UNIVERSIDAD DE VALLADOLID

ESCUELA TÉCNICA SUPERIOR

DE INGENIEROS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

GRADO EN INGENIERIAS DE TECNOLOGÍAS DE TELECOMUNICACIÓN

Estudio de la seguridad en redes BSN aplicadas al ámbito sanitario

---

AUTORA: **Marina Benito Alonso**

TUTORA: **Isabel de la Torre Díez**

16 de mayo de 2016

A mis padres, por su continuo apoyo incondicional, su paciencia durante todos estos años de carrera y sus alegrías con mis triunfos.

A mis hermanos Marta, Jesús y Pablo por cada día disfrutado juntos.

A mis amigos y amigas, por estar siempre ahí y por sus ánimos durante todo el tiempo que me ha llevado este trabajo.

A Clara, gracias por tu ayuda, apoyo y consejos a pesar de la distancia, sé que siempre puedo contar contigo.

A mis compañeros de carrera por todos los años compartidos y disfrutados.

A mis compañeros de trabajo, por los consejos que me habéis brindado desde la experiencia.

A mi tutora Isabel, por su paciencia, su ayuda y su tiempo invertido en mí.

Y por último a Alejandro, por su infinita ayuda cada día y su apoyo incondicional, por ser una de esas personas que dejan huella, gracias por seguir queriendo caminar juntos.

RESUMEN

Hoy en día todas las herramientas relacionadas con la tecnología, las redes inalámbricas e incluso aplicaciones móviles se han vuelto imprescindibles en la mayor parte de los aspectos cotidianos de nuestras vidas, esto incluye el cuidado de la salud y los hábitos de vida saludables. Por esto en los últimos años se ha producido un importante desarrollo de las redes de sensores de área corporal (*Body Sensors Networks*, BSN) que permiten un control permanente del cuerpo humano.

El uso de estas redes está motivado por la creciente necesidad de atención médica constante, ya que en un mundo en el que cada vez hay más personas con enfermedades cardiovasculares, hipertensión o diabetes, una detención precoz puede ayudar a mejorar la calidad de vida de los pacientes, además de ampliar su autonomía con respecto a las redes anteriores o a las redes por cable. Por otro lado una monitorización permanente y una revisión continua pueden ayudar al médico a elegir el tratamiento más adecuado y personalizado para cada persona. Estas redes de sensores aún tienen que superar muchos retos como son el tamaño o la mejor distribución en el cuerpo del paciente para que no interfiera en el día a día del usuario.

La seguridad cada día es más importante en todos los ámbitos relacionados con las Tecnologías de la Información y la Comunicación (TIC), pero lo es más aún cuando está la salud de los pacientes en juego. La confiabilidad y la privacidad son requerimientos necesarios para que los pacientes se sientan seguros con los sensores, pero también lo es la fiabilidad, puesto que no se podrá realizar un seguimiento adecuado ni obtener el mejor diagnóstico si no pueden ser procesados todos los datos medidos debido a que estos se pierdan o dañen antes de llegar a su destino.

El objetivo de este trabajo es proporcionar una revisión de los artículos y publicaciones referentes a la seguridad de las BSN aplicadas al ámbito sanitario en los últimos años, de forma que sirva como punto de partida y ayude, en un futuro próximo, a desarrollar aplicaciones que mejoren la seguridad en el diagnóstico y tratamiento de pacientes con enfermedades crónicas.

ABSTRACT

Nowadays, every technology tools, wireless networks, and even mobile applications have become necessary in daily aspects of everyday life, included healthcare and healthy lifestyle. Thus, in the last years has taken place an important development of the Body Sensor Networks (BSN) to let a continuous monitoring.

The use of this networks is motivated by the increasing need of continuous medical care. We live in a world in which is increasing the number of people who suffer cardiovascular diseases, hypertension or diabetes, so, an early detection of them, can improve patient's quality of life, also expand their autonomy of previous networks or wire networks. On the other hand a continuous monitoring could help the doctor to choose the most appropriate and personalized treatment for each person. This sensor networks have to overcome many challenges as body size or the best distribution in the body patient in order to not interfering in the patient daily life.

Security is becoming increasingly important in all areas related to information and communications technology (TIC), and becomes even more important when patients health is involved. Confiability and privacy are necessary requirements for patients to feel secure with the sensors, but the reliability is necessary too, because if all measured data are lost or damage before reaching their destination, it cannot be made an adequate monitor or make the best diagnosis.

The aim of this work is to provide an article and publications review of the security for BSN applied to the healthcare field in the last years, in order to enable the development of applications to improve the patient's diagnosis and treatment with chronic diseases.

Palabras clave: Redes de sensores, privacidad, fiabilidad, seguridad, m-health.

Índice.

Índice de Ilustraciones

Índice de Tablas

1. INTRODUCCIÓN

1.1. Motivación

El objetivo de este trabajo es dar una visión general sobre la seguridad de las redes de sensores de área corporal (*Body Sensor Network*, BSN), también conocidas como redes de área corporal (*Body Area Network*, BAN) o redes de sensores inalámbricas de área corporal (*Wireless Body Sensor Network*, WBSN), y su evolución a través de los años, fomentado por el gran interés que han suscitado estas nuevas tecnologías enfocadas al cuidado de la salud y a las aplicaciones médicas.

El uso de las tecnologías ha facilitado mucho nuestra vida cotidiana, pero también ha fomentado una vida mucho más sedentaria. Según la Organización Mundial de la Salud (OMS) actualmente hay 41 millones de niños con obesidad, esto está llevando a que cada vez haya más personas que padezcan enfermedades cardiovasculares y diabetes. Hay 422 millones de personas en el mundo que tienen diabetes [1], de las cuales más del 90% son del tipo 2, además las enfermedades cardiovasculares son la principal causa de muerte en el mundo, más del 30% [2]. Todo ello sumado al envejecimiento de la población, que en los últimos años se ha incrementado rápidamente, hace que sea más necesario un sistema sanitario más eficiente y adecuado a este sector de la población, puesto que son los pacientes con más enfermedades crónicas, y más propensos a cardiopatías, ictus, deterioro sensorial o diabetes. Estas tendencias están provocando que cada vez haya más pacientes que requieren de atención médica, lo que está motivando el desarrollo de redes de sensores que permitan una atención más rigurosa y personalizada, y terapias más eficientes que faciliten el diagnóstico y la recuperación del enfermo. En el caso de las personas con diabetes una monitorización frecuente permite administrar la dosis de insulina adecuada, lo que puede reducir el riesgo de desmayos, ceguera, pérdida de circulación y otras complicaciones médicas que pueden ocurrir en pacientes que llevan años con esta enfermedad.

Actualmente cualquiera tiene acceso a pulseras electrónicas y relojes inteligentes cada vez más sofisticados que han revolucionado la monitorización personal a tiempo real, este año se estima que se venderán 50 millones de relojes inteligentes y 35 millones de pulseras electrónicas. Contabilizan las calorías ingeridas, controlan el pulso al realizar cualquier actividad o durante el sueño e incluso las horas que se duerme. Existen, además, aplicaciones que miden la temperatura corporal, la tensión arterial o el nivel de glucosa como si se estuviese en una sala de observación de la consulta del médico. Se pueden sincronizar al teléfono móvil, *Smartphone* o a una *Tablet* y desde el ahí el propio paciente puede llevar un control sobre su salud e ir viendo su evolución. Este continuo desarrollo en las nuevas tecnologías aplicadas al ámbito de la salud ha llevado a generar un nuevo término conocido como *m-health* (salud móvil).

Ilustración 1. Ejemplo de uso de una Tablet en los hospitales. Fuente: *http://mundocontact.com/5-componentes-tecnologicos-para-el-hospital-del-futuro*

A pesar de que este trabajo se centra en redes de sensores dedicadas al cuidado de la salud, también están en auge en otros ámbitos como en los deportes, el bienestar, el sector de la industria militar, el entretenimiento y en general en multitud de aplicaciones que requieren información procedente de las señales del cuerpo humano.

1.2. Visión general

Las redes de sensores de área corporal consisten en una serie de sensores interconectados y distribuidos alrededor del cuerpo humano con el fin de recoger, procesar y analizar datos e información para la función que han sido implementados. En los últimos años se ha originado un repentino interés en biosensores inteligentes y dispositivos de monitorización portátil con el fin de conseguir un control permanente del cuerpo humano. Las BSNs se centran en sistemas de monitorización portátiles y en tiempo real con el objetivo de asegurar una continua monitorización de los pacientes, mientras les proporciona la libertad de movimientos y de este modo mejorar la calidad del cuidado de la salud [3]. Hacer los dispositivos cada vez más pequeños para mejorar la movilidad y la accesibilidad es uno de los aspectos que se encuentra en constante desarrollo.

