UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE INFORMÁTICA

# TESINA DE LICENCIATURA

**Título:** WSN para servicios públicos metropolitanos
**Autores:** Candia Agustín, Varela Leonardo Néstor
**Director:** Luis Marrone
**Codirector:** -
**Asesor profesional:** -
**Carrera:** Licenciatura en Sistemas

## Resumen

*El avance de la tecnología en materia de comunicaciones, hardware, integración y consumo energético, está dando pie al desarrollo de infinidad de soluciones tecnológicas que, si bien algunas de ellas existían en ámbitos específicos, en la actualidad están comenzando a integrarse a la vida de las personas. En ese sentido, las redes de sensores inalámbricos están tomando un papel preponderante en la expansión hacia la "Internet de cosas". Dentro de este paradigma, nos interesa focalizarnos dentro del concepto de Ciudades Inteligentes, y en las redes de sensores como condición sine qua non para el desarrollo de megalópolis del futuro. En la actualidad existen numerosos desarrollos y estándares sobre redes de sensores inalámbricas, pero aún no han proliferado de forma masiva en aplicaciones que intervengan en la vida cotidiana, de acuerdo con el potencial que estas presentan. Por estos motivos nos ha resultado interesante investigar el estado del arte, como ha sido el camino transitado y las capacidades reales de estas tecnologías hoy en día, para poder plantear un escenario de futuros trabajos en torno a esta temática.*

## Palabras Claves

*Redes Inalámbricas de sensores, Wireless, Ciudades Inteligentes, IEEE 802.15.4, Bajo consumo, Sustentabilidad, Servicios, ZigBee, Hardware, Calidad del aire.*

## Trabajos Realizados

*Se realizó una investigación teórica sobre las tecnologías involucradas en las redes de sensores y sus campos de aplicación. Con el conocimiento obtenido se desarrolló un prototipo de red de sensores funcional, haciendo uso del protocolo ZigBee montado sobre una placa Arduino, orientada a mediciones en la calidad del aire. Se integró la red con un servicio de base de datos no relacional en la nube, para persistencia y generación de estadísticas.*

## Conclusiones

*El desarrollo de protocolos de comunicación que permitan un bajo consumo con altas prestaciones y los avances en hardware, establecen una base para la comunicación de datos sensados en pos de brindar servicios en ciudades inteligentes. Se abren escenarios que permiten a la comunidad informática realizar nuevos aportes a la mejora de la calidad de vida de los ciudadanos, con una potencialidad aún inestimable.*

## Trabajos Futuros

*Análisis de viabilidad y propuesta de servicios para SmartCities orientado a problemáticas en el entorno local.*
*Implementación de Sistemas Operativos en redes de sensores inalámbricas.*
*Profundizar en servicios para OpenData.*
*Analizar el uso de BigData en modelos de simulación y sistemas de predicción.*
*Estudio de mecanismos de seguridad en WSNs.*

**Fecha de la presentación:** Septiembre de 2017

# INDICE

# Índice de figuras

## Índice de Tablas

# INTRODUCCIÓN

## Motivación

El constante crecimiento de las ciudades, en muchos casos sin un planeamiento anticipado, conlleva nuevos desafíos en el desarrollo de estructuras de gobierno más agiles, nuevos servicios al ciudadano y un eficiente uso de los recursos.

El avance de la tecnología en materia de comunicaciones, hardware con sistemas embebidos, integración y consumo energético, está dando pie al desarrollo de infinidad de soluciones tecnológicas que, si bien algunas de ellas existían en ámbitos específicos y de forma aislada, en la actualidad están comenzando a integrarse unas a otras y en la vida de las personas.

En ese sentido, las redes de sensores inalámbricos están tomando un papel preponderante en la expansión hacia la “Internet de cosas”. Dentro de este paradigma, nos interesa focalizarnos en el concepto de Ciudades Inteligentes, y en las redes de sensores como condición sine qua non para el desarrollo de megalópolis del futuro.

En la actualidad existen numerosos desarrollos y estándares sobre redes de sensores inalámbricas, pero aún no han proliferado de forma masiva en aplicaciones que intervengan en la vida cotidiana, de acuerdo con el potencial que estas presentan.

Por estos motivos nos ha resultado interesante investigar el estado del arte, como ha sido el camino transitado y las capacidades reales de estas tecnologías hoy en día, para poder plantear un escenario de futuros trabajos en torno a esta temática.

## Objetivo

El objetivo del presente documento es analizar las tecnologías involucradas en torno a las redes de sensores inalámbricas (WSN, Wireless sensor networks), sus características, campos de aplicación y casos concretos desarrollados en la actualidad.

Luego, utilizar los conocimientos adquiridos oportunamente, para el desarrollo de un prototipo de WSN para servicios públicos en ciudades inteligentes, como punto de partida para:

- Difundir su versatilidad y usos posibles.
- Ofrecer una solución basada en tecnologías de Software y Hardware libre.
- Analizar la viabilidad de implementar el paradigma de “Ciudad Inteligente” en un contexto local.

- Promover el desarrollo de soluciones que optimicen la utilización de recursos y brinden servicios a la comunidad.

## Presentación

Desarrollaremos en la primera parte de este trabajo de tesis distintas tecnologías sobre redes de sensores inalámbricas y el aporte que brindan a diferentes proyectos en ciudades inteligentes y en otros campos de aplicación específicos. Como veremos en todos los casos, las redes de sensores inalámbricas se vuelven un elemento indispensable sobre el cual sustentar estos proyectos. En algunos casos se podría prescindir de las mismas, aumentando costos y limitando funcionalidades. Mientras que otros proyectos serian técnicamente inviables sin la existencia de las WSN.

Sea cual fuera el campo de aplicación, en todos los casos será necesario distribuir un número grande de sensores e interconectarlos entre sí, de manera que los datos recolectados puedan ser enviados a mecanismos de almacenamiento, desde donde se puedan tomar decisiones con esta información. Esto nos traerá aparejados desafíos en cuanto al enrutamiento de esta información entre los nodos, el bajo consumo de energía y mantenimiento de los mismos, la seguridad en las comunicaciones y los modelos para procesar este volumen de información.

También analizaremos las regulaciones en torno a las temáticas de Ciudades Inteligentes y el Internet de las Cosas, paradigmas íntimamente relacionados con las redes de sensores.

En la parte 2 describiremos el desarrollo de un prototipo utilizando algunas de las tecnologías analizadas. La pregunta que intentamos responder es: ¿Es posible crear una red de sensores para servicios de ciudades inteligentes, con hardware libre, componentes disponibles en el mercado local y software libre existente?

# PARTE 1

# Marco Teórico

# 1. Evolución hacia las redes de sensores

## 1.1. Antecedentes

La idea original de las MANET (*Mobile Ad-hoc NETwork*) tuvo origen en el año 1972. En ese entonces las MANET eran conocidas como redes de radio-paquete llamadas PRNET (*Packet Radio Networks*). La agencia conocida como *Defense Advanced Research Projects Agency* (DARPA, agencia que patrocinó la ARPANET, luego devenida en Internet), se encargó de dar patrocinio a las MANET originales.

La evolución de redes de sensores tiene su origen en iniciativas militares. Como predecesor de las redes de sensores modernos se considera el proyecto SOSUS (*Sound Surveillance System*) desarrollado por los Estados Unidos: una red de sensores sumergidos en el mar, los cuales tenían el objetivo de detectar e informar la presencia de submarinos soviéticos.

Podemos tomar también como un importante antecedente a las redes de sensores, la aparición de las comunicaciones inalámbricas en equipos móviles realizadas por primera vez en el año 1973 en la compañía Bell Labs en un proyecto que sentó las bases de la telefonía celular actual. Paralelamente IBM se encontraba en el desarrollo de comunicaciones de datos inalámbricas, utilizando señales infrarrojas.

Durante los ‘80 nace el proyecto SURAN (*Survivable Radio System*). Esponsoreado por DARPA y con participación de corporaciones del ámbito privado, el mismo tiene como objetivo el desarrollo de un conjunto de radio routers MANET que permitan manejar las comunicaciones en el campo de batalla moderno.

La implementación estaba orientada a conseguir equipos pequeños, de bajo costo y bajo consumo energético, que pudieran soportar los sofisticados algoritmos de comunicación de paquetes por radio, desarrollados por DARPA con anterioridad. Además de brindar la robustez necesaria para las condiciones de despliegue adversas. Como resultado de estas investigaciones del grupo SURAN se obtuvieron importantes avances en materia de algoritmos de ruteo, mecanismos de seguridad y autenticación de la red, y herramientas de simulación y prueba. [1]

En el ámbito de las comunicaciones móviles, marca un hito la aparición en el año 1987 de la primera especificación del estándar GSM *(Global System for Mobile communications, 2G,*

*segunda generación de celulares)*, para la digitalización en la transmisión de voz y datos. Empezando a hacerse las primeras implementaciones a principio de los años 90. [2]

En el año 1994 de la mano de DARPA, nace el programa GLOMO (*Global Mobile Information System*), el cual tiene como objetivo brindarles a usuarios de dispositivos móviles inalámbricos conectividad a Internet, independiente de la ubicación.

Durante el año 1997, la IETF (*Internet Engineering Task Force),* una organización abierta para la generación de estándares de internet, crea un grupo de trabajo para la creación de estándares de protocolos de enrutamiento para redes ad-hoc. Al día de hoy, este grupo continúa trabajando en la investigación y desarrollo de estándares asociados a las redes ad hoc. [3]

Hacia principios del año 2000 surge una evolución del 2G, que incorpora ahora la posibilidad de transmitir datos. Estos son los servicios de GPRS y EDGE, que se los suele denominar como la generación de redes celulares 2.5G.

Sobre estos servicios comenzaron a implementarse en la industria las comunicaciones inalámbricas M2M (*machine to machine*), para dar pie al sensado y control remoto de ciertas instalaciones. Se puede decir que el paradigma M2M constituye un claro antecedente en el desarrollo de las Redes de Sensores inalámbricas y al paradigma del Internet de las Cosas (IoT) [4] [5]

Por su parte, la IEEE (*Institute of Electrical and Electronics Engineers*) sienta las bases formales para las redes de sensores inalámbricas, producto de la fuerte adopción de sus estándares IEEE 802.11 y 802.15 en el mercado.

Podemos notar, que desde sus inicios el desarrollo e implementación de las WSN se ha centrado principalmente para fines militares, experimentales o bien industriales (monitoreo y control de gases, fluidos, de redes eléctricas, de rutas marítimas). Hoy en día se vislumbra un escenario donde las WSN, empiezan a tener un rol más preponderante en aplicaciones con impacto más directo en la sociedad y en la vida diaria de las personas con el surgimiento del Internet de las Cosas o IoT.

## 1.2. Redes Inalámbricas

Para entender mejor el funcionamiento las Redes de Sensores, nos resulta importante empezar clasificando las redes inalámbricas según su tipo de conexión, acorde a lo establecido en el estándar 802.11: el Modo Infraestructura y el Modo Ad hoc.

### 1.2.1. Modo infraestructura

El modo infraestructura establece que dos dispositivos inalámbricos deben conectarse entre sí mediante al menos un punto de acceso. De esta manera, para poder comunicar dos equipos es necesario que ambos estén al alcance de un punto de acceso en común, para el caso más básico, o que exista conectividad entre los puntos de acceso a los cuales accede cada equipo. A esta área básica conformada por el punto de acceso y las terminales se lo suele llamar BSS o célula (como lo define la IEEE).

Es posible vincular varios puntos de acceso con una conexión llamada sistema de distribución (o SD) para formar un conjunto de servicio extendido o ESS. El sistema de distribución también puede ser una red conectada, un cable entre dos puntos de acceso o incluso una red inalámbrica.

Un ESS se identifica a través de un ESSID (identificador del conjunto de servicio extendido), que es un identificador de 32 caracteres en formato ASCII que actúa como su nombre en la red. El ESSID, a menudo abreviado SSID, muestra el nombre de la red y de alguna manera representa una medida de seguridad mínima ya que una estación debe saber el SSID para conectarse a la red extendida.

Cuando una estación se une a una BSS, envía una solicitud de sondeo a cada canal. Esta solicitud contiene el ESSID que la célula está configurada para usar y también el volumen de tráfico que su adaptador inalámbrico puede admitir. Si no se establece ningún ESSID, la estación escucha a la red para encontrar un SSID.

Cada punto de acceso transmite una señal en intervalos regulares. Esta señal, que se llama señalización, provee información de su BSSID, sus características y su ESSID, si corresponde. El ESSID se transmite automáticamente en forma predeterminada, pero por razones de seguridad se recomienda deshabilitar esta opción.

Cuando un dispositivo se mueve dentro de un ESS, puede suceder que quede fuera del alcance de un BSS para pasar a estar al alcance de otro, o que haya un BSS con mejor calidad de señal del que se encuentra conectado. En una misma red, puede haber múltiples BSS (cada uno con un identificador denominado BSSID). Es este caso, los BSS intercambian información de las estaciones entre sí, a fin que las mismas puedan moverse entre puntos de acceso de forma totalmente transparente. [6]

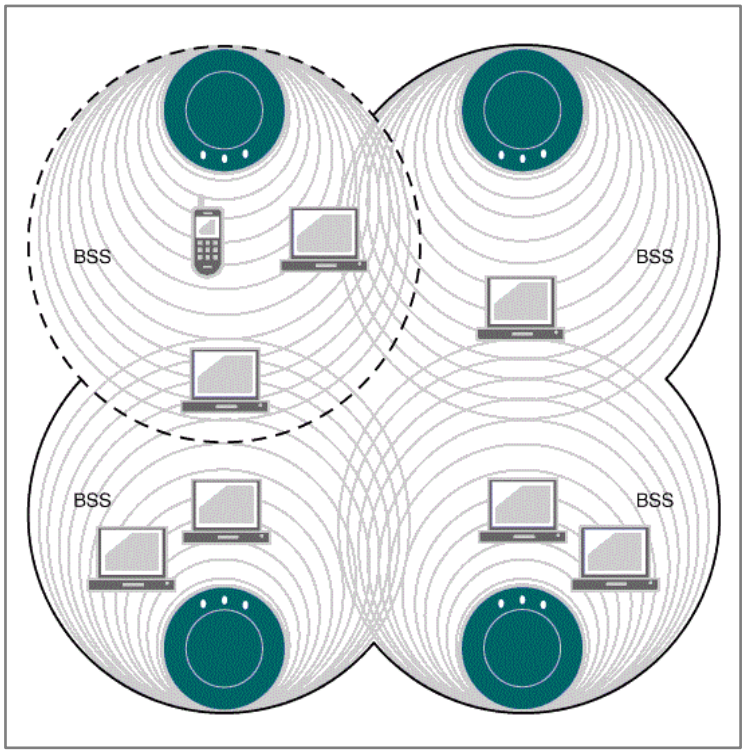



Fig. 1 - Modo Infraestructura [7]

### 1.2.2. Modo Ad Hoc

Esta configuración está basada en la conexión peer to peer, o punto a punto, de forma tal que las estaciones pueden comunicarse directamente, sin ningún tipo de infraestructura previa, como puntos de acceso o routers. En este caso un BSS estaría compuesto por dos equipos interconectados.

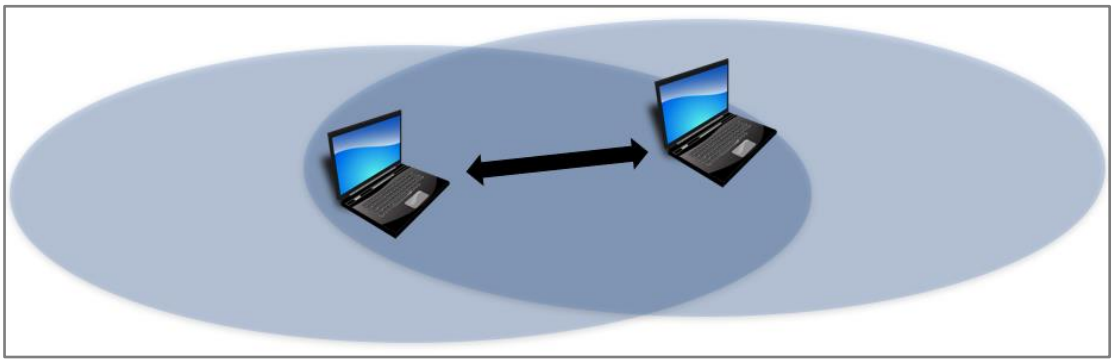


Fig. 2 - Modo Ad Hoc

Para redes más complejas, la comunicación de dos equipos dependerá que los mismos estén a un alcance directo, o que exista un camino de equipos interconectados punto a punto. [6]

## 1.3. Redes Móviles Ad Hoc (MANET)

Nos resulta importante destacar un concepto muy relacionado con la aparición de las WSN, como son las Redes Móviles Ad Hoc (Mobile Ad Hoc Networks).

Cuando hablamos de MANETs nos referimos a un sistema de nodos móviles inalámbricos que de forma dinámica pueden auto-organizarse en topologías de redes arbitrarias y temporales. Los nodos, por lo tanto pueden ser interconectados en áreas sin una infraestructura de comunicación preexistente o cuando el uso de la infraestructura requiere extensión inalámbrica. [8]

Debemos mencionar que en la implementación de estas redes móviles ad hoc, pueden verse involucradas diversas tecnologías o protocolos inalámbricos existentes, los cuales tendrán beneficios y limitaciones de acuerdo al ambiente de aplicación donde se quieran desarrollar.

Actualmente los protocolos más difundidos para redes MANET son el AODV y el OLSR, aunque existen soluciones basadas en protocolos de mayor difusión comercial que permiten armar redes ad hoc con ciertas limitaciones. Son ejemplo de esto último Bluetooth o WiFi Direct para redes inalámbricas de área personal (*wireless personal area networks*, WPAN) así como IEEE 802.11 en modo ad hoc para redes inalámbricas de área local.

Esta introducción a las redes MANET la hemos expuesto dado que guardan una estrecha relación con las redes inalámbricas de sensores (WSN), las cuales son foco de este trabajo. No obstante, existen diferencias que las caracterizan más específicamente, separando unas de las otras.

Entre las diferencias más importantes podemos destacar:

- El modo típico de comunicación en WSN es a partir de múltiples fuentes de datos a un receptor (algo así como un multicast inverso) en lugar de la comunicación entre un par de nodos. En otras palabras, los nodos sensores utilizan comunicación principalmente multicast o broadcast, mientras que la mayoría de MANETs son sobre la base de las comunicaciones punto a punto. [9]
- En la mayoría de los escenarios los propios sensores no son móviles (aunque los fenómenos que detectan sí pueden serlo); esto implica que la dinámica en los dos tipos de redes sea diferentes. [9]
- Debido a que los datos recogidos por múltiples sensores se basan en fenómenos comunes, existe potencialmente un grado de redundancia en los datos que se están comunicando por las diversas fuentes hacia la WSN, lo que no es generalmente el caso en las MANET. [9]

- Un recurso crítico en las WSN es la energía, lo que generalmente no es así en las MANETs dado que, al ser manejadas por humanos, los dispositivos pueden ser reemplazados o recargados periódicamente. Dependiendo del tipo de aplicación, un nodo de una WSN puede estar funcionando de forma desatendida durante semanas, meses o incluso años. [9]
- El número de nodos de sensores en una WSN puede ser de varios órdenes de magnitud mayor con respecto a la cantidad de nodos que pueden intervenir en una MANET. [9]

## 2. Redes inalámbricas de sensores (WSN)

Una red de sensores es una infraestructura compuesta por elementos de cómputo, medición y comunicación, que permiten a un administrador o sistema autónomo instrumentar, observar y reaccionar a eventos y fenómenos en un ambiente específico. [9]

Cuando hablamos de sensores nos referimos a un dispositivo que convierte una entrada proveniente de un fenómeno físico a una señal electrónica, la cual puede ser interpretada por un humano o bien servir de entrada a un sistema informático. Entre las señales convencionales a medir podemos enumerar entre otras, intensidad de luz, presión, temperatura, humedad, gases.

Las redes de sensores inalámbricas son un tipo de red Ad Hoc inalámbrica (por lo que comparte muchas características y limitaciones con las MANET), con un objetivo muy específico, el cual es determinar la existencia o características de un evento en particular.

Las WSN tienen características únicas, tales como, las restricciones de energía y la vida limitada de la batería, la adquisición de datos redundantes, bajo ciclo de trabajo, ancho de banda limitado y flujo de datos “muchos a uno”. En consecuencia, se necesitan nuevas metodologías de diseño a través de una serie de disciplinas, incluyendo, pero no limitado a, el transporte de la información, gestión de red y operacional, confidencialidad, integridad, disponibilidad y procesamiento in-network/local [10] [9].

Estas limitaciones están asociadas a los ambientes en los que se desarrollan comúnmente las aplicaciones de este tipo de redes. Dichos ambientes poseen características como la falta de acceso a una fuente de energía convencional, distancias y ubicación variable de los nodos, condiciones ambientales desfavorables para las comunicaciones o el funcionamiento de dispositivos electrónicos estándar, eventos que se producen con frecuencias aleatorias, nodos sensores propensos a fallas, nodos densamente desplegados, entre otros factores [9].

Es de esperar que las WSN en muchos casos tengan una capacidad limitada de despliegue y de entrada de datos. Además, la ubicación de algunos de estos dispositivos puede ser difícil de alcanzar. En consecuencia, los protocolos que se usen en las WSN deberían requerir una configuración mínima, estar listos para su uso inmediato, ser de fácil arranque y, además, capacitar a la red para la auto-restauración dada la característica inherente de poca confiabilidad de estos dispositivos. [11]

Dado que la topología en este tipo de redes es totalmente dinámica y basada en eventos, y teniendo en cuenta la alta probabilidad de variación del número de nodos conectados y/o en operación, uno de los focos de investigación en WSN se encuentra en los algoritmos de ruteo, los cuales deberán diseñarse teniendo en cuenta características específicas de este tipo de redes. En particular se vuelve prioritario encontrar soluciones de encaminamiento de paquetes que reduzcan al mínimo las transmisiones que deban realizar los nodos sensores, ya que estas constituyen el principal consumo de energía del dispositivo [12]. Analizaremos más adelante en este trabajo, diferentes soluciones existentes.

Los nodos que conforman las redes de sensores inalámbricas, suelen ser dispositivos de hardware extremadamente simples, con capacidades de procesamiento y memoria limitados, poder de transmisión de corto alcance. Teniendo en cuenta la densidad y escala que comprende estas redes, un hardware simple nos permitirá abaratar costos, reducir mantenimiento y prolongar el uso de las baterías.

Con el surgimiento y constante crecimiento de esta tecnología en la última década, diferentes tipos de aplicaciones posibles surgen día a día. Entidades gubernamentales y privadas se han volcado a la implementación de diferentes soluciones, que van desde Sensado Medio-ambiental a control de flujo vehicular, seguridad edilicia y aplicaciones de domótica, control de producción, monitoreo de hábitat de especies protegidas, distribución de energía eléctrica, aplicaciones bélicas en campos de batalla, entre otras. Haremos un análisis más profundo de estos campos de aplicación en el capítulo de Campos de aplicación de las WSN.

En respuesta a las necesidades emergentes en materia de redes de sensores, distintas empresas comienzan a desarrollar soluciones propietarias, lo que trajo problemas de interoperabilidad entre los diversos fabricantes.

Surge entonces la necesidad de un estándar de comunicación inalámbrica de baja tasa de transmisión para redes de sensores apuntados a este tipo de redes, y así es como la IEEE publica la primera versión del Estándar 802.15.4 en el año 2003. Este estándar define las capas física y de acceso al medio del modelo OSI para redes de baja transferencia y bajo consumo energético [13]. Analizaremos en más profundidad este estándar en la sección dedicada al IEEE 802.15.4.

## 2.1. Arquitectura de las redes de sensores inalámbricas

La infraestructura que compone una red de sensores la podemos resumir en las siguientes componentes:

I. Los **nodos sensores** que son dispositivos con recursos restringidos de energía, comunicación, memoria y capacidad de cómputo, cuya función principal es realizar la medición de un fenómeno específico y transmitir el resultado de la misma. [9].

Un nodo sensor podemos decir que estará constituido por cuatro componentes básicos, como muestra la figura siguiente.

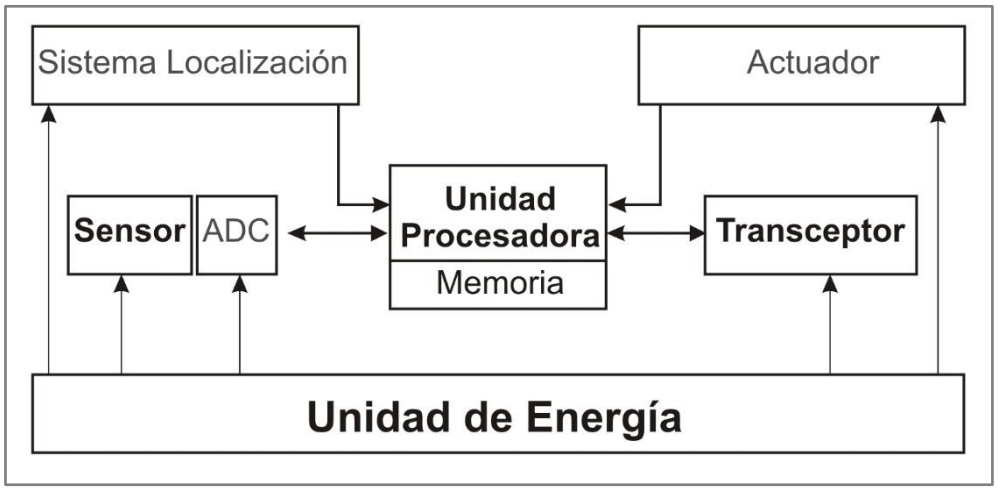



**Fig. 3 - Estructura de un nodo sensor [14]**

Una **unidad sensora**, una **unidad procesadora**, una **unidad transceptora**, y una **unidad de energía**, aunque pueden tener también componentes adicionales dependiendo de su aplicación como un sistema de localización, un generador de energía o un movilizador (actuador).

Si deseáramos una definición más formal de sensor, podemos recurrir a la de la IEEE 1451.6 [15], que lo define como "*Un dispositivo electrónico que produce datos eléctricos, ópticos o digitales derivados de una condición o evento físico. Los datos producidos a partir de los sensores son transformados electrónicamente, por otro dispositivo, en información (salida) que es útil en la toma de decisiones hecha por dispositivos o individuos (personas)´inteligentes."*, considerándolo para el alcance de esta norma como sinónimo del transductor, al que describe como *"un dispositivo electrónico que transforma la energía de una forma a otra..."*.

Usaremos a lo largo del documento la terminología de "motas sensoras", "celdas de monitoreo", "dispositivos sensores" o simplemente "nodos", como sinónimos de los "nodos sensores" aquí especificados.

Para el alcance de este trabajo, podemos decir entonces que la **unidad sensora** cuenta con un transductor que convierte una señal no interpretable por el sistema, en otra variable interpretable por dicho sistema. En este contexto, las señales analógicas del mundo físico producidas por los sensores son convertidas a señales digitales por un conversor analógico a digital (ADC), las cuales se trasmiten a través de un bus a la unidad procesadora.

La **unidad procesadora**, generalmente acompañada de una unidad de almacenamiento, controla los procedimientos necesarios para que el nodo sensor colabore con los demás en la realización de las tareas de sensado. Esta unidad de proceso estará compuesta principalmente por un microcontrolador o un microprocesador. En el caso de usar microcontroladores (ejemplo el ATMEL328 de Arduino), serán unidades más simples, con menor potencia de cálculo y abocados a una tarea concreta. En el caso de utilizarse microprocesadores (ejemplo las Raspberry Pi con su procesador Broadcom), estos serán más costosos, pero se contará con una mayor capacidad de procesamiento.

La **unidad transceptora** que es el dispositivo encargado de las comunicaciones, enviando y recibiendo paquetes de/hacia una red inalámbrica.

La **unidad de energía** o fuente de alimentación es otro de los componentes críticos, y en el terreno de las WSN, apunta al uso de baterías. Estas pueden ser abastecidas por unidades de captadoras de energía como es el caso de las células solares.

Los Nodos Sensores suelen diseñarse de manera de optimizar los ciclos de procesamiento, permitiendo modos de reposo que ayuden a obtener un ahorro energético [8].

Existen en el mercado sensores para medir distintos tipos de magnitudes, entre los que podemos mencionar:

- Aceleración
- Magnetismo
- Higrómetros/Humedad
- Posición lineal y angular
- Desplazamiento y deformación
- Velocidad lineal y angular
- Fuerza y par (deformación)
- Presión
- Caudal
- Temperatura
- Sensores de presencia
- Sensores táctiles

- Visión artificial
- Sensor de proximidad
- Sensor acústico (presión sonora)
- Sensores de acidez
- Sensor de luz ambiente
- Sensores captura de movimiento

II. Una **red de interconexión inalámbrica** (basada en algún protocolo como 802.15.4 por ejemplo). En algunas aplicaciones concretas, pueden verse como ciertos nodos (particularmente gateways de red o sinks), cuentan con soporte para más de un protocolo de comunicación.

III. Los **sumideros o sinks**, que son nodos centrales con mayor capacidad de comunicación y cómputo, hacia los cuales se transmite la información recolectada por los nodos sensores. Según el campo de aplicación, el sumidero puede pertenecer a la red de sensores (y actuar como otro sensor), o bien ser una entidad externa a la red o funcionar como un gateway a otra red más grande, como redes corporativas en Internet. La información recolectada por los sumideros en algunos casos, es transmitida hacia otros equipos de mayor jerarquía llamados “estaciones base”, los cuales ya son equipos externos de la red, desde donde se gestiona la misma y se procesa la información obtenida en grandes volúmenes [9].

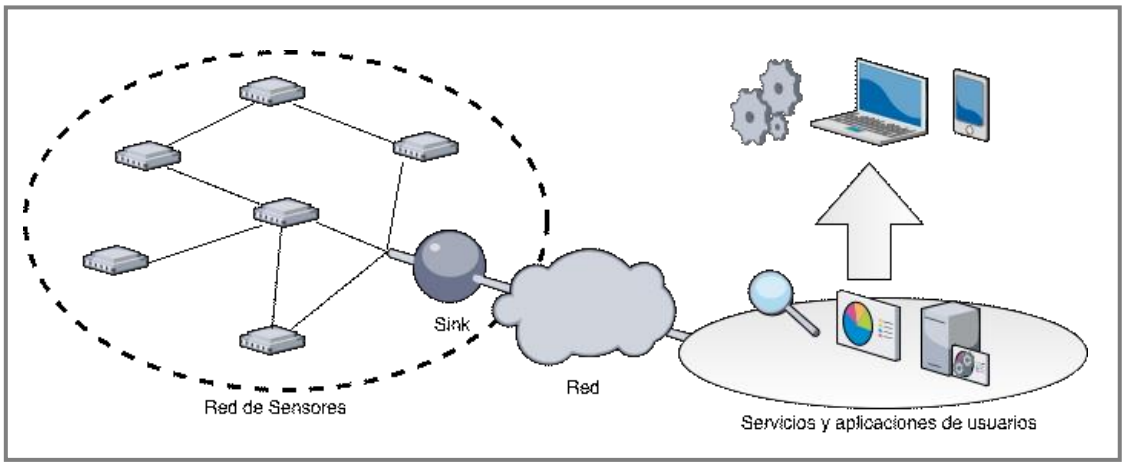



**Fig. 4 - Participantes en una WSN**

Dependiendo de la aplicación, un nodo puede dedicarse a una función particular y poseer diferentes capacidades de computación, comunicación y energéticas.

Algunas soluciones proponen designar un nodo coordinador con capacidades diferentes a los sensores normales, mientras que otras alternativas proponen un conjunto de nodos homogéneos donde los coordinadores forman parte del grupo de sensores. Los nodos

también podrían actuar como retransmisores de información obtenida por otros nodos (denominados genéricamente como nodos enrutadores o *routers*). [16]

Teniendo en cuenta esto, las redes de sensores pueden estructurarse de la siguiente manera:

- **Estrella:** todos los nodos se comunican con un nodo central pre-definido. Este nodo concentrador, necesariamente deberá tener capacidades de cómputo y comunicación superiores a los demás nodos de la red. La principal limitación se da en que los nodos no se comunican entre sí, de manera que si un nodo no tiene alcance de radio con el nodo central, no podrá establecer comunicación con la red.
- **Malla multisalto:** se pueden obtener canales de comunicación entre cualquier par de dispositivos estableciendo la conectividad entre los nodos por medio de vínculos multisalto. Los nodos además de transmitir la información obtenida de su sensado, pueden actuar como retransmisores de la información de otros nodos.

  Esta estructura implica links redundantes lo cual otorga una mayor robustez que las estructuras basadas en árbol. En contraposición, los nodos requieren un mayor tiempo de actividad y procesamiento, lo cual conlleva un mayor consumo energético. [8]
- **Árbol (ClusterTree):** implica una jerarquía de nodos, donde existen nodos sensores básicos y nodos coordinadores. Los nodos sensores solo pueden comunicarse con su coordinador, y los coordinadores se comunican entre sí formando caminos de múltiples saltos para alcanzar el sink. Existe un único camino de cada nodo básico al sink, lo que le otorga menos robustez en comparación a la malla, con lo cual no es un modelo recomendado para aplicaciones con nodos de frecuente movilidad, ya que la estructura de árbol es frágil y necesita ser reajustada frecuentemente con los cambios conectividad. [8]

  La principal ventaja es que se optimiza la vida útil de los nodos básicos, ya que se maximizan los tiempos de reposo en los mismos (al no tener que actuar como retransmisores), obteniéndose un ahorro energético considerable. [8]

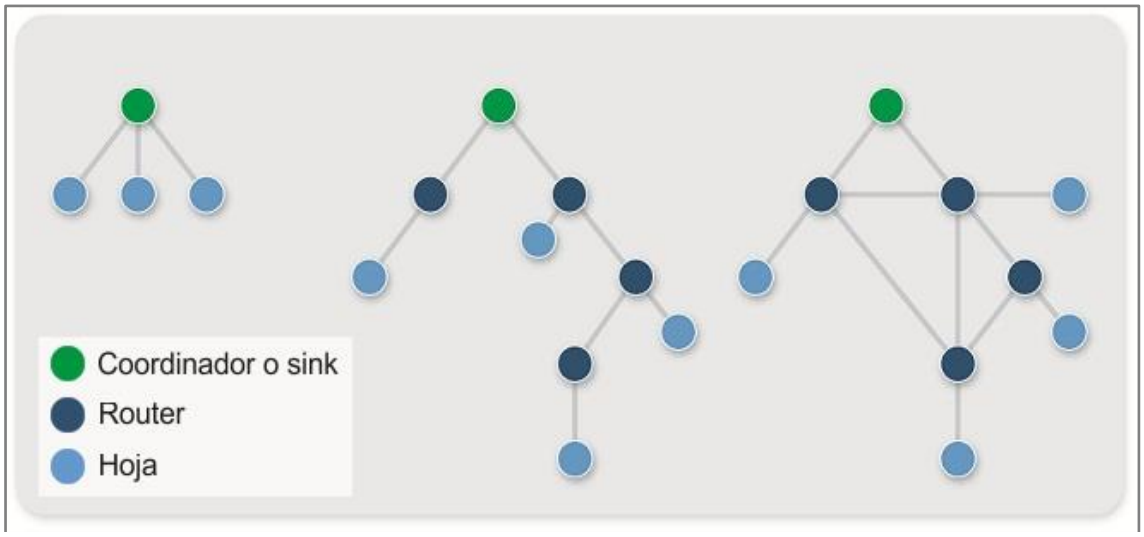



Fig. 5 - Topologías en WSN

## 2.2. El desafío del enrutamiento

El ruteo en las WSN implica un gran desafío, dadas las características propias de este tipo de redes, con respecto a otras de similares características como podrían ser las MANETs o las redes de telefonía celular.

En primer lugar, dado el número considerablemente grande de nodos sensores que se pueden llegar a desplegar, el autor [11] plantea la complejidad de un esquema tradicional de direccionamiento IP global, dado que la sobrecarga producida para el mantenimiento de los identificadores sería demasiada (sin embargo, veremos más adelante en la sección de protocolos que algunos como 6LoWPAN ya dan soporte a IPv6 de forma nativa). Además, los nodos pueden estar distribuidos de manera ad hoc, de forma tal que la red debe tener la capacidad de auto-organizarse y funcionar bajo las conexiones que produzcan sin pre-establecimientos, y todo esto de manera desatendida. En las WSN la obtención de los datos, muchas veces, es más importante que conocer la identificación de los nodos que la envían. [17]

Otro factor a tener en cuenta es que la mayoría de las aplicaciones requieren el envío de información desde múltiples nodos sensores hacia alguna/s estación/es, en contraposición con las redes convencionales. Aunque esto no implica que la información pueda viajar en otros sentidos (por ejemplo, multicast o peer to peer).

Por otra parte, los nodos sensores tienen fuertes restricciones de energía, procesamiento y almacenamiento. Lo cual requiere de un manejo cuidadoso de los recursos.

Uno de los requerimientos que aparecen frecuentemente en las WSN es la necesidad de conocer la ubicación de los nodos sensores, dado que la recolección de datos suele estar

basada en ubicación. En la actualidad no es muy factible colocar un sensor GPS en cada nodo sensor (por problemas de consumo y dado que pueden tener un mal desempeño en ambientes cerrados), por lo que se deben buscar soluciones basadas en triangulación de señales con nodos de los cuales se conoce a priori su ubicación.

Finalmente, la información obtenida por los sensores está generalmente basada en un fenómeno en común, por lo cual hay grandes posibilidades que se genere información redundante. Esa redundancia debe ser aprovechada por los algoritmos de ruteo, a fin de minimizar el consumo energético y optimizar el uso del ancho de banda. Usualmente las WSN son datacéntricas, en el sentido que los datos son requeridos en base a ciertos atributos. O por decirlo de otro modo, poseen un direccionamiento basado en los atributos. Es así como, en vez de obtenerse la información de un nodo mediante un identificador, los datos son solicitados por un par de atributo-valor (por ejemplo, puede solicitarse que transmitan los nodos cuyo atributo “temperatura” sea mayor a “40C°”).

Debido a estas diferencias, se han propuesto muchos nuevos algoritmos para el problema de enrutamiento en redes inalámbricas de sensores.

Estos mecanismos de enrutamiento han tenido en cuenta las características inherentes de redes inalámbricas de sensores, junto con los requisitos de la aplicación y de la arquitectura.

Para minimizar el consumo energético diversos autores han propuesto protocolos de ruteo ya conocidos, como así también soluciones específicas para las WSN como [17]:

- Agregación de datos
- Procesamiento “en la red”
- Clustering
- Asignación de diferentes roles a los nodos
- Métodos datacéntricos

Los protocolos desarrollados para las MANET, pueden acercar algunas soluciones, pero para otros casos deberán tenerse en cuenta las características propias de las redes de sensores inalámbricas.

Algunos factores que afectan la performance de los paquetes que se envían en este tipo de redes y que se deben tener en cuenta al momento de diseñar e implementar algoritmos de ruteo:

- **Instalación de los sensores:** es altamente dependiente del tipo de aplicación que deseamos monitorear. Si la distribución de los nodos se hace manualmente, en ubicaciones predeterminadas, el ruteo es definido por caminos preestablecidos. En otros casos, las ubicaciones de los nodos se presentan en forma aleatoria, no

uniforme (en general, porque la aplicación así lo demanda), tornándose necesarias las comunicaciones entre nodos en modo ad hoc multisalto. [17]

- **Bajo Consumo de energía sin pérdida de precisión:** debemos considerar cuidadosamente algunos aspectos claves relacionados con el uso de energía: energía por bit recibido correctamente, energía por evento reportado, relación retardo/energía, vida útil de la red [18]. En redes multisalto, el nodo pasará a jugar un rol dual, pudiendo funcionar como emisor y como router. En caso de falla de algún sensor, la red puede llegar a verse afectada y necesitar de cambios en el re - enrutamiento de los paquetes. [17]
- **Modelo de notificación de Datos:** el modo en que se obtiene la información de los sensores puede clasificarse según sean *Basados en Tiempo, Basados en Eventos, Basados en Demanda e Híbridos.* Los modelos *Basados en Tiempo* son ideales para aplicaciones que requieren de un monitoreo periódico. En este caso, los sensores se activan cada periodo de tiempos fijos para sensar en su campo de interés y transmitir el valor sensado. En el caso de los modelos *Basados en Eventos o Por Demanda*, los nodos sensores se activan ante cambios significativos en un valor sensado que se generó por una situación no predecible, o bien por demanda de una estación externa a la red la cual que requiere información de los nodos en tiempo real. Una combinación de estas técnicas puede dar forma a diversos modelos *Híbridos,* según el tipo de fenómeno que deseamos monitorear. Una vez más, del modelo de notificación de datos es que se encuentre inmersa nuestra red, dependerá el aprovechamiento de energía y la estabilidad de la misma.
- **Heterogeneidad de los Nodos:** distintos tipos de nodos pueden ser instalados en una red de sensores. Esta diferenciación puede darse en términos de capacidad de cómputo, poder de transmisión o disponibilidad de energía. Algunas aplicaciones requerirán del sensado de distintos fenómenos (humedad, presión, temperatura), los cuales podrán ser analizados por un mismo sensor o por varios sensores con un hardware de sensado diferente. El modelo de notificación entre estas distintas funcionalidades también puede variar (puede darse el caso que no sea de interés medir la presión atmosférica cada 1 minuto, pero si la temperatura), lo cual se deberá tener en cuenta al momento de diseñar la red. También vimos algunas estructuras jerárquicas de red, como el ClusterTree, que proponen nodos con capacidades de enrutamiento particulares (Cluster head o nodo coordinador) para comunicar la información de los nodos que tienen conectados y enrutar paquetes entre sí.
- **Tolerancia a Fallas:** una característica inherente de las redes de sensores, es que los nodos que las conforman tienen altas probabilidades de quedar fuera de servicio, ya sea por fallas en el hardware, por carencia de energía en sus baterías, por limitación del alcance de radio o simplemente por hechos de vandalismo. Esto puede

llegar a generar zonas ciegas dentro de la red y comportamientos anormales de la misma. Los protocolos de enrutamiento y MAC deben autoadaptarse y generar nuevos links y rutas para el enrutamiento de paquetes hacia las estaciones base o sinks. La tasa de transmisión como también el alcance de radio frecuencia pueden llegar a ser variables de ajuste en los nodos para extender su vida útil. Es importante lograr el mayor nivel posible de redundancia y auto-adaptación a estas situaciones, para lograr una mayor tolerancia a fallas y lograr que la red siga cumpliendo con sus objetivos de monitoreo.

- **Escalabilidad:** el orden de magnitud en las redes de sensores va de decenas, a centenas hasta miles de nodos. A su vez, la densidad de los nodos podría ir aumentando en la red, sin necesidad de hacer modificaciones en la misma, sino más bien esperando un comportamiento auto-organizado. La escalabilidad en WSN debe considerarse integralmente tanto en el hardware como en el software. Para el hardware, escalabilidad implica sensibilidad y alcance de los sensores, ancho de banda y uso de la energía. Referente al software podemos asociar a la escalabilidad con la fiabilidad de los comandos de difusión y transferencia de datos, gestión de grandes volúmenes de datos y la utilización de algoritmos escalables para el análisis. Debe considerarse que el aumento del número de equipos conlleva a un aumento de las transmisiones necesarias, con lo que se aumenta el consumo energético global de la WSN. Una alternativa es realizar mediciones no tan frecuentes del parámetro investigado, y así disminuir el número de transmisiones [10].
- **Movilidad de la red:** dependiendo de la naturaleza de la aplicación, puede darse que los nodos o incluso las estaciones base, cuenten con cierta movilidad física. El ruteo de mensajes a nodos móviles, es un desafío a tener en cuenta siendo que la estabilidad de la red se puede ver comprometida, como también ciertos parámetros de energía y ancho de banda. Algo más complejo aún podría darse si el fenómeno a monitorear es dinámico. En estos casos se requerirá de un modo de adquisición de datos periódico, casi constante, para no perder la precisión deseada del fenómeno en cuestión analizado. Para casos donde el foco de monitoreo se estático, se pueden adoptar modos de funcionamientos de la red reactivos, donde los nodos se despiertan al momento que sucede el evento, transmiten a su sumidero o sink, y luego se colocan en un estado de reposo.
- **Medio de transmisión:** suponemos en el alcance de este trabajo, que el medio sobre el que se comunican estas redes multisalto, es siempre el medio inalámbrico. Por ende, las redes de sensores heredarán los problemas tradicionales de las comunicaciones inalámbricas, como ser, interferencias de múltiples orígenes sobre el canal, desvanecimiento de la señal, alta tasa de errores, alcance acotado, ancho de banda limitado, entre otras. A estos desafíos, se le sumarán también las ya

mencionadas características de un hardware simple con serias limitaciones de energía. A fines del acceso al medio, se deberá contemplar una capa de acceso al medio (MAC). Una aproximación al tema se da con el uso de protocolos que utilizan multiplexación por división en el tiempo (TDMA), que demostró ser más económico en términos de uso de energía, que los protocolos basados en CSMA.

- **Conectividad y área de cobertura:** el despliegue de una zona de sensores con alta densidad de nodos, implicará cierto nivel de aislamiento entre ellos y un alto grado de conectividad. Esto sin embargo no implica que no se produzcan cambios en la topología de red, producto del desplazamiento de los nodos móviles o bien de fallas críticas en estos. A su vez, debemos considerar que la visión del medioambiente que tienen un nodo en particular es muy limitada, dado su radio de alcance y precisión. Éste será un parámetro más que se deberá tener en cuenta al momento de diseñar una red de sensores inalámbrica.
- **Agregación de datos:** Dado que los sensores pueden producir una cantidad de datos significativamente redundante, paquetes de datos similares provenientes de diferentes nodos pueden ser pre-procesados a fin de reducir la cantidad de transmisiones que realizan. La agregación de datos es la combinación de datos provenientes de múltiples orígenes, de acuerdo a una función de agregación (por ejemplo, eliminación de duplicados, máximo, mínimo, promedio, etc.). Esta técnica puede ser utilizada para ahorrar energía y optimizar las transmisiones de datos en varios protocolos de ruteo.
- **Calidad de servicio (QoS)**: En muchas aplicaciones se necesita que la información obtenida desde los sensores sea transmitida dentro de un periodo de tiempo, ya que si llegara retrasada ésta sería inservible. De este modo, encontramos que los tiempos empleados para la comunicación de los datos son un factor importante en ciertas aplicaciones donde el tiempo de entrega es una restricción. No obstante, en varias aplicaciones se valora más la optimización del consumo de energía (y por lo tanto el tiempo de vida de la red) que la calidad de los datos enviados. En la medida que la energía se agota puede ser necesario establecer técnicas de ruteo que disipen el consumo por los diferentes nodos, y obtener así mayor tiempo de vida de la red en su totalidad.

### 2.2.1. Protocolos de Ruteo

Existen diferentes formas de clasificar a los protocolos de ruteo, dependiendo del enfoque que se use para realizar esta tarea. Uno de los enfoques posibles nos permite clasificar los protocolos según su estructura, pudiendo ser **Planos, Jerárquicos o Basados en locación.**

Dentro de cada clasificación, mencionaremos brevemente a modo de ejemplo algunos de los protocolos más conocidos y sus particularidades para optimizar las comunicaciones en un entorno de redes de sensores:

I. **Protocolos de ruteo planos:** En esta clasificación todos los nodos de la red tienen un mismo rol, y trabajan juntos en la tarea del sensado. Dado que generalmente estas redes poseen un gran número de nodos, no es factible asignarle un identificador a cada uno. Esto conlleva al desarrollo de un ruteo datacéntrico dónde la estación base envía consultas a ciertas regiones y espera por la información sensada por los dispositivos ubicados en tales regiones. Dado que la información es requerida a través de consultas, se hace necesaria la identificación basada en atributos, de manera tal que, en vez de utilizar direcciones para la consulta a un nodo particular, estas son realizadas a todos los nodos que poseen el atributo buscado. [17]

En el ruteo datacéntrico, a diferencia del basado en dirección o identificación de un nodo, el sink o estación base, envía encuestas solicitando datos específicos a regiones particulares y espera el retorno de los datos de esa región. ***SPIN*** y ***Directed Diffusion*** son dos de los protocolos iniciales que plantearon estas cuestiones, y que motivaron la aparición de otros técnicas datacéntricas basadas en éstos.

- ***SPIN*** (*Sensor protocol for information via negotiation*)

  Es una familia de varios protocolos datacéntricos basados en negociación. EL funcionamiento es común a todos, aplicando distintas variantes según el caso.

