente.

Los sensores pueden estar clasificados en tres categorías:

- **Sensores pasivos omnidireccionales:** Los sensores pasivos captan los datos sin necesidad de manipular el entorno. Son autoalimentados y solo usan la energía para amplificar la señal analógica captada. No hay ninguna noción de ‘dirección’ involucrada en estas mediciones.

- **Sensores pasivos unidireccionales:** Son sensores pasivos que tienen bien definida la dirección desde donde deben captar la información. Un ejemplo típico es una cámara.

- **Sensores activos:** Este tipo de sensores sondean el ambiente, por ejemplo un radar o un sonar o algún tipo de sensor sísmico que generan ondas expansivas a través de pequeñas explosiones.

En suma, cada nodo sensor puede ser equipado con dispositivos sensores tanto como acústicos, sísmicos, infrarrojos, video cámaras, mecánicos, de calor, temperatura, radiación, entre otros. La figura 2.9 muestra algunos tipos de sensores que pueden presentarse en un nodo sensor tales como un micrófono (figura 2.9 (a)) que puede ser usado para captar señales del medio ambiente, un fotómetro (figura 2.9 (b)) que es capaz de medir la cantidad de fotones recibidos, un diodo detector de luz (figura 2.9 (c)) , acelerómetro (figura 2.9 (d)) que es un sensor capaz de medir la aceleración de un objeto, un sensor de humedad (figura 2.9 (e)), un sensor de radiación (figura 2.9 (f)), un sensor de luz ultravioleta (figura 2.9 (g)), un sensor de fuerza motriz (figura 2.9(i)).



Figura 2.9: Diferentes tipos de sensores

La tendencia es producir sensores a gran escala, a precios bajos, con mejor capacidad de cómputo y de tamaño reducido como se observa en la figura. 2.10 (dimensiones).

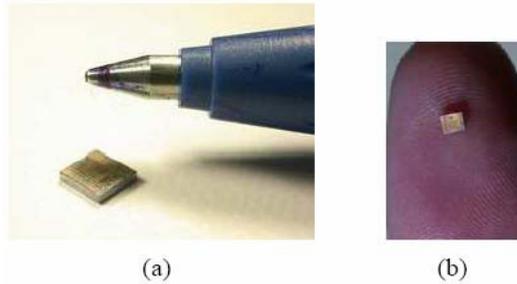


Figura 2.10: Tamaño de los sensores

2.2.2 Software de un Nodo Sensor

Numerosos y variados son los sistemas operativos existentes hoy para sistemas embebidos, mas no todos satisfacen las restricciones que imponen las Redes de Sensores Inalámbricas (RSI), motivo por el cual muchos de ellos quedan descartados inmediatamente.

De esta forma nuestro extenso espacio de decisión se reduce a unos pocos elementos. A continuación se presentarán tres de los principales Sistemas Operativos para redes de sensores, que cumplen con los requisitos.

Los tres sistemas presentan capas de abstracciones para independizar al programador de los niveles inferiores (hardware). Mediante *Drivers* se comunican aplicación y hardware, al igual que los sistemas operativos para arquitecturas x86. El estudio se basará en cómo manejan las tareas y eventos que ocurren en cada nodo.

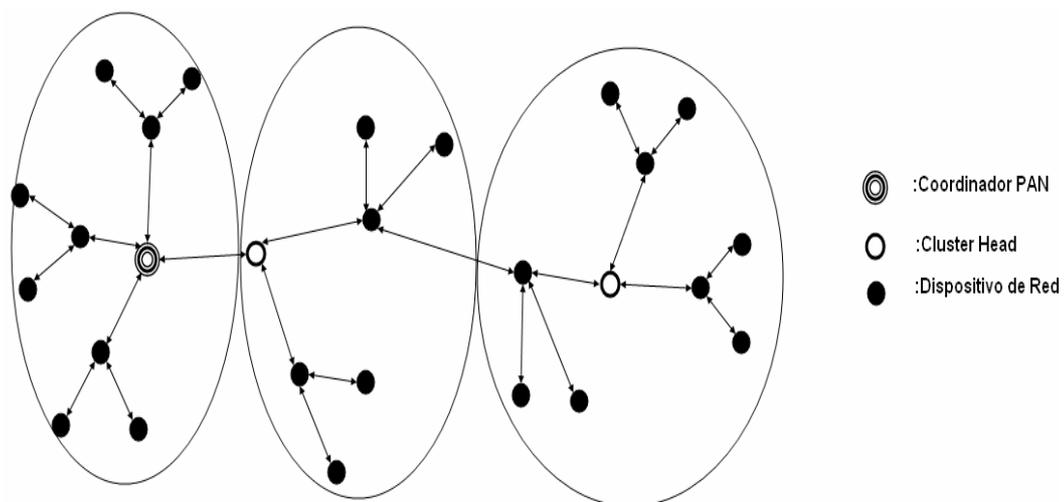


Figura 2.11: Diagrama de topología cluster-tree de una red ad-hoc

2.2.2.1 PalOS

Es un sistema operativo desarrollado por la UCLA (Universidad de California).

El modelo de ejecución se muestra en la Figura 2.12 donde se observa que cada tarea mantiene una propia cola de eventos. La tarea puede interactuar con una entrada o salida física. En la fase de inicialización del programa, cada tarea registra una tarea de eventos en la programación del sistema. Si la tarea 1 desea hablar con la tarea 2, postea un evento en la cola de eventos de la tarea 2, usando una funcionalidad del *Scheduler* (organizador o programador) del sistema, para que luego la tarea 2 capture ese evento al preguntar al *Scheduler* si tiene algún evento para él.

Para un correcto funcionamiento de esta estructura de software, es necesario que un “timer” maneje la periodicidad con que una tarea registra eventos. La forma en que se implementa es a través de una tarea “timer”. Esta posee tres colas:

1. “Cola Nexa”, encargada de interactuar con las demás tareas (recibe el envío de otras tareas).
2. “Cola Delta”, en la cual se ordenan los distintos eventos dependiendo del tiempo de expiración
3. “Eventos Expirados”, donde se van colocando para su posterior ejecución.

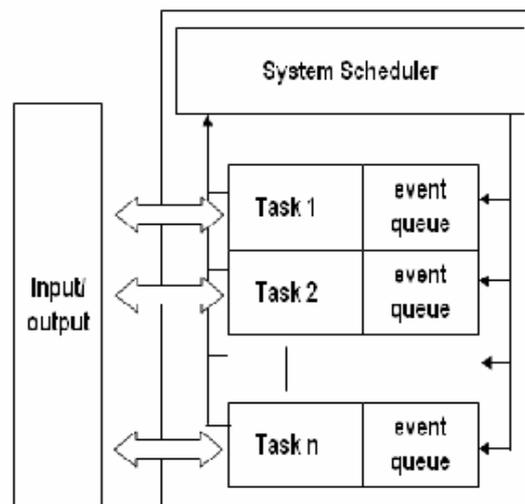


Figura 2.12: Modelo de ejecución

2.2.2.2 SOS

SOS fue desarrollado en la Universidad de UCLA específicamente en el “Networked and Embedded Systems Lab (NESL)”. Implementa un sistema de mensajería que permite múltiples hebras entre la base del sistema operativo y las aplicaciones, las cuales pasan a ser módulos que pueden ser cargadas o descargadas en tiempo de ejecución sin interrumpir la base del sistema operativo. Además procura remediar algunos de las limitaciones propias de la naturaleza estática de muchos de los sistemas precursores a éste (por ejemplo TinyOS).

El principal objetivo de SOS es la reconfigurabilidad. Ésta se define como la habilidad para modificar el software de nodos individuales de una red de sensores, una vez que estos

han sido desplegados físicamente e inicializado su funcionamiento. En el caso de encontrar un problema, en caso de no contar con esta solución, habría sido necesario recolectar todos los nodos para poder modificar su software.

La capacidad de dinámicamente de agregar o remover módulos, permite la construcción de software mucho más tolerante a fallos. Esto presenta dos grandes ventajas: uno es el hecho de poder realizar actualizaciones de forma fácil, el otro es la capacidad de anular el funcionamiento de algún módulo defectuoso, de algún nodo que pertenece a la red.

Además de las técnicas tradicionales usadas en el diseño de sistemas embebidos, las características del kernel de SOS son:

- Módulos cargados dinámicamente.
- Programación flexible de prioridades.
- Subsistema para manejo de memoria dinámica.

Las capas de abstracción de hardware y drivers son de la misma forma que para el sistema PalOS.

A continuación se muestra un esquema de la arquitectura de SOS:

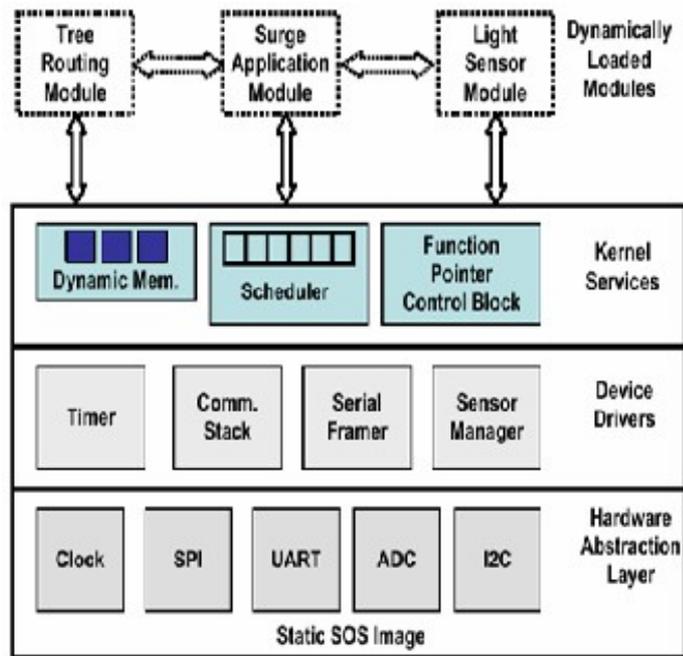


Figura 2.13: Capas funcionales de SOS

2.2.2.3 TinyOS

TinyOS, fue desarrollado por la Universidad de Berkeley (California). TinyOS puede ser visto como un conjunto de programas avanzados, el cual cuenta con un amplio uso por parte de comunidades de desarrollo, dada sus características de ser un proyecto de código abierto (Open Source). Este “conjunto de programas” contiene numerosos algoritmos, que nos permitirán generar enrutamientos, así como también aplicaciones pre-construidas para sensores.

Está escrito en base a NesC, un meta-lenguaje que se deriva de C, diseñado para responder a las necesidades que existen en los sistemas embebidos. El método de diseño es orientado a componentes. Cada componente usa eventos y comandos que rápidamente permitan la transición de un estado a otro. Además existen tareas, que solicitan el contexto de ejecución de la CPU para realizar cómputos o procesamientos duraderos. Estas tareas se ejecutan completamente con respecto a otras tareas, es decir, las tareas no pueden dividirse para comenzar con otra y luego retomarlas, más si pueden ser interrumpidas periódicamente por acontecimientos de una prioridad más alta (eventos).

Actualmente se utiliza una cola FIFO (primero en entrar, primero en salir) para el scheduler, no obstante un mecanismo alternativo podría ser agregado fácilmente. En la Figura 2.14 se muestra el funcionamiento del kernel.

Esta basado en un modelo de programación por componentes, lo cual propaga las abstracciones del hardware en el software. Tal como el hardware responde a cambios de estado en sus pines de entrada/salida, nuestras componentes responden a eventos y a los comandos en las interfaces de entrada/salida.

En resumen TinyOS consiste en un pequeño scheduler y un gráfico de componentes. Esto se puede observar en la Figura 2.15, donde se muestra como se compone una componente, destacando cuatro elementos relacionados, y detallados a continuación:

1. Manejador de comandos.
2. Manejador de eventos
3. Un frame de tamaño fijo y estáticamente asignado, en el cual se representa el estado interno de la componente. Un frame es un bloque que proporciona el contexto en el cual se ejecuta el programa y se almacenan variables.
4. Un bloque con tareas simples.

Su buen desempeño y su desarrollo abierto, han afectado positivamente en el mejoramiento del sistema en sí, e influido en la creación de herramientas que facilitan el diseño y trabajo, tales como simuladores, administradores de bases de datos, máquinas virtuales que permiten reprogramación en línea, etc.

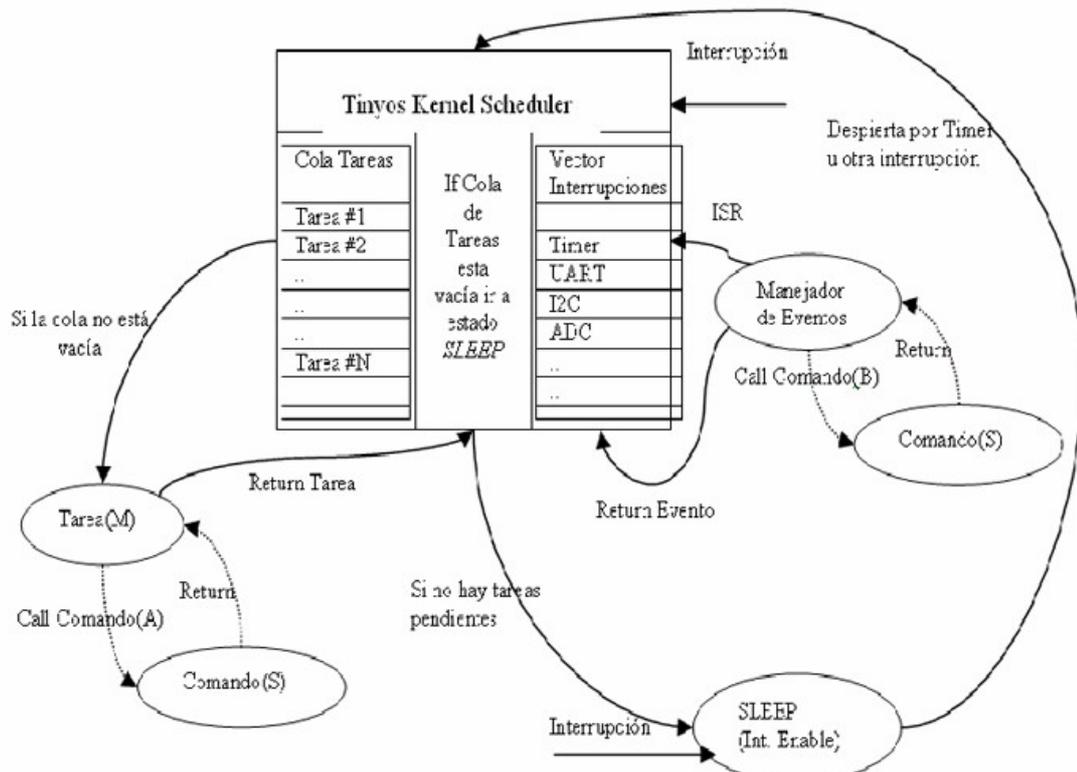


Figura 2.14: Planificador Kernel TinyOS

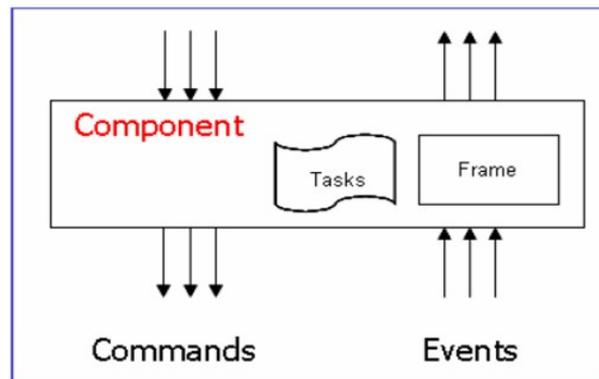


Figura 2.15: Modelo de componentes de TinyOS y interacción de componentes

Además destaca el hecho de contar con una cantidad numerosa de aplicaciones preconstruidas, las que implementan procesamientos de datos y algoritmos de enrutamiento.

	TinyOS	PalOS	SOS
Lenguaje	Programado en nesC, meta-lenguaje especialmente diseñado para el funcionamiento de las redes de sensores inalámbricas	Escrito en ansi C	Escrito en ansi C
Flexibilidad y Dinamismo.	Si bien no incorpora ni comunicación entre tareas, ni manejo dinámico de componentes en el sistema nativo, existen aplicaciones que permiten su incorporación, sin disminuir el desempeño.	Permite comunicación entre procesos. A través de las colas de eventos	Permite manejo dinámico de memoria y modificaciones “al vuelo”
Madurez	Versiones estables y en constante desarrollo	Versión estable pero bajo desarrollo de aplicaciones	Aún se encuentra en proceso de estandarización.
Plataformas	AVR , MSP430 y Microchip	AVR y ARM	AVR y ARM
SopORTE	Mucha Documentación y grupos de apoyo.	Tutoriales	Tutorial Básico

Figura 2.16: Principales variables a considerar

2.2.2.4 LINUX

Linux es un sistema operativo tipo Unix que se distribuye bajo la Licencia Pública General de GNU (GNU GPL), es decir que es software libre. Su nombre proviene del kernel

de Linux, desarrollado en 1991 por Linus Torvalds. Hablar de Linux es sólo referirse al Kernel, el núcleo del sistema. El núcleo sólo es una interfaz que permite comunicar el hardware con los programas. Por lo que el Kernel solo no forma el sistema operativo.

Un sistema GNU/Linux empotrado simplemente hace referencia a un sistema empotrado basado en el kernel de Linux. Es importante destacar que no existe un kernel específico para sistemas empotrados, es decir, no necesitamos crear un kernel especial para sistemas empotrados. A menudo se utilizan las versiones oficiales del kernel de Linux para construir un sistema. Por supuesto, es necesario configurar el mismo para dar soporte especial al hardware de un determinado equipo. Fundamentalmente, un kernel utilizado en un sistema empotrado difiere de un kernel usado en una computadora de escritorio o servidor en la configuración del mismo al momento de compilarlo.

La arquitectura de un sistema GNU/Linux está formado por un conjunto de componentes, y el kernel Linux es sólo una parte de este conjunto.

Inmediatamente sobre el hardware se sitúa el kernel. El kernel es el componente central del sistema operativo. Sus funciones son principalmente administrar el hardware de manera coherente y justa mientras se le otorga un nivel de abstracción familiar, a través de las APIs, a las aplicaciones de nivel de usuario.

Entre otras tareas relevantes de un sistema operativo, el kernel Linux maneja dispositivos, administra los accesos de E/S, controla los procesos y administra el uso compartido de memoria.

Dentro del kernel, la interfaz de bajo nivel es específica para cada configuración de hardware, sobre la cual, el kernel ejecuta y provee control directo de los recursos hardware. Típicamente, los servicios de bajo nivel manejan operaciones específicas de la CPU, operaciones de memoria específicas a la arquitectura, y provee interfaces básicas para dispositivos.

La capa de alto nivel provee abstracciones comunes a todos los sistemas Unix, incluyendo procesos, archivos, sockets y señales. Este nivel de abstracción se mantiene constante aunque difiera el hardware.

Entre estos dos niveles de abstracción, el kernel necesita lo que se denomina componentes de interpretación para comprender e interactuar con datos estructurados provenientes de, o hacia ciertos dispositivos.

Los diferentes tipos de sistemas de archivos y los protocolos de red son ejemplos de fuentes de datos estructurados. El kernel necesita interpretarlos e interactuar a fin de proveer acceso a los datos provenientes desde estas fuentes o hacia las mismas.

2.2.2.5 .NET Micro Framework

La .NET Micro Framework fue creada desde el inicio como una solución .NET para dispositivos integrados pequeños de sensores industriales e instrumentación para sistemas empotrados. Además de estar totalmente integrada con Visual Studio, el kit de desarrollo de software .NET Micro Framework (SDK) viene equipado con un emulador extensible para simular capacidades de hardware. La estructura permite a los desarrolladores de dispositivos conectar diversas soluciones de hardware para prácticamente cualquier dispositivo periférico mediante conexiones de comunicación estándares de la industria y unidades gestionadas personalmente.

La .NET Micro Framework dispone de ofertas integradas de Microsoft en un nuevo mercado de dispositivos que se basan en procesadores de 32 bits de bajo coste y están constreñidos en términos de memoria, potencia de la batería y otros recursos. Ofreciendo paradigmas de programación potentes y modernos a este terreno, .NET Micro Framework

pretende acelerar la innovación de dispositivos pequeños y conectados.

- Requiere sólo unos pocos cientos de kilobytes de RAM, y tan poco como 512 K de memoria flash.
- Soporta procesadores con y sin MMU.
- Dispone de una interface de control de energía que permite que la aplicación maximice la vida de la batería.

Hasta ahora la gente de Microsoft a publicado el SDK del Microsoft .NET Micro Framework 2.5 el cual nos permitirá desarrollar aplicaciones para pequeños dispositivos utilizando para tal motivo, Visual Studio, C#. Esta parte de Visual Studio es gratis y puede descargarse de la página Web de Microsoft, su descarga es de apenas 9 Mb y en inglés por ahora para Visual Studio 2005 con SP1. Microsoft .NET Micro Framework es un pequeño subconjunto reducido de clases, en donde podemos desarrollar soluciones en C# para pequeños dispositivos, para trabajar con este pequeño Framework necesitamos disponer de Microsoft Visual Studio 2005 Standar o superior, y un sistema operativo Windows XP, Windows Vista o Windows Server 2003. Dispone de un conjunto de librerías .NET completamente integradas enfocadas al uso en sistemas empotrados.

Varias empresas están apostando por esta tecnología, Digi International Inc dio a conocer sus planes para un lanzamiento previo del kit de desarrollo Digi Connect ME para Microsoft .NET Micro Framework. El Digi Connect ME incluye soporte para redes Ethernet, un puerto en serie y señales de propósitos generales entrada/salida (GPIO). Es la primera solución disponible para .NET Micro Framework para dar apoyo a las redes Ethernet. EmbeddedFusion, que entrega soluciones centrales de hardware y software integrado para desarrolladores de sistemas integrados, anunció el Meridian CPU, que es un módulo central CPU que incorpora procesador Freescale i.MXS, RAM, Flash y .NET Micro Framework. Para asistir a los desarrolladores en el aprendizaje de cómo se aplica .NET Micro Framework en varios escenarios integrados, EmbeddedFusion también creó la plataforma de desarrollo Tahoe, que permite la experimentación y exploración de .NET Micro Framework justo fuera de la caja.

Freescale también introdujo un kit de desarrollo para .NET Micro Framework que permite a los clientes entregar soluciones diferenciadas en el mercado con rendimiento ARM9 a muy baja potencia.

Además, Rhode Consulting, un especialista en tecnologías Microsoft Windows Embedded, anunció la disponibilidad del kit de evaluación de FlexiDis con .NET Micro Framework instalado. La plataforma FlexiDis utiliza los procesadores centrales Atmel ARM7 y ARM9 con velocidad de hasta 180 MHz. La combinación de esas velocidades, hasta 16 MB de memoria flash y SDRAM, y una pantalla QVGA de 2,2 hace de FlexiDis un componente de elección para varios tipos de aplicaciones industriales en las que se requieren HMI integrado o soluciones de visualización.

2.2.2.6 eCos

eCos (embedded Configurable operating system) es un sistema operativo de código abierto, gratuito y de operación en tiempo real desarrollado para sistemas empotrados y para aplicaciones que necesiten un procesador con múltiples sesiones. Puede ser personalizado para cumplir los requisitos que la aplicación precise, con cientos de opciones, pudiendo llegar a la mejor combinación entre el rendimiento en tiempo real y el hardware necesario.

Este sistema es programable bajo lenguaje C y tiene capas y APIs compatibles para POSIX y μ ITRON.

eCos fue diseñado para aparatos con un tamaño de memoria sobre cientos de kilobytes o con requerimientos en tiempo real. Puede ser usado en hardware con muy poca RAM

soportando Linux empotrado a partir de un mínimo de 2 MB de RAM, sin incluir las necesidades de la aplicación y del servicio.

eCos funciona correctamente en una amplia variedad de plataformas hardware como pueden ser, ARM, CalmRISC, FR-V, Hitachi H8, IA-32, Motorola 68000, Matsushita AM3x, MIPS, NEC V8xx, Nios II, PowerPC, SPARC, and SuperH. Incluido con la distribución de eCos disponemos de RedBoot, una aplicación de código abierto que usa la capa de abstracción de hardware de eCos que provee soporte de arranque para sistemas empotrados.

eCos fue inicialmente desarrollado por Cygnus Solutions, aunque más tarde fue comprado por Red Hat. A principio de 2002 cesó el desarrollo de eCos y colocó al personal que estaba trabajando en el proyecto formando su propia compañía, eCosCentric, para continuar con su desarrollo y dar soporte comercial para eCos. En enero de 2004, a partir de una solicitud de los desarrolladores de eCos, Red Hat aceptó transferir los derechos de eCos a la Fundación de Software Libre. Esta transferencia fue finalmente ejecutada en octubre de 2005.

eCosPro está formado por una distribución de eCos y RedBoot creada por eCosCentric y está orientado a desarrolladores que quieran integrar eCos y RedBoot dentro de productos comerciales. Está definido como estable, completamente testado, certificado y con soporte, sin embargo, algunas de sus características no han sido liberadas como software libre.

2.2.2.7 uC/OS

MicroC/OS-II (comúnmente llamado μ C/OS-II o uC/OS-II), es un sistema operativo multitarea, en tiempo real, basado en prioridad preventiva, de bajo coste donde el kernel está escrito principalmente en el lenguaje de programación C. Es principalmente entendido para uso en sistemas empotrados.

La designación II es debido a que es la segunda generación de un kernel que originalmente fue publicado en 1992 en la segunda parte de un artículo en la revista Embedded Systems Programming bajo el título μ C/OS The Real-Time Kernel y escrito por Jean J. Labrosse (ISBN 0-87930-444-8). El autor intentó describir como funciona un sistema operativo portable por dentro y las razones por las que fue desarrollado. Pero rápidamente todo esto tomó un rumbo comercial.

uC/OS-II es soportado por Micrium Inc y se obtiene bajo licencia del producto, aunque el uso de este sistema operativo es gratis para uso educacional o no comercial. Adicionalmente Micrium distribuye otros productos de software como uC/OS-View, uC/CAN, uC/TCP-IP, uC/FS, uC/GUI, uC/MOD-BUS, uC/LCD, uC/USB (Mass Storage Device and Bulk) y un largo grupo de aplicaciones para uC/TCP-IP como software cliente para DHCP, POP3, SMTP, FTP, TFTP, DNS, SMTP, y TTCP. El software en su modalidad de servido incluye HTTP, FTP y TFTP. PPP es también disponible. Está disponible para la mayor cantidad de procesadores y placas que existen en el mercado y es adecuado para el uso en sistemas empotrados donde la seguridad es crítica como en aviación, sistemas médicos o instalaciones nucleares.

2.2.2.8 Contiki

Contiki es un pequeño sistema operativo de código abierto, altamente portable y multitarea, desarrollado para uso en pequeños sistemas, desde ordenadores de 8-bit a sistemas empotrados sobre microcontroladores, incluyendo nodos de redes de sensores. El nombre Contiki viene de la famosa balsa Kon-Tiki de Thor Heyerdahl. A pesar de incluir multitarea y una pila TCP/IP, Contiki sólo requiere varios kilobytes de código y unos cientos de bytes de RAM. Un sistema totalmente completo con una GUI requiere aproximadamente 30 kilobytes

de RAM.

El núcleo básico y la mayor parte de las funciones principales fueron desarrolladas por Adam Dunkels en el grupo de sistemas de redes empotradas en el instituto sueco de ciencias computacionales.

Contiki fue diseñado para sistemas empotrados con poca cantidad de memoria. Una configuración típica de Contiki es 2 kilobytes de RAM y 40 kilobytes de ROM. Contiki consiste en un núcleo orientado a eventos, el cual hace uso de protohilos, sobre el cual los programas son cargados y descargados dinámicamente. También soporta multihilado apropiativo opcional por proceso, comunicación entre procesos mediante paso de mensajes a través de eventos, al igual que un subsistema GUI opcional, el cual puede usar un soporte directo de gráficos para terminales locales, terminales virtuales en red mediante VNC o sobre Telnet

Contiki funciona en una variedad de plataformas, desde microcontroladores empotrados, como el MSP430 y el AVR, a viejas computadoras domésticas. El tamaño del código está en el orden de los kilobytes y el uso de la memoria puede configurarse para que sea de sólo unas decenas de bytes.