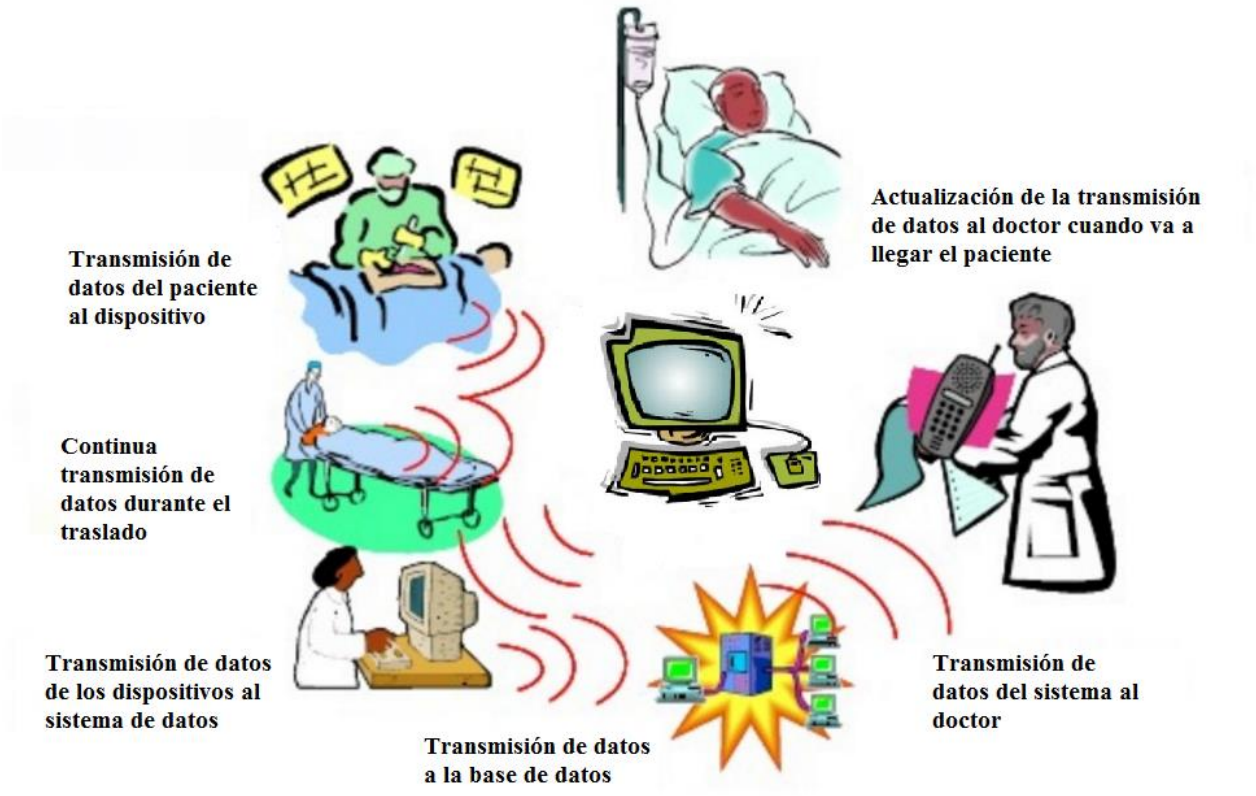

Ilustración 2. Visión general de una BSN. Fuente: Propia

Durante muchos años la monitorización y el control de las enfermedades se han realizado dentro de los hospitales bajo un entorno clínico y donde todo está esterilizado. Un ambiente muy alejado del entorno real de los pacientes en su vida diaria. Las BSN hacen posible que el médico pueda llevar un control más fiable de sus pacientes permitiéndoles realizar su día a día con total normalidad y pudiendo ver que es lo que más afecta o mejor les conviene.

1.3. Contexto.

Además de la monitorización de los parámetros fisiológicos con los que es posible detectar irregularidades que puedan resultar un riesgo para la vida de los pacientes, una BSN deber tener en cuenta que una persona es muy sensible a las condiciones externas que le rodean e incluso a los cambios medioambientales. Dentro de lo que se puede considerar el contexto de una persona se encuentran las actividades que realiza, la temperatura del entorno o la hora del día. Por ejemplo que un sensor detecte un rápido incremento de su frecuencia cardiaca no siempre significa que esté sufriendo un episodio cardiaco, puede ser simplemente que se haya producido un cambio en su actividad física o que esté realizando deporte.

La actividad innata de las personas produce un movimiento corporal natural de forma continua, una ligera limitación que hace que el entorno que rodea a la persona, los factores medioambientales y el estado físico de la persona deben ser tenidos en cuenta dentro de las BSNs.

Una BSN debe reconocer el escenario en el que se encuentra de forma flexible para poder añadir un nuevo contexto al sistema siempre que el entorno cambie o eliminarlo si ya no es necesario seguir percibiéndolo. Para ello el sistema debe ser adaptativo, y cómo las aplicaciones reales de una BSN funcionan durante largos periodos de tiempo, es importante que el sistema no solo sea capaz de aprender nuevos contextos sino que también no olvide los contextos que previamente fueron aprendidos para no tener que aprender el contexto de nuevo.

1.4. Investigaciones actuales.

Actualmente ya existen ordenadores con las dimensiones de un grano de arena que pueden informar a los médicos de lo que ocurre dentro del cuerpo humano. Se mueven por el torrente sanguíneo o se alojan en los tejidos y pueden atacar a las células cancerígenas de un tumor cuando comienza a desarrollarse, reducir el dolor o almacenar información vital.

Investigadores suizos han desarrollado el primer chip que se puede ingerir para monitorizar a tiempo real y de manera continua los niveles de colesterol, azúcar, PH o la temperatura corporal. Un equipo británico ha diseñado píldoras con microprocesadores que pueden comunicarse con el médico mediante mensajes de texto para que el doctor pueda saber si las píldoras están actuando de forma adecuada. Existen también circuitos integrados en cápsulas que actualmente tienen una gran utilidad detectando los niveles de grasa y otros nutrientes en pacientes obesos y que son capaces de generar señales que engañan al estómago cuando ya se ha comido lo suficiente creando una sensación de saciedad.

Aunque aun está en desarrollo lo que está revolucionando el mundo de la diabetes y de la medición de los niveles de glucosa es un tatuaje digital, que puede adherirse a la piel o insertarse como un implante subcutáneo [4]. Puede medir el flujo sanguíneo durante 24h y sin que el paciente tenga que permanecer inmóvil. Se trata de un sensor flexible que utiliza una corriente eléctrica suave para medir los niveles de glucosa en sangre, evitando así las molestias de tener que pincharse la yema de los dedos varias veces al día, y permite conocer la dosis necesaria de insulina que necesitaría suministrarse

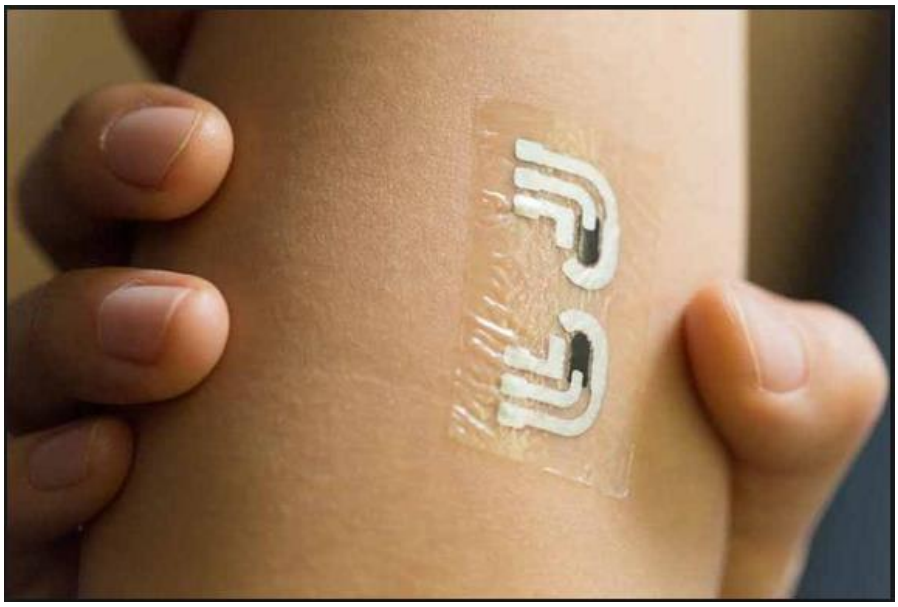

Ilustración 3. Ejemplo de tatuaje digital para diabéticos. Fuente: *http://www.omicrono.com/2015/01/un-tatuaje-que-mide-los-niveles-de-azucar-en-sangre-sin-agujas*.

No solo se han desarrollado dispositivos y aplicaciones que necesiten estar en el interior del cuerpo humano para mejorar la salud de los pacientes, también se están desarrollando otras aplicaciones y dispositivos que mejoran la calidad de vida de personas con alguna discapacidad o enfermedad de forma mucho menos invasiva. Como la tecnología del calzado háptico que ayuda a orientarse a personas con problemas visuales. Son unas plantillas que informan mediante vibraciones donde debe girar la persona que las lleva puestas conectadas al *Smartphone* mediante bluetooth.

2. REDES DE SENSORES Y FUNDAMENTOS

Antes de comenzar con la seguridad, es importante dar una visión de cómo se encuentran actualmente las BSN en el ámbito sanitario de manera que ayude a comprender mejor los fundamentos que han llevado a la necesidad de desarrollar este tipo de redes, también es importante ver cómo se implementan y cuál es su funcionamiento, además de entender porque la seguridad es un factor tan importante en las redes de sensores dedicadas a la salud del cuerpo humano.

Tras un repentino interés en los últimos años en el control y la monitorización del cuerpo humano, principalmente en el campo de la medicina y dirigido al cuidado de la salud, surgieron las redes de sensores inalámbricas de área corporal (WBSN), equipadas con sensores biomédicos y circuitos de baja potencia, que permiten comunicaciones inalámbricas.

Una WBSN está compuestas por una serie de pequeños nodos, compuestos por sensores biomédicos, detectores de movimiento y dispositivos de comunicación inalámbrica, estos nodos recogen las señales del cuerpo humano y las transmiten de forma inalámbrica a una unidad central donde son procesadas. Gracias a que se comunican de forma inalámbrica tienen muchas ventajas como la ubicación, la movilidad y la interoperabilidad, además estos nodos pueden estar también equipados con actuadores como los marcapasos o dispositivos capaces de inyectar medicamentos para mejorar la calidad de vida del paciente.

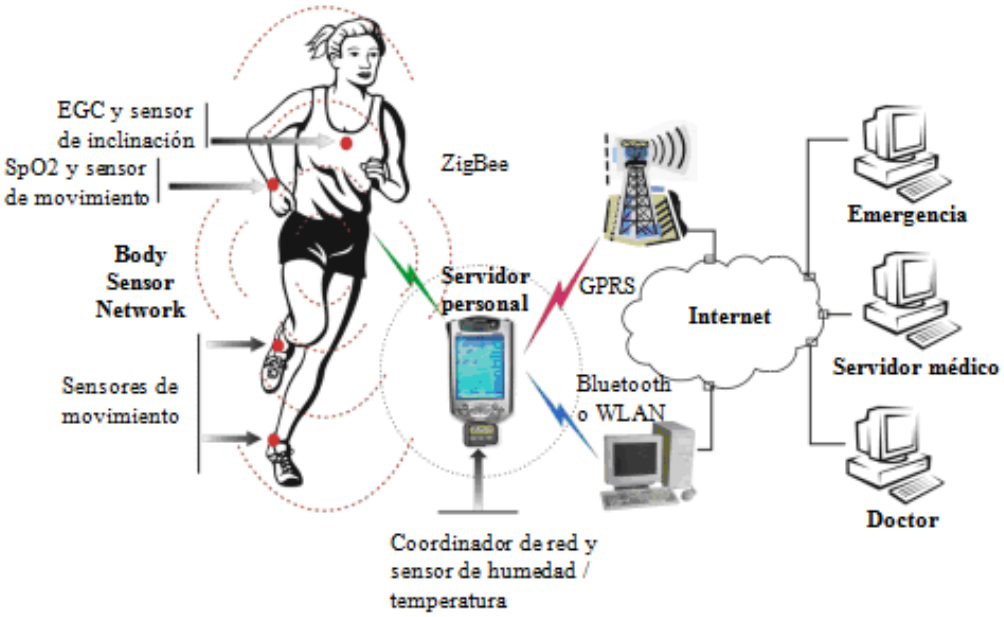

Ilustración 4. Arquitectura de una BSN. Fuente: [36].