  Cada nodo usa una estructura de metadatos para describir el tipo de datos que ha sensado. Luego esta información es transmitida a los demás nodos para negociar si transmitir el dato propiamente dicho o descartarlo, eliminando la información redundante que circula en la red y ahorrando energía. (Es importante para beneficiarse de esta técnica que los paquetes de los metadatos sean más pequeños que los datos en sí).Los nodos vecinos que requieren de esa información, la solicitan y le es transmitida

  Las variantes *SPIN-1 y SPIN-2,* incorporan además del mecanismo de negociación, un manejador de recursos que lleva registro de la energía consumida, información que es solicitada antes de cada transmisión. De esta manera, un nodo que registra un límite inferior en su capacidad de energía, comienza a tener menos participación en las comunicaciones entre nodos vecinos (nodos a un salto de distancia).

  Estos protocolos son aptos para entornos móviles, ya que la decisión de reenvío se basa en la información que tiene de sus vecinos.

  Como desventaja de SPIN, se tiene que no es recomendable para aplicaciones que requieran una periódica fiabilidad de los datos sensado, ya que el mecanismo de

aviso a través de metadatos no garantiza que un dato requerido por un nodo alejado (no vecino), le llegue a tiempo.

- ***Directed Diffusion***

  Los datos generados por los nodos de sensor son referenciados por pares de atributo-valor. La idea principal del paradigma Directed Diffusion es combinar los datos procedentes de fuentes diferentes en una ruta (agregación dentro de la red) eliminando la redundancia, minimizando el número de transmisiones, así ahorrando energía de la red y prolongando su vida útil.

  A diferencia de SPIN donde un nodo publicaba cuando tenía un dato sensado que podría llegar a interesar al resto, este protocolo funciona con un esquema de encuesta por demanda. La estación base o *sink*, solicita información de un tipo (denominados *interest*), y la información se va transmitiendo de nodo en nodo (los cuales van formando aristas con atributo-valor denominadas *gradientes*) por toda la red, y luego la comunicación vuelve con los datos agregados y la respuesta al sink. Mecanismos de cacheo son implementados para mejorar la performance de la red.

  El modelo de consultas por demanda no es recomendado para ambientes donde se requiera monitoreo y envío continuo de datos.

- **ACQUIRE *(Active Query Forwarding in sensor Networks)***

  Este protocolo datacéntrico considera la red de sensores inalámbricos como una base de datos distribuida, dividiendo las consultas realizadas por una estación base en sub-consultas secundarias. Cada nodo responde al pedido con la información que tiene en cache. En caso de no contar con información actualizada, dispara la consulta a sus vecinos hasta tanto poder resolverla. Por último, la información retorna a la estación base por el camino inverso o bien por el camino más corto.

- **EAR *(Energy Aware Routing)****:*

  Este protocolo reactivo, tiene como objetivo incrementar el tiempo de vida de la red. A diferencia de *Directed Diffusion,* mantiene una lista de caminos elegidos aleatoriamente (descartando los más costosos). Al utilizarse estos caminos de manera aleatoria, se produce un balance en el desgaste energético de cada uno de los nodos que componen el camino (suponiendo que todos inician con el mismo estado).

**II. Protocolos de ruteo jerárquicos:** las redes jerárquicas o basadas en cluster, poseen características específicas que las posicionan de manera favorable en términos de escalabilidad y eficiencia. En estas redes, los nodos con mayores capacidades de energía son seleccionados para tareas de pre-procesamiento y traspaso de información, mientras que en los nodos con menor disponibilidad de energía se prioriza la tarea de sensado. Esto

implica la creación de grupos o cluster, y la selección de ciertos nodos coordinadores o clusterheads, los cuales tendrán tareas especiales de agregación y ruteo multisalto de paquetes. Con esta configuración basada en cluster se reduce la cantidad de transmisiones a las estaciones bases, aumentando la performance general en términos de escalabilidad, vida útil de la red y eficiencia energética.

- **LEACH *(Low Energy Adaptive Clustering Hierarchy)***

  El protocolo elige aleatoriamente los coordinadores (*clusterheads*), los cuales van rotando para balancear el gasto energético involucrado.

  Para su funcionamiento, los nodos básicos sensan la información y la envían a su *clusterhead,* el cual realiza la agregación (con lo cual reduce el monto de datos a enviar) y la transmite a su nodo *sink* (solo envía si hubo cambios). LEACH supone que cada coordinador tiene conexión con un *sink*. Los nodos básicos pueden dormir cuando no están sensando.

  Entre las ventajas es su modo distribuido que no requiere de un conocimiento global de la red. Además produce ahorro enérgico debido a la agregación en el clusterhead.

  Como desventaja, el protocolo supone que cada nodo tiene potencia suficiente para transmitir al *sink*. Esto puede llegar a complicarse en redes de área amplia.

- **PEGASIS *(Power-Efficient Gathering in Sensor Information Systems)***

  Es una mejora del LEACH, apuntando a reducir el consumo energético. La idea es que cada nodo solo se comunique con sus nodos vecinos más cercanos (los cuales se detectan en base a la intensidad de la señal) y luego se turnen por rondas para enviar a la estación base. El ahorro energético se produce, por un lado, al generar rondas organizadas y balanceando las comunicaciones de los clusterheads. Por otro lado, al armar los clusters con nodos adyacentes geográficamente, se reduce la potencia necesaria para la trasmisión.

- **TEEN *(Threshold-sensitive Energy Efficient Protocols)***

  En TEEN los sensores se encuentran constantemente sensando la variable física determinada según su aplicación (lo cual lo hace muy adecuado para entornos que requieran un monitoreo continuo), pero las trasmisiones se realizan con menor frecuencia. Se apoya en el principio que es menor el costo energético que se utiliza al sensar, que el utilizado al transmitir a la estación base.

  Al formarse el cluster, se envían a los nodos que lo componen , dos valores: un umbral máximo (*hard threshold*) y un umbral mínimo (*soft threshold).*

  Solo se transmitirá al clusterhead, si el valor sensado supero el umbral máximo determinado Luego el nodo guardará ese último valor trasmitido, y solo volverá a transmitir si un nuevo sensado supera el umbral máximo, con una diferencia mayor al

umbral mínimo. Con esta política se ahorran comunicaciones innecesarias para el dominio de la aplicación, pero se garantiza la trasmisión de los valores críticos.

***APTEEN***, es una versión hibrida de TEEN, que varía en tiempo de ejecución las variables que rigen los umbrales máximos y mínimos, acorde a las necesidades de la aplicación o de un usuario.

**III. Protocolos de ruteo basados en ubicación:** En este tipo de ruteo, los nodos son direccionables por medio de su ubicación. La distancia entre los nodos que interactúan puede determinarse en base a la potencia de las señales entrantes. La coordinación de los nodos puede llevarse a cabo intercambiando información entre nodos vecinos. De manera alternativa, la ubicación de los nodos puede ser establecida directamente, con comunicación satelital, mediante el sistema de GPS, siempre que los nodos estén equipados con receptores GPS de baja potencia. De esta manera, el nodo puede conocer su posición y transmitirla a sus vecinos, pudiéndose armar rutas más eficientes para envío de paquetes según la adyacencia de los nodos.

Otro aspecto a considerar a fines de ahorro de energía en un esquema basado en locación, es la frecuencia y ubicación de los nodos que pasarán a estar en un modo "bajo consumo" o "apagado", para evitar dejar zonas de la red sin cobertura. Esta agenda de desconexión, prioridades de ruteo y selección de coordinadores, serán variables a tener en cuenta al momento de implementar un protocolo

- **GAF (*Geographic Adaptive Fidelity*)**

  GAF es un protocolo basado en locación que fue pensado inicialmente para redes móviles adhoc (*MANETs*), pero su funcionamiento aplica también para las WSN.

  La red es dividas en zonas y se forma una grilla. Dentro de cada zona, se agrupa un conjunto de nodos, los cuales van rotando en su accionar: mientras unos se coloca en modo *sleep*, otro queda despierto y se encarga de las tareas de monitoreo y transmisión.

  Cada nodo usa su geo-posicionamiento para asociarse a una grilla determinada. Mientras más nodos haya asociados a una grilla, más redundancia tendrá esa zona y será energéticamente más duradera.

  Es un protocolo apto para nodos móviles, ya que antes de dejar la zona asignada por su posición, el nodo da aviso a sus vecinos, para que otro tome la posición de cluster de la zona.

  Puede verse al GAF como un protocolo jerárquico orientado a locación, pero sin funciones de agregación como describimos anteriormente que realizan algunos de los protocolos jerárquicos.

- **GEAR *(Geographic and Energy Aware Routing)***

  Utiliza información geográfica y energética al momento de evaluar una ruta hacia un destino. La idea es restringir a una sola región las consultas por demanda (*interest*), y evitar enviarlas a toda la red.

  Cada nodo sabe su propia ubicación y el nivel de energía restante, y aprende sobre todas las ubicaciones de sus vecinos y los niveles de energía restantes a través de un simple mecanismo de intercambio de mensajes “HELLO”. Basándose entonces la ubicación de la región destino y los niveles de energía de los nodos, se establece una métrica para definir la ruta óptima desde la estación base a la región de destino.

Otro tipo de clasificación que se pueden realizar sobre los protocolos de ruteo puede estar enfocada en el tipo de operación que desempeñen. Éstos pueden ser clasificados como basados en múltiples caminos, basados en consulta, basados en negociación, basados en QoS *(Quality of Service)* o basados en coherencia. [17]

- **SAR (*Sequential Assignment Routing*)**

  Es uno de los primeros protocolos pensados para WSN que introduce el uso de Calidad del Servicio (QoS). Las decisiones para el ruteo se basan en tres factores: recursos de energía, QoS en cada camino y nivel de prioridad del paquete. SAR arma un árbol con los caminos posibles entre los nodos y la estación base, descartando los caminos con baja energía o sin garantías de QoS.

Si bien ofrece una buena tolerancia a fallas y recuperación ante cambios de red, es costoso de mantener las tablas de enrutamiento en una red con muchos nodos.

Una tercera clasificación puede ser basada en el momento en que establece la ruta para encaminar los paquetes de datos. En este sentido pueden ser **proactivos o reactivos**. En el caso los protocolos proactivos, las rutas son calculadas antes de ser necesario cualquier envío de datos, armando tablas de ruteo (esta solución es la más indicada para casos donde la topología es más bien estática). En el caso de los protocolos reactivos, las rutas se establecen dinámicamente por demanda (Lo cual se ajusta mejor a redes donde los sensores poseen mayor movilidad, a costa de un mayor consumo energético por cada paquete enviado) [17].

## 2.3. Seguridad de la Información

Como parte del análisis a tener en cuenta al momento de montar una red de sensores inalámbrica, se encuentran los aspectos de seguridad de la información a considerar y que son de vital importancia en pos de preservar los derechos de privacidad y confidencialidad de las comunicaciones.

La seguridad de la información, según los estándares de la familia ISO 27000 [19], consiste en la preservación de la confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

En el contexto actual, con entornos distribuidos y descentralizados, se hace indispensable la transmisión constante de grandes volúmenes de datos a través de redes públicas, atravesando multitud de medios. La necesidad de seguridad ha ido creciendo a medida que crecía esta interconexión global, pero también debido al tipo de información en tránsito. El despliegue de miles de nodos (muchas veces con soporte de hardware y software mínimas) hacen a las WSN susceptibles a posibles ataques por parte de agentes externos.

Un resumen de las amenazas básicas que puede afectar a un sistema de redes inalámbricas de sensores puede profundizarse en [14] y [20].

La principal característica que va a orientar los ataques a estas redes consiste en la naturaleza del medio de comunicación. Las comunicaciones inalámbricas utilizan el espectro electromagnético, por lo que un atacante con la cobertura adecuada podría interceptar la información sin ser detectado. Adicionalmente, muchas de las aplicaciones de estas redes se desarrollan en entornos no controlados e incluso hostiles, por lo que la seguridad física de los sensores tampoco puede controlarse. [14]

Según el esquema mencionado, las características que pueden llegar a verse afectadas son las siguientes:

**Confidencialidad**

Se apunta a que la información de un sistema sea accesible para lectura solamente a aquellas personas, entidades o sistemas autorizados. [19]

La amenaza a la confidencialidad se encuentra en la intercepción de la comunicación por un agente no autorizado, ilustrado en la siguiente figura. La probabilidad de que esto ocurra dependerá del medio físico, siendo por su naturaleza el medio inalámbrico el más propenso a este tipo de vulnerabilidad.

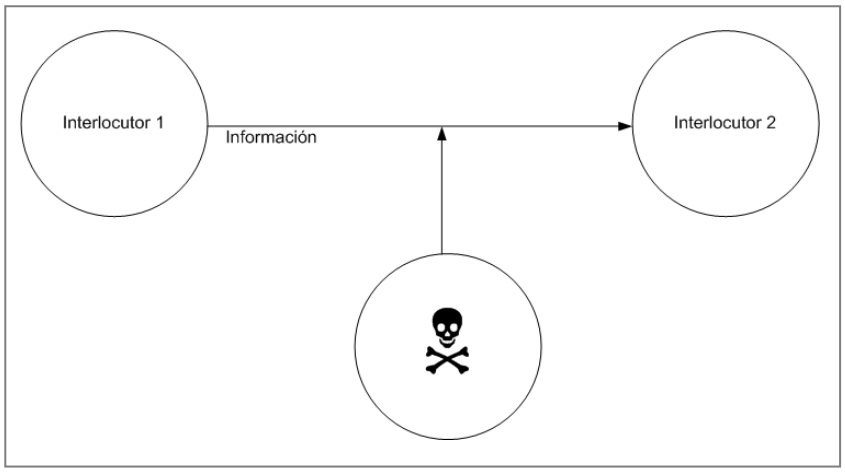
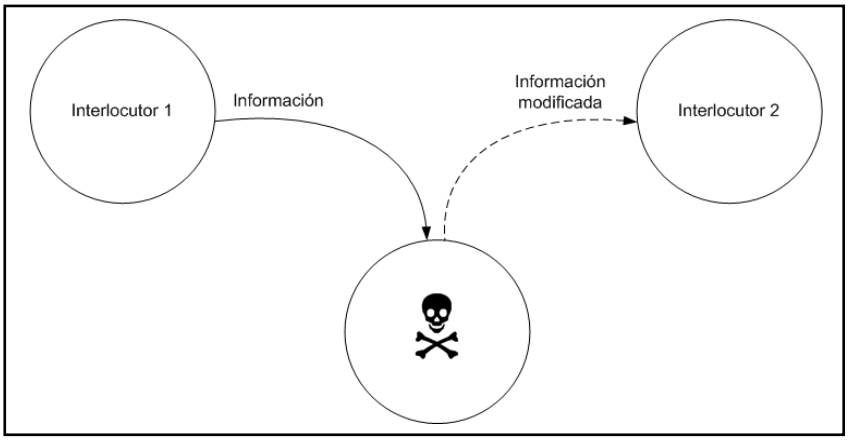



Fig. 6 - Ataque a la Confidencialidad [14]

**Integridad**

Exige que los elementos de un sistema puedan ser modificados solo por aquellas personas, entidades o sistemas autorizados [19]. La modificación incluye escritura, modificación, cambio de estado, borrado y creación.

Las amenazas a la integridad vienen dadas por un acceso no autorizado y por la posibilidad de alterar la información en tránsito. Al igual que el caso de la intercepción, la probabilidad de éxito de esta amenaza dependerá de la facilidad del atacante de acceder al




canal, pero sus efectos pueden ser muy perjudiciales si no es detectado.

Fig. 7 - Ataque a la Integridad [14]

**Disponibilidad**

Exige que todos los elementos de un sistema estén disponibles a los grupos autorizados.

La amenaza a la disponibilidad se encuentra en la interrupción de las comunicaciones, ya sea interviniendo sobre el medio, sobre los interlocutores o sobre los elementos intermedios involucrados en la comunicación, como se ilustra en la siguiente figura.

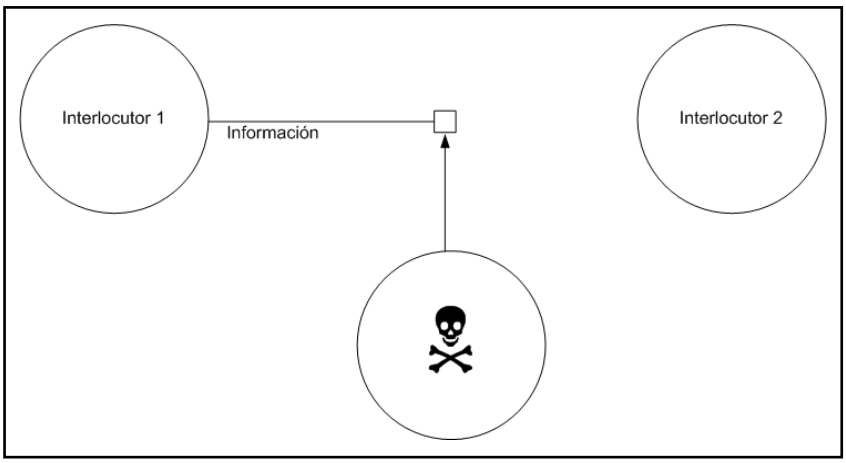



**Fig. 8 - Ataque a la Disponibilidad [14]**

*En consonancia con la importancia de la seguridad en los ambientes de redes de sensores y más específicamente en el contexto del Internet de las Cosas (IoT), el Senado de Estados Unidos publicó un proyecto de Ley en el año 2017 para regular la seguridad de los dispositivos y equipamiento que se adquiera por parte de las diferentes agencias de Gobierno. Entre otras cosas exige buenas prácticas de seguridad en equipos con salida a internet como cámaras, routers u otro tipo de dispositivos. Por ejemplo, se prohibiría que un usuario y contraseña venga configurado por defecto en el software (harcoded) y no pueda cambiarse. [21]*

## 2.4. Internet de las Cosas

Un concepto muy utilizado y pocas veces aclarado en los últimos años en el campo del TICs, viene dado por el **Internet de las Cosas o IoT** *(Internet of Things*).

En el desarrollo del presente trabajo haremos mención a muchas tecnologías en materia de hardware y software, protocolos y aplicaciones concretas que vienen a cubrir una demanda existente en el campo del IoT. Un negocio que estima conectar 1500 millones de dispositivos para el año 2022 según estimaciones de la empresa Ericsson [22] o incluso hasta 50 mil millones según otras estimaciones. [23]

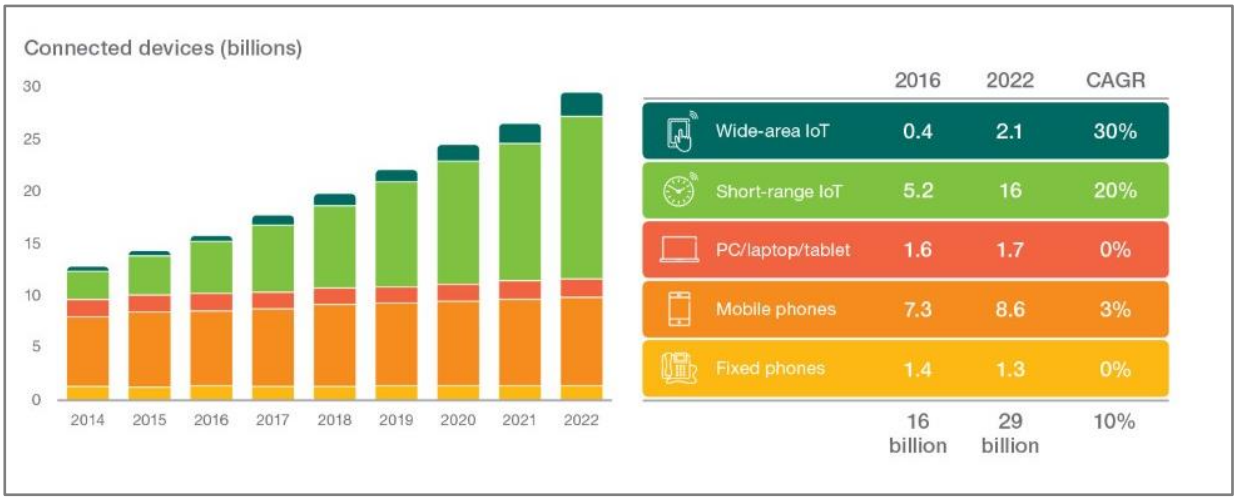



**Fig. 9 - Estimaciones dispositivos conectados [22]**

Antes de pasar a desarrollar distintas tecnologías que darán sustento a este paradigma, nos resulta primordial poder establecer un marco definitorio para el Internet de las Cosas.

La UIT (Unión Internacional de Telecomunicaciones) lo define como la "*Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación presentes y futuras.*

*Aprovechando las capacidades de identificación, adquisición de datos, procesamiento y comunicación, IoT utiliza plenamente las "objetos" para ofrecer servicios a todos los tipos de aplicaciones, garantizando a su vez el cumplimiento de los requisitos de seguridad y privacidad*". [24]

Cuando se habla de objetos en este contexto se involucra, por ejemplo al entorno que nos rodea, los robots industriales, los bienes, los equipos eléctricos y software de aplicaciones.

La conexión de estos objetos de mundo físico y virtual con una infraestructura de comunicación viene dado por el uso de **dispositivos** que son equipos con "… *capacidades obligatorias de comunicación y capacidades opcionales de detección, accionamiento, adquisición, almacenamiento y procesamiento de datos…"* recabando... *"…diversos tipos de información y suministrándolo a las redes de la información y la comunicación para su ulterior procesamiento".* [24]

Las aplicaciones IoT son de diversos tipos, por ejemplo, "sistemas de transporte inteligente", "red de suministro eléctrico", "cibersalud" o "hogar inteligente". [24]

En relación con estas definiciones, aparece íntimamente relacionado el concepto de "**Ciudad Inteligente**". Analizaremos en el Capítulo 5 más profundamente este campo,

diferentes normativas internacionales que comienzan a regular su aplicación y el aporte que las redes de sensores inalámbricas pueden hacer en este terreno.

# 3. Estándares para WSN

En la actualidad tenemos variados protocolos, muchos de los cuales han sido estandarizados por diferentes organizaciones conformadas por distintos actores de la industria. En muchos casos comparten un mismo dominio de aplicación, volviéndose competidores en el mercado, sin embargo, en otros casos se observan marcadas diferencias que los hacen a unos más aptos para ciertos entornos (como ser el caso de ISA y Wireless Hart para industria), pero con limitaciones en otros contextos.

Antes de pasar a describir un conjunto de protocolos que nos resultaron de interés, nos resulta primordial mencionar los estándares de diferentes organizaciones.

El grupo de trabajo de la IEEE 802.15 basó sus estándares en distintas alternativas para redes de área personal inalámbricas o WPAN (*Wireless Personal Area Network*), siendo las WPAN una de las iniciativas que sirvieron de punto de partida para muchas de las tecnologías de redes de sensores utilizadas hoy en día. La IEEE ideó tres clases diferentes teniendo en cuenta su rango de datos, consumo de energía y calidad de servicio (QoS). Las WPAN **802.15.3** son las de mayor velocidad, pensadas para transmisión de aplicaciones multimedia con altos niveles de QoS. Las WPAN **802.15.1** (bluetooth), con velocidades y consumos intermedios. Y por último las WPAN **802.15.4** (también clasificadas con las siglas LR-WPAN, por *low rate* - WPAN), sobre la cual se basan las especificaciones de muchos de los protocolos para redes de sensores de corto y medio alcance y baja tasa de datos. Sobre estas últimas indagaremos más en este capítulo.

Una alternativa a las redes definidas en la IEEE, lo conforman protocolos basados en el estándar **ISO/IEC 14543-3-10** *Wireless Short-Packet Protocol* (Protocolo inalámbrico de paquetes cortos) y la recomendación **ITU G.9959** (Transceptores de radiocomunicación digital de corto alcance y banda estrecha).

Otro enfoque para redes de sensores es posible con las redes del tipo **LPWAN** (*Low Power Wide Area Network*). Detallaremos dos de los protocolos más importantes para redes de sensores con menor tasa de datos pero con mayor alcance, como lo son SigFox y LoraWAN, como así también dos alternativas sobre redes celulares que son LTE-M y NB-IOT, todos éstos propicios para el desarrollo de aplicaciones urbanas e interurbanas.

Se resume en la siguiente figura, un gráfico comparativo de los distintos protocolos a desarrollar:

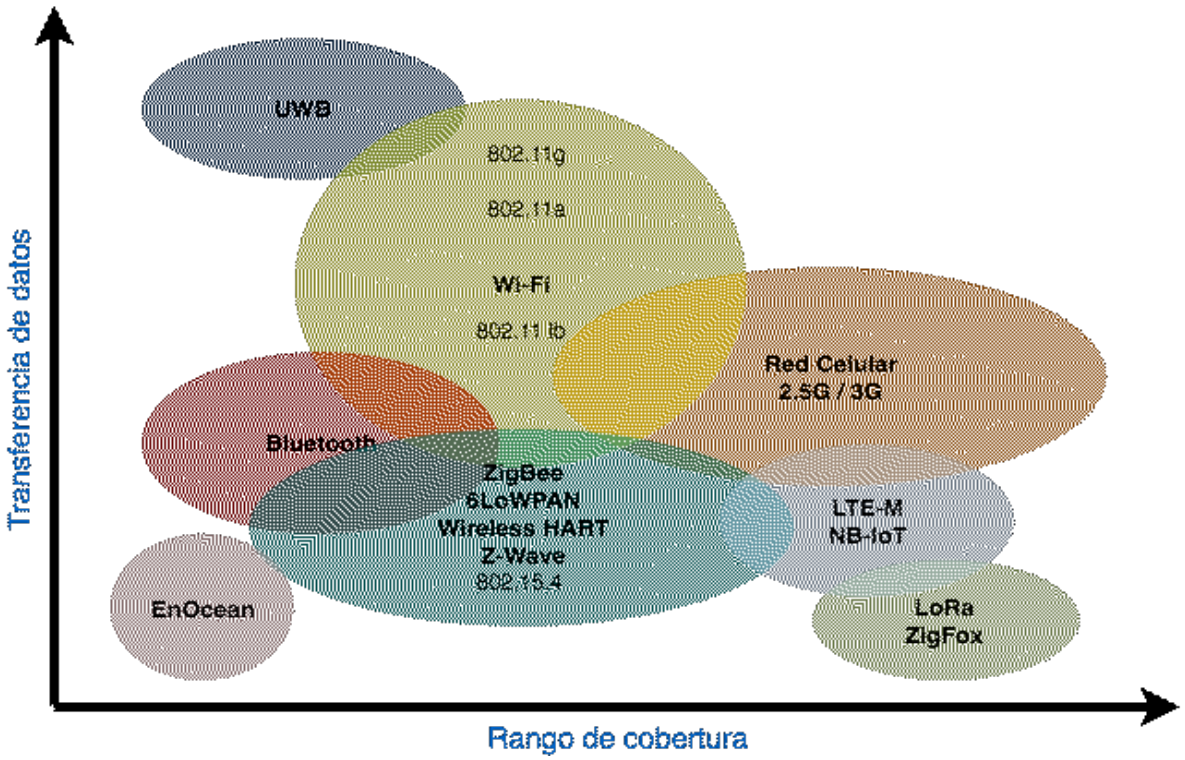



Fig. 10 - Protocolos para redes de sensores

## 3.1. IEEE 802.15.4

Este estándar nace como producto del grupo de investigaciones 802.15 de la IEEE, especializado en el desarrollo de tecnologías inalámbricas de área personal (WPAN).

IEEE 802.15.4 (primer versión publicada en el año 2003) es un estándar que define el nivel físico y el control de acceso al medio de redes inalámbricas de área personal con tasas bajas de transmisión de datos (*low-rate wireless personal area network,* LR-WPAN). La actual revisión del estándar se aprobó en 2011.

Es la base sobre la que se define la especificación de ZigBee, 6LoWPAN y otros protocolos que analizaremos a continuación, cuyo propósito es ofrecer una solución completa para este tipo de redes construyendo los niveles superiores de la pila de protocolos que el estándar no cubre.

Entre las características provistas por el estándar podemos resumir las siguientes:

- Topología en forma estrella o punto a punto.
- Manejo de direcciones únicas de 64 bits o direcciones cortas de 16 bits.
- Alocación de tiempos de transmisión garantizados (*guaranteed time slots, GTS*).
- Acceso al canal mediante el uso de CSMA-CA *(carrier sense multiple access with collision avoidance)* o ALOHA.
- Confirmación de paquetes (*ACS*) para fiabilidad de las comunicaciones.
- Diseño de las tramas para bajo consumo, manteniendo una complejidad mínima, pero a la vez garantizando una robustez en canales ruidosos.
- Indicación de calidad del enlace.

**Topología de Red**

En una red 802.15.4 pueden participar dos tipos de dispositivos: el FFD (*full-function device*), con mayor capacidad de procesamiento y energía, capaz de actuar como coordinador de una red y el RFD (*reduced-function device*) que sería un dispositivo con capacidades de hardware y batería reducidas, que no puede actuar como coordinador y que se encuentra asociado a un coordinador para transmitir su información.

El estándar IEEE 802.15.4 soporta múltiples topologías para su conexión en red, entre ellas estrella y punto a punto (*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.

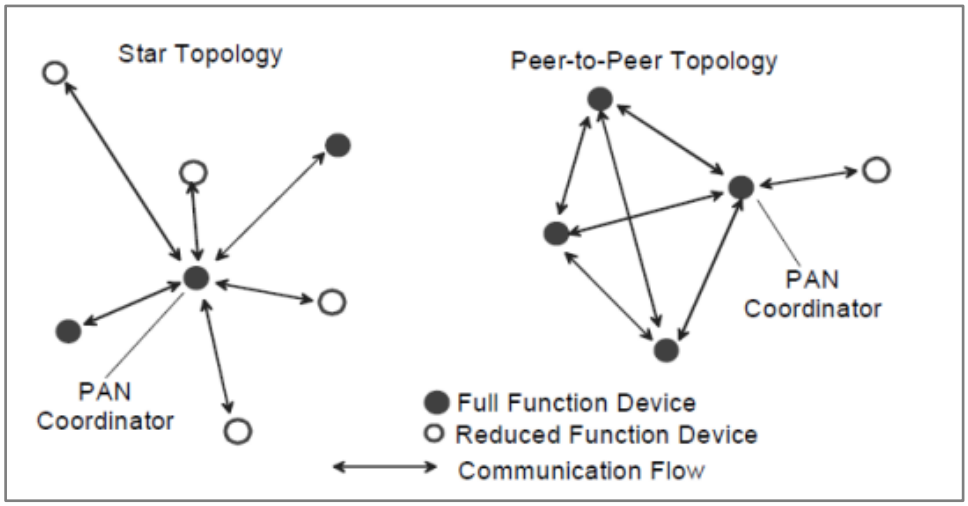



**Fig. 11 - Topologías Estrella y Punto a Punto [13]**

En la topología de **Estrella** la comunicación es establecida entre los dispositivos y un controlador central, denominado el Coordinador de red PAN.

En las comunicaciones ***Peer to Peer,*** también existe la figura del coordinador de red, pero con la diferencia que un dispositivo puede comunicarse con cualquier otro de la red siempre y cuando esté dentro del rango de alcance.

Todo los dispositivos que operan en la red (cualquiera fuera su topología) tendrán un única dirección de 64 bits (denominada dirección extendida) y una dirección corta de 16 bits asignada por el coordinador cuando el dispositivo es asociado a la red.

Las redes *Peer to Peer* permiten el armado de formaciones de red más complejas, como mallas o árboles, pudiéndose establecer caminos multisalto entre los participantes. Esta funcionalidad debería ser complementada con servicios de capas superiores no cubiertas por este estándar. [13]

**Arquitectura 802.15.4**

Un dispositivo estará compuesto de al menos una capa física (PHY), que contendrá el transceptor de radio frecuencia con su mecanismo de control, y una capa de control de acceso al medio (MAC) que proveerá el acceso al canal físico para todo tipo de transferencias. Las capas superiores, le brindarán los servicios para manejo de la red (capa de red) y aspectos funcionales (capa de aplicación). Estas capas superiores no son definidas en el alcance del IEEE 802.15.4. Se observa en la siguiente figura una abstracción de la arquitectura mencionada:

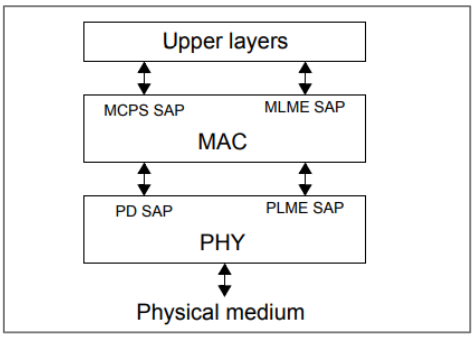



Fig. 12 - Arquitectura dispositivo LR-WPAN [13]

**Estructura de las tramas**

IEEE 802.15.4 define cuatro tipo de tramas: beacon, comando, ack y datos.

Si bien la capa física admite un tamaño de paquete máximo de **127 bytes**, la carga útil de datos (payload), en el peor de los casos puede llegar a ser 81 bytes, debido a las diferentes cabeceras involucradas. A saber:

*MaxPHYPacketSize (127 bytes, máximo tamaño de paquete de la capa física) – MaxFrameOverhead (25 bytes) – MaxSecurityFrame (21 bytes si se usa AES 128 )*= **81 bytes**

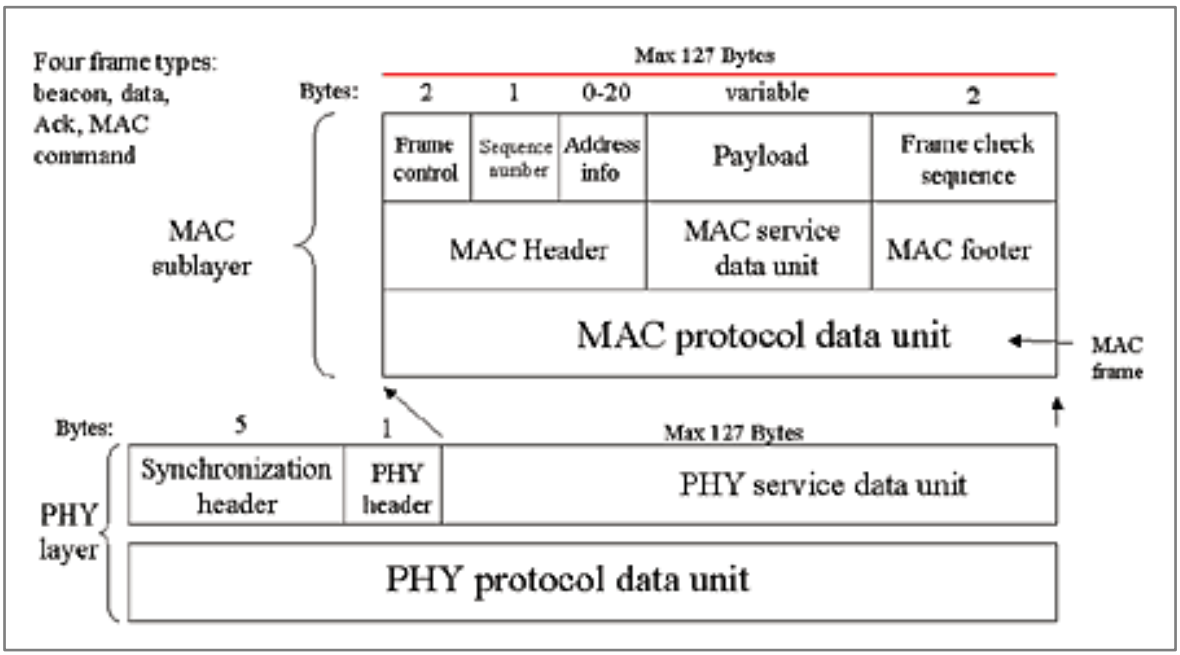



Fig. 13 - Formato capas MAC y PHY [25]

**Capa MAC**

La pila de protocolos de la IEEE 802 divide a la capa de Enlace de Datos (DLL o *Data Link Layer)* en dos sub capas, la sub capa de enlace de acceso a medios (*Medium Access Control,* MAC) y la subcapa de control de enlaces lógicos (*Logical link control*, LLC). El LLC es común a todos estándares 802, mientras que la sub capa MAC dependerá del hardware de radio frecuencia involucrado.

Entre las funciones de la subcapa MAC podemos enumerar:

- La asociación y la disociación a un coordinador de la red PAN. Con tramas especificas pensadas para tal fin, un coordinador que desea armar una PAN, comenzará la misma enviando *beacons*, "avisando" a otros dispositivos que estén dentro del rango que se quieran unir. Luego mediante un mecanismo *request-response* (solicitud y respuesta), se produce la asociación de un nodo a la red. De manera similar, tanto el coordinador como un nodo de la red, puede solicitar la disociación (baja) de la PAN a la que se encuentra dado de alta.
- Reconocimientos de entrega de trama (*acks*), enviados por el receptor una vez que se ha recepcionado correctamente un paquete (en el caso que sea solicitado por el emisor en el encabezado de la trama original).
- Mecanismos de acceso al canal. Puede utilizar *CSMA-CA*, donde el dispositivo antes de trasmitir sensa el canal y solo transmite si se encuentra inactivo, caso contrario espera un tiempo aleatorio y vuelve a chequear la disponibilidad. La otra opción es *ALOHA,* donde el dispositivo directamente transmite al medio, sin tener en cuenta si otros están transmitiendo. Esta última opción puede ser apropiada en redes con poca cantidad de nodos o envíos poco frecuentes, donde las probabilidades de colisión son menores.
- Validación de tramas, calculando un CRC de 16 bits sobre el encabezado de la trama MAC y sobre la porción de datos (*payload*).
- Garantía del manejo de las ranuras de tiempo y manejo de balizas (*beacons*). La subcapa MAC puede funcionar con dos modos: con o sin *beacons.* En el primer caso se utiliza una estructura denominada *Superframe* que permite reservar espacios de tiempo fijo para algunos dispositivos con comunicaciones críticas. En el modo sin beacons, no hay reservas del canal y la comunicación funciona normalmente compitiendo por el mismo.

**Capa Física - PHY**

El rango de frecuencias sobre el cual pueden operar los dispositivos compatibles con este estándar son 780MHz, 868MHz, 915MHz y 2450MHz, pudiendo utilizar hasta 27 canales.

Los tipos de modulación posibles son: O-QPSK, MPSK, BPSK, ASK, GFSK, que dependiendo de su aplicación en las diferentes frecuencias mencionadas nos darán la tasa máxima de datos (kb/s), las cuales van desde los 20kbps hasta 250kbps como máximo. [13]

La capa física definida en este estándar será la responsable de las siguientes tareas:

- Activación y desactivación del radio transceptor.
- Recepción y transmisión de paquetes.
- Detección de energía en el canal de operación actual. Es un estimado de la potencia de la señal recibida lo cual sirve de parámetro al algoritmo que seleccionará el canal sobre el cual operar.
- Seleccionar frecuencia de operación.
- Gestionar el indicador de calidad de enlace en los paquetes recibidos (LQI, *link quality indicator*). Esta medida es una métrica de la fuerza/calidad de la señal, que podría llegar a ser usado por capas superiores.
- Evaluación del canal y sensado de la portadora para evitar colisiones (CSMA-CA).

**Seguridad Implementada**

El estándar IEEE 802.15.4 establece una serie de medidas que permitirán autenticar a los dispositivos que formen parte de la red, imposibilitando que se asocien a la misma, dispositivos que no estén autorizados.

La seguridad se obtiene del cifrado simétrico, el cual cubrirá los requisitos de confidencialidad e integridad. El algoritmo de cifrado usado es AES (*Advanced Encryption Standard*) con una longitud de claves de 128 bits (16 Bytes).

Este algoritmo no solo se utiliza para cifrar la información, sino también para validarla. Mediante un “código de integridad del mensaje” (MIC), también denominado “código de autenticación del mensaje” (MAC), añadido al final del mensaje, se consigue dotar de integridad a las comunicaciones. Este código asegura la integridad de la cabecera MAC y del *payload* (datos de aplicación), a la vez que asegura que el emisor es quien dice ser.

La trama se construye cifrando ciertas partes de la cabecera MAC con la clave que establezca la política de gestión de claves, y que será conocida por los nodos que se estén comunicando. El estándar no especifica cómo han de gestionarse las claves o las políticas de autenticación que deben aplicarse. Estas tareas deben ser tratadas por las capas superiores, por ejemplo las capas provistas por ZigBee o 6LoWPAN.

Si se recibe una trama de algún nodo no confiable, el código MIC generado no corresponderá con el que fue enviado en la trama, al haberse generado con una clave diferente. El código MIC puede tener varios tamaños, 32, 64 y 128 bits, aunque siempre se

construye utilizando el algoritmo AES de 128 bits. Este tamaño únicamente indica cuántos bits se añadirán al final de cada trama. La confidencialidad de las comunicaciones se conseguirá cifrando el contenido del *payload* mediante el algoritmo AES y una clave de 128 bits. [26]

## 3.2. ZigBee

ZigBee es un estándar que define un conjunto de protocolos para el armado de redes inalámbricas de corta/media distancia y baja velocidad de datos.

Este estándar fue desarrollado por la Alianza ZigBee, que tiene a cientos de compañías desde fabricantes de semiconductores y desarrolladores de software a constructores de equipos OEMs e instaladores. Desarrolla un protocolo que adopta al estándar IEEE 802.15.4 para sus 2 primeras capas, es decir la capa física (PHY) y la subcapa de acceso al medio (MAC) y agrega la capa de red y de aplicación.

El estándar ZigBee fue diseñado para cumplir con las siguientes especificaciones:

- Ultra bajo consumo y baja potencia que permita usar equipos a batería .
- Bajo costo de dispositivos y de instalación y mantenimiento de ellos.
- Alcance corto (típico menor a 50 metros. Dependiendo del radio utilizado se puede extender este alcance).
- Optimizado para ciclo efectivo de transmisión menor a 0.1 %.
- Velocidad de transmisión menor que 250kbps. Típica: menor que 20kbps.
- Puede trabajar tanto en las bandas de 2.4GHz como en la de 868/915MHz.
- Utiliza la modulación DSSS *(Direct Sequence Spread Spectrum)*, para lograr menor interferencia en las comunicaciones.
- Usa CSMA-CA *(Carrier Sense Multiple Access Collision Avoidance)* para acceso al canal.
- Produce alto rendimiento y baja latencia para dispositivos de bajo ciclo de trabajo, muy adecuado para el uso de sensores y controles.
- 64 bits de direccionamiento determina una cantidad máxima de1.8.10 ^19 dispositivos.
- 16 bits para identificar redes que determina un total de 65536 redes.

### Tipos de nodos ZigBee

El estándar especifica 3 tipos de nodos que pueden estar en una red: coordinador, ruteador y dispositivo final.

- Coordinador: es obligatoria la presencia de uno y solo un nodo coordinador dentro de la red. Actúa como nodo raíz en la topología árbol y es responsable del arranque de la red, configuración de los parámetros de red (PAN ID, establecer el canal a usar), admisión de nodos y asignación de direcciones de red. Según las políticas de seguridad definida, podrá actuar como “Centro de confianza” de la red.

El coordinador requiere de un dispositivo de función completa (FFD) ya que necesita más potencia de cómputo. También es importante que la fuente de alimentación sea permanente y segura ya que este dispositivo nunca entrará en modo “dormir”.

- Ruteador: es un nodo de tipo FFD pero que no es el coordinador. La utilidad de éstos es para extender la cobertura de la red y para aumentar la confiabilidad con la creación de rutas adicionales de datos. Considerando que puede encaminar paquetes de dispositivos asociados, tampoco podrá entrar en modo “dormir”.
- Dispositivo final: estos nodos se pueden comunicar con un nodo ruteador o un nodo coordinador. Estos nodos tienen menos potencia de cómputo y usualmente son alimentados a batería. Son dispositivos de funcionalidad reducida (RFD) según el estándar IEEE 802.15.4. [18]. Pueden dormir largos periodos de tiempo y luego levantarse para sensar una magnitud específica y trasmitirla.

**Manejo de capas**

Dado que es un estándar, y para lograr interoperabilidad entre distintos fabricantes que implementen ZigBee, el protocolo se organiza en capas las cuales se separan modularmente en componentes y funciones. En la figura a continuación se muestran las capas del protocolo ZigBee. Estas se basan en el modelo de referencia ISO para interconexión de sistemas abiertos OSI. Este modelo cuenta con 7 capas, pero ZigBee usa solo 4 capas con el objeto de simplificar la arquitectura para el armado de una red de baja tasa de transmisión, simple y de bajo consumo. Las 2 capas inferiores, o sea la capa física (PHY) y la capa de acceso al medio (MAC) son las definidas por el Estándar IEEE 802.15.4. Las capas de red (NWK) y de aplicación (APL) se definen en ZigBee. Cada capa se conecta con las capas adyacentes por medio de un SAP (*Service Access Point*).

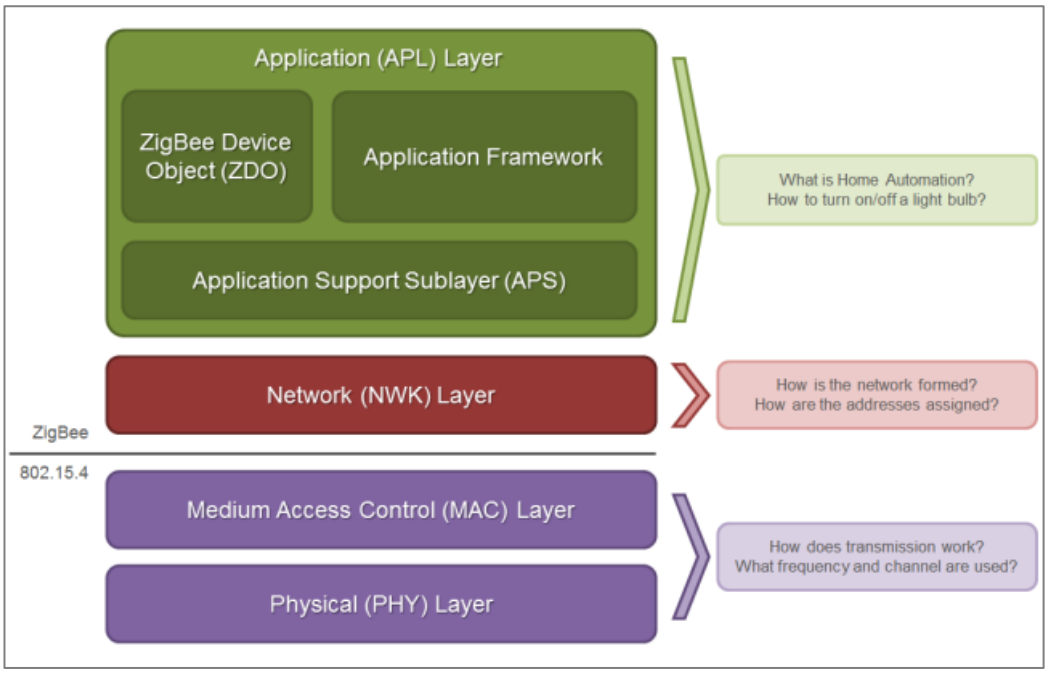



**Fig. 14 - Capas ZigBee [27]**

Para las capas Física (**PHY**) y Capa de acceso al medio (**MAC**), aplican los mismos conceptos desarrollados anteriormente en el apartado del estándar IEEE 802.15.4. ZigBee hará uso de estas capas pre definidas para disponer entre otras cosas de servicios para acceso al medio, seleccione de canales, definir potencias de transmisión, definir calidad de los enlaces, asociación de nodos, encriptación de las tramas, entre otros.

Se menciona alguna de las funciones de las dos capas implementadas por el protocolo ZigBee, la capa de red y la de aplicación:

**Capa de red (NWK)**

**Funcionamiento del Protocolo**

La capa de red provee a ZigBee funciones para el armado y manejo de redes y una interfaz simple para relacionarla con las aplicaciones de los usuarios.

Antes que un nodo ZigBee pueda conectarse con la red debe unirse a una red existente o bien formar una nueva. Solo los nodos coordinadores pueden formar una nueva red a la cual se le asigna un identificador “PAN ID”. Cada nodo se identifica inicialmente con su dirección MAC de 64 bits. Luego en el proceso de asociación a la red, se le asigna una nueva dirección más corta de 16 bits, que será la utilizada para comunicarse con otros nodos a través de la red (de esta manera se ahorra espacio en cabeceras).