2.2.2.9 MANTIS

El sistema operativo MANTIS (Multimodal system for Networks of In-situ wireless Sensors) suministra un nuevo sistema operativo empotrado de plataforma múltiple para redes de sensores inalámbricos. Ante el incremento de complejidad de las tareas realizadas por las redes de sensores como compresión, agregación y procesamiento de señales, los multiprocesos en MANTIS sensor OS (MOS) permiten interpaginar complejas tareas con tareas susceptibles al tiempo para así mitigar los problemas en los saltos de buffers.

Para conseguir una eficiencia en el uso de la memoria, MOS es implementado para que utilice una pequeña cantidad de RAM. Usando menos de 500 bytes de memoria, incluyendo el kernel, los controles de tiempo y la pila de comunicación. Para conseguir la eficiencia energética, el controlador de eficiencia energética de MOS hace que el microcontrolador duerma después de ejecutar todas las tareas activas, reduciendo el consumo de energía a un rango de μA .

Una de las características principales de MOS es la flexibilidad en el soporte de múltiples plataformas como PCs, PDAs y diferentes plataformas de microsensores. Otra de las características destacada del diseño de MOS es el soporte de control remoto, permitiendo una reprogramación dinámica y un acceso remoto.

2.2.2.10 BTnut

Sistema operativo de código abierto creado para correr dentro de sistemas empotrados BTnodes. Fue diseñado principalmente para el procesador Atmel ATmega128 (el cual forma parte de los motes BTnodes) y por lo tanto es el más recomendado para esta clase de motes.

La actual compilación de sus programas (la conversión de código C a código máquina) es realizada usando gcc-avr, el cual es un compilador de C libre para la plataforma de procesadores Atmel. Podemos diferenciar tres partes: las rudimentarias librerías C que son implementadas por la parte avr-libc de gcc-avr; las rutinas de alto nivel construidas para avr-libc por Nut/OS; y los drivers específicos para el funcionamiento del mote BT-node proporcionados por BTnut.

2.2.3 Lenguajes de Programación

La programación de sensores es complicada, entre otras dificultades está la limitada capacidad de cálculo y la cantidad de recursos. Y así como en los sistemas informáticos tradicionales encontramos entornos de programación prácticos y eficientes para depurar código, simular... en estos microcontroladores todavía no hay herramientas comparables.

Podemos encontrar lenguajes como:

- nesc: lenguaje que utilizamos para nuestras motas, y que está directamente relacionado con TinyOS. (Como es el más utilizado entraremos en detalle después)
- Protothreads: específicamente diseñado para la programación concurrente, provee hilos de dos bytes como base de funcionamiento.
- SNACK: facilita el diseño de componentes para redes de sensores inalámbricas, sobre todo cuando la información o cálculo a manejar es muy voluminoso, complicado con nesc, este lenguaje hace su programación más fácil y eficiente. Luego es un buen sustituto de nesc para crear librerías de alto nivel a combinar con las aplicaciones más eficientes.
- c@t: iniciales que hincan computación en un punto del espacio en el tiempo (Computation at a point in space (@) Time)
- DCL: Lenguaje de composición distribuido (Distributed Compositional Language)
- galsC: diseñado para ser usado en TinyGALS, es un lenguaje programado mediante el modelo orientado a tarea, fácil de depurar, permite concurrencia y es compatible con los módulos nesc de TinyOS
- SCTL (Sensor Query and Tasking Language): como su nombre indica es una interesante herramienta para realizar consultas sobre redes de motas.

2.2.3.1 Nesc

El lenguaje de programación NesC (Network Embedded Systems C), de sintaxis similar a C, está optimizado para las limitaciones de memoria en las redes inalámbricas de sensores. También está orientado a componentes y especialmente está diseñado para programar en redes de sensores bajo el sistema operativo TinyOS.

Una aplicación NesC está formada por uno o más componentes enlazados entre ellos y de esta manera forman un ejecutable. Cada componente proporciona y utiliza interfaces bidireccionales ya que son el único punto de comunicación hacia otros componentes y en ella se puede realizar múltiples instancias hacia una misma, como por ejemplo en el caso que un componente necesite dos temporizadores, en este caso tendrá que hacer dos instancias a la interfaz que proporcione el temporizador. Gracias al uso de interfaces, conseguimos una unión de componentes de manera estática, mejor análisis del programa y un aumento de la eficiencia en lo que a tiempos de ejecución se refiere y en la robustez del diseño.

La implementación de los componentes en Nesc se realiza mediante módulos y configuraciones. Los módulos proporcionan el código de la aplicación en que se implementan los eventos de una o varias interfaces formadas por una agrupación de comandos y eventos, mediante los cuales conseguimos dar respuesta a algún suceso determinado como puede ser al recibir cierto mensaje desde cierto componente. Las configuraciones comúnmente conocidas por wiring, son utilizadas para ensamblar otros componentes de manera conjunta en que se conectan las interfaces utilizadas por los componentes con las interfaces proporcionadas por otros, es decir, se encargarán de unir diferentes componentes en función de sus interfaces ya sea mediante comandos o eventos.

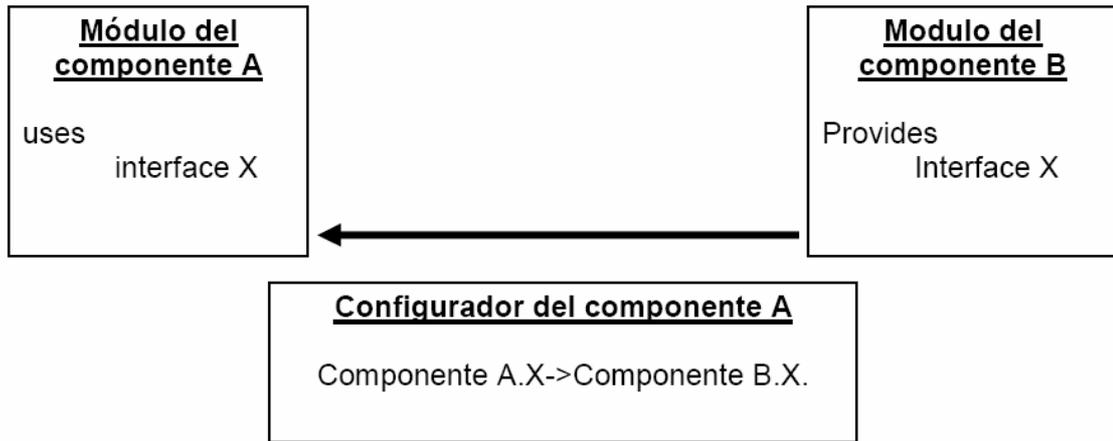


Figura 2.17: Ejemplo código NesC

A partir de la figura anterior, tal y como indican sus códigos, el componente B proporciona la interfaz X al componente A para que éste la utilice.

2.2.4 Diseño de Red

Una parte muy importante en las redes, es tener en cuenta que en base al tipo de aplicación, el diseño de la red puede variar. Las áreas a considerar para un diseño son:

TOPOLOGÍA

La topología es generalmente cambiante para las redes de Sensores Ad hoc. Es decir, los nodos se despliegan de manera aleatoria. Una vez desplegados no se requiere de la intervención humana, haciendo la configuración y el mantenimiento completamente autónomos. En la organización de la topología, cada nodo busca información completa de la red o parte de ella, con el fin de mantener las estructuras de información de la red actualizadas.

RUTEO

La responsabilidad de un protocolo de ruteo es el intercambio de información, encontrando el camino más confiable para alcanzar el destino deseado teniendo en consideración la distancia, el requerimiento mínimo de energía y el tiempo de vida del enlace inalámbrico; búsqueda de la información en el caso de que la conexión falle; reparación de los enlaces caídos gastando el mínimo de potencia de procesamiento y ancho de banda.

ENERGÍA

Un cuello de botella que se tiene en la operación de los nodos sensores es la capacidad de energía. Los sensores tienen una vida intrínsecamente dependiente del tipo de batería que se utiliza. (Ni-Cd, Ni-Mh, Li-Ion).

Así mismo, el hardware diseñado para los nodos deberá tener un consumo óptimo de energía como requerimiento primordial. El microcontrolador, el sistema operativo y el software de aplicación deberán optimizar la conservación de energía, inclusive desde el punto

de escoger las instrucciones y su codificación, para que las instrucciones más ocupadas utilicen la menor potencia posible. Otros diseños optimizan el consumo de energía con la minimización de sistemas síncronos y/o el concepto de sistemas asíncronos globales y síncronos solamente en pequeñas porciones locales que lo necesiten.

SINCRONÍA

Los nodos sensores deberán ser capaces de sincronizarse uno con otro de manera completamente distribuida, para que la calendarización del multiplexado en tiempo pueda ser impuesta y ordenada de forma temporal la detección de eventos sin ninguna ambigüedad. Dado que los nodos en una red inalámbrica de sensores operan de forma independiente, sus relojes podrán o no, estar sincronizados. Esto podría causar dificultades cuando se trate de integrar e interpretar información sensada en diversos nodos.

ESCALABILIDAD

A medida que el número de sensores aumenta, el potencial de que existan fallos en la comunicación entre los nodos se incrementa de manera exponencial. Como consecuencia se requiere de un mejor control que mantenga a la red conectada a pesar del decremento en el ancho de banda utilizable. Aquí la escalabilidad y la certeza en la red son rubros que se contraponen, ya que al tener una red más densa, es más probable tener fallos en base a la comunicación de los nodos.

CALIDAD DE SERVICIO

La calidad del servicio puede interpretarse en las redes de sensores por enlace, por flujo de información o por funcionamiento de nodo. En estas redes, tanto la red como el *host* pueden tener situaciones que requieren de una buena coordinación.

La falta de coordinación central y de un límite de recursos puede desencadenar un problema. El nivel de servicio y sus parámetros están asociados al tipo de aplicación. La comunicación en tiempo real sobre una red de sensores deberá de ser garantizada a pesar de tener un máximo de retraso, un ancho de banda mínimo y otros parámetros involucrados en la calidad del servicio.

TOLERANCIA A FALLOS

La red debe ser capaz de modificar algún aspecto de ella donde se presente un fallo. La fallo deberá de ser identificada y resuelta en un tiempo promedio. Esté rubro es muy importante primordialmente para aplicaciones militares y para aplicaciones civiles donde existe un riesgo de pérdida de vida por fallo de un equipo electrónico. La falta de una comunicación central y un medio compartido hace que la red sea vulnerable a ataques más que en redes alámbricas, pues existen muchos puntos de acceso a la red, que cuando no existen mecanismos de detección de intrusos, facilitan los ataques.

AUTO-ORGANIZACIÓN

Es una de las propiedades más importantes que se deben exhibir en una red Ad-hoc. Entre las principales actividades que se efectúan mediante la auto-organización es la de búsqueda de nodos adyacentes, organización de la topología y la re-organización de la topología. Durante la fase de búsqueda, cada nodo de la red recolecta información acerca de

los vecinos y mantiene la información en estructuras. Por ende, se demanda que periódicamente se transmitan pequeños paquetes llamados *beacons*, que vigilan en el canal para detectar cualquier actividad del vecino. En la fase de reorganización requieren información confiable de la topología, ya sea en base a la movilidad de los nodos, la cantidad de energía de los nodos o la eficiencia en los enlaces, en caso de que se haya suscitado un cambio de último momento.

Las redes de sensores están formadas por un conjunto de pequeños dispositivos denominados nodos sensores, con capacidad limitada de cómputo y comunicación, cuyo tiempo de vida depende de una batería adjunta al dispositivo. El tiempo de vida de la red de sensores dependerá por tanto del tiempo de vida de la batería de sus nodos. Estos dispositivos se encuentran dispersos de manera ad-hoc en una determinada área a monitorizar.

Típicamente, el modelo seguido por las aplicaciones es el siguiente: realizar una serie de mediciones sobre el medio, transformar dicha información en digital en el propio nodo y transmitirla fuera de la red de sensores vía un elemento gateway a una estación base, donde la información pueda ser almacenada y tratada temporalmente para acabar finalmente en un servidor con mayor capacidad que permita componer un histórico o realizar análisis de datos.

En una red de sensores inalámbricos, por lo tanto, podemos encontrar:

- Nodos inalámbricos
- Puertas de enlace
- Estaciones base

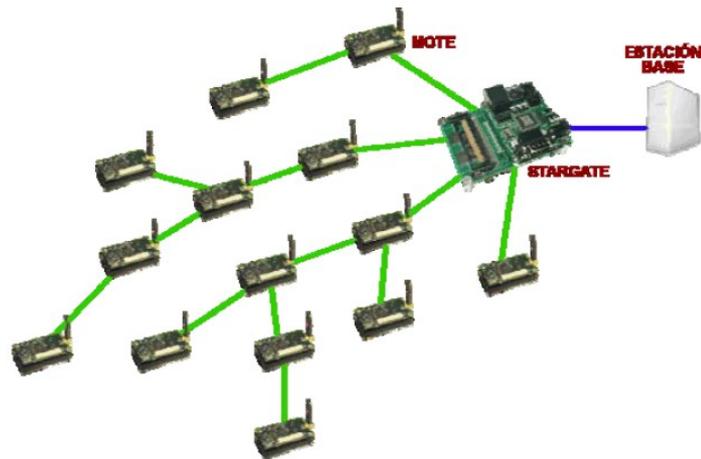


Figura 2.18: Distribución de una red de sensores

PUERTA DE ENLACE

Elementos para la interconexión entre la red de sensores y una red de datos (TCP/IP). Es un nodo especial sin elemento sensor, cuyo objetivo es actuar como puente entre dos redes de diferente tipo.

En este tipo de aplicaciones donde se usan redes de sensores, éstas no pueden operar completamente aisladas y deben contar con alguna forma de monitoreo y acceso a la información adquirida por los nodos de la red de sensores. De aquí surge la necesidad de conectar las redes de sensores a infraestructuras de redes existentes tales como Internet, redes de área local (LAN) e intranets privadas. Los dispositivos que realizan la función de interconectar dos redes de diferente naturaleza se les llama dispositivo puerta de enlace; pero

el término más conocido en el ambiente de las redes es gateway.

ESTACIÓN BASE

Recolector de datos basado en un ordenador común o sistema empujado. En una estructura normal todos los datos van a parar a un equipo servidor dentro de una base de datos, desde donde los usuarios pueden acceder remotamente y poder observar y estudiar los datos.

TOPOLOGIAS

Hay varias arquitecturas que pueden ser usadas para implementar una aplicación de WSN como pueden ser estrella, malla o una híbrida entre ellas dos. Cada topología presenta desafíos, ventajas y desventajas. Para entender las diferentes topologías es necesario conocer los diferentes componentes de la WSN.

- **Nodos finales:** Compuesto por sensores y actuadores donde se capturan los datos sensores. Para las redes basadas en ZigBee son llamados RFD (Reduced Functional Devices).



- **Routers:** Dan cobertura a redes muy extensas pudiendo salvar obstáculos, problemas de congestión en la emisión de la información y posibles fallos en alguno de los aparatos.



- **Puertas de enlace:** Recoge los datos de la red, sirve como punto de unión con una red LAN o con Internet.



Topología se refiere a la configuración de los componentes hardware y como los datos son transmitidos a través de esa configuración. Cada topología es apropiada bajo ciertas circunstancias y puede ser inapropiada en otras. La idea de una red de sensores surge gracias a las posibilidades que nos da la tecnología.

-Una **topología en estrella (monosalto)** es un sistema donde la información enviada sólo da un salto y donde todos los nodos sensores están en comunicación directa con la puerta de enlace, usualmente a una distancia de 30 a 100 metros. Todos los nodos sensores son idénticos, nodos finales, y la puerta de enlace capta la información de todos ellos. La puerta de enlace también es usada para transmitir datos al exterior y permitir la monitorización de la red.

Los nodos finales no intercambian información entre ellos, sino que usan la puerta de enlace para ello, si es necesario.

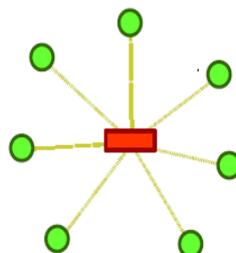


Figura 2.19: Topología en estrella

La topología en estrella es la que menor gasto de energía desarrolla, pero por el contrario esta limitada por la distancia de transmisión vía radio entre cada nodo y la puerta de enlace. Tampoco tiene un camino de comunicación alternativo en caso de que uno de los nodos tenga obstruido el camino de comunicación, lo que lleva a que en este caso la información de ese nodo sea perdida.

-La **topología en malla** es un sistema multisalto, donde todos los nodos son routers y son idénticos. Cada nodo puede enviar y recibir información de otro nodo y de la puerta de enlace. A diferencia de la topología en estrella, donde los nodos solo pueden hablar con la puerta de enlace, en ésta los nodos pueden enviarse mensajes entre ellos.

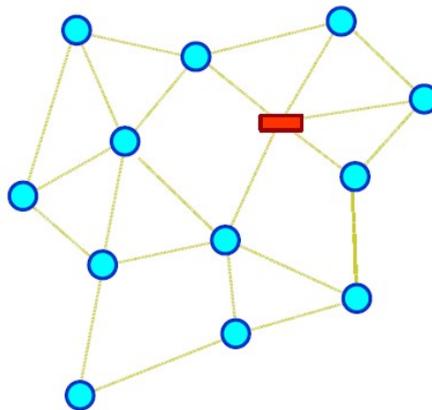


Figura 2.20: Topología en malla

La propagación de los datos a través de los nodos hacia la puerta de enlace hace posible, por lo menos en teoría, crear una red con una extensión posible ilimitada. Este tipo, también es altamente tolerante a fallos ya que cada nodo tiene diferentes caminos para comunicarse con la puerta de enlace. Si un nodo falla, la red se reconfigurará alrededor del nodo fallido automáticamente.

Dependiendo del número de nodos y de la distancia entre ellos, la red puede experimentar periodos de espera elevados a la hora de mandar la información.

-La **topología híbrida estrella-malla** busca combinar las ventajas de los otros dos tipos, la simplicidad y el bajo consumo de una topología en estrella, así como la posibilidad de cubrir una gran extensión y de reorganizarse ante fallos de la topología en malla. Este tipo crea una red en estrella alrededor de routers pertenecientes a una red en malla. Los routers dan la posibilidad de ampliar la red y de corregir fallos en estos nodos y los nodos finales se conectan con los routers cercanos ahorrando energía.

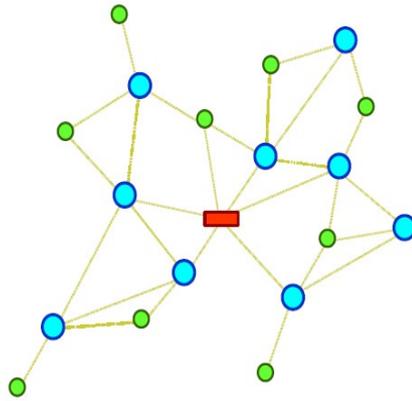


Figura 2.21: Topología híbrida

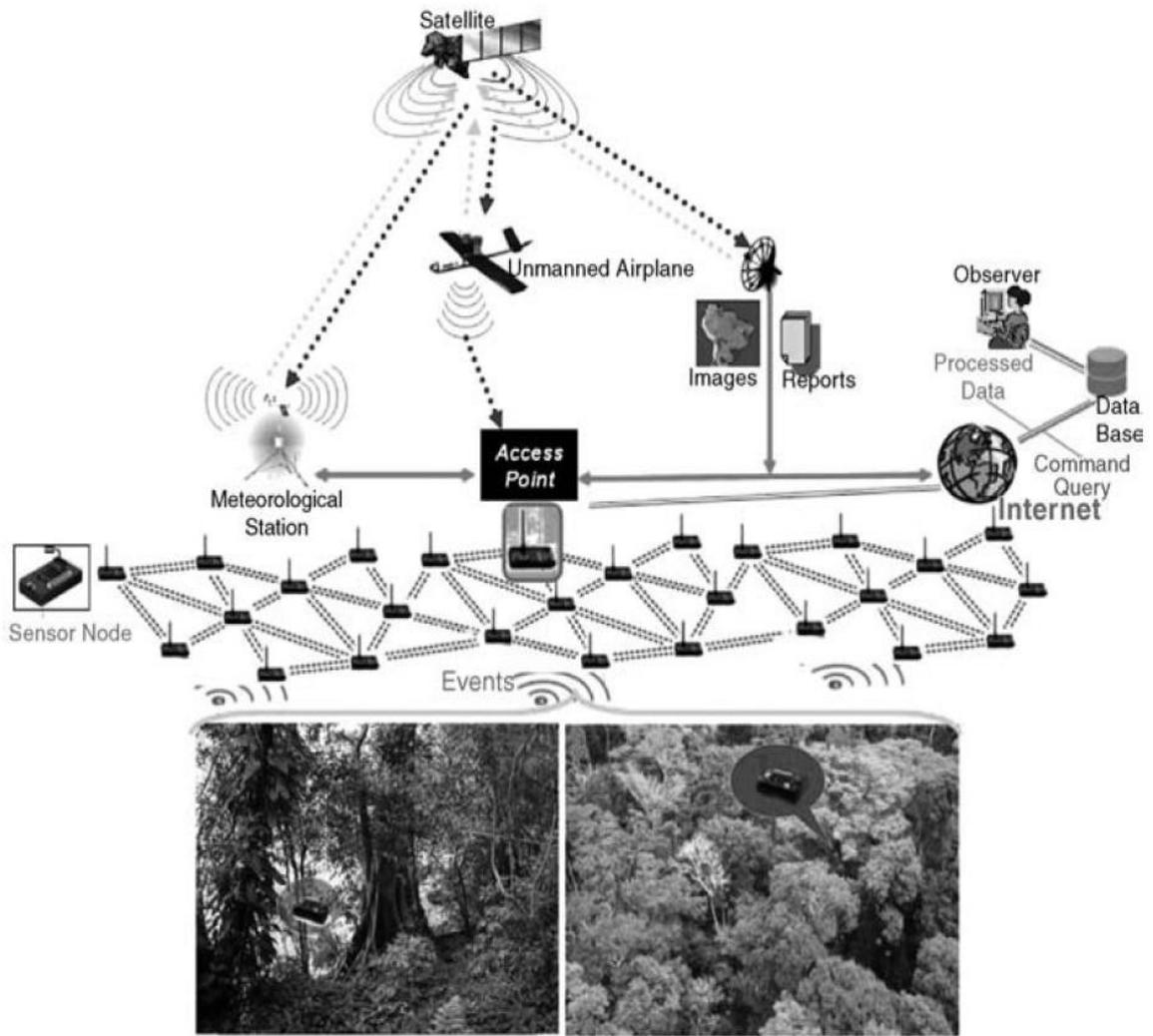


Figura 2.22: Ejemplo monitorización de una selva tropical

2.2.5 Aplicaciones

Las aplicaciones de las redes de sensores son diversas :



Figura 2.23: Diferentes aplicaciones de las redes sensores

2.2.5.1 Militar

El apoyo militar fue el primer propósito por el cual empezó a investigarse esta área. Tener conocimiento en tiempo real del campo de batalla es esencial para el control, las comunicaciones y la toma de decisiones.

La red de sensores puede ser rápidamente desarrollada sin tener que realizar una infraestructura como puede suceder en otros casos como un radar, y pasar a recoger información inmediatamente. Por ejemplo, imagina el siguiente escenario donde una compañía petroquímica ha sufrido ataques. Esto genera una explosión en la parte de almacén de productos primarios. Un gas contaminante desencadena la creación de una nube con elementos sumamente contaminantes ya sean por la adición de gases o partículas sólidas o líquidas en suspensión en proporciones distintas a las naturales.

La generación y difusión de agentes contaminantes como el dióxido y monóxido de carbono, óxidos de nitrógeno y azufre, entre otros, desempeñan un papel importante que se presenta en un origen puntual que puede dispersarse sobre una zona geográfica amplia. En el caso del dióxido de nitrógeno, exposición a corto plazo en altos niveles (40 microgramos/ 3 m) puede causar cambios irreversibles en el tejido pulmonar similares a un enfisema. En el grupo de los óxidos de nitrógeno, se tienen reacciones varias que parten de producir lluvia ácida hasta producir alucinaciones o un estado eufórico.

La función que desempeña la red es de dar a conocer la trayectoria de la combinación de gases, su velocidad y su forma. Para ello, se emplean SensorNeTSwats.

Estos nodos sensores son desplegados mediante vehículos aéreos manipulados que sobrevuelan el área afectada. Un experimento así se realizó en el Desierto del Mojave al Sur de California por el Profesor Kris Pister de la Universidad de California, Berkely. Cada nodo sensor fue equipado con un microprocesador, un sistema de RF (radio frecuencia). La figura 2.24 muestra un conjunto de nodos que se desplegaron aleatoriamente. En base a la información que adquieren los nodos se sabe la dirección a la que se dirige el gas y la velocidad del mismo. Los nodos son cuadros pequeños que se denotan por el color rojo y verde.

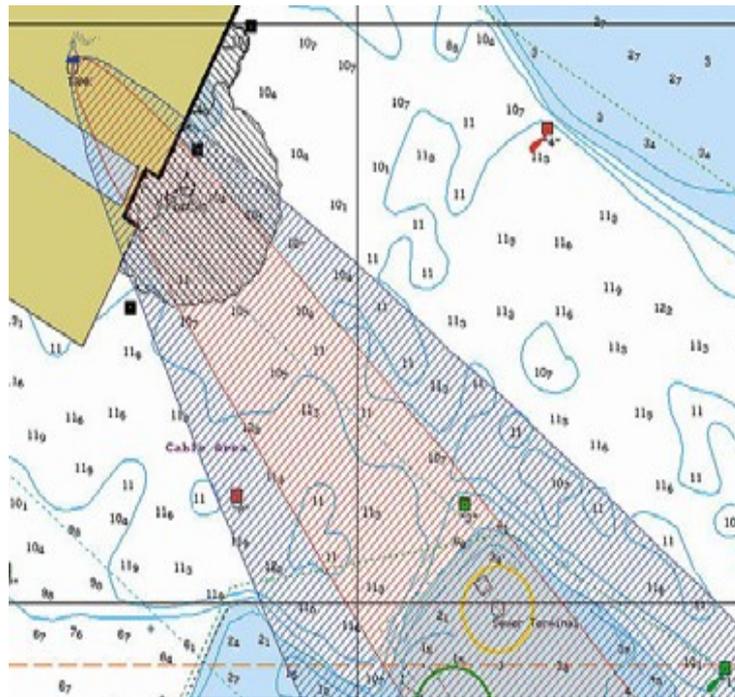


Figura 2.24: Imagen de la dispersión del gas en el área

2.2.5.2 Medio Ambiente

Los sensores se emplean para el medio ambiente en el caso de incendios forestales, detección de inundaciones y exploración de animales en su hábitat natural.

En el caso de monitoreo del medio ambiente se tiene un experimento de la conservación de la fauna mediante el sensado de intrusos (humanos, animales u otros depredadores) automatizado en la isla de Great Duck, en las costas del estado de Maine en el noreste de los Estados Unidos.



Figura 2.25: Vista aérea de la isla

Un equipo de ingenieros de la Universidad de California (Berkeley), monitorean el comportamiento de las aves en sus nidos durante ciertas temporadas. Esto mediante nodos inalámbricos que reportan la información obtenida de estas aves denominadas *petrels*.



Figura 2.26: Petrels

Con esto, es posible que un grupo de biólogos del Colegio Atlántico, observen la actividad de los *petrels* en dicha isla desde el confort de sus oficinas mediante el enlace satelital que permite la comunicación de los nodos con la base en California y de vuelta al estado de Maine. Los parámetros de estudio fueron la cantidad de luz que penetra en los nidos, la temperatura a la que se encuentran con o sin la presencia de las aves, y la humedad. En la figura 2.27 se observan las posiciones donde los sensores son desplegados.



Figura 2.27: Distribución de los sensores

En el caso del monitoreo de los glaciares para entender el cambio climático que involucra un cambio del nivel del mar debido al calentamiento global, es importante entender como los glaciares contribuyen en la liberación de agua fresca al mar. Esto puede causar altos crecimientos del nivel del mar y grandes cambios en la temperatura y por lo tanto en las mareas marinas. El comportamiento de un glaciar y sobre todo de su movimiento puede llevarnos a predecir cambios futuros en su comportamiento.

Durante el verano de 2004 fue estudiado el comportamiento del glaciar Briksdalsbreen en Noruega por medio de redes de sensores inalámbricas. El objetivo fue entender la dinámica del glaciar con respecto al cambio climático.