2.1. Cambio de las Redes de Sensores Inalámbricas (WSN) a las redes de sensores inalámbricas de área corporal (WBSN)

Las WBSNs surgieron como una nueva generación de redes inalámbricas de sensores (*Wireless Sensor Network*, WSN). Estas redes se desarrollaron inicialmente para la vigilancia y la monitorización de aplicaciones militares, puesto que consisten en redes altamente distribuidas y organizadas. Las principales características que diferencian a las WBSNs y las WSNs son las siguientes [3]:

- ✓ Arquitectura. En una WSN cada nodo actúa como nodo sensor y como nodo coordinador, sin embargo en una red WBSN se encuentran dos tipos de nodos, los sensores que actúan en el interior o sobre el cuerpo humano y los coordinadores cuya función es transmitir los datos obtenidos.
- ✓ Tasa de trasmisión. Debido a que las WBSNs se utilizan para el seguimiento de las actividades del cuerpo humano, la transmisión de datos es continua y a un ritmo constante, a diferencia de las redes inalámbricas de sensores, donde los eventos pueden ocurrir de manera irregular.
- ✓ Movilidad. Los nodos de una WBSN se mueven en grupo y en la misma dirección, al contrario que en las WSN en los que cada nodo se mueve de manera individual.
- ✓ Número de sensores. En el caso de un red WBSN el número de nodos utilizados depende del usuario y de la aplicación para la que esté pensada, pero por lo general no se utilizan tantos como en una red inalámbrica, ya que no tienen una alta de redundancia ante fallos.

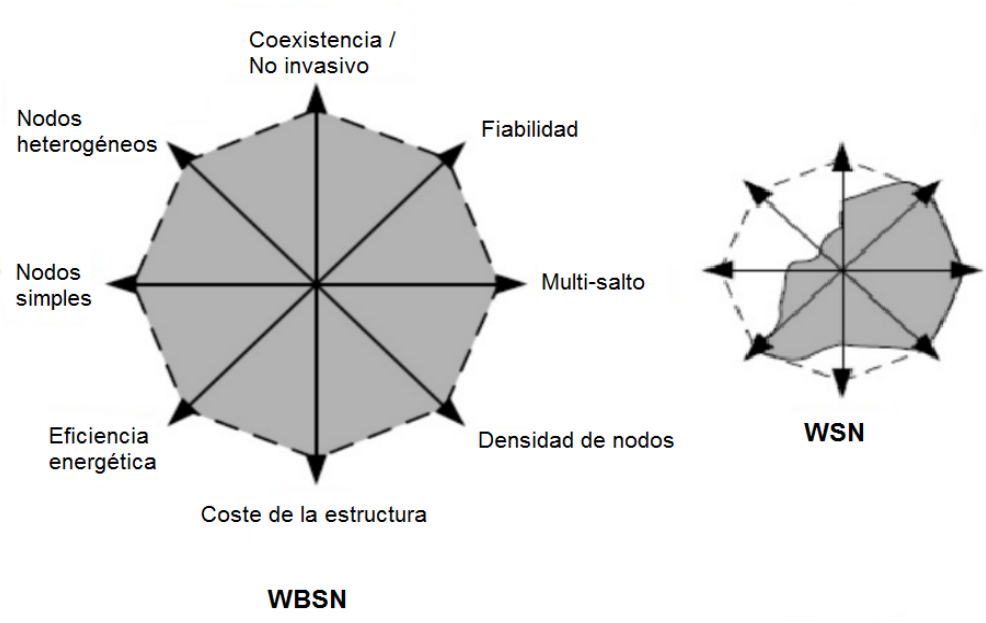

Ilustración 5. Comparativa entre una WBSN y una WSN. Fuente: Propia.

En la siguiente tabla se pueden ver las principales diferencias entre las redes WBSN y las redes WSN.

	Redes de sensores inalámbricas (WSN)	Redes inalámbricas de sensores de área corporal (WBSN)
Escala	Disponen de una amplia área de cobertura (metros o kilómetros)	Cobertura limitada por el cuerpo humano (centímetros o metros)
Número de nodos	Posibilidad de un gran número de nodos	Pocos, limitados por el espacio disponible.
Precisión	Compensada por la redundancia de los nodos	Compensada por la precisión y robustez de los nodos
Funciones de los nodos	Cada nodo dedicado a una única tarea	Cada nodo puede dedicarse a múltiples tareas
Tamaño de los nodos	Preferiblemente pequeños pero no fundamental	Es fundamental que sean pequeños
Topología de la red	Generalmente fija o estática	Más variable acorde al movimiento del cuerpo
Tolerancia ante fallos	Nodos fácilmente remplazables	Los nodos implantados son difícilmente remplazables
Biocompatibilidad	No se tiene en cuenta en la mayoría de las aplicaciones	Necesaria en los implantes y en algunos sensores externos
Obtención de energía	Energía solar, eólica, baterías	Baterías, movimiento corporal, calor corporal
Nivel de seguridad	Bajo	Alto para proteger la información del paciente
Tecnología inalámbrica	Bluetooth, ZigBee, GPRS, WLAN…	Tecnologías de baja potencia

Tabla 1. Diferencias entre WSN y WBSN. Fuente: Propia.

2.2. Estandarización de las WBANs.

En Noviembre de 2007 la asociación de estándares IEEE formó el IEEE 802.15 grupo de trabajo 6 debido al interés y a la necesidad de mejorar las aplicaciones de las redes inalámbricas de área corporal (*Wireless Body Area Networks*, WBAN) al cuidado de la salud [5], y comenzó a operar como tal en Enero de 2008 en Taipei. Se desarrolló "un estándar de comunicación optimizado para dispositivos de baja potencia que operan sobre o alrededor del cuerpo humano (pero no limitado a humanos) para servir a una variedad de aplicaciones incluyendo las aplicaciones médicas, electrónicas de consumo, entretenimiento y otros" [6].

El 6 de Febrero 2012 se aprobó el estándar que regula las BAN, IEEE 802 para redes de área local y metropolitana – Parte 15.6: Redes de área corporal inalámbricas.

El propósito que define este estándar es "proveer un estándar internacional de comunicación inalámbrica de corto alcance (por ejemplo el cuerpo humano), baja potencia, y altamente fiable para usar en la proximidad, o en el interior, de un cuerpo humano. La tasa de datos, normalmente superior a 10Mbps, puede satisfacer una evolución del entretenimiento y servicios al cuidado de la salud. Las actuales redes de área personal (*Personal Area Networks*, PANs) no se puede considerar que estén cerca de las médicas

(no se pueden aproximar al tejido humano) ni a las regularizaciones de la comunicación relevantes para algunas aplicaciones medioambientales. Tampoco soportan la combinación de fiabilidad, QoS, baja potencia, y no interferencias requeridas, por lo general dirigidas a las aplicaciones de redes de área corporal (BAN)" [7].

2.3. Sensores

Los sensores son la parte más importante de una WBSN ya que conectan el mundo físico con los sistemas electrónicos. La principal_finalidad de los sensores dentro de una WBSN es recoger las señales del cuerpo humano procedentes de las actividades físicas o de las condiciones fisiológicas del usuario portador de estos sensores. El número de sensores depende de la aplicación que utilice el usuario final.

2.3.1. Tipos de sensores

Tipos de sensores más apropiados y más empleados en las BSN según algunos investigadores [8-9]:

- ✓ Sensores de movimiento.
  Éstos son principalmente los acelerómetros o giroscopios que se emplean para estimar y monitorizar el cuerpo humano y los diversos patrones de movimiento. Los acelerómetros miden la fuerza gravitatoria y la inclinación, mientras que los giroscopios miden el desplazamiento angular, combinados se puede obtener información acerca de los patrones de movimiento. Esta capacidad es indispensable para multitud de aplicaciones especialmente en el ámbito del cuidado de la salud.
- ✓ Sensores bioeléctricos.
  Este tipo de sensores se utilizan para medir variaciones eléctricas sobre la piel de los pacientes que puede estar directa o indirectamente relacionado con la actividad o situación de un órgano específico. Dentro de este tipo encontramos los electrocardiogramas (EGC), que normalmente tienen forma de almohadillas circulares, y se colocan alrededor del torso y de las extremidades para monitorizar la actividad del corazón y envían la señales cardiacas, los electromiogramas (EMG), que son sensores colocados sobre la piel y mide la capacidad física de los músculos, y los electroencefalogramas (EEG), que son sensores utilizados para monitorizar la actividad cerebral.
- ✓ Sensores electroquímicos.
  Este tipo de sensores generan una salida eléctrica producida por una pequeña reacción entre el agente químico de un sensor y alguna sustancia corporal. Por ejemplo un sensor que mide la cantidad de glucosa en la corriente sanguínea o un sensor que monitoriza la concentración de dióxido de carbono en la respiración.
- ✓ Sensores de presión.

Generalmente los sensores de presión se utilizan para monitorizar cambios de presión en la planta del pie en tiempo real proporcionando un análisis de la presión, un reconocimiento corporal o el gasto de energía. Estos sensores siempre están conectados por cable con un microcontrolador externo.

- ✓ Sensores de presión arterial.
  Son sensores que se ubican en el brazo y miden la fuerza que ejerce la circulación de la sangre por las paredes de los vasos sanguíneos y de las arterias.
- ✓ Sensores ópticos.
  Son dispositivos que emiten y reciben luz tanto en la banda de luz visible como en la banda de infrarrojos y se utilizan para medir la saturación de oxígeno en la sangre de forma no invasiva.
- ✓ Sensores de temperatura.
  Son los sensores más comunes y de un mayor uso cotidiano. Se coloca sobre la piel en diferentes partes del cuerpo para medir la temperatura corporal.
- ✓ Sensores de respiración.
  Estos sensores generalmente están formados por varios de los sensores anteriores, como los sensores de presión, acelerómetros o giroscopios. Estos sensores están continuamente monitorizando al paciente debido a que se utilizan en el tratamiento de enfermedades respiratorias, y obtienen la información detectando la contracción y expansión del pecho o del abdomen.