Como ya se mencionó, ZigBee usa las topologías de IEEE 802.15.4 para transferencia de datos y agrega las topologías de árbol y de malla. Debido al relativo alcance de cada nodo, frecuentemente un paquete debe ser retransmitido varias veces por intermedio de ruteadores. Lo destacable es que el ruteo en cualquier topología usada se hace en la capa de red y entonces no es necesaria ninguna programación adicional en la capa de aplicación. Gráficamente podemos observar las topologías de red que pueden armarse:

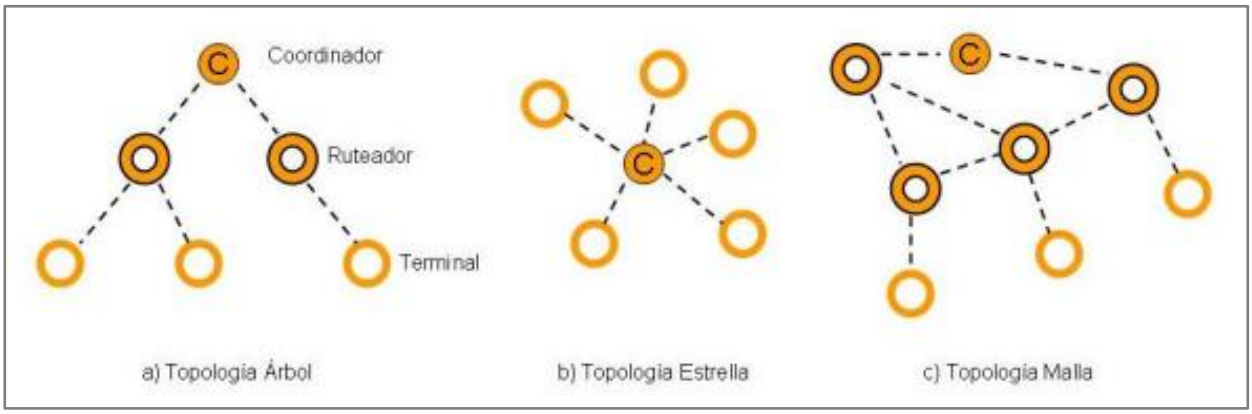



**Fig. 15 - Topologías ZigBee [18]**

**Topología estrella**

- Es la más sencilla. Corresponde a la topología estrella de la IEEE 802.15.4.
- Un coordinador con uno o varios nodos hijos.
- El rango de la red está limitado al rango de transmisión del coordinador.
- La red es fácil de configurar.
- El coordinador es el único nodo que rutea paquetes.
- Es un caso especial de la topología árbol. Es un árbol con profundidad máxima 1.

**Topología árbol**

- Los nodos ruteadores pueden tener nodos hijos.
- Hay comunicación directa solo a través de la relación padre-hijo.
- Ruteo jerárquico con un único camino posible entre 2 nodos.

**Topología malla**

- Es una extensión de la topología de comunicación entre pares (peer to peer).
- Los nodos ruteadores pueden tener nodos hijos.
- Hay comunicación directa entre dos nodos FFD siempre que estén separados a una distancia menor al rango de transmisión entre ellos.

- Los nodos terminales solo pueden intercambiar datos con sus respectivos nodos padres.
- Es posible el ruteo dinámico. El mejor salto en una ruta es una optimización de gasto energético, tiempo, seguridad y confiabilidad. [18]

**Ruteo**

Existen 3 tipos de comunicación de mensajes: broadcast, multicast y unicast:

- Un mensaje tipo *broadcast* tiene como destino a todo dispositivo que lo pueda recibir.
- Un mensaje *multicast* se envía solo a un grupo de dispositivos.
- Un mensaje *unicast* contiene la dirección de un único dispositivo.

A fines de la comunicación, en la capa de red se implementa un algoritmo que permite balancear entre costo por unidad, gasto de batería, complejidad de implementación para lograr una relación costo desempeño adecuada a la aplicación. Un algoritmo muy utilizado por su simplicidad y bajo requerimiento de procesamiento es el AODV *(Ad hoc On-Demand distance Vector)*, definido en la RFC 3561 [28].

Con AODV, al ser un protocolo reactivo, los nodos mantienen una tabla de ruteo para los destinos conocidos, y en caso de querer conectarse con un nodo cuya ruta es desconocida disparan una serie de mensajes de descubrimiento para encontrar la nueva ruta, es decir, lo hacen por demanda.

Mientras la ruta se mantenga activa, el AODV se encuentra pasivo, hasta tanto se produzca una modificación de la misma y cada uno de los nodos involucrados deba actualizar nuevamente sus tablas de ruteo con los nuevos “saltos” descubiertos (ZigBee permite hasta 30 saltos intermedios en una ruta de extremo a extremo).

En este contexto AODV presenta dos ventajas: por un lado no consume excesivos recursos para mantener actualizadas sus tablas de ruteo (de hecho ZigBee utiliza una adaptación de AODV escalado para dispositivos con memoria RAM de entre 2 y 4Kb), y por otro lado, permite dinámicamente ajustar las rutas ante inconvenientes que se vayan dando en el uso de la misma. [29]

Entre las responsabilidades de la capa de red podemos resumir las siguientes:

- Establecer una nueva red brindando topologías como árbol o malla.
- Agregar o quitar a un dispositivo a/de la red.
- Garantizar la comunicación dentro de toda la red más allá del alcance de un único nodo.
- Asignar direcciones de red a los dispositivos brindando una interfaz unificada para todos ellos.

- Sincronizar entre dispositivos usando balizas (beacons).
- Descubrimientos de vecinos y actualización de rutas para encaminar paquetes.
- Proveer mecanismos de seguridad.

**Capa de aplicación (APL)**

La **Capa de Aplicación** juego un rol fundamental en la interoperabilidad entre aplicaciones de distintos fabricantes. Incluye a la vez 3 subcapas: Subcapa de Soporte de Aplicaciones o APS *(Application support sublayer)*, Objetos Dispositivos ZigBee o ZDO *(ZigBee Device Object)* y Framework de Aplicación.

La capa de aplicación (APL) en ZigBee es la que se encarga de las aplicaciones específicas de los usuarios. El desarrollo de las aplicaciones se ve facilitado por el hecho de que la APL tiene interfaces a la capa RED.

Entre las funciones de esta capa podemos mencionar:

- Mantener los enlaces entre los dispositivos que comportante un mismo servicio y descubrir nuevos dispositivos que lo compartan. Por ejemplo, se podrían buscar todos los dispositivos del tipo “lámpara”, para agregarlo a nuestra lista de dispositivos controlables en un ambiente de domótica.
- Gestión de Perfiles. Un perfil caracteriza tipos de dispositivos, formato de los mensajes, acciones y funciones que se usarán en ciertas aplicaciones. Estos podrán ser Públicos (que permiten a otros fabricantes acceder a través de una interfaz) o Privados (que son exclusivos de un fabricante para brindar funcionalidades propietarias).
- Simplificar el manejo de la red por parte de las aplicaciones de los usuarios (haciendo uso de los Objetos ZigBee o ZDO), por ejemplo, descubriendo dispositivos vecinos o manejando potencia de trasmisión.
- Manejo de Clusters. Los clústeres son un grupo de comandos y atributos que definen lo que un dispositivo puede hacer. Un dispositivo puede admitir varios clústeres para realizar una variedad de tareas. La mayoría de los clústeres son definidos por Alianza ZigBee y se listan en la librería de cluster ZigBee (o *ZCL*) [30]. Algunos ejemplos de cluster son:
    - 0x0006 - On/Off (Switch)
    - 0x0008 – Nivel de control (Dimer)
    - 0x0201 - Termostato
    - 0x0202 – Control de ventilador
    - 0x0402 – Control de temperatura
    - 0x0406 – Sensor de ocupación

**Seguridad implementada**

ZigBee implementa dos capas de seguridad adicionales en la parte superior de la 802.15.4: las capas de seguridad de Red y Aplicaciones. Todas las políticas de seguridad se basan en el algoritmo de cifrado AES 128, por lo que la arquitectura de hardware implementada previamente para el nivel de enlace (capa MAC) sigue siendo válida. Cada capa del protocolo (APS, NWK y MAC) es responsable de la seguridad de las tramas iniciadas en esa capa. Por simplicidad se usa una misma clave para todas las capas.

En el esquema de seguridad planteado se incorpora la figura del "Centro de confianza" o *Trust Center.* Este nodo será el encargado de gestionar las claves para encriptación de toda la comunicación que se genere en la red.

Hay tres tipos de claves: maestro, enlace y claves de red. [26]

- Claves Maestras: Puede venir preinstaladas en cada nodo de fábrica o ser enviada en una comunicación inicial con el *Centro de confianza*. Su función es mantener confidencial el intercambio de claves de enlace entre dos nodos en el procedimiento de establecimiento de clave (*SKKE- Symmetric-Key Key Establishment*).
- Claves de Enlace: Son únicas entre cada par de nodos. Estas claves son administradas por el nivel de aplicación. Se utilizan para cifrar toda la información entre cada uno de los dos dispositivos. Utiliza la clave maestra en el handshake (intercambio de mensajes) inicial, hasta tanto se establezca la clave de enlace para cifrar las comunicaciones entre dos nodos específicos. Permite crear un túnel virtual entre dos nodos de la red.
- Clave de red: Es una clave única compartida entre todos los dispositivos de la red. Es generado por el *Trust Center* (que es normalmente el coordinador o un nodo dedicado) y regenerado a intervalos diferentes. Cada nodo tiene que obtener la clave de red para unirse a la red. Una vez que el centro de confianza decide cambiar la clave de red, la nueva se distribuye a través de la red utilizando la antigua clave de red. El nodo coordinador o Centro de Confianza dedicado es quien debe autenticar y validar cada dispositivo que intenta unirse a la red.

Entre cada par de dispositivos pueden utilizarse siempre ambas claves, de Red y de Transporte. En el caso de utilizar siempre las claves de transporte, será necesario más espacio de memoria reservado.

Para garantizar la integridad la autenticidad e integridad de los datos, es decir, que los mismos son válidos y que no sufrieron transformación alguna, el transmisor acompaña al

mensaje con un código especial que en ZigBee lo llaman Código de Integridad de Mensaje (MIC: Message Integrity Code). El MIC se genera con un método que conocen tanto el emisor como el receptor, de manera que un dispositivo no autorizado no debería poder crear este MIC. ZigBee y 802.15.4 soportan MIC de 32, 64 y 128 bits.

Si lo que se desea es tener confidencialidad lo que se debe hacer es encriptar el mensaje.

EL MIC en ZigBee se genera usando el protocolo CCM* (*Enchanced Counter with Cipher Block Chaining Message Authentication Code*) en conjunto con AES de 128 bit [31]. Además de cifrar la información, lleva asociado un contador de tramas, de manera de garantizar que un intruso no retenga el mensaje y lo envíe más tarde. En caso que se intente modificar el contador de tramas, el MIC calculado no coincidirá con el MIC del mensaje, desechándose el mismo.

Se brinda más detalle del funcionamiento, configuración y performance de los nodos ZigBee sobre la arquitectura del integrado XBee de la empresa DIGI, en el desarrollo del prototipo en la parte 2 del presente trabajo.

## 3.3. 6LoWPAN

El estándar 6LoWPAN es desarrollado por la IETF (Internet Engineering Task Force, la organización que está a cargo de todos los estándares de Internet para garantizar su interoperabilidad) como una capa de adaptación entre la capa de red (IP) y las capas inferior. Concretamente el propósito del estándar es la comunicación IPv6 con la tecnología de comunicación inalámbrica de "baja potencia y comunicación con pérdidas" (*LLN - Low Power and Lossy Networks* en los términos de la IETF) ofrecido por el IEEE 802.15.4.

Al igual que en 802.15.4 se permite el armado de redes estrella o *peer-to-peer.* También permite el armado de redes Mesh, involucrando en este caso a capas superiores (capa de red).

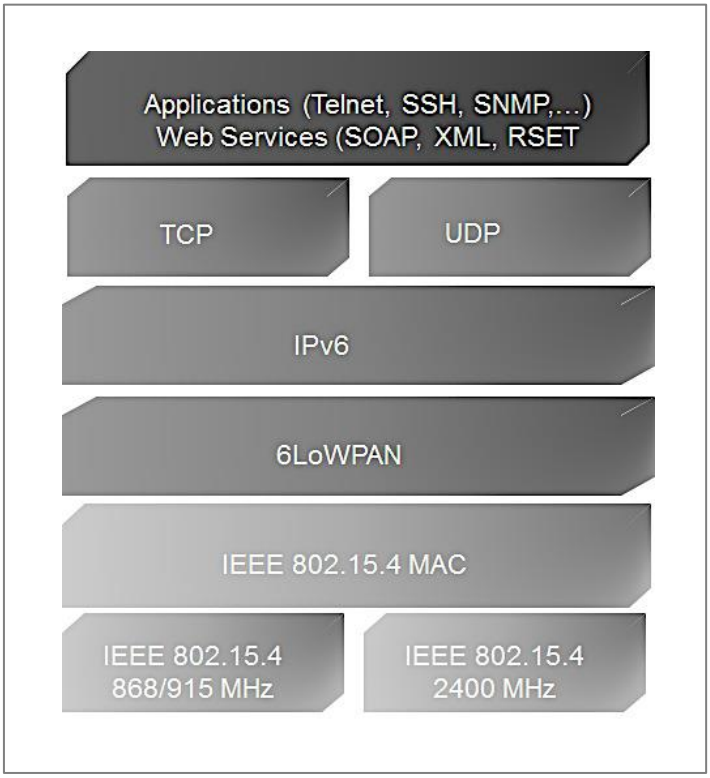



**Fig. 16 - 6LoWPAN en la pila de protocolos [11]**

6LoWPAN apunta a simplificar la interfaz entre redes de sensores e Internet. De este modo una red WPAN puede integrarse fácilmente a Internet, permitiendo crear con facilidad aplicaciones donde esta interacción sea necesaria. A diferencia por ejemplo de redes ZigBee, no sería necesaria una capa suplementaria como Gateway para salir a Internet. Cada dispositivo podrá tener conexión extremo a extremo haciendo uso de las capas provistas por 6LoWPAN.

En contrapartida tenemos que los nodos sensores suelen tener capacidades de procesamiento muy limitadas, afectando en algunos casos a las posibilidades que el protocolo brinda.

Entre las tareas que debe realizar la capa de 6LoWPAN para adaptarse a las limitaciones de los nodos y del propio Estándar 802.15.4 a través del cual encamina los paquetes, podemos mencionar las siguientes:

- **Segmentación y reensamblaje:** algunos de los desafíos que deben enfrentarse al querer utilizar IPV6 sobre 802.15.4 es el tamaño de las tramas. Como vimos en la sección del estándar de la IEEE 802.15.4 el tamaño máximo disponible para transmisión de paquetes es de 127 bytes. Por su parte, IPv6 requiere que cada paquete en Internet tenga una MTU (unidad máxima de transferencia) de 1280 Octetos (bytes) o más. En cualquier enlace que no pueda transmitir un paquete de 1280 bytes en una sola pieza, la segmentación y el reensamblaje deberán ser realizados en una capa por debajo de IPv6. [32]. Para ello, se agrega una capa en 6LoWPAN llamada capa de adaptación que fragmenta y rearma los paquetes. [27]
- **Compresión de cabecera:** dado que en el peor de los casos el tamaño máximo disponible para transmisión de paquetes IP en una trama IEEE 802.15.4 es de 81 octetos (teniendo en cuenta que 127 bytes es el tamaño máximo de un paquete definido en la capa física, menos 25 bytes de la capa MAC, menos 21 bytes en el caso de usarse AES 128 para encriptación), y que la longitud de la cabecera IPv6 es de 40 bytes (sin cabeceras extendidas opcionales), esto nos deja solo 41 bytes para las capas superiores del protocolo, como UDP y TCP. La cabecera UDP usa 8 bytes y la cabecera TCP usa 20 bytes. Esto deja 33 bytes para datos en UDP y 21 octetos para datos en TCP. Además, como se señaló antes, se necesita una capa para fragmentación y reensamblaje lo que utilizará más bytes y dejará menos espacio para los datos. Entonces, si uno fuera a usar el protocolo como está, se estaría haciendo un uso excesivo de la fragmentación y reensamblaje, incluso cuando los paquetes tengan apenas decenas de octetos de largo. Esto explica la necesidad de comprimir la cabecera. [33] [34]
- **Mensajes multicast:** dado que el multicasting no es soportado por el 802.15.4, los paquetes multicast de IPv6 deben transportarse como tramas de difusión (broadcast) en las redes IEEE 802.15.4. Esto debe hacerse de manera que las tramas de difusión sean atendidas solo por dispositivos dentro de la PAN específica del enlace en cuestión.
- **Gestión de la red:** en IPV6 existe un nuevo mecanismo llamado autoconfiguración de direcciones sin estado (*Stateless Address Autoconfiguration* o SLAAC) que no existía en IPv4. Permite configurar automáticamente todos los parámetros de red en

un dispositivo IP usando directamente el mismo enrutador que proporciona conectividad a la red. La ventaja de SLAAC es que simplifica la configuración de dispositivos de bajos recursos como sensores, cámaras u otros, que tienen baja capacidad de procesamiento, conectándolos a la red y rápidamente logrando que puedan transmitir (a través del intercambio de los denominados RA o "*Router Advertisements*"), algo denominado como un funcionamiento *plug&play*. [35]

**Mecanismos de Ruteo**

Dependiendo en que capa se encuentre el mecanismo de ruteo, se pueden definir dos categorías: "Mesh Under" o "Route Over".

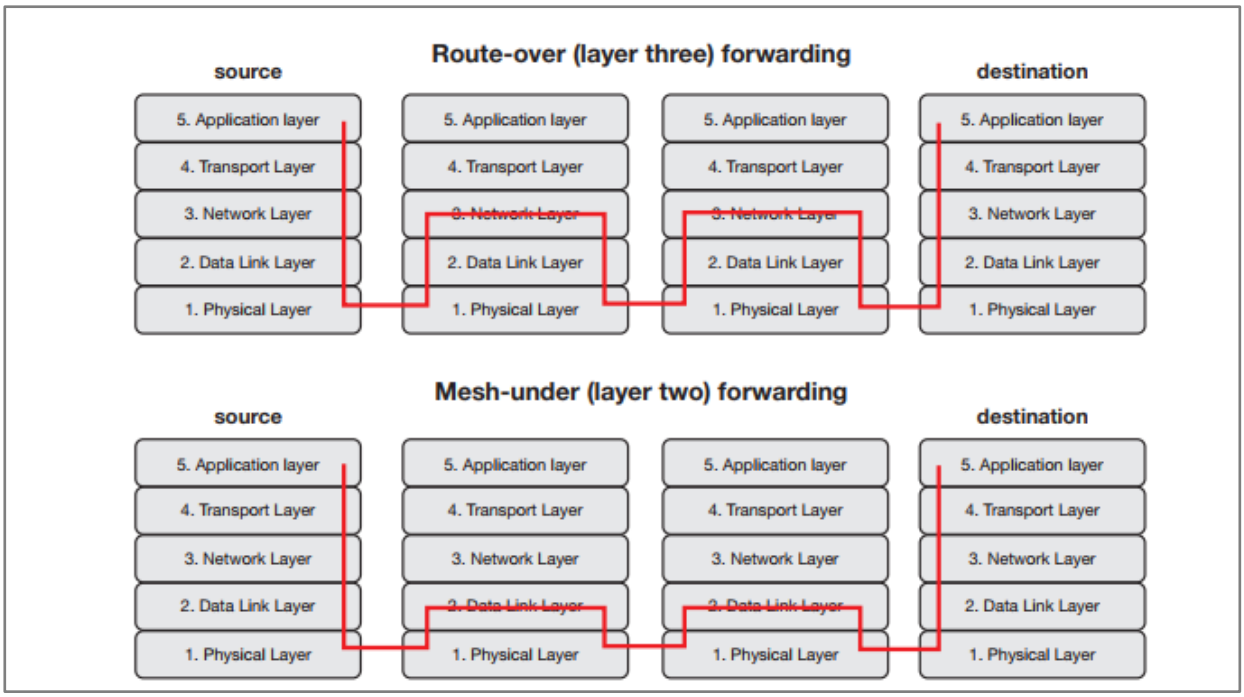



Fig. 17 - Categorías de ruteo 6LoWPAN [36]

*Mesh-Under* utiliza las direcciones de capa 2 o Enlace para ir reenviando los datos, haciéndolo de manera transparente a las capas superiores.

En redes *Route-over* el encaminamiento se produce a nivel IP, donde cada salto de la red representa un dispositivo router con IP. El uso de este tipo ruteo basado en IP es más apropiado para el diseño de redes más potentes y escalables.

El RFC 6550 (los RFC son los informes técnicos generados por el comité de la IETF, denominados *Request for Comment o RFC*) especifica el protocolo de enrutamiento "IPv6 para Redes con pérdidas" RPL [37] , que proporciona un mecanismo tráfico multipunto-a-punto de los dispositivos dentro de la red 6LoWPAN hacia un dispositivo central (por

ejemplo, un servidor en Internet) así como punto-a-multipunto desde el punto central hasta los dispositivos dentro de la red 6LoPWAN.

**Seguridad Implementada**

A nivel seguridad 6LoWPAN cuenta con mecanismos complementarios para garantizar los aspectos de seguridad de la información. Por un lado hace uso de las capas inferiores descriptas anteriormente en el IEEE802.15.4, donde como vimos, la capa de enlace provee autenticación y encriptación.

Si TCP corre en la red, existen mecanismos de transporte seguro como TLS (*Transport layer security*- RFC 5246), mientras que si se elije hacerlo sobre UDP la opción es DTLS (*Datagram Transport Layer Security* – RFC 6347). Tanto TLS como DTLS, requerirán de recursos de procesamiento suficientes en el dispositivo para el cifrado de la información, en algunos casos incluso puede llegar a utilizarse un hardware dedicado. [36]

En el caso de utilizarse TCP, deberá tenerse en cuenta que es un protocolo orientado a conexión con un mayor retardo (*overhead*) para entablar las comunicaciones, lo cual no siempre es deseable en una red con dispositivos que demanden ultra-bajo consumo. Por este motivo, la elección de UDP (protocolo no orientado a conexión) puede ser una mejor opción considerando que es más “liviano”. [36]

Por último y no menos importante, 6LoWPAN contará con IPsec para garantizar confidencialidad, integridad y autenticación, encriptando y firmando digitalmente cada mensaje. IPsec se encuentra definido en varias RFCs (2401, 2406, 2409, 2411) y define dos modos de uso: AH (*authentication header*), que asegura la autenticación del emisor, y ESP (*Encapsulation Security Payload*), que garantiza la confidencialidad, integridad y autenticación.

A modo resumen, podemos mencionar las siguientes bondades del 6LoWPAN al basarse en un esquema IP, particularmente IPv6:

- Mayor espacio de direccionamiento (128 bits), lo que garantiza alrededor de 670 billones de direcciones por cada milímetro cuadrado de la superficie del planeta. Esto permitirá conectar absolutamente todos los dispositivos ya existentes y todos los que se diseñen en los próximos años.
- El uso de un estándar común, basado en IP de extremo a extremo evita el problema de las redes interconectadas por protocolos que no son inter-operables.
- Formato de cabecera simplificada, lo cual reduce el overhead de procesamiento en los equipos de enrutamiento.
- Autoconfiguración de direcciones (SLAAC) a través de uso de mensajes de ICMPv6.

- La naturaleza ubicua de las redes IP permite el aprovechamiento de infraestructuras existentes. Mejoras en la movilidad (MIPv6) de redes.
- Las tecnologías basadas en IP ya existen, son bien conocidas, de funcionamiento comprobado y disponible en muchas partes. Esto va a permitir una adopción fácil y barata, una buena interoperabilidad y un desarrollo de las capas de aplicación más fácil.

## 3.4. WirelessHART

La Fundación de Comunicaciones HART (HCF) es la organización propietaria de la tecnología y la autoridad central del protocolo HART, encargada de su especificación y mantenimiento. La componen entre ellas empresas como SIEMENS y HONEYWELL.

No podemos hablar de WirelessHART [38] sin antes hablar de su antecesor cableado, en el cual está basado: el protocolo HART, el cuál es el más ampliamente usado en industrias de proceso, con más de 40 millones de instrumentos de campo que lo soportan.

HART es un protocolo de comunicación bidireccional que proporciona acceso a datos entre los instrumentos de campo inteligentes y sistemas host. Un host puede ser cualquier aplicación de software, desde dispositivos de mano o laptops, a controles de proceso de planta, seguridad u otro sistema usando cualquier plataforma de control. La comunicación se produce entre dos dispositivos habilitados para HART, normalmente un dispositivo inteligente de campo y un sistema de control o monitorización.

WirelessHART es un protocolo de comunicaciones inalámbricas para aplicaciones de automatización de procesos. Añade capacidades inalámbricas a la tecnología HART mientras mantiene la compatibilidad con dispositivos, comandos y herramientas HART existentes.

En el año 2007 se publica la revisión 7 del protocolo que incluye las especificaciones para redes de sensores inalámbricas. El WirelessHART hereda parte del stack de comunicación de HART, modificando las capas inferiores, cambiando la manera de trasmisión de la alámbrica a la inalámbrica.

### Seguridad en WirelessHART

Un aspecto importante en este protocolo son las medidas de seguridad robustas que implementa.

Para garantizar la seguridad de los datos, WirelessHART maneja encriptación estándar AES de 128 bits con clave de cifrado única para cada mensaje. También posee un doble mecanismo de verificación de integridad de datos y autenticación de dispositivos: A nivel de capa de sesión realiza un chequeo de integridad a fin de verificar que el contenido del paquete de datos no fue alterado, mientras que a nivel de capa de enlace la verificación incluye la validación de la información de ruteo, con el objetivo de prevenir ataques que modifiquen información de las capas de red y transporte.

Además, permite rotar de manera automática o manual, las claves de cifrado utilizadas para unirse a la red.

Por otro lado, en lo que respecta a la seguridad de la red, éste protocolo realiza saltos de canales, posee múltiples niveles de clave de seguridad para acceso, permite verificar los intentos de acceso fallidos de un dispositivo a fin de identificarlo como “deshonesto” y reporta integridad de los mensajes y fallas de autentificación. [39]

**Tipos de dispositivos**

Existen 3 tipos de dispositivos en una red WirelessHART:

- Administrador de Red: sistema backend para administración de la red e interoperabilidad con dispositivos HART cableados.
- Gateway: encargado de funciones de ruteo dentro de la red, administra también funciones de seguridad.
- Dispositivo de campo: sensor con adaptador wireless incorporado para cumplir con las funciones de negocio necesarias. Existen en el mercado adaptadores para adaptar al formato inalámbrico sensores con tecnologías HART.

**Modo Ráfaga**

WirelessHART posee un modo denominado *Burst Mode* o Modo Ráfaga [40] que optimiza la comunicación inalámbrica. Para esto, en lugar de funcionar en tiempo real, periódicamente el dispositivo envía al Administrador de Red un conjunto de peticiones. El Administrador de Red intenta reprogramar los espacios de tiempo del TDMA. Si lo consigue, el dispositivo tendrá disponible la ventana de tiempo requerida en la cual puede realizar lecturas o escrituras en ráfaga. Este mecanismo permite realizar un importante ahorro de energía.

**Características principales:**

- Se basa en el IEEE 802.15.4-2006 con una velocidad de 250kbps.
- Frecuencia de operación de 2400 – 2483.5Mz. (2,4GHz ISM)
- Usa modulación O-QPSK Direct Sequence Spread Spectrum (DSSS).
- Potencia de transmisión de 10 dBm (nominal) ajustable.
- Utiliza TDMA y channel hopping para evitar las colisiones en la comunicación.
- Tecnología de malla: auto organizado y auto-reparable (Smart Mesh).
- Alta eficiencia energética.
- Alcance de hasta 250m en línea de visión. [41]
- Posee muchos años de operación en el mercado industrial, siendo uno de los protocolos más difundidos y probados.

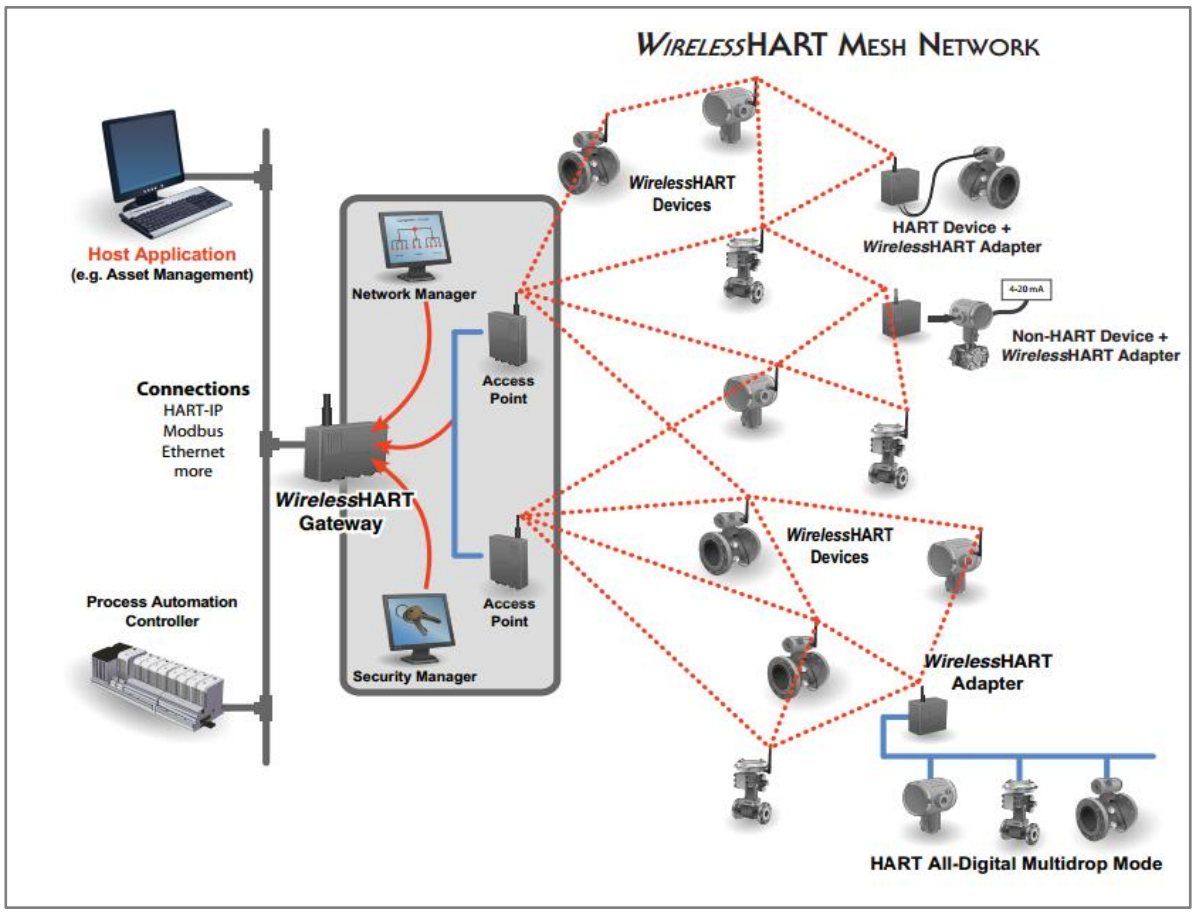



Fig. 18 - Ejemplo de topología WirelessHART [39]

En resumen, WirelessHART es la versión inalámbrica de un protocolo que es estándar para control de procesos industriales. Hace mucho hincapié en la seguridad, y fácilmente pueden encontrarse en el mercado numerosos dispositivos, los cuales no son de propósito general (como en el caso de ZigBee) sino que están fuertemente orientados a procesos industriales.

Sólo por citar un ejemplo, la empresa SMAR ofrece una repetidora WirelessHART modelo RP400CS [42], la cual viene dotada de una batería que (según el manual) le permite una duración de 6 años, con el dispositivo en "*Burst Mode*" de 8 segundos, a 25ºC y con, por lo menos, tres equipos vecinos.

## 3.5. ISA SP100.11a

ISA (*International Society of Automation* o Sociedad Internacional de Automatización) es una asociación de más de 30.000 profesionales involucrados en el diseño, desarrollo y aplicación de dispositivos y sistemas que sensan, miden y controlan procesos industriales y operaciones de fabricación. [43]

ISA SP100.11a es un protocolo de comunicaciones inalámbricas desarrollado por ISA con el objetivo de servir en aplicaciones industriales. En el año 2014 se convierte en un estándar de la IEC, el IEC 62734. [44]

A diferencia de otros protocolos de WSN como WirelessHART o ZigBee, SP100.11a soporta múltiples protocolos industriales (como Profi, Mod, FF e inclusive HART) mediante una infraestructura wireless simple. Además, posee diferentes niveles de performance que lo habilitan para aplicaciones de automatización en fábricas, no solo aplicaciones de procesos. [43]

ISA100.11a define la pila de protocolos, la gestión del sistema y las funciones de seguridad para su uso en redes inalámbricas de baja potencia y baja velocidad (actualmente IEEE 802.15.4). Sin embargo, no especifica una capa de aplicación con un protocolo de automatización de procesos o una interfaz con un protocolo existente. Sólo especifica herramientas para construir una interfaz.

El protocolo está definido las siguientes capas del modelo OSI [45]:

**Capa física**: Está basada en el estándar IEEE 802.15.4-2006 a 2.4GHz.
**Capa de enlace:** Además de los servicios framing, detección de errores y gestión de bus, definidos en el modelo OSI para esta capa, la capa de enlace de ISA100.11a agrega los siguientes servicios:

- Enlace local de direccionamiento.
- Reenvío de mensajes.
- Gestión de la capa física.
- Salto de canal adaptable.
- Control de mensajes, control de tiempo e integridad.
- Detección y recuperación de pérdida de mensajes.
- Sincronización del reloj.

**Capa de red:** Está conformada por el protocolo 6LoWPAN.

**Capa de transporte:** Admite un servicio sin conexión basado en UDP con una comprobación de integridad de mensajes mejorada y seguridad de extremo a extremo.

**Capa de aplicación:** Actualmente ISA100.11a no define una capa de aplicación.

Éste protocolo introduce 6 clases para las comunicaciones inalámbricas (desde clase 5 a clase 0), basándose en el análisis de comunicaciones entre dispositivos en aplicaciones industriales:

I. La clase 5 define los elementos relacionados con el monitoreo sin consecuencias operacionales inmediatas. Esta clase cubre las aplicaciones sin requisitos de puntualidad estrictos. Los requisitos de fiabilidad pueden variar.

II. La clase 4 define monitoreo con consecuencias operacionales a corto plazo. Esto incluye alarmas u otra información que requiera de mayor comprobación o la participación de un técnico de mantenimiento.

III. La clase 3 cubre las aplicaciones de control de bucle abierto, en el que un operador, en lugar de un controlador, "cierra el círculo" entre la entrada y la salida. El horizonte de tiempo para esta clase es en una escala humana, medido en segundos y minutos.

IV. La clase 2 consiste en el control de supervisión de bucle cerrado, y las aplicaciones tienen generalmente constantes de tiempo largas, con la escala de tiempo medido en segundos a minutos.

V. La clase 1 está destinada al control de regulación de bucle cerrado. Incluye el control de motores y ejes, así como también el control de flujo primario y control de presión. Normalmente el tiempo de respuesta de esta información es crítico.

VI. La clase 0 define las medidas de emergencia relacionadas con la seguridad, que siempre son críticos para las personas y la planta. La mayoría de las funciones de seguridad son, y serán, llevadas a cabo por redes cableadas dedicados a fin de limitar los modos de falla y la vulnerabilidad a eventos externos o ataques. Ejemplos de esta categoría son bloqueo de seguridad, cierre de emergencia y control de incendios. [46]

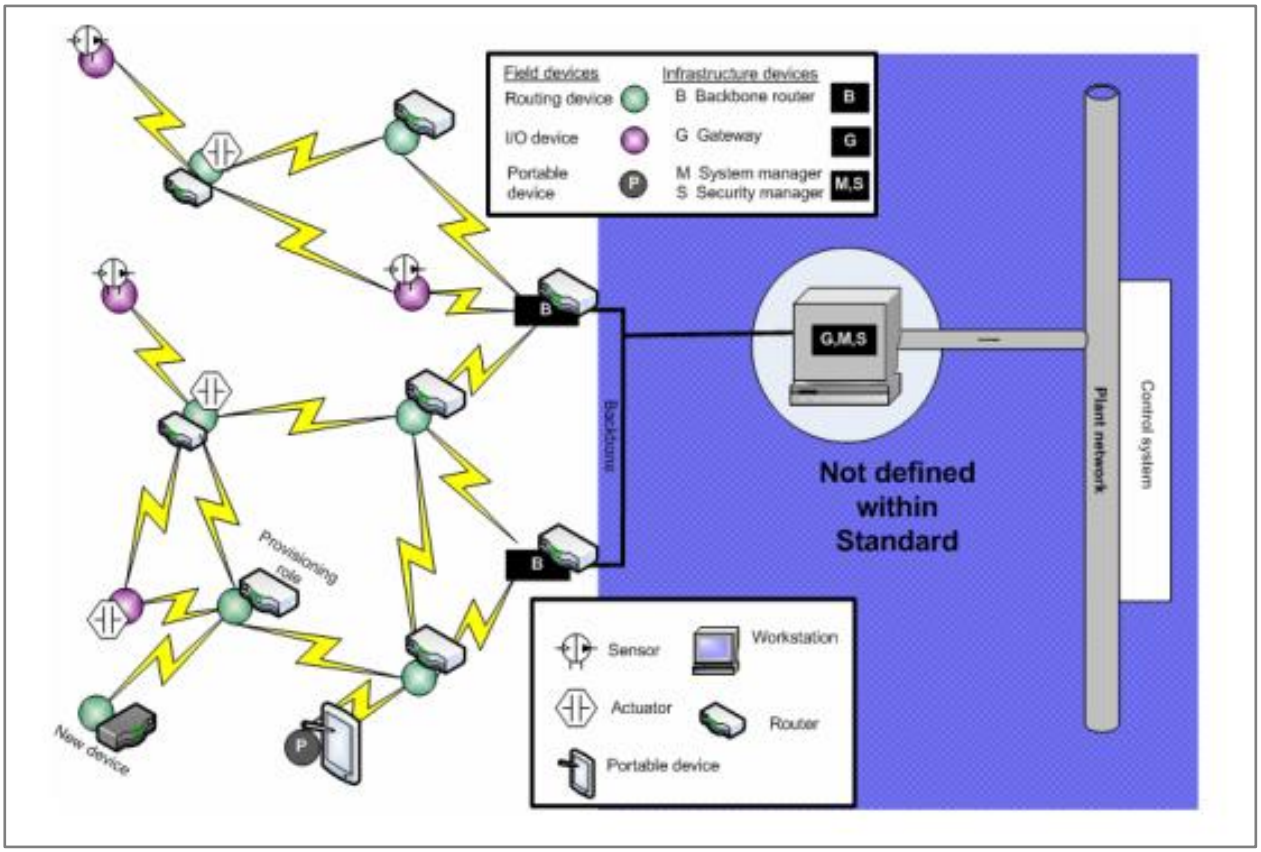



**Fig. 19 - Arquitectura de una red ISA100.11 [45]**

Algunas de las características de ISA SP100.11a son [43]:

- Asegura la interoperabilidad de dispositivos de múltiples proveedores.
- Incluye solo los radios de 2.4GHz definidos en 802.15.4-2006.
- Utiliza salto de canal para soportar la coexistencia y aumentar la fiabilidad.
- Utiliza una única capa de aplicación que proporciona tanto capacidad de uso del protocolo nativo como también tunneling de protocolo.
- Proporciona seguridad simple, flexible y escalable, frente a las principales amenazas industriales aprovechando la seguridad de 802.15.4-2006.
- Ofrece capacidad de conexión de dispositivos en malla o estrella.
- Soporta aplicaciones de automatización de fábricas.
- Soporta aplicaciones de baja latencia.
- Permite implementaciones de bajo costo.

## 3.6. ISO/IEC 14543-3-10. EnOcean

La empresa EnOcean [47] nace en el año 2001 como un desprendimiento de Siemens. Su investigación está enfocada en el desarrollo de sensores inalámbricos libres de mantenimiento para uso en el campo de la industria y la construcción principalmente (*Smart buildings).*

En el año 2008 se crea la EnOcean Alliance, que reúne a distintos fabricantes de dispositivos que implementan el estándar propuesto por EnOcean. Componen esta alianza más de 300 empresas que desarrollan hardware y software.

Con la publicación del estándar ISO/IEC 14543-3-10 [48] para las capas inferiores y la capa de aplicación definida por la EnOcean Alliance, se apunta a lograr una interoperabilidad completa entre dispositivos desarrollados por diferentes fabricantes. De esta manera, un sensor de una empresa podrá comunicar su información a un gateway o concentrador desarrollado por otro fabricante, y a su vez éste dar aviso a un actuador inalámbrico desarrollado por un tercero.

El principio básico sobre el que trabajan es su tecnología patentada de "**recolección de energía inalámbrica**". El objetivo es diseñar sensores para redes de corto alcance y muy bajo consumo, y que incluso puedan prescindir del uso de baterías. Esto funciona bajo el principio de cambios de estado en los valores que sensan (temperatura, luz, presión, vibraciones, movimiento). Al momento de alterarse alguno de estos valores, se genera suficiente energía como para que microcontroladores de ultra bajo consumo puedan transmitir una señal. Esto lo hacen con "conversores", que no son más que dispositivos de hardware que recolectan la energía proveniente de movimiento, luz o temperatura, para convertirla en energía eléctrica [49]. Esta reducida energía es suficiente para generar un paquete de datos denominado "telegrama", el cual se transmite por un dispositivo de radiofrecuencia, ambos (telegrama y dispositivo) ajustados a las definiciones del protocolo ERP (*EnOcean Radio Protocol*) y del perfil de dispositivo EEP (*EnOcean Equipment Profil) respectivamente.* [50]

Luego estas señales ya son captadas y procesadas por otros dispositivos sensores, actuadores o repetidores con fuentes de alimentación constantes (cableados o a batería).

**Estándar ISO/IEC 14543-3-10: *Wireless Short-Packet Protocol* (WSP- Protocolo inalámbrico de paquetes cortos)**

El estándar ISO/IEC 14543-3-10 define las tres primeras capa del modelo OSI (física, enlace y red.) de un protocolo optimizado para soluciones basadas en recolección de energía (*energy harvesting*). Ver Tabla 1:

| *Estándar* | *Capa* | *Servicios* | *Unidad de datos* |
|---|---|---|---|
| *ISO/IEC 14543-3-10* | Red | • Telegramas con dirección de destino (encapsulación / desencapsulación)<br>• Conversión de telegramas de “switch”<br>• Repetición | Telegrama |
| | Enlace | • Estructura de subtelegrama<br>• Algoritmos de hash<br>• Temporización de subtelegramas<br>• Manejo de colisiones | Subtelegrama |
| | Física | • Codificación y decodificación<br>• Transmisión y recepción inalámbrica | Bits / frame |

**Tabla 1 - Capas ISO/IEC 14543-3-10**

El diseño de este protocolo se caracteriza por mantener comunicaciones de corta duración, poco frecuentes y en su mayoría unidireccionales, además de utilizar frecuencias de comunicación que proporcionan un buen alcance incluso a baja potencia de transmisión y evitando colisiones provenientes de perturbadores.

El protocolo consta de tres tipos de componentes: transmisor, receptor y repetidor, siendo este último opcional.

**Capa física**

En la capa física, los datos se transmiten en la banda de frecuencias de 315MHz o 868,3MHz con una velocidad de transmisión de 125 kbit/s utilizando la codificación de desplazamiento de amplitud (ASK). La distancia funcional del sistema es de hasta 300m en línea de visión incluyendo y hasta 30m en edificios. La duración de un bit es de 8µs. Los datos se transmiten en frames. Una trama consta de un preámbulo, una secuencia de inicio de la trama, las subtramas y la secuencia de fin de trama.

Por usar las frecuencias antes mencionadas, este protocolo obtiene una serie de ventajas (en comparación a otros protocolos que trabajan en las bandas 2.4GHz) como hacerlo menos propenso a interferencias de muchos dispositivos que operan en torno a los 2.4GHz

y al tener un rango mayor la onda de radio, obtiene un mejor alcance dentro de interiores (penetrando muros y amoblados). [51]

### Capa de enlace

El subtelegrama se transfiere a la capa de enlace donde se comprueba la integridad de datos. Si la comprobación de integridad de datos falla, el subtelegrama se descarta.

Otra tarea de esta capa es gestionar la temporización del subtelegrama recibido / transmitido. La temporización se basa en un algoritmo que asegura que la probabilidad de colisiones de subtelegramas en tránsito sea lo más baja posible. Para reducir el riesgo de colisión, el protocolo WSP utiliza, cuando es posible, una técnica de "escuchar antes de hablar" (LBT).

### Capa de red

Una de las responsabilidades de esta capa es el proceso de repetición, que se utiliza cuando las señales inalámbricas son demasiado débiles para alcanzar directamente al receptor. Esto implica dispositivos intermedios, es decir, repetidores que se han instalado entre el emisor y el receptor final de la señal inalámbrica.

Otro proceso que se realiza en esta capa consiste en el manejo de telegramas con dirección de destino. La mayoría de los telegramas se transmiten en modo broadcast. Sin embargo, si se trata un telegrama con dirección de destino, el mismo está en un formato encapsulado y la capa de red es la encargada de desencapsularlo cuando corresponda.

Existe también un proceso conversión entre telegramas de “switch”. Este tipo de telegrama particularmente pequeño y por lo tanto de muy bajo consumo de energía. Se denomina un "telegrama de switch" porque se utilizó por primera vez en dispositivos de recolección de energía que se energizaron girando un interruptor. El proceso se encarga de cambiar el formato del telegrama al formato genérico.

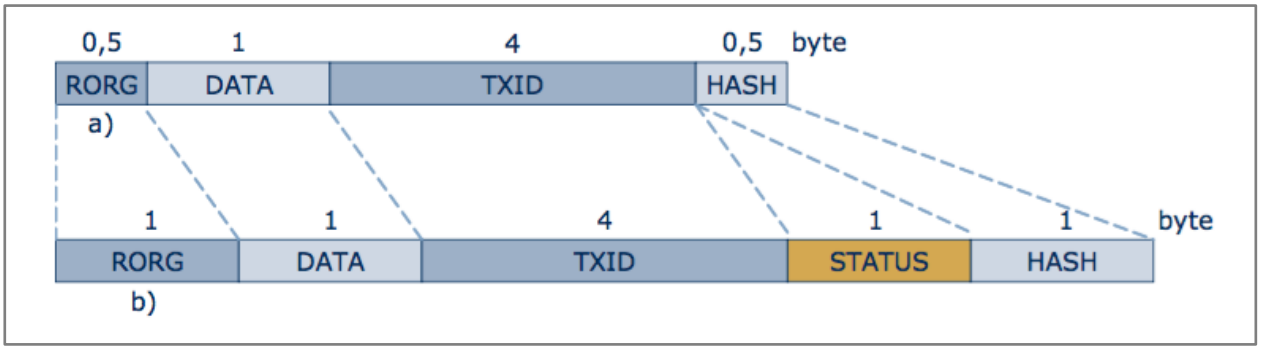



**Fig. 20 - Cambio de formato de telegrama de switch a genérico [50]**

**EEP, la capa de aplicación de EnOcean**

Montada sobre el protocolo ISO/IEC 14543-3-10, está la capa de aplicación denominada EEP (EnOcean Equipment Profile) o Perfil de Equipo EnOcean. Esta define los diferentes tipos de telegramas que pueden enviarse ya sea para transferencia de datos o como comandos para actuadores.

La definición de esta capa va creciendo con el aporte de diferentes fabricantes, según las necesidades que estos presentan para comunicación de nuevos dispositivos, y la posterior aceptación de la EnOcean Alliance.

Más allá de los posibles comandos o formatos de información, hay tres aspectos que vale la pena mencionar sobre EEP:

- Existen tramas para comunicación bidireccional, a pesar que el espíritu del protocolo sean las comunicaciones broadcast.
- Hay tramas que establecen mecanismos de ACK.
- Hay tramas específicas para transmisiones seguras, no obstante la encriptación (y el método que se utilice para ésta) es responsabilidad del dispositivo y no está definida en el protocolo.

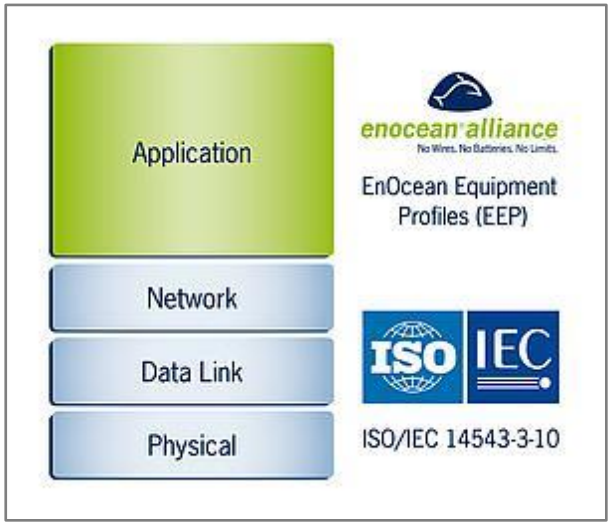



**Fig. 21 - Capas del protocolo de EnOcean [47]**

## 3.7. Z-Wave

El protocolo Z-Wave [52] es una tecnología inalámbrica basada en comunicaciones de Radio Frecuencia diseñada específicamente para el control, seguimiento y aplicaciones de lectura de estado en ambientes residenciales y comerciales.