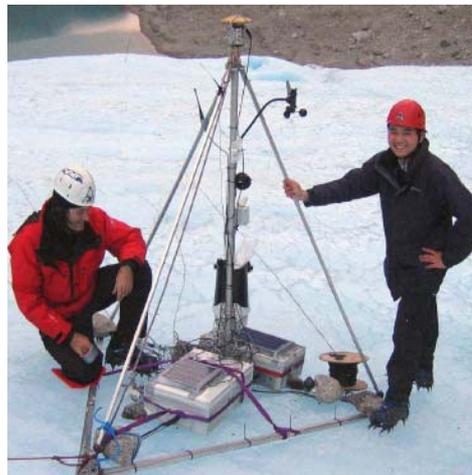


Figura 2.28: Investigadores tomando datos del glaciar

2.2.5.3 Salud

En el ámbito de la salud, las redes de sensores pueden llevar a cabo acciones que monitoreen pacientes, diagnostiquen enfermedades, administren la medicina, monitoreen el

movimiento de pacientes dentro del hospital y demás funciones.

Lore et al describe una aplicación biomédica que se aplica para restaurar la visión de los pacientes con enfermedad retiniana externa, como retinitis pigmentosa (RP), o degeneración macular asociada a la edad, mediante una retina artificial. Especialmente, para pacientes que han perdido sólo el funcionamiento de la retina. El proyecto SSIM (Smart Sensors and Integrated Microsystems), se realiza por medio de un chip prótesis en la retina. Este chip está formado por 100 micro sensores, construido e implementado en un ojo humano. De esta manera, el paciente cuya visión se limita o se nubla puede adquirir un nivel de percepción un poco tosco que permite realizar sus actividades diarias sin problema alguno.

Sin embargo, se sospecha que en altos valores relacionados con la severidad en la degeneración del implante (chip) epiretiniana debe estar, en principio, en coordinación con el vítreo. Abajo se muestra la figura 2.29 que denota la localización del chip dentro de ojo.

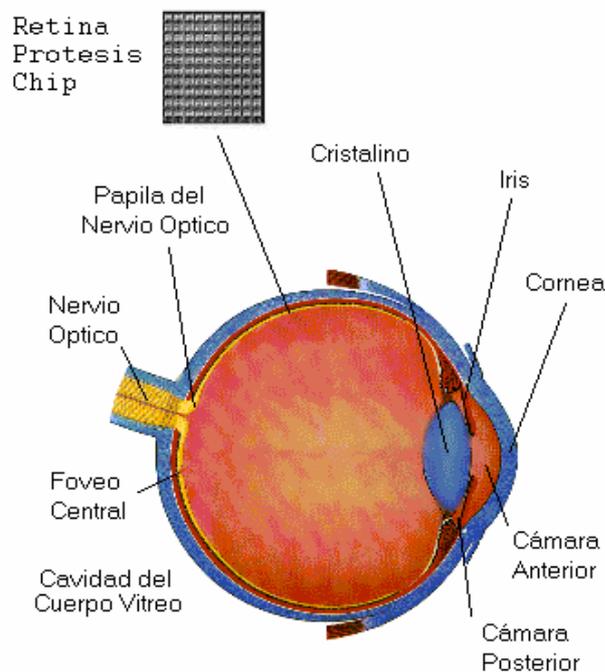


Figura 2.29: Ojo humano con chip integrado

En cuestión se propone un mecanismo basado en redes de sensores inteligentes para facilitar la monitorización de parámetros en humanos que evite su hospitalización y que les permita, en la medida de lo posible, seguir con su actividad cotidiana. Cuando la prueba a realizar no se reduce a unos minutos de monitorización, sino que se deben recopilar datos a lo largo de una noche o incluso a lo largo de uno o varios días con el fin de obtener la suficiente información para llevar a cabo un diagnóstico fiable. En estos casos suele requerir la hospitalización del paciente, lo que implica un perjuicio para el mismo y para los servicios médicos encargados de realizar la prueba, ya que se produce una saturación de los centros hospitalarios.

Actualmente el tratamiento de diabetes pasa por la diaria monitorización de los niveles de glucosa en sangre del paciente. Para ello se usan lancetas de forma que mediante una punción se obtiene la cantidad de sangre necesaria para realizar el análisis. Este sistema presenta una serie de inconvenientes ya que la punción continuada varias veces al día, durante muchos años, puede llegar a dañar la piel e incluso los vasos sanguíneos de la zona. Mediante la implantación de sensores inalámbricos inteligentes se podrían realizar mediciones continuas sin necesidad de que el paciente sienta dolor alguno y dichas mediciones serían transmitidas a un receptor externo. De esta forma se podría llevar un control aún más exhaustivo de los niveles de glucosa alertando con mayor rapidez al usuario de las posibles fluctuaciones en los niveles que se produjesen.

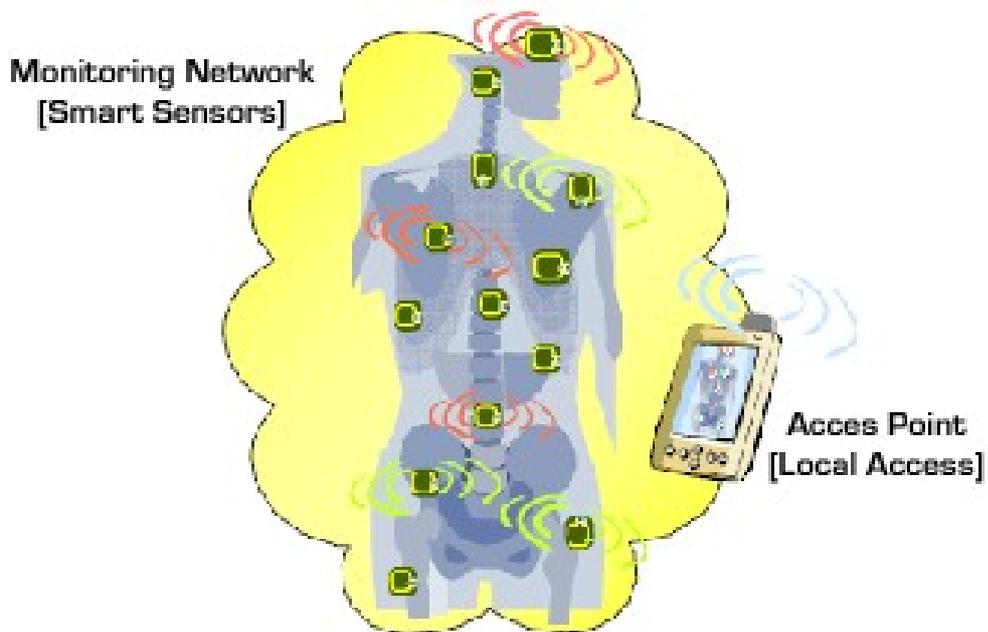


Figura 2.30: Monitorización de un paciente

En el escenario planteado se ha introducido un punto de acceso inalámbrico que actúa como gateway de la red inalámbrica de sensores inteligentes. Una vez que los sensores son accesibles a través de este punto de acceso, podrán ser integrados fácilmente con el resto de sistema Web ya que utilizan los mismo estándares de comunicación e intercambio de información. Este escenario permite, no sólo que el propio paciente monitorice dichos datos, sino que además pueda ser utilizada por el personal médico haciendo uso de las infraestructuras que ya existen.

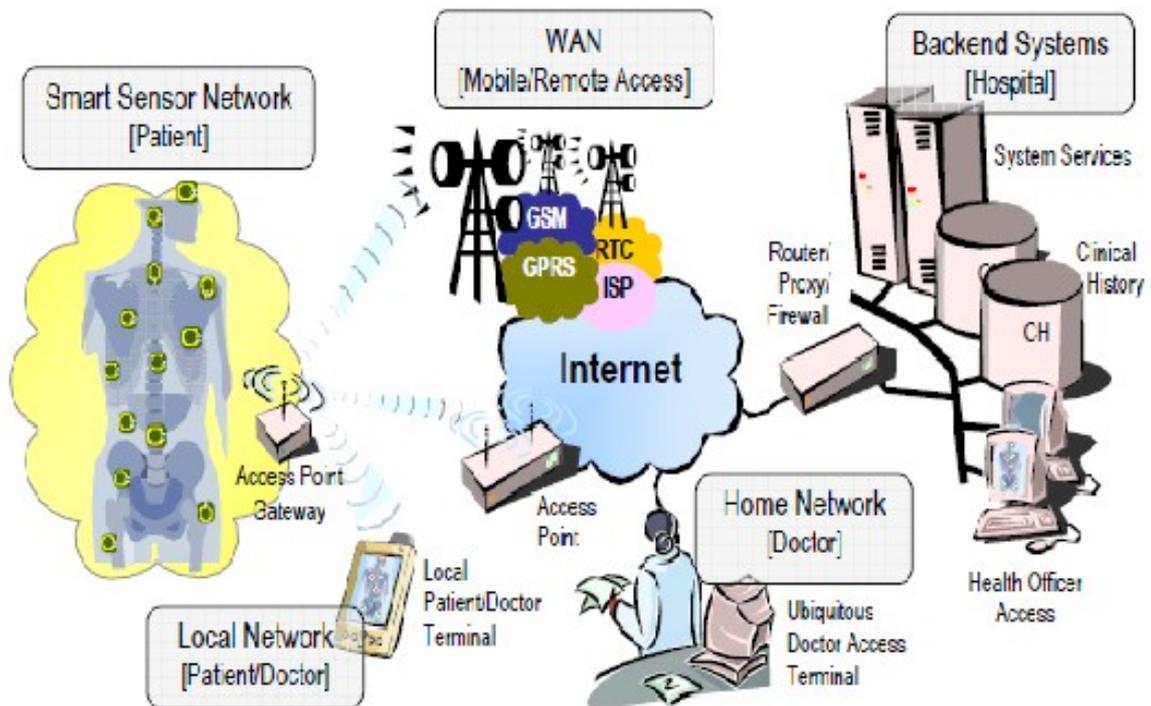


Figura 2.31: Ejemplo de seguimiento de un paciente

Al integrar el sistema de monitorización con el resto de servicios de Internet se abre un abanico de posibilidades anteriormente inimaginables. Los datos podrían ser consultados por una red médica de forma remota, de este modo se le dota al paciente de mayor libertad de movimiento, en otras palabras, se consigue una mayor transparencia para el usuario. Los datos obtenidos también pueden ser registrados junto con los historiales médicos almacenados en los sistemas hospitalarios. Con todo ello se está logrando que los sistemas de sensorización se integren con el resto de elementos conformando la llamada piel digital.

El siguiente paso en la evolución de las redes de sensores es la introducción de ontologías. La inclusión de una ontología permite el paso del plano sintáctico al plano semántico (Semantic Web Service), esto es, les dotamos de la capacidad de saber utilizar las herramientas de las que disponen. Gracias a las ontologías se les da la posibilidad de ser conscientes de su existencia y de la de otros Web Service ya que los sensores serán capaces de autoregistrarse, autodescribirse, autoorganizarse y cooperar entre ellos. Se amplía su capacidad cognitiva, ya que se es consciente de la información con la que se está trabajando y por lo tanto se le dota de la capacidad de actuar en consecuencia. Por ello no sólo disponen de la capacidad de monitorizar sino de la capacidad de actuar de una manera cognitiva. Todo ello permite que puedan interactuar con otros sensores, tanto de su propia red como de otra externa, y con los elementos que están monitorizando.

2.2.5.4 Estructuras

En cuanto al monitoreo de estructuras, las redes de Sensores tiene un gran aplicación. Tanto en Estados Unidos como en Canadá, se estima que se tiene económicamente 25 trillones de dólares invertidos en estructuras civiles. La tecnología denominada SHM

(Structure Health Monitoring) trabaja con la identificación y monitoreo de fallos en estructuras como puentes, edificios y otras construcciones que fueron edificadas durante los años noventas. Un proyecto que se lleva actualmente en San Francisco, California, es el de evaluar las vibraciones del puente Golden Gate. Una placa de sensores se coloca junto con un acelerómetro a un convertidor ADC de 16 bits como se observa en la figura 2.32. La placa de sensores se conecta a una Mica Mote y se coloca en el puente para realizar el análisis de movimiento debido al paso de los automóviles. En la figura 2.33 y la 2.34 respectivamente, se muestra la arquitectura geográfica de la red. Un conjunto de nodos sensores posicionados manualmente en el puente se conectan entre sí y envían a un control central que almacena y procesa los datos obtenidos.



Figura 2.32: Placa del sensor

La figura 2.32 denota la placa llamada Mica Mote donde se le coloca el Sensor. Tiene un microcontrolador tipo ATmega128. Una memoria de programa de 128KB y una memoria RAM de 4 KB. Opera a 2.7 volts y tiene una potencia activa de 60mW. La potencia de recepción es de 29mW, para una potencia de transmisión de 42mW. Además cuenta con una tasa de transferencia de 38.4 kbps.



Figura 2.33: Arquitectura geográfica

Los nodos sensores se colocan en diversas partes del puente, con la finalidad de monitorear diversas áreas de la estructura y comparar la información obtenida para analizar el movimiento que se efectúa por el flujo de vehículos.



Figura 2.34: Monitoreo de estructuras

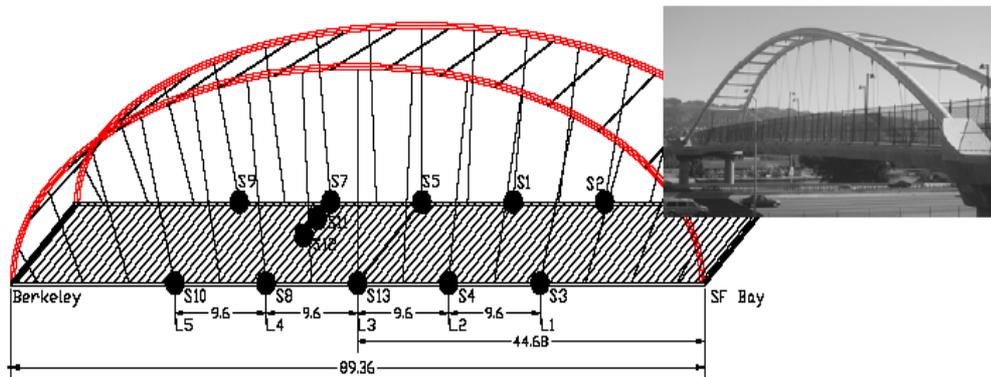


Figura 2.35: Puntos en los que se colocan los sensores en los puentes

Se ve claramente donde es colocado el sensor. Es el barandal a lo largo del puente. Es factible que sense las vibraciones provocadas por los vehículos en movimiento y las vibraciones, aunque mínimas, de las de los *transeúntes*.

2.2.5.5 Agricultura

La agricultura constituye una de las áreas donde se prevé que pueda implantarse con mayor rapidez este tipo de tecnología. Por ejemplo, las redes de sensores favorecen una reducción en el consumo de agua y pesticidas, contribuyendo a la preservación del entorno. Adicionalmente, pueden alertar sobre la llegada de heladas, así como ayudar en el trabajo de las cosechadoras. Gracias a los desarrollos que se han producido en las redes de sensores

inalámbricos en los últimos años, especialmente la miniaturización de los dispositivos, han surgido nuevas tendencias en el sector agrícola como la llamada agricultura de precisión. Esta disciplina cubre múltiples prácticas relativas a la gestión de cultivos y cosechas, árboles, flores y plantas, ganado, etc. Entre las aplicaciones más interesantes se encuentra el control de plagas y enfermedades.

Por medio de sensores estratégicamente situados, se pueden monitorizar parámetros tales como el clima, la temperatura o la humedad de las hojas, con el fin de detectar rápidamente situaciones adversas y desencadenar los tratamientos apropiados. La gran ventaja del uso de esta tecnología es la detección a tiempo y la aplicación óptima de los pesticidas, únicamente en aquellas zonas donde resulta realmente necesario.



Figura 2.36: Sensor agrícola del proyecto LOFAR de la lucha contra el hongo Fitóftora

-El mantenimiento y cuidado de espacios y parques naturales resulta complejo en gran medida por las especiales características de los mismos. Se trata de áreas de grandes dimensiones, en algunos casos de difícil acceso, que están repletos de especies vegetales y animales que hay que preservar, por lo que la supervisión de los mismos debe realizarse empleando métodos lo menos intrusivos posibles.

Nuevamente las redes inalámbricas de sensores pueden resultar de gran ayuda en este tipo de tareas. Los sensores, de pequeño tamaño, pueden disimularse con en el entorno, procesando los datos de diversos parámetros ecológicos y transmitiendo la información de forma inalámbrica hasta un centro de control, situado normalmente en la caseta de los guardias forestales. De este modo, se evita en la medida de lo posible la circulación de personas y vehículos por el parque. Entre los parámetros a monitorizar podemos enumerar: temperatura, humedad, crecimiento de árboles y arbustos, desplazamientos de especies, *conteo de animales, caudales de ríos, etc.*

-Los viñedos Camalie, en Estados Unidos, tienen uno de los sistemas más avanzados de medida de la humedad del suelo. Usan la tecnología inalámbrica desarrollada por la Universidad de Berkeley en colaboración con Intel y comercializada por Crossbow.

La aplicación consiste en optimizar la irrigación, reduciendo el consumo de agua, la energía utilizada en el bombeado y mejorando la calidad de la uva. Se proporciona una monitorización del sistema de irrigación, mostrando fallos que pueden tener un impacto sustancial a largo plazo.



Figura 2.37: Control de viñedos

Una vez implantado el sistema se comprobó un importante crecimiento en la producción, además de un descenso en el consumo de energía a la hora de usar las instalaciones.



Figura 2.38: Sistema de riego

2.2.5.6 Automoción

Con las características de las WSN, los coches podrán pronto estar disponibles para hablar unos con otros y con infraestructuras dentro de carreteras y autopistas. Los sensores pueden aplicarse en las ruedas del vehículo para dar asistencia al conductor y avisar de posibles mensajes de alerta.

Por ejemplo durante un frenazo de emergencia, un mensaje de emergencia desde el coche que frena puede enviarse a todos los coches cercanos para que éstos tomen medidas respecto a este evento. Otra aplicación interesante es la recogida de datos de tráfico en tiempo real. La información de la que puede disponer un coche que venga en dirección contraria puede ser valiosa. Un vehículo puede recibir información de otro vehículo sobre dónde están situados los atascos de tráfico, la velocidad y densidad del tráfico o información de sensores fijos.

Toda esta información puede ser transmitida de vehículo a vehículo para evitar atascos y planificar rutas alternativas.

PROYECTO CAPSTONE DE FORD

Con el 70% de los vehículos de la compañía Ford siendo remodelados es importante estar al día y conocer las nuevas opciones y lanzamientos. Ford esta mirando nuevas maneras de innovar a la hora de recoger medidas de sus vehículos. Las redes de sensores están incrementando su inteligencia y además pueden obtener datos, no sólo limitados a luz, temperatura, humedad y movimiento.

Un equipo de la universidad de Michigan, junto con Ford, está diseñando y desarrollando una manera de identificar cuantas veces un vehículo es inspeccionado por un comprador potencial. Esto podría incluir cuantas veces una puerta es abierta, el capo fue levantado o el maletero fue inspeccionado. Los eventos estudiados podrían extenderse también a cuando una persona ocupó un asiento y cuanto tiempo perduró en él.

El entorno por definición, puede ser muy dinámico, haciendo de la posibilidad de conectarse en una red en malla crítico a largo plazo.

CONTROL DEL TRAFICO

Las redes de sensores son el complemento perfecto a las cámaras de tráfico, ya que pueden informar de la situación del tráfico en ángulos muertos que no cubran las cámaras y también pueden informar a los conductores de una situación, en caso de atasco o accidente, que permita a estos tener la capacidad de reacción para tomar rutas alternativas.

DISTRIBUCION DEL TRAFICO MEDIANTE REDES AD-HOC EN VEHICULOS

Los vehículos son considerados como un área para desarrollar aplicaciones sobre WSN. El objetivo de la investigación relatada es crear una gran red de sensores usando los vehículos como portadores de los sensores, además de sus proveedores de energía. Estos nodos irían transmitiendo información relativa a la situación, velocidad, dirección..., que permitirían poder realizar un control del tráfico en diferentes situaciones.

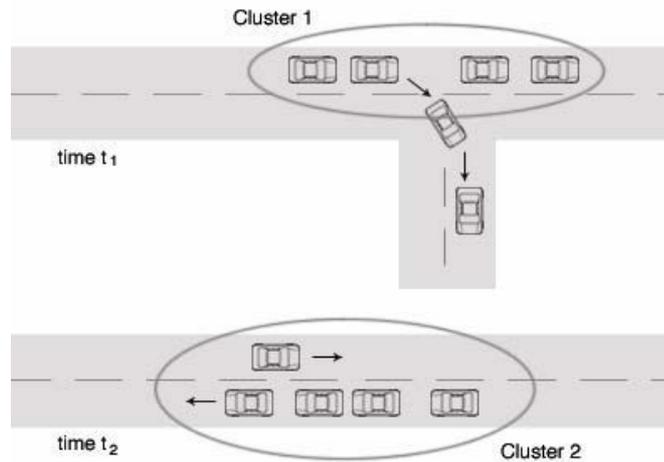


Figura 2.39: Control del tráfico

Además se tendrían varias puertas de enlace fijas que captarían información también, llegando a actuar en *cruces semafóricos*.

2.2.5.7 Domótica

Los servicios que ofrece la domótica se pueden agrupar según cinco aspectos o ámbitos principales:

1. **Ahorro energético:** El ahorro energético no es algo tangible, sino un concepto al que se puede llegar de muchas maneras. En muchos casos no es necesario sustituir los aparatos o sistemas del hogar por otros que consuman menos sino una *gestión eficiente* de los mismos.
 - Climatización: programación y zonificación.
 - Gestión eléctrica:
 - Racionalización de cargas eléctricas: desconexión de equipos de uso no prioritario en función del consumo eléctrico en un momento dado
 - Gestión de tarifas, derivando el funcionamiento de algunos aparatos a horas de tarifa reducida
 - Uso de energías renovables

2. **Confort:** Conlleva todas las actuaciones que se puedan llevar a cabo que mejoren el confort en una vivienda. Dichas actuaciones pueden ser de carácter tanto pasivo, como activo o mixtas.
 - Iluminación:
 - Apagado general de todas las luces de la vivienda
 - Automatización del apagado/ encendido en cada punto de luz
 - Regulación de la iluminación según el nivel de luminosidad ambiente
 - Automatización de todos los distintos sistemas/ instalaciones / equipos dotándolos de control eficiente y de fácil manejo

- Integración del portero al teléfono, o del videoportero al televisor
 - Control vía Internet
 - Gestión Multimedia y del ocio electrónicos
 - Generación de macros y programas de forma sencilla para el usuario
3. **Seguridad:** Consiste en una red de seguridad encargada de proteger tanto los **Bienes Patrimoniales** y la **seguridad personal**.
- Simulación de presencia.
 - Alarmas de Detección de incendio, fugas de gas, escapes de agua, concentración de monóxido en garajes.
 - Alerta médica. Teleasistencia.
 - Cerramiento de persianas puntual y seguro.
 - Acceso a Cámaras IP
4. **Comunicaciones:** Son los sistemas o infraestructuras de comunicaciones que posee el hogar.
- Ubicuidad en el control tanto externo como interno, control remoto desde Internet, PC, mandos inalámbricos (p.ej. PDA con WiFi), aparellaje eléctrico.
 - Transmisión de alarmas.
 - Intercomunicaciones.
5. **"Telegestión y Accesibilidad":** Diseño para todos, un diseño accesible para la diversidad humana, la inclusión social y la igualdad. Este enfoque constituye un reto Ético y creativo. Donde las personas con discapacidad reducida puedan acceder a estas tecnologías sin temor a un obstáculo del tipo de tecnología o arquitectura.

Para crear la red domotica compuesta por los diferentes elementos de los que se compone el sistema, se pueden utilizar diversas tecnologías.

Interconexión de Dispositivos	Redes de Control y Automatización	Redes de Datos
<ul style="list-style-type: none"> • IEEE 1394 (FireWire). • Bluetooth. • USB. • IrDA 	<ul style="list-style-type: none"> • KNX • Lonworks • X10 • EIB • EHS • Batibus 	<ul style="list-style-type: none"> • Ethernet • Homeplug • HomePNA • WiFi

Figura 2.40: Clasificación de tecnología de redes domésticas

Persianas controladas por email

Por ejemplo si enviamos un email con el tema "Activar" a una dirección de correo determinada, se encienden las luces de la casa, el equipo de música, y se abren las persianas, simulando la presencia de personas.

En este caso el montaje es más complicado, dado que debemos interactuar con componentes mecánicos (persianas) y electrónicos no automatizados (equipo de música).

El ordenador tendría que estar conectado a la Red y comprobar el correo electrónico cada pocos minutos. Una vez recibido, se activaría un programa que comprobaría el tema del mensaje y, si coincidiese con "Activar", ejecutaría un software de control (herramientas como Outlook permiten automatización de acciones mediante comparación de texto en un mensaje).

Este programa de control, vinculado a unas tarjetas "controladores" instaladas en el PC, ordenaría al "actuador" de la persiana que activara un motor para elevarla durante un tiempo determinado, o hasta que la potencia requerida para moverla superara un límite, que significaría que hemos llegado al tope.

Infrarrojos para encender el equipo de música

Para activar el equipo de música, podemos tener un emisor de infrarrojos asociado al ordenador, además de haber memorizado la señal del mando que activaría dicho equipo. De igual manera, aunque más costoso, podríamos optar por la vía más "cinematográfica", con un pequeño brazo robótico que pulsaría un botón.

Las posibilidades de la domótica son enormes, con sensores de luz, temperatura, sonido, imagen, y un largo etcétera que le permiten a nuestro equipo conocer su entorno y actuar en consecuencia.

CONTROL DOMOTICO DE UN EDIFICIO

Aplicaciones de este tipo en el control de una oficina o una casa hacen que el tiempo de permanencia dentro de ésta sea mucho más agradable para el ser humano.

El uso de sensores empotrados puede reducir ampliamente los costes de una monitorización de una construcción donde tener un conocimiento de la temperatura y de la luz para poder regular los sistemas de calefacción y aire acondicionado, así como las luces.

SISTEMA INTELIGENTE DE CONTROL DE LUZ

Un control eficiente de la energía dedicada al alumbrado de comercios puede llegar a ahorrar un 40% del consumo de energía. A pesar de este ahorro estos sistemas no están nada extendidos en este tipo de construcciones.

La meta de esta investigación era reducir el consumo de energía así como crear un entorno de luminosidad ante las preferencias del usuario. Se optó por utilizar WSN ante el mayor precio y menor flexibilidad de un sistema cableado centralizado.

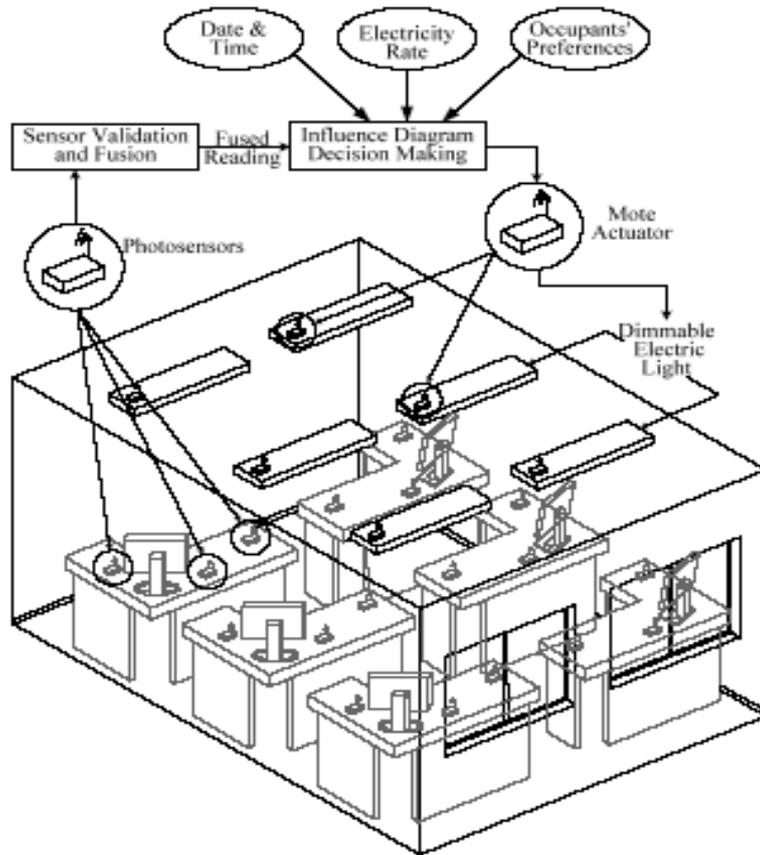


Figura 2.41: Sistema de iluminación inteligente en oficinas

2.3 Alternativas de consumo

La tecnología EnOcean utiliza la energía del ambiente, como la luz, la pulsación mecánica o la temperatura para desarrollar productos inalámbricos radio – como interruptores, detectores de presencia, termostatos o contactos de ventana. Los módulos de EnOcean están basados en convertidores miniaturizados de energía, electrónica altamente integrada y diseñada con una tecnología radio muy fiable.