En términos de la seguridad del paciente los sensores bioeléctricos, por ejemplo, se consideran más importantes que los sensores de temperatura, por lo que estos sensores deben proporcionar una mayor fiabilidad y se les debe dar una preferencia de transmisión ante una situación de falta de los recursos compartidos, como por ejemplo de ancho de banda.

2.3.2. Sensores en el diseño de una BSN

A la hora de diseñar una BSN es necesario tener en cuenta una serie de requerimientos en función de la aplicación para la que vaya a ser utilizada. Es impensable implantar un sensor con un gran tamaño o corrosivo en un paciente. Según su función es mejor utilizar un tipo de sensor u otro [10].

- ✓ Cantidad de datos medidos.
  Existen dos categorías, una formada por los sensores cuya adquisición de datos se realiza a tiempo real, por lo que tienen un gran consumo de potencia y una transmisión de datos muy grande, en este grupo están incluidos los acelerómetros, giroscopios, sensores EEG, sensores EMG y los sensores visuales y auditivos. En la otra categoría se encuentran los sensores que recogen variaciones discretas de las señales fisiológicas, la cantidad de datos transmitidos es mucho menor que los anteriores, aquí podemos incluir los sensores de temperatura, humedad o de

presión en sangre.

- ✓ Posición de los nodos sensor.

  Se puede dividir en dos categorías. Los primeros son los sensores portátiles, como son los sensores de temperatura o presión, en los cuales el tamaño y el peso del sensor deben ser tenidos en cuenta en su diseño. Y los segundos son los sensores implantables, que pueden ser implantados, inhalados o ingeridos en el cuerpo, es fundamental que estos sensores sean pequeños, no corrosivos y biocompatibles.

- ✓ Ajuste automático.

  En función de su capacidad para ajustarse automáticamente se encuentran los sensores que se pueden ajustar automáticamente adaptándose para ofrecer el mejor tratamiento al paciente, y los sensores que no son capaces de adaptarse debido a su diseño más sencillo, son los que se utilizan más habitualmente en las BSNs.

- ✓ En función del medio de transmisión de datos.

  Es necesaria una tecnología de baja potencia debido a que los sensores utilizan el cuerpo humano como medio de transmisión. Es fácilmente integrable en los dispositivos que van situados sobre el cuerpo humano y como la comunicación está construida sobre él la seguridad de la comunicación es mayor que con los sensores de otro tipo de redes de sensores o redes inalámbricas, aunque por otro lado la velocidad de la comunicación es menor que la de un sensor inalámbrico.

2.3.3. Canales de comunicación

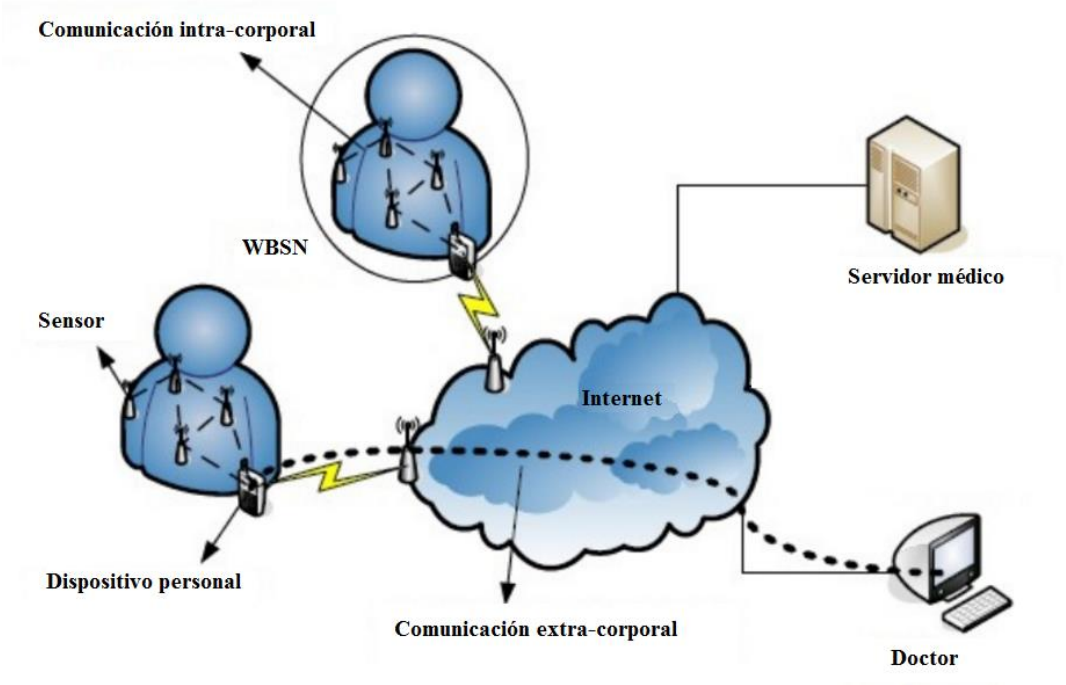

Ilustración 6. Canales de comunicación en un WBSN. Fuente: Introducción a las redes de sensores *http://bit.ly/26zOLka*

El grupo de trabajo IEEE802.15.6 definió tres tipos de nodos:

- ✓ Nodo implantado. Se coloca dentro del cuerpo humano, ya sea en el interior del tejido corporal o inmediatamente bajo la piel.
- ✓ Nodo sobre el cuerpo. Se coloca sobre la superficie de la piel o a un máximo de 2 centímetros de distancia.
- ✓ Nodo externo. No está en contacto directo con la piel (entre unos pocos centímetros y hasta 5 metros de distancia desde el cuerpo).

Se pueden distinguir dos tipos de comunicación dentro de una WBSN, la comunicación intra-corporal y la comunicación extra-corporal. Dentro de la primera se pueden distinguir dos subtipos de comunicaciones, la comunicación entre los sensores corporales y la comunicación entre los sensores corporales y el dispositivo personal. Y el segundo tipo es la que se realiza entre el dispositivo personal y el médico o centro facultativo [11]. Cada una de estas comunicaciones tiene sus propias características.

Canal WBSN intra-corporal	Canal WBSN extra-corporal
Pérdidas adicionales de 30-35 dB más que en el espacio libre	Línea de visión (LoS) / No línea de visión (NLoS)
Las pérdidas de paso aumentan exponencialmente entre 3 y 4 veces según la parte del cuerpo a considerar	Las pérdidas de paso aumentan exponencialmente entre 5 y 6 veces según la parte del cuerpo a considerar
La altura y distancia de la antena también producen pérdidas	En NLoS se producen más pérdidas que en LoS
Se pierden 20 db más a los 5 mm que a los 5 cm	Los movimientos de las ramas pueden causar pérdidas de más de 30 dB

Tabla 2. Diferencias entre el canal intra-corporal y el extra-corporal. Fuente: Propia.

2.3.4. El nodo sensor inalámbrico

El diagrama de bloques de un nodo sensor de un sistema BSN es el siguiente [12].

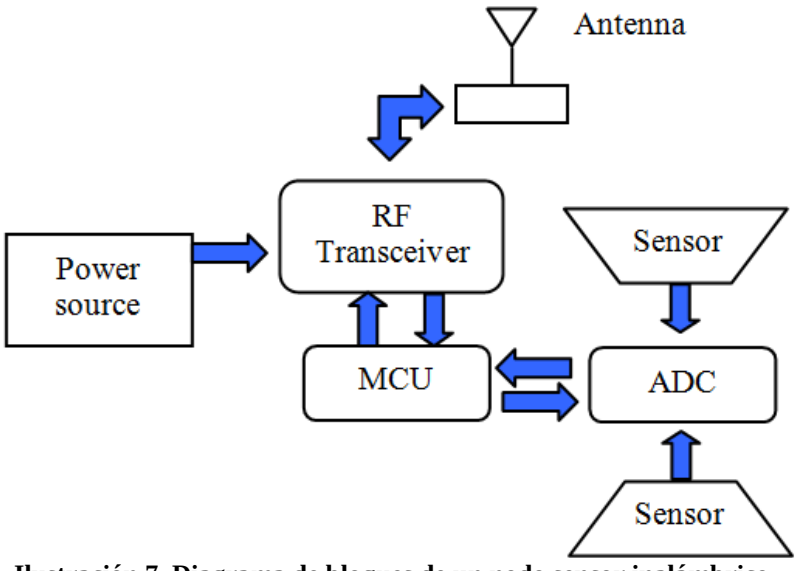

Ilustración 7. Diagrama de bloques de un nodo sensor inalámbrico. Fuente: Propia.

MCU: Es la Unidad Microcontroladora. Recibe órdenes del transmisor de radiofrecuencia (RF) y envía dos señales de potencia control para cada función del nodo sensor. La señal de control de selección de la frecuencia de muestreo la envía el MCU al multiplexor del generador de frecuencia de muestreo variable para seleccionar la frecuencia de muestreo. La administración de energía del MCU se diseña mediante un algoritmo adaptativo de baja potencia, que cambia la función del nodo sensor con cada ciclo de comunicación, y solo consume potencia cuando es usado el nodo sensor. Por ejemplo, en el caso de aplicaciones para medir la temperatura corporal, el controlador de potencia está dormido la mayoría del tiempo y solo pasará a un estado en el que consuma potencia cuando es necesario. En el estado de sueño todas funciones del nodo sensor estarán apagadas a excepción del MCU.

Fuente de alimentación: La mayor parte del consumo de energía se produce en la transmisión de datos, y el menor mientras los sensores están midiendo y durante el procesamiento de los datos. Las baterías son una de las principales fuentes de energía para los biosensores

ADC: El Convertidor Analógico Digital consiste en un modulador, un filtro y un circuito de muestreo. El modulador toma continuamente muestras de voltaje con el fin de detectar las variaciones de las bioseñales y convierte esas lecturas a señales digitales. La señal digital es filtrada a través del filtro digital y muestreada por el circuito de muestreo. Las señales biomédicas pueden ser incrementadas aún más en el ADC, por lo que la banda de ruido puede ser suprimida.

Sensor: Puede ser cualquier tipo de sensor para medir señales biomédicas como los mencionados en el apartado 2.3.1.

Antena: Debe ser adecuada en cuanto al tamaño del sensor, la ganancia, la adaptación de impedancia y la eficiencia, además de tener en cuenta posibles interferencias con otros dispositivos inalámbricos.