Es una tecnología de comunicación inalámbrica que es ideal para automatización mediante redes de topología de malla de dos vías, de corto alcance.

Está basado en la especificación **G.9959 de la ITU** [53], la cual especifica las capas físicas y de control de acceso al medio.

Este protocolo consta de 5 capas: Física, de acceso al medio, de transporte, de red y de aplicación. [54]

En la **capa física**, Z-Wave soporta diferentes frecuencias, las cuales cambian su implementación dependiendo del país. En el caso de Argentina se basa en el estándar FCC CFR47 Part 15.249, utilizando las frecuencias 908.40MHz y 916.00MHz. [55]

Para la modulación utiliza GFSK ("*Gaussian Frequency Shift Keying*" o en español "Modulación por desplazamiento de frecuencia gausiana"). Esta combinación le permite tasas de transferencia que van desde 9.6 a 100kbps. [56]

La **capa de acceso al medio** implementa un mecanismo para evitar colisiones, que consiste en que los nodos estén en modo de recepción cuando no transmitan, y luego retrasan una transmisión si la capa MAC está actualmente en la fase de datos en el receptor.

Esta capa contiene en sus tramas un HomeID que es el identificador de la red, y un NodeID que identifica al dispositivo que está transmitiendo. Se permiten hasta 232 nodos en una misma red.

Otro dato importante de esta capa es que posee un mecanismo que permite la operación en un modo de bajo consumo, el cual consiste en dormir a los nodos y despertarlos según un patrón específico.

La **capa de transporte** Z-Wave es principalmente responsable de la retransmisión, el acknowledgment de paquetes, despertar nodos de red en bajo consumo y la autenticación del origen de los paquetes.

La **capa de red** en la encargada del ruteo de los mensajes entre los nodos. Esta capa es la encargada de escanear y conocer la topología de la red para establecer las rutas. La información de ruteo se almacena en el nodo controller.

Finalmente, la **capa de aplicación** permite el desencriptado de datos y además gestiona los comandos de aplicación, que realizan las operaciones sobre los dispositivos conectados.

Este protocolo ha ido evolucionando en diferentes aspectos. Uno de ellos a destacar es la seguridad. En noviembre de 2016 la Z-WAVE Alliance anuncia un nuevo framework de seguridad para su protocolo [57], dado que se encontraron vulnerabilidades en su mecanismo de encriptación con AES. Este nuevo paquete de mejoras en la seguridad (denominado S2) incluye los siguientes aspectos:

- Comunicaciones seguras tanto para dispositivos locales (home-based) como para hubs o gateways en el caso de funciones en la nube. Esto elimina el riesgo de que los dispositivos sea hackeados cuando son agregados a la red.
- Uso de un código QR o pin en los dispositivos para que se autentiquen en la red de manera unívoca.
- Se eliminó el riesgo de hacks comunes como "*man in the middle*" o "Fuerza Bruta", mediante el uso de algoritmos de intercambio seguro de claves ampliamente aceptados en la industria. Puntualmente se utiliza *Elliptic Curve Diffie-Hellman* (ECDH).
- Se mejoró la seguridad de las comunicaciones de Z-Wave sobre IP, mediante el uso de túneles TLS 1.1.

**Topología**

Z-Wave permite topologías tipo mesh. Para ello, los diferentes nodos deben ser configurados según su rol, como se describe a continuación:

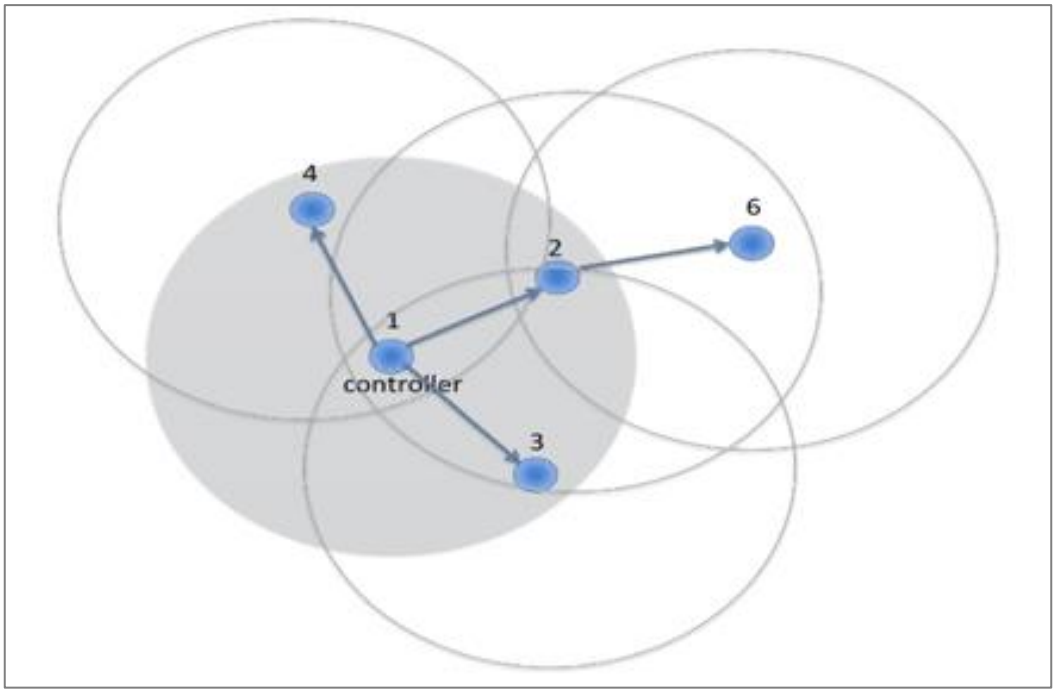



**Fig. 22 - Redes Mesh en Z-Wave [58]**

- Nodo controller: Se puede comunicar con todos los nodos, siempre que los mismos estén al alcance o exista una ruta hacia ellos.
- Nodo esclavo router: Es nodo es capaz de responder al nodo del que ha recibido un mensaje, y puede enviar mensajes a nodos para los cuales existe una ruta directa, y fueron configurados previamente.
- Nodo esclavo: Sólo puede responder al nodo del cual recibió un mensaje. [58]

Características principales:

- Tecnología de baja potencia de comunicación por RF que soporta redes de malla completa sin la necesidad de un nodo coordinador.
- Opera en la banda sub-1GHz; insensible a la interferencia de Wi-Fi y otras tecnologías inalámbricas en el rango de 2,4GHz (Bluetooth, ZigBee, etc).
- Diseñado específicamente para aplicaciones de control y estado, soporta velocidades de datos de hasta 100kbps, con encriptación AES128, IPV6, y modo multicanal.
- MAC y PHY según especificación ITU-T G.9959.
- Interoperabilidad completa a través de la capa 5 con la compatibilidad hacia atrás con todas las versiones.

**LPWANs: redes de sensores inalámbricas de largo alcance**

Como complemento a los protocolos analizados anteriormente que podríamos agruparlos por su rango de alcance dentro de las denominadas WPANs (*Wireless personal area network*), pasaremos a detallar a continuación diferentes protocolos y especificaciones para redes inalámbricas LPWANs (*low power wide area networks),* que son redes con un rango de alcance mayor, pero a costa de una reducción en su tasa de datos. Además veremos en todos los casos, que la arquitectura de red se limita a conexiones en forma de estrella, donde múltiples nodos sensores transmiten regularmente a un punto central o estación base con capacidades de energía garantizadas y conexión con un gateway de red o enlace directo con internet.

Desarrollaremos brevemente las especificaciones de **LoRa/LoRaWan, SigFox** y las opciones basadas en las redes celulares como **LTE-M** y **NB-IOT**.

## 3.8. LoRa

*Lora Alliance* definió en el año 2015 una especificación para redes LPWAN *(low power wide area network)* denominado **LoRa** (abreviatura de "Long Range") pensado para redes Wireless con nodos operados a batería y baja tasa de transmisión datos. En el modelo de capas OSI, las especificaciones estarían referidas a la capa física.

La alianza Lora es una organización abierta y el estándar también lo es. Quizás una de sus críticas se da en que las licencias para la fabricación de sus radios de comunicación solo los posee la empresa Semtech [59], de manera que existen pocos proveedores de hardware y aquellos que quieran desarrollar esta tecnología deberán pagar sus correspondientes regalías a Semtech.

La radio modulación patentada por **LoRa** apunta a lograr comunicaciones de largo alcance (se estima entre 2km a 5km en entornos urbanos y hasta 15km en zonas despejadas), manteniendo el bajo consumo de los equipos. A cambio de esto, resigna en las velocidades de datos, las cuales se encuentran en el orden de los /seg (desde 0.3kbps a un máximo 50 kbps.). Esto claramente, define la aplicabilidad de esta tecnología, la cual lógicamente no será apropiada para transferir grandes volúmenes de datos, pero encajará perfectamente en las necesidades de comunicaciones para el mundo de aplicaciones IoT. El esquema de modulación definido en LoRa se encuadra dentro de los de amplio espectro y puede trabajar en un rango de frecuencias variable desde 137MHz a 1020MHz. En este rango se cuenta con bandas no licenciadas (ISM bands) de uso en varias partes del mundo como son las de 169MHz, 433MHz, 868MHz y 915MHz, lo cual es otro punto a favor de esta tecnología. [60]

Además de las especificaciones en la capa física, la *Lora Alliance* define una capa de comunicación denominada **LoRaWAN,** con la cual se complementan para dar servicios de red como ser confirmación de mensajes, encriptación, multicasting y activación/registración en la red "*over the air*".

La arquitectura de red planteada en las redes LoRa consisten en una topología de estrella, con uno o más dispositivos repetidores (*Gateways*) que encaminan los mensajes de cada uno de los dispositivos finales (*End nodes*, que realizan la función de sensado) hacia un servidor central de red (*Network server*).

Gráficamente se puede observar en la siguiente figura:

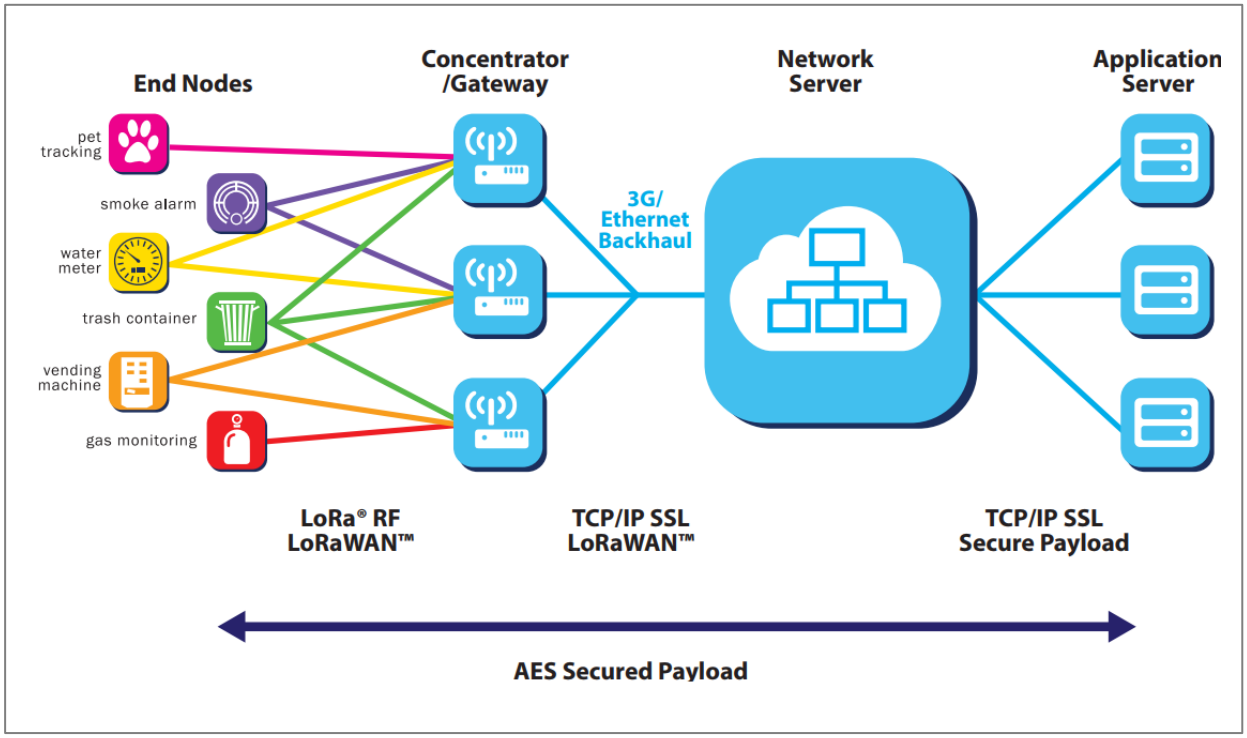



Fig. 23 - Arquitectura de Red LORA [60]

*El Proyecto "**TheThingsNetWork**" , es un comunidad abierta que pretende armar Redes LoRa abiertas para dar cobertura de forma gratuita a hobbistas e investigadores para desplegar una red de sensores. Ver más detalle en : https://www.thethingsnetwork.org*
*Una red LoRa puede ser formada por cualquier persona o empresa que despliegue los Nodos finales y antenas propias con Gateways LoRaWAN, y armar de esta forma su red privada de sensores. A diferencia de las redes SigFox donde se ve involucrado un operador en el medio (ver más detalle en el presente documento)*

Los dispositivos finales transmiten a la red y no hacia un Gateway particular, de manera que la información puede ser recibida por más de un Gateway a la vez (facilitando la movilidad del nodo entre distintos Gateways). Cada uno de ellos reenvía la información hacia el servidor de red en la nube (Network server), normalmente haciendo uso de una conexión celular, satelital, Ethernet o WiFi. Es en el servidor de red, donde reside la inteligencia y el poder de procesamiento para coordinar la red, lo cual incluye tareas como confirmación de paquetes (seleccionando a uno de los gateways de la red para devolver el ACK al nodo que transmitió), asociación de nodos, filtrado de paquetes redundantes y chequeos seguridad, tasas de velocidad adaptivas (ADR), entre otras.

Mediante un esquema de velocidad de datos adaptativa (ADR), LoRa permite que la comunicación entre dispositivos finales y gateways pueda variar dinámicamente en diferentes canales de frecuencia y velocidades de datos. La selección de la velocidad de datos es una compensación entre el intervalo de comunicación y la duración del mensaje. Esto permite maximizar tanto la duración de la batería de los dispositivos finales como la capacidad total de la red, gestionando el servidor de red individualmente la velocidad de datos y la salida de radio frecuencia para cada dispositivo final.

LoRaWAN define 3 clases diferentes de dispositivos finales, dependiendo del tipo de aplicación que se vaya a implementar: La principal diferencia radica en los tiempos de downlink disponibles en el nodo (*dowlink* sería la comunicación desde el Servidor de red al dispositivo final).

- *Dispositivos Clase A:* cada transmisión (*uplink*) es seguida de dos ventanas de tiempo cortas para recibir información desde el Network server (normalmente acks). El tiempo de recepción en el que el dispositivo está listo para el download se calcula en base a un algoritmo random (del tipo ALOHA). Si el *downlink* no fue realizado en esas dos ventanas de tiempos definidas, el Servidor deberá esperar hasta la próxima transmisión (*uplink*) para volver a transmitirle información al nodo. Los dispositivos configurados como *Clase A* son los más eficientes en términos de consumo de energía.
- *Dispositivos Clase B:* además de funcionar como los clase A, los dispositivos *Clase B* agregan ventanas de tiempo extra en base a una agenda determinada, sincronizada por un Beacon enviado por el Gateway. Esto permite al servidor conocer cuando el end device está listo para recibir.
- *Dispositivos Clase C:* son dispositivos que brindan una funcionalidad bi-direccional de forma continua, pudiendo recibir información (downlink) en cualquier momento, excepto cuando se encuentran trasmitiendo. [60]

Para garantizar la seguridad las redes LoRaWAN, consideran los siguientes aspectos: antes de comenzar una transmisión el Nodo End device debe ser “Activado”, para ello el servidor de red le requiere su:

- *Dirección única de dispositivo (DevAddr).*
- *Clave de red basada en AES 128 (Network Session Key).* Soporta encriptación en la comunicación entre los nodos finales y gateways, servidores de red y servidores de aplicación.
- *Clave de aplicación basada en AES 128 (AppSKey).* Permite cifrar los contenidos del paquete (payload) a nivel aplicación. Solo el nodo final y el servidor de aplicación puede desencriptar el contenido del mensaje.

Estos 3 parámetros puede ser seteados ya desde fabrica pudiendo el nodo darse de alta en la red y comenzar a transmitir. O bien pueden configurarse en un handshake inicial entre el dispositivo y el Servidor de aplicación.

## 3.9. SigFox

SigFox es una compañía francesa fundada en el año 2009 y que diseñó su red Wireless de bajo consumo, baja tasa de datos y largo alcance (LPWAN), empleando una tecnología propietaria para la comunicación por radiofrecuencia en las bandas no licenciadas de 868MHz y 915MHz, modulando mediante la tecnología UNB (*Ultra Narrow Band*).

La arquitectura de red planteada es una estrella de single hop similar a la de una red celular, con estaciones bases que recepcionan los paquetes de datos transmitidos desde los nodos finales. Luego la información es subida a la nube de la empresa SigFox, quién la distribuye a los servidores de aplicación de sus clientes:


Fig. 24 - Redes SigFox [61]

SigFox propone la creación de una red independiente a la que, para conectarse, es necesario incorporar un chip que sea compatible con la misma. Para ello trabaja con diversos proveedores de hardware como Texas Instruments, Atmel, Silicon Labs y otros para poder ofrecer distintos tipos de transceptores y componentes de conexión a su red. Al mismo tiempo están comenzando a cerrar acuerdos con distintos proveedores de telecomunicaciones, para combinar infraestructuras y plataformas de gestión ya desplegadas (como ser el acuerdo con Telefónica para México, Colombia, Brasil y Argentina celebrado en 2017 [62] ). SigFox podrá actuar como un complemento a las redes actuales (GSM, LTE o NB-IOT a futuro) o actuar de forma independiente a éstas.

Las comunicaciones en las redes SigFox son bidireccionales, con una tasa máxima de 1000bps, aunque dándole prioridad a los paquetes de Uplink (transmisión desde los nodos a la estación base): se permiten subir hasta 140 paquetes por día con un payload máximo de 12 bytes y un downlink de 4 mensajes diarios con un payload de 8 bytes.

Como se observa, la cantidad de paquetes y el tamaño máximo de los mismos, encasilla su campo de aplicación claramente hacia el mundo del IoT, donde se puede prescindir de las bondades de mayor ancho de banda, a favor de lograr una mayor autonomía de las baterías y simplicidad del hardware de comunicaciones.

La seguridad en las redes SigFox comienza en los objetos transmisores o nodos finales. Estos contienen una clave secreta para encriptación de los paquetes. Esta clave se encuentra en una memoria de solo lectura no accesible en el chip de comunicación.

Cada uno de los mensajes recibidos en el Cloud SigFox, incluyen una firma digital para autenticar al emisor e incluye además un número de secuencia para evitar la repetición de paquetes.

Otra medida de seguridad, se da con el hecho que cada emisor envía el paquete tres veces con diferentes frecuencias aleatorias, de manera que es menos vulnerable a un ataque. Lo mismo se da con los tiempos de downlink seleccionados por el nodo, es decir, los momentos en los que “escucha” y que puede recibir un mensaje, son aleatorios y no fácilmente detectables por un intruso.

A su vez, entre las estaciones base (gateways) y la nube SigFox, la información viaja por un link punto a punto estableciendo un canal privado virtual (VPN). Y entre la nube y las app consumidoras, las comunicaciones se hacen mediante HTTPs. [61]

## 3.10. LTE-M y NB-IOT

Dentro del grupo de las LP-WAN (*low power Wide área networks*), otros dos protocolos asociados a la infraestructura de las redes celulares son el **LTE-M** y el **NB-IOT**, introducidos por la asociación 3GPP ("*3rd Generation Partnership Project*" - asociación de empresas de telecomunicaciones, encargados entre otros, de la evolución de los protocolos para telefonía partiendo desde el GSM, pasando por el GPRS, el 3G y 4G-LTE [63]).

Tanto las especificaciones de **LTE-M** (es el término simplificado de la industria para el estándar LTE-MTC o *Long Term Evolution for Machines communications*) como de **NB_IOT** *(Narrow Band for Internet of Things***)** fueron publicados por 3GPP en la especificación Release 13. Estos protocolos, son unas de las opciones fomentadas por las empresas operadoras telefónicas y proveedores de tecnologías afines (como Vodafone, At&T, Huawei, Ericsson, LG, Nokia, Bell, Telefónica, Orange entre otros), sobre todo considerando que en muchos casos les permitiría, usando una infraestructura ya desplegada para las redes 3G/4G, cubrir nuevos modelos de negocios que surjan en el ámbito del IoT.

También servirían para reemplazar antiguas infraestructuras desplegadas sobre todo en soluciones industriales (M2M, *machine to machine*), donde aún se utilizan sensores comunicados por tecnología GPRS [5]. Esta tecnología encuentra sus limitaciones en dos puntos fundamentalmente: un costo alto promedio de un plan de datos para cada uno de los sensores desplegados y el consumo energético de la comunicación, que sería un problema a enfrentar en ambientes con acceso limitado a una fuente de energía constante.

Con estos protocolos se apunta a una tecnología de área amplia de baja potencia que soporta IoT a través de una menor complejidad del dispositivo y logrando proporcionar una cobertura extendida, al tiempo que permite la reutilización de las antenas de comunicación LTE ya instaladas, debiendo en principio solo actualizarse el software y stack de protocolos que soportan las mismas.

Entre los objetivos es que permitan una vida útil de la batería de hasta 10 años o más para una amplio espectro de casos de uso y reduciendo los costos de equipos de comunicación a instalar un 20-25% de los GPRS actuales.

Soportado por todos los principales fabricantes de equipos móviles, chipset y módulos, se espera que las redes LTE-M y NB-IOT coexistan con las redes móviles 2G, 3G y 4G, beneficiándose de todas las características de seguridad y privacidad de las redes móviles, como el respaldo a la confidencialidad de la identidad del usuario, la autenticación de la entidad, la confidencialidad, la integridad de los datos y la identificación del equipo móvil.

Se espera que los lanzamientos comerciales de redes LTE-M y NB-IOT tengan lugar a nivel mundial en 2017/18. [64]

**Características en común:**

- Baja tasa de datos.
- Hardware económico.
- Largo alcance.
- Bajo consumo de batería.

**Diferencias:**

- **NB-IOT** está focalizado en el mercado Europeo. Incluye menos velocidad de datos, a un menor costo y menor consumo.
- **LTE-M** está enfocado en el mercado Norteamericano. Soporta mayor ancho de banda (incluyendo voz), conexiones móviles, pero tiene un mayor consumo energético.

## Conclusiones de los protocolos analizados

Luego del análisis realizado sobre distintas opciones para montar una red de sensores prototípica, de la cual se muestra más detalle en la segunda parte de este trabajo, hemos definido utilizar el protocolo **ZigBee**, haciendo uso de los chips de radiofrecuencia de la empresa DIGI, denominados comercialmente como *XBeeProS2B*. [65]

Entre las características que consideramos mínimas para el armado de una red de sensores y aquellas que consideramos deseables, las siguientes nos resultaron concluyentes para la elección del tipo de red armada:

- Disponibilidad en el mercado local y precio acorde.
- Bajo consumo.
- Seguridad: encriptación de las tramas.
- Posibilidad de armar redes *peer to peer* o *Mesh*, para extender el alcance de la red.
- Entorno de configuración (XCTU), estable y con una interfaz amigable al usuario.
- Preparado para modos *Sleep.*
- La velocidad máxima (250kbps) es más que suficiente para el monitoreo y transmisión de datos sensados, incluso con frecuencias de muestreo altas (enviando varios datos por minuto)
- El hardware de la empresa DIGI, tiene buena performance en términos de alcance y estabilidad de la red.
- Librerías de comunicación disponibles para su uso en entorno del IDE Arduino.

# 4. Protocolos de Aplicación

Hemos hablado a lo largo de este capítulo, de diferentes soluciones tecnológicas para comunicar datos inalámbricamente en una red de sensores. Algunas arquitecturas comunican datos entre nodos sensores de bajo consumo hasta llegar a otros con mayor capacidad de enrutamiento o directamente a una estación base, el cual por su mayor poder de cálculo o disponibilidad de energía, se encargará de consolidar los datos en un servidor local o en un cloud service.

En todas las arquitecturas planteadas, se tomó como punto de partida las claras limitaciones en poder de cálculo, memoria o disponibilidad de energía en muchas de las soluciones de redes de sensores para IoT que se plantean hoy. Así como las capas inferiores y medias de estas redes (física, enlace y red), se adaptaron a estas características, lo mismo debe esperarse de los protocolos de capas superiores (capa de aplicación).

En particular, nos resulta interesante mencionar dos alternativas que optimizan el intercambio de información a nivel aplicación y que vienen tomando fuerza los últimos años, como lo son el protocolo **MQTT** y **COAP**. Otras opciones a contemplar son XMPP (*Extensible Messaging and Presence Protocol*), RESTFUL Services (*Representational State Transfer*), AMQP (Advanced Message Queuing Protocol) o Websockets.

Deberá tenerse en cuenta al momento de elegir qué tipo de información se maneja, las frecuencias de muestreo, tipo y calidad del enlace, y si se requiere de una comunicación bidireccional (alimentando con los datos de los sensores un servidor en la nube y pudiendo ejecutar comandos por demanda desde aplicaciones de usuarios en dispositivos finales). En la figura siguiente puede observar las distintas capas de comunicación involucradas:

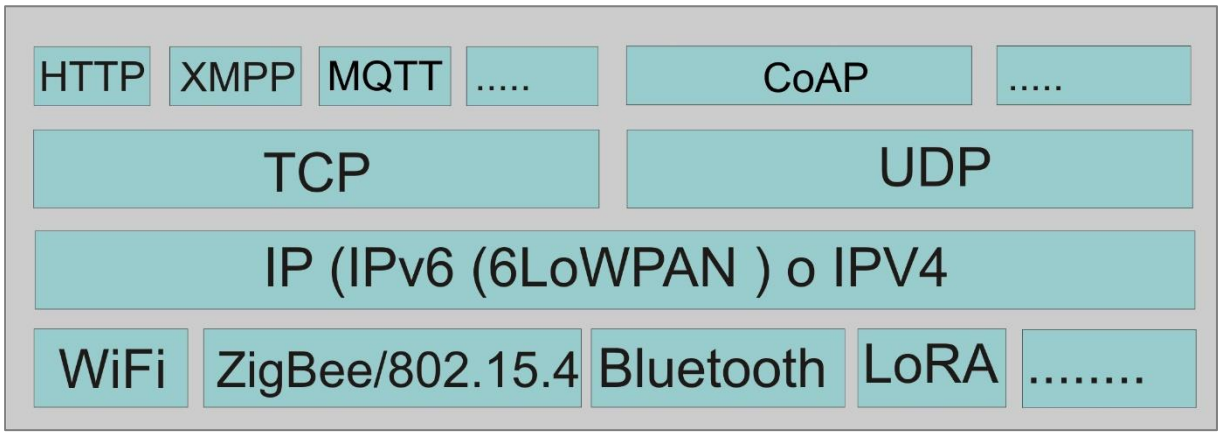



Fig. 25 - Capas de comunicación en WSN

## 4.1. MQTT (Message Queue Telemetry Transport)

Es un protocolo desarrollado por IBM en el año 1999 y desde el 2014 en su versión 3.1.1 se ha convertido en un estándar del comité OASIS en su categoría IoT/M2M [66]. En un principio fue diseñado para entablar comunicaciones entre equipos de campo de la industria del petróleo, a fines de optimizar la información recolectada la cual se enviaría sobre un soporte satelital lento, inestable y costoso. (Puede verse un interesante artículo de uno de los inventores del protocolo en [67]).

Las especificaciones del protocolo fueron liberadas en 2013 y puede usarse de manera gratuita para integrarlo a soluciones de cualquier índole. Todo el código fuente fue donado al proyecto Eclipse Paho. [68]

MQTT utiliza un modelo de "Publicación/Suscripción" requiriendo el uso de un broker (servicio intermediario) central para gestionar y enrutar los mensajes entre los diferentes actores de la red. Ciertos nodos publican información y otros se suscriben para recibir contenidos basados en algún tipo de clasificación (por ejemplo: un servicio meteorológico podría suscribirse a todos los nodos de una red que sensen datos de temperatura y humedad, pero no a aquellas publicaciones de otros nodos que sensan ppb-partes por billón- de monóxido de carbono). En la práctica, los brokers MQTT están suscriptos en todas las publicaciones de los nodos y luego la distribuyen entre los consumidores.

**Fortalezas del MQTT:**

- Transparencia de conexión entre nodos *("Space decoupling"):* la conexión a nivel IP solo debe darse entre el nodo y su broker, de manera que un dispositivo puede publicar y suscribirse a la información publicada sin conocimiento de los demás dispositivos de la red, ya que todo se realiza a través del broker. Considerando que MQTT funciona sobre TCP, esto reduce los retrasos asociados a la apertura de sesiones y puertos por cada conexión.

- Asincrónico*:* cada nodo puede publicar o consumir información independientemente del estado de otros nodos: mientras uno publica al broker, otro nodo suscripto a los datos del primero puede estar realizando otra operación o incluso mantenerse en un estado de bajo consumo "dormido" (una vez despierto, el broker se encargará de bajarle las novedades a las que se encuentra suscripto). Esta práctica reduce ciclos de operación (energía) en todos los nodos de la red.
- Seguridad*:* si bien la encriptación no es una funcionalidad nativa del protocolo, dado que corre sobre TCP, podría implementar TLS/SSL para encriptar el tráfico entre nodos y broker. Una cuestión a considerar serán los recursos extras involucrados en el intercambio de mensajes para cifrar la información.
- Calidad de servicio (QoS): soporta distintos niveles de "calidad" (nivel 0,1 y 2) para brindar una mayor garantía en la entrega de paquetes.
    - Nivel 0 *(Envío y olvido- "Fire and Forget")* no brinda garantías de entrega, el emisor simplemente envía una secuencia de bytes y se desentiende del mismo. Pensado para escenarios con gran cantidad de datos repetidos no críticos.
    - Nivel 1 *(Al menos una vez):* este nivel intenta garantizar que el destinatario reciba al menos una vez el mensaje. Una vez que un mensaje publicado es recibido y comprendido por el destinatario deseado, reconoce el mensaje con un mensaje de acuse de recibo (PUBACK) dirigido al nodo de publicación. Hasta que el PUBACK sea recibido por el emisor, se almacena el mensaje y lo retransmite periódicamente.
    - Nivel 2 *(exactamente una vez):* este nivel intenta garantizar que el destinatario recibe y decodifica el mensaje. Es el nivel de QoS MQTT más seguro, confiable y costoso en términos de comunicación. El emisor envía un mensaje anunciando que tiene un mensaje QoS nivel 2. El destinatario recibe la información, la decodifica e indica que está listo para recibir el mensaje. El emisor transmite su mensaje y una vez que el destinatario entiende el mensaje, completa la transacción con un acuse de recibo.
- Último estado LWT *("last will and testament").* MQTT proporciona un mensaje de "último testamento (LWT)" que se puede almacenar en el broker en caso de que un nodo se desconecte inesperadamente de la red. Este LWT conserva el estado y el propósito del nodo, incluyendo los tipos de comandos que publicó y sus suscripciones. Si el nodo desaparece, el broker notifica a todos los suscriptores del

LWT del nodo. Y si el nodo vuelve a conectarse, se lo notifica de su estado anterior. Esta característica es útil para redes inestables con alta tasa de fallos.

**Algunos puntos débiles del protocolo:**

- Broker central: en sistemas que tienen un solo broker central, puede convertirse en un único punto de fallo para la red completa. Por ejemplo, si el broker fuera un nodo sin un respaldo de batería, en caso de interrupción eléctrica la red completa quedaría inoperante.

- TCP: así como comentamos la ventaja de que MQTT corriera sobre TCP, también tiene su lado negativo. TCP fue diseñado originalmente para dispositivos con más memoria y recursos de procesamiento que los que pueden estar disponibles en una red de sensores. TCP requiere que las conexiones se establezcan en un proceso handshake de varios pasos antes de intercambiar cualquier mensaje. Esto aumenta los tiempos de activación de la comunicación ("*wake up time*") y reduce la duración de la batería a largo plazo. Para contrarrestar esto, los sockets TCP suelen mantenerse abiertos entre sí mediante el uso de una sesión persistente, lo que de nuevo puede ser costoso de lograr con dispositivos con restricciones de energía y recursos.

  Otro problema asociado al uso de TCP se da con el mecanismo utilizado por este protocolo para la detección de congestión, basado en la pérdida de paquetes (escenario que puede llegar a ser bastante común en el contexto de una WSN). Esto conlleva a que TCP reduzca la tasa de transferencia con la finalidad de no colapsar aún más los enlaces. Pero esto trae aparejado un menor uso del ancho de banda del enlace y por ende en una degradación en el *throughput* (velocidad real de transporte de datos) y un retardo mayor en las comunicaciones: esto no debería ocurrir por cuanto no hay congestión en la red, el evento claramente es pérdida de paquete por naturaleza del medio físico empleado. Una posible solución a esto, seria algún mecanismo que retroalimente a la red con las diferentes causas por las cuales la pérdida de paquetes ha ocurrido (calidad del enlace inalámbrico, fallos en el nodo sensor, o realmente por una congestión) y de acuerdo a esto tomar la decisión más inteligente.

## 4.2. MQTT - SN: Una versión aún más reducida del MQTT.

El *MQTT-SN (MQTT for Sensor Networks)* deriva del MQTT y conserva el mismo principio de funcionamiento, con las siguientes particularidades que lo hacen aún más apto para ciertos ambientes embebidos donde la criticidad de los datos se ve superada por un enlace muy limitado:

- Soporta ID de tópicos en lugar de nombres de tópicos. Al registrarse un tópico especifico se envía el nombre (por ejemplo “”/hogar/living/zon11/temperatura”) y un ID de 2 bytes al bróker. Esto permite ahorrar espacio al momento de publicar o consumir un recurso, ya que estaríamos enviando un número entero en lugar de una cadena de caracteres más compleja. Estos Ids de tópicos podrían también ya estar definidos en un Gateway MQTT-SN, de manera que incluso se evita la primera etapa de registro.

- No se requiere del stack TCP/IP. Pudiendo correr sobre un link serial o bien sobre UDP, en ambos casos soluciones claramente más livianas que TCP.

- Como desventaja, es que seguramente requiramos de una especie de Gateway para publicar la información de los nodos en una red de capas superiores basada en IP.

## 4.3. CoAP (Constrained Application Protocol)

Es el protocolo definido por la **IETF** para el “uso en nodos y redes limitadas” en su RFC 7252 [69].

CoAP es un protocolo basado en cliente/servidor proporcionando un modelo de comunicación compatible con la arquitectura REST, pero implementando un subconjunto de sus instrucciones y haciéndolo más apto para nodos con claras limitaciones de memoria y procesamiento (Constrained RESTful Environments -CoRE).

Para comprender mejor, la **arquitectura REST** es una arquitectura de comunicación entre procesos basada en mensajes HTTP, que se estructuran en formato JSON (el cual es más reducido que XML). REST es una arquitectura cliente/servidor, donde el servidor pone a disposición un punto de acceso o API por cada entidad que gestione. Luego el cliente opera sobre esa entidad, realizando diferentes acciones dependiendo del método HTTP utilizado. Por ejemplo, si se accede a la API mediante el método GET, entonces el servidor devolverá el recurso solicitado, mientras que si se accede a la misma API con método

POST, entonces el servidor estará creando (y eventualmente persistiendo) un nuevo objeto de dicha entidad.

Entre los objetivos al diseñar el protocolo CoAP se pensó en una interacción fácil con HTTP, soporte para descubrimiento de servicios/recursos, multicasting, intercambio de mensajes de manera asincrónica, un formato de paquete reducido y corriendo sobre una capa de transporte con un nivel de confiabilidad opcional (datagramas sobre UDP).

El funcionamiento de CoAP es similar al modelo cliente/servidor del HTTP, pero en la práctica en un entorno nodo-a-nodo (machine to machine), los roles de cliente y servidor se van intercambiando. Un *request* en CoAP es enviado al cliente para requerir una acción determinada en un recurso determinado (identificado con una URI) en un servidor (que puede ser otro nodo). El servidor entonces responde enviando un código de respuesta que incluye una representación de un recurso. Los métodos usados son los ya conocidos en el ambiente web http *Get, Put, Post y Delete.*

Fortalezas del CoAP:

- UDP*:* si bien CoAP se ejecuta sobre UDP, que es menos confiable que TCP, base su confiabilidad en la repetición de mensajes en lugar de conexiones consistentes.
  Los datagramas UDP también permiten ciclos más rápidos de activación y transmisión, así como paquetes más pequeños con menos sobrecarga. Esto permite que los dispositivos permanezcan en estado dormido durante períodos de tiempo más largos, conservando la energía de la batería.
- Soporte Multicast*:* dado que está montado sobre IPV6, éste nativamente soporta multicasting de mensajes, enviando paquetes de uno a muchos y de muchos a muchos.
- Seguridad: sobre UDP sería posible y recomendable montar una capa de encriptación utilizando DTLS.
- Servicio de búsqueda de recursos *(Resource/service discovery):* dependiendo del tipo de nodo (por ejemplo si tiene mucha o poco disponibilidad de energía), podría comunicarse con una URI de un recurso específico o acceder a una URI diferentes (que por ejemplo permita tiempos de latencia mayores).

- Asincronismo/Observer*:* si bien CoAP funciona en un esquema request/report, puede simularse un modo de funcionamiento asincrónico con los llamados "Observers". Con una idea similar al broker MQTT, el nodo 1 podría "observar" ciertos tipos de mensajes del nodo 2. Una vez que el nodo 1 despierta, el mensaje le es transmitido. Esto se logra, con un tercer nodo que almacene temporalmente el mensaje y luego lo transmita.
- Confiabilidad de los paquetes *(QoS):* en CoAP los mensajes puede ser trasmitidos como "Confirmables" o "No confirmables". En el primer caso, el mensaje es retransmitido hasta tanto se reciba un ACK del mismo ID de mensaje. En los caso de los mensajes "no confirmables", ningún ACK es requerido (similar al MQTT "Fire and Forget"). De todas formas, se trasmite un ID de mensaje para evitar duplicados en el receptor.

Quizás el mayor punto débil en torno a CoAP sea su maduración dentro de la industria. MQTT es un protocolo más probado, y también resulta más fácil encontrar recursos (librerías) para un despliegue más ágil en comparación a hacerlo con CoAP.

**Comparativa entre ambos:**

Nos resulta interesante citar un trabajo de investigación [70], donde se analiza la performance de ambos protocolos corriendo un mismo software como gateway. En el mismo se observa, que la performance de los mismos está asociada a las condiciones de la red. En redes con poca pérdida de paquetes **MQTT** demostró menos retrasos que **CoAP**, mientras que cuando se da la situación contraria en escenarios con mucha perdida de paquetes, **CoAP** tiene menos retardos para enviar información. Para tamaños de paquetes pequeños y a igual tasa de errores, **CoAP** genera menos tráfico que **MQTT**, para asegurar comunicaciones confiables. Mientras que cuando el tamaño de paquetes se incrementa, MQTT genera menos tráfico que el CoAP (esto podría entenderse dado que UDP tiene más posibilidades de perder un datagrama que cuando se corre bajo TCP, lo cual obliga a CoAP a retransmisiones completas más frecuentes).

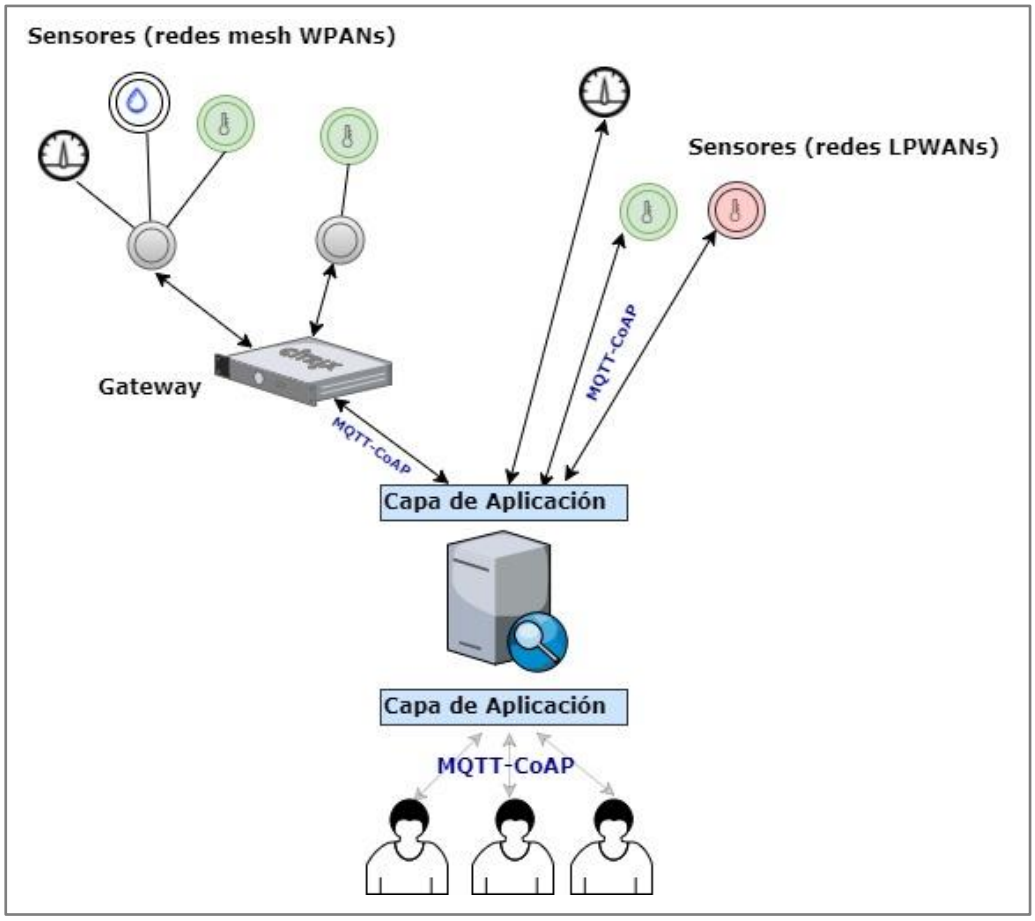



**Fig. 26 - Ejemplo esquema de comunicación**

# 5. Sistemas Operativos para Redes de sensores

Los avances en las redes de comunicaciones permitieron que los nodos sean cada vez más pequeños, flexibles y de bajo costo. Hoy estos nodos interactúan entre sí y con otros dispositivos como sensores y actuadores para formar redes de comunicación que se basan en dispositivos con CPUs de bajo consumo y poca memoria.

Estas características hacen que existan nuevas motivaciones para el desarrollo de sistemas operativos. [71]:

- **Recursos limitados:** las motas tienen recursos físicos muy limitados, debido a los objetivos de tamaño pequeño, bajo costo y bajo consumo de energía. Las motas actuales consisten en procesadores de alrededor de 1 MIPS (1 millón de instrucciones por segundo. Un procesador actual ronda las 30.000 MIPS) y decenas de kilobytes de almacenamiento. Por citar un ejemplo, los desarrolladores de TinyOS afirman que no esperan que las nuevas tecnologías eliminen estas restricciones. La idea es que la Ley de Moore se aplique en vías de reducir el tamaño y el costo, en lugar de aumentar la capacidad.
- **Concurrencia reactiva:** en una aplicación típica red de sensores, un nodo es responsable del muestreo de aspectos de su entorno a través de sensores, manipulación de actuadores, realizar procesamiento local de datos, transmisión de datos, ruteo de datos hacia otros nodos, y participar en diversas tareas de procesamiento distribuido, como por ejemplo agregación estadística. Muchos de estos eventos, tales como la gestión del hardware de radio, requieren respuestas en tiempo real. Esto requiere un enfoque de gestión de concurrencia que reduzca errores potenciales respetando las limitaciones de recursos y de tiempo.
- **Flexibilidad:** la variación en el hardware y las aplicaciones y el ritmo de innovación requieren un sistema operativo flexible que sea:
    - Específico de la aplicación para reducir el espacio y potencia.
    - Independice la frontera entre hardware y software.

  Además, el sistema operativo debe soportar modularidad de grano fino e interposición para simplificar la reutilización y la innovación.
- **Bajo consumo:** las demandas de tamaño y costo, así como la operación desatendida hacen que la baja potencia sea un objetivo clave de diseño de las motas. La densidad de la batería se duplica aproximadamente cada 50 años, lo que

hace que la alimentación del hardware sea un desafío permanente. Aunque la recolección de energía ofrece muchas soluciones prometedoras, en la muy pequeña escala de las motas podemos obtener solo microvatios de potencia. Esto es insuficiente para el funcionamiento continúo de hasta los diseños más eficientes energéticamente.

Existen varios sistemas operativos que persiguen estos objetivos. Muchos de ellos actualmente se ofrecen como soluciones IoT, dado el importante crecimiento que este concepto en los últimos años. Crecimiento que se ve reflejado en un incremento importante en la venta de microcontroladores y que fuerza a los desarrolladores de sistemas operativos embebidos a acompañar los crecientes. [72]
A continuación mencionamos algunos de ellos con sus características más relevantes.

## 5.1. TinyOS

No es un sistema operativo en el sentido tradicional; es un framework de programación para sistemas embebidos y un conjunto de componentes que permiten la construcción de un sistema operativo específico de cada aplicación. Tiene un modelo de programación basado en componentes, codificada en el lenguaje NesC, un dialecto del C. [71]

Este sistema de código abierto fue desarrollado en la Universidad de Berkeley, California, con el objetivo de satisfacer varios aspectos que hacen al desarrollo de aplicaciones basadas en redes de sensores. Está diseñado para funcionar sobre el propio hardware de los nodos, dándole al desarrollador una interfaz que lo abstrae de la comunicación con el hardware, así como también lo abstrae de aspectos relacionados con las comunicaciones. Todo esto encuadrado en las limitaciones y características que las redes de sensores imponen, aquellas de las que hemos ido hablando a lo largo de esta tesis.

Sólo para contextualizar lo descripto, una aplicación típica basada en TinyOS es de aproximadamente 15K de tamaño, de las cuales el sistema operativo base es de aproximadamente 400 bytes. [71]

## 5.2. Contiki

Contiki OS es un sistema operativo de código abierto desarrollado en el lenguaje C para uso en pequeños sistemas con arquitecturas desde 8 a 32 bits, mantenido por una amplia comunidad de desarrolladores [73]. Está enfocado para correr en dispositivos con menos de 8kb de memoria ram y alrededor de 50 kb de memoria flash para memoria de programa.

Contiki es independiente de una plataforma de hardware específica y puede correr en una amplia variedad de arquitecturas (MSP430, AVR, ARM) de diferentes fabricantes.

Entre las características que posee Contiki podemos destacar:

- Protohilos, para ahorro de memoria y un mejor control de flujo del programa. Es un mecanismo basado en eventos y en la programación multithread. Brinda métodos para alocación de memoria por parte del programador: memb, mmem, malloc.
- Soporte para protocolos UDP, IPv4 e IPv6, y para nuevos protocolos de bajo consumo como 6LoWPAN, COAP y RPL.
- Modos de funcionamiento bajo consumo, con rutinas implementadas para "dormir" a los dispositivos por un tiempo determinado o hasta que acontezca un suceso significativo (interrupción), pudiendo extender la duración de las baterías por años.
- Entorno de simulación Cooja. Este poderoso entorno de simulación permite programar sobre múltiples plataformas de hardware y realizar pruebas sobre entornos simulados a gran escala. Luego el mismo código que emulamos puede ser grabado al hardware de producción sin modificaciones.
- Actualización "*on the fly*". Permite actualizar el binario del nodo sensor a través de la red, sin necesidad de replegar toda la red instalada.