Figura 2.42: Modelo energía renovable

La combinación de estos elementos permite fabricar dispositivos fundamentales para la automatización de edificios y viviendas, así como la automatización industrial y logística sin necesidad de alimentación ni baterías. Los requerimientos de energía del sistema radio EnOcean son tan bajos que tan solo con el convertidor electromecánico, la pequeña alimentación de una célula solar o la diferencia de temperatura es suficiente para alimentarlo y poder transmitir hasta 3 veces una trama EnOcean. Cada trama digital RF contiene la dirección-ID de 32 bits de cada transmisor. La duración del telegrama es tan corta que se puede considerar el riesgo de colisión de ráfagas en el interfaz radio como nulo. De tal manera pueden coexistir miles de dispositivos dentro de una instalación o un edificio con un grado inmejorable de fiabilidad.

Además la tecnología EnOcean está certificada por el instituto alemán ECOLOG como la tecnología radio con un grado de polución electromagnética 100 veces menor que un interruptor convencional de 220V.

Una tecnología para todas las aplicaciones

EnOcean suministra módulos para fabricantes OEM que desarrollen dispositivos inalámbricos para la automatización de edificios y viviendas así como otros mercados. Actualmente existen más de 100 compañías en el mundo que desarrollaron 350 dispositivos basados en esta tecnología.

En España por ejemplo la tecnología EnOcean se utiliza en dos de los edificios más emblemáticos de la nueva área de negocios en el norte de Madrid – para manejar la iluminación y las persianas. En Torre Espacio funcionan más de 4.200 dispositivos EnOcean y en Torre de Cristal más de 1.400 dispositivos.



Figura 2.43: Sistema de renovación de energía

EnOcean es la tecnología perfecta para remodelaciones y reformas al no necesitar cables y con un mantenimiento nulo al no disponer de batería para alimentarse. Es una tecnología que facilita la integración en sistemas de gestión de edificios disminuyendo los costes de instalación así como el tiempo de integración.



Figura 2.44: Dispositivos EnOcean

Con el lanzamiento de la nueva plataforma Dolphin, EnOcean saca al mercado un sistema con prestaciones y funcionalidades más innovadoras, en el estado del arte de las tecnologías inalámbricas, llegando a un consumo en modo sleep de 80 nA, con un consumo de 5 nA de la RAM necesaria para almacenar datos en dicho modo de funcionamiento. La nueva arquitectura Dolphin expande el portfolio actual de módulos pudiendo configurar vía software a través del entorno de programación DolphinStudio las funcionalidades de bidireccionalidad, conmutación, regulación, repetidor, medida de variables analógicas y modos de funcionamiento sobre una misma plataforma hardware.

3. Estándares de Comunicación Orientados a Redes WSN

3.1 Tecnología Inalámbrica

La comunicación vía radio usa el espectro electromagnético para enviar información. Cuando una corriente eléctrica pasa por un cable crea un campo electromagnético que envía ondas en todas direcciones, en forma parecida a la luz, que también es parte del espectro, pero a frecuencias mucho más altas. Con una antena y energía adicional es posible transmitir las señales a gran distancia. La frecuencia de onda puede modificarse de forma que las señales no interfieran entre sí, lo que permite aprovechar una mayor parte del espectro.

Las tecnologías inalámbricas pueden clasificarse en cinco grandes grupos, de acuerdo con la distancia que viaja cada tipo de señal. Primero están las comunicaciones **satelitales**, como el sistema de posicionamiento global (GPS, por sus siglas en inglés), formado por 24 satélites manejados por las fuerzas armadas de Estados Unidos, las cuales envían constantemente señales a dispositivos en tierra. Sin embargo, estas señales sólo viajan del satélite al aparato receptor.

Otra categoría, y con señales de dos vías, están las tecnologías de **telefonía celular** de cobertura amplia como GSM y CDMA. Entre las versiones avanzadas de ‘tercera generación’ (3G) destacan HSDPA y LTE, desarrolladas por la industria de los celulares. Un contendiente prometedor es WiMax, tecnología basada en los estándares de Internet con respaldo de la industria informática.

Una tercera categoría incluye **señales de menor alcance** utilizadas para conectar dispositivos dentro de una habitación o un edificio, como los sistemas Wi-Fi para conectarse a Internet dentro de hoteles o aeropuertos, o Zigbee, protocolo de comunicaciones inalámbricas que sirve para interconectar sensores.

Un avance reciente es la tecnología de banda ultra ancha (UWB), que utiliza frecuencias sumamente altas de cobertura muy limitada para transmitir grandes volúmenes de información, por ejemplo, para enviar un video desde un iPod o un dispositivo similar a un televisor.

En cuarto lugar están los **protocolos para enlazar dispositivos en una "red de área personal"** (PAN, personal area network). Por ejemplo Bluetooth, utilizado para enviar la señal del teléfono celular a un auricular inalámbrico.

El último tipo de comunicaciones son las que se dan **cerca de una antena transmisora** (NFC, near-field communications). En este caso, el dispositivo receptor debe estar cerca del sistema emisor, por ejemplo, al pasar por un edificio o en el transporte público. Una variante son las etiquetas de identificación por radiofrecuencia (RFID, por sus siglas en inglés), utilizadas por tiendas departamentales y otros usuarios.

Cuando pasan por un lector, estas etiquetas envían la información que tienen almacenada. Estos sistemas de radio son tan diferentes entre sí como la luz lo es del sonido; así, los satélites no pueden rastrear etiquetas RFID, lo cual permite descartar riesgos para la intimidad.

Podemos ver como se distribuyen las diferentes tecnologías inalámbricas dependiendo de la velocidad de transmisión y de su utilización.

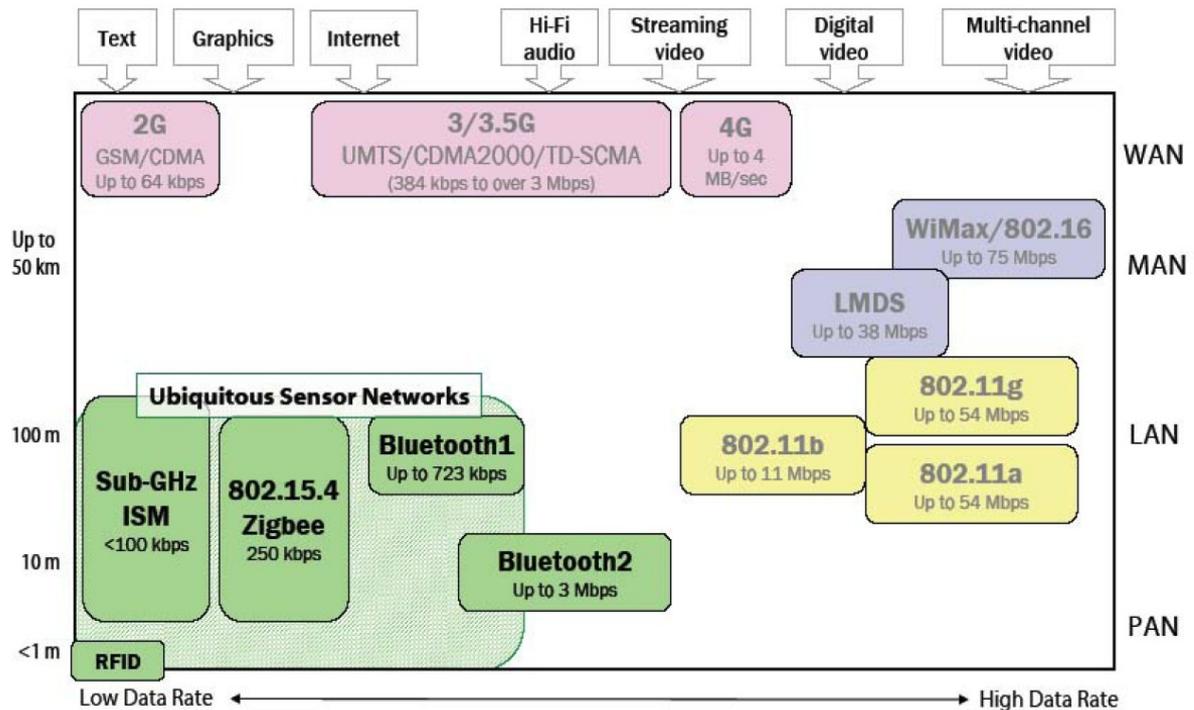


Figura 3.1 Diferentes tecnologías inalámbricas

También podemos estudiar éstas a través del coste que suponen comparado con la cobertura y la velocidad.

	Transferencia de datos por segundo	Cobertura	Costo en dólares (año 2008)
WiMax	15Mb	5 Km	8
Celular 3G	14 Mb	10 Km	6
Celular 2G	400 K	35 Km	5
Wi-Fi	54 Mb	50-100 m	4
Bluetooth	700 K	10 m	1
Zigbee	250 K	30 m	4
UWB	400 Mb	5-10 m	5
RFID	1-200 k	0.01-10 m	0.04

Figura 3.2 Principales tecnologías inalámbricas

Claramente se ve que los protocolos más adecuados para ser usados en WSN son los protocolos **Bluetooth** y **Zigbee**. A pesar de que ZigBee es muy similar a Bluetooth podemos encontrar algunas diferencias que hacen más adecuado el protocolo Zigbee para las WSN:

- Una red ZigBee puede constar de un máximo de 65535 nodos distribuidos en subredes de 255 nodos, frente a los 8 máximos de una subred Bluetooth.

- Zigbee tiene un menor consumo eléctrico que el Bluetooth. En términos exactos, ZigBee tiene un consumo de 30mA transmitiendo y de 3µA en reposo, frente a los 40mA transmitiendo y 0.2mA en reposo que tiene el Bluetooth. Este menor consumo se debe a que el sistema ZigBee se queda la mayor parte del tiempo dormido, mientras que en una comunicación Bluetooth esto no se puede dar, y siempre se está transmitiendo y/o recibiendo.
- Zigbee tiene una velocidad de hasta 250 kbps, mientras que Bluetooth es de hasta 3 Mbps.

Debido a las velocidades de cada uno, uno es más apropiado que el otro para ciertas cosas. Por ejemplo, mientras que el Bluetooth se usa para aplicaciones como los teléfonos móviles y la informática casera, la velocidad del ZigBee se hace insuficiente para estas tareas, desviándolo a usos tales como la domótica, los productos dependientes de una batería, los sensores médicos, y en artículos de juguetería, en los cuales la transferencia de datos es menor.

3.2 Pila de Protocolos ZIGBEE

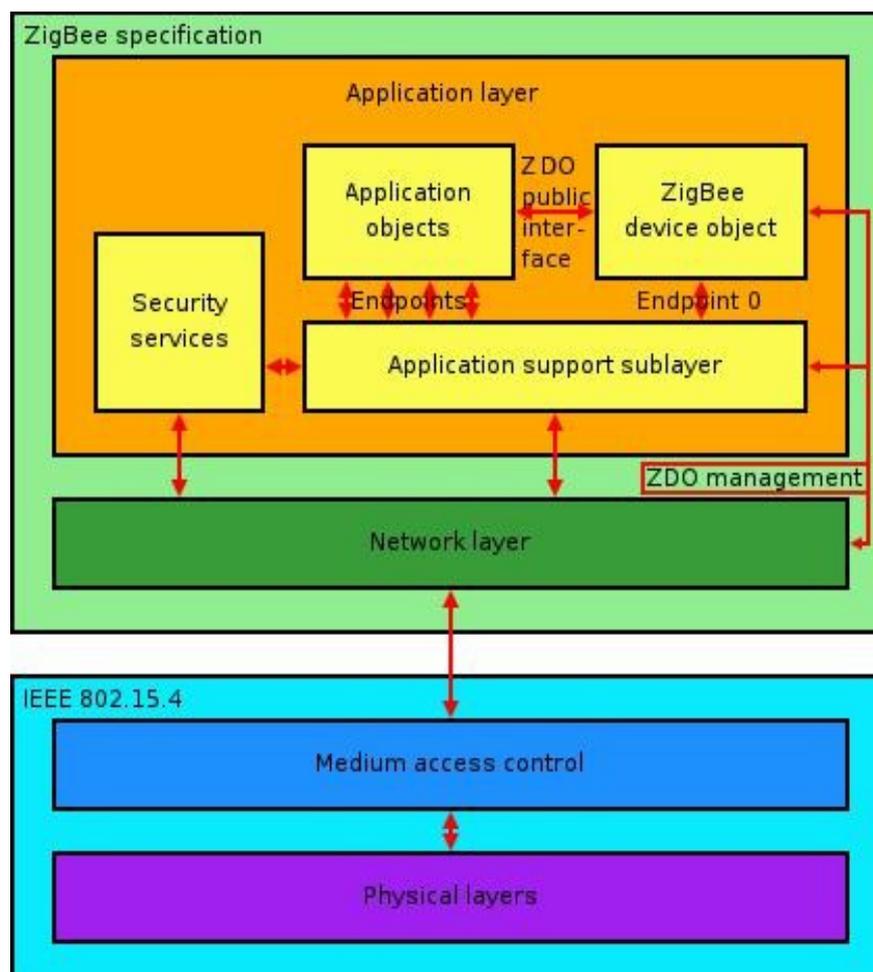


Figura 3.3 Pila protocolos

La relación entre IEEE 802.15.4-2003 y ZigBee es parecida a la existente entre IEEE 802.11 y Wi-Fi Alliance. La especificación 1.0 de ZigBee se aprobó el 14 de diciembre de 2004 y está disponible a miembros del grupo de desarrollo (ZigBee Alliance).

ZigBee utiliza la banda ISM para usos industriales, científicos y médicos; en concreto, 868 MHz en Europa, 915 en Estados Unidos y 2,4 GHz en todo el mundo. Sin embargo, a la hora de diseñar dispositivos, las empresas optan prácticamente siempre por la banda de 2,4 GHz, por ser libre en todo el mundo.

El desarrollo de la tecnología se centra en la sencillez y el bajo coste más que otras redes inalámbricas semejantes de la familia WPAN, como por ejemplo Bluetooth. El nodo ZigBee más completo, requiere en teoría cerca del 10% del hardware de un nodo Bluetooth o Wi-Fi típico; esta cifra baja al 2% para los nodos más sencillos. No obstante, el tamaño del código en sí es bastante mayor y se acerca al 50% del tamaño del de Bluetooth.

En 2006 el precio de mercado de un transceptor compatible con ZigBee se acercaba al dólar y el precio de un conjunto de radio, procesador y memoria rondaba los tres dólares. En comparación, Bluetooth tenía en sus inicios (en 1998, antes de su lanzamiento) un coste previsto de 4-6 dólares en grandes volúmenes; a principios de 2007, el precio de dispositivos de consumo comunes era de unos tres dólares.

La primera versión de la pila suele denominarse ahora ZigBee 2004. La segunda versión de junio de 2006 se denomina ZigBee 2006, y reemplaza la estructura MSG/KVP con una librería de clusters, dejando obsoleta a la anterior versión. ZigBee Alliance está trabajando con la versión de 2007 de la pila para adecuarse a la última versión de la especificación, en concreto centrándose en optimizar funcionalidades de nivel de red (como agregación de datos). También se incluyen algunos perfiles de aplicación nuevos, como lectura automática, automatización de edificios comerciales y automatización de hogares en base al principio de uso de la librería de clusters.

La tecnología Zigbee es mas robusta que las otras tecnologías como puede verse en la figura.

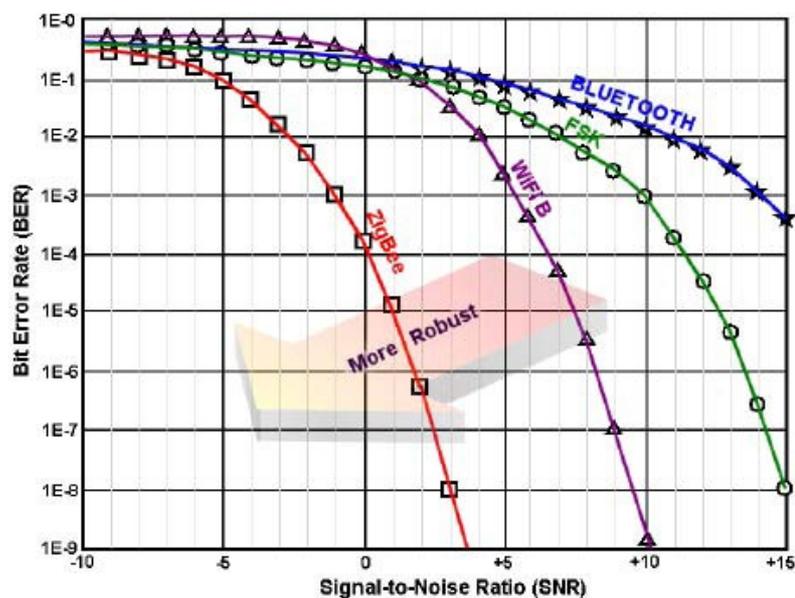


Figura 3.4 Robustez tecnologías inalámbricas

El estándar IEEE 802.15.4 ha sido desarrollado para entornos hostiles y medios compartidos en los que puede ocurrir que haya colisiones de tramas, que exista ruido o que las tramas no lleguen correctamente, por lo que han definido una serie de mecanismos para que sea robusto:

- CSMA-CA: sistema basado en la detección de portadora evitando colisiones. Su esquema de funcionamiento lo hace excelente compartiendo el medio.
- Tramas con confirmación (ACK): cuando enviamos tramas, se nos devuelve una trama ACK confirmando que la trama de datos o cualquier otra ha sido recibida correctamente.
- Verificación de los datos (CRC): mediante un polinomio generador de grado 16 se obtiene la redundancia y se puede comparar el CRC enviado con el calculado en el destino a fin de verificar que el dato se haya transmitido correctamente.
- Restricciones de consumo: la cantidad de energía que consume un nodo cuando escucha el canal es muy baja
- Seguridad: implementa seguridad de clave sim'etrica mediante el est'andar de encriptacion AES. El manejo y gestion de las claves es derivado a capas superiores.

En conclusion resultan ideal para redes de sensores, escalables, con muchos dispositivos, pocos requisitos de anchos de banda, y donde se requiera una duracion muy prolongada de la bateria.

3.3 Protocolo de Comunicación IEEE 802.15.4



Figura 3.5 Pila OSI

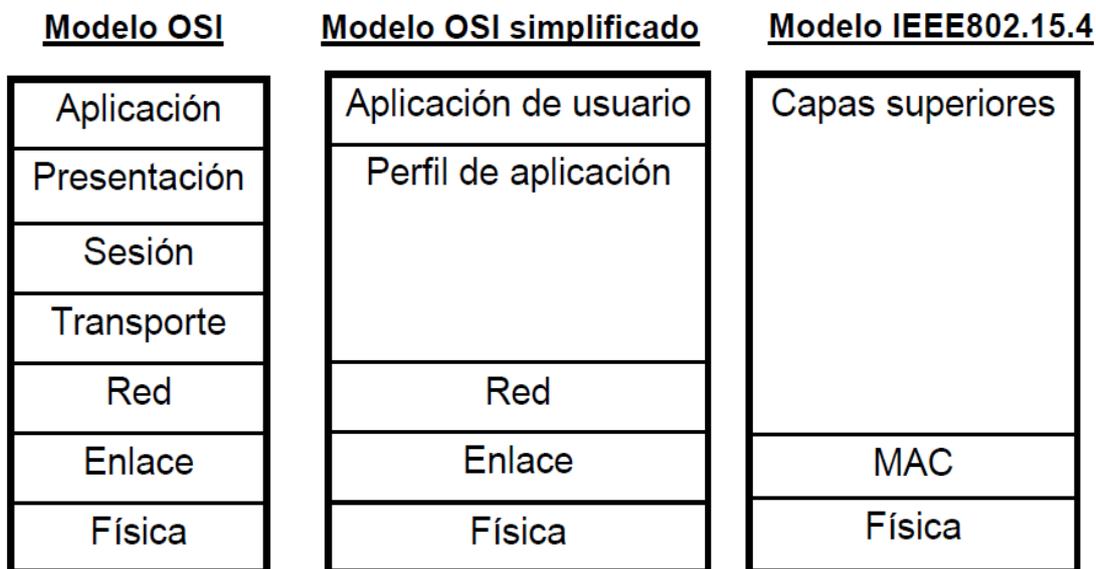


Figura 3.6 Arquitectura de capas orientadas a WSN

Propiedad	Rango
<i>Rango de transmisión de datos</i>	868 MHz:20kb/s; 915 MHz:40kb/s; 2.4 GHz:250kb/s.
<i>Alcance</i>	20 – 30 m (indoor).
<i>Latency</i>	Por debajo de los 15 ms.
<i>Canales</i>	868/915 MHz: 11 canales. 2.4 GHz: 16 canales.
<i>Bandas de frecuencia</i>	Dos PHY: 868/915 MHz y 2.4 GHz.
<i>Direccionamiento</i>	Cortos de 8 bits o 64 bits IEEE
<i>Canal de acceso</i>	CSMA-CA y CSMA-CA ranurado
<i>Temperatura</i>	El rango de temperatura industrial: -40° a +85° C

Figura 3.7 Propiedades del IEEE 802.15.4

Como podemos observar en la figura Arquitectura de capas orientadas a WSN, 802.15.4 se encarga únicamente de definir el nivel físico y el control de acceso al medio (MAC).

Por lo que respecta al nivel físico, este se encarga de proporcionar el servicio de transmisión de datos sobre el medio y además controla el transceptor de radiofrecuencia, el consumo de energía de la señal y la selección de canales de acceso.

El control de acceso al medio (MAC) utiliza la tecnica CSMA CD (Carrier Sense Multiple Acces Collision Avoidance) y de esta manera evita colisiones de tramas. En el caso de que un nodo desee transmitir una trama, en primer lugar el tansceptor escuchara el medio. En caso que el medio este ocupado, la transmision no podra realizarse, y tendra que esperarse un cierto tiempo para volver a intentarlo, asi sucesivamente hasta que encuentre el canal libre.

Las capas del protocolo IEEE 802.15.4 están a su vez constituidas por primitivas. Las primitivas son servicios que una capa o subcapa proporciona al usuario de una capa de nivel superior para capacitarlo en la construcción de funciones que empleen recursos de capas inferiores. Estas primitivas describen el flujo de información que caracteriza una dotación de servicio, y se clasifican en cuatro tipos:

- # Petición: Evento generado por el usuario que desencadena la solicitud de un servicio a la capa correspondiente.
- # Indicación: Una indicación es un evento generado para informar al usuario de una petición de servicio, ya sea remota o interna.
- # Respuesta: Una primitiva de respuesta la genera el usuario para completar un procedimiento desencadenado por una indicación.
- # Confirmación: Tras una petición de servicio, se requiere una confirmación del proveedor de servicio al usuario para completar una operación.

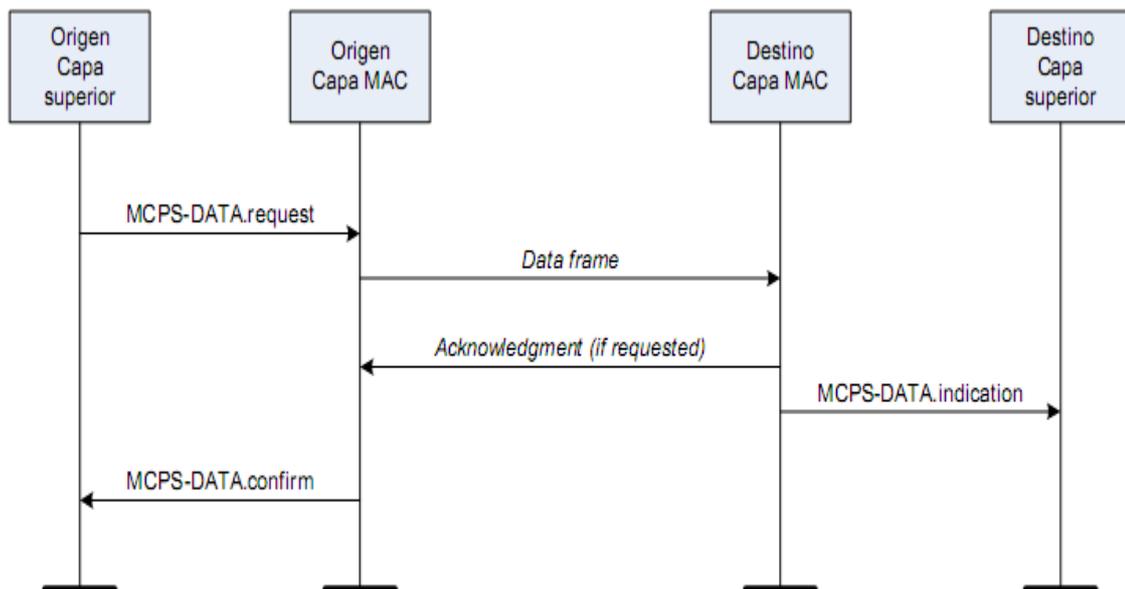


Figura 3.8 MAC Data Service

El flujo de información entre dos dispositivos se rige por una serie de reglas específicas que conocemos genéricamente con el nombre de protocolo de comunicación. Este protocolo debe ajustarse a las necesidades propias de la aplicación.

A lo largo de esta sección, se va a realizar una breve descripción del estándar 802.15.4.

3.3.1 *Capa de Red*

En las redes tradicionales por cable, la capa de red es responsable de la topología de construcción y mantenimiento de la red, así como de nombrarla y de los servicios de enlace, es decir, de las tareas necesarias de direccionamiento y seguridad. Estos mismos servicios existen para redes inalámbricas para el hogar, sin embargo representan un reto mayor por la necesidad de ahorro de energía de estas redes. Las redes que se construyan dentro de esta capa del estándar IEEE 802.15.4 deben auto organizarse y auto mantenerse para que de esta forma se reduzcan los costes totales para facilitar su uso. El estándar IEEE 802.15.4 soporta múltiples topologías para su conexión en red, entre ellas la topología tipo estrella y la topología peer-to-peer. La topología a escoger es una elección de diseño y va a estar dado por la aplicación a la que se desee orientar. Algunas aplicaciones como periféricos e interfaces de PC, requieren de conexiones de baja potencia de tipo estrella, mientras que otros como los perímetros de seguridad requieren de una mayor área de cobertura por lo que es necesario implementar una red peer-to-peer. Al final del tema hablaremos sobre los protocolos de encaminamiento.

3.3.2 *Capa de Enlace de Datos*

El proyecto IEEE 802 divide al DLL en dos subcapas, la subcapa de enlace de acceso a medios (Medium Access Control, MAC) y la de control de enlaces lógicos (Logical link control, LLC). El LLC es común a todos estándares 802, mientras que la subcapa MAC depende del hardware y varía respecto a la implementación física de esta capa. La figura 3.9 ilustra la forma en que el estándar IEEE 802.15.4 se basa en la organización internacional para la estandarización (ISO) del modelo de referencia para la interconexión de sistemas abiertos (OSI).

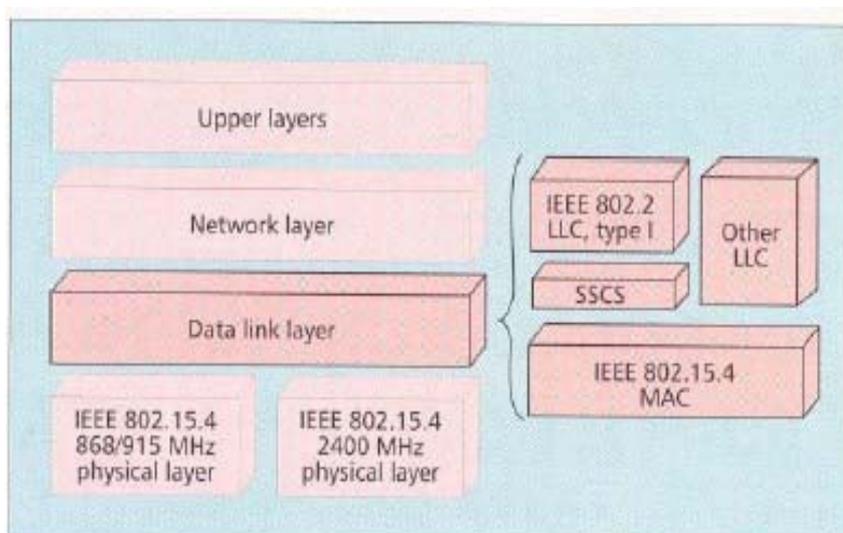


Figura 3.9 Relación del IEEE 802.15.4 con el sistema OSI

Las características del MAC IEEE 802.15.4 son: la asociación y la disociación, reconocimientos de entrega de trama, mecanismos de acceso al canal, validación de trama, garantía del manejo de las ranuras de tiempo, y manejo de guías. Las subcapas MAC proporcionan dos tipos de servicios hacia capas superiores que se acceden a través de dos puntos de acceso a servicios (SAPs). Los servicios de datos MAC se acceden por medio de la

parte común de la subcapa (MCPS-SAP), y el manejo de servicios MAC se accede por medio de la capa MAC de manejo de identidades (MLME-SAP). Esos dos servicios proporcionan una interfase entre las subcapas de convergencia de servicios específicos (SSCS) u otro LLC y las capas físicas. El administrador de servicios MAC tiene 26 primitivas, haciéndolo muy versátil para las aplicaciones hacia las que fue orientado.