2.4. Arquitectura

Como cualquier sistema de comunicación en la actualidad, las redes de sensores de área corporal inalámbricas están formadas por una serie de capas y protocolos que definen como debe realizarse la comunicación. El estándar IEEE 802.15.6 define esas capas y protocolo.

2.4.1. Topología de la red

La topología de la red afecta tanto a las características del sistema, al consumo de energía, a la carga de tráfico y a la robustez de los nodos, como a la elección del protocolo a nivel de enlace y del protocolo de enrutamiento. La topología habitualmente más

utilizada y que define el estándar IEEE 802.15.6 es la topología en estrella. Los nodos, para comunicarse, se organizan de manera que un *hub* controla la comunicación entre ellos y todos los nodos están directamente conectados al *hub* [10].

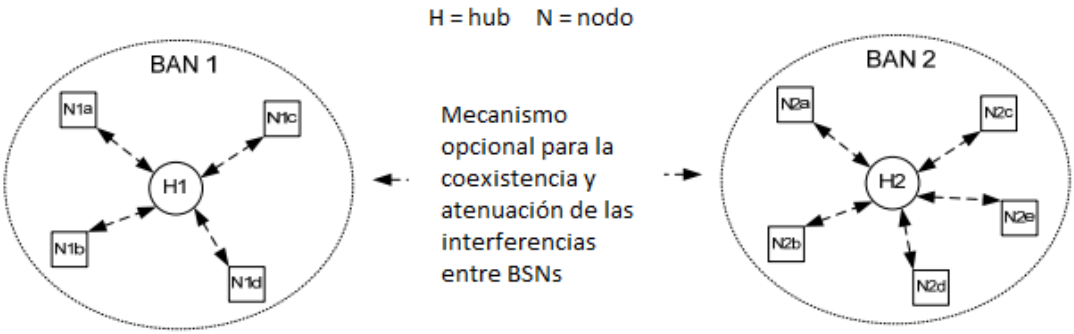

Ilustración 8.Topología de la red BSN definida por IEEE 802.15.6. Fuente: [7].

Aunque esta topología es la más utilizada por su simplicidad cuando no se requiere una comunicación directa entre los sensores tiene algunas desventajas, como la dificultad de los nodos más alejados para comunicarse con el *hub* debido a las limitaciones de energía o los fallos de las conexiones entre los nodos colocados en diferentes partes del cuerpo debido a la baja tasa de recepción de datos.

Una topología más compleja pero más adecuada para las redes multisalto es la topología en malla. Es más robusta y está mejor distribuida, cada nodo necesita una menor cantidad de energía para comunicarse con un nodo vecino y si un nodo falla el resto de la red puede seguir funcionando, por contra punto requiere sensores más inteligentes y consume en conjunto más energía, por lo que es adecuada cuando todos o la mayoría de los sensores necesitan intercambiar datos entre ellos. Una solución que están adoptando algunos investigadores [11] es la topología *cluster-tree* que facilita la comunicación directa entre sensores pero reduce la complejidad de la topología en malla. La comunicación entre los sensores es sencilla porque todos los sensores conocen sus nodos inferiores y su nodo superior, y solo los nodos con acceso a la red requieren una mayor complejidad, además el consumo de energía es menor.

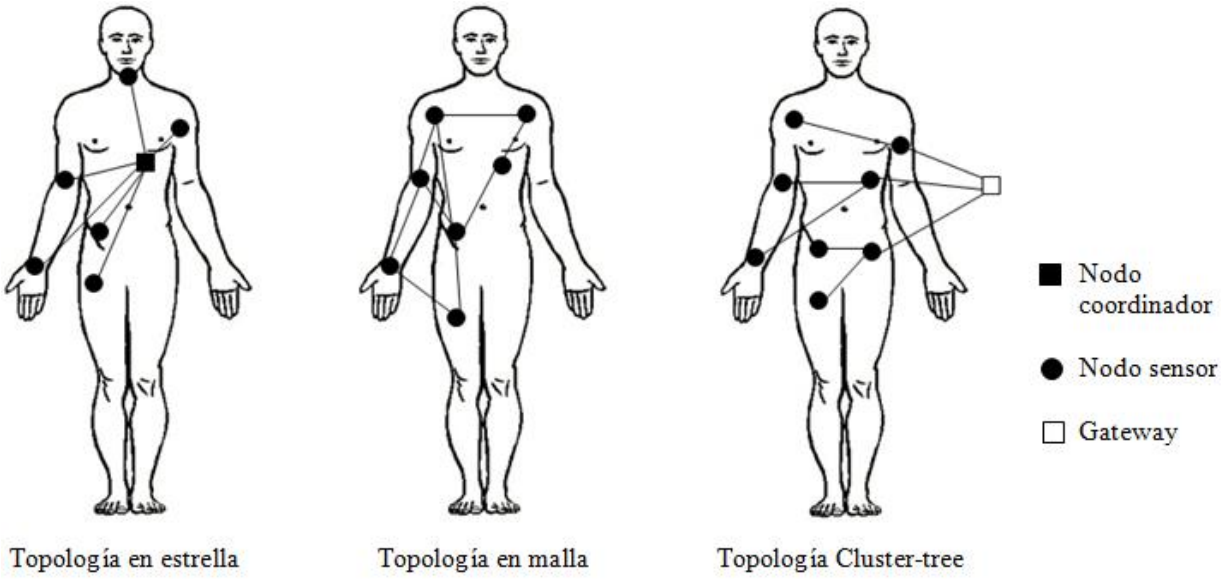

Ilustración 9. Distribución de los sensores en el cuerpo humano. Fuente: Propia.

Sensor	Topología	Velocidad de datos
Acelerómetro / Giroscopio	Estrella	Alta
Medidor de glucosa en sangre	Estrella	Alta
Medidor de presión	Estrella	Baja
Sensor de gas CO2	Estrella	Muy baja
ECG	Estrella	Alta
EEG	Estrella	Alta
EMG	Estrella	Muy alta
Temperatura	Estrella	Muy baja
Video/imagen	P2p	Muy alta

Tabla 3. Topología y velocidad de datos para los distintos tipos de sensores. Fuente: Propia.

2.4.2. Capa física

Es la parte más baja de la estructura de una BSN y es la responsable de codificar y decodificar señales, generar el preámbulo para la sincronización, transmitir y recibir bits y proporcionar la especificación del medio de transmisión. Sus características afectan directamente al comportamiento de la red al completo, por lo tanto una buena elección del canal de transmisión es fundamental. El principal reto de una BSN, con respecto a las redes inalámbricas convencionales, es que el canal en el que ocurre la comunicación es afectado por la proximidad del cuerpo humano, debido a que es un medio dispersivo y con altas pérdidas.

El estándar 802.15.6 especifica tres canales:

2.4.2.1. Canal de banda estrecha (*Narrowband*, NB).

Su función es activar y desactivar los nodos transmisores, la transmisión y recepción de datos a través del canal y estimar un canal libre de transmisión dentro del propio canal.

Durante la transmisión, al servicio de unidad de datos de la capa física (*physical-layer service data unit*, PSDU) se le añade un preámbulo y una cabecera de protocolo de convergencia de la capa física (*phsysical-layer convergence protocol*, PLCP). Después, en el receptor, la cabecera y el preámbulo ayudan a la demodulación, decodificación y entrega al protocolo de unidad de datos de capa física (*physical-layer protocol data unit*, PPDU). El preámbulo es lo primero que debe ir en una PPDU ya que ayuda al receptor durante la sincronización. En segundo lugar va la cabecera que contiene la información necesaria para ayudar a decodificar la PSDU en el receptor. Esta cabecera además de los parámetros de la capa física contiene una secuencia de comprobación (*header check sequence*, HCS), y unos bits de paridad para mejorar la robustez de la cabecera.

El último elemento de una PPDU es el PSDU, que está formado por la concatenación de la cabecera MAC, con el cuerpo de la trama MAC y una secuencia de comprobación de trama (*frame check sequence*, FCS)

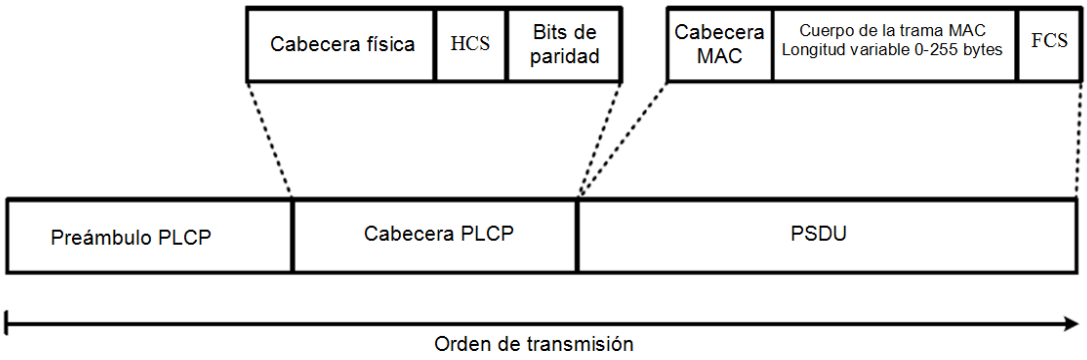

Ilustración 10. Formato de la unidad de datos del canal NB. Fuente: Propia.

Dentro de este canal se engloban cuatro canales que abarcan gran parte del espectro de frecuencias de banda estrecha. *Medical Implant Communications Service* (MICS) [13], es una de las bandas más apropiadas para las redes con baja tasa de datos (402 - 405 MHz). *Wireless Medical Telemetry Service* (WMTS) [14], se utiliza para la monitorización y telemetría inalámbrica de los pacientes en los hospitales proporcionando una gran movilidad pero tiene una gran limitación y es que no está disponible en todo el mundo (420 - 450 MHz, 863 – 870 MHz, 902 – 928 MHz, 950 – 958 MHz). La Comisión Federal de Comunicaciones (FCC) aprobó el uso de la banda de 2360 hasta 2400 MHz debido al interés que presentaba esta banda en el uso de la medicina y las BSNs en particular [11]. Y la *Industrial Scientific Medical* (ISM) [15], es la más utilizada para los sensores implantados y permite una fácil integración con las BSNs (2400 – 2483.5 MHz).