## 5.3. RIOT

Riot es un sistema operativo de código abierto desarrollado en el lenguaje C++, diseñado para escenarios de IoT [74]. Al igual que TinyOs y Contiki, está optimizado para bajos recursos de memoria, alta eficiencia energética, programación modularizada y múltiples librerías de comunicación (IPv6, 6LoWPAN, UDP, RPL, CoAP).

Este sistema operativo es compatible con la mayoría de los dispositivos IoT y microcontroladores de 8, 16 y 32 bits.

Tiene soporte para *multi-threading* con una sobrecarga muy baja para la gestión de los hilos (menos de 25 bytes por hilo).

Capacidad de procesamiento en tiempo real, debido a la baja latencia de interrupciones: cada aproximadamente 50 ciclos de reloj.

## 5.4. Tizen

Tizen es un sistema operativo de código abierto, basado en Linux, construido desde el principio para satisfacer las necesidades del ecosistema de dispositivos móviles y conectados, incluyendo fabricantes de dispositivos, operadores móviles, desarrolladores de

aplicaciones y proveedores de software independientes. Tizen está abierto a todos los miembros que deseen participar.

Existen varios perfiles, orientados a las diferentes soluciones (wereables, TV, mobile, etc.) y un perfil común, el cual permite ser adaptado según los requerimientos de memoria, procesador y energía. La versión más liviana podría funcionar con solo 256 MB de RAM y 1 GB de espacio de almacenamiento no volátil.

El perfil común soporta arquitecturas de procesador dx86_64 (Atom), i586, armv7l y aarch64.

Recientemente la empresa Samsung anunció que sacará al mercado un sistema operativo IoT, basado en Tizen. Desde entonces Samsung ha aportado gran cantidad de mejoras al proyecto, como la compatibilidad con el framework de desarrollo .NET [75].

## 5.5. Android Things

Android Things, antes llamado Google Brillo, es el sistema operativo IoT de Google. Como su nombre lo describe, está basado en Android y adaptado para su funcionamiento en dispositivos con recursos de hardware bajos o medios. Los recursos que requiere al menos deben ser de 512 MB de memoria RAM y 4 GB de almacenamiento, limitando claramente su aplicación en microcontroladores más básicos. [76]

Las principales características de este sistema operativo son:

- API de entrada y salida a dispositivos: Soporta comunicación con la mayoría de los sensores y actuadores usando protocolos estándar e interfaces.
- Permite crear APIs de hardware a medida.
- Soporta algunas aplicaciones nativas como calendario, diccionario y gestor de downloads, entre otras.
- Integra un kit de desarrollo para soportar interfaces gráficas.
- Tiene soporte para un subconjunto de servicios de "*Google Services*" como por ejemplo el servicio de ubicación (*Location Service*)

## 5.6. Windows 10 IoT

Windows 10 IoT es el Sistema operativo para IoT de Microsoft. Es un sistema operativo que solo funciona sobre arquitecturas ARM, X86 y x64 (con requerimientos de memoria ram mínimos de 512 MB y 2 GB para almacenamiento), pero que posee mucha flexibilidad, especialmente desde el punto de vista del desarrollo.

Las aplicaciones para este sistema operativo pueden realizarse en una gran cantidad de lenguajes de programación como C++, C#, Python o Node.js. Luego, las aplicaciones se ejecutan en un contexto de virtualización que les permite portabilidad con cualquier dispositivo Windows.

Otra característica destacable es la existencia del framework de "*IoT Gateway SDK*" que les da a las aplicaciones la capacidad de utilizar *Cortana, OpenCV y CognitiveServices*, entre otros servicios de la plataforma Microsoft Azure para soluciones de avanzada. [77]

### Reflexiones

Existen varios sistemas operativos que se adaptan a las soluciones de redes de sensores. A su vez cada uno de ellos posee diferentes requerimientos de hardware y brindan diferentes servicios. Los más reducidos (como TinyOs, Contiki y RIOT) funcionan como una capa de abstracción al hardware, mientras que los más avanzados, aquellos que están siendo desarrollados y mantenidos por las grandes empresas de la industria de la tecnología, permiten el desarrollo de aplicaciones integradas con servicios en la nube y poseen librerías para funcionalidades avanzadas, pero a costa de más altos requisitos de hardware (ejemplo Tizen, Microsoft IOT y Android Things). El abanico de posibilidades es grande y optar por uno o por otro depende en gran medida de la solución que se desee implementar.

Por otro lado, se puede apreciar una clara tendencia de la industria a orientar los sistemas operativos de microcontroladores a soluciones IoT, donde la función de los dispositivos no se limita al sensado, sino a ofrecer utilidades con valor para usuarios finales.

Entendemos que este campo es una temática compleja en la cual se puede ahondar mucho más fuera del contexto del presente trabajo.

# 6. Campos de aplicación de las WSN

Es difícil dar una definición abarcativa sobre los campos de aplicación de las WSN, ya que estas tienen variadas utilidades, y sus aplicaciones crecen constantemente en función de las necesidades. En este trabajo nos centraremos particularmente en los aportes de esta tecnología al terreno de las Smart Cities.

Podemos mencionar diferentes áreas de aplicación como lo son: las redes de distribución de energía eléctrica y la distribución de recursos como el agua potable o de riego; en la optimización de sistemas de transportes y tránsito vehicular; para monitoreo ambiental y toma de decisiones ante catástrofes naturales; aplicaciones en el campo de la domótica y la construcción de edificios inteligentes, como así también en el mantenimiento de grandes estructuras construidas por el hombre (puentes, represas, oleoductos, etc.); servicios de atención al ciudadano, como el seguimiento en materia de salud para pacientes críticos, asistencia al ciudadano ante emergencias, en materia de seguridad o incluso plataformas para el desarrollo del turismo.

Dentro de cada área existen variadas implementaciones, las cuales resuelven necesidades específicas e implementan diferentes tecnologías existentes en materia de protocolos y hardware. Describiremos en el presente trabajo algunos proyectos concretos que nos resultaron de interés en diferentes ciudades y otros campos de aplicación.

Antes de enfocarnos en el aporte que las redes de sensores brindarán en pos del desarrollo de las “ciudades inteligentes” y contar distintos proyectos llevados a cabo en la actualidad, nos resulta primordial establecer un marco descriptivo para este concepto, que involucra no solo temáticas en torno a las TICs, sino también enfoques y discusiones multidisciplinarias.

## 6.1. Contexto y definiciones

Diversos factores socio-económicos han llevado a un aumento de la densidad de la población, generado principalmente por un crecimiento poblacional y una alta concentración en grandes urbes del mundo. Al día de hoy, más de la mitad de la población del mundo se encuentra viviendo en áreas urbanas.

Según diversos estudios publicados [78], esta tendencia se seguirá profundizando, generando que en una misma área poblada convivan más personas por kilómetro cuadrado promedio, habiendo estimaciones que para el año 2050 el 66% de la población mundial residirá en áreas urbanas. En el caso de Argentina, ese porcentaje se eleva al 92%, lo cual pone de manifiesto la magnitud de la problemática. [79]

Esta dinámica crea la necesidad de pensar prioritariamente en modelos de desarrollo que organicen los procesos dentro de las ciudades, por medio de sistemas que promuevan el uso eficiente de los recursos, además, potencialicen la actividad económica y promuevan el desarrollo social. [80]

Esto conlleva el replanteo de muchas situaciones para analizar, como ser, la generación y distribución de recursos básicos (agua y energía para hogares e industria), aumento de disponibilidad habitacional y fuentes de trabajo, adecuación de infraestructura vial y de los servicios de telecomunicaciones, optimización de los recursos energéticos y desarrollo de nuevos modelos sustentables en armonía con el medio ambiente donde nos encontramos inmersos. Todo esto claro, a fin de lograr una mejora en la calidad de vida de los ciudadanos que habitan estas ciudades.

Para englobar todos estos aspectos que una ciudad inteligente debería considerar, nos resultó conveniente citar algunas fuentes que resuman conceptualmente estas ideas:

*"Una Smart City es toda ciudad que mejora la calidad de vida de sus ciudadanos y su sostenibilidad ambiental, utilizando la eficiencia tecnológica y contando con la participación de la sociedad".* [81]

*"Las ciudades y las comunidades Inteligentes son un modelo que integra energía, transporte, información y comunicación con el objetivo de catalizar el progreso en áreas donde: (i) la producción, distribución y uso de energía, (ii) la movilidad y transporte y (iii) las tecnologías de la información y la comunicación están íntimamente ligadas y ofrecen nuevas oportunidades interdisciplinarias para mejorar los servicios y reducir el consumo de recursos: energía, gases de efecto invernadero y otras emisiones contaminantes*". [82]

*"Una ciudad que ofrece soluciones sistémicas (integradas e interconectadas) basadas en tecnologías que pueden reducir los costos financieros y humanos/sociales al tiempo que aumentan la calidad de vida, con visión y compromiso para crear nuevas formas de trabajar juntos en las comunidades*". [83]

*"Una ciudad que combina las TIC y la tecnología de la Web 2.0, diseñando y planeando esfuerzos para desmaterializar y agilizar los procesos administrativos gubernamentales y ayudar a identificar nuevas e innovadoras soluciones a la complejidad de la gestión de la ciudad, con el fin de mejorar la sostenibilidad y la habitabilidad".* [84]

*"Una ciudad que monitorea e integra las condiciones de todas sus infraestructuras críticas incluyendo carreteras, puentes, túneles, vías, transporte público, aeropuertos, puertos marítimos, comunicaciones, energía, agua, a fines de optimizar su utilización, realizar mantenimientos preventivos y controles de seguridad, para brindar una mejor calidad de vida a sus ciudadanos".* [85]

Un aspecto a destacar en lo relacionado a las Smart Cities es que existen infinidad de definiciones, cada una desde la óptica de quien la desarrolla. Para evitar ambigüedades y sentar las bases sobre las cuales se puedan desarrollar estándares, la ITU (*International Telecomunication Union*) realizó un reporte técnico, el cual estuvo a cargo de la ITU-T (*Telecommunication Standarization sector of ITU*) y tuvo como objetivo la creación de una definición concreta de Smart City, en base a las definiciones existentes. Dicha definición es la siguiente [86]:

Una ciudad inteligente y sostenible es una ciudad que aprovecha la infraestructura ICT (*Information and Communication Technology*) de una manera adaptable, fiable, escalable, accesible, segura y resistente para:

- Mejorar la calidad de vida de sus ciudadanos.
- Garantizar un crecimiento económico tangible, como mejores niveles de vida y oportunidades de empleo para sus ciudadanos.
- Mejorar el bienestar de sus ciudadanos, incluyendo atención médica, bienestar, seguridad física y educación.
- Establecer un enfoque ambientalmente responsable y sostenible que "satisfaga las necesidades de hoy sin sacrificar las necesidades de las generaciones futuras".
- Simplificar los servicios basados en infraestructura física, tales como transporte (movilidad), agua, servicios públicos (energía), telecomunicaciones y sectores manufactureros.
- Reforzar la prevención y la manipulación de los desastres naturales o provocados por el hombre, incluida la capacidad para hacer frente a los efectos del cambio climático.
- Proporcionar mecanismos eficaces y bien equilibrados de regulación, cumplimiento y gobernanza con políticas y procesos apropiados y equitativos de manera estandarizada.

ITU 2014/10 - Smart sustainable cities: An analysis of definitions

Es importante destacar que las definiciones que la conforman no tienen un rigor técnico en el contexto de las redes de datos, sino que definen aspectos que las ciudades deben cumplir. Dichos aspectos pueden ser suplidos por servicios en los cuales la tecnología juega

un papel preponderante. Las redes de sensores son una herramienta para brindar estos servicios, o pueden ser un medio facilitador de los mismos, como se desarrolla a lo largo del presente documento.

A pesar de la distancia que posee la definición, al analizarla más en profundidad nos encontraremos con definiciones objetivas y fácilmente asociables a soluciones tecnológicas. Podemos analizar, por ejemplo, la premisa mencionada en la definición sobre "Mejorar la calidad de vida de sus ciudadanos". Para ello veamos una definición integradora sobre "Calidad de Vida".

> *"Calidad de vida es un estado de satisfacción general, derivado de la realización de las potencialidades de la persona. Posee aspectos subjetivos y aspectos objetivos. Es una sensación subjetiva de bienestar físico, psicológico y social. Incluye como aspectos subjetivos la intimidad, la expresión emocional, la seguridad percibida, la productividad personal y la salud objetiva. Como aspectos objetivos el bienestar material, las relaciones armónicas con el ambiente físico y social y con la comunidad, y la salud objetivamente percibida"*. [87]

## 6.2. Otros factores que influyen en el desarrollo de ciudades inteligentes

Si bien el concepto o enfoque de Ciudad Inteligente cambia de acuerdo a las necesidades que se buscan solucionar o la vocación de la ciudad (actividad económica principal), podemos analizar diversos factores en común que deberán tenerse en cuenta al momento de proyectar una ciudad de este tipo. Diversos autores y casos de estudios analizados, plantean desafíos no solo tecnológicos sino también de índole política, económica, social y natural. Claro que el foco de esta tesina, se centra en el aspecto tecnológico, más específicamente en el aporte que las Redes de Sensores inalámbricas pueden brindar, pero nos resultó interesante dejar planteado estas otras cuestiones, que en mayor o menor medida, son claves para emprender un desarrollo a gran escala.

En este sentido, IBM ha sido una de las pioneras desde el año 2008 desarrollando un área de I+D denominada "Planeta Inteligente", la cual tiene como objetivo el desarrollo y divulgación de avances para la integración de sistemas inteligentes a la vida de las personas. Para ello se plantea la necesidad de *"profundos cambios en la gestión y gobernanza hacia enfoques mucho más colaborativos".* [88].

Como se aprecia en la anterior definición, los enfoques "inteligentes" van mucho más allá del desarrollo meramente tecnológico. En ese sentido, Planeta Inteligente define que una ciudad inteligente debe ser encarada desde tres áreas fundamentales:

- Planificación y gestión.
- Infraestructura.
- Servicios a las personas.

Las ciudades más inteligentes impulsan el crecimiento económico sostenible y la prosperidad para sus habitantes. Sus dirigentes disponen de herramientas para analizar los datos que les permitirán tomar mejores decisiones, anticiparse a los problemas y coordinar los recursos para actuar de forma eficiente. En este sentido, la gran cantidad de información que puede ser obtenida en una ciudad es la fuente de alimentación para que, mediante soluciones tecnológicas, se asista a gobernantes y ciudadanos.

En el siguiente gráfico se puede observar la clasificación de las áreas de interés realizado por IBM:

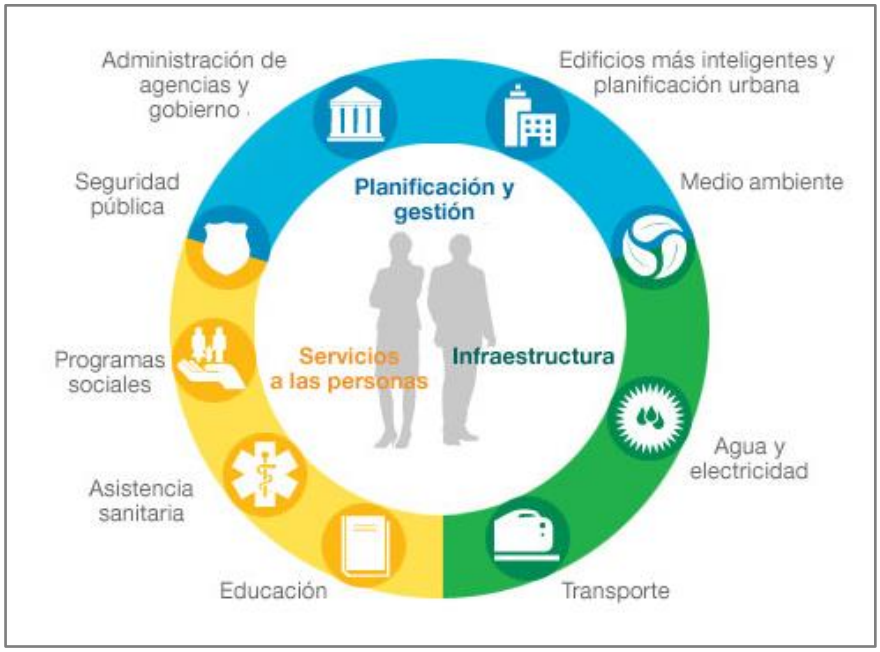



**Fig. 27 - Planeta I+D IBM [88]**

- **Servicios de gestión y planificación**: La planificación y la gestión requieren de la creación y puesta en marcha de mecanismos que permitan a la ciudad desarrollar todo su potencial manteniendo la eficiencia en las operaciones diarias. Los dirigentes deben disponer de información que les permita ver de forma global el manejo de las operaciones, la gestión de emergencias y el cumplimiento de la ley, la administración de agencias y gobiernos y la planificación urbanística, incluyendo edificios inteligentes. [88]
- **Servicios de infraestructura**: Los servicios de infraestructura dan calidad de vida a las ciudades. Son servicios básicos que atienden tanto necesidades como

comodidades para ciudadanos y empresas. Dentro de este grupo se encuentran los servicios de agua y electricidad, transportes y zonas verdes, entre otros. [88]

- **Servicios a las personas:** Los servicios a las personas atienden a las necesidades de los ciudadanos como individuos. Esto incluye aspectos relacionados con las de bases de desarrollo, asistencia social como por ejemplo los servicios de mano de obra, programas sociales, asistencia sanitaria y educación. [88]

Como podemos deducir de los puntos anteriormente mencionados, la implementación de servicios inteligentes (o la creación de ciudades inteligentes), afecta de forma directa e indirecta en la calidad de vida de los ciudadanos. La eficiencia en el uso de recursos, la gestión de mantenimiento, el soporte para funciones administrativas, etc. tienden a optimizar la forma en que el ciudadano interactúa con la ciudad y se desarrolla en ella. Una ciudad inteligente apunta a ser más justa, segura y confortable que aquella que no lo es, aunque ambas dispongan de los mismos recursos humanos, económicos y ambientales, por la eficiencia en que dichos recursos son administrados.

## 6.3. Normalizaciones

Desde el año 2014 distintas entidades de estandarización y redacción de normas, han venido trabajando para publicar sus propias normativas relacionadas a los aspectos que deberán regularse en el campo de las redes de sensores para Internet de las Cosas y más precisamente en el ámbito de las Smart Cities.

Entre los que podemos mencionar se encuentran los principales organismos de alcance internacional como:

- ITU (Unión Internacional de Telecomunicaciones)
- ISO (Organización Internacional de Normalización)
- IEC (Comisión Electrotécnica Internacional)
- CEN (Comité Europeo de Normalización)
- IEEE (Instituto de Ingeniería Eléctrica y Electrónica)

Y países desarrollados en la materia, que han avanzado en su propia estandarización. Entre ellos podemos mencionar los siguientes:

- NIST / ANSI (Estados Unidos)
- AENOR (España)
- BSI (Reino Unido)
- DKE/DIN (Alemania)

En la siguiente tabla resumimos las publicaciones o grupos de trabajos que se han ido armando en torno a la temática de Internet de las Cosas y Ciudades Inteligentes:

| Organismo | Estándar/Grupo de Trabajo |
|---|---|
| International Standards Organization (ISO) | Áreas de trabajo del Comité técnico ISO/TC 268:<br><br>• **ISO/TR 37101:2016**<br>Desarrollo sustentable en comunidades<br>• **ISO/TR 37120:2014**<br>Indicadores para el desarrollo de comunidades sustentables<br>• **ISO/TR 37150:2014 / 37151:2015**<br>Infraestructuras para comunidades inteligentes<br><br>[89] [90] [91] |
| International Telecommunications Union (ITU) | Grupo de trabajo en ciudades inteligentes y sostenibles:<br>• **SG5**: medioambiente y cambio climático<br>• **SG20**: internet de las cosas (IoT) y ciudades y comunidades inteligentes (SC&C)<br>[86] |
| International Electrotechnical Commision (IEC) | Joint Technical Comitee entre la IEC y la ISO<br>• **ISO/IEC 20005:2013 "*Sensor Networks*"**<br>• **ISO/IEC JTC 1/SG 1** "***Smart Cities*"**<br>• Grupo de Trabajo **ISO/IEC JTC 1/ WG10**. Tiene bajo desarrollo la norma **ISO/IEC CD 30141** "*Internet of Things Reference Architecture (IoT RA)*"<br>• Subcomité de la **ISO/IEC JTC 1/SC 41**<br>"*Internet of Things and related technologies*". Está dividido en dos grupos de trabajos: WG1 – Redes de Sensores y WG2 Internet de las Cosas<br><br>[92] |
| IEEE | IEEE está trabajando en estándares para las siguientes áreas:<br><br>• *IoT*<br>▪ **IEEE P2413** " *Draft Standard for an Architectural Framework for the Internet of Things (IoT)"* |

| Organismo | Estándar/Grupo de Trabajo |
|---|---|
| | • *Smart Energy: Connecting to Smart Grids*<br>▪ **IEEE 1547** series "Handling distributed resources in electric power systems"<br>▪ **IEEE 1815** series "Electric power systems communications"<br>▪ **IEEE 2030** series "Smart Grid, including electric vehicle infrastructure, microgrid, energy storage"<br><br>• *Smart Networking and Connectivity*<br>▪ **IEEE 802** series "Wired and wireless networking"<br>▪ **IEEE 802.22** series "Wireless regional area networks (WRAN)"<br>▪ **IEEE 1451** series "Addressing sensors (adopted by ISO/IEC)"<br>▪ **IEEE 2700** series "Sensors performance"<br><br>• *Smart Transportation*<br>▪ **IEEE 1609** series "Intelligent transportation"<br>▪ **IEEE 2030.1.1** "Technical Specifications of a DC Quick Charger for Use with Electric Vehicles"<br>▪ **IEEE P2690** "Draft Standard for Charging Network Management Protocol for Electric Vehicle Charging Systems"<br>▪ **IEEE P2040** series "Connected, automated, and intelligent vehicles".<br><br>• *Smart Homes and Buildings*<br>▪ **IEEE 1888** series "Ubiquitous green community control networks"<br>▪ **IEEE 1905.1** "Convergent digital home network for heterogeneous technologies"<br><br>• *E-Health*<br>▪ **ISO/IEEE 11073** "Personal Health Data (PHD)"<br><br>• *Clod Computing*<br>▪ **IEEE P2301 / P2302** "Cloud Portability and Interoperability"<br><br>[93] [94] |

| Organismo | Estándar/Grupo de Trabajo |
|---|---|
| European Standards Organizations (CEN/CELENEC/ETSI) | **Smart and Sustainable Cities and Communities Coordination Group (SSCC-CG)**<br>• Reporte con definiciones y recomendaciones.<br>• Desarrollo de estándares para soluciones para ciudades y comunidades inteligentes.<br>• Intercambios con la ITU, ISO y IEC.<br>[95] |
| British Standards Institute (BSI) | Suite de publicaciones (PAS) del British Standards Institute – BSI en torno a la temática de SmartCities:<br>• **PAS 180** – Terminologías<br>• **PAS 181** – Estándar para plataformas<br>• **PAS 182** – Modelo de datos<br>• **PD 8100** – Resumen ejecutivo Smart cities<br>• **PD 8101** – Planeamiento y desarrollo de comunidades sustentables.<br>• **BS 8904-11000** - Gestión y trabajo colaborativo entre los diferentes participantes<br>[96] |
| Asociación Española de Normalización y Certificación (AENOR) | Normas de diferentes grupos de trabajo sobre temáticas de:<br>Infraestructura – **PNE 178101 - 178106**<br>• Indicadores y semántica – **PNE 178201**<br>• Gobierno – **PNE 178301/178303**<br>• Movilidad – **PNE 178302**<br>• Medio ambiente - **PNE 178401**<br>• Turismo – **PNE 178501/178502**<br>[97] |
| American National Standards Institute (ANSI) | Red ANSI para el desarrollo de ciudades inteligentes y sustentables (**ANSSC**).<br>[98] |
| National Institute of Standards and Technologies (NIST) | Trabajando en el desarrollo de una plataforma para IOT en SmartCities<br>[99] |
| German Standards (DKE/DIN) | **Smart City Standardization Roadmap**<br>**Grupo de trabajo NA 172-00-12 AA** |

| Organismo | Estándar/Grupo de Trabajo |
|---|---|
| | Se define agenda de trabajo en :<br>Edificios, seguridad, movilidad, Smart grid (energía), organización urbana, producción y logística.<br>[100] |
| China National IT Standardization TC (NITS) | Los siguientes organismos están trabajando en proyectos para normalización de actividades relacionadas a SmartCities:<br>NITS (Comité Nacional de estandarización)<br>MIIT (Ministerio de Industria y IT)<br>NDRC(Comisión Nacional de Desarrollo)<br>MOHURD(Ministerio de Vivienda y desarrollo Urbano-Rural)<br>• *Application guide on Smart Cities SOA Standards*<br>• *Technology Reference Model for Smart Cities Build*<br>• *Smart Cities Evaluation Model: Information Infrastructure*<br>• *Smart Cities Evaluation Model: Information Application and Service*<br>• *Smart Cities Evaluation Model: Construction and Management*<br>• *Technology on Information Security*<br>[101] |

**Tabla 2 - Organismos de estandarización**

De algunos de estos participantes, nos interesa describir brevemente las líneas de trabajo que nos resultaron de interés en algunos de ellos: la ITU, ISO y AENOR de España.

### 6.3.1. ITU

A partir del año 2015, la ITU crea la comisión de estudio **CE20** para desarrollar normas y directrices que impulsen a las tecnologías de IoT a abordar los retos del desarrollo urbano.

Estructuralmente se dividió en dos grupos de Trabajo:

- Grupo de Trabajo 1 (WP1): **Internet of Things (IoT)**
- Grupo de Trabajo 2 (WP2): **Smart cities and Communities (SC&C)**

El objetivo principal de estos trabajos será entonces:

“La normalización de arquitecturas de extremo a extremo para IoT, y mecanismos para la interoperabilidad de aplicaciones IoT y conjuntos de datos empleados por diversos sectores industriales orientados verticalmente”. [102]

En las propuestas técnicas de la ITU se plantea el desafío de pasar de un esquema verticalista con proveedores de soluciones con esquemas cerrados hacia un esquema con plataformas que permitan una integración horizontal e integrada para las comunidades. Ver gráfico siguiente:

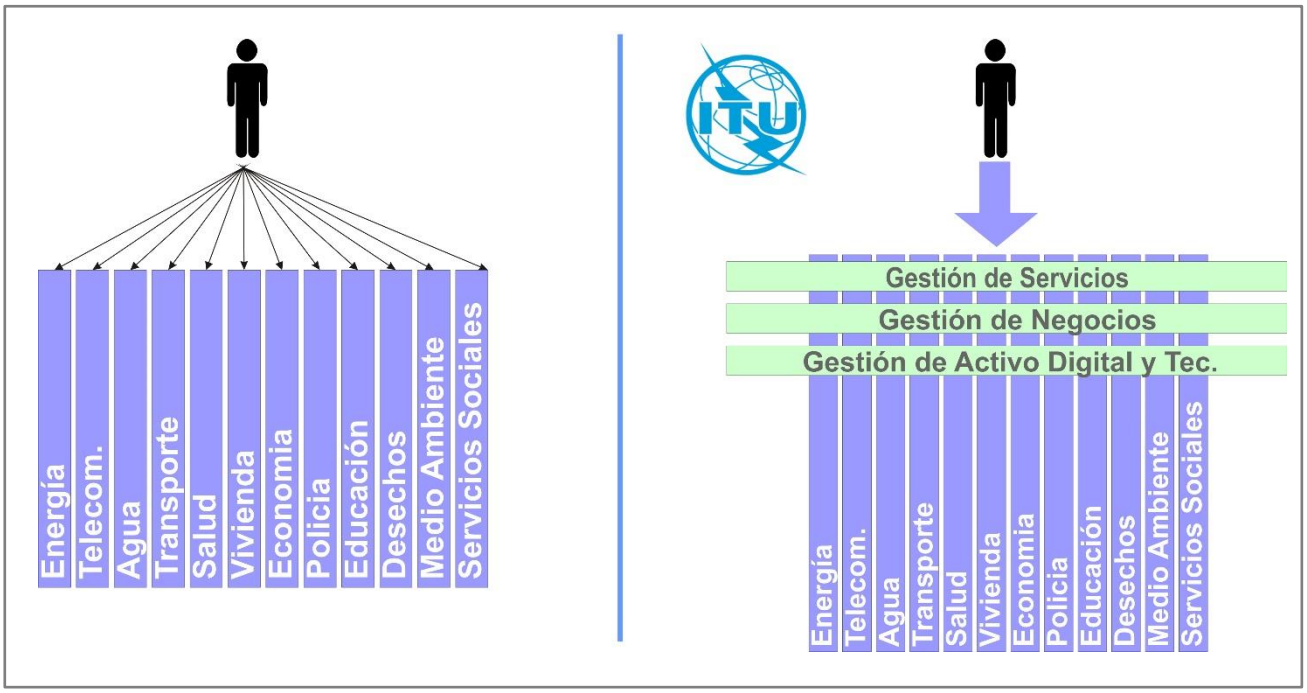



**Fig. 28 - Arquitectura de servicios SSC [86]**

Desde el punto de vista técnico la ITU se propone abordar otros retos de IoT, como:

- **Seguridad**, debilidades a ser tratadas antes de que el IoT llega a escalas grandes, por ejemplo en redes criticas como Energía, Agua y Transporte.
- **Fortalecer y proteger al usuario final,** riesgos de seguridad, datos privados, soberanía y residencia de los datos.
- **Interoperabilidad y Riesgo de Silos de IoT,** entre plataformas de proveedores desarrolladas independientemente. Interoperabilidad de aplicaciones IoT garantizada mediante conformidad coordinada con normas comunes.
- **Falta de cohesión en el Desarrollo de Normas,** amplio esfuerzos de normalización, necesitando de una mayor cooperación y armonización.

Los grupos de trabaja de la ITU han venido publicando diferentes Reportes Técnicos con los lineamientos y consideraciones técnicas para el desarrollo de ciudades inteligentes y sostenibles, como así también indicadores para ir monitoreando su evolución.

Un tipo de clasificación generada se realizó en base a las distintas infraestructuras de servicios, que en convergencia con el campo de las TICs, se las cataloga dentro del grupo "*Smart*". A saber [86]:

- *Smart energy* (energía)
- *Smart buildings* (edificios y obras públicas)
- *Smart transportation* (transporte)
- *Smart water* (agua)
- *Smart waste* (residuos)
- *Smart physical safety and security (*seguridad)
- *Smart health care* (salud)
- *Smart education* (educación)

Tomando en cuenta el alcance definido anteriormente de las SSC (*Smart Sustainable City*) la ITU define las siguientes categorías y parámetros para evaluar el nivel de servicios de una ciudad [86]:

| **Infraestructura y Tecnología** | **Sustentabilidad** |
|---|---|
| • Transporte<br>• Construcciones<br>• Servicios de emergencias<br>• Salud<br>• Planeamiento Urbano<br>• Seguridad<br>• Educación | • Medioambiente y peligros naturales<br>• Agua: consumo y desperdicios<br>• CO2: emisiones, reducción<br>• Calidad de aire: NO, SO, material particulado.<br>• Residuos: sólidos, agua, uso de la tierra<br>• Políticas: reciclado, reducción desperdicios<br>• Energía: consumo, intensidad |
| **Gobierno** | **Economía** |
| • Organización<br>• Leyes, Justicia<br>• Resiliencia<br>• Liderazgo<br>• Regulaciones ambientales | • Estabilidad económica<br>• Capital humano<br>• Nivel de las instituciones<br>• Madurez financiera<br>• Capital físico<br>• Capacidad de producción, recursos |

**Tabla 3 - Categorías para evaluar una Ciudad Inteligente**

### 6.3.2. ISO/TC 268: Comité Técnico - Ciudades y comunidades sostenibles

**ISO 37101:2016** [89]

La ISO 37101 establece un sistema de gestión para el desarrollo sostenible, apoyando a las comunidades a poner en marcha una estrategia de desarrollo sostenible que tenga en cuenta su contexto económico, social y ambiental.

Entre sus objetivos se mencionan:

- Generar y construir un consenso sobre el desarrollo sostenible dentro de las comunidades.
- Mejorar la sostenibilidad, y la resistencia de las estrategias, programas o planes en el territorio.
- Mejorar el medio ambiente local, crear un lugar más feliz y más saludable para los ciudadanos, y construir comunidades que puedan anticiparse y adaptarse a los desastres naturales, crisis económicas y el cambio climático.

**ISO/TS 37151:2015** [91]

Presenta una visión general de los principios y requisitos para analizar y medir las infraestructuras comunitarias (como la energía, el agua, el transporte, los residuos y las TIC). Se centra en que se puede medir y relacionar con los problemas de la comunidad.

Se analizan los requisitos para los principales interesados (*stakeholders*), buscando identificar las necesidades y clasificándolas en 3 perspectivas diferentes:

- Para los residentes: acceso a servicios, seguridad, accesibilidad, calidad de vida.
- Para los gestores comunitarios: eficiencia en su operatoria diaria, eficiencia económica, accesibilidad a la información comunitaria, resiliencia (capacidad de adaptación frente a un estado o situación adversa).
- Para el medio ambiente: uso eficientes de los recursos, mitigación del cambio climático, reducción de polución.

**ISO 37120:2014** [90]

Este estándar internacional de la ISO define y establece un conjunto de indicadores a ser tenidos en cuenta para medir la performance de una ciudad en términos de la calidad de sus servicios y calidad de vida. Es aplicable a cualquier ciudad, municipio o gobierno local que se comprometa a medir su desempeño de una manera comparable y verificable, independientemente de su tamaño y ubicación.

Debido a que en la práctica existen diferentes indicadores, los cuales no se encuentran estandarizados ni son consistentes en el tiempo ni entre ciudades, la ISO propone esta lista de indicadores agrupados por temas. Los mismos se dividieron dependiendo de su criticidad como *recomendación* ("*Supporting indicators*") y otros como *mandatorios* ("*Core indicators*").

Entre los indicadores para las ciudades tenemos los siguientes:

1. Económicos
2. Educación
3. Energía
4. Medio Ambiente
5. Finanzas publicas
6. Gestión ante emergencias
7. Gobernanza
8. Salud
9. Recreación
10. Seguridad
11. Albergues para asistencia
12. Tratamiento de la basura
13. Telecomunicaciones e innovación.
14. Transporte
15. Planeamiento Urbano
16. Uso del Agua
17. Sanitización del agua

### 6.3.3. AENOR – ESPAÑA

España es uno de los países pioneros y más avanzados en temas de regulación de *Smart Cities*. La AENOR (Asociación Española de Normalización y Certificación), creó en el año 2012 el comité de investigación **AEN/CTN 178 "Ciudades Inteligentes".**

El Comité Técnico de Normalización **AEN/CTN 178** tiene una subestructura de subcomités y grupos de trabajo que han venido publicando el desarrollo de las diferentes normas UNE ("Una Norma Española"):

1. Subcomité SC1 "Infraestructuras"
2. Subcomité SC2 "Indicadores y Semántica"
3. Subcomité SC3 "Gobierno y Movilidad"
4. Subcomité SC4 "Energía y Medio Ambiente"
5. Subcomité SC5 "Destinos turísticos"

Normas publicadas por **AENOR**:

| Área | Proyecto de norma | Título |
|---|---|---|
| **Infraestructuras** | PNE 178101 | Ciudades Inteligentes. Infraestructuras. Métricas para las Redes de los Servicios Públicos |
| | PNE 178102 | Ciudades Inteligentes. Infraestructuras. Redes municipales multiservicio |
| | PNE 178103 | Ciudades Inteligentes. Infraestructuras. Convergencia de los Sistemas de Gestión-Control en una Ciudad Inteligente |
| | PNE 178104 | Ciudades Inteligentes. Infraestructuras. Sistemas integrales para una Ciudad Inteligente |
| | PNE 178105 | Ciudades Inteligentes. Infraestructuras. Accesibilidad universal, planeamiento urbano y ordenación del territorio |
| | PNE 178106 | Ciudades Inteligentes. Infraestructuras. Guías de Especificaciones para Edificios Públicos |
| **Indicadores Y Semántica** | PNE 178201 | Ciudades inteligentes. Definición, requisitos e indicadores |
| **Gobierno** | PNE 178301 | Ciudades Inteligentes. Datos Abiertos (Open Data) |
| | PNE 178303 | Ciudades inteligentes. Gestión de activos de la ciudad. Especificaciones |
| **Movilidad** | PNE 178302 | Ciudades inteligentes. Interoperabilidad de puntos de recarga. Requisitos mínimos para considerar interoperable una infraestructura de recarga de vehículos eléctricos |
| **Medio Ambiente** | PNE 178401 | Ciudades inteligentes. Alumbrado público. Tipología de telecontrol según zonificación |
| **Destinos Turísticos** | PNE 178501 | Sistema de gestión de los destinos turísticos inteligentes. Requisitos |
| | PNE 178502 | Indicadores de los destinos turísticos inteligentes |

**Tabla 4 - Normas AENOR [97]**

Entre las normas publicadas, algunas han tenido una mayor recepción de parte de la comunidad internacional y han sido adoptadas por la ITU para su implementación. Estas son la 178104, 178301, 178402, 178305 y la 178502. [97]

## 6.4. Proyectos en el contexto de Ciudades Inteligentes - Casos de Estudio

Teniendo en cuenta las categorías definidos por la ITU [80], a continuación desarrollamos distintos proyectos que involucran múltiples campos de aplicación, pero que tienen en común el uso de las redes de sensores y tecnologías de la información para dar solución a problemas concretos.

Hablaremos de casos particulares que sirven a modo de ejemplo en los siguientes terrenos:

- "*Smart Energy*" en la provincia de Mendoza-Argentina y casos de estudio de monitoreo en consumo en hogares.
- "*Smart Water*" investigaciones de la Universidad de Birmingham – Reino Unido y un caso de desarrollo para medición de canales de riego en Bio-Bio-Chile.
- "Smart Buildings", en el monitoreo del estado de salud de estructuras en el California-USA.
- "*Smart Transportation"*, en Santander-España y Beijing-China.
- "*Smart physical safety and security*", control de incendios en Galicia y Asturias-España control de radiación en Fukushima-Japón, y proyecto para asistencia a cuerpo de bomberos.
- "*Smart health care*", diferentes estudios basados en redes de área personal (Wireless area body networks).

### 6.4.1. Smart Grid "Red Inteligente Ciudad General San Martín, Mendoza"

En la ciudad de San Martín, provincia de Mendoza, se está llevando a cabo un proyecto piloto para el armado de una "Smart Grid". En este tipo de redes eléctricas la distribución y la gestión de la electricidad se actualizan mediante la incorporación de comunicaciones bidireccionales de avanzadas y capacidades de computación ubicua para mejor el control, la eficiencia, la fiabilidad y la seguridad. El objetivo es la implementación de un sistema de gestión que permita la operación, mantenimiento y control más eficiente de las redes existentes de Media y Baja Tensión en un área determinada, sobre la cual, se desarrollará un sistema de Redes Inteligentes con interconexión de generación distribuida fotovoltaica y automatización de la Red de Media Tensión, abarcando una zona con un mínimo de cinco mil (5.000) usuarios. [103]

La red abarca desde el generador central tradicional o basado en nuevas tecnologías de generación, las plantas distribuidoras y el consumidor final, ya sea industrial u hogareño.

Como parte de la solución se destaca:

- El uso de medidores y concentradores inteligentes en el domicilio de los usuarios finales.
- Sistema de comunicaciones entre medidores y concentrador/ concentrador y servidor (red mesh).
- Sistema de gestión proporcionando monitoreo, protección y optimización automáticamente al funcionamiento de los elementos interconectados.
- Integración del nuevo sistema de tele medición al sistema comercial existente.

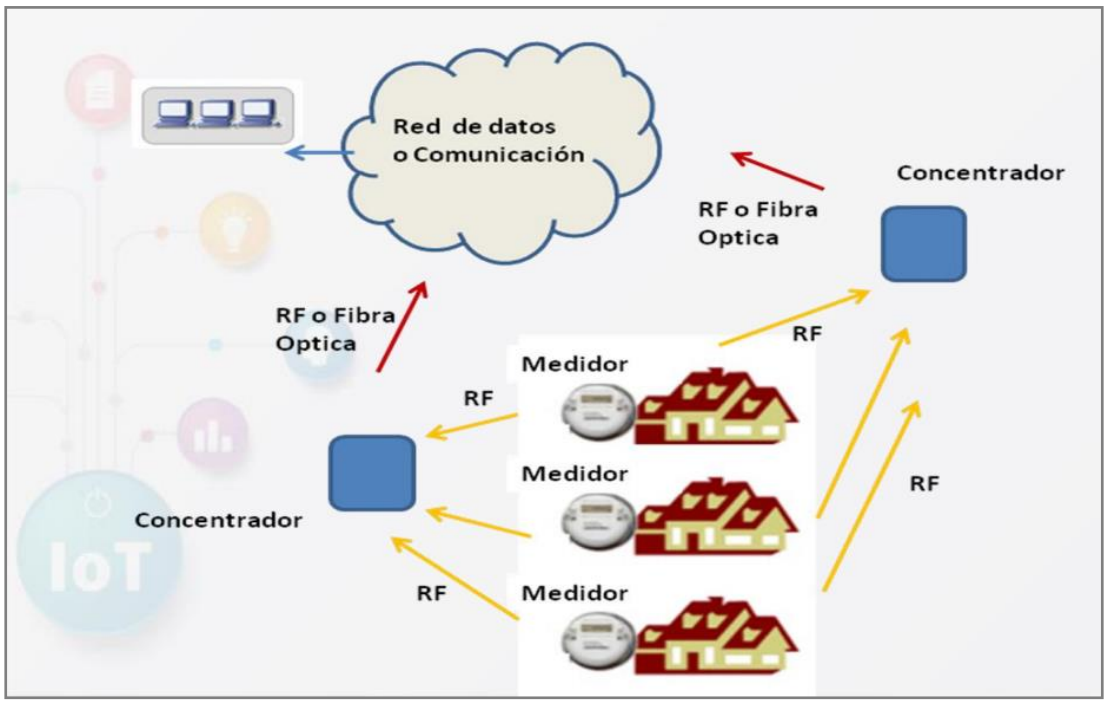



Fig. 29 - Smart Grid [103]

**Sistema de red bidireccional basado en Radiofrecuencia**

Este sistema de red bidireccional, permite la incorporación de un nuevo paradigma basado en el acceso de los usuarios como actores del sistema de provisión de energía eléctrica. Esto es, suponiendo que un usuario tuviera un sobrante de energía, por ejemplo, mediante la utilización de paneles fotovoltaicos.

Entre las ventajas que este sistema brindará podemos destacar

- Utilización de tarifas horarias y tiempos de uso, lo que trae aparejado una reducción en las facturas mensuales. Servicios de consumo prepago.
- Medición de energía activa y reactiva.
- Lectura de energía bidireccional. Impacto de energías renovables en la red.
- Detección de interrupciones y restablecimiento del servicio.

- Mantenimiento preventivo y rápidas reposiciones. Capacidad de desconexión del servicio. Detección de fallos y pérdidas. Reducción de apagones
- Sin lecturas manuales de los medidores. Reducción de costos operativos y de gestión.
- Disminución del hurto de energía, fraude y vandalismo.

Como complemento al caso de estudio mencionado anteriormente, es interesante el trabajo desarrollado en [104] , donde se apunta al sensado del consumo de cada uno de los electrodomésticos que funcionan en un “hogar inteligente”. El método planteado consiste en colocar un sensor para analizar la corriente y voltaje de entrada a la casa. Monitoreando estas variables, se puede analizar cambios en las señales producto del encendido de algún aparato eléctrico. La información es clasificada y se le asigna a cada equipo una “firma de voltaje”. Utilizando un algoritmo para reconocimiento de patrones, se analiza el espectro de la señal y se compara el mismo contra una base ya conocida de firmas, pudiendo obtenerse el detalle del consumo que genera cada aparato en un hogar en tiempo real.

### 6.4.2. Sistema de distribución de agua en áreas urbanas

Siendo el agua uno de los principales recursos dentro de las áreas urbanas, tanto para clientes residenciales, como para edificios públicos o empresas, la distribución debe pensarse de manera eficiente y regulada, y con más controles aun si el suministro es para consumo humano.

Un sistema de distribución consistirá típicamente de una toma o punto de recolección, una planta de tratamiento y/o reservorio, y una red de distribución típicamente construida en cañerías bajo tierra, hasta llegar a la locación del consumidor.

Este sistema de distribución básico tiene claras limitaciones, por ejemplo, al momento de detectar pérdidas en una cañería subterránea. Contar con la posibilidad de sensores distribuidos en todo el sistema, relevando datos de interés, nos permitiría detectar y prevenir pérdidas de agua, medir niveles en reservorios o incluso medir la calidad del agua.

Un modelo de sensado para una arquitectura básica de distribución de agua [105], puede observarse en la siguiente figura:

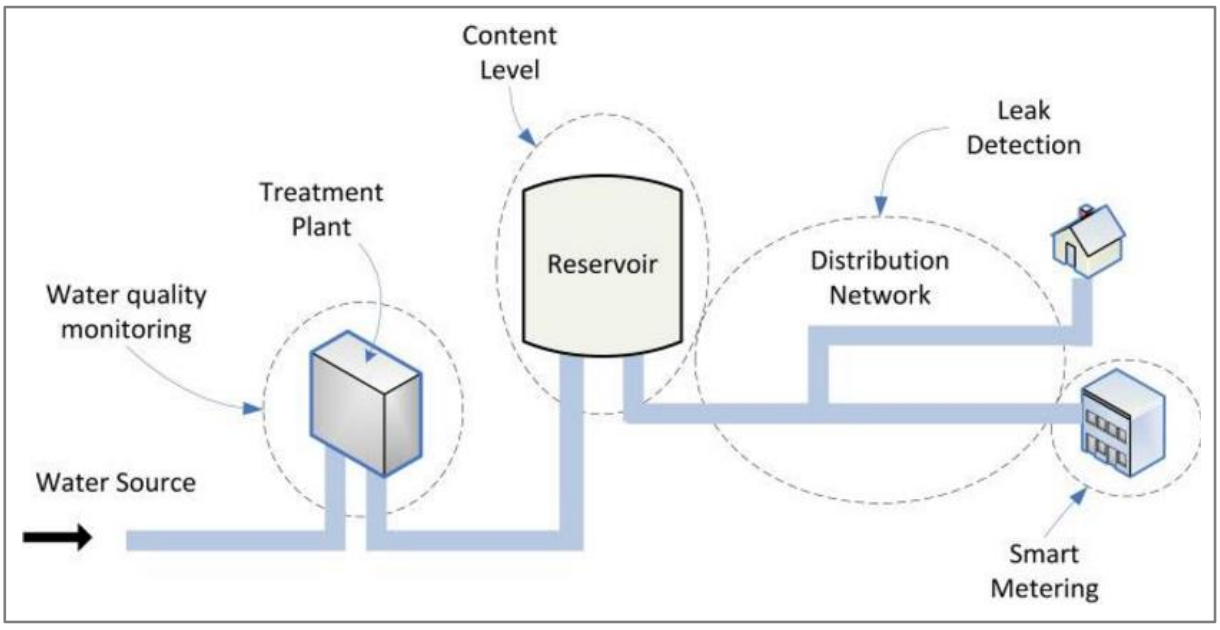



**Fig. 30 - Sistemas de Distribución de agua [105]**

En este caso, para el ingreso de agua se utiliza sensores de presión piezorresistivos (su resistencia eléctrica cambia cuando se los somete a un esfuerzo o estrés mecánico) y sensores para medir el PH del agua en las plantas de tratamiento. En los tanques reservorios plantean el uso de sensores de ultrasonido y presión para medir nivel. Pero quizás lo más interesante se da en el despliegue de acelerómetros y sensores de presión

dentro de las cañerías para detectar potenciales pérdidas de agua y su localización. Esto se realiza analizando las señales recibidas y haciendo uso de la función Wavelet De Haar.

La utilización de sensores para medir temperatura del agua circulante, es otra de las posibles aplicaciones que tendría sentido aplicar en regiones con climas muy fríos, donde la congelación del agua puede generar cortes en el suministro o incluso daños graves en cañerías. Los sensores podrían llegar a advertir de esta situación como para desplegar con anticipación los planes de contingencia adecuados.

Otro trabajo de investigación realizado en la Universidad de Birmingham desarrollado en [106], propone la utilización de sensores de detección de luz (con la utilización de un emisor láser) y acelerómetros para medir otras variables.

El uso de un emisor láser alineado con un sensor óptico (LDR), permite medir una variable de intensidad de luz recibida, la cual es interrumpida por el paso del agua en la tubería. De esta manera se puede inferir el grado de pureza del agua y asociado a esto su calidad. También podría ser usado para detectar posibles roturas en las cañerías (al ingresar tierra u oxido en la cañería, tornando más turbia el agua que circula).