3.3.2.1 *Formato General de Tramas MAC*

La unidad básica de transporte es la trama. En el estándar se definen cuatro tipos de tramas: la beacon, la trama de datos, el acknowledgment y la trama de control. En este apartado daremos unas nociones básicas sobre la funcionalidad y estructura de cada una de las tramas sin entrar en consideraciones sobre la función de cada uno de los campos.

A la trama del MAC se le denomina unidad de datos de protocolos MAC (MPDU) y se compone del encabezado MAC (MHR), unidad de servicio de datos MAC (MSDU), pie de MAC (MFR). El primer campo del encabezado de trama es el campo de control. Este indica el tipo de trama MAC que se pretende transmitir, especifica el formato y la dirección de campo y controla los mensajes reconocimiento. En pocas palabras, la trama de control especifica como es el resto de la trama de datos y que es lo que contiene.

El tamaño de las direcciones puede variar entre 0 y 20 bytes. Una trama de datos puede contener información de la fuente y del destinatario, mientras que la trama de enterado no contiene ninguna información de ninguna dirección. Por otro lado una trama de guía solo tiene información de la dirección de la fuente. Esta flexibilidad en la estructura ayuda a incrementar la eficiencia del protocolo al mantener los paquetes lo más reducido que se puede.

Las **beacons** son tramas emitidas por el coordinador de la red con fines de sincronismo, identificación de la PAN y configuración de la supertrama. En redes balizadas las beacons se emiten de forma periódica y delimitan el alcance de una supertrama. Las redes no balizadas utilizan las beacons para indicar su presencia como respuesta a una petición beacon request.

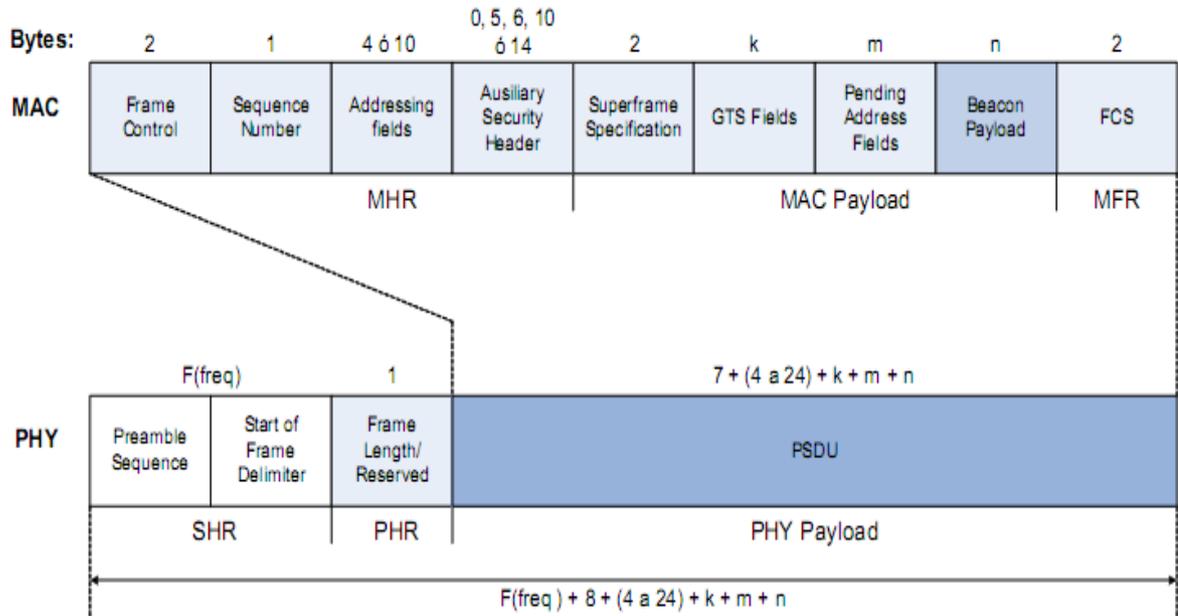


Figura 3.10 Formato de una trama *beacon* según el estándar IEEE 802.15.4

Las dimensiones de los campos Preamble Sequence y Start of Frame Delimiter vienen dadas en función de la frecuencia de trabajo. Para la banda de 2,4 GHz:

Preamble Sequence – 4 bytes (8 símbolos)

Start of Frame Delimiter – 1 byte (2 símbolos)

Las tramas de **datos** se emplean en las transferencias de información y se rigen por la siguiente estructura:

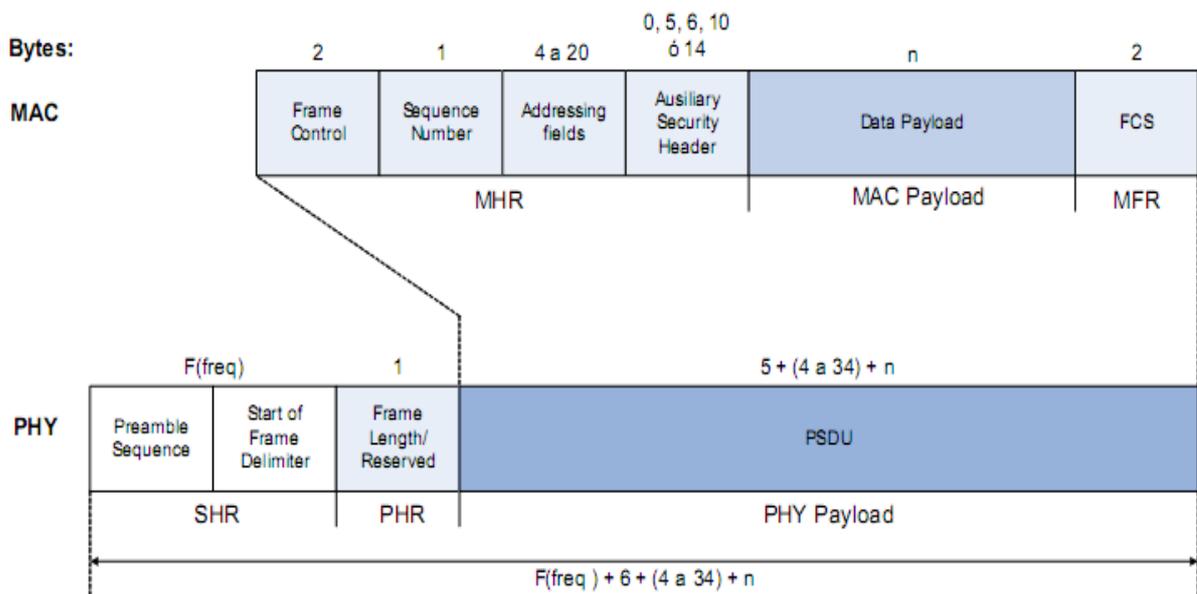


Figura 3.11 Formato de una trama de *datos* según el estándar IEEE 802.15.4

Los **acknowledgments** se envían como confirmación a una recepción correcta.

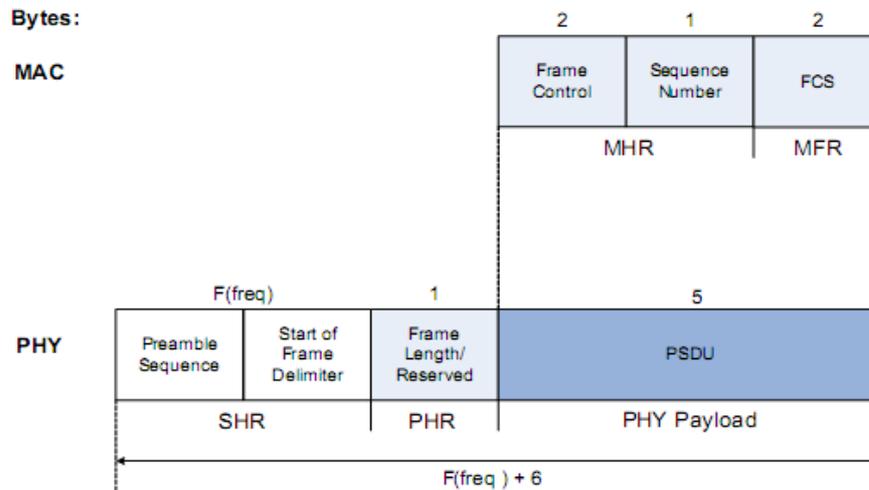


Figura 3.12 Formato de una trama *acknowledgment* según el estándar IEEE 802.15.4

Las tramas de control se utilizan para enviar órdenes de control a bajo nivel entre dispositivos. Como es lógico, un FFD debe implementar una mayor cantidad de tramas de control, en tanto que un RFD sólo está obligado a transmitir y/o recibir una serie de tramas de control selectas, suficientes para su funcionamiento correcto.

Identificador de trama de control	Nombre del comando	RFD	
		Tx	Rx
0x01	Association Request	X	
0x02	Association Response		X
0x03	Disassociation notification	X	X
0x04	Data request	X	
0x05	PAN ID conflict notification	X	
0x06	Orphan notification	X	
0x07	Beacon request		
0x08	Coordinator realignment		X
0x09	GTS request		
0x0a-0xff	Reserved		

Figura 3.13 Tramas de control

La trama de **control** se rige por la siguiente estructura de campos:

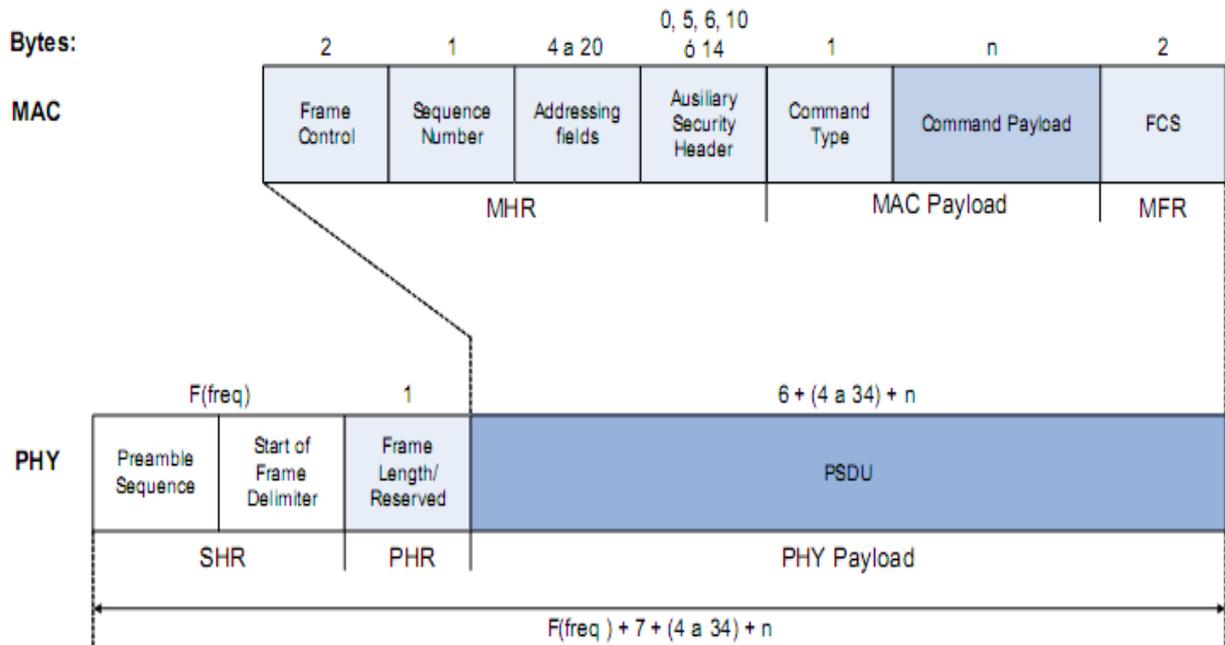


Figura 3.14 Formato de una trama de *control* según el estándar IEEE802.15.4

3.3.2.2 La estructura de las super-tramas

Algunas aplicaciones requieren anchos de banda dedicados a lograr estados latentes para un consumo de baja potencia. Para lograr dichos estados latentes el IEEE 802.15.4 se puede operar en un modo opcional llamado superestructuras (superframes).

En un superframe, un coordinador de red, denominado el coordinador PAN, transmite superframes de guía en intervalos definidos. Estos intervalos pueden ser tan cortos como unos 15 ms o tan largos como 245 s. El tiempo entre cada uno de ellos se divide en 16 ranuras de tiempo (slots) independientes a la duración de cada superframe. Un aparato o instrumento puede transmitir cuando desee durante una ranura de tiempo. Pero debe terminar su transmisión antes de la siguiente superframe.

Un superframe consiste en un periodo denominado CAP (Contention Access Period) seguido de otro periodo denominado CFP (Contention Free Period) y un periodo inactivo en el cual el coordinador puede entrar en el modo de ahorro de energía y no necesita controlar su red. Un nodo puede transmitir datos en el periodo CAP empleando el algoritmo CSMA-CA, sin embargo el coordinador de PAN puede asignar intervalos o ranuras de tiempo a un solo dispositivo que requiera un determinado ancho de banda permanentemente o transmisiones latentes bajas. Estas ranuras de tiempo asignadas son llamadas ranuras de garantía (GTS) y juntas forman el periodo de contención libre (CPF) (Fig. 3.15). El tamaño del periodo de contención libre puede variar dependiendo de la demanda de los demás aparatos asociados a la red. Cuando el GTS se utiliza, todos los dispositivos deben de completar todas sus transacciones de contención de base antes de que el periodo de contención libre comience.

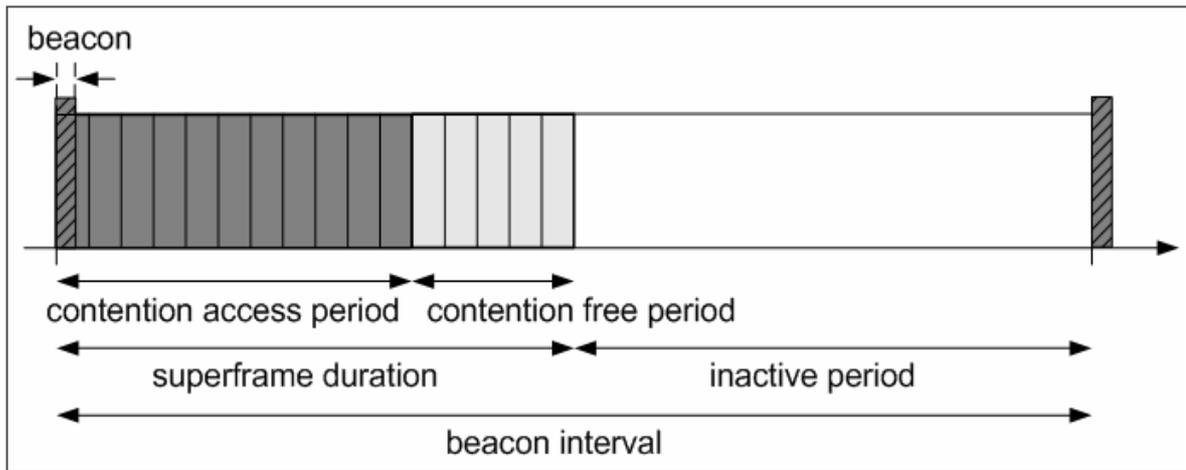


Figura 3.15 Estructura super-trama

En una red beacon-enabled, se emplea el mecanismo de acceso al canal slotted CSMA/CA, por lo que los dispositivos deben esperar a las tramas de sincronismo para transmitir datos. Cualquier dispositivo, que desee transmitir durante el periodo de acceso de contención, espera a que empiece la siguiente ranura de tiempo y después determina si algún otro dispositivo se encuentra transmitiendo en la misma ranura de tiempo. Si algún otro dispositivo se encuentra transmitiendo en dicho slot, el dispositivo se repliega a un número aleatorio de slots o indica un fallo en la conexión después de varios intentos. Además en una red beacon-enabled, las tramas de acknowledgment no utilizan CSMA. En la siguiente figura, se muestra el funcionamiento de este tipo de redes.

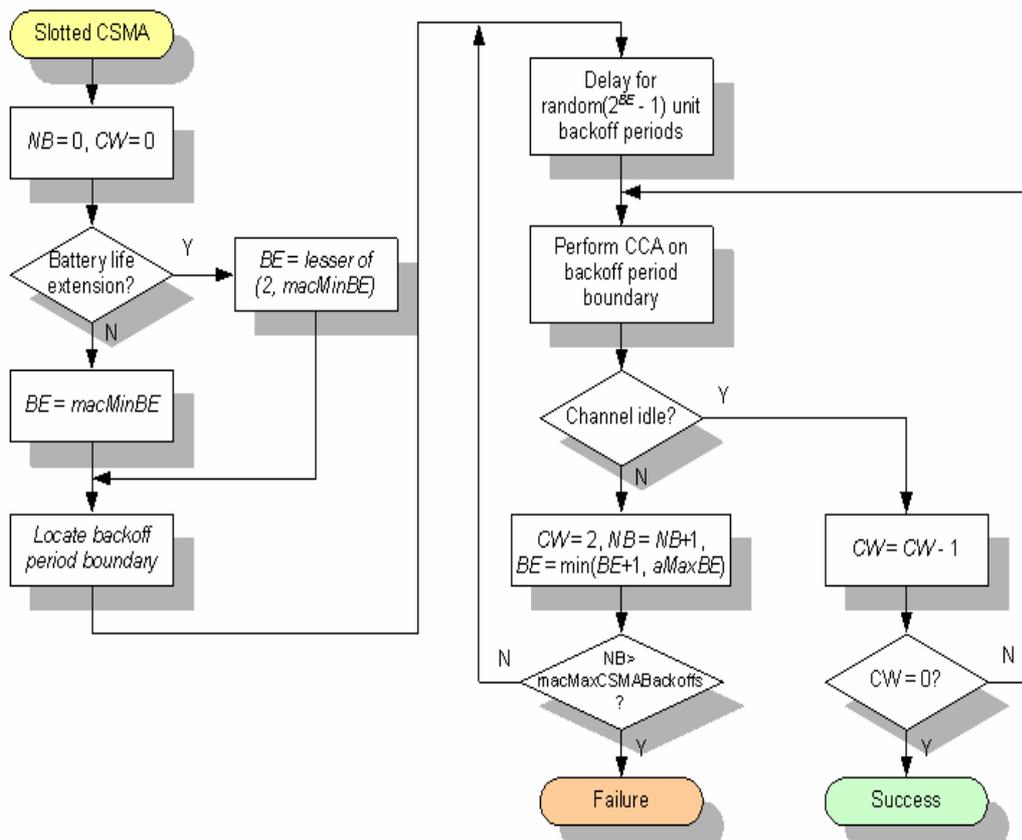


Figura 3.16 Slotted CSMA/CA

En una red non-beacon-enabled se emplea el mecanismo de acceso al canal unslotted CSMA/CA, por lo que los dispositivos no deben esperar a las tramas de sincronismo para transmitir datos. En este tipo de redes, los dispositivos están continuamente activos y a la espera de recibir paquetes, lo que requiere requisitos de potencia mayores. En la siguiente figura, se muestra el funcionamiento de este tipo de redes.

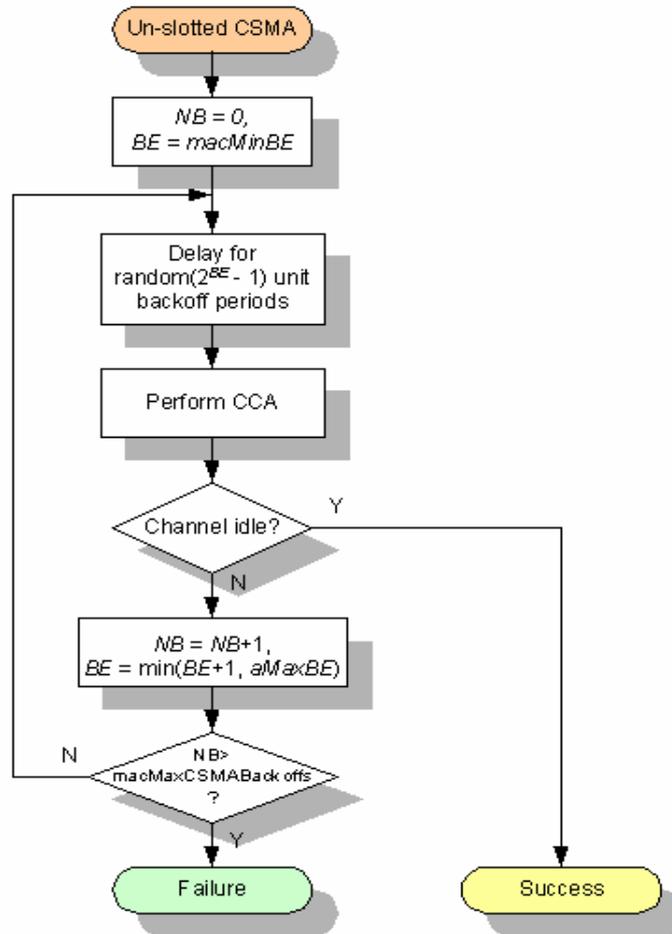


Figura 3.17 UnSlotted CSMA/CA

3.3.2.2.1 Intercambio de tramas entre dispositivos

Los intercambios de tramas entre dispositivos están perfectamente regulados en el estándar y se distinguen en tres tipos:

1-Transferencia de datos destinada al nodo coordinador

Una solicitud de comunicación con el coordinador requiere previamente de la sincronización a través de una baliza, si están habilitadas, seguida de una transmisión con CSMA-CA y una confirmación.

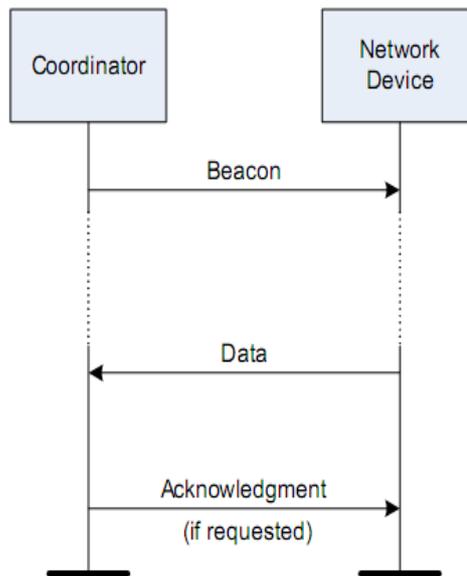


Figura 3.18 Comunicación destinada a un coordinador en redes balizadas

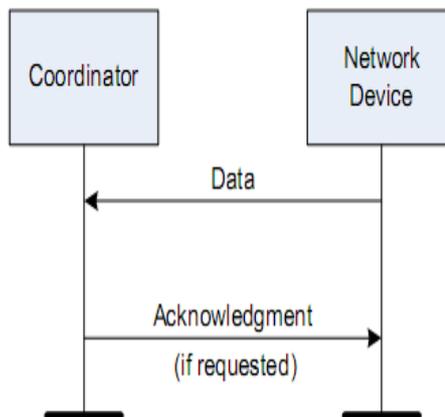


Figura 3.19 Comunicación destinada a un coordinador en redes no balizadas

2-Transferencia de datos iniciada por el nodo coordinador

En redes que emplean balizas periódicas, el nodo coordinador informa a través de la beacon que tiene datos pendientes. El dispositivo al que van destinados los datos solicita el inicio de la comunicación con un mensaje data request que indica su disponibilidad.

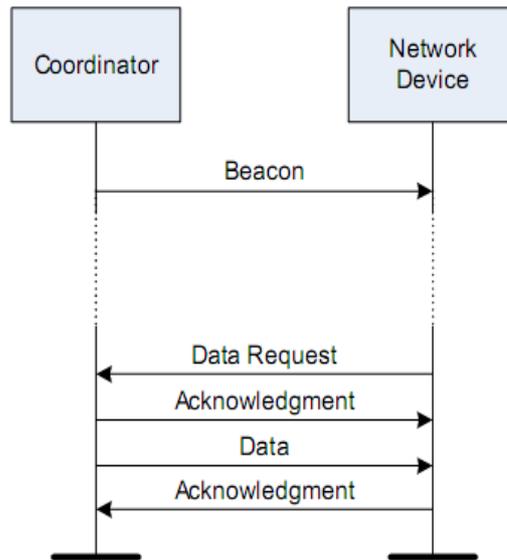


Figura 3.20 Comunicación originada en un coordinador en redes balizadas

En caso de no emplear beacons, los nodos envían data request periódicamente y el coordinador, al recibir la notificación, envía los datos pendientes o informa en la trama confirmación si no tiene información para transmitir.

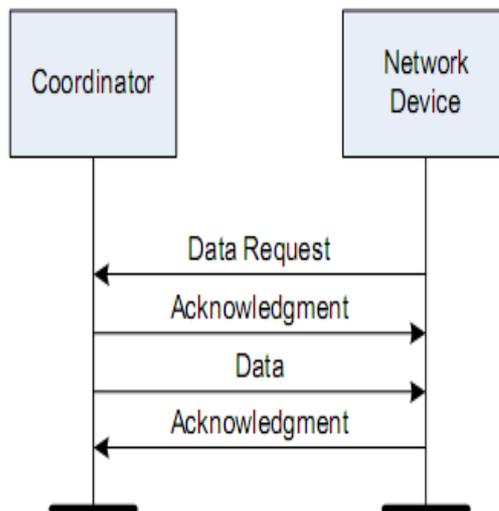


Figura 3.21 Comunicación originada en un coordinador en redes no balizadas

3-Comunicación punto a punto

En redes punto a punto cuyos dispositivos pueden comunicarse indistintamente de su clasificación lógica (coordinadores y dispositivos finales), un intercambio de tramas requiere que el nodo destinatario se encuentre permanentemente en estado de escucha o que haya un fuerte sincronismo establecido entre los miembros de una comunicación. En el primer caso, el envío de paquetes puede efectuarse normalmente a través de un CSMA-CA no ranurado. El segundo caso requiere un algoritmo de sincronismo cuya complejidad le sitúa fuera del alcance del estándar.

3.3.2.3 *Mecanismo GTS (Guaranteed Time Slot)*

GTS es un método de QoS en el sentido que permite que cada dispositivo tenga una duración específica en cada supertrama, para hacer lo que desee sin contención o latencia.

Algunas aplicaciones requieren banda ancha para conseguir latencia baja. Para acoplar estas bajas latencias, la IEEE 802.15.4 LRWPAN puede operar en modo opcional de supertrama. El tiempo entre dos beacon es dividido entre ranuras de tiempo iguales independiente de la duración de la supertrama. Un dispositivo puede transmitir en cualquier tiempo durante una ranura, pero la mayoría completa esta transmisión antes de la siguiente supertrama de beacon.

El mecanismo de GTS, asigna un periodo de libre contención para que los dispositivos que lo necesiten, transmitan sus datos sin tener que luchar por el medio mediante el algoritmo de CSMA/CA. Los slots del periodo de libre contención son asignados por el coordinador, por lo que cada nodo solo podrá transmitir en los slots asignados. De esta forma, se pueden asegurar los requisitos de ancho de banda, y lo que es más importante, los requisitos de latencia.

3.3.2.4 *Escaneo pasivo del medio*

Este mecanismo lo emplean los dispositivos para poder asociarse a un coordinador. Su funcionamiento es simple, y consiste en analizar todos los canales disponibles y comprobar si hay algún coordinador enviando beacons en dicho canal. A partir de dicho envío de beacons, se extraen parámetros de calidad de dicho coordinador y se almacenan. Una vez analizados todos los canales, se determina el coordinador que ofrece un mayor factor de calidad, y el dispositivo se asocia a dicho coordinador.

3.3.2.5 *Mecanismo de orfandad*

Tras varios intentos fallidos de comunicación dentro de un cierto tiempo, las capas superiores de la pila de protocolos pueden concluir que el dispositivo ha quedado huérfano. Dicho puede tratar de reajustarse con el grupo al que pertenecía, en cuyo caso inicia el mecanismo de orfandad.