2.4.2.2. Canal de ultra banda ancha (*Ultrawideband*, UWB).

Esta banda está diseñada para ofrecer un rendimiento sólido de las BSNs ya que proporciona un gran margen de posibilidades de aplicaciones de alto rendimiento, robustez, baja complejidad y el funcionamiento de ultra baja potencia. El interés de esta banda radica en el nivel de potencia de la señal que proporciona niveles de potencia de señal seguros para el cuerpo humano y baja interferencia para otros dispositivos, por lo que se puede utilizar para monitorizar la respiración los latidos del corazón de los pacientes. Ofrece, además, una interfaz de datos a la capa MAC bajo el control del protocolo de convergencia de la capa física (*physical layer convergence protocol,* PLCP).

Ofrece tres niveles de funcionalidad. Activación y desactivación de los transmisores de radio, los bits de PPDU son convertidos a señales de radiofrecuencia RF para la transmisión en un medio inalámbrico y proporciona una estimación de un posible canal desocupado para verificar la actividad en un medio inalámbrico.

Existen dos tipos de tecnologías UWB, radio impulso UWB (IR-UWB) y modulación en frecuencia de banda ancha (FM-UWB). En una BSN, el hub debe implementar o un transmisor IR-UWB solo o transmisores IR-UWB y FM-UWB en el mismo hub, por otro lado los dispositivos pueden implementar un transmisor IR-UWB o un transmisor FM-UWB, o ambos.

Tiene dos niveles de operación, el modo por defecto, que se usa en tanto en aplicaciones medicinales como las no medicinales, y el modo de alta QoS que se usa para aplicaciones medicinales con alta prioridad.

Cada PPDU está formado por una cabecera de sincronización (*synchronization header,* SHR), una cabecera de la capa física (*physical layer header,* PHR), y la PSDU.

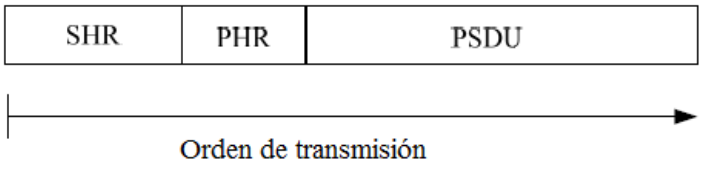

Ilustración 11. Estructura de una PPDU. Fuente: Propia.

La PSDU contiene el protocolo MAC de la unidad de datos (MPDU) y unos bits de paridad para el modo por defecto y el modo de funcionamiento QoS.

Opera en las frecuencias para la banda de bajas frecuencias entre 3244.8 MHz y 4742.4 MHz y para las altas frecuencias entre 6240 MHz y 10233.6 MHz [16].

2.4.2.3. Canal para comunicaciones en el cuerpo humano (*Human Body Communications*, HBC).

Esta banda toma el cuerpo humano como medio de transmisión de datos por lo que solo se utiliza para las BSNs. La banda de operación se centra en 21 MHZ (18.375- 23.625 MHz).

En cuanto a la estructura está formado por un preámbulo PLCP, un delimitador de comienzo de trama (*Start Frame Delimiter*, SFD), una cabecera PLCP, y la PSDU, que está compuesta a su vez por una cabecera MAC, el cuerpo de la trama MAC, y una secuencia de verificación de trama (FCS).

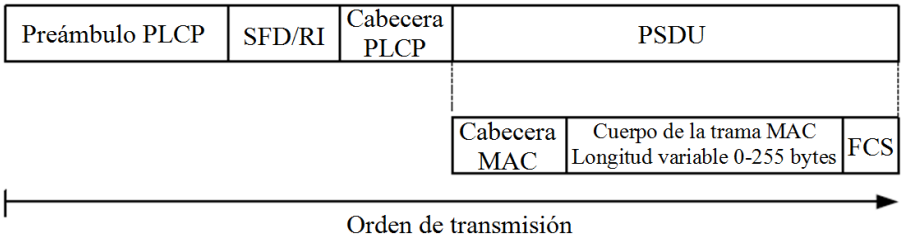

Ilustración 12. Estructura del paquete HBC. Fuente: Propia.

El preámbulo es una secuencia de cuatro tiempos para conseguir la sincronización de paquetes por el receptor.

El campo SFD/RI se usa como delimitador de comienzo de trama (SFD) cuando el envío de paquetes es continuo o como indicador de ratio (*rate indicator*, RI) en el caso del envío de paquetes a ráfagas. Al contrario que el preámbulo, la secuencia SFD se genera solo una vez. Este campo además debe indicar la tasa de transmisión de paquetes cuando se usa en el modo RI. En este modo el receptor puede detectar la velocidad de los datos de los paquetes de entrada sin que sea necesario consultar la cabecera, lo que incrementará la eficiencia de transmisión.

2.4.3. Capa MAC.

La capa MAC es la que permite el acceso al medio de transmisión. Su objetivo principal es conseguir un máximo rendimiento, con un mínimo retardo, maximizando el tiempo de vida de la red de sensores, controlando el gasto de energía producido por colisiones, tiempos de escucha en los que el nodo está inactivo o el coste de los paquetes.

Cada nodo o fuente de datos no genera tráfico al mismo ritmo y en el mismo momento, y debido a que en la mayor parte de los casos es fundamental que la entrega de los datos se produzca a tiempo real una latencia muy alta puede resultar intolerante. Además la transmisión de datos puede debilitarse y puede producirse la pérdida de paquetes debido a los movimientos del cuerpo humano y al medio ambiente. Por esto es

necesario buscar un diseño del control de acceso al medio eficiente, con bajo consumo de energía y fiable.

Para minimizar el consumo de potencia del nodo sensor, la capa MAC debe ser cuidadosamente diseñada para controlar el ciclo de trabajo del módulo RF. Normalmente el protocolo MAC para este tipo de redes opera a ciclos de trabajo muy bajos para alargar el tiempo de vida de los nodos sensores.

Muchos autores han propuesto los siguientes protocolos MAC para las BSN, aunque no se deciden por uno en concreto:

- ✓ Sondeo. Protocolo sin contención pero centralizado. Se produce una alta sobrecarga de la red por los mensajes de sondeo del nodo central al resto de nodos para saber si tienen datos para transmitir.
- ✓ Protocolo flexible basado en sondeo [17]. Se necesita sincronización periódica. El nodo central va preguntando al resto de nodos si tienen datos para transmitir, como en el funcionamiento normal, cuando detecta que hay un nodo tiene datos urgentes para transmitir cambia al modo de operación urgente y le da toda la prioridad.
- ✓ Acceso por sondeo de peso [18]. Los nodos sensores se dividen por grupos y a cada grupo se le da un peso. Cada nodo transmite paquetes según su peso, los nodos con peso más alto podrán transmitir todos sus paquetes pudiendo dejar a los de peso más bajo sin servicio.
- ✓ Protocolos basados en contención o protocolos de acceso aleatorio. Su comportamiento se degrada cuando la carga total del tráfico aumenta.
- ✓ Aloha. Para aplicaciones de baja potencia. No requiere una señal de control centralizada. Mínimo retardo de transferencia para redes de tráfico bajo.
- ✓ CSMA: Para aplicaciones de baja potencia. No requiere una señal de control centralizada. Tienen un mínimo retardo de transferencia para redes de tráfico bajo. Comprueba que el medio esté libre antes de transmitir.
- ✓ CSMA/CA: Además de las características de CSMA, solo permite a un nodo sensor comunicarse y enviar paquetes a la vez. Tiene un bajo retardo de propagación y una buena fiabilidad en redes de tamaño pequeño. Altas probabilidades de colisión en nodo con tráfico alto.
- ✓ Acceso múltiple por división en tiempo (*Time Division Multiple Access,* TDMA). Protocolo sin contención pero centralizado. Necesaria sincronización. El canal se

divide en ranuras de tiempo que se asignan a los nodos. Cada nodo únicamente transmite en su ranura de tiempo.

- ✓ *Heartbeat-Driven* MAC (H-MAC) [19]. Basado en el protocolo TDMA para BSN. Está enfocado a mejorar la eficiencia energética utilizando el ritmo de los latidos del corazón en la sincronización, gracias a que es algo inherente en todos los cuerpos humanos. El ritmo es obtenido por los biosensores detectando los picos de frecuencia de los latidos.

- ✓ *Context-aware* MAC (CA-MAC) [20]. Protocolo híbrido entre los protocolos basados en contención y los protocolos basados en TDMA. Es un protocolo adaptativo que conoce el estado del tráfico de la red y la tasa de transmisión de los nodos en cada momento y lo utiliza para dar la prioridad de transmisión a los nodos según vaya variando el tráfico de peticiones en el medio.

- ✓ *Multi-Dimensional Traffic Adaptive* MAC (MDTA-MAC) [21]. Diseñado para el tráfico multi-dimensional. Minimiza el gasto de energía y el retardo. Utiliza el ciclo de trabajo y el formato de trama de IEEE 802.15.6. La prioridad se da en función del tipo de tráfico.

- ✓ *Distributed Queuing* MAC (WhMAC) [22]. Protocolo de muy baja potencia basado en TDMA. Utiliza las características de las BSN inalámbricas para una transmisión flexible de señales fisiológicas. Los sensores pueden transmitir en función del tipo de sensor y el nivel de emergencia.

El estándar IEE 802.15.6 define tres modos de acceso. Testigo habilitado con super trama, sin testigo habilitado con super-trama y sin testigo habilitado sin super trama. Es el propio mecanismo de acceso al medio el que explica como pueden ser integrados esos tres modos en los nodos sensores.

3. MÉTODOLOGÍA

Este documento es un estado del arte basado en la recopilación de información y la evolución a lo largo de los últimos años de un tema relevante y con mucho recorrido en el campo de las telecomunicaciones enfocado a la telemedicina.

Todo lo aquí expuesto está apoyado en información recogida de artículos obtenidos de diferentes bases científicas, libros especializados en el tema así como páginas web, además de valoraciones propias.

Principalmente las bases científicas en las que se basó la búsqueda por orden fueron:

- IEE Xplore [23].

- Science Direct [24].

- PubMED [25].

Dicha búsqueda se realizó de la red de la Universidad de Valladolid para poder acceder a la totalidad del artículo, en vez de únicamente al abstract. En estas páginas web fue donde se encontró la mayor parte de los artículos científicos. En primer lugar se ha realizado un filtrado por el título del artículo, si parecía enfocado a algún aspecto de los tratados en este trabajo o no, y en segundo lugar por el abstract que en la mayor parte de los casos ha llevado a leer parte o la totalidad del artículo. La mayor parte de los artículos se obtuvieron de la base de datos IEE Xplore, debido a que fue la primera base de datos en la que se buscó, y la mayoría de los artículos se repetían en las otras bases de datos.