El acelerómetro de dos ejes se utilizó con el mismo propósito que los transductores piezoeléctricos: para detectar daños en la cañería. Los sensores piezoeléctricos generan una señal eléctrica al ser sometidos a una presión mecánica (como podría darse en la deformación de un caño por oxidación o una fuerza aplicada por un agente externo). El acelerómetro nos permite detectar la alineación del caño en torno a un parámetro conocido. Si se lo coloca en las juntas de las cañerías, podría detectarse, por ejemplo, cuando un movimiento de tierra externo (en cañerías enterradas) ocasiona que la junta trabaje y a posteriori, comience a perder agua.

Una alternativa a los métodos anteriormente mencionados propone aplicar un método menos invasivo para la red cañerías, instalando anillos exteriores con sensores de fuerza (FSR), minimizando futuras pérdidas donde se instaló el sensor, reduciendo costos de instalación e incluso facilitando la implementación en tendidos de cañerías ya operativos.

El método basado en el uso de sensores FSR se basa en la medición de cambios en el diámetro de una tubería, generado por la presión interna que genera un líquido o gas circulante. De manera, que un cambió en la presión interna (producto de una potencial pérdida de agua por rotura) podría ser detectado eficientemente. Considerando que se hace un despliegue denso de sensores, posicionados estratégicamente, se podría analizar donde se produce un cambio en las señales capturadas y determinar entre que sensores (y por ende en que tramo del conducto) se halla la posible rotura.

Un esquema gráfico de esta solución puede verse en la siguiente figura:

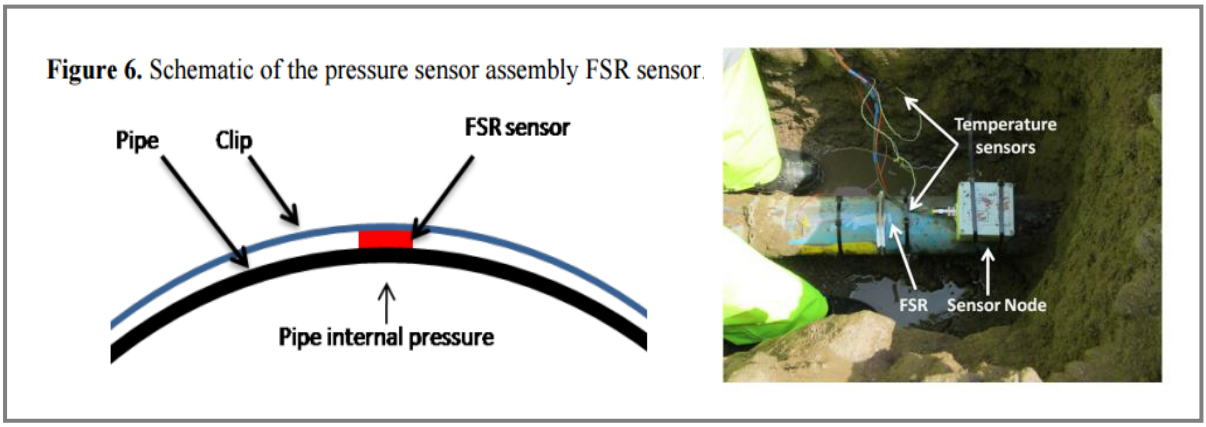



Fig. 31 - Sensor para control de cañerías de agua [107]

Es importante aclarar que la precisión con que se detecte estos cambios estará asociada a factores como el material con el que está construida la tubería, el diámetro y el espesor de la misma, como así también la presión de bombeo con la que se trabaje.

Otro sensor utilizado como complemento en este trabajo, fue el de temperatura. Considerando que una pérdida de agua, por mínima que sea, en el tiempo puede llegar a cambiar la temperatura en torno al suelo que la rodea. De esta manera, rangos de temperatura fuera de lo normal (donde “normal”, estará basado en datos estadísticos que el sistema deberá ir procesando), nos permitiría inferir que se produjo un daño en la tubería.

En la mayoría de los casos mencionados en este trabajo de tesina, una de las principales limitaciones que deberán sobrellevar las redes de sensores inalámbricas será el consumo y la disponibilidad de energía. Si nos enfocamos en particular en el contexto de monitoreo de infraestructura bajo tierra (como una red de tuberías), se deberán tener muy en cuenta no solo cuestiones relacionados al uso eficiente de la energía, sino también cuestiones como la robustez que deberá tener el nodo sensor, el alcance de las radio frecuencias, la posibilidad de montarlo en soluciones existentes y el difícil (prácticamente nulo) acceso para mantenimiento (ya sea por roturas o para mantenimiento de las baterías). Algunos de estos factores son los que se deberán tener en cuenta al momento de diseñar una solución para monitorear este tipo de redes. [107]

### 6.4.3. Soluciones para la Agricultura: Medición de caudales para riego

El estudio se realizó en la red de canales administrados por la "Asociación de Canalistas del Canal Bio-Bío Negrete" (ACCBBN) ubicada en la comuna de Negrete, Provincia de Bio-Bío, VIII Región, Chile.

El objetivo fue la implementación de una red de monitoreo de caudales en una red de distribución de agua de riego utilizando tecnologías de transmisión de datos y estimación in situ de caudales mediante estaciones de aforo. En las redes de distribución del agua con fines de riego, se presentaban tres problemas principales: (1) La distancia a la que se encuentran los puntos de medición y su distribución espacial (2) Las dificultades topográficas y topológicas que presentan la red, y (3) El acceso de múltiples usuarios a la visualización de la información del estatus de la red de canales.

Debido a las distancias que implica una red de este tipo, se ideó una solución basada en 3 tipos de nodos, acorde a las capacidades de procesamiento y comunicaciones necesarias: un **nodo sensor de caudal**, un **nodo base o ruteador** para comunicaciones mayores a 1.5km y un **nodo puente** que actúa como interfaz adaptadora entre las dos redes.

El nodo de medición de caudal o nodo final, se compone de un transmisor ZigBee, un microcontrolador PIC 16F877 a 8MHz, un sensor de distancia ultrasónico y un sensor de temperatura. Se utilizó un transmisor XBee-Pro de DIGI bajo el protocolo ZigBee para la transmisión de datos a distancias menores de 1600 m. Este nodo procesa y envía las lecturas análogas realizadas por el sensor ultrasónico dispuesto para sensar la altura de agua presente en el canal y la correlación con el caudal instantáneo.

La información recolectada es enviada a un nodo puente o ruteador, el cual permite el flujo de datos desde la red ZigBee a una red de largo alcance, para conexión con los nodos base.

El nodo base está compuesto por un transmisor XTend y un microcontrolador para la gestión de la energía, ya que debido a la mayor demanda de potencia fue necesario alimentar los nodos mediante paneles solares. La función asignada a estos nodos es la de servir de interface entre un servidor local y el resto de los nodos de la macrored. Para la transmisión a largo alcance se seleccionó la tecnología FHSS. Este permite lograr comunicaciones a distancias mayores de 1600m, llegando a tener un alcance en línea de visión para ambientes exteriores de 22km y 64km con una antena de alta ganancia. [108]

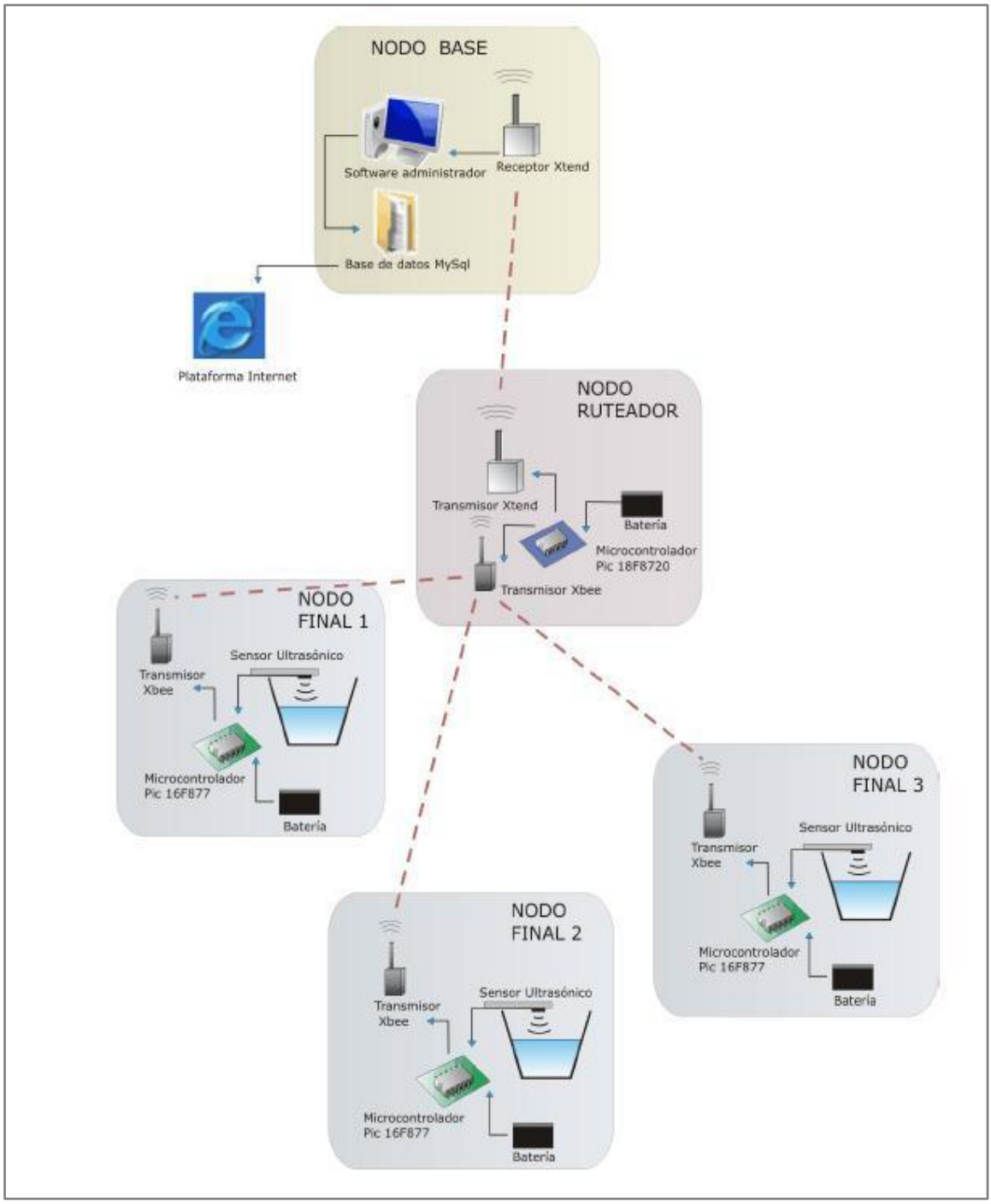



**Fig. 32 - WSN para medición de caudal en canales de riego [108]**

### 6.4.4. Detección de Incendios

La empresa DIMAP-Factorlink junto con a la empresa Libelium ha desarrollado e integrado un sistema de detección de incendios forestales. Este sistema cubre cerca de 210 hectáreas en la región norte de España comprendiendo comunidades de Asturias y Galicia. [109]

El objetivo de este sistema es proveer a diferentes organizaciones de una infraestructura de monitoreo ambiental, la cual tenga la capacidad de gestionar alertas y ofrecer alarmas de alerta temprana.

La solución consta de tres partes principales:

1. La red inalámbrica de sensores.
2. La red de comunicaciones.
3. El centro de recepción.

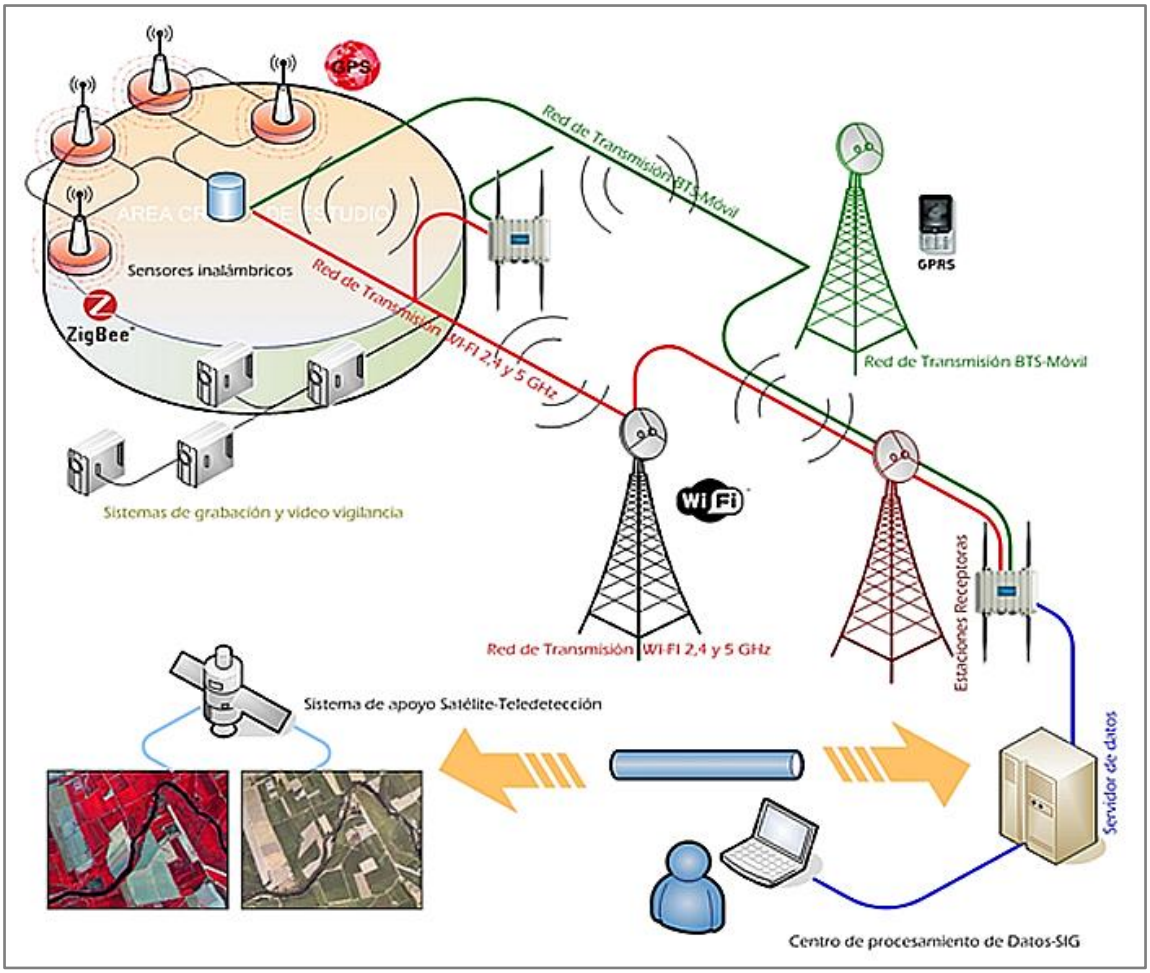



**Fig. 33 - Red para detección de incendios [109]**

Para el sensado se desplegaron 90 nodos, cada uno con sensores para la medición de temperatura, humedad relativa, Monóxido de Carbono y Dióxido de Carbono, dispuestos en ubicaciones estratégicas. Además, cada nodo cuenta con la electrónica necesaria para

poder ampliar los sensores que posee, permitiendo la instalación de sensores de Moléculas de Oxígeno (O2), Metano (CH4), Moléculas de Hidrógeno (H2), Amoníaco (NH3), Isobutano (C4H10), Etanol (CH3CH2OH), Tolueno (C6H5CH3), Sulfuro de Hidrógeno (H2S), Dióxido de Nitrógeno (NO2) y presión atmosférica.

Cada sensor cuenta con una etapa amplificadora, que es configurable en cada sensor de forma independiente, lo que permite una mejor integración de cada nodo. Esta característica nos permite controlar la precisión de cada nodo de acuerdo a la región de interés. Además, es posible controlar la potencia de cada nodo por separado y en tiempo real.

Si algunos de estos parámetros medidos van por encima del umbral configurado, entonces el sistema analiza la información y reacciona enviando una alarma a los bomberos. Ellos sabrán al instante que hay un incendio y dónde se encuentra con exactitud, debido a que cada nodo puede integrar un GPS, que proporciona la posición exacta y la información de marca de tiempo fecha/hora (*timestamp*). Los bomberos podrán saber hacia dónde se está propagando el fuego con información en tiempo real, lo cual es importante a fin de conocer el comportamiento del mismo.

Los nodos tienen tres modos de funcionamiento, en todos los casos de bajo consumo:

- Modo encendido: 9mA
- Modo durmiendo: 62µA
- Modo hibernación: 0,7µA

Los nodos se encuentran durmiendo o hibernando la mayor parte del tiempo para ahorrar batería. Sólo se encienden en intervalos de tiempo definidos por el usuario. Durante el encendido toman los datos con los sensores, realizan la comunicación inalámbrica de los datos obtenidos y vuelven nuevamente a “dormir”. Los nodos fueron, además, instalados con un panel solar. Lo que les permite, gracias a su bajo consumo, un nivel de autonomía suficiente para ser completamente autónomos.

Se utilizaron diferentes modelos de dispositivos XBee (los cuales utilizan el protocolo ZigBee) para las comunicaciones. El alcance de estos modelos varía entre 500m y 6km para la “línea de vista”. En esta implementación buscó un equilibrio entre la exactitud de las lecturas y la fiabilidad de las comunicaciones, estableciendo los nodos con una separación media de 1,5km.

A su vez se instalaron dos dispositivos especiales, los cuales soportan varias tecnologías de comunicación como ZigBee, GRPS y WiFi. Estos dos dispositivos son los encargados de recolectar la información proveniente de los nodos y luego transmitirla directamente al centro de procesamiento, vía WiFi. Este dispositivo también puede alimentarse por paneles solares para funcionar sin problemas en el bosque.

Toda la información recibida en el centro de procesamiento se almacena en una base de datos MySQL. Luego es utilizada por un sistema GIS (*Geographic Information System*) denominado SISVIA, que permite visualizar los datos mediante mapas 2D y 3D.

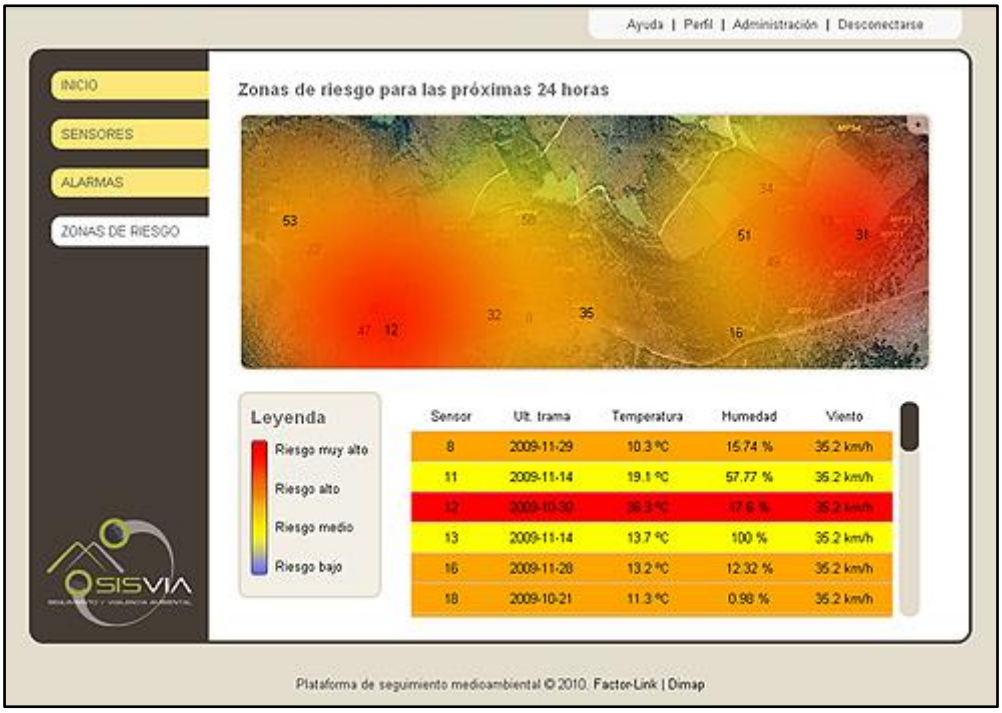



**Fig. 34 - Sistema SISVIA [109]**

### 6.4.5. Monitoreo ambiental para aplicaciones de seguridad nacional

Este campo de aplicación incluye la detección de químicos, sensores inalámbricos biológicos, radiológicos y nucleares (sensores para los productos químicos tóxicos, explosivos y agentes biológicos).

Una aplicación que vale la pena mencionar es el uso de las **WNS para el control de niveles de radiación**. [109]

Después del desastre de Fukushima, sucedido por el terremoto y posterior tsunami en Japón, la empresa Libelium decidió crear un nodo WSN que tome mediciones de radiación en el ambiente.

La idea es simple, cada nodo actúa como un contador Geiger autónomo e inalámbrico. Se mide el número de conteos por minuto detectada por el tubo Geiger y envía este valor utilizando protocolos ZigBee y GPRS para el punto de control. El sistema se alimenta con baterías internas de alta carga lo que garantiza una vida de años.

Estos nodos permiten la detección en tiempo real de niveles peligrosos de radiación, sin limitarse a un perímetro controlado, ya que pueden ser instalados en ambientes exteriores, gracias a su autonomía y comunicación inalámbrica.

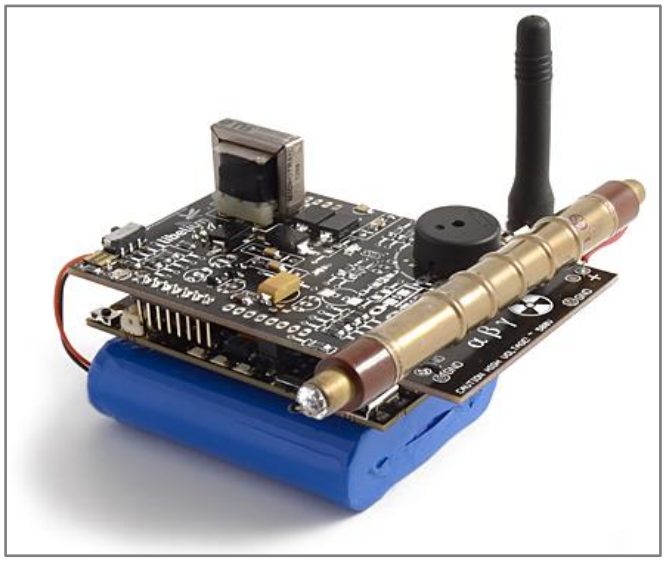


Fig. 35 - Mota Libelium [109]

La red de sensores está formada por docenas de dispositivos sensores desplegados en los alrededores de la planta de energía nuclear y llegando a las ciudades más cercanas. Los nodos sensores se instalan en las luces de la calle y en árboles, tomando energía de la batería interna que, al mismo tiempo se recarga mediante un pequeño panel solar que da vida ilimitada al sistema. Los nodos leen el valor del tubo Geiger durante un intervalo de tiempo específico y calculan el número de cuentas por minuto que se generan por la interacción de las partículas radiactivas. A continuación, este valor se envía utilizando la radio ZigBee a la puerta de enlace de la red que almacena la información en una base de datos en Internet.

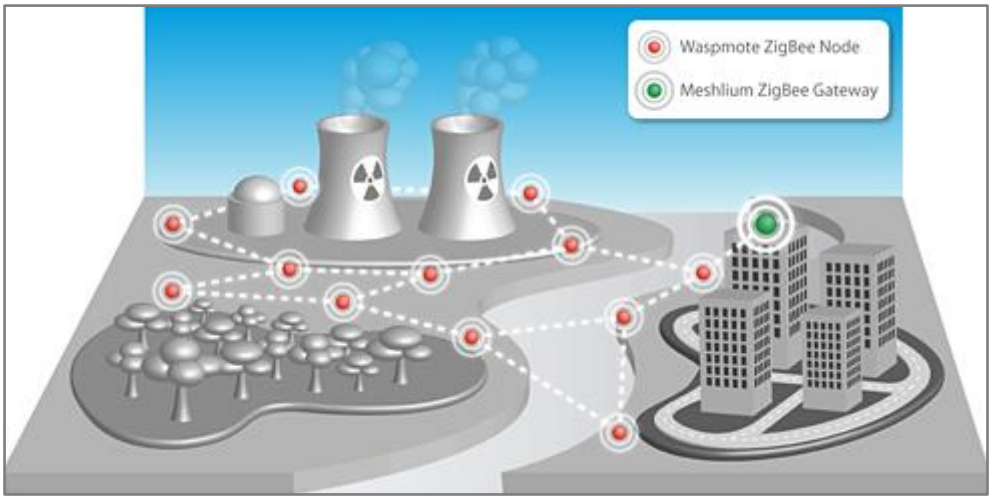



Fig. 36 - Esquemático de una red para detección de niveles de radiación [109]

En el caso de obtenerse medidas de radiación en zonas donde no era esperado hacerlo, se pueden desplegar nuevos sensores, ampliando la red original, en razón de pocas horas.

Cada nodo sensor está compuesto por:

- Unidad central
- Placa de sensado de radiación junto con el tubo Geiger
- Unidad ZigBee
- Unidad GPRS
- Unidad GPS
- Batería recargable de Litio de 6000mA

### 6.4.6. Monitoreo de Salud de Estructuras

En el campo del Monitoreo de Salud de estructuras (*Structural Health Monitoring* - SHM), el objetivo es monitorear los cambios de estado que ocurre en las componentes principales que componen la estructura y que pudieran afectar su performance.

Entre los parámetros más comunes a sensar en el ámbito del SHM están los químicos (pH, oxidación, corrosión), mecánicos (tensión, estrés y deformación) y físicos (temperatura y humedad).

Hay dos variables que entran en juego en el campo del SHM, que son la escala de tiempo en la que se analiza un cambio de estado (factor sensado), y el grado de severidad de dicho cambio.

En base a esto, se desprenden dos diferentes focos de sensado: uno de ellos centrado en detectar la respuesta de la estructura ante una situación excepcional (como podría ser un terremoto, un tornado, una explosión), y otro en un monitoreo continuo para detectar a tiempo cambios en las propiedades o comportamiento de la estructura.

Como particularidad de este campo de aplicación de las WSN, encontramos que el monitoreo de estructuras requiere de una alta frecuencia de muestreo, tamaño de muestras de datos mayores y ciclos de trabajos más exigentes. Centrándose en la fidelidad y volumen de datos, más que en optimizar el consumo de energía de los nodos.

Un ejemplo de este tipo de monitoreo, es el desarrollado para el Puente Golden Gate [110]. En dicho puente se estableció una red de sensores para el monitoreo continuo de su estructura, mediante la medición de las vibraciones en diferentes puntos del mismo.

Cada nodo sensor mide las vibraciones mediante el uso de 3 acelerómetros MEMS y la temperatura ambiente con un sensor destinado a tal fin.

Se estableció una red multisalto con antenas bidireccionales, desplegando una cantidad aproximada de 70 nodos sensores, con una distancia máxima entre nodos de 85 metros, según se observa en la figura a continuación:

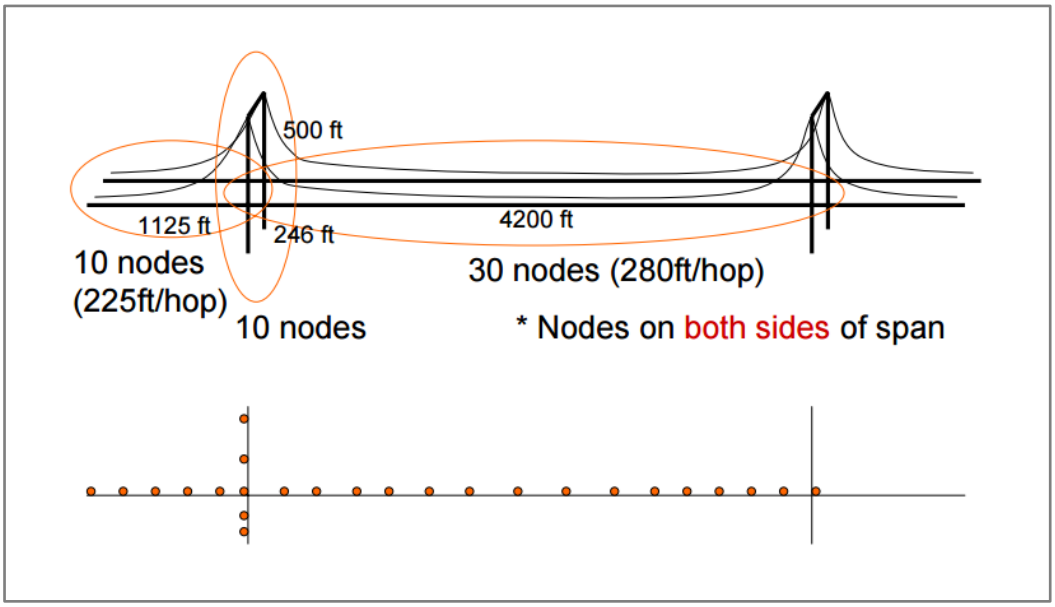



Fig. 37 - WSN en el puente Golden Gate [110]

Para alimentación de los nodos se usaron 3 baterías de litio, que brindaron una vida útil de hasta 23 días de operación.

Entre las ventajas del uso de una WSN para el monitoreo de estructuras en comparación con los métodos de medición tradicionales (cableados), se destaca un menor costo por nodo instalado; menores costos de mantenimiento; al no ser cableado, la instalación es menos invasiva para con la estructura estudiada; los bajos costos permiten una mayor densidad de puntos de sensado.

### 6.4.7. Sistemas de transporte Inteligente

El considerable crecimiento del parque automotor registrado en los últimos 20 años, sobre todo en las grandes ciudades, ha llevado a la necesidad de gestionar políticas y definir acciones concretas para disminuir el impacto del uso del automóvil en la salud de los propios ciudadanos y en pos de mitigar su impacto socio-ambiental.

Con mayor o menor suceso, se han ido poniendo en práctica planes para mejorar la distribución de automóviles en calles y autopistas; la gestión de parcelas de estacionamientos en lugares públicos y privados; la coordinación con sistemas de transporte público; la distribución de carriles por tipo de vehículos; semaforización basada en horarios o flujo vehicular; cabinas de telepeaje, entre otras medidas que se han ido desarrollando para disminuir el impacto del gran flujo vehicular en ciudades importantes.

Algunos proyectos que nos resultaron interesantes mencionar por la utilización que se hizo de redes de sensores inalámbricas, son los de los de las ciudades de Beijín (China) y Santander (España).

#### Control de tránsito en Beijín

En la ciudad de Beijing-China, se ha implementado un sistema para recolección de datos de tráfico automotor, complementando redes basadas en infraestructura con redes de sensores inalámbricas. En este caso se integró redes de sensores basadas en ZigBee con redes preexistentes cableadas basadas en Ethernet y CAN.

En las arterias principales se utilizó la red cableada CAN para transmisiones masivas de datos en tiempo real hacia los nodos concentradores. Para tramos de autopista menos críticos se utilizaron nodos sensores inalámbricos debido a su costo más bajo y una instalación más sencilla.

La arquitectura de la red se compone de dispositivos con distintas jerarquías y funciones específicas [111]. A saber:

- **Nodo de red:** nodos sensores existentes, adaptados para comunicarse con la red de sensores a implementar.
- **Nodo Wireless:** es el nodo principal de la red de sensores. Integra la electrónica del sensor (para medir temperatura, velocidad, sentido y carga de la carretera), junto con las capacidades comunicacionales inalámbricas.
- **Nodo Master:** es un concentrador de nodos de red y nodos Wireless. Tiene tareas asociadas a fusionar y pre procesar información que viene en crudo de los nodos, y

ejecutar tareas de networking como direccionamiento y manejo de topologías, y también asignación de tareas por demanda a los nodos controlados.

- **Nodo de área Central:** es el coordinador de los nodos Master. Realiza tareas de procesamiento de información y actúa como interfaz con las capas de aplicación de un sistema.

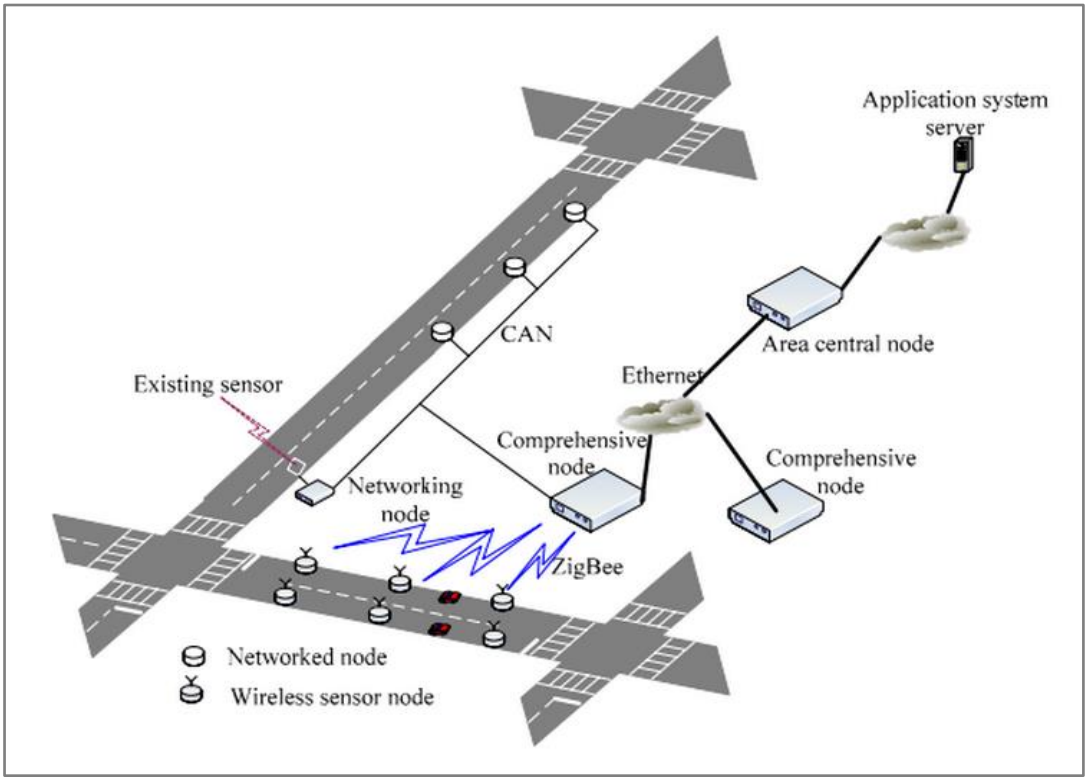



Fig. 38 - Control de tránsito en Beijing [111]

## Proyecto Smart Santander

El proyecto SMART SANTANDER, ha sido desarrollado por varias empresas e instituciones, y tiene como objetivo diseñar, implementar y validar en Santander y su entorno una plataforma compuesta de sensores, actuadores, cámaras y pantallas para ofrecer información útil a los ciudadanos. Una gran cantidad de motas han sido desplegadas para controlar diferentes parámetros como el ruido, la temperatura, la luminosidad, el CO2 y espacios de estacionamiento [109], entre otros.

Además, el proyecto propone el primer centro de investigación del mundo a escala de ciudad, con soporte para los principales servicios brindados por ciudades inteligentes y está orientado al desarrollo de soluciones bajo el paradigma de Internet de las Cosas. El proyecto prevé la instalación de 20.000 sensores en las ciudades de Belgrado, Guildford, Lübeck y Santander (en ésta última, se prevé la instalación de 12.000 sensores).

El objetivo de este despliegue es estimular el desarrollo de aplicaciones de varios tipos por parte de los usuarios, como la investigación avanzada experimental en tecnologías de IoT o pruebas de aceptabilidad de usuarios [112].

La arquitectura de alto nivel ya fue resuelta y consta de componentes existentes y probados. A continuación, puede observarse un diagrama de la misma:

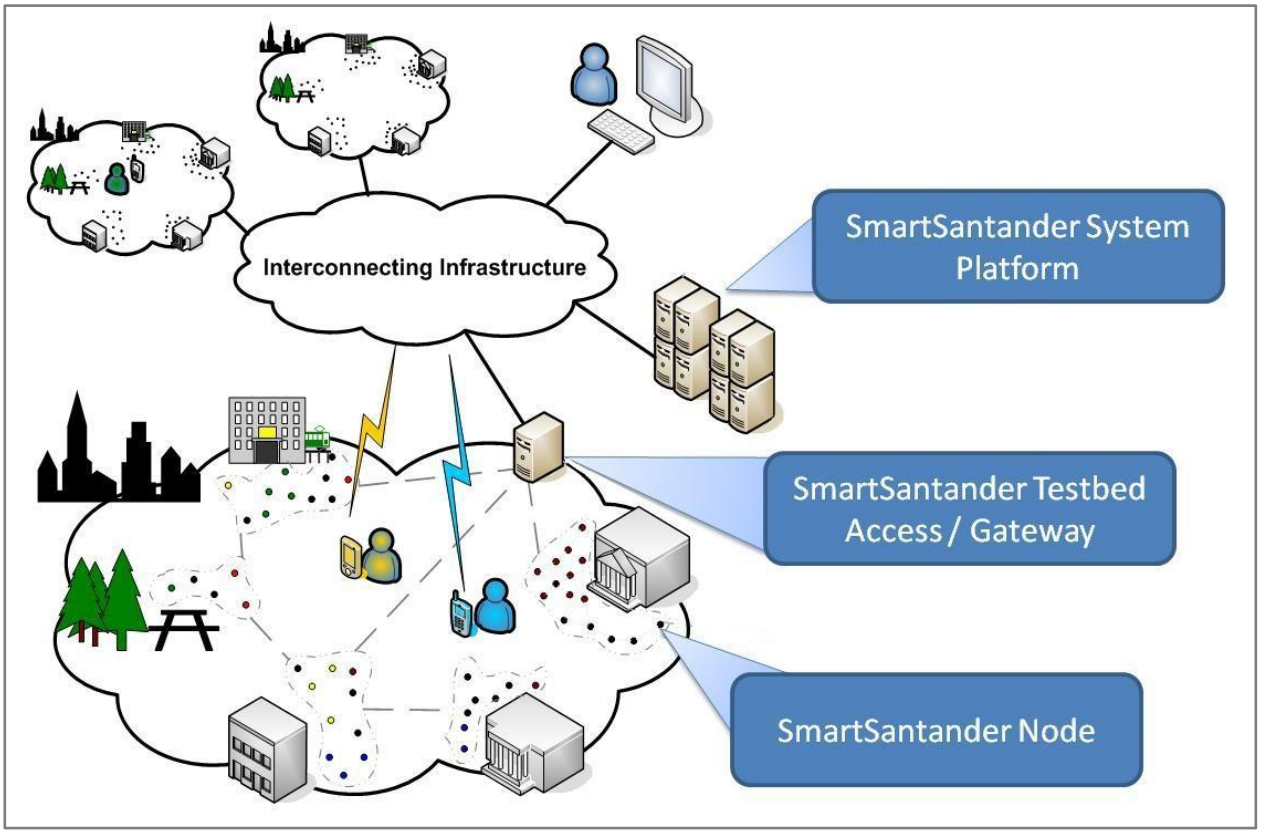



**Fig. 39 - Solución Smart Santander [112]**

En la actualidad ya existen soluciones que se encuentran operativas, las cuales fueron montadas sobre la arquitectura mencionada. Un ejemplo de esto es el proyecto de Smart Parking.

El Smart Parking consiste en una red de sensores inalámbrica que brinda información precisa sobre los lugares de estacionamiento libres, a fin de permitir a los conductores ahorrar tiempo y combustible, a la vez que indirectamente se minimizan las emisiones de CO2 y las posibilidades de atascamiento en el tráfico. El conocimiento puntual de los lugares disponibles para estacionamiento evita que los vehículos circulen en búsqueda de los mismos, siendo que el conductor puede dirigirse directamente al lugar donde estacionará su auto.

Los sensores fueron instalados en el pavimento, de manera que reconocen la llegada o salida de un vehículo del lugar que sensan, para luego transmitir estos eventos a una red dispuesta por la ciudad.

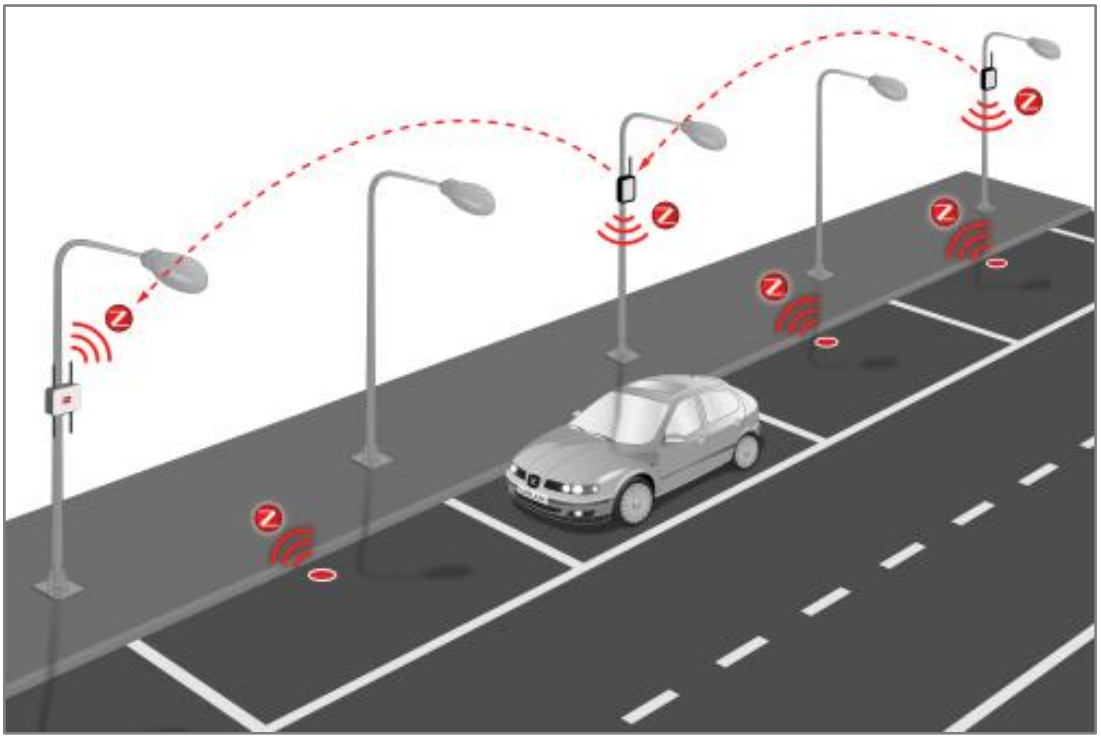


**Fig. 40 - Soluciones para Smart Parking [109]**

Para ello se utilizaron motas con dispositivos ZigBee (XBee Pro) que comunican por radio a sus gateways en frecuencias de 2.4GHz o 868/900MHz, los eventos de llegada o salida de vehículos.

El uso de dispositivos ZigBee de bajo consumo permiten que cada mota pueda estar operativa y libre de mantenimiento durante cinco años, durante los cuales funcionan mediante una batería.

Cada sensor se comunica directamente a su Gateway colocado en los postes de alumbrado público, el cual transmite la información a través de una red mesh.

**Fig. 41 - Nodos sensores en el pavimento para Smart Parking [109]**

Las motas son lo suficientemente robustas como para funcionar enterradas en el pavimento sin sufrir daños. Y el software posee la capacidad de ser actualizado a través de la misma red si se requiriera una actualización en su funcionamiento.

### 6.4.8. Asistencia y Servicios al cuerpo de Bomberos

Distintas investigaciones se han desarrollado en torno a las WSN, para la prevención y temprana detección de incendios, como así también para asistencia al personal de bomberos en su accionar cotidiano.

Entre las soluciones existentes, nos resultó de especial interés una que parte del principio que la red de sensores no se encuentra previamente instalada, sino que son los mismos agentes de bomberos la que la despliegan a lo largo del edificio al llegar.

Para esta solución, se cuenta con nodos estáticos y móviles transportados por los bomberos, y una estación central de procesamiento (implementada en un vehículo apto, en las inmediaciones del edificio).

Al arribar al lugar del siniestro y dependiendo del plano del edificio se despliegan los nodos estáticos (funcionando como enrutadores / repetidores).

Mientras que los nodos móviles son transportados en el mismo traje de protección que utiliza cada oficial de bombero. (Ver imagen debajo). Luego, toda la información es transmitida a la estación central. [113]

**Fig. 42 - Nodo móvil para asistencia a Bomberos [113]**

La placa es una mota desarrollada en la plataforma TelosB (más información en [114])

Todos los nodos cuentan con sensores para medir temperatura, humedad y concentraciones de $CO_2$, $CO$, hidrógeno y otros gases de hidrocarburos.

**Funcionamiento**

Los nodos estáticos recolectan periódicamente las medidas de los sensores y los envían a la estación central utilizando rutas dinámicas multi-salto (mediante la utilización del protocolo para ruteo CTP, *Collection Tree Protocol*).

Pero lo más interesante reside en los valores sensados por el nodo móvil en el traje del oficial de bomberos, ya que permite mantener actualizada las concentraciones de gases tóxicos a los cuales estuvo expuesto (acumulado) y su posición dentro del edificio. De esta manera, se pueden planear rutas de escape en caso de ser necesarios. Para el tema del posicionamiento (poco eficiente con GPS en interiores) se usaron métodos basados en los indicadores de señal recibida (RSSI). De todas formas, esta solución sigue enfrentándose a problemas de reflexión e interferencias con el medio donde se despliegan. Para reducir estos efectos, se propone un método adaptivo donde cada nodo posee un rango RSSI que el nodo estático sabe reconocer y así poder determinar con mayor precisión la ubicación del nodo móvil.

En caso de una emergencia el oficial de bomberos, podrá disparar una solicitud de "guía de escape" en su nodo móvil. Éste comenzará a enviar señales broadcast de "escape", las cuales serán replicadas a través de la red y recibidas por la estación central. La estación central se encuentra todo el tiempo estimando rutas seguras en base a las lecturas de sensores recibidas y transmite aquella que cumpla con las mejores métricas. Como respuesta a estos paquetes de emergencia, se emiten paquetes de respuesta con las rutas óptimas para una salida "segura" del edificio. Los paquetes incluyen un contador incremental, de manera que se puedan descartar rutas obsoletas que han llegado demoradas.

### 6.4.9. Soporte a Sistemas de Salud

Una de los alcances importantes que se dan en el ámbito de las redes de sensores es referido al campo de la salud.

La miniaturización de la electrónica, el avance de la nanotecnología y las comunicaciones inalámbricas de bajo consumo, supondrán en un futuro no muy lejano, un significativo avance en materia de salud. Este avance deberá cubrir una alta demanda de pacientes mayores de 65 años, que según estimaciones demográficas se duplicarán con respecto de los años 90 para el 2025, considerando el aumento promedio de la edad de vida que se viene experimentando.

La IEEE viene trabajando en el desarrollo de redes personales de corto alcance (WBAN´s o *Wireless Body Area Networks*) y publicó en el año 2012 el estándar 802.15.6, el cual define las comunicaciones alrededor o dentro de un cuerpo (no necesariamente humano). Define la utilización de las ya existentes bandas de frecuencia industrial médica (ISM) aprobados por distintos cuerpos de reguladores, el soporte de calidad del servicio (QoS), parámetros de ultra bajo consumo y velocidades de hasta 10Mbps. Esta norma considera los efectos sobre las antenas portátiles debido a la presencia de una persona, como así también los patrones de radiación, para reducir al mínimo la tasa específica de absorción (SAR) en el cuerpo. [115]

Hay diferentes investigaciones para aplicar al campo de la medicina este tipo de redes. Con sensores incorporados (interna o externamente) al cuerpo del paciente se podrían monitorear distintos parámetros vitales como frecuencia del corazón, respiración, presión sanguínea o temperatura del cuerpo. Estos datos podrían ser actualizados constantemente en un servidor central, donde una aplicación dará avisó al médico de turno de mediciones anormales e incluso le brindará gran cantidad de datos estadísticos para toma de decisiones.

Otros trabajos presentan propuestas para casos de emergencia, generando paquetes de información prioritarios para aquellos pacientes más delicados. Este protocolo adaptivo, está basado en el comportamiento de las colonias de hormigas. [116]

### 6.4.10. Singapore - Smart Nation

La república de Singapur puso en marcha su agencia de investigación IDA (*Infocomm Development Authority of Singapore*) [117] para el desarrollo de diversas plataformas de servicios orientadas a convertir a la Nación entera en un “ecosistema digital”, donde se llegue a una conectividad de “todos, todo, en todos lados, todo el tiempo” (E3A), basado en el crecimiento exponencial del Internet de las cosas (IoT) hacia un futuro a corto plazo.