El dispositivo huérfano debe ser capaz de buscar el coordinador al que pertenecía en el canal adecuado. Para ello genera una notificación de orfandad y se queda durante un tiempo escuchado el canal. Si el coordinador recibe una notificación de orfandad de un dispositivo huérfano que anteriormente pertenecía a su grupo, este enviará un comando para la realineación con el coordinador, para que de esta forma el dispositivo que ha quedado huérfano pueda restablecer su condición de miembro de la agrupación. Los dispositivos que reciban dichas notificaciones y comandos de orfandad, y no sean huérfanos, los ignorarán.

Si mediante el mecanismo de orfandad no se logra localizar el grupo adecuado y su coordinador, el dispositivo puede iniciar un escaneo pasivo o activo con el fin de encontrar otro grupo para unirse, o quizás empezar su propio grupo.

3.3.3 *Capa Física*

La capa física es la responsable de difundir la información por el medio de transmisión. Especifica las propiedades físicas y eléctricas de los componentes del hardware, la velocidad de transmisión y si la comunicación es unidireccional o bidireccional.

El IEEE 802.15.4 ofrece dos opciones de PHY que combinan con el MAC para permitir un amplio rango de aplicaciones en red. Ambas PHYs se basan en métodos de secuencia directa de espectro extendido (DSSS). Se utiliza DSSS debido a los bajos costes de implementación digital en circuitos integrados, y ambas comparten la misma estructura básica de paquetes low-duty-cycle con operaciones de bajo consumo de energía. La principal diferencia entre ambas PHYs radica en la banda de frecuencias. La PHY de los 2.4 GHz, especifica operación en la banda industrial, médica y científica (ISM), que prácticamente está disponible a nivel mundial, mientras que la PHY de los 868/915 MHz especifica operaciones en la banda de 865 MHz en Europa y 915 MHz en la banda ISM en Estados Unidos. Mientras que la movilidad entre países no se anticipa para la mayoría de las aplicaciones de redes en las casas, la disponibilidad internacional de la banda de los 2.4 GHz ofrece ventajas en términos de mercados más amplios y costos de manufactura más bajos. Por otro lado las bandas de 868 MHz y 915 MHz ofrecen una alternativa a la coexistencia creciente y demás interferencias (hornos de microondas, etc) asociadas a la banda de 2.4 GHz. Y mayores rangos por enlace debido a que existe menores pérdidas de propagación.

Existe una segunda distinción de las características de la PHY es el rango de transmisión. La PHY de 2.4 GHz permite un rango de transmisión de 250 kb/s, mientras que la PHY de los 868/915 MHz ofrece rangos de transmisión de 20 kb/s y 40 kb/s respectivamente. Este rango superior de transmisión en la PHY de los 2.4 GHz se atribuye principalmente a un mayor orden en la modulación, en la cual cada símbolo representa múltiples bits. Los diferentes rangos de transmisión se pueden explotar para lograr variedad de objetivos o aplicaciones. Por ejemplo la baja densidad de datos en la PHY de los 868/915 MHz se puede ocupar en lograr una mayor sensibilidad y mayores áreas de cobertura, con lo que se reduce el número de nodos requeridos para cubrir un área geográfica, mientras que el rango superior de transmisión en la PHY de los 2.4 GHz se puede utilizar para conseguir throughput mayores y poca latencia. Se espera que en cada PHY se encuentren aplicaciones adecuadas a ellas y a sus rangos de transmisión.

3.3.3.1 *Canalización*

En el IEEE 802.15.4 se definen 27 canales de frecuencia entre las tres bandas (ver figura 3.22 y 3.23). La PHY de los 868/915 MHz soporta un solo canal entre los 868 y los 868.6 MHz, y diez canales entre los 902.0 y 928.0 MHz. Debido al soporte regional de esas dos bandas de frecuencias, es muy improbable que una sola red utilice los 11 canales. Sin embargo, las dos bandas se consideran lo suficientemente cercanas en frecuencia que se puede utilizar el mismo hardware para ambos y así reducir costos de manufactura. La PHY de los 2.4 GHz soporta 16 canales entre los 2.4 y los 2.4835 GHz con un amplio espacio entre canales (5 MHz) esto con el objetivo de facilitar los requerimientos de filtrado en la transmisión y en la recepción.

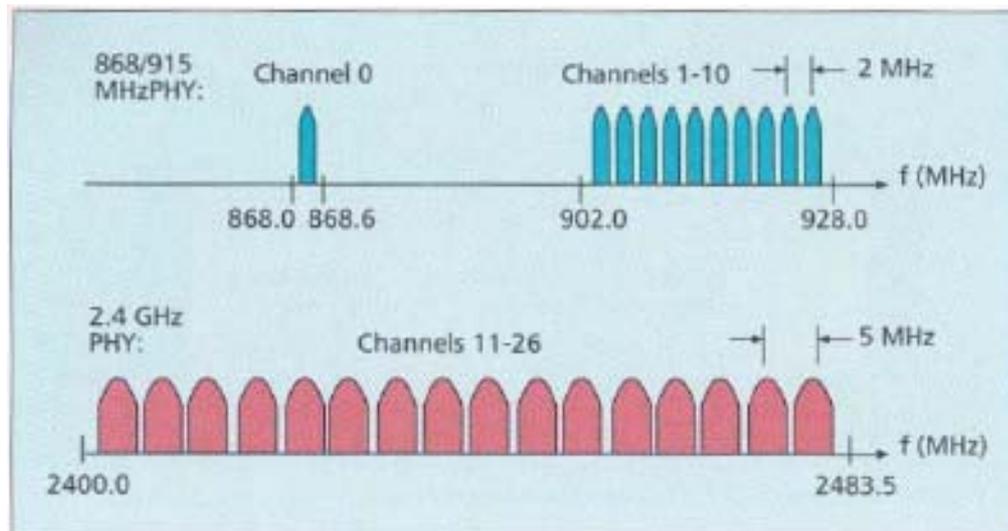


Figura 3.22 Estructura de canales del IEEE 802.15.4

Channel number	Channel center frequency (MHz)
$k = 0$	868.3
$k = 1, 2, \dots, 10$	$906 + 2(k - 1)$
$k = 11, 12, \dots, 26$	$2405 + 5(k - 11)$

Figura 3.23 Frecuencia de los canales IEEE 802.15.4

Dado que el hogar es propenso a tener múltiples redes inalámbricas trabajando en las mismas bandas de frecuencias, así como una interferencia no intencionada de las diferentes aplicaciones, la capacidad de relocalización dentro del espectro será un factor importante en el éxito de las redes inalámbricas. El estándar fue diseñado para implementar una selección dinámica de canales, a través de una selección específica de algoritmos la cual es responsabilidad de la capa de red.

La capa MAC incluye funciones de búsqueda que sigue paso a paso a través de una lista de canales permitidos en busca de una señal de guía, mientras que la PHY contiene varias funciones de bajo nivel, tales como la detección de los niveles de energía recibidos, indicadores de calidad en el enlace así como de conmutación de canales, lo que permite asignación de canales y agilidad en la selección de frecuencias. Esas funciones son utilizadas por la red para establecer su canal inicial de operación y para cambiar canales en respuesta a una pausa muy prolongada.

3.3.3.2 Estructura de trama a nivel físico

El encapsulado es la adición de información a una unidad de datos para su administración y rastreo. A nivel físico (PPDU, PHY Protocol Data Unit), el encapsulado viene definido en el estándar IEEE 802.15.4 y consta de:

- Un preámbulo de 32 bits con fines de sincronización a nivel de símbolo.
- Un byte que delimita el inicio del paquete y se utiliza en la sincronización a nivel de trama
- Un campo de 8 bits constituye la cabecera de nivel físico e indica la longitud de la PHY
- Service Data Unit (PSDU).
- Hasta 127 bytes de datos.

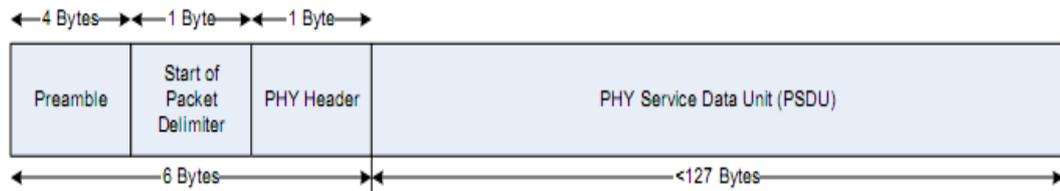


Figura 3.24 Estructura de una trama PPDU según el estándar IEEE 802.15.4

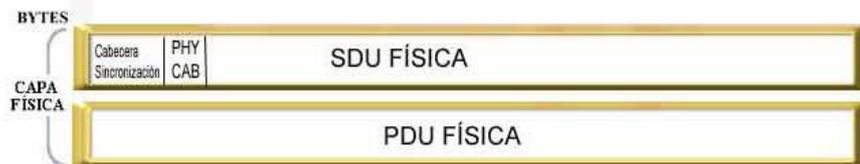


Figura 3.25 Paquete PHY

3.3.3.3 Frecuencias y modulación

La capa Física del estándar IEEE 802.15.4 especifica cuatro bandas de frecuencia, con sus modulaciones y factores de ensanchado correspondientes.

PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (Kchips/s)	Modulation	Bit rate (Kb/s)	Symbol rate (Ksímbolos/s)	Symbols
868/915	868-868,6	300	BPSK	20	20	Binary
	902-928	600	BPSK	40	40	Binary
868/915 (opcional)	868-868,6	400	ASK	250	12,5	20-bit PSSS
	902-928	1600	ASK	250	50	5-bit PSSS
868/915 (opcional)	868-868,6	400	O-QPSK	100	25	16-ary ortogonal
	902-928	1000	O-QPSK	250	62,5	16-ary ortogonal
2450	2400-2483,5	2000	O-QPSK	250	62,5	16-ary ortogonal

Figura 3.26 Frecuencias, modulaciones y parámetros de ensanchado del estándar IEEE 802.15.4

La publicación del estándar en 2003 definía las bandas obligatorias. En 2006, la revisión añadía las bandas opcionales con nuevas modulaciones y factores de ensanchado.

Las bandas de frecuencia disponibles se regulan a nivel regional. En general, la banda de 2400-2483,5 MHz es la única disponible (de la tabla anterior) a nivel mundial sin necesidad de licencias y sin limitaciones de aplicación y ciclo de trabajo. Estas consideraciones la han llevado a ser seleccionada como la banda principal del protocolo IEEE 802.15.4.

En la banda de trabajo (2,4GHz) la tasa de transferencia de 250 Kb/s es el resultado de una modulación que se rige por el diagrama:

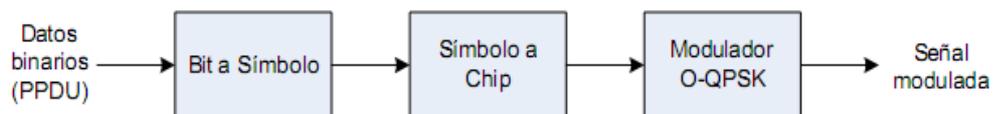


Figura 3.27 Funciones de modulación y ensanchado

Para el mapeo de símbolos se emplea la trama PPDU (PHY protocol data unit) cuya estructura detallaremos más adelante, en este mismo capítulo. Cada byte se mapea en dos símbolos, a los que se les aplica posteriormente una secuencia de ensanchado (DSSS, Direct Sequence Spread Spectrum) de 32 chips por símbolo. Finalmente, las secuencias de chip se modulan sobre la portadora utilizando una modulación O-QPSK (Offset Quadrature Phase-Shift Keying). Los chips pares se modulan sobre la portadora en fase (I), y los impares en cuadratura (Q), decalados T_c (donde T_c es la inversa de la tasa de chip, 2Mchips/s) respecto los que se transmiten en la portadora I.

Ej. Modulación del símbolo 0

Secuencia de chip correspondiente al símbolo 0:

11011001110000110101001000101110

Señal modulada en banda base:

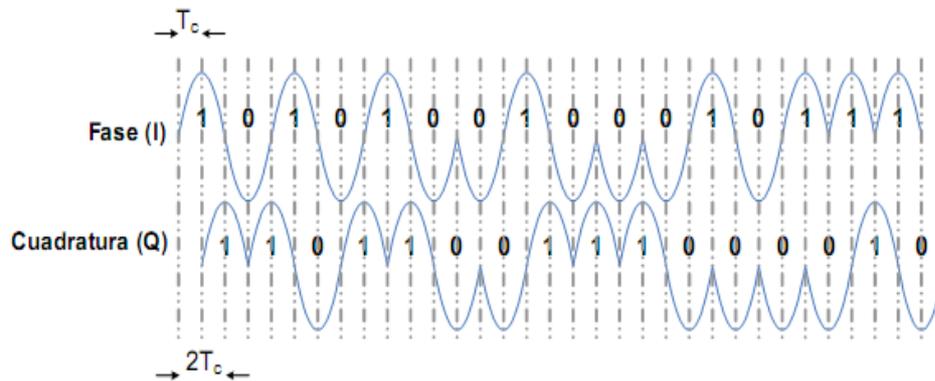


Figura 3.28 Señales I/Q moduladas en banda base de la secuencia correspondiente al símbolo 0. $T_c=0,5\mu s$

3.3.3.4 Sensitividad y Rango

Las especificaciones actuales de sensibilidad del IEEE 802.15.4 especifican -85 dBm para la PHY de los 2.4 GHz y de -92 dBm para la PHY de los 868-915 MHz. Dichos valores incluyen suficiente margen para las tolerancias que se requieren debido a las imperfecciones en la manufactura de la misma manera que permite implementar aplicaciones de bajo costo. En cada caso, los mejores artículos deben de ser del orden de 10 dB mejores que las especificaciones.

Naturalmente el rango deseado estará en función de la sensibilidad del receptor así como de la potencia del transmisor. El estándar especifica que cada dispositivo debe de ser capaz de transmitir al menos 1 mW, pero dependiendo de las necesidades de la aplicación, la potencia de transmisión puede ser mayor o menor, la potencia actual de transmisión puede ser menor o mayor (dentro de los límites de regulación establecidos). Los dispositivos típicos (1mW) se espera que cubran un rango de en tre 20-30m, sin embargo, con una buena sensibilidad y un incremento moderado en la potencia de transmisión, una red con topología tipo estrella puede proporcionar una cobertura total para una casa. Para aplicaciones que requieran mayor tiempo de latencia, la topología tipo mesh ofrecen una alternativa atractiva con coberturas caseras dado que cada dispositivo solo necesita suficiente energía para comunicarse con su vecino más cercano.

3.3.3.5 *Interferencia de y para otros dispositivos*

Los dispositivos que operan en la banda de los 2.4 Ghz pueden recibir interferencia causada por otros servicios que operan en dicha banda. Esta situación es aceptable en las aplicaciones que utilizan el estándar IEEE 802.15.4, las cuales requieren una baja calidad de servicio (QoS), no requiere comunicación asíncrona, y se espera que realice varios intentos para completar la transmisión de paquetes. Por el contrario, un requerimiento primario de las aplicaciones del IEEE 802.15.4 es una larga duración en baterías. Este objetivo se logra con poca energía de transmisión y muy pocas ciclos de servicio. Dado que los dispositivos IEEE 802.15.4 se la pasan dormidos el 99.9 por ciento del tiempo, y ocupan transmisiones de baja energía en el spread spectrum, deben estar trabajando en las vecindades de la banda de los 2.4 GHz.

Debido a que las redes de sensores inalámbricos se basan en la transmisión de señales vía radio frecuencia, es muy común que señales de este tipo penetren la red y distorsionen a información que los dispositivos están enviando y recibiendo. Este tipo de ataques se han analizado y se tienen identificados los más comunes.

Interferencia constante

Emite una señal de radio constante, y puede ser implementada utilizando un generador de señales que constantemente envía una señal de radio o un dispositivo inalámbrico que continuamente envía bits aleatoriamente a un canal sin seguir ninguna etiqueta o capa MAC (Control de Acceso al Medio).

Interferencia engañosa

En lugar de enviar aleatoriamente bits, este tipo de ataques agrega paquetes de datos en un canal sin ningún espacio entre el siguiente paquete transmitido. Como resultado, un comunicador normal será engañado pues no sabrá si deba enviar un paquete de datos, no podrá identificar si es información legal o interferencia.

Interferencia aleatoria

Alterna entre modo SLEEP e interferencias. Específicamente después de emitir interferencias, deja de emitir señales de radio y entra en modo SLEEP. Mientras está en la fase de interferencias se comporta como Interferencia Constante o Engañosa.

Interferencia reactiva

No emiten cuando el canal está inactivo, pero empiezan a transmitir una señal de radio cuando detectan actividad en el canal. Este tipo de interferencias son más difíciles de detectar, lo que se convierte en una ventaja.

A partir de esta identificación de interferencias y ataques, se han desarrollado una serie de estrategias para la detección de alguna de estas irregularidades de la red.

Detección de interferencias

En el momento se cuentan con cuatro estrategias para conocer qué tipo de interferencia está afectando el buen funcionamiento de la red.

Fuerza en la señal

La distribución de la fuerza de la señal se verá afectada en caso de una interferencia. Dos enfoques que se aproximan a la detección de interferencias usando este método, comparan la magnitud promedio de la señal con el umbral calculado del ruido del ambiente y así clasificar la forma de la señal, así tenerla como referencia en caso que se presente de nuevo ese tipo de señales de interferencia.

Tiempo de detección de envío de información

Esta estrategia resulta provechosa cuando se cumplen dos condiciones: la interferencia no es reactiva ni aleatoria y el protocolo MAC determina cuando un canal está inactivo comparando el nivel de ruido con un umbral fijo.

Proporción de entrega de paquetes de datos

Puede utilizarse para detectar la presencia de perturbaciones, como el dispositivo que emite estas interferencias corrompe las transmisiones, lleva a que éste indicador sea menor, es decir, a que se entren menor proporción de paquetes de datos en un tiempo dado.

Estrategias avanzadas de detección

Tiene que ver con estrategias multimodales como combinaciones de la anterior (Proporción de entrega de paquetes y Fuerza en la señal). En un escenario sin interferencias, una gran Fuerza en la Señal corresponde a un alto PDR (Proporción de entrega de paquetes). Sin embargo un PDR bajo además que puede ser también una señal con poco fuerza, también puede ser que existan interferencias y la señal sea fuerte pero las perturbaciones dificultan la detección de la señal.

3.4 Compatibilidad entre WIFI y ZIGBEE

Ambos estándares comparten parte del espectro y la elección de los canales debe hacerse adecuadamente para minimizar las interferencias.

En la grafica siguiente podemos ver cuanta energía y en que frecuencias opera la radio en las dos tecnologías inalámbricas. No se emite en un solo canal sino que ocupan varias bandas de frecuencia. La asignación del canal de radio se hace en el centro de la banda de frecuencias (en el centro de la joroba).

Podemos observar que el canal WiFi es más ancho que el canal Zigbee, lo que quiere decir que WiFi ocupa más espectro de radio frecuencia que Zigbee.

De la misma forma que el 802.15.4, los canales se regulan a nivel regional: en Europa están disponibles los canales 1 al 13, en tanto que en EEUU el mayor canal permitido en la banda de 2,4GHz es el 11.

En EEUU, resulta óptimo configurar las redes que trabajen con 802.15.4 en el canal 26 (incluso el 25), puesto que la banda disponible para WiFi se reduce a 2,401GHz - 2,473GHz:

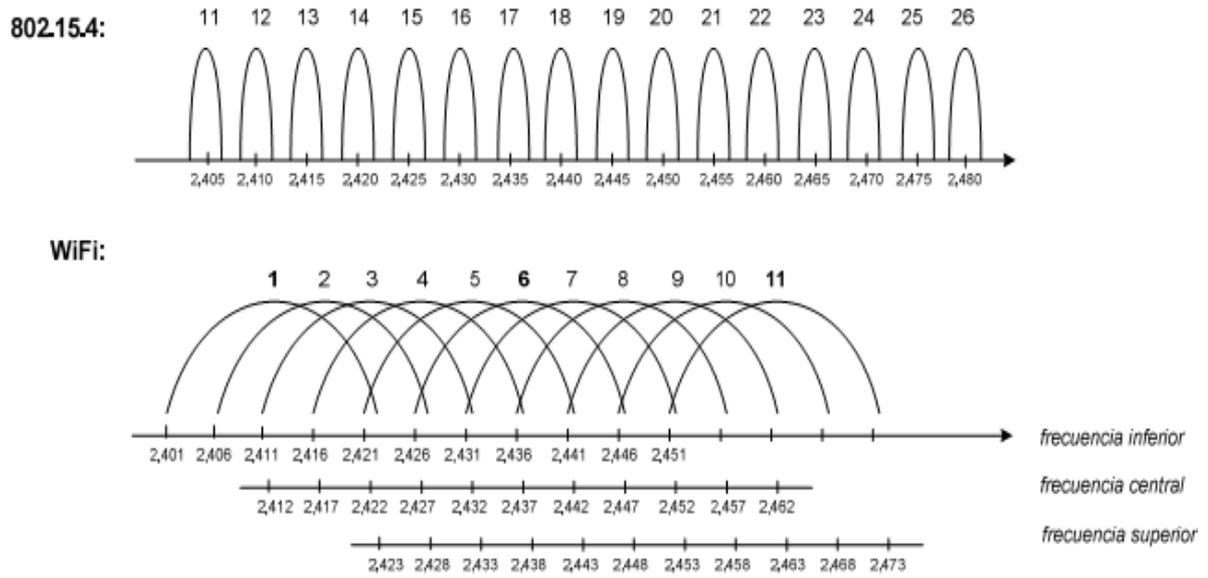


Figura 3.29 Interferencia con Wifi, regulación americana

Como podemos apreciar en la figura superior, los canales 25 y 26 no comparten banda con WiFi.

En cuanto se introducen los canales 12 y 13 (regulación europea), la banda de frecuencias que presentan interferencias crece, y es necesario realizar un mapa de asignación de canales para hallar los que presentan menor interferencia con el 802.15.4:

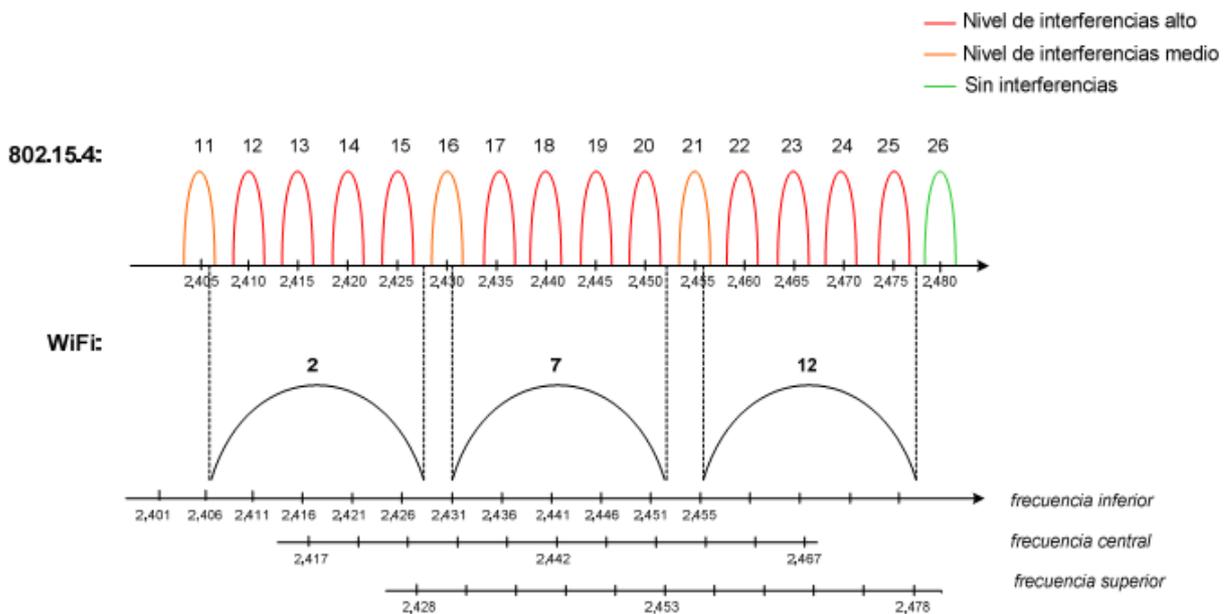


Figura 3.30 Interferencia con Wifi, regulación europea. Canales 2, 7 y 12

En la figura superior se representa el nivel de interferencias en caso de configurar la red WiFi en los canales 2, 7 y 12. Las combinaciones de canales más habituales de WiFi son: 1,6 y 11; 2, 7 y 12; 3, 8 y 13.

3.4.1 Regulación europea para la banda 2400 Mhz

Como se ha comentado antes, la gestión de frecuencias y potencias de transmisión se regulan a nivel regional. En Europa, los parámetros básicos de la capa física del protocolo 802.15.4 para la banda principal de 2,4 GHz son:

Parámetro	Especificaciones
Banda de frecuencia	2400MHz a 2483,5 MHz
Potencia transmitida	100mW ERP máximos
Modulación	O-QPSK
Símbolos	16-ario ortogonal
Tasas de transmisión	
Velocidad de bit	250 Kb/s
Velocidad de símbolo	62,5 Ksimbolos/s
Velocidad de chip	2 Mchips/s
Canales	16; $F_c = 2405 + 5 \cdot (k-11)$ MHz, para $k = 11, 12, \dots, 26$
Espaciado entre canales	5 MHz
Sensibilidad	- 85dBm (PER < 1%)

Figura 3.31 Regulación europea para la banda de 2400 MHz

3.4.2 Comparativa estándares Wireless

Estándar	Ancho de banda	Consumo de potencia	Ventajas	Aplicaciones
Wi-Fi	Hasta 54 Mbps	400 mA transmitiendo 20 mA en reposo	Gran ancho de banda	Navegar por Internet, redes de ordenadores transferencia de ficheros
Bluetooth	1 Mbps	40 mA transmitiendo 0.2mA en reposo	Interoperatividad, sustituto del cable	Wireless USB, móviles, informática doméstica
802.15.4	250 Kbps	1,8 mA transmitiendo 5,1 μ A en reposo	Batería de larga duración, bajo coste	Control remoto, productos dependientes de la batería, sensores etc.

Figura 3.32 Estándares Wireless

Comparativa entre tecnologías inalámbricas			
	Wi-fi a/b/g (802.11)	Bluetooth (802.15.1)	ZigBee (802.15.4)
Frecuencias de trabajo	2.4 GHz (b y g) / 5.0 GHz (a)	2.4 GHz	2.4 GHz, 868 MHz y 915 MHz
Tamaño de la pila	~1 Mb	~1 Mb	~20 Kb
Tasa de transferencia	54 Mbps	1 Mbps	250 kbps (2.4 GHz) 40 kbps (915 MHz) 20 kbps (868 MHz)
Número de canales	11 – 14	79	16 (2.4 GHz) 10 (915 MHz) 1 (868 MHz)
Tipo de datos	Digital	Digital, audio	Digital, texto
Cobertura entre nodos internos	100m	10m – 100m	10m – 100m
Número de dispositivos	32	8	255 / 65535
Tiempo de conexión a la red	Hasta 3s	Hasta 10s	30ms
Requisitos de alimentación / duración	Media – Horas	Media – Días	Muy Baja – Años
Consumo de potencia	400mA transmisión 20mA en reposo	40mA transmisión 0.2mA en reposo	30mA transmisión 3mA en reposo
Difusión en el mercado	Alta	Media	Baja
Arquitecturas	Estrella	Estrella	Estrella, Árbol, Punto a punto y Malla
Aplicaciones	Conexión a internet, web, email, video	Ordenadores y teléfonos móviles	Control y monitorización de bajo costo, localización
Precio	Elevado	Medio	Bajo
Complejidad	Complejo	Complejo	Simple
Puntos fuertes	Velocidad, flexibilidad	Prestaciones, coste	Robustez, consumo, coste, flexibilidad, escalabilidad

Figura 3.33 Comparativa de características entre diversas tecnologías inalámbricas

3.5 Protocolos de Encaminamiento

Los protocolos de encaminamiento nos permiten crear rutas hacia los destinos deseados. Los protocolos tradicionales propios de redes fijas no se adaptan bien a este tipo de entornos tan dinámicos y, por tanto, será necesario el diseño específico de protocolos para proporcionar un comportamiento eficiente a la red. Los criterios de diseño para una red de sensores dependen directamente de la aplicación ya que no es lo mismo la latencia para una aplicación de monitoreo, que para una aplicación de vigilancia.