Inicialmente la búsqueda fue general, para tener una idea global de cuál es situación en la que se encuentran actualmente las redes de sensores de área corporal. Buscando por los términos BSN y BAN. De estas búsquedas solo se han utilizado los artículos científicos enfocados a la telemedicina. La mayoría de los artículos eran actuales por lo que se ha realizado una búsqueda más avanzada para encontrar los artículos más antiguos, y se ha observado que la cantidad de información disminuía considerablemente.

La ilustración 13 presenta, en función del año de publicación, los artículos revisados para este trabajo.

Después se realizó una búsqueda avanzada según las diferentes secciones en las que se quería enfocar el trabajo. Inicialmente, cómo son los sensores y cuál es la mejor distribución sobre el cuerpo humano, además de cómo se debe estructurar esta red de telecomunicaciones y como se transmite la información.

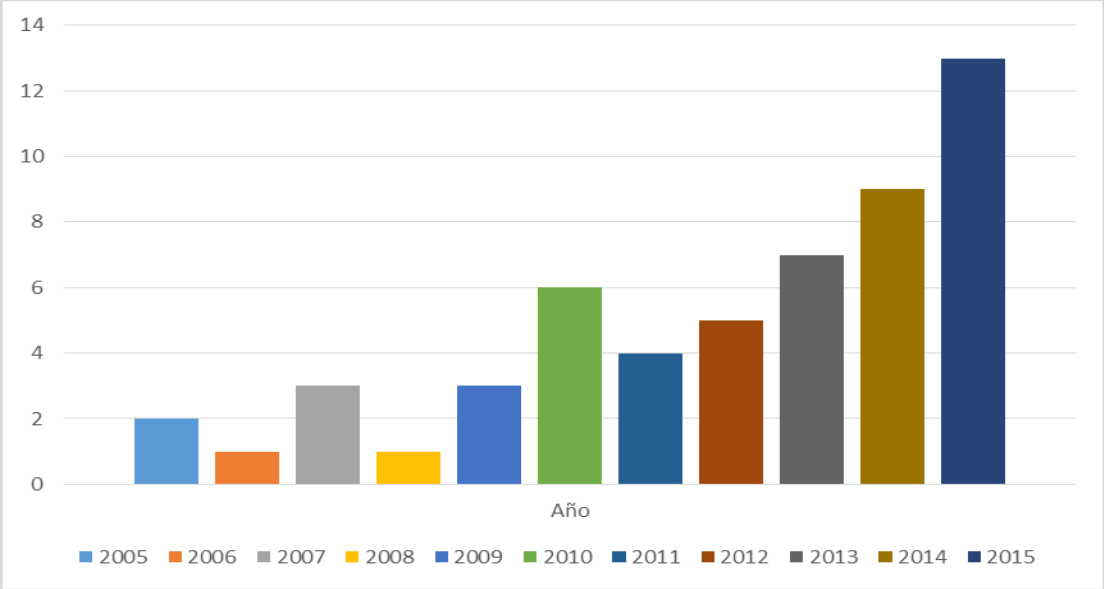

Ilustración 13. Número de artículos revisados por año de publicación. Fuente: Propia.

Durante esta búsqueda se percibió la importancia de la seguridad en estas redes de sensores de área corporal, tanto en cómo se debe encriptar la clave y los distintos mecanismos para evitar la vulneración de los datos, como en la importancia de la fiabilidad y la robustez de la red para que ninguna información se pierda en la transmisión. Por lo que tiene un gran peso en este documento.

A continuación se representa el número de artículos científicos obtenidos en función de las distintas secciones del documento.

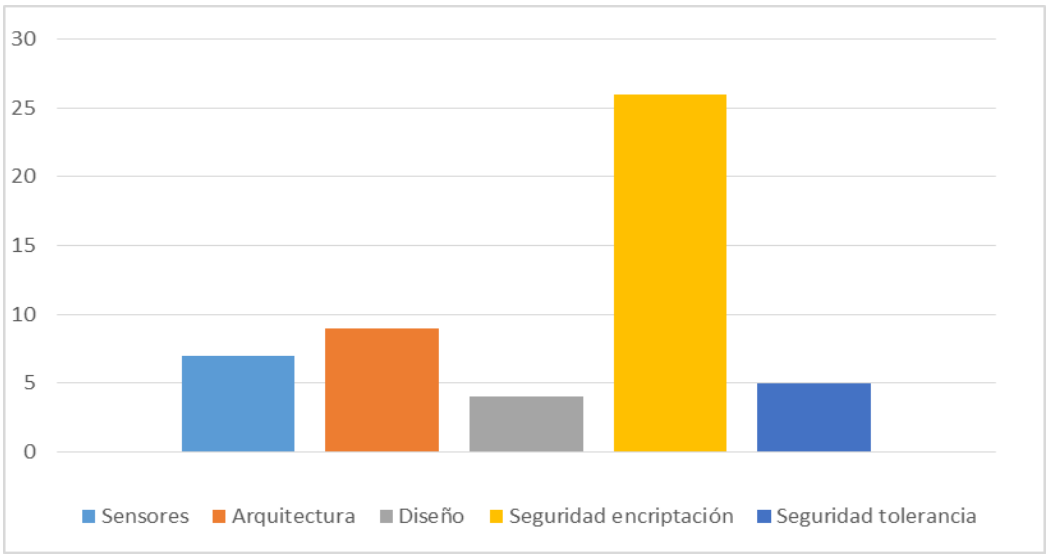

Ilustración 14. Número de artículos revisados en función del contenido. Fuente: Propia.

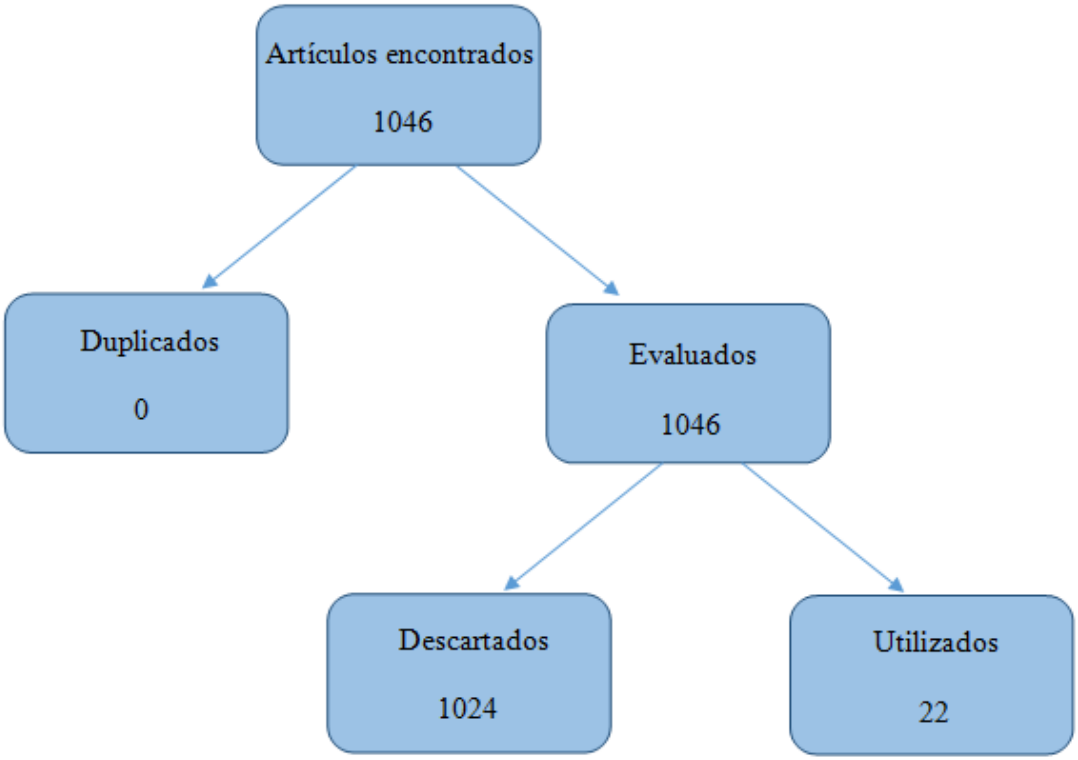

Ilustración 15. Diagrama de flujo de los artículos revisados de la base de datos IEEE. Fuente: Propia.

Ilustración 16. Diagrama de flujo de los artículos revisados de la base de datos Science Direct. Fuente: Propia.

Ilustración 17. Diagrama de flujo de los artículos revisados de la base de datos PubMed. Fuente: Propia.

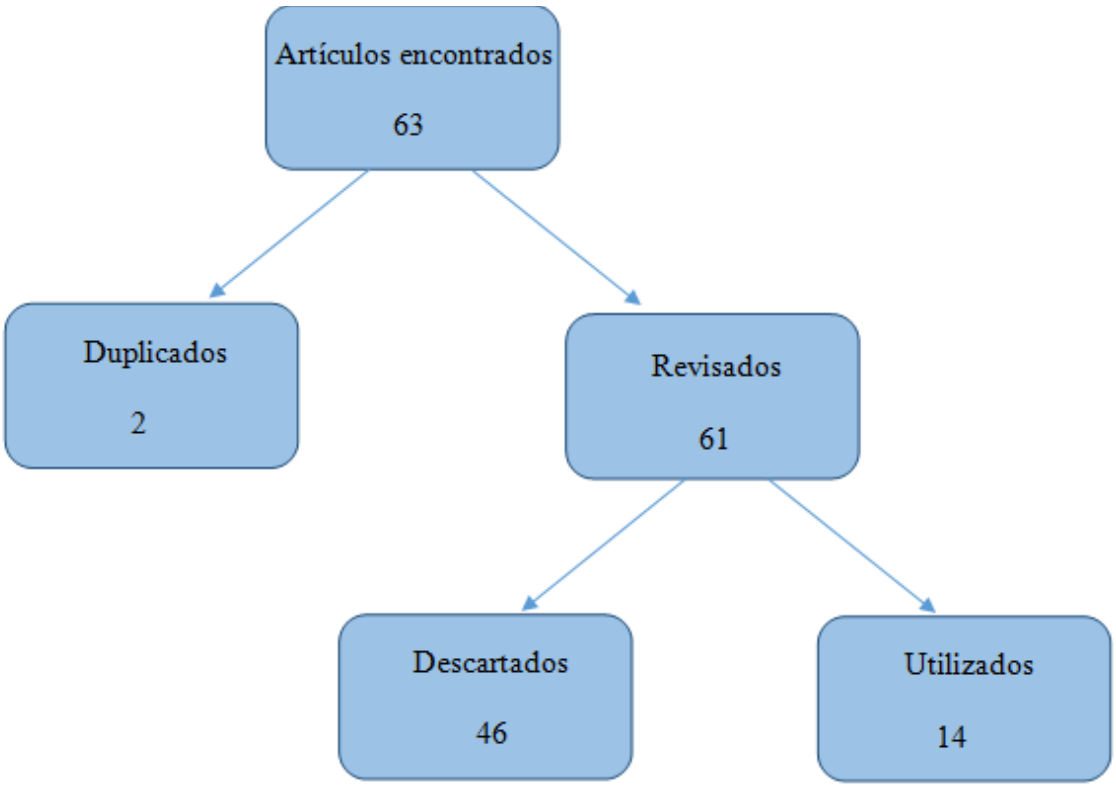

Ilustración 18. Diagrama de flujo de los artículos revisados de otras bases de datos. Fuente: propia.