El proyecto no solo apunta a lograr una mejor calidad de vida de sus habitantes, sino también para encarar problemáticas futuras, como ser la alta densidad de población y un envejecimiento de la pirámide poblacional.

El proyecto está apoyado en distintas áreas de interés que el Gobierno ha declarado, como ser:

- Creación de una agencia de investigación especifica.
- Creación de una infraestructura de red de banda ancha (cableada e inalámbrica) para acceso público a lo largo de todo el territorio.
- Promoción a empresas nacionales y extranjeras del sector de IT para inversiones.

- Desarrollo de programas en el Sistema educativo para la promoción de futuros ingenieros altamente capacitados.
- Políticas de gobierno electrónico para un funcionamiento eficiente del Estado.

Considerando la multiplicidad de dispositivos que formaran parte de esta red nacional, se definieron políticas en la redacción de estándares para el desarrollo de aplicaciones y servicios, a través de la ITSC (*Information Technology Standards Committee*)

- TR38 *Technical Reference for sensor network for smart nation* (*public areas*)
- TR40 *Technical Reference for sensor networks for smart nation* (*homes*)

Estos estándares apuntan principalmente a lograr interoperabilidad entre dispositivos IoT y sistemas de diversos fabricantes, reduciendo costos de desarrollo, operación y mantenimiento.

Entre ellos figuran las redes 802.15.4 para redes de sensores de área personal.

Una de las características destacables de esta iniciativa en torno de las redes de sensores, es el desarrollo de un prototipo "*Agregation Gateway Box*", dispositivo que proveerá de alimentación eléctrica y conectividad a un grupo de sensores dentro de un radio determinado. Este equipo permitirá una infraestructura común para las agencias u organizaciones que quieran acceder a los sensores, cambiando así el paradigma de múltiples organizaciones con redes de sensores propias, a una infraestructura de sensores común sobre la cual montar múltiples servicios.

### 6.4.11. Australia-Big Data para Smart Cities

Red Aurin: Australia'surban intelligence network. [118]

Desarrollado por la Universidad de Melbourne, el proyecto contempla generar una infraestructura de datos para investigación, dando acceso a gran cantidad de datos generados desde múltiples fuentes, entre las cuales se encuentran diferentes sensores que aporta los datos obtenidos a una WSN. El portal de Aurin provee cerca de 1300 conjuntos de datos de 30 fuentes diferentes, incluyendo información demográfica, de vivienda, transporte, recursos energéticos y uso del agua. Esta es accesible a través de herramientas para búsqueda y datawarehousing de código abierto.

Sobre esta base de conocimiento, distintos proyectos de investigación, prototipos y simulación se han venido desarrollando para propiciar un crecimiento inteligente y sustentable de las ciudades de Australia. Se pueden destacar proyectos orientados al área de salud, desarrollo de viviendas y al transporte peatonal. Describimos brevemente éste último.

**Proyecto Walkability**: este desarrollo tiene como objetivo definir un escenario de viabilidad peatonal (o “caminabilidad” si derivamos de su traducción del inglés) en un entorno determinado. Para ello se contemplan y procesan variables de distinto tipo y origen, como ser carreteras en áreas adyacentes, densidad residencial, redes de trenes/tranvías, imágenes aéreas para medición de tráfico vehicular, frecuencia y cantidad de paradas de autobuses. Teniendo en cuenta todas estas variables, se propone llegar a un simulador de software basado en agentes “inteligentes” (recomendamos la lectura de bibliografía relacionada a programación de modelos basados en agentes autónomos - ABM) lo más preciso posible, el cual servirá como herramienta para que arquitectos y urbanistas, diseñen diferentes escenarios y analicen su impacto en el comportamiento de este simulador peatonal.

Finalmente, el trasfondo de este trabajo apunta a incentivar el desarrollo de comunidades más saludables (hay sobrada evidencia de las graves consecuencias que conlleva para la salud el sedentarismo) y menos dependiente del uso del automóvil. Se espera entonces, el crecimiento de la densidad poblacional, pero en un ambiente eficientemente conectado por transporte público, y con zonas peatonales amigables que incentiven al ciudadano a su caminata diaria.

Puede accederse a la herramienta de simulación de manera gratuita desde el sitio de AURIN: http://115.146.85.19:9999/agent-walkability/agent-model.html

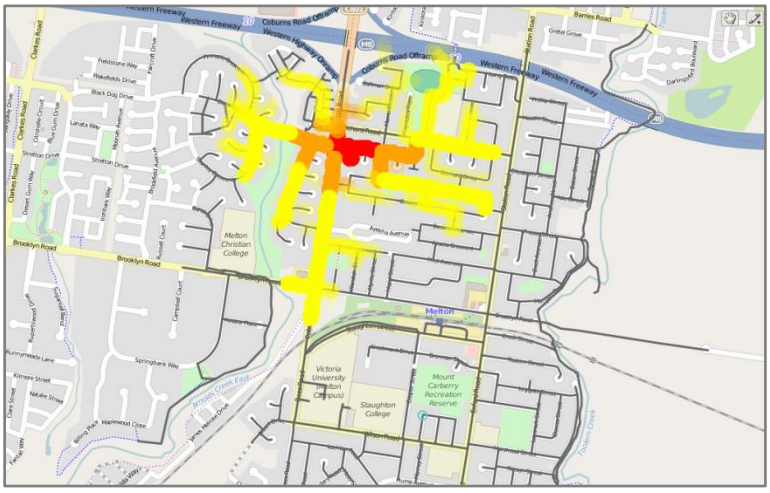



**Fig. 43 - Proyecto Walkability [118]**

### 6.4.12. Songdo – Corea, ciudad piloto para el desarrollo de una Smart City

La ciudad de Songdo (Corea) [119], es un distrito ideado en el año 2001 y que se ha venido desarrollando hasta la actualidad, a fines de crear una ciudad financiero-industrial en las cercanías de la capital Seul. Se desarrolla en un espacio de 600 hectáreas, sobre un terreno ganado al mar, a diferencia de otras ciudades que crecieron como aglomeración de personas o crecimientos periféricos en grandes metrópolis no controlados.

Partiendo entonces desde cero, esta ciudad fue ideando políticas claras en torno a urbanización, optimización de recursos energéticos, transporte, cuidado e inserción en el medioambiente, priorizando el bienestar de sus futuros habitantes y modelando lo que es, en principio, todas las características deseables de una ciudad inteligente:

- Espacios comunes: se definieron grandes pulmones verdes (40% del territorio), para purificación del aire y esparcimiento.
- Transporte: con 25km de bici-sendas y caminos peatonales, líneas de subte y ómnibus públicos, esperan poder cubrir el 90 % de los desplazamientos de la población.
- Se definieron sistemas de recarga para vehículos eléctricos en cada estacionamiento público (todos los estacionamientos serán subterráneos).
- Sistemas para reutilización de agua de lluvia y agua no potable para otros usos (riego, limpieza, canales).
- Se idearon sistemas de cañerías neumáticos para eliminación de residuos, desde los edificios a centros de procesamiento y clasificación de la basura. Eliminando de esta manera los sistemas clásicos de recolección con camiones y potes o bolsas de basura en las calles.
- Se definieron políticas para la utilización de materiales de construcción, cuyos desperdicios sean reciclables en un 75%.
- Los edificios deberán contar con certificaciones de los estándares ASHRAE o similar, para reducir la emisión de CO2.
- Redes de fibra óptica son desplegadas por toda la ciudad para conexionado a redes de alta velocidad de todos los edificios públicos, oficinas, hogares e industria.

Entre las características de redes de sensores implementadas podemos resumir algunas que ya hemos venido mencionando, como ser:

- Monitoreo en edificios del consumo de electricidad y agua.
- Utilización de tecnologías RFID en automóviles para sensado de tráfico vehicular.
- Luminarias en calles con intensidad regulada según la presencia de peatones.

## Conclusión sobre Smart Cities

- El uso de la palabra inteligente en el contexto de este trabajo, deberá quedar en claro que aplica siempre y cuando se haga un uso concreto, fiable, interoperable y seguro de la infraestructura de las TICs.

- Aparece asociado a las Smart Cities, el concepto de "resiliencia". Las ciudades que sean resilientes serán capaces de poder prever y actuar ante situaciones de riesgos previsibles (catástrofes naturales, cambio climático, crisis económicas, entre otras) y llegado el caso que se produzcan estos acontecimientos fortuitos, poder superarlos, regenerarse y adatarse a futuras amenazas, gracias al uso de la tecnología y de la inteligencia de sus ciudadanos.

- Teniendo en cuenta el recorrido que hicimos de los diferentes entes de estandarización, donde se considera a la Ciudad Inteligente y Sostenible como un **Sistema de Sistemas,** será vital que se desarrolle un modelo conceptual en común y una plataforma de trabajo (*framework*) que integre a todos los "verticales" (proveedores de subsistemas específicos), para garantizar la interoperabilidad y sacarle el mejor provecho a la gestión de la ciudad.

- En una ciudad inteligente deberán evitarse los "silos" de información generados por cada uno de los sistemas de información troncales que conforman una ciudad y apuntar a una visión holística. Esto no solo garantizará un uso óptimo de los recursos, sino que además permitirá que se distribuya información vital para todas las áreas de gobierno o civiles involucradas que deban tener acceso a ésta. Un claro ejemplo de esto puede darse con el diseño de protocolos de emergencia para mitigar los efectos que produzcan desastres naturales o accidentes de gran magnitud.

- Algunos países están comenzando a clasificar y dar acceso público a la información masiva generada por las diferentes instituciones de Gobierno, en lo que se denomina el *"Open Data*", un aspecto más que deseable en la transición a una *Smart City*. Datos de áreas de la economía, de medio ambiente, de educación, de salud, de transporte entre otros, son accesibles bajo un formato específico, y con particular cuidado de mantener el anonimato.

Esto no solo permite transparentar la gestión de gobierno y democratizar el acceso a la información, sino también que abre el juego para que diferentes empresas de software y universidades puedan desarrollar infinidad de aplicaciones para múltiples usos en la comunidad. Ejemplo de esto puede verse en la plataforma abierta del

Reino Unido en https://data.gov.uk/, con más de 400 aplicaciones desarrolladas desde su puesta en práctica en el año 2011 [120] o la red AURIN de Australia. [118]

- Deberán considerarse como un aspecto critico a gestionar las cuestiones relativas a la **seguridad de la información**. La multiplicidad de proveedores de dispositivos IoT que subirán datos sensibles a la nube, deberán ajustarse a los estándares y buenas prácticas en materia de seguridad. No solo podrán verse afectadas cuestiones relacionadas a la privacidad de las personas, sino también sistemas claves en el funcionamiento de una ciudad como ser los de distribución de agua potable, control del tránsito vehicular, cámaras de seguridad, tratamiento de residuos, entre otros.

- Tendremos la posibilidad de observar en un futuro a mediano-largo plazo, el desarrollo de estas ciudades inteligentes ya como un ente sistémico, que involucre no solo sistemas informáticos hoy autónomos en su mayoría (como por ejemplo, sistemas de estacionamientos para automóviles, sincronización de semáforos en avenidas, canalización de desagües pluviales, sistemas de alarmas ante desastres naturales, sistemas para clasificación de residuos, sistemas para la optimización de recursos energéticos, etc.), sino también a los ciudadanos que las habitarán.

Los habitantes de la ciudad pasarán a ser no solo destinatarios-beneficiarios de los servicios y facilidades que estas ciudades brinden sino también parte integrante de la solución. Hoy en día, el grado de desarrollo en materia de hardware y aplicaciones para dispositivos móviles es tal, que las mismas pueden formar parte del conjunto sensor-actuador que alimente a un sistema superior. Un ejemplo de esto podemos verlo en los servicios que brinda Google Maps, donde cada usuario de Smartphone está compartiendo información de su ubicación, velocidad y recorrido que realiza, y luego esta información es procesada y devuelta a los usuarios en forma de informe de tránsito en tiempo real, sin necesidad de servicios de información externos o sensores especiales, más que los teléfonos de los propios usuarios.

- Es esperable que en una ciudad inteligente, los estímulos que generen cada uno de sus subsistemas integrantes, cambiarán su propio estado, generando una reacción sistémica, predeterminada y en tiempo real. Por ejemplo, podríamos pensar que un atasco detectado en una determinada autopista de la ciudad, genere una reacción en todo el ruteo del tránsito de la ciudad para lograr un mejor balanceo de carga en las calles, dando aviso a la semaforización de las vías alternativas y al cuerpo de oficiales de tránsito correspondientes, para así lograr superar el imprevisto de la manera más eficiente.

# PARTE 2

# Desarrollo de un prototipo para WSN

# 7. Desarrollo del prototipo

## 7.1. Objetivo

Luego de haber mencionado las tecnologías involucradas en torno a las redes de sensores inalámbricas, sus características, campos de aplicación y casos concretos desarrollados en la actualidad, nos hemos propuesto el desarrollo de un prototipo de WSN con el objetivo de corroborar la viabilidad y el aporte que pueden hacer a las ciudades inteligentes.

Concretamente, se desarrolló un prototipo funcional para dar soporte a un servicio para medición de calidad del aire dentro del casco urbano de la ciudad.

Como se menciona en [79], se seguirá produciendo un crecimiento en la densidad urbana de las grandes ciudades del país. Particularmente en nuestra región se suman además dos focos importantes de generación de contaminantes a la atmosfera: el Polo Petroquímico de Ensenada y el excesivo tránsito vehicular del casco urbano. [121]

El control de la polución está alineado con legislaciones vigentes en diferentes países, en los cuales se establecen parámetros máximos de contaminación. Se evidencia la importancia de controlar las emisiones antropogénicas y su impacto en la mejora de la calidad de vida de la población.

Un modelo de redes de sensores inalámbricas permitiría medir determinados parámetros del aire en diferentes puntos de la ciudad y generar estadísticas que permitan la toma de decisiones y alimentar modelos de simulación (como el analizado en [122]). Tomaremos como referencia la "*Guía de calidad del aire de la OMS relativas al material particulado, el ozono, el dióxido de nitrógeno y el dióxido de azufre".* [123]

Concretamente mediremos material particulado respirable en forma sólida o líquida (polvo, cenizas, hollín, partículas metálicas, cemento y polen, entre otras). A las de diámetro aerodinámico igual o inferior a los 10 μm o 10 micrómetros (1 μm corresponde a la milésima parte de un milímetro) se las denomina PM10 y a la fracción respirable más pequeña, PM2.5. Estas últimas están constituidas por aquellas partículas de diámetro aerodinámico inferior o igual a los 2,5 micrómetros, es decir, son 100 veces más delgadas que un cabello humano.

Las pruebas relativas al material particulado (MP) suspendido en el aire y sus efectos en la salud pública coinciden en efectos adversos para la salud con las exposiciones que experimentan actualmente las poblaciones urbanas. El abanico de los efectos en la salud es amplio, pero se producen en particular en los sistemas respiratorio y cardiovascular. [121]

Los límites establecidos por la OMS para el MP son los siguientes:

**PM 2.5:** 10 µg/m3, media anual 25 µg/m3, media de 24 horas

**PM 10:** 20 µg/m3, media anual 50 µg/m3, media de 24 horas

Tomando como base los efectos conocidos en la salud, se necesitan guías tanto de la exposición breve (24 horas) como de la prolongada (media anual) para los dos indicadores de la contaminación por MP. [123]

## 7.2. Desarrollo

### 7.2.1. Descripción de la red Prototipada

El prototipo de red de sensores planteada tiene como objetivo sensar la calidad del aire midiendo partículas en suspensión PM2.5 y PM10 y condiciones ambientales asociadas a la medición tales como humedad y temperatura. Para ello, se conectaron sensores específicos para este tipo de muestreo y hardware dedicado para las comunicaciones. En base a estas mediciones se propone analizar el desempeño del protocolo **ZigBee** en conjunto con la plataforma de hardware libre **Arduino**, un hardware de radio frecuencia de mediano alcance (**XBee**) y el integrado **ESP8266** para comunicaciones **WiFi**, el cual nos facilitará el acceso a un Cloud service vía el protocolo **MQTT**.

El conjunto de la información sensada será transmitida a una plataforma para IoT en la nube (**Thingsboard.io**), desde donde poder procesar el conjunto de los datos recibidos, monitorear el estado de la red y generar estadísticas, partiendo del almacenamiento histórico de tramas en una base de datos **NoSql Cassandra.**

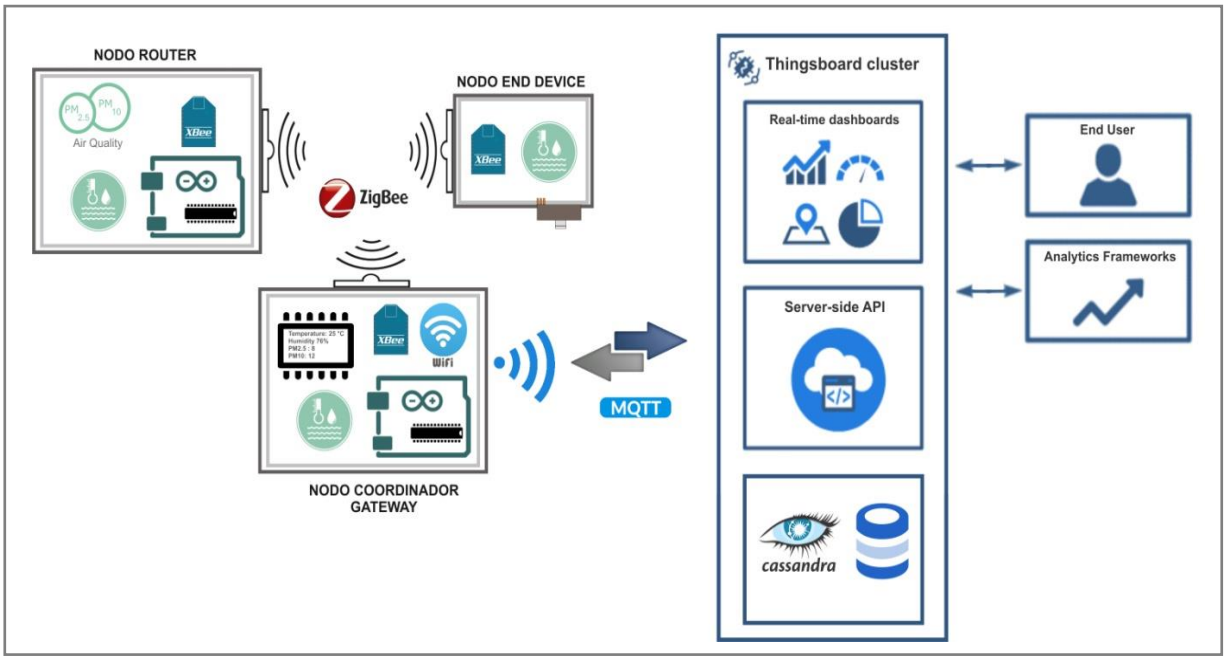



Fig. 44 - Arquitectura del prototipo desarrollado

**Componentes involucradas:**

- Una **mota de sensado simple (End Device)** con capacidad de procesamiento mínimo y una óptima performance para bajo consumo. Conecta un sensor de temperatura TMP36 y un disparador manual de propósito general, para simular la interacción de un agente externo. La información sensada se envía a través de la antena de radio frecuencia XBEE Pro-S2B. En la red Mesh desplegada, actúa en Modo End device (hoja).
- Una **mota de sensado compleja (Router)** con un microcontrolador adicional (Arduino Uno R3, la cual le brinda un mayor poder de procesamiento y capacidad de ruteo, pero eleva su consumo de energía. Conecta un sensor de partículas SDS011 de la empresa Nova fitness y un sensor digital de temperatura y humedad DHT22. Transmite la información sensada a través de la antena de radio frecuencia XBEE modelo Pro-S2B. En la red Mesh desplegada, actúa en Modo Router.

- Una **mota coordinadora**, con un microcontrolador adicional (Arduino Mega 2560), para sensado local de temperatura y humedad (conectando el modelo DHT22), recepción de los datos informados por los otros nodos y envío hacia el Cloud Server Thingsboard.io. Recibe información de la red de sensores, a través de la antena de radio frecuencia XBEE modelo Pro-S2B, actuando en Modo Coordinator. Para la conexión a internet utiliza el integrado ESP8266. La visualización del estado y de los paquetes recibidos se hace a través de un display LCD 20x4 con bus I2C.

Fig. 45 - Prototipo de placas desarrolladas

- Una instancia de **Software de Monitoreo** ejecutándose en un servidor en internet, para procesamiento de la información recibida por los nodos de la red e interfaz con usuarios finales de la aplicación. Se eligió trabajar con la plataforma open-source para IoT **THINGSBOARD.IO**. El acceso a la misma se realiza a través del link:

https://demo.thingsboard.io, ingresando las credenciales correspondientes para visualización de datos:

User: demo@tesis.info

Pass: demo1234

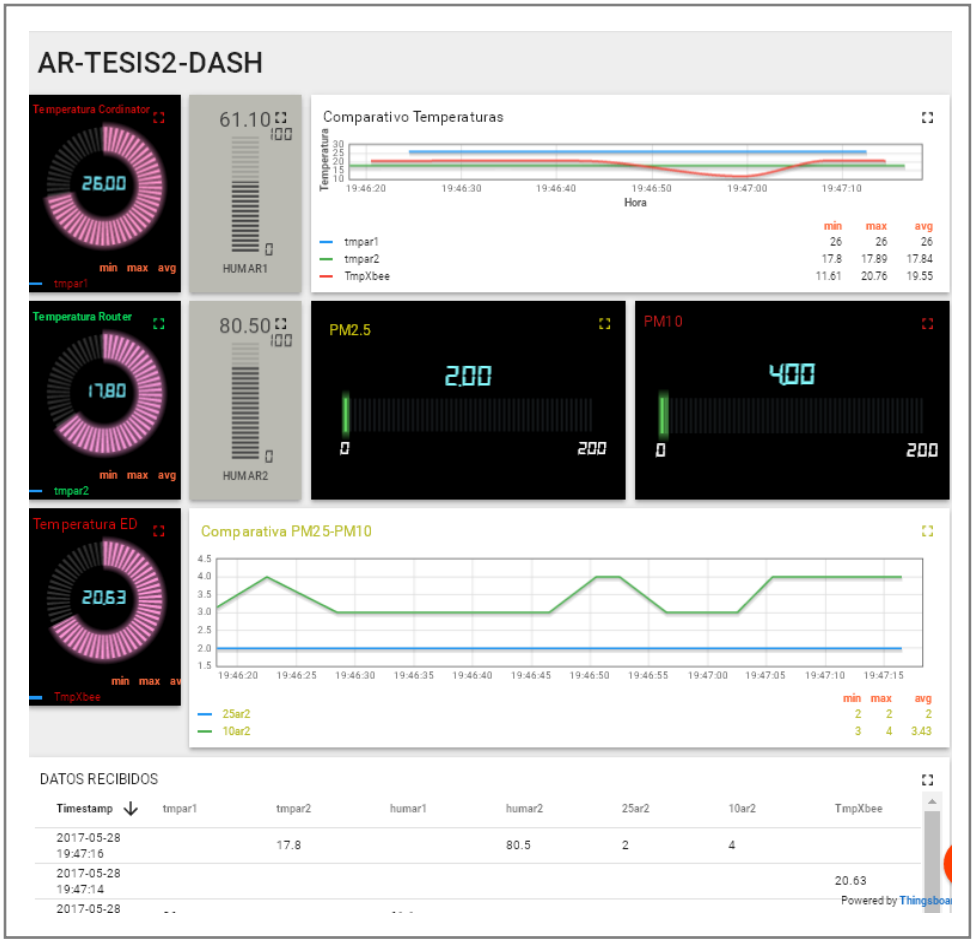



Fig. 46 - Dashboards de la plataforma ThingsBoard

### 7.2.2. Funcionamiento del prototipo

En el prototipo desarrollado, tanto el **nodo Router** como el **nodo End Device**, se encuentran configurados para transmitir a intervalos regulares, y colocándose en un modo reposo (bajo consumo) el resto del tiempo. Dependiendo de la criticidad que necesitamos en la frecuencia de muestreo, tendrá mayor o menor sentido configurar estos intervalos. En muchas ocasiones, el consumo de energía no es un problema real que deba enfrentarse en el proyecto, pero si puede que lo sea la cantidad de datos que podamos procesar o el desgaste de los sensores que utilizamos (por ejemplo, el sensor de partículas utilizado cuenta con una vida útil de 8000hs de funcionamiento según especificaciones del fabricante). Por lo tanto, no solo la autonomía de las baterías sea una variable a tener en cuenta al momento de desarrollar una solución para WSN.

En el **Nodo Router**, el hecho de incorporar un microcontrolador, nos da la ventaja de poder manejar mejor el flujo de información, agregarle procesamiento a la misma (por ejemplo, podríamos promediar los muestreos y enviar cada media hora un solo paquete a la red) y contar con una calidad del servicio superior.

La principal desventaja se da en términos de costos (procesador, memoria, buses, PCBs que debamos agregar o Arduino Uno en nuestro caso), horas de desarrollo de la solución y en consumo de energía. Detallaremos más adelante los consumos estimados que hemos analizado.

La rutina principal itera realizando las siguientes funciones:

- Comunicación con sensor de temperatura y humedad (DHT22), el cual nos envía el valor por una entrada digital del Arduino. A la misma se accede utilizando las librerías propias de sensor.
- Comunicación con sensor de Partículas (SDS011*)*. La misma es un tanto más compleja porque se realiza por UART con un formato de paquetes en serie definido por el fabricante, a saber:

| The number of bytes | Name | Content |
|---|---|---|
| 0 | Message header | AA |
| 1 | Commander No. | C0 |
| 2 | DATA 1 | PM2.5 Low byte |
| 3 | DATA 2 | PM2.5 High byte |
| 4 | DATA 3 | PM10 Low byte |
| 5 | DATA 4 | PM10 High byte |
| 6 | DATA 5 | ID byte 1 |
| 7 | DATA 6 | ID byte 2 |
| 8 | Check-sum | Check-sum |
| 9 | Message tail | AB |

Check-sum: Check-sum=DATA1+DATA2+...+DATA6 。

**Tabla 5 - Especificaciones paquetes sensor SDS011 [124]**

Siendo la fórmula para obtener los valores de (microgramo) **µg/ m3** (metro cúbico):

**PM2.5 (µg /m3) =** ((PM2.5 High byte *256) + PM2.5 low byte)/10

**PM10 (µg /m3) =** ((PM10 high byte*256) + PM10 low byte)/10

- Armado de trama de datos para envío al XBee. El paquete podrá contener como máximo 255 bytes (sin fragmentación, el máximo sería 84 bytes). En nuestro caso, solo utilizaremos 12 bytes, para el envío de la temperatura, humedad. PM2.5 y PM10.
- La función de comunicación a través del módulo XBee, la hacemos por el puerto serie conectándolo por la entrada/salida UART en ambos extremos. Toda la información que se le escriba en el puerto serie, es información que se transmite a la red (dependiendo del direccionamiento previamente configurado, el paquete podrá viajar a otro nodo router o bien viajar directamente al coordinador). Utilizamos la librería de Andrew Rapp <XBee.h> [125], la cual nos brinda suficiente abstracción en el manejo de los paquetes y con pocos comandos logramos una comunicación eficiente con los módulos XBee, tanto para envío como para recepción de información. En todos los casos, el uso de la librería debe hacerse con los XBee funcionando en modo API (ver descripción de los modos en el presente documento).

El **Nodo End Device**, como se comentó anteriormente, es una mota con un procesamiento mínimo, y su principal componente electrónico es la antena de radio frecuencia XBee ProS2B. La antena viene montada en un PCB con entradas/salidas analógicas y digitales, las cuales son gestionadas por el firmware que corren los mismos.

Existen diferentes versiones de firmware dependiendo del modelo del XBee y modo de funcionamiento (end device, router o coordinador), pero en ningún caso es posible programarle rutinas para procesamiento de la información sensada por el modulo. Sobre los módulos solo es posible realizar configuraciones para determinar las entradas y salidas digitales que vamos a utilizar y cómo vamos a utilizarlas (direccionamiento, tipos de entrada, frecuencias de muestreo, modos sleeps, configuraciones básicas de seguridad, etc.).

Para el prototipo desarrollado se conectó como entrada analógica el sensor TMP36 y como entrada digital un sensor de apertura convencional, simplemente para que nos indique un 0 o 1 en la entrada.

Finalmente, el **Nodo Coordinador**, quien incorpora la antena XBee configurada como coordinador de la red y monta un Arduino Mega 2560, ejecutará rutinas de sensado local y principalmente, actuará como Gateway de la red para transmisión de los datos al mundo exterior.

La rutina principal itera realizando las siguientes funciones:

- Conexión y chequeo de estatus de la red WIFI. Se setean las credenciales para conexión al Access Point de la red (en principio se establecen por código fuente dos alternativas, un router WiFi local y una conexión por telefonía móvil como backup en caso de fallo en la primera).
- Conexión con el Servidor MQTT. Utilizamos los métodos de la librería de Nick O'Leary <PubSubClient.h> [126], para la conexión con el servidor de Thingsboard .IO y la posterior publicación de datos.
- Comunicación con sensor de temperatura y humedad (DHT22) local, el cual nos envía el valor por una entrada digital del Arduino. A la misma se accede utilizando las librerías propias de sensor.
- Comunicación con los demás nodos de la red ZigBee. Hacemos uso una vez más de la librería <XBee.h>, para la recepción de información de los demás nodos en la red. En el caso del End Device, la misma antes del envío debe convertirse a escala Celsius, ya que el dato recibido se encuentra expresado en función del voltaje (10 mv por grado).
- Publicación de datos vía WiFi al servidor MQTT. Se arman las tramas (payload) para publicar al bróker MQTT. La librería permite un máximo de 128 bytes, por lo cual nos sobra espacio para la cantidad de datos que estamos transmitiendo por vez.

### 7.2.3. Armando la RED MESH

Una red mesh ZigBee comienza por un coordinador. Una vez que la red ha sido creada, otros nodos pueden ir sucesivamente agregándose. Por defecto los nodos XBee, vienen configurados como tipo router, por ende, debemos elegir uno de ellos y configurarlo como Coordinador.

Para la configuración de los nodos, y considerando que todos ellos van a funcionar en Modo API, debemos usar la herramienta **XCTU**, en nuestro caso la versión 6.2.0.

Lo primero que configuramos será el **Coordinador**. Éste será el responsable de seleccionar un canal para operación (si no lo seteamos, escanea y busca un libre por defecto), un PAN ID para identificación de la red (elegimos el código 2001) y las políticas de seguridad (elegimos no encriptar la información por el momento).

Otros variables a configurar incluyen parametrizaciones del puerto serie, potencia de la antena emisora, canales de entrada /salida (en nuestro prototipo, el sensor de temperatura lo conectamos directo al Arduino).

Una vez que el coordinador levantó la red, permitirá que nuevos dispositivos puedan unirse (hasta un total de 20).

Luego configuramos los nodos como **Router**, al igual que el coordinador, deberán realizar un escaneo activo buscando por redes disponibles para unirse. Una vez incorporado, recibe una dirección de 16 bits aleatoria del dispositivo que permitió su incorporación. A menos que se lo fuerce, un router seguirá participando del mismo canal y red, incluso después de un reinicio eléctrico. Cada router puede permitir la conexión de hasta 20 nodos.

Entre los parámetros a configurar vamos a setear la dirección destino (puede ser la del coordinador, la de otro router o bien la dirección Cero (0x00000000), que apunta directamente al coordinador de la red). Los demás parámetros son dejados en su configuración por defecto (En nuestro prototipo los sensores son conectados a las entradas del Arduino).

Por último, los **End Device**, escanean la red y al igual que los routers reciben una dirección de 16 bits del dispositivo que permitió su incorporación a la red (ya sea de un router o del coordinador de la red). Dado que el End Device puede programarse para que alterne periodos de actividad y de descanso (Sleep times), dependerá del dispositivo que le permitió unirse a la red para que reciba y almacene temporalmente los mensajes hasta tanto el end device despierte de su letargo eléctrico.

En nuestro caso las configuraciones que se hicieron fueron para permitir la lectura de los pines AD0 y AD1, declarando la primera como entrada analógica (sensor de temperatura TMP36) y la segunda como una entrada digital (pulsador). Por último se configuró el modo para ahorro de energía, seteando los parámetros del “Sleep Mode”:

- Sleep Mode= Cyclic Sleep [4]
- ST (sleep time before sleep)= 1388 (5000 ms)
- SP (sleep cycle period)=1F4 (5000ms)

Ejemplo configuración en herramienta XCTU:

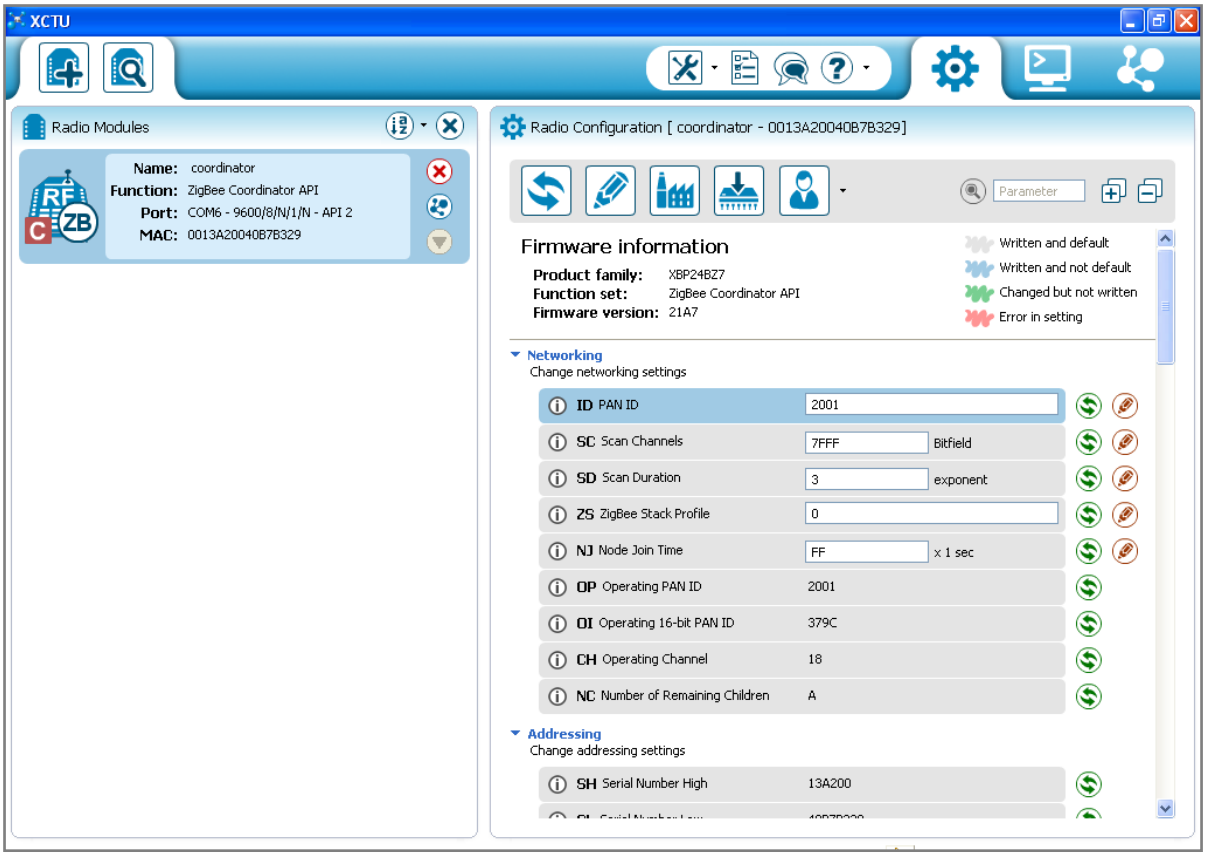



Fig. 47 - Herramienta de configuración XCTU

### 7.2.4. Herramientas y componentes utilizados

**Arduino IDE (versión 1.6.9)**

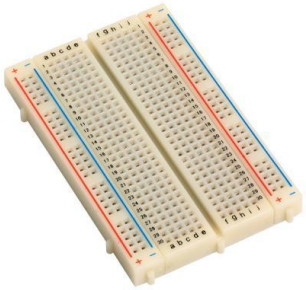
Es el entorno de desarrollo de código abierto utilizado para la programación de las placas Arduino. Esta plataforma posee librerías para interactuar fácilmente con el hardware de la placa y poder enviar/recibir señales de sensores, encender leds, accionar motores, entre otras funcionalidades.

**X-CTU (versión 6.2.0.)**

Es la herramienta oficial provista por el fabricante DIGI para la configuración de los chips de radio frecuencia XBee. Además de permitir la configuración de distintos parámetros de configuración (firmware del dispositivo, modo de funcionamiento, Identificación de Red, dirección destino, pines de E/S digitales y analógicos, modos de ahorro de energía, etc.), el X-CTU tiene herramientas para monitoreo y pruebas de alcance en las comunicaciones.

Se debe tener en cuenta que en modo comando, los radios XBee también podrían ser configurados utilizando una herramienta de comunicaciones serie (como por ejemplo Hyperterminal) sin necesidad de utilizar el X-CTU.

**Hardware utilizado**

| | | |
|---|---|---|
|  |  |  |
| *1.Modulo XBee Pro S2* | *2.Placa Arduino Uno R3* | *3.Adaptador XBee USB explorer* |
|  |  |  |
| *4.Arduino Mega 2560* | *5.Sensor temperatura TMP_36* | *6.Protoboard 300 puntos* |
|  |  |  |
| *7.Fuente alimentación 3.3-5 v.* | *8.Humedad y temperatura DHT22* | *9.Gabinete aluminio* |

| | | |
|---|---|---|
|  |  |  |
| *10.Circuito Adaptador para XBee* | *11.Sensor SDS011* | *12.LCD 20x4 líneas con bus I2C* |

**Tabla 6 - Componentes de Hardware utilizados**

1. ***Módulo XBee Pro S2B (2.4GHz)**:* es un módulo de radio frecuencia desarrollado por la empresa DIGI International para la interconexión y comunicación entre dispositivos, basados en el protocolo de red IEEE 802.15.4. Permiten una comunicación muy simple y confiable entre microcontroladores, computadores, sistemas y cualquier dispositivo con un puerto serial.
    - Soporta conexiones de redes punto a punto, punto a multipunto y peer to peer.
    - La mayoría de estos modelos operan en la frecuencia de 2.4GHz, aunque algunos de mayor alcance lo hacen a 900MHz.
    - Auto ruteo. Soporte para armado de redes mesh.
    - Baja tasa de transferencia: 250kbps.
    - Puertos de E/S digital: 12.
    - Puertos E/S Analógicos: 4.
    - Soporta Modo bajo consumo.

2. ***Placa Arduino Uno r3/ Mega 2560**:* Arduino es una plataforma para desarrollos prototípicos con una placa que soporta un microcontrolador de la marca Atmel y toda la circuitería de soporte, que incluye reguladores de tensión, puerto USB (para alimentación y/o programación del módulo), puertos de entrada/salida digitales y analógicos. Existen en el mercado distintos modelos de Arduino, los cuales se

diferencian en la capacidad de procesamiento, memoria y la cantidad de puertos de comunicación.

El microcontrolador se programa mediante el lenguaje de programación Arduino (basado en Wiring) y el entorno de desarrollo Arduino (basado en Processing). Tiene dos espacios de memoria bien diferenciados: un cargador del programa principal (o bootloader), el cual se ejecuta al inicio e invoca al programa principal cargado en otro espacio de memoria, donde se encuentran las rutinas propias del desarrollo.

Para el prototipo utilizamos los modelos Arduino Uno-R3 y Arduino Mega2560. Los mismos tienen las siguientes características técnicas:

| | **UNO R3** | **MEGA2560** |
|---|---|---|
| Microcontrolador | ATmega328 | ATmega2560 |
| Entradas/Salidas | 14 pines digitales de I/O | 54 pines digitales de Entrada/Salida |
| Puertos analógicos | 6 | 14 |
| Memoria Flash | 32k | 256k |
| Memoria SRAM | 2k | 8k |
| EEPROM | 1k | 4k |
| Clock | 6MHz | 16MHz |

**Tabla 7 - Especificaciones Arduino**

3. **Adaptador XBee-Usb Explorer**: es una placa necesaria para la programación del módulo XBee a través de un puerto USB. Esta programación (configuraciones de los pines de entrada, modo de funcionamiento, direccionamiento) del módulo puede realizarse a través de un emulador de terminal a través de los puertos serie (Hyperterminal, Tera Term , por ejemplo) o utilizando el software “XCTU” provisto por el fabricante DIGI , el cual permite configuraciones avanzadas y en un entorno más “amigable” para el usuario.

4. **Circuito adaptador para XBee:** es una placa para adaptar el módulo XBee al calce milimétrico de las protoboards. Para ello también es necesaria la utilización de pines (headers) metálicos, los cuales deben soldarse al circuito para su conexión.

5. **Sensor Temperatura TMP-36:** es un sensor analógico de bajo voltaje para medición de temperaturas, con un rango de operación entre -40°C y +125°C, y una precisión de +/-2°C. Este sensor cuenta con 3 pines: uno para conexión a tierra (GND), otro para alimentación (2.7 v a 5.5 v) y un tercer pin que genera una salida en voltaje proporcional a la temperatura sensada, tomando como referencia 10 mV/°C

6. **Sensor Temperatura DHT-22:** es un sensor digital de bajo voltaje para medición de temperatura y humedad. Para las temperaturas cuenta con un rango de operación entre -40°C y +80°C, y una precisión de +/-0.5°C. Para la medición de humedad ambiente posee un rango entre 0% y 100%, con una precisión del 2%. Utilizamos para leer los valores medidos, librerías propias del entorno de Arduino para el sensor.

7. **Protoboard:** es un tablero con orificios que se encuentran conectados eléctricamente entre sí de manera interna, habitualmente siguiendo patrones de líneas, en el cual se pueden insertar componentes electrónicos y cables para el armado y prototipado de circuitos electrónicos. A fines del desarrollo de una tesis, es una componente que permite ahorrar mucho tiempo e ir haciendo modificaciones en nuestra arquitectura de mota diseñada.

8. **Fuente alimentación 3.3v:** son los elementos que necesitamos para proveer de alimentación a los módulos XBee.

9. **Gabinete de aluminio:** se diseñó artesanalmente y para fines demostrativos un gabinete en aluminio y acrílico, que permitió montar el hardware para cada una de las motas sensoras. Si se piensa en el uso de una mota sensora en condiciones ambientales más severas (como ser ambientes exteriores, húmedos, con temperaturas extremas), deberemos considerar el uso de cajas con una mejor aislación. Para ello, vale la pena analizar las normas IEC 60529, en particular, las consideraciones en torno a la protección contra ingreso de polvo y líquidos, dependiendo del tipo de aplicación que se pretenda.

10. **LCD 20x4 líneas con bus I2C:** pantalla retroiluminada para mostrar hasta 4 líneas de 20 caracteres como máximo cada una. Posee interfaz I2C, la cual nos facilita el

cableado, utilizando solo 4 pines (con la interfaz paralela deberíamos usar 11 pines). I2C es un protocolo en bus que permite conectar varios dispositivos sobre un bus físico, asignándoles una dirección a cada componente.

11. **Sensor Partículas PM2.5 y PM10 (SDS011):** sensor para medir partículas en suspensión desarrollado por la empresa NovaFitness. Puede detectar partículas de un tamaño mínimo de 0.3 microns (milésima parte de un milímetro). El mismo devuelve la cantidad de partículas en una escala de (microgramo) µg/ m3 (metro cúbico), siendo su escala de 0 a 999 ug/m3, tanto para la escala de partículas menores de 2.5 y menores de 10 microns. Tiene un margen de error máximo del 15%.

    El principio de funcionamiento se basa en dispersión de láser: cuando pasan por el área de detección las partículas, la luz es dispersada y se transforma en señales eléctricas. Luego estas señales se amplifican y procesan, pudiendo determinar el número y el diámetro de las partículas.

## 7.3. Pruebas en campo del prototipo

Realizamos diferentes ensayos en exteriores, para determinar un estimado de alcance de las motas sensoras con las antenas **XBee Pro S2B**, tanto en un entorno rural despejado como un entorno urbano con más interferencias.

Estas medidas son solo a modo ilustrativo, ya que no fueron realizadas con herramientas de precisión (se usó la herramienta Google Earth para medir distancias entre puntos y un software contador de paquetes en el Nodo Coordinador para calcular la tasa de paquetes perdidos), pero de todas maneras nos pueden llegar a servir de referencia para trabajos futuros.

Debe considerar además, que en todos los casos, se probaron los nodos a la altura de una persona y no montados sobre una estructura más acorde.

Inicialmente se intentó determinar la distancia máxima en que pueden llegar a alejarse los nodos. Para ello se procedió en ir alejando el Nodo End Device del Nodo Coordinador y analizar a qué distancia máxima llega la comunicación en un modo estable sin pérdida de paquetes o con una mínima pérdida.

**Observamos que cuando se llega al límite de la distancia máxima comienzan a perderse paquetes, hasta un punto donde el Nodo End Device pierde la conexión con su coordinador.**

El otro análisis que pretendíamos realizar es para comprobar la capacidad de conexión que tienen los nodos desde diferentes distancias. Por ejemplo en el caso de que los nodos se apagarán repentinamente, verificar que capacidad tienen para volver a comunicarse entre ellos y hasta que distancia son capaces de conseguirlo.

**Observamos que en situaciones donde la comunicación ya se tornaba inestable, la capacidad de reentablar una comunicación es casi nula. Debe retrocederse y reducir las distancias entre los nodos, para lograr que el End Device se emparente nuevamente con el coordinador para trasmitir los datos sensados.**

Detalle de las pruebas realizadas:

**a) Exteriores sin obstáculos: Visión directa**

Prueba de transmisión punto a punto, entre nodo Coordinador y Nodo End Device. En acceso a la localidad de O´Higgins, provincia de Buenos Aires. Alcance estimado: 900m


Fig. 48 - Prueba de Alcance en campo abierto

**b) Exteriores sin obstáculos: Visión directa con tránsito vehicular**

Prueba de transmisión punto a punto, entre nodo Coordinador y Nodo End Device. En avenida 52 Paseo del Bosque, de la ciudad de La Plata. Alcance estimado: 700m.


Fig. 49 - Prueba de alcance en avenida de ciudad de La Plata

**c) Exteriores con obstáculos : Visión directa con obstáculos**

Prueba de transmisión punto a punto, entre nodo Coordinador y Nodo End Device. En barrio Parque Saavedra, de la ciudad de La Plata. Alcance estimado: 200m.


Fig. 50 - Prueba de alcance en ciudad de La Plata con obstáculos

**d) Exteriores con obstáculos: Sin Visión directa.**

Prueba de transmisión punto a punto, entre nodo Coordinador y Nodo End Device. En barrio centro de la ciudad de La Plata. Alcance estimado: 130m.


Fig. 51 - Prueba de alcance en ciudad de La Plata sin visión directa

Algunas **conclusiones** de las pruebas en campo:

- Independientemente del entorno en que se instalen los nodos sensores (y que nos determinará el alcance máximo real que podemos tener entre dos nodos de nuestra red), sería recomendable tener en cuenta para el diseño de la red, que las distancias máximas entre dos nodos, se determinen teniendo en cuenta una situación estable con la menor perdida de paquetes posibles como para garantizar una buena reconexión entre dos pares de nodos, en caso de que uno de ellos se "apague" momentáneamente.
- La tasa de paquetes recibidos por el nodo disminuye al aumentar la distancia entre dispositivos (lo cual es lógico considerando que se usa una potencia de transmisión fija), pero los ensayos realizados **presentan una desviación respecto a las indicaciones dadas por el fabricante**, que hablan de hasta 1.5km de distancia entre dos nodos XBeePro S2B [65]. Queda para futuros trabajos probar estos mismos componentes, con antenas que le otorguen una mayor ganancia y una esperable mejoría en el alcance entre dos nodos.
- Pensando en una de Red tipo MESH, se observó que el ruteo **se adapta rápidamente a los cambios en la red desplegada**. Si bien no se disponía de una gran cantidad de nodos para probar, se contaba con la cantidad mínima de nodos para armar una red mesh ZigBee (con un nodo Coordinador, un Router y un End Device) se probaron casos de desconexión para ver que el nodo End Device, detecte la desconexión y busque un nuevo router/coordinador hacia donde encaminar los paquetes.