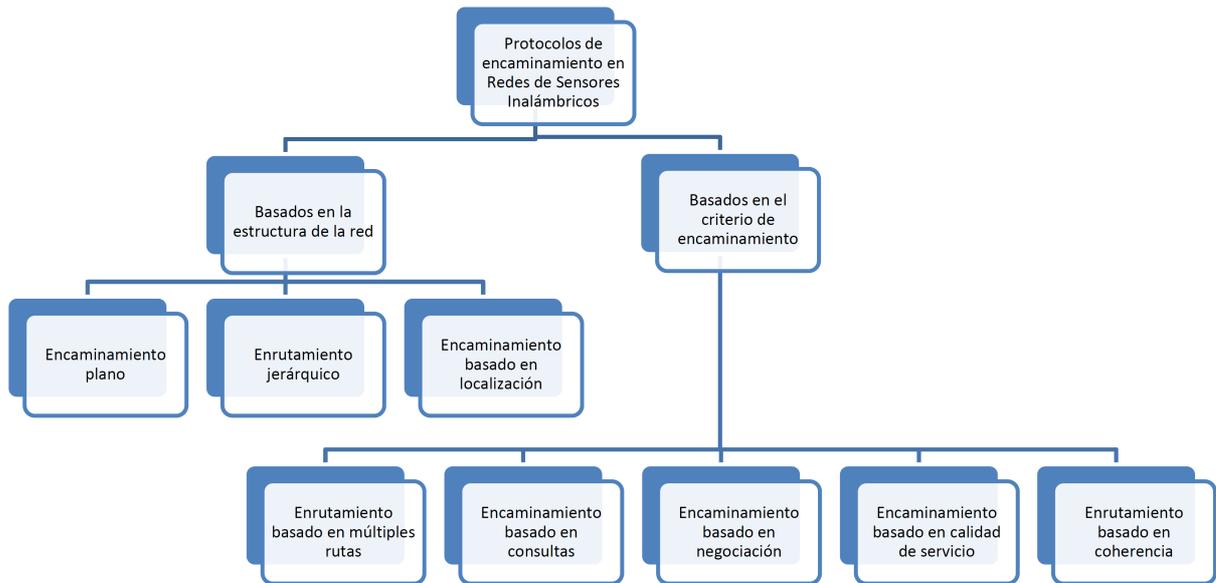


Figura 3.34 Protocolos de encaminamiento en redes de sensores inalámbricos.

Si nos fijamos en la clasificación en función de la estructura de la red encontramos tres clases distintas de protocolos de encaminamiento. Los denominados flat-based, hierachical-based y los location-based.

- Los flat-based son aquellos protocolos que asumen que todos los nodos poseen las mismas características y juegan el mismo papel dentro de la red.
- Los **hierachical-based** también se conocen como cluster-based son aquellos protocolos en los cuales los nodos juegan papeles diferentes dentro de la red, de manera que en la mayoría de casos se tiende a la creación de clusters o grupos de nodos dentro de los cuales tenemos unos nodos encargados de capturar información del entorno y otros encargados de transmitir y procesar dicha información. De esta manera se facilita la Data Agregation, la transmisión de información de múltiples sensores agregada.
- Los **Location-based** se basan en el conocimiento de la posición de cada uno de los dispositivos conformadores de la red. El direccionamiento de los nodos se realiza mediante la ubicación de cada uno de ellos y en la mayoría de estos protocolos se calcula la distancia entre nodos mediante la detección de la potencia recibida de los vecinos.

A nivel operacional se pueden encontrar cinco clases de protocolos de encaminamiento. Los multipath-based, query-based, negotiation-based, qos-based, coherent-based.

- **Multipath-based:** Los protocolos basados en multipath se basan en mantener mas de una ruta desde los nodos sensores hasta la estación base. De esta manera se consigue aumentar la tolerancia del protocolo a posibles fallos en la red. Los principales inconvenientes de estas soluciones son que acostumbran a implicar un aumento en el consumo energético y el tráfico en la red.
- **Query-based:** En este tipo de soluciones cuando una estación base desea obtener información de la red se genera una query o consulta. Esta consulta consiste en propagar un mensaje por la red de sensores de manera que cuando un nodo sensor la recibe y dispone de la información requerida la envía a través de la red hasta el origen de la consulta.
- **Negotiation-based:** Los protocolos de encaminamiento que usan mecanismos de negociación tienen por objetivo eliminar información redundante de manera que se realiza una negociación previa con el nodo al que se desea transmitir con el objetivo de transmitir solamente la información que no esta ya disponible en el nodo.
- **QoS-based:** Los protocolos de encaminamiento que implementan calidad de servicio son capaces de mantener un compromiso entre la energía consumida en la red y la calidad de la transmisión.
- **Coherent-based:** las técnicas de enrutamiento emplean diferentes técnicas de procesamiento de datos. En general, los nodos sensores cooperan entre sí en el procesamiento de datos. Los nodos que realizan el procesado se denominan agregadores. En el enrutamiento coherente, los datos se enviarán a los agregadores después de un procesamiento mínimo. El procesamiento mínimo típicamente incluye tareas como creación de marcas de tiempo y supresión de duplicados. El procesamiento coherente se selecciona normalmente para realizar un enrutamiento eficiente energéticamente.

Finalmente, se pueden clasificar los protocolos de encaminamiento en función del mecanismo utilizado para encontrar la ruta hasta el destino.

Por una parte, en los **protocolos proactivos**, periódicamente se envía información de encaminamiento para que en cualquier momento cualquier nodo pueda comunicarse con cualquier otro de la red. Esta característica proporciona una rápida respuesta ante solicitudes de ruta y ofrece un buen comportamiento en situaciones donde la tasa de movilidad es alta. Sin embargo la sobrecarga que se introduce en la red con información de control es alta como el consumo. Entre estos protocolos podemos destacar el protocolo DSDV (Destination-Sequenced Distance Vector).

Por otra parte, los **protocolos reactivos** sólo crean rutas cuando es necesario. Son protocolos bajo demanda donde la sobrecarga es mucho menor, pero los retrasos de establecimiento de rutas son mayores. Podemos nombrar AODV (Ad hoc On-Demand Distance Vector) como protocolo reactivo. Existen algunos protocolos híbridos en los que se mantiene una filosofía proactiva en un ámbito local y reactiva a nivel más global, como el protocolo ZRP (Zone Routing Protocol).

Los principales protocolos utilizados son:

- Destination-Sequenced Distance Vector (DSDV). DSDV es esencialmente una modificación del algoritmo de encaminamiento Vector Distancia Bellman-Ford desarrollado por C.Perkins y P.Bhagwat en 1994, bien conocido por su utilidad en redes fijas, como por ejemplo en el protocolo RIP. En este algoritmo, los nodos vecinos intercambian periódicamente (proactivo) sus tablas de encaminamiento enteras para estimar la distancia a la que se encuentran los demás nodos no vecinos. Las modificaciones introducidas por DSDV proporcionan básicamente la obtención de rutas sin bucles mediante la introducción de números de secuencia para la determinación de las rutas más nuevas. Aunque DSDV sólo proporciona un camino para cada destino, siempre elige el camino más corto basándose en el número de saltos hacia este destino. DSDV utiliza dos tipos de mensajes de actualización, uno más grande (full-dump) y otro mucho más pequeño (incremental). Los mensajes incrementales pueden utilizarse para actualizaciones intermedias entre envíos periódicos (full-dump) de la tabla entera de encaminamiento. Además se realizan estimaciones de los tiempos de establecimientos de ruta que retrasarán el envío de mensajes incrementales para evitar envíos en cadena de estos mensajes. La principal desventaja es la necesidad de mantener constantemente actualizadas las tablas de enrutamiento, lo que puede llegar a dar problemas por consumo de las baterías.
- Optimized Link-State Routing Algorithm (OLSR): OLSR incorpora la filosofía utilizada en protocolos tradicionales como OSPF de 'Estado de los Enlaces'. En este algoritmo todos los nodos se intercambian mensajes para formarse una visión consistente de toda la red y así poder decidir el encaminamiento de paquetes. OLSR tiene del mismo problema que DSDV debido a la necesidad de intercambio de un gran número de mensajes periódicos (proactivo). Aquí, el problema podría llegar a ser mayor, ya que además de mensajes 'hello' a los vecinos, envía mensajes de control 'tc' (Topology Control) que se retransmiten a todos los nodos de la red. Sin embargo se ha conseguido una gran optimización en la retransmisión de estos mensajes con la incorporación de la técnica de retransmisión multipunto, a través de la cual, los mensajes sólo son retransmitidos por el mínimo número de nodos necesarios para alcanzar a todos los demás. Estos nodos son conocidos como grupo de retransmisores multipunto (MPR's).
- Dynamic Source Routing (DSR): Es otro de los principales protocolos utilizados en las WSN y muy similar a AODV. El protocolo DSR se fundamenta en el encaminamiento desde el origen, es decir, los paquetes de datos incluyen una cabecera de información acerca de los nodos exactos que deben atravesar. No requiere ningún tipo de mensajes periódicos (reactivo), disminuyendo así la sobrecarga con mensajes de control. Además ofrece la posibilidad de obtener, con la solicitud de una ruta, múltiples caminos posibles hacia el destino. Tampoco son un problema, a diferencia de la mayoría de protocolos de encaminamiento en este tipo de redes, los enlaces unidireccionales. Para poder realizar el encaminamiento en el origen, a cada paquete de datos se le inserta una cabecera DSR de opciones que se colocará entre la cabecera de transporte y la IP. Entre dichas opciones se incluirá la ruta que debe seguir el paquete nodo a nodo. Cada nodo mantiene una memoria caché de rutas en la que se van almacenando las rutas obtenidas a través de procesos de descubrimiento de rutas ya sean propias o obtenidas a través de escuchas en la red. En los procesos de descubrimiento de rutas se generan mensajes de solicitud, respuesta y error siendo

estos mensajes 'route request', 'reply' y 'error' respectivamente. Contempla dos procedimientos principales que son: el descubrimiento y el mantenimiento de las rutas. El descubrimiento de rutas se inicia con un paquete Route Request, tras lo cual se realiza el intercambio de información hasta la conclusión de este procedimiento, y finaliza el procedimiento con un mensaje Route Reply generado cuando se ha alcanzado el destino final.

El procedimiento de mantenimiento de rutas se inicia cuando existe una transmisión fallida con una ruta conocida, generándose un mensaje Route Error, tras lo cual se volverá a usar el procedimiento Route Discovery para determinar una nueva ruta.

- Ad Hoc On-Demand Distance Vector (AODV): Este protocolo está pensado para ser utilizado en una red ad hoc con nodos móviles, que se caracteriza por cambios frecuentes de conectividad debido al posible movimiento de los nodos. En el protocolo AODV los nodos mantienen una tabla de encaminamiento para los destinos conocidos (empleando el algoritmo vector distancia). Inicialmente esta tabla estará formada por sus vecinos. Solamente se le añadirán destinos nuevos cuando sea necesario, es decir, cuando un nodo necesita comunicarse con otro que no está en su tabla, inicia un proceso de descubrimiento de ruta (reactivo) hacia el destino concreto. Para ello se emiten mensajes de descubrimiento de ruta 'rreq' que se van propagando entre todos los nodos de modo similar al DSR. En cambio, aquí los nodos generan una tabla de encaminamiento inversa para que puedan regresar las contestaciones 'rrep' a las solicitudes de ruta al nodo que la originó. Se recomienda el uso de mensajes 'hello' entre vecinos para determinar la conectividad, aunque para reducir el volumen de estos mensajes, sólo debe permitirse su envío a los nodos que estén transmitiendo datos. El objetivo principal de este protocolo es retransmitir el mínimo número de paquetes posible para ahorrar energía. Debemos destacar además la utilización de las técnicas de "búsqueda secuencial por anillos" y "reparación local del enlace" así como también que es capaz de proporcionar soporte multicast.

4. Mercado de las WSN

4.1 Introducción

En el año 1998 Crossbow Technologies, el mayor fabricante de nodos sensores de la actualidad y el mayor proveedor dentro de los principales grupos de investigación, puso en el mercado el primer modelo de nodo sensor o 'mote', iniciando así una evolución que continúa actualmente. Con estos nodos como hardware de referencia, la Universidad de Berkeley tiene la iniciativa más importante y la que más repercusión ha tenido: el desarrollo en el año 2003 de un sistema operativo capaz de gestionar los recursos de las motes y permitir la ejecución de aplicaciones. Este sistema operativo, denominado TinyOS es considerado en la actualidad el estándar de facto. Probablemente el éxito de TinyOS se debe a que ofreció una referencia común a los investigadores, de manera que facilitó oportunidades para que otros pudieran comenzar a trabajar y por tanto dando cohesión a las distintas soluciones.

Podemos ver la evolución del mercado según ON World, In-stat, WTRS y Harbor Research.

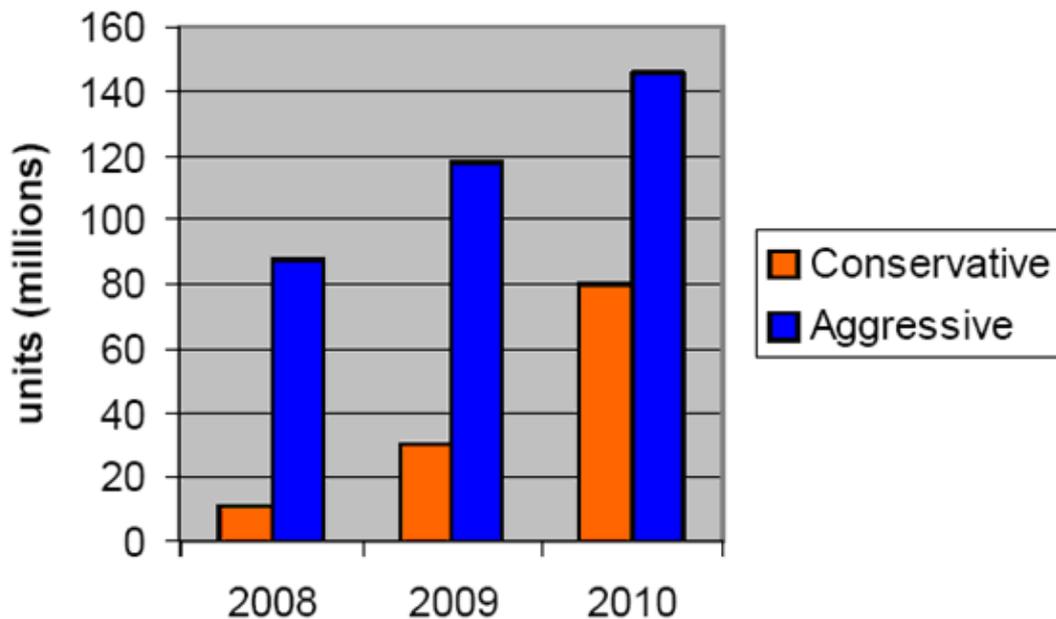


Figura 4.1: Evolución del mercado

Según un estudio realizado por On World, el mercado de redes de sensores inalámbricas está experimentando un alto crecimiento en la demanda, porque cada vez más empresas quieren instalar este tipo de red.

El estudio de ON World se llama "Wireless Sensor Networks: Growing Markets, Accelerating Demand", y está basado en los resultados de una encuesta realizada con 147 empresas. Incluye predicciones sobre producción e ingresos en ocho mercados de redes de sensores inalámbricas, además de análisis y resultados sobre motivación del sector, avances en las aplicaciones actuales de redes de sensores y las últimas tendencias del mercado.

Según la directora de investigación de ON World, durante 2005 se utilizarían al menos un millón de nodos de redes de sensores inalámbricas. Además, las redes de 500 nodos o más son cada vez más frecuentes y existen ya varios casos de miles de nodos en una sola red.

El informe concluye que existe en la actualidad una demanda ‘abrumadora’ de soluciones ofrecidas por redes de sensores inalámbricas por parte de empresas industriales. De las empresas sondeadas para el estudio, 29 por cien utilizan WSN mientras que más de 40 por cien consideran muy probable la posibilidad de que realicen pruebas piloto con redes de sensores inalámbricas dentro del próximo año y medio.

A pesar del gran futuro de esta tecnología, todavía hay barreras que hacen que muchas empresas no opten por ella.

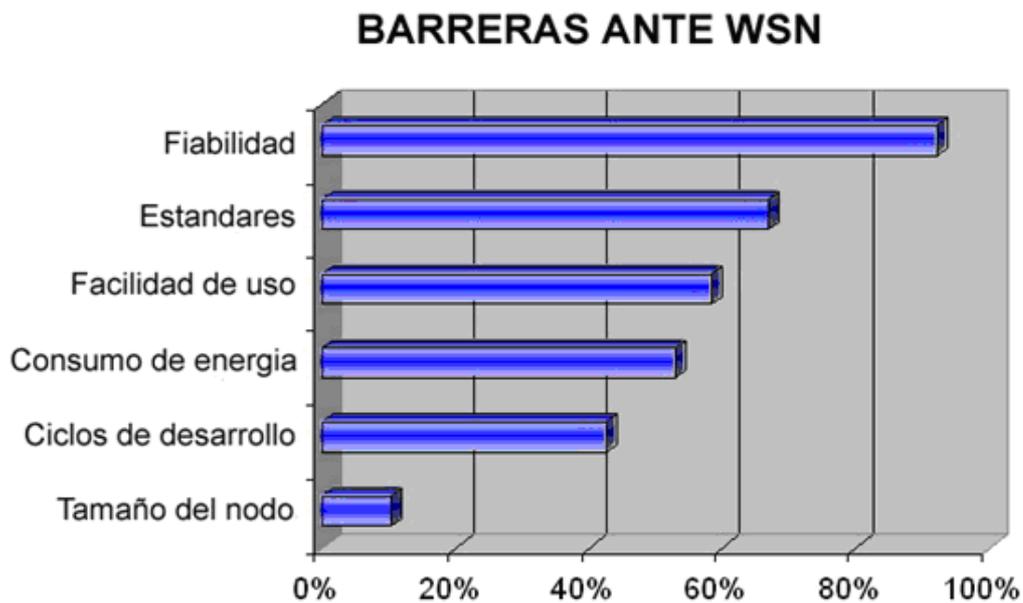


Figura 4.2: Barreras de adopción de WSN

4.2 Mercado de actualidad

Las principales casas que disponen de tecnología para redes de sensores inalámbricas son las siguientes.

CROSSBOW

La tecnología desarrollada por Crossbow ha estado a la vanguardia de la tecnología de sensores inteligentes durante más de una década y ha enviado cientos de miles de sensores inteligentes a más de 4000 clientes a lo largo del mundo. Hoy, Crossbow es el líder en cuanto a tecnología de sensores inalámbricos.



<http://www.xbow.com/>

Especializada en el mundo de los sensores, es una empresa que desarrolla plataformas hardware y software que dan soluciones para las redes de sensores inalámbricas. Entre sus productos de módulos inalámbricos podemos encontrar las plataformas Mica, Mica2, Micaz, Mica2dot, telos, telosb, Iris e Imote2. Dispone también de gran cantidad de módulos gateway y placas sensoras.

Estudian aplicaciones realizadas con estas tecnologías y más concretamente son los módulos inalámbricos de la gama MicaZ e Imote2 y los gateways MIB600 Ethernet Gateway, SPB400 Stargate Gateway, NB100 Stargate Netbridge y IIB2400 Imote2 Interface.

SENTILLA

Otra de las empresas dedicadas a las redes de sensores inalámbricas es Sentilla, también llamada anteriormente MoteIV. Es la encargada de los motes Tmote Sky, diseñados también por la Universidad de Berkeley y preparados para ser usados por TinyOS. Fue Joseph Polastre, antiguo doctorando de un grupode trabajo de esta universidad quien formó la compañía MoteIV. Ha desarrollado la plataforma Tmote Sky y Tmote Invent.



<http://www.sentilla.com/>

SHOCKFISH

Shockfish SA ha desarrollado la plataforma TinyNode pensando en aplicaciones industriales. La misión de esta empresa es hacer de puente entre la investigación académica y el mundo laboral de la industrial en el entorno de redes de sensores inalámbricos.



<http://www.shockfish.com/>

La filosofía de diseño de TinyNode es suministrar una plataforma tanto para proyectos académicos como para aplicaciones industriales. El módulo del núcleo de TinyNode 584 es un nodo sensor de bajo consumo y dispone de conectividad, almacenamiento y alimentación.

Btnode

Los módulos fabricados por BTnode han sido desarrollados por el ETH Zurich, conjuntamente por el Computer Engineering and Networks Laboratory (TIK) y el Research Group for Distributed Systems.



<http://www.btnode.ethz.ch/>

Actualmente, los BTnodes son usados en dos grandes proyectos de investigación, apoyando a la plataforma de desarrollo inicial, estos son NCCS MICS y Smart-Its.

EMBER

Ember es uno de los promotores de la Zigbee Alliance y las soluciones propuestas por esta empresa cumplen la capa física según el estándar IEEE 802.15.4.



<http://www.ember.com/>

La tecnología Ember basada en Zigbee es la adecuada para aplicaciones de redes de sensores escalables que requieran una implementación en malla de bajo consumo como automatizaciones en edificios, entre otras.

SUN

Sun SPOT (Sun Small Programmable Object Technology) es un mote para WSN desarrollado por Sun Microsystems. El aparato está construido bajo la normativa estándar IEEE 802.15.4. Al contrario de otros nodos inalámbricos, el Sun SPOT está construido bajo la máquina virtual Java Squawk.



<http://www.sunspotworld.com/>

Nano-RK

La casa Nano-RK ha desarrollado la plataforma FireFly como una plataforma de nodos inalámbricos de bajo consumo y bajo coste, con la idea de dar el mejor soporte en aplicaciones en tiempo real.



<http://www.nanork.org/>

4.2.1 Comparativa de Nodos Inalámbricos

En la siguiente tabla podemos comparar las principales características de varios de los nodos inalámbricos de las marcas comentadas anteriormente.

Nombre	Casa	Microcontrolador	Transmisor	Memoria Programas y datos	Memoria externa	Programación	Comentarios
EM250	Ember	12MHz XAP2b 16-bit	2.4GHz IEEE 802.15.4 Compliant Transceiver	5kB RAM	128kB Flash	C	
Mica	Crossbow	Atmel ATMEGA103 4 MHz 8-bit CPU	RFM TR1000 radio 50 kbit/s	128+4K RAM	512K Flash	nesC Programming	TinyOS Support
Mica2	Crossbow	ATMEGA 128L	Chipcon 868/916 MHz	4K RAM	128K Flash		TinyOS, SOS and MantisOS Support
Mica2Dot	Crossbow	ATMEGA 128		4K RAM	128K Flash		
MicaZ	Crossbow	ATMEGA 128	TI CC2420 802.15.4/ZigBee compliant radio	4K RAM	128K Flash	nesC	TinyOS, SOS, MantisOS and Nano-RK Support
Telos	Crossbow	Motorola HCS08		4K RAM			Contiki, TinyOS, SOS and MantisOS Support
TelosB	Crossbow	Texas Instruments MSP430 microcontroller	250 kbit/s 2.4 GHz IEEE 802.15.4 Chipcon Wireless Transceiver	10k RAM	48k Flash		Contiki, TinyOS, SOS and MantisOS Support
T-Mote Sky	Sentilla	Texas Instruments MSP430 microcontroller	250 kbit/s 2.4 GHz IEEE 802.15.4 Chipcon Wireless Transceiver	10k RAM	48k Flash		Contiki, TinyOS, SOS and MantisOS Support
IMote	Intel	ARM core 12 MHz	Bluetooth with the range of 30 m	64K SRAM	512K Flash		TinyOS Support
IMote 1.0	Intel	ARM 7TDMI 12-48 MHz	Bluetooth with the range of 30 m	64K SRAM	512K Flash		TinyOS Support
IMote 2.0	Crossbow	Marvel PXA271 ARM 11-400 MHz	TI CC2420 802.15.4/ZigBee compliant radio	32MB SRAM	32MB Flash		Microsoft .NET Micro, Linux, TinyOS Support
Iris	Crossbow	ATmega1281	Atmel AT86RF230 802.15.4/ZigBee compliant radio	8K RAM	128K Flash		nesC TinyOS, MoteWorks Support
SunSPOT	Sun Microsystems	ARM 920T	802.15.4	512K RAM	4 MB Flash		Java Squawk J2ME Virtual Machine Nano-RK RTOS Support
FireFly	Nano-RK	Atmel ATmega 1281	Chipcon CC2420	8K RAM	128K FLASH ROM, 4K EEPROM	C Programming	
BTNode rev.3	BTNode	Atmel ATmega 128L	Bluetooth subsystem: Zeevo ZV4002, supporting AFH/SFH	64+180 Kbyte RAM	128 Kbyte FLASH ROM, 4 Kbyte EEPROM	Standard C Programming	TinyOS Support
eyesIFXv2.1	BTNode	Texas Instruments MSP430F1611	Infineon TDA5250	10 KB RAM	48 KB FLASH		

Figura 4.3: Comparativa de nodos inalámbricos

4.3 Empresas destacadas

4.3.1 Libelium

Libelium es una empresa de diseño y fabricación de hardware para la implementación de redes sensoriales inalámbricas, redes malladas y protocolos de comunicación para todo tipo de redes inalámbricas distribuidas. El equipo de I+D está formado por ingenieros especializados en las ramas de telecomunicaciones, informática, electrónica y diseño industrial.

Sus instalaciones se encuentran en el Centro Europeo de Empresas e Innovación CEEIARAGON. Actualmente disfrutan de la calificación Spin Off de la Universidad de Zaragoza, como prueba del carácter innovador de sus investigaciones y de la de Empresa Innovadora de Base Tecnológica reconocida por Ances. En tan sólo un año, han conseguido que sus desarrollos estén presentes en empresas, universidades y centros de investigación de más de 40 países en los cinco continentes. En Agosto de 2008 recibieron la concesión de la ayuda NEOTEC, financiación necesaria para el desarrollo y salida al mercado de nuevos productos de Libelium.

Sus principales líneas de investigación y desarrollo son:

–Waspnote: dispositivo sensorial de bajo consumo para la creación de redes sensoriales inalámbricas.

–Meshlium: único router multitecnología que integra en una máquina las tecnologías Wifimesh (2.4GHz - 5GHz), ZigBee, GPRS, GPS y Bluetooth.

–N-vio: plataforma de marketing de proximidad y envío de mensajes por Bluetooth.

En la actualidad lideran el grupo de trabajo RedSens embebido en el marco de trabajo de la Asociación de Empresas de Electrónica, Tecnologías de la Información y Telecomunicaciones de España, formado por las principales empresas españolas dedicadas al sector de las telecomunicaciones y la electrónica.

Han recibido numerosos premios por su actividad emprendedora y sus desarrollos innovadores.

Mejor Proyecto de Investigación 2006

"Red sensorial para la detección precoz de incendios forestales" (Consejo Económico y Social de Aragón)

Bancaja Jóvenes Emprendedores 2006

IDEA

Categoría Sociedad de la información 2006 (Fundación Emprender en Aragón)

Vivero SIMO 2007

Empresa seleccionada (SIMO y Fundetec)

Generación XXI 2007

(LUA multimedia y Fundación Emprender en Aragón)

Networking Activo 2007

Redes Sociales con Bluetooth

Aster 2008

Mejor Emprendedor (ESIC)

Premio empresa junior 2009

Asociación de Ingenieros de Telecomunicación de Aragón

Emprendedor XXI 2009

EIBT 2009

Mejor Empresa de Reciente Creación (ANCES)

Bancaja Empresas Base Tecnológica 2009

Premio "Best of Sensors Expo" 2010

Categoría "Adquisición de Datos" para Waspote

Noticia de actualidad (Diciembre de 2009)

La empresa aragonesa Libelium acaba de hacer pública una nueva plataforma de dispositivos para la creación de Redes Sensoriales Inalámbricas. Estas redes permiten controlar por medio de cientos de sensores interconectados inalámbricamente lo que está sucediendo en tiempo real en un entorno determinado. Entre otras cosas permiten detectar incendios forestales cuando son colocados en las copas de los árboles, o incluso las crecidas repentinas del nivel del agua cuando se despliegan por las orillas de los ríos.

En entornos urbanos encuentran varios campos de actuación. Por un lado, en la detección de calidad del ambiente, puesto que permiten medir la cantidad de agentes contaminantes tales como CO, CO₂. Por otro lado, posibilitan la creación de redes de control energético "smart metering" que permiten conocer la energía que se está utilizando en un punto determinado y disminuir así consumos no necesarios.

Estos dispositivos sensoriales se comunican entre sí mediante sistemas inalámbricos de distintas frecuencias, lo que les permite evitar las interferencias que causan las redes Wifi en entornos urbanos.