**Análisis Consumos de Energía en las Motas Sensoras**

Como parte de la investigación, nos resultó de interés analizar el consumo de cada uno de las motas desarrolladas a fin de contar con un estimativo de energía promedio consumida por cada una de ellas.

Teniendo en cuenta las hojas técnicas de cada uno de los componentes involucrados, se pueden estimar los siguientes consumos:

| End Device | mAh |
|---|---|
| Al encender y conectar(picos) | 55 |
| Transmitiendo | 25 |
| **Total** | **40** |

| Coordinador | mAh |
|---|---|
| LCD | 38 |
| RF - XBee | 46 |
| WiFi - Esp8266 | 130 |
| Arduino Mega | 90 |
| **TOTAL** | **304** |

| Router | mAh |
|---|---|
| Sensor SDS011 | 60 |
| RF - XBee | 40 |
| Arduino Uno | 46 |
| **TOTAL** | **146** |

Se desglosó independientemente cada una de las componentes, como para tener una mejor aproximación. Se tuvieron en cuenta distintas configuraciones a nivel hardware y software, que influyen notoriamente en el consumo de energía, como lo son:

- La des/conexión de componentes externos para visualización (LCD, Leds), que no cumplen un papel funcional de la solución, sino más bien que se utilizan para fines de debug.

- Modos Sleep: como mencionamos a lo largo del documento, una de las grandes bondades de las redes de sensores, es su capacidad para configurarse en modos de bajo consumo. En particular para las redes ZigBee que utilizamos esto puede realizarse **solo** en los nodos configurados como End Devices (ya que los nodos routers y coordinador deben mantenerse levantados para el ruteo y almacenamiento temporal de mensajes hacia y desde los End Devices).

- Conociendo el consumo de los radios en funcionamiento continuo (transmitiendo y/o recibiendo), podemos armar ciclos de trabajo variados dependiendo de las necesidades del campo de trabajo a analizar. Disminuir la frecuencia de muestreo y colocar al End Device en modo reposo, nos permitiría prolongar la vida útil de la batería.

- En caso de armarse una red MESH donde participen Nodos Router como encaminadores entre los End Device y el coordinador de la red, deberá tenerse en cuenta que tanto el Router como el Coordinador son nodos que consumen más energía, sobre todo teniendo en cuenta que no pueden configurarse con modos Sleep. Además si el Coordinador actúa como Gateway de la red, tendrá considerablemente más gastos de procesamiento y comunicaciones (en nuestro prototipo además de “hablar” ZigBee con la red de sensores, sube datos a la nube vía WiFi).
  Por todo esto, al momento de armar una solución para Ciudades Inteligentes basadas en WSN, deberemos considerar como una de las prioridades el tema del suministro energético que deberán tener estos nodos.

## 7.4. Radios XBee

Los radios XBee pueden configurarse para funcionar en dos modos:

- Application Transparent ("modo transparente") - AT
- Application Programming Interface ("modo API") - API

Debido al pequeño microcontrolador con que cuentan los radios XBee Serie 2, no existe espacio suficiente para almacenar las instrucciones para ambos modos (AT Comando y API). De modo que el firmware que le instalemos será diferente, ya sea para soportar modo AT o modo API [127].

Nota: Particularmente en nuestro prototipo implementado, usamos el modo API.

**Modo de Operación Transparente - AT**

Se denomina modo transparente porque el radio pasa la información inalámbricamente tal cual como la recibió por su/s puertos de entrada seriales. Cuando se opera de este modo, un módulo XBee estaría actuando como si fuera una línea serie punto a punto, haciendo de cuenta como si se conectaran dos dispositivos por un cable.

Si bien es sencillo para lograr comunicaciones entre pocos nodos, presenta varias limitaciones para armar una red de sensores amplia, como ser:

- No permite leer o setear configuraciones a dispositivos remotos de la red.
- Para la comunicación entre varios nodos, primero debe configurarse la dirección destino y luego transmitir.
- No es posible identificar el origen de los paquetes, ya que los mismos viajan sin indicar la dirección origen.
- La información recibida no incluye detalles de la transmisión, no pudiendo indicar éxito o falla en la misma.

Dentro del modo AT, se pueden diferenciar dos estados diferentes: *modo comando*, cuando le estamos enviando comandos por consola para configuración, y *modo transparente,* cuando el radio ya configurado, envía inalámbricamente lo recibido por un pin hacia otro radio que espera recibir la información.

Para acceder a las configuraciones, el modo AT permite un modo comando a través del puerto serie. Se ingresa al mismo enviado una secuencia predeterminada (caracteres +++), y luego el comando con el parámetro de configuración. En la siguiente tabla se muestran los comandos más usados en la configuración de un radio:

| Comando | Acción |
|---|---|
| **+++** | Ingresar al modo comando |
| **ATID xpid** | Retorna el PAN ID de la red configurada o bien setea el parámetro que le enviemos como el nuevo PAN ID (xpid en este ejemplo) |
| **ATSH/ATSL** | Retorna la dirección única que tiene el radio de fábrica (# de serie) |
| **ATDH/ATDL** | Retorna la dirección destino que tiene configurado el radio |
| **ATWR** | Escribe al firmware la configuración que le hayamos |

| Comando | Acción |
|---|---|
| | hecho anteriormente. |
| **ATD0…ATD7 / ATP0…ATP1** | Permite configurar los pins de E/S del XBee. Enviando distintas opciones puede deshabilitarse ( valor 0), configurar como entrada analógica (valor 2), entrada digital (valor 3), salida digital (valores 4 y 5) |
| **ATRE** | Resetear a valores de fábrica todas las configuraciones. |

**Tabla 8 - Modo AT por comandos XBee**

Por defecto, el módulo XBee arranca funcionando en *modo transparente*. Si recibe la secuencia para ingresar al *modo comando* (+++), entonces detiene las comunicaciones y cambia al *modo comando*, escuchando las instrucciones que reciba. Si luego de 10 segundos no recibe ningún parámetro, entonces retorna automáticamente al *modo transparente.*

**Modo de Operación API**

En el modo de operación API, un protocolo determina como es intercambiada la información. La misma se estructura en paquetes organizados (API frames) en un determinado orden. De esta manera, se permite comunicaciones más complejas sin necesidad de programar un protocolo propio. Por lo tanto, toda la información entrante o saliente del XBee, contendrá frames con información extra como por ejemplo la dirección destino, calidad de la señal, cantidad de saltos, etc.

Esto nos permite:

- Leer o configurar dispositivos remotamente.
- Transmitir datos uno a uno o a múltiples destinos fácilmente.
- Gestionar códigos de error o confirmación de éxito en las comunicaciones realizadas.
- Ejecutar herramientas de diagnóstico y actualizaciones de firmware de los módulos "*over the air*".

En el modo API, la estructura de comunicación (frame) está compuesta por una serie de bytes que indican los distintos tipos de paquetes que transmite:

| **Delimitador** | **Longitud** | | **Datos** | **Checksum** |
|---|---|---|---|---|
| *Byte 1* | *Byte 2* | *Byte 3* | *Byte 4.. Byte n* | *Byte n +1* |
| *0x7E* | MSB | LSB | Estructura API (*) | Single Byte |

(*)Existen distintos tipos de API frames

| Tipo de Frame | Descripción |
|---|---|
| 0x08 | AT command (immediate) |
| 0x17 | Remote Command Request |
| 0x8A | Modem Status |
| 0x09 | AT command (queued) |
| 0x88 | AT command response |
| 0x10 | TX request |
| 0x8B | TX response |
| 0x90 | RX received |
| 0x92 | RX I/O data received |
| 0x95 | Node Identification Indicator |
| 0x97 | Remote Command Response |

**Tabla 9 - Modo API XBee**

## 7.5. ThingsBoard.IO

Es una plataforma opensource para el desarrollo ágil de proyectos sobre IOT lanzada al mercado en el año 2016. Nos permite fácilmente:

- Gestionar alta de sensores y atributos de los mismos.
- Recolectar y visualizar gráficamente en tiempo real los datos recolectados.
- Procesar la información y disparar acciones programadas.
- Conectar con otros sistemas externos.
- Brinda extensiones (plugins) ya desarrolladas para aplicación en casos concretos.

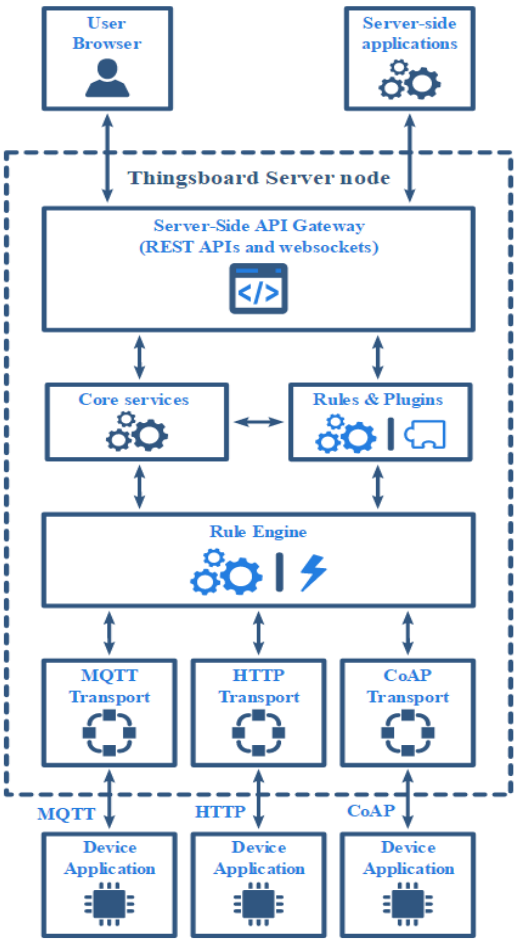
Thingsboard está diseñado para balancear la carga de trabajo entre múltiples nodos, los cuales funcionalmente serán idénticos y podrán gestionar tanto aplicaciones desde el lado del dispositivo (Device API) como del lado del servidor (server-side API). [128]

Para conexión del lado del dispositivo, la *device API* soporta los protocolos :

- **MQTT**
- **CoAP**
- **HTTP**

Del lado del servidor , se cuenta con el núcleo API REST y un conjunto de APIs específicos que son proporcionados por varios plugins:

- **Administration REST API**
- **Attributes query API**
- **Timeseries query API**
- **RPC API**




Thingsboard se presenta como una plataforma robusta, escalable y tolerante a fallas, basando su arquitectura en un cluster de nodos. Utiliza Apache Zookeeper [129] para sincronización de servicios entre nodos y adopta técnicas de Hashing consistente [130] para distribución de carga entre los nodos desplegados.

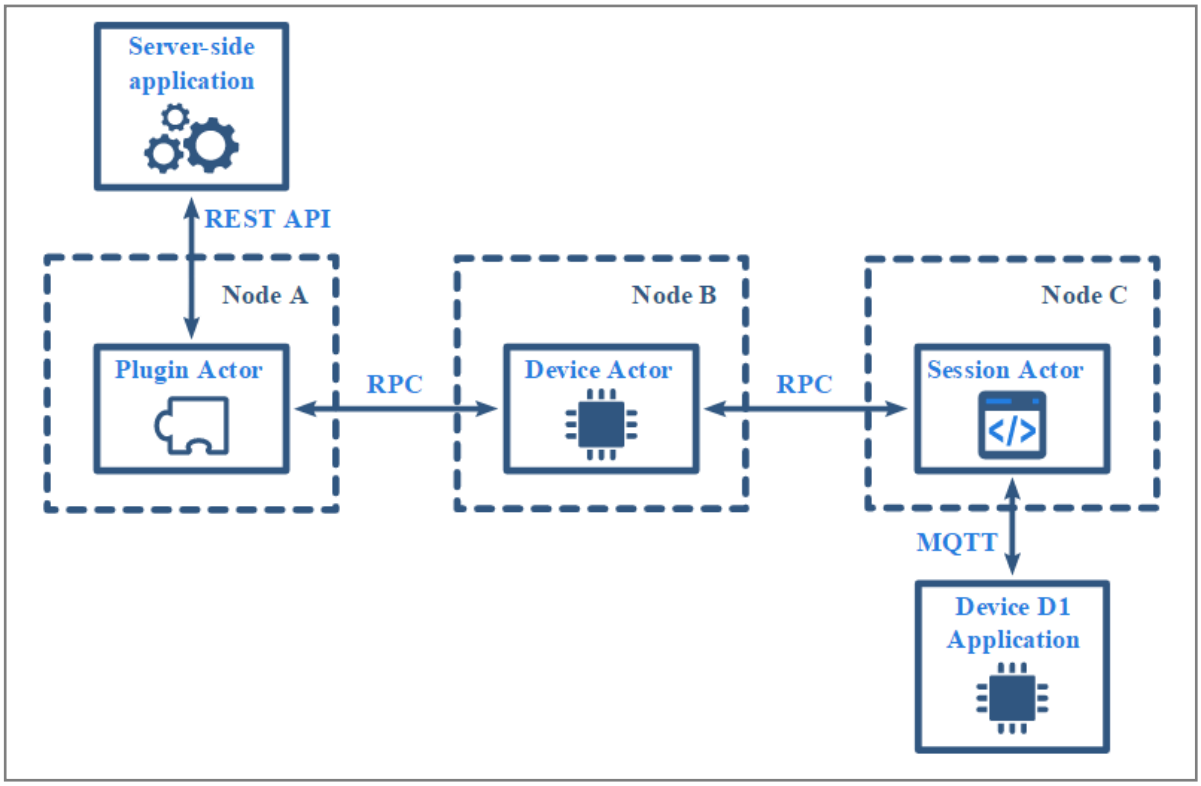



Fig. 52 - Cluster de Nodos ThingsBoard

En lo relativo a prácticas de **Seguridad,** puede configurarse Thingsboard para funcionar con *SSL* sobre HTTP(s) y MQTT.

A nivel autenticación de dispositivos, actualmente soporta el uso de credenciales basadas en *Tokens* para todos los protocolos y también soporta el uso de *certificados X.509* para MQTT.

Herramientas de terceros utilizadas en el proyecto:

- **AKKA**: plataforma de desarrollo para aplicaciones distribuidas altamente concurrentes, basado en el paradigma de "Modelos basado en Actores". (http://akka.io/)
- **Zookeeper:** para sincronización de servicios entre nodos. [129]
- **gRPC:** plataforma para alta performance en conexión con servicios vía RPC. [131]
- **Cassandra:** base de datos NoSQL, para aplicaciones que requieren alta disponibilidad y escalabilidad [132].

## 7.6. Bases de datos NoSQL

Los sistemas NoSQL (también llamados *Not Only SQL*, aunque no hay una convención acerca de la proveniencia de su nombre) son bases de datos distribuidas y no relacionales

diseñadas para el almacenamiento de datos a gran escala y para el procesamiento masivo de datos en paralelo a través de un gran número de servidores de productos básicos. También utilizan lenguajes y mecanismos no-SQL para interactuar con datos. [133]

En los RDBMS, la información se estructura en tablas cuya cantidad de columnas es fija y de tipos de datos discretos e invariables.

Para la abstracción y modelado de datos complejos, los datos contenidos en las tablas se relacionan mediante claves foráneas y mecanismos de integridad referencial. Esta característica es la que le da el nombre de bases “relacionales”.

Para el manejo de los datos en las bases relacionales, se utiliza el leguaje SQL, el cual permite relacionar datos y obtener resultados que se desprendan de la asociación de los datos contenidos. Uno de los mecanismos utilizados es, por ejemplo, la cláusula JOIN utilizada para relacionar tablas.

Otra característica de los RDBMS es la garantía de las propiedades ACID (*Atomicity, Consistency, Isolation and Durability),* lo que garantiza que las operaciones se ejecutarán completamente o no lo harán, que no se afectarán entre sí, que la integridad de los datos no será violada y que la información almacenada estará allí para ser accedida.

Este tipo de mecanismos pareciera cumplir con todo lo que se puede esperar de sistemas de almacenamiento. No obstante, la masificación del acceso a datos, la necesidad de procesar volúmenes crecientes, exigencias de performance y nacimiento de conceptos como BigData y otras utilidades como Machine Learning, hicieron que nuevos requisitos aparezcan y que otras características ponderen por sobre las propiedades ACID.

El problema con las bases de datos relacionales es que su performance se degrada rápidamente en la medida que el volumen de información crece.

En contrapartida a los RDBMS, las bases de datos NoSQL son diseñadas para escalar fácilmente en la medida que crecen. [134]

La característica más visible de las bases de datos NoSQL es la ausencia de estructuras tabulares (tablas de columnas fijas y filas dinámicas, con integridad referencial), las cuales fueron reemplazadas por estructuras de datos más complejas.

### 7.6.1. Big Data

Big data describe una estrategia holística de gestión de la información que incluye e integra muchos nuevos tipos de datos y de gestión de datos junto con datos tradicionales. [135]

Para entender mejor el concepto de Big Data, veamos una definición existente denominada “Las tres V”:

- **Volumen**: Big Data requiere el procesamiento de grandes volúmenes de datos, muy granulados. El objetivo es contar con mucha información, incluso de valores desconocidos, como por ejemplo clicks en una página web, tráfico de red, datos de sensores, etc. Dependiendo de la organización, el volumen de información podría variar desde decenas de terabytes hasta cientos de petabytes.

- **Velocidad**: Se requiere de gran velocidad para la recepción del volumen de datos generado. Además varias aplicaciones de Big Data, como por ejemplo actuadores en IoT o marketing en e-commerce, requieren de acciones en tiempo real, a partir del rápido análisis de los datos almacenados.

- **Variedad**: Actualmente los datos pueden no ser estructurados. De esta manera, el análisis de texto, audio y video requieren de procesamiento adicional, para adjuntarle metadatos (estos sí son estructurados) que permitan el uso de esta información de tipos heterogéneos, en conjunto con datos estructurados [136].

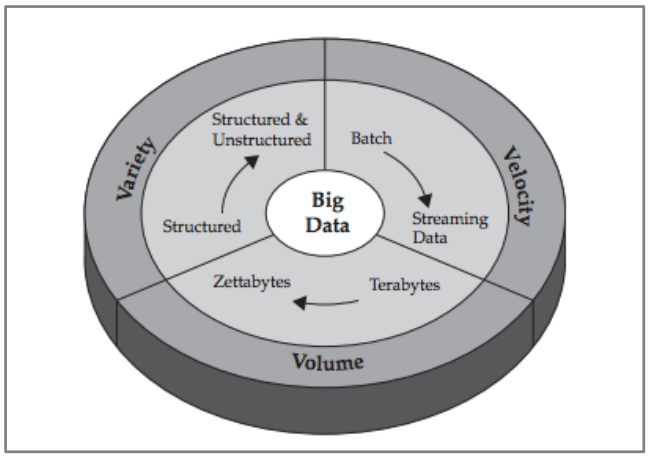



**Fig. 53 - Big Data: Volumen, Velocidad y Variedad [136]**

Existen fuentes [135] que agregan una V más a la definición, incluyendo el **Valor**: En grandes cantidades de información hay un valor que debe ser descubierto para ser explotado. Análisis estadísticos para comprender tendencias y anticiparse a eventos, así como la comprensión del interés de un cliente, son ejemplos del valor que los datos poseen

Habiendo dado una descripción acerca de qué es Big Data, cabe preguntarnos cuándo aplica usarlo. En este sentido hemos encontrado infinidad de fuentes donde mencionan

diferentes áreas de aplicación y motivos por los cuales debería usarse este paradigma, en nuestro caso optamos por quedarnos con los siguientes puntos, que por su generalidad los consideramos suficientemente abarcativos:

- Las soluciones Big Data son ideales para analizar no solo datos estructurados en bruto, sino también datos semiestructurados y no estructurados de una amplia variedad de fuentes.
- Las soluciones de Big Data son ideales cuando todos o la mayoría de los datos necesitan ser analizados en comparación con una muestra de los datos; o cuando una muestra de datos no es tan eficaz como un conjunto mayor de datos de los cuales podemos obtener análisis.
- Las soluciones Big Data son ideales para el análisis iterativo y exploratorio cuando las mediciones empresariales sobre los datos no están predeterminadas. O sea, cuando no se poseen métricas bien definidas, Big Data puede aportarnos datos valiosos.

### 7.6.2. Apache Cassandra

Habiendo definido los conceptos de bases de datos NoSQL y Big Data, veamos las características de esta base de datos que ha ido tomando relevancia en el mundo del desarrollo en la nube, hasta posicionarse como el más (o uno de los más) difundido motor de base de datos distribuidas.

Cassandra es una base de datos distribuida, NoSQL y orientada a soluciones de Big Data. Fue desarrollada por Apache Software Foundation y su primera versión data de 2008. Está escrita en Java, y se basa en los modelos de dos bases de datos NoSQL anteriores: Amazon Dynamo y Google Bigtable. [134]

**Garantiza disponibilidad y tolerancia a particiones, además de brindar consistencia eventual**, lo que significa que no se garantiza que todos los procesos vean la misma versión de cada ítem. Si bien eventualmente los datos estarán consistentes existe un periodo de tiempo denominado “Ventana de inconsistencia” donde los datos aún están siendo replicados entre los nodos.

Cuando decimos que Cassandra es una base de datos distribuida, queremos decir que tiene la capacidad de funcionar en la nube, distribuyendo sus capacidades de procesamiento y almacenamiento en nodos. La comunicación entre estos se realiza por medio de conexiones peer-to-peer.

Una de las grandes **ventajas** que posee es la escalabilidad lineal. Esto significa que la capacidad de lecturas y escrituras crece proporcionalmente a la cantidad de nodos que

posea. Además, soporta nodos con commodity-hardware (mínimos requerimientos), y la adición de estos puede llevarse a cabo sin *downtime* [132]. De esta manera, cuando se requieran mayores capacidades de respuesta, simplemente se agregan nodos en tiempo de ejecución. Este modelo de escalabilidad lineal puede explotarse aún más si se posee un esquema de autoscaling como el brindado por Amazon EC2 del conjunto de AWS.

Una de las **desventajas** de Cassandra es que las lecturas son relativamente lentas en comparación con las escrituras. En contrapartida, una gran ventaja de Cassandra es que grandes volúmenes de datos no degradan su velocidad de escritura, tornándola una excelente opción cuando el flujo de datos que se almacena es grande. [134]

# Conclusiones

- En virtud de la investigación realizada y los resultados obtenidos en el desarrollo del prototipo, concluimos que son varios los factores a tener en cuenta al momento de diseñar una red de sensores, por lo que deberían ser contemplados al menos los siguientes aspectos:
    - Que problemática se desea atacar y/o qué servicio se quiere brindar.
    - De donde se puede obtener la información necesaria.
    - Que tipos de sensores se necesitan para obtener esa información.
    - Determinar la densidad de nodos mínima, condiciones ambientales y contexto de funcionamiento sobre el cual se va a trabajar.
    - Que plataforma de hardware es la más adecuada para montar esos sensores.
    - Necesidad de actuadores.
    - Como se comunica la información sensada hacia un backend. Determinando protocolo y configuración del mismo.
    - Dinámica de los datos: volumen, persistencia, criticidad, disponibilidad y necesidad de agregación en distintos niveles.
    - Como se transforman los datos obtenidos en información de valor.

- Si bien en un principio el uso de las WSN fue pensando en un ámbito más acotado y particular (para fines militares o de investigación), hoy en día se encaminan como un pilar de un paradigma aún más grande: Internet de las Cosas. Sistemas embebidos interconectados les darán un potencial inestimable a sectores como la industria, la energía, la salud, la actividad comercial, la infraestructura urbana, el control ambiental, solo para mencionar algunos. La agregación de información funcionará ya no solo para el análisis estadístico, sino también para una mejor comprensión y modelización de cómo funciona la ciudad en términos de consumo de recursos, servicios y modos de vida.

- Habiendo desarrollado un prototipo funcional y luego de recabar información sobre distintas investigaciones y casos de estudio implementados con éxito en diferentes regiones del mundo, concluimos que en nuestro país y más precisamente en nuestra ciudad, resulta viable la implementación de diferentes "soluciones inteligentes" a problemáticas cotidianas como son: un transporte público ineficiente, congestionamientos de tránsito en las principales arterias y calles de la ciudad, contaminación sonora y ambiental, suministro y calidad del agua potable, zonas inundables por lluvias, ineficiencia en el uso de energía en hogares y edificios

públicos, niveles de inseguridad altos, entre otras cuestiones que nos afectan a diario. Consideramos que las redes de sensores, van a ser un pilar de las TICs sobre el cual desarrollar soluciones concretas en pos de mejorar la calidad de vida de los ciudadanos en torno a estas y otras problemáticas.

- El desarrollo del prototipo fue un caso de éxito, desde el punto de vista de haber logrado establecer una red de sensores utilizando las tecnologías analizadas e incorporando todos los componentes que hacen al servicio seleccionado y que juegan un papel indispensable en el contexto de Smart City analizado. El prototipo es operativo de extremo a extremo, desde el sensado hasta la visualización de información consolidada, involucrando en este camino todos los aspectos analizados teóricamente como: hardware de sensado y procesamiento, software de pre-procesamiento y comunicación, protocolos de comunicación concretos para WSN, capacidades de los mismos, antenas de RF, recolección de datos, almacenado en la nube, procesamiento y presentación de información estadística en tiempo real.

- El prototipo diseñado permite la fácil adaptación para trabajar con sensores de múltiples propósitos y diseñados por diferentes fabricantes. Esto nos da la ventaja de pensar en un único desarrollo a nivel plataforma y variados usos posibles en el campo de prueba.

- Si bien nos hemos volcado al momento de armar el prototipo en algunas tecnologías y estándares en particular (ZigBee, MQTT, Cassandra), de la investigación realizada nos queda la certeza que cada dominio de aplicación tendrá un escenario particular para analizar y por ende, no se puede concluir que para el contexto de las WSN (y menos aún en el de IoT), exista una solución única y perfecta basada en un estándar particular. Cada campo de aplicación deberá analizarse caso por caso, teniendo en cuenta diversos factores como disponibilidad de recursos, frecuencias de muestreo, volúmenes de datos, escalabilidad deseada, ambiente externo, criticidad de la información, niveles de seguridad deseados, son algunos a mencionar.

- Durante el desarrollo de la tesina, nos hemos encontrado con diferentes ejes conceptuales y paradigmas que involucran diversos aspectos en el ámbito de la informática, ya que se tocan contenidos propios de redes de comunicación, protocolos, arquitectura de microcontroladores, programación en bajo y alto nivel, bases de datos, cloud computing. También nos fue necesario investigar sobre otras temáticas totalmente ajenas al contenido curricular de la carrera, incluyendo

aspectos de otras disciplinas como la electrónica, telecomunicaciones, arquitectura y urbanismo, sociología, salud, y medio ambiente. De esto concluimos, que el perfil profesional involucrado en el desarrollo de soluciones para ciudades inteligentes, claramente involucra **no solo** al perfil informático.

- Resulta de vital importancia el aporte de los diferentes entes internacionales de Estandarización (como la IEEE, ISO, ITU e ISOC entre otros) en torno a la temática de Smart Cities, contribuyendo y generando herramientas para todos los participantes involucrados, incluyendo pero no limitándonos a fabricantes de hardware (microcontroladores, equipos de radio, sensores); empresas desarrolladoras de software; y personal de Gobierno u otros entes de control. Algunas de las cuestiones que estos estándares pretenden aclarar giran en torno a unificación de terminologías, el uso de Plataformas multipropósito, indicadores a utilizar, performance de sensores y redes de comunicación, seguridad de la información, fiabilidad y accesibilidad de los datos generados.

- La distribución de la información para una gestión eficiente de la ciudad solo será posible si se piensa en una estructura integradora entre los diferentes proveedores de sistemas y soluciones *smart* (verticales). Esto traerá claros beneficios de interoperabilidad entre las múltiples instituciones del Gobierno y también posibilitará la definición de políticas "*Open Data*".

## Trabajo Futuro

Algunos campos que excedieron el alcance de esta tesis, pero consideramos interesantes para profundizar en el campo de las Redes de Sensores inalámbricas concretamente, o bien ya en el terreno propio de las Smart Cities o el Internet de Las Cosas, son:

- Realizar un relevamiento y comparativa entre diferentes Sistemas Operativos que se encuentran hoy en día disponibles en el mercado. Entendemos que cada SO podrá adaptarse mejor o peor a un tipo de aplicación, a un entorno físico y/o a un hardware de base.
- Analizar rendimiento de radios en frecuencias 2.4GHz vs. radios de 900MHz. Teóricamente obtendríamos un mejor desempeño en términos de distancias en los segundos. A fines de desplegar una red de sensores en una ciudad (con mayor

cantidad de obstáculos e interferencias), quizás la frecuencia de 900MHz nos arroje mejores resultados.

- Como vimos en el estudio realizado existen múltiples campos de aplicación posibles para desarrollar en una ciudad. Algunos de los campos de trabajo que pueden llegar a generar información valiosa con la utilización de este tipo de tecnologías en nuestro entorno local pueden ser: los Sistemas de distribución de agua (control de fugas, calidad del agua, calidad del servicio), control de tráfico vehicular y asignación de estacionamientos, cuestiones de seguridad en la vía pública, optimización en la recolección de residuos, entre otros.
- Profundizar en técnicas de recolección de la información, clasificación y anonimación para políticas de Open Data.
- Analizar el uso del BigData asociado a redes de sensores, para alimentar modelos de simulación y sistemas de predicción.
- Buenas prácticas en el desarrollo de software para soluciones del campo de las IoT, enfocado en el uso óptimo de recursos de energía limitados.
- Mecanismos de seguridad en protocolos de comunicación y dispositivos ultra livianos.

# Bibliografía


[1] D. A. Beyer, «Accomplishments of the DARPA SURAN Program,» 1990.

[2] GSMA, «GSMA web site,» [En línea]. Available: http://www.gsma.com/.

[3] IETF-RFC 2501, «Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations,» 1999.

[4] Link Labs, «linkk-labs.com,» 2015. [En línea]. Available: https://www.link-labs.com/blog/what-is-m2m.

[5] N. Hunn, «Nick Hunn,» 2015. [En línea]. Available: http://www.nickhunn.com/m2ms-impending-hole-in-the-air/.

[6] «IEEE 802.11 Standard for Information technology,» 2012.

[7] «Juniper Networks,» [En línea]. Available: https://www.juniper.net/documentation/en_US/junos-space-apps/network-director2.0/topics/concept/wireless-ssid-bssid-essid.html.

[8] M. Ilyas, The Handbook of Ad Hoc Wireless Networks, CRC Press, 2003.

[9] K. SOHRABY, D. MINOLI y T. ZNATI, WIRELESS SENSOR NETWORKS Technology, Protocols, and Applications, Wiley-Interscience, 2007.

[10] E. O. Sosa, CONTRIBUCIONES AL ESTABLECIMIENTO DE UNA RED GLOBAL DE SENSORES INALAMBRICOS INTERCONECTADOS, 2011.

[11] A. L. Colina, Internet de las Cosas, 2015.

[12] I. DIETRICH y F. DRESSLER, «On the Lifetime of Wireless Sensor Networks,» Dept. of Computer Science, University of Erlangen, Germany, 2009.

[13] «IEEE 802.15.4-2011 IEEE Standard for Information technology,» 2011.

[14] C. G. Arano, «IMPACTO DE LA SEGURIDAD EN REDES INALÁMBRICAS DE SENSORES IEEE 802.15.4,» 2010.

[15] IEEE - 1451, «grouper.ieee.org,» [En línea]. Available: http://grouper.ieee.org/groups/1451/6/TermsDefinitions.htm.

[16] K. Akkaya y M. Younis, «A survey on routing protocols for wireless sensor networks,» Science Direct, 2003.

[17] J. N. Al-Karaki y A. E. Kamal, «Routing Techniques in Wireless Sensor Networks: A Survey».

[18] J. P. Dignani, «ANÁLISIS DEL PROTOCOLO ZIGBEE,» La Plata, 2011.

[19] «ISO.org,» [En línea]. Available: https://www.iso.org/isoiec-27001-information-security.html.

[20] J. P. Walters, Wireless Sensor Network Security: A Survey, 2006.

[21] «Document Cloud,» [En línea]. Available: https://www.documentcloud.org/documents/3911338-Internet-of-Things-Cybersecurity-Improvement-Act.html.

[22] «Ericsson.com,» 2016. [En línea]. Available: https://www.ericsson.com/en/mobility-report/internet-of-things-forecast.

[23] P. Howard, «Data Share: How big is the IoT,» 13 Junio 2015. [En línea]. Available: http://philhoward.org/data-share-how-big-is-the-iot/].

[24] UIT, «Recomendación UIT-T Y.2060,» 2012.

[25] «SensorMag,» [En línea]. Available: http://archive.sensorsmag.com/articles/0603/14/main.shtml.

[26] Libelium. [En línea]. Available: http://www.libelium.com/security-802-15-4-zigbee/.

[27] Digi, «Digi.com - ZigBee,» [En línea]. Available: https://www.digi.com/resources/documentation/Digidocs/90001942-13/#concepts/c_zb__stack_layers.htm%3FTocPath%3DZigBee%2520in%2520a%2520nutshell%7C_____2.

[28] IETF-RFC 3561, «IETF.org,» [En línea]. Available: https://datatracker.ietf.org/doc/rfc3561.

[29] D. Gislason, Zigbee Wireless Networking, Elsevier - Newnes.

[30] NXP, «NXP.com,» [En línea]. Available: http://www.nxp.com/docs/en/user-guide/JN-UG-3077.pdf.

[31] Z. Alliance, «Estandar ZigBee 3.0».

[32] IETF-RFC2460, «IETF.org,» [En línea]. Available: https://www.ietf.org/rfc/rfc2460.txt.

[33] IETF-RFC4919, «IETF.org,» [En línea]. Available: https://datatracker.ietf.org/doc/html/rfc4919.

[34] IETF-RFC6282, [En línea]. Available: https://tools.ietf.org/html/rfc6282.

[35] IETF-RFC4862, «IETF.org,» [En línea]. Available: https://tools.ietf.org/html/rfc4862.

[36] T. Instrument, «Texas Instrument,» [En línea]. Available: http://www.ti.com/lit/wp/swry013/swry013.pdf.

[37] IETF-RFC6650, «IETF.org,» [En línea]. Available: https://tools.ietf.org/html/rfc6550.

[38] Hart Communication Fundation, «Hart Communication Protocol,» 2015. [En línea]. Available: http://en.hartcomm.org/. [Último acceso: 10 2015].

[39] «fieldcommgroup.org,» [En línea]. Available: https://fieldcommgroup.org/wirelesshart-security.

[40] M. G. #. J. N. #. T. L. #. a. M. B. Johan Akerberg ˚ #1, «Deterministic Downlink Transmission in WirelessHART Networks enabling Wireless Control».

[41] «emb.cl,» [En línea]. Available: http://www.emb.cl/electroindustria/articulo.mvc?xid=1399.

[42] W. Hart, «RP400 Series».

[43] D. Sexton, *SP100.11a Overview,* GE Global Research, ISA, 2007.

[44] A. Ristaino, «isa100wci.org,» [En línea]. Available: https://isa100wci.org/en-US/Documents/Presentations/2014-Oct-15-ISA100-Wireless-IEC62734-Approval.

[45] M. Nixon, «A Comparison of WirelessHARTTM and ISA100.11a,» 2012.

[46] K. L. Marko Paavola, «Wireless Sensor Networks in Industrial Automation,» InTech, 2010.

[47] «EnOcean.com,» EnOcean GmbH, 2015. [En línea]. Available: https://www.enocean.com/.

[48] ISO/IEC, «ISO/IEC DIS 14543-3-10 Wireless Short-Packet (WSP) protocol optimized for energy,» 2011.

[49] E. W. Alliance, «EnOcean.com,» [En línea]. Available: https://www.enocean.com/en/technology/energy-harvesting.

[50] A. EnOcean, «EnOcean Equipment Profiles (EEP) v.2.6.7,» 2017.

[51] «Electronic Product Design & Test,» 30 1 2013. [En línea]. Available: http://www.epdtonthenet.net/article/55818/ISO-IEC-14543-3-10-a-new-wireless-standard.aspx.

[52] «Z-Wave Alliance website,» [En línea]. Available: http://www.z-wavealliance.org/].

[53] ITU-G9959, «ITU.int,» 2015. [En línea]. Available: https://www.itu.int/rec/T-REC-G.9959-201501-I/es.

[54] rfwireless-world-ZWStack, «rfwireless-world,» [En línea]. Available: http://www.rfwireless-world.com/Tutorials/z-wave-protocol-stack.html.

[55] ZWAVE, «ZWAVE-Frequency,» [En línea]. Available: http://z-wave.sigmadesigns.com/wp-content/uploads/2016/08/Z-Wave_Frequency_Coverage.pdf.

[56] rfwireless-world, «rfwireless-world,» [En línea]. Available: http://www.rfwireless-world.com/Tutorials/z-wave-device-conformance-testing.html.

[57] ZWAVE, «ZWave Security,» [En línea]. Available: http://z-wavealliance.org/z-wave-alliance-announces-new-security-requirements-z-wave-certified-iot-devices/].

[58] vesternet.com, «vesternet.com,» [En línea]. Available: http://www.vesternet.com/resources/technology-indepth/understanding-z-wave-networks.

[59] «Semtech.com,» [En línea]. Available: http://www.semtech.com/.

[60] A. Lora, «lora-alliance.org,» [En línea]. Available: https://www.lora-alliance.org.

[61] «Sigfox.com,» [En línea]. Available: https://www.sigfox.com/.

[62] «Sigfox.com/telefonica,» [En línea]. Available: https://www.sigfox.com/en/news/sigfox-and-telefonica-strike-global-deal-offer-iot-services-worldwide.

[63] «3GPP.com,» [En línea]. Available: http://www.3gpp.org.

[64] «GSMA.com,» [En línea]. Available: https://www.gsma.com/iot/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/.

[65] Digi, «DIGI.com,» [En línea]. Available: https://www.digi.com/resources/documentation/digidocs/PDFs/90000976.pdf.

[66] OASIS. [En línea]. Available: https://www.oasis-open.org/committees/tc_cat.php?cat=iot.

[67] IBM, «IBM.com-MQTT,» [En línea]. Available: https://www.ibm.com/podcasts/software/websphere/connectivity/piper_diaz_nipper_mq_tt_11182011.pdf.

[68] Eclipser.org, «Eclipse Paho,» [En línea]. Available: https://eclipse.org/paho/.

[69] K. H. C. B. Z. Shelby, «The Constrained Application Protocol (CoAP),» 2014.

[70] A. V. ,. U. d. S. Xiaoping Ma, «researchgate.net,» [En línea]. Available: https://www.researchgate.net/publication/267636202_Performance_evaluation_of_MQTT_and_CoAP_via_a_common_middleware.

[71] S. M. A. W. D. G. J. P. J. H. R. S. M. W. K. W. E. B. D. C. Philip Levis, «TinyOS: An Operating System for Sensor Networks».

[72] S. M. ElKazak, «GEN600 Final Technical Report: Research in Internet of Things' Operating Systems,» [En línea]. Available: https://es.slideshare.net/SalahuddinElKazak/research-in-internet-of-things-operating-systems-iot-oss.

[73] «Contiki,» 2015. [En línea]. Available: http://www.contiki-os.org/].

[74] «Riot OS,» 2016. [En línea]. Available: http://www.riot-os.org/].

[75] TIZEN, «https://www.tizen.org/,» [En línea]. Available: https://www.tizen.org/.

[76] Android, «https://developer.android.com/things/sdk/index.html,» [En línea]. Available: https://developer.android.com/things/sdk/index.html.

[77] Microsoft, «Windows 10 IoT - Platform overview,» 2016. [En línea]. Available: https://www.microsoft.com/en-us/windowsforbusiness/windows-iot.

[78] Naciones Unidas, «Naciones Unidas,» 2014. [En línea]. Available: http://www.un.org/es/development/desa/news/population/world-urbanization-prospects-2014.html.

[79] Ministerio de Ambiente y Desarrollo sustentable, «ambiente.gob.ar,» 2017. [En línea]. Available: http://ambiente.gob.ar/ciudades-sustentables/creacion-de-la-unidad-ciudades-sustentables/.

[80] Centro de Investigación y Desarrollo en Tecnologías de la Información y las Comunicaciones, «CIUDADES INTELIGENTES: Bases de un modelo de medición de la Inteligencia de la Ciudad.,» *RTC,* vol. 63, pp. 29 - 36.

[81] «Mobile Amplus,» [En línea]. Available: http://www.mobileamplus.com/es/blog/santander-modelo-espanol-de-smart-city/#.VHunoDHF-Sq.

[82] European Commision, *Smart cities and communities - European innovation partnership,* Bruselas, 2012.

[83] R. a. L. S. Moss Kanter, «Informed and Interconnected: A Manifesto for Smarter Cities,» Harvard Business School General Management , 2009.

[84] D. Toppeta, «The Smart City vision: How Innovation and ICT can build smart, “liveable”, sustainable cities.,» The Innovation Knowledge Fundation, 2010.

[85] R. E. Hall, «The vision of a smart city,» 2nd International Life Extension Technology Workshop, Paris, 2000.

[86] ITU-T Focus Group on Smart Sustainable Cities, «Shaping smarter and more sustainable cities,» 2016. [En línea]. Available: http://wftp3.itu.int/pub/epub_shared/TSB/ITUT-Tech-Report-Specs/2016/en/flipviewerxpress.html.

[87] R. Ardila, «Calidad de vida: una definición integradora,» *Revista Latinoamericana de Psicología,* vol. 35, nº 2, pp. 161-164, 2003.

[88] IBM, «IBM - Ciudades inteligentes,» [En línea]. Available: https://www.ibm.com/smarterplanet/us/en/.

[89] ISO 37101:2016, «ISO.org,» 2016. [En línea]. Available: https://www.iso.org/obp/ui/#iso:std:iso:37101:ed-1:v1:en.

[90] ISO 37120:2014, «ISO.org,» 2014. [En línea]. Available: https://www.iso.org/obp/ui/#iso:std:iso:37120:ed-1:v1:en:tab:A.1.

[91] ISO 37151:2015, «ISO.org,» 2015. [En línea]. Available: https://www.iso.org/obp/ui/#iso:std:iso:ts:37151:ed-1:v1:en:fig:1.

[92] ISO/IEC - JTC 1/SC 41, «ISO.org,» [En línea]. Available: https://www.iso.org/committee/6483279.html.

[93] IEEE, «standards.ieee.org,» [En línea]. Available: http://standards.ieee.org/develop/msp/smartcities.pdf.

[94] IEEE, «smartcities.ieee.org,» [En línea]. Available: https://smartcities.ieee.org/.

[95] «cencenelec.eu,» 2015. [En línea]. Available: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/SmartLiving/City/SSCC-CG_Final_Report-recommendations_Jan_2015.pdf.

[96] BSI, «Smart cities overview – Guide (PD 8100:2015),» 2015.

[97] AENOR-CTN 178, «NORMALIZACIÓN EN CIUDADES INTELIGENTES-ESPAÑA,» 2015.

[98] ANSI, «Ansi.org - ANSI Network on Smart and Sustainable Cities (ANSSC),» [En línea]. Available: https://www.ansi.org/standards_activities/standards_boards_panels/anssc/overview?menuid=3.

[99] NIST, «Nist.gov,» [En línea]. Available: https://pages.nist.gov/smartcitiesarchitecture/.

[100] DKE-German Standardization roadmap Smart City, «DKE.de,» 2014. [En línea]. Available: https://www.dke.de/resource/blob/778248/d2afdaf62551586a54b3270ef78d2632/the-german-standardization-roadmap-smart-city-version-1-0-data.pdf.

[101] Ministry of Industry and Information Technology (MIIT), «Comparative Study of Smart Cities in Europe and China,» 2014.

[102] ITU, «Itu.int,» 2015. [En línea]. Available: http://www.itu.int/net/pressoffice/press_releases/2015/22-es.aspx#.WZz8ZFGGPIU.

[103] G. Mercado, J. M. D. Peña, R. Stasi, G. López y A. Burlot, «SG-SM - Smart Grid San Martin».

[104] E. L. S. G. G. C. M. S. R. S. N. P. Jon Froehlich, «Disaggregated End-Use Energy Sensing for the Smart Grid,» *P E R V A S I V E computing,* 2010.

[105] B. d. C. e. S. G. P. H. Gerhard P. Hancke, «The Role of Advanced Sensing in Smart Cities,» National Institute of Health - USA, Basel, 2012.

[106] D. N. C. D. C. M. W. A. M. T. Nicole Metje, «Smart Pipes—Instrumented Water Pipes, Can This Be Made a Reality?,» National Institute of Health - USA, Basel.

[107] N. M. D. N. C. C. J. A. Ali M. Sadeghioon, «SmartPipes: Smart Wireless Sensor Networks for Leak Detection in Water Pipelines,» *Journal of Sensor and Actuator Networks,* pp. 64 - 78, 3 2014.

[108] C. Correa, R. Ruíz y D. Rivera, «Monitoreo de Caudales en Canales Usando Redes de Sensores Inalámbricas,» Facultad de Ingeniería Agrícola, Universidad de Concepción.

[109] Libelium, «Libelium web site,» [En línea]. Available: http://www.libelium.com.

[110] S. Kim, «Wireless Sensor Networks for Structural Health Monitoring,» 2005.

[111] H. ZHAN, C. PAN, J. YANG, H. DONG, Y. QIN y L. JIA, «SN-UTIA: A Sensor Network for Urban Traffic Information,» de *IEEE Intelligent Vehicles Symposium*, 2010.

[112] «Smart Santander,» [En línea]. Available: http://www.smartsantander.eu/.

[113] J. R. M.-d. D. A. O. B. Alberto De San Bernabe Clemente, «A WSN-Based Tool for Urban and Industrial Fire-Fighting,» National Institute of Health, Basel, 2012.

[114] ADVANTICSYS , «https://telosbsensors.wordpress.com,» [En línea]. Available: https://telosbsensors.wordpress.com.

[115] «802.15.6-2012 - IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks».

[116] W. L. F. M. M. A. Marcelo Sousa, «Cognitive LF-Ant: A Novel Protocol for Healthcare Wireless Sensor Networks,» National Institute of Health - USA.

[117] Singapore Government, «https://www.tech.gov.sg/,» [En línea]. Available: https://www.tech.gov.sg/.

[118] AURIN Technical Committee , «https://aurin.org.au/,» [En línea]. Available: https://aurin.org.au/.

[119] Republic of Korea, «http://songdoibd.com/,» [En línea]. Available: http://songdoibd.com/.

[120] «Data.gov.uk,» [En línea]. Available: https://data.gov.uk/.

[121] CIMA, Centro de Investigaciones del Medio Ambiente, Facultad de Ciencias Exactas, «CONTAMINACIÓN DEL AIRE POR COMPUESTOS ORGÁNICOS VOLÁTILES Y MATERIAL PARTICULADO EN LA PLATA Y ENSENADA,» 2011.

[122] G. B. S. N. G. María E Manzur, «MODELO DE DISPERSIÓN DE CONTAMINANTES ATMOSFËRICOS,» 2012.

[123] OMS, «Guia de calidad del aire,» 2006.

[124] Nova Fitness Co.,Ltd, «Laser PM2.5 Sensor specification - Product model: SDS011 V1.3,» 2015.

[125] A. Rapp, «https://github.com/andrewrapp/xbee-Arduino,» [En línea]. Available: https://github.com/andrewrapp/xbee-Arduino.

[126] N. O'Leary, «https://github.com/knolleary/pubsubclient,» [En línea]. Available: https://github.com/knolleary/pubsubclient.

[127] D. International, «ZigBee RF Modules,» 2016.

[128] «Thingsboard.io,» [En línea]. Available: https://thingsboard.io/].

[129] Apache Software Foundation, «https://zookeeper.apache.org/,» [En línea]. Available: https://zookeeper.apache.org/.

[130] M. Meyer, «The Simple Magic of Consistent Hashing,» 20 12 2011. [En línea]. Available: https://dzone.com/articles/simple-magic-consistent.

[131] GRPC, «http://www.grpc.io/),» [En línea]. Available: http://www.grpc.io/).

[132] Apache Software Foundation, «http://cassandra.apache.org,» [En línea]. Available: http://cassandra.apache.org.

[133] S. A. H. A B M Moniruzzaman, «NoSQL Database: New Era of Databases for Big data Analytics - Classification, Characteristics and Comparison,» *International Journal of Database Theory and Application,* vol. 6, nº 4, 2013.

[134] A. P. D. P. Ameya Nayak, «Type of NOSQL Databases and its Comparison with Relational Databases,» *International Journal of Applied Information Systems (IJAIS),* vol. 5, nº 4, marzo 2013.

[135] ORACLE, «Oracle.com,» [En línea]. Available: https://www.oracle.com/es/big-data/index.html.

[136] P. C. Zikopoulos, Understanding Big Data, 2012.