Para disminuir el consumo de las comunicaciones se han creado protocolos basados en los mecanismos de comunicación usados por enjambres de insectos tales como abejas y luciérnagas. El concepto es que toda la red esté sincronizada de forma que todos los dispositivos sensoriales sean capaces de enviarse la información al mismo tiempo.

Este concepto ha sido bautizado por Libelium como "el latir de la red", según explica David Gascón, Director de I+D de Libelium y responsable directo de la nueva plataforma sensorial.

Waspote es el resultado de 2 años de investigación por parte de Libelium, empresa de diseño y fabricación de hardware para la implementación de redes sensoriales inalámbricas, redes malladas y protocolos de comunicación para todo tipo de redes inalámbricas distribuidas. XX"El mayor reto de esta plataforma ha sido disminuir el consumo de los dispositivos al mínimo, mientras que se aumentaban sus posibilidades comunicación y de integración de nuevos sensores. Los resultados han sido un éxito. Un consumo de tan solo 0.7 micro amperios en estado de reposo permiten a los nodos sensoriales vivir durante años ininterrumpidamente. Por otro lado, la integración módulos de comunicación de alta sensibilidad permiten una comunicación de varios kilómetros entre los dispositivos", apunta David Gascón.

La idea final de la plataforma sensorial Waspote es que sea usada por empresas de todo el mundo de forma que puedan crear soluciones específicas en mercados verticales. Para ello, Libelium completa esta plataforma con una extensa documentación y ayuda técnica, de cara a facilitar el desarrollo de proyectos y nuevas plataformas de servicios por terceras empresas. Bajo el lema "Think, Develop, Go!", Libelium intenta incentivar la creatividad del resto del mercado tecnológico y apoyar el surgimiento de nuevos productos y formas de negocio.

4.3.2 Jennic

Jennic es una compañía de semiconductores líder en la revolución de la conectividad inalámbrica, proporcionando microcontroladores inalámbrica para una amplia gama de aplicaciones de la energía, el medio ambiente, seguimiento de activos y mercados de consumo.

Los productos de la compañía incluyen la más baja potencia de microcontroladores de última generación inalámbrica, módulos, plataformas de desarrollo, el protocolo y software de aplicación, con especial atención a IEEE802.15.4, ZigBee y normas 6LoWPAN.

Con sede en Sheffield, Reino Unido, Jennic ofrece ventas de primera clase y un apoyo mundial.

Uno de los modelos más destacados de Jennic es el JN5121-xxx-M00, que es un módulo de montaje superficial que permite a los usuarios implementar sistemas de IEEE802.15.4 con el mínimo tiempo al mercado y al menor coste. Se elimina la necesidad de un desarrollo largo y costoso de la tarjetas de radiofrecuencia y suites de prueba. El módulo JN5121 utiliza un microcontrolador Jennic inalámbrico para proporcionar una solución completa, incluyendo todos los componentes de RF. Todo lo que se requiere para desarrollar y fabricar el control inalámbrico o productos de detección es conectar una fuente de alimentación y periféricos tales como interruptores, actuadores o sensores, lo que simplifica considerablemente el desarrollo de productos.

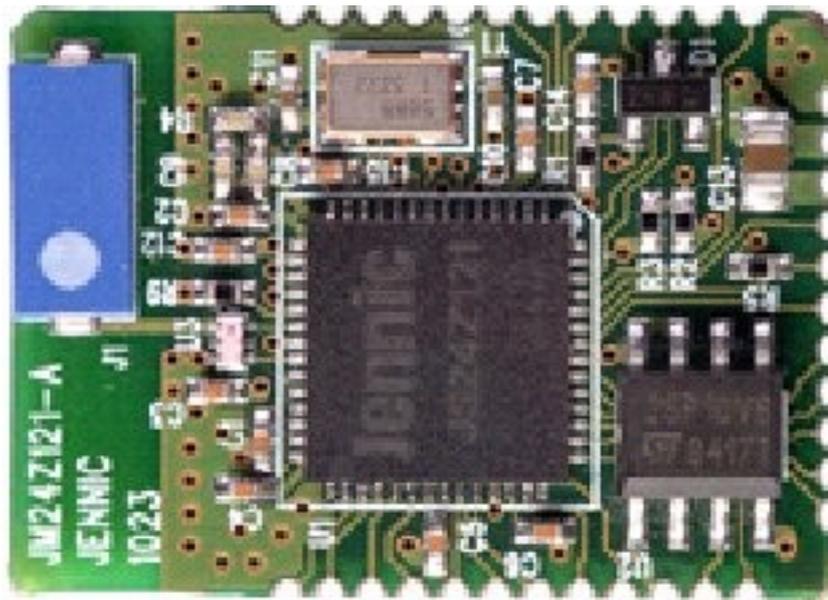


Figura 4.4: Dispositivo JN5121

El JN5121 es la primera serie de microcontroladores inalámbricos monochip, de bajo coste y bajo consumo y que se basa en el estándar IEEE802.15.4 en la banda de 2,4 Ghz. Se trata de un microcontrolador de 32 bits, 16 Mhz con arquitectura RISC, 64K de ROM, 96K de RAM, 128 bytes de RAM no volátil además de periféricos: 21 E/S digitales, 4 entradas y 2 salidas analógicas, 2 puertos serie. La implementación de la capa MAC del estándar IEEE802.15.4 se realiza mediante Hw, liberando al uC de esta tarea. Software de desarrollo y evaluación disponibles con opción de protocolos ZigBee.

4.4 Actualidad y líneas futuras

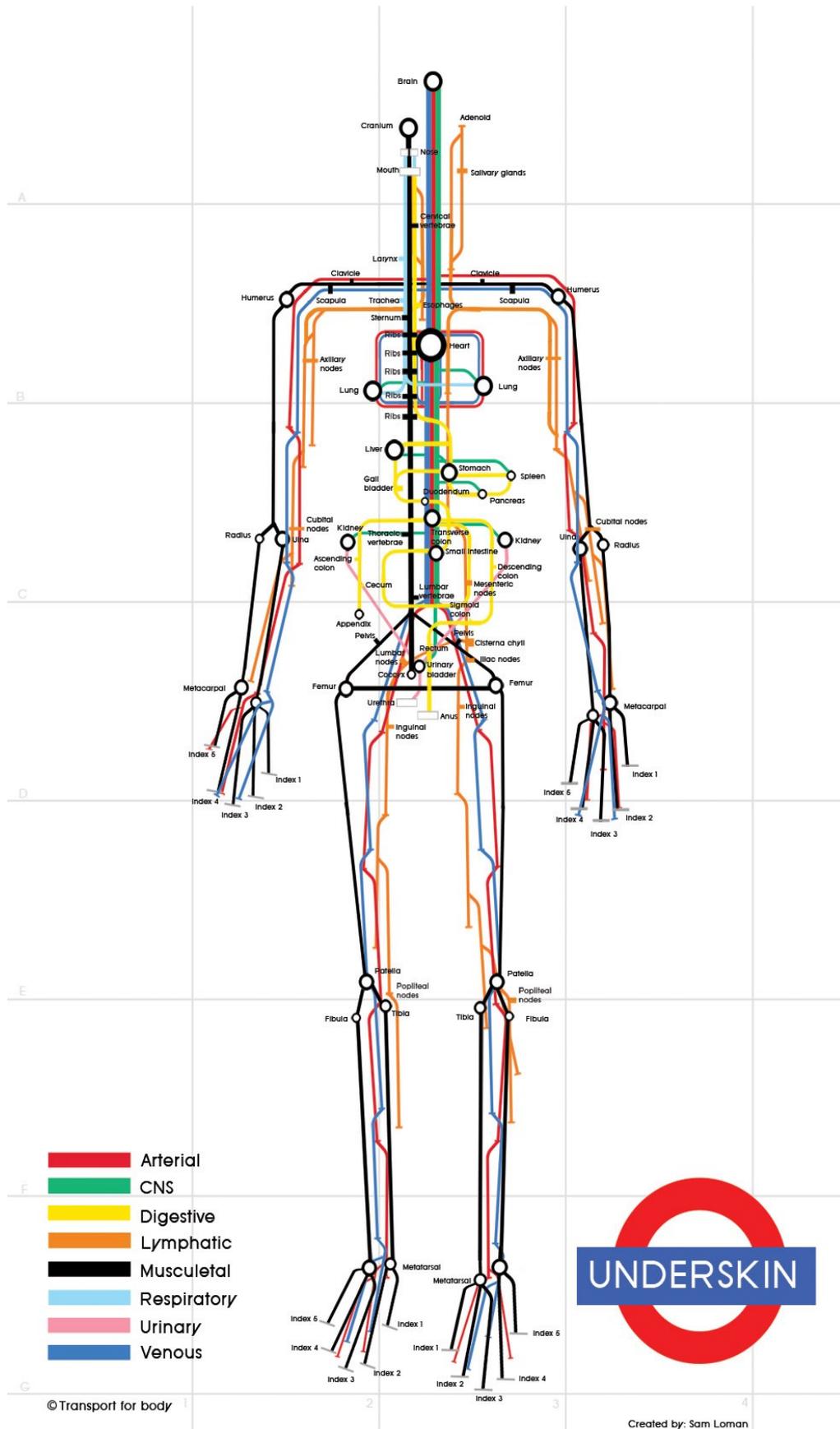


Figura 4.5: Sensores en el organismo

Proyecto SenseWeb de Microsoft

Con **SenseWeb** nos encontramos ante un desarrollo nacido de Microsoft que pretende crear aplicaciones que permitan visualizar de forma sencilla y eficaz datos procedentes de redes de sensores. De momento, se ha presentado un modelo de mapa de sensores y diversos documentos y vídeos que muestran hacia dónde camina este desarrollo, una vuelta de tuerca más al apasionante mundo de las redes de sensores asociadas a software GIS:

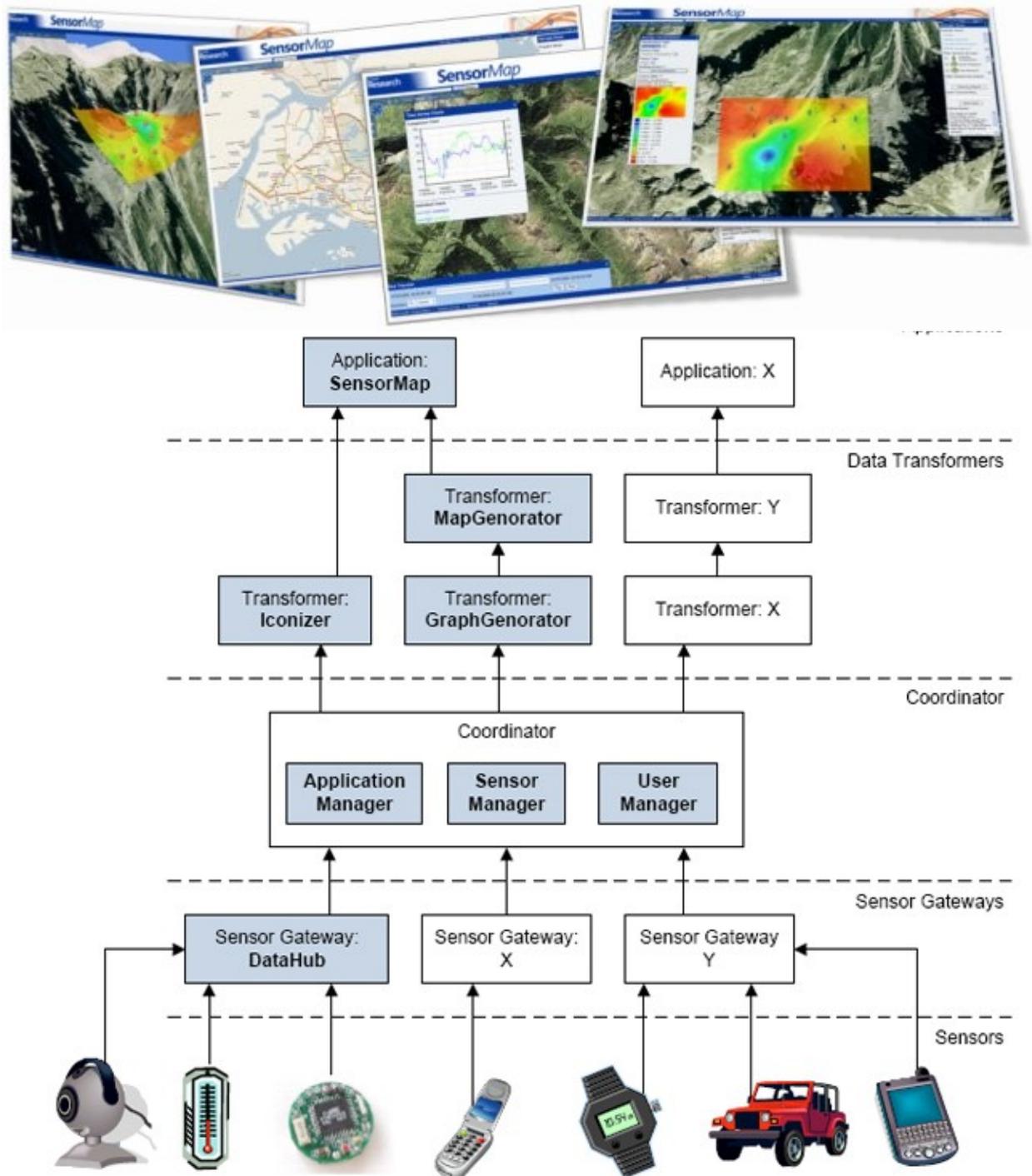


Figura 4.6: Esquema de SenseWeb

El futuro del marketing y TV, biometría para vender más

Aunque nadie parece saber cómo funcionan los rankings de audiencia ni cómo se miden, seguro que no colocan sensores en los espectadores para medir sus constantes vitales en respuesta a lo que ven por pantalla.

Pues eso es lo que ha hecho la revista Wired durante la última Super Bowl. Para ello midieron tres parámetros: la conductancia de la piel (o sudoración), el ritmo cardíaco y la actividad. La combinación de estas medidas la llamaron algo así como “enganche” con el spot que se estaba emitiendo. Los resultados pueden verse superpuestos sobre los anuncios que se emitieron, siendo el del juego Dante’s Inferno el que mayor interés despertó.



Figura 4.7: Sensado emocional de anuncios

Redes inalámbricas para ver a través de las paredes

Científicos de la Universidad de Utah, en Estados Unidos, afirman que la forma en que varían las trayectorias de las señales de radio de cualquier red inalámbrica puede revelar el movimiento de las personas situadas en dicha red, y dentro de un espacio cerrado. Según informa la revista Technology Review, la técnica ha sido ya probada con una red formada por 34 nodos, de estándar IEEE 802.15.4, que es normalmente utilizado para definir el nivel físico y el control de acceso a redes inalámbricas de área personal con tasas bajas de transmisión de datos. La técnica ha demostrado ser efectiva, aunque puede mejorar.

La base de dicha técnica es la siguiente: la potencia de las señales de las redes inalámbricas es la suma de todas las trayectorias que las ondas de radio siguen para llegar hasta un receptor. Los cambios en el volumen de espacio a través del que circulan las señales ocasionan una variación en la potencia de éstas. Estos cambios pueden ser producidos, por ejemplo, por el movimiento de las personas que se encuentren dentro de las trayectorias de dichas señales. Por tanto, observando el volumen del espacio de muchas señales, que son recogidas por múltiples receptores, es posible construir una imagen de los movimientos que se estén produciendo dentro del ámbito de la red inalámbrica en funcionamiento.

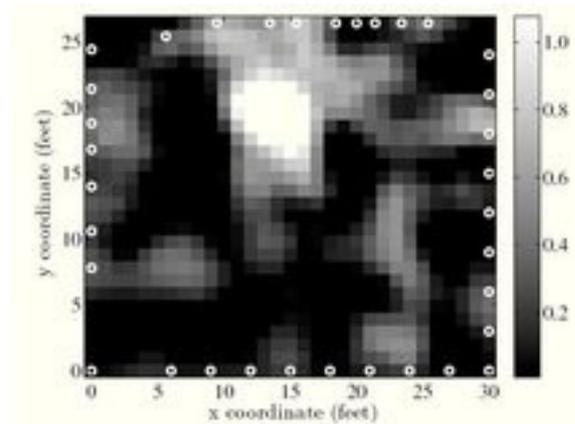


Figura 4.8: Representación visual a través de paredes

Nintendo Wii hace de la pulsioximetría un juego (June 6, 2009)

Nintendo ha anunciado en la exposición E3 que van a lanzar un pulsioxímetro para la Wii. Lo van a llamar Wii Vitality Sensor y comentan que el dispositivo “inicialmente medirá el pulso del usuario y otras señales corporales”. Esas otras señales (en plural) del cuerpo sólo puede significar la saturación de oxígeno en la sangre (singular), pero será interesante cómo Nintendo usa estos dos indicadores vitales en un juego.

De acuerdo con la nota de prensa de la compañía japonesa, “Nintendo quiere ofrecer información al usuario sobre su mundo interior”. Una posible aplicación de interés sería en combinación con la Wii Fit, en programas de rehabilitación médica, etc.

O tal vez para ofrecer un final alternativo a Resident Evil. “Tu pulso es demasiado alto. Demasiado débil y asustado...GAME OVER”



Figura 4.9: Pulsioximetría con Wii

Pachube: el youtube de los sensores

Pachube es un servicio Web que permite compartir en tiempo real información proveniente de objetos equipados con tags, o sensores; ya sea una persona, o un objeto en cualquier parte del mundo. El objetivo es facilitar la interacción entre entornos remotos, tanto físicos como virtuales.

Pachube es un poco como Youtube, sólo que, en vez de compartir videos, este servicio permite monitorizar y compartir información del entorno en tiempo real proveniente de sensores con conexión a Internet. Pachube hace de mediador entre entornos, sirviendo de entrada (capturar información de sensores remotos), como de salida (sobre actuadores remotos).

Un servicio así permitiría también crear un blog donde los datos de los sensores son los que “escriben” la propia página.

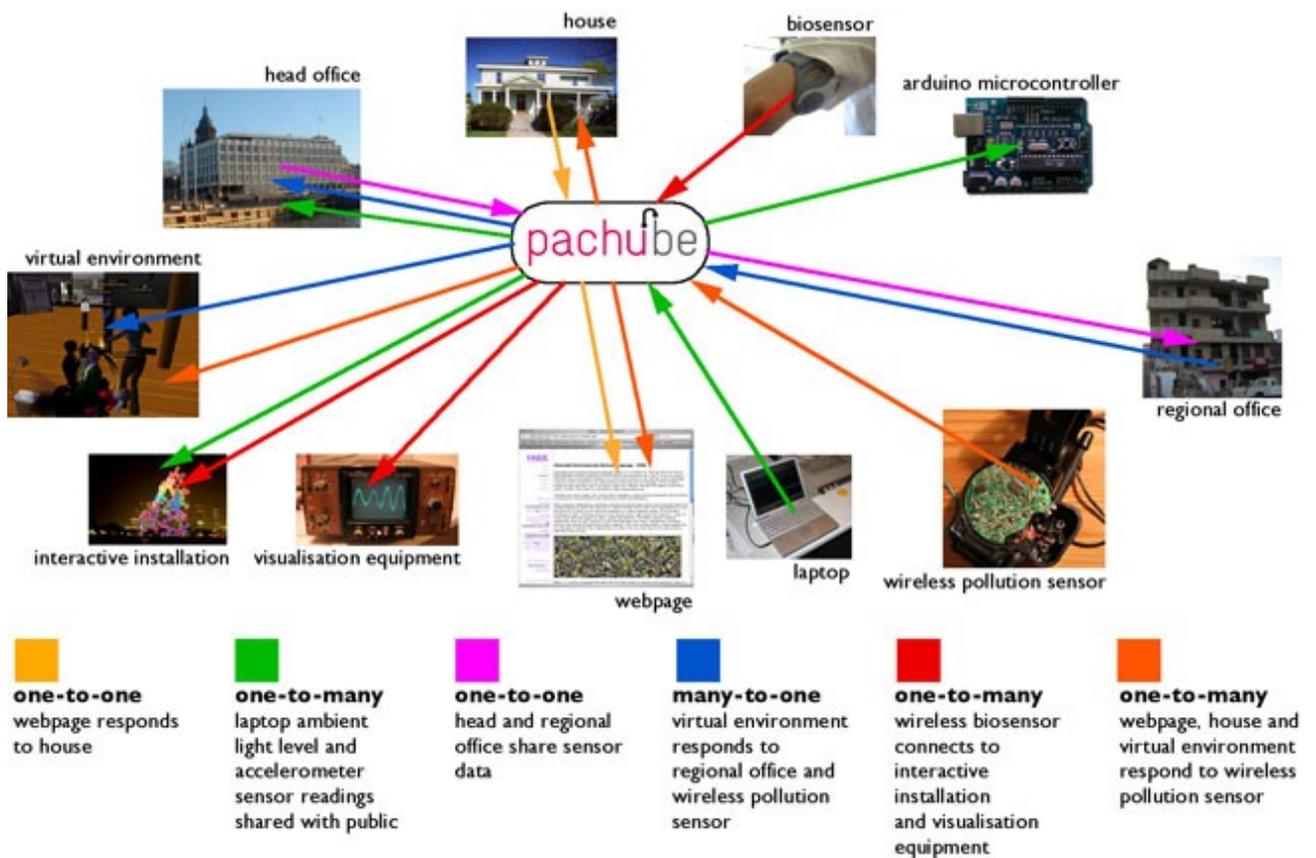


Figura 4.10: Servicios Pachube

5. Conclusiones

Tras haber estudiado a fondo las redes de sensores inalámbricos observamos que son una mejora bastante evidente frente a las tradicionales redes wireless, debido a varios factores como son: la durabilidad del tiempo de vida de las baterías, lo cual permite una mayor portabilidad de los nodos sensores y que estos puedan registrar mayores sucesos al poder permanecer más tiempo en ciertos lugares, los protocolos de encaminamiento de las redes de sensores permiten que aparte de ganar en cuanto a durabilidad también se gane en eficiencia a la hora de evitar colisiones entre paquetes, lo que asegura también un menor número de tráfico innecesario en la red, y en cuanto al precio cada vez más se está equiparando el desembolso para la construcción de una red wireless frente a una red de sensores inalámbricos, por lo que es una competencia directa.

Debido a las excelentes características de este tipo de redes, en la actualidad se están utilizando las redes de sensores en infinidad de proyectos relacionados con distintos campos como pueden ser: medio ambiente, salud, el ámbito militar, construcción y estructuras, automoción, domótica, agricultura, etc. Gracias a la utilización de esta tecnología en los diversos campos se está alcanzando un mayor nivel de control y monitorización lo cual lleva a una mejora del manejo del medio en que se están utilizando y de respuesta frente a inconvenientes o simplemente para el perfeccionamiento del mismo. El incremento de estos nodos en nuestro día a día conlleva un mayor interés por conseguir un mejor rendimiento y funcionamiento.

La enorme investigación que hay hoy en día sobre las redes de sensores inalámbricos han promovido que se investiguen y desarrollen muchos protocolos de enrutamiento en función de la utilidad que va a tener esa red de sensores, es decir de la aplicación directa en que va a ser utilizada, pues no es lo mismo una red de monitorización de un campo de uvas que una red de seguridad perimetral en un conflicto bélico. Estos protocolos no solo han beneficiado a las redes de sensores sino que gracias a ellos el desarrollo de estos protocolos han podido ser extrapolados hacia otras tecnologías como la wireless o la de cableado, permitiéndoles un mayor rendimiento.

Este tipo de redes actualmente, está llevando una revolución tecnológica similar a la que tuvo la aparición de Internet, pues las aplicaciones parecen ser infinitas, además se habla de redes de vigilancia global del planeta capaces de registrar seguimiento de personas y mercancías concretas, monitorizar tráfico, y varias iniciativas y proyectos de investigación han despertado gran interés para ser aplicados en la práctica. Claro todo esto parecen grandes ventajas en un futuro, pero la mala utilización podría acabar con la privacidad de mucha gente porque se están llegando a miniaturizar tanto los nodos que pueden ser tan pequeños como para estar en cualquier lugar sin ser detectados y funcionando sin ningún tipo de problemas, por eso esperemos que el desarrollo sobre estas redes sirva solo para la mejora de nuestras vidas.

Acrónimos

3G	3rd Generation
ACK	ACKnowledgement
ADC	Analog-to-Digital Converter
AES	Advanced Encryption Standard
API	Application Programming Interface
ARM	Advanced RISC Machines
CAP	Contention Access Period
CDMA	Code Division Multiple Access
CFP	Contention Free Period
CPU	Unidad Central de Procesamiento
CRC	Cyclic Redundancy Check
CSMA-CA	Carrier Sense, Multiple Access, Collision Avoidance
DHCP	Dynamic Host Configuration Protocol
DLL	Data Link Layer
DNS	Domain Name System
DSSS	Direct Sequence Spread Spectrum
E/S	Entrada/Salida
EEPROM	Electrically-Erasable Programmable Read-Only Memory
FIFO	First In First Out
FPGA	Field Programmable Gate Array
FTP	File Transfer Protocol
GIS	Geographic Information System
GPIO	General Purpose Input/Output
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GSM	Global System for Mobile Communications
GTS	Guaranteed Time Slot
GUI	Graphical User Interface
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
ISM	Industrial, Scientific and Medical
ISP	Internet Service Provider
LAN	Local Area Network
LLC	Logical Link Control
MAC	Medium Access Control
MEMS	Micro-Electro-Mechanical Systems
MMU	Memory Management Unit
NESL	Networked and Embedded Systems Lab
OSI	Open System Interconnection
PDA	Personal Digital Assistant
PHY	PHYSical

PIC	Programmable Interface Controller
POP3	Post Office Protocol 3
PPP	Point-to-point Protocol
QoS	Quality of Service
QVGA	Quarter Video Graphics Array
RADAR	RADio Detection And Ranging
RAM	Random-Access Memory
RF	Radio Frecuencia
RFD	Reduced Functional Devices
RFID	Radio Frequency Identification
RISC	Reduced Instruction Set Computing
ROM	Read-Only Memory
RSI	Red Sensorial Inalámbrica
SDK	Kit de Desarrollo de Software
SDRAM	Synchronous Dynamic Random Access Memory
SHM	Structure Health Monitoring
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
SONAR	Sound Navigation And Ranging
SPI	Serial Peripheral Interface
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial file transfer Protocol
UART	Universal Asynchronous Receiver/Transmitter
UWB	Ultra-WideBand
VNC	Virtual Network Computing
WiFi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access
WPAN	Wireless Personal Area Networks
WSN	Wireless Sensor Network
ZigBee	ZigBee

Bibliografía

R. Verdone, D. Dardari, G. Mazzini and A. Conti, Wireless sensor and actuator networks, Academic Press, 2008.

A. Boukerche and others, Algorithms and protocols for wireless sensor networks, Wiley, 2009.

I.F. Akyildiz, Ad hoc networks, Elsevier, 2004.

R. F. Martínez, J. O. Meré, F. J. M. Pisón Ascacíbar, A. G. Marcos, Redes inalámbrica de sensores: teoría y aplicación práctica, Universidad de la Rioja, 2009.

F. R. Pascual, profesor UPV, Redes de sensores inalámbricos,
<http://www.radioptica.com>.

N. Aakvaag, J. E. Frey, Redes de sensores inalámbricos, Revista ABB, 2006.

R. H. Hoecker, Estudio sobre el actual desarrollo comercia en RSI y componentes que forman un nodo sensor.

I. Stojmenovic. *Handbook of sensor networks. algorithms and architectures*. Wiley, 2005.

J. Grande. *Plataforma experimental de localización en una WSN mediante el uso de ondas sonoras*. UPM, 2008.

A. Bermudez, R. Casado, E. M. García, A. Gómez, F. J. Quiles, J. R. Ruiz-Gallardo, Empleo de una red de sensores en el reajuste del modelo de comportamiento del fuego en incendios forestales, Sevilla-España Wildfire 2007, 2007.

Wireless Sensor Networks. F. L. LEWIS. Smart Environments: Technologies, Protocols, and Applications Ed. D.J. Cook and S.K. Das, John Wiley, New York, 2004.

<http://focus.ti.com/docs/toolsw/folders/print/smartftm-studio.html#Technica%20Documents>

<http://ambientintelligence.wordpress.com/tag/wsn/>

<http://www.sensor-networks.org/>

<http://www.libelium.com>

<http://www.rtve.es/mediateca/videos/20100426/tres14---sensores/755090.shtml>

<http://www.youtube.com/watch?v=rXsXRZQEKHU>

<http://www.domodesk.com/>

<http://atom.research.microsoft.com/sensewebv3/sensormap/>

<http://domotica-online.com/>

<http://issuu.com/edgardo/docs/mc-thesis>

<http://www.zigbee.org/>