Este trabajo se divide principalmente en dos grandes apartados. En el primero se estudia en que consiste una BSN, como son los sensores que la componen, su funcionamiento, arquitectura y sus capas de transmisión. En el siguiente apartado se tratan los aspectos relacionados con la seguridad de una BSN, cómo debe ser encriptada la información para que no esté expuesta a posibles violaciones de seguridad y cómo evitar que haya fallos en el envío de información entre los nodos y que ésta no se pierda debida a un fallo de transmisión. Por último se exponen las conclusiones finales y posibles investigaciones futuras.

4. RESULTADOS: SEGURIDAD EN REDES BSN

¿A dónde van a parar nuestros datos cuando se aceptan las condiciones de uso de una aplicación? A pesar del control estricto de los datos sanitarios a los que están sujetos los aparatos de telemedicina suministrados por los hospitales, el abuso está a la orden del día. Y cuando esto ocurre, los datos y la información no pueden cambiarse como si de una cuenta bancaria se tratase puesto que muchas enfermedades son para toda la vida. Los datos médicos, personales e intransferibles, son muy codiciados por los *hackers,* se paga por ellos diez veces más que por los datos de las tarjetas de crédito. En 2014 fueron robados datos de casi 80 millones de clientes a la aseguradora Anthem [26]. Y según expertos en seguridad el 20% de las aplicaciones que requieren crear una cuenta transmiten las contraseñas sin encriptación lo que permite que cualquier atacante pueda tener acceso a los datos.

Desde el momento en el que son recogidos y almacenados o enviados a otro nodo receptor los datos son expuestos a todo tipo de violaciones, lo fundamental que debe ser tenido en cuenta a la hora de realizar un buen diseño de una BSN son los mecanismos de seguridad. Puesto que una BSN trata con los datos personales de la salud de los pacientes una BSN segura debe proporcionar privacidad, confidencialidad, integridad y soportar tanto la autentificación como la autorización.

No es una tarea sencilla proporcionar todos estos requerimientos debido a la limitación de la potencia de procesamiento, la energía y la memoria, además, hay que tener en cuenta que la mayor parte de los usuarios no son expertos en el uso de estas redes de sensores, la vida útil de los dispositivos y la itinerancia de los nodos sensores. También es importante que tengan una buena tolerancia ante cualquier fallo, si un sensor se pierde o deja de funcionar debe poder ser remplazado fácilmente sin que esto afecte a la integridad del sistema completo.

4.1. Criptografía.

Desde que los datos médicos son recogidos por los sensores, la seguridad y la privacidad se convierten en elementos fundamentales de una BSN debido a que los datos se asocian directamente a un paciente en particular, además, los datos deben ser fácilmente accesibles ante una emergencia por el personal cuyo acceso esté permitido. Todo esquema que proporcione cualquiera de las características fundamentales frente a la seguridad como son la autentificación, la confidencialidad o la encriptación debe ser diseñado de manera que asegure una baja carga computacional y un bajo consumo de potencia debido a las sobrecargas, minimizando el número de mensajes intercambiados y utilizando el menor número de operaciones computaciones criptográficas.

4.1.1. Caso de ejemplo.

Para entender mejor la importancia y la necesidad de la criptografía en las redes

BSN se propone un escenario como caso de ejemplo [27].

- Alicia lleva una BSN que monitoriza y recoge los datos de su electrocardiograma cuando ella está fuera de casa. Un día, Alicia se desmaya y la llevan a un hospital para atenderla, por lo que los datos recogidos por la BSN deben estar almacenados de forma que puedan ser fácilmente accesibles ante una emergencia.

- Después del incidente, Alicia enseña a su BSN a recoger algunos datos adicionales. A Alicia le gustaría que su información estuviese restringida solo a algunos médicos en una emergencia. Sin embargo, no puede predecir qué médico o en qué hospital será atendida, y a lo mejor no está capacitada físicamente en ese momento para autorizar a ningún doctor. Un esquema seguro de una BSN debería ser capaz de tolerar este tipo de situaciones.

- Con todos los datos almacenados, se puede hacer muy tedioso acceder solo a los datos que el doctor necesite para curar a Alicia ante una emergencia. Por lo que una BSN debe ser capaz de limitar el acceso a los datos recogidos, incluso cuando son acumulados en un espacio público de almacenamiento.

- La familia y los amigos de Alicia están preocupados por su estado de salud, así que para tranquilizarlos, a Alicia le gustaría que algunas personas tuviesen acceso a alguna parte de los datos recogidos por la BSN. Un buen esquema de seguridad debe tener la suficiente flexibilidad para permitir que Alicia pueda permitir el acceso adicional a quien ella elija.

4.1.2. Requerimientos de privacidad y seguridad.

✓ Proteger la privacidad del paciente desde el lugar de almacenamiento de los datos, no solo porque los datos puedan ser borrados sino que también se intente aprender el contenido de los datos de los pacientes.

✓ Que la tolerancia de los sensores de una BSN no se vea comprometida. Ya sea por un sensor perdido o robado, un sensor de una de BSN no debería permitir que alguien no autorizado obtenga datos del paciente.

✓ Prevenir el acceso no autorizado a la información. El mismo doctor debería poder acceder a unos datos sí y a otros no si no es autorizado. Además debe asegurar que los datos recibidos vengan de un sensor real y no sea un señuelo ya que los tratamientos y decisiones médicas están basadas en información recibida de esos nodos.

✓ Asegurar la integridad de los datos. Esto permite la verificación de los datos. Los datos no deben ser alterados ni modificados durante la transmisión ya que una

alteración no autorizada de los datos puede provocar un diagnóstico erróneo.

- ✓ Flexible en la concesión de permisos. El paciente puede decidir permitir el acceso a sus datos a distintas personas y generar distintas claves para cada acceso.

4.1.3. Autenticación.

La autenticación es una parte fundamental de una BSN ya que es una garantía que asegura la identidad a los nodos en los que se produce la comunicación. Cada nodo debe tener la seguridad de que los paquetes que recibe proceden de un emisor real, seguro y confiable, puesto que, por mucho que la red esté provista de un buen sistema de encriptación de datos, si el sistema no es capaz de asegurar que todos los nodos pertenecen a la misma BSN y no hay ningún intruso, la red no será confiable. El intercambio de los datos de autenticación entre el paciente y el hospital se debe producir antes de comenzar el tratamiento, para no permitir el acceso a los datos del paciente o al tratamiento, e incluso evitar un cambio de las dosis o del procedimiento del tratamiento por parte de personal no autorizado. Además de una autenticación entre paciente y hospital, deberá realizarse una autenticación entre hospitales en el caso de que el tratamiento se fuera a llevar a cabo por más de un doctor o personal médico de distintos centros.

La pregunta es simple, ¿Cómo los nodos sensores dentro de una BSN pueden saber que está asociados al mismo individuo y no hay ningún nodo intruso? La solución que inicialmente se planteó, y que en la actualidad se sigue teniendo en cuenta, fue utilizar las señales biométricas que proporciona el cuerpo humano. Ya en el 2005, Bao *et al* [28], propusieron un esquema de autenticación basado en biométricas, en el que se utiliza la información extraída de las señales fisiológicas para proporcionar una verificación e identificación mutua entre los sensores de una BSN. En concreto, y debido a que las señales fisiológicas como la huella dactilar o el patrón del iris utilizadas en otros sistemas de encriptación no son válidas ni seguras para las BSN ya que no varían con el tiempo, en este estudio se utiliza la alteración del ritmo cardiaco como señal fisiológica. Las características únicas y totalmente aleatorias de estas señales proporcionan una comunicación segura. De este modo, dos sensores, que se intentan comunicar, colocados en diferentes partes de la misma persona tendrán una copia independiente pero simultánea de esta característica biométrica, si el sensor no pertenece a la misma persona, esta medida tendrá una diferencia significativa. Más tarde, en [29], utilizaron esta misma idea generando la señal biométrica a partir del intervalo entre pulsos (IPI), estudiando, además, la tasa de rechazo falsa (FRR), en la que un nodo puede rechazar a otro que pertenece a la misma BSN, y la tasa de aceptación falsa (FAR), en la que un nodo puede aceptar a otro que no pertenece a su BSN.

En esta misma dirección surgió la idea de utilizar el electrocardiograma (ECC) como señal biométrica [30], debido a su naturaleza más estable en un largo periodo de tiempo, a

que no requiere un esfuerzo computacional adicional y a sus características únicas de robustez que combinan factores simpáticos y parasimpáticos del cuerpo humano. Esta idea ha sido ampliamente aceptada en los últimos años, y ya en el año 2015, Shen *et al*, basándose en este tipo de autenticación, propusieron un esquema en el que es necesario una autenticación en tres pasos. En primer lugar entre el paciente y el personal sanitario para resistir los posibles ataques maliciosos de intrusos cuando el doctor está fuera de servicio o el sensor del paciente no funciona correctamente. En segundo lugar debe ser una autenticación mutua entre los sensores médicos y el ordenador o dispositivo utilizado por el doctor. Y en tercer lugar entre cada par de sensores, para facilitar añadir o eliminar sensores o renovar la clave de grupo [31].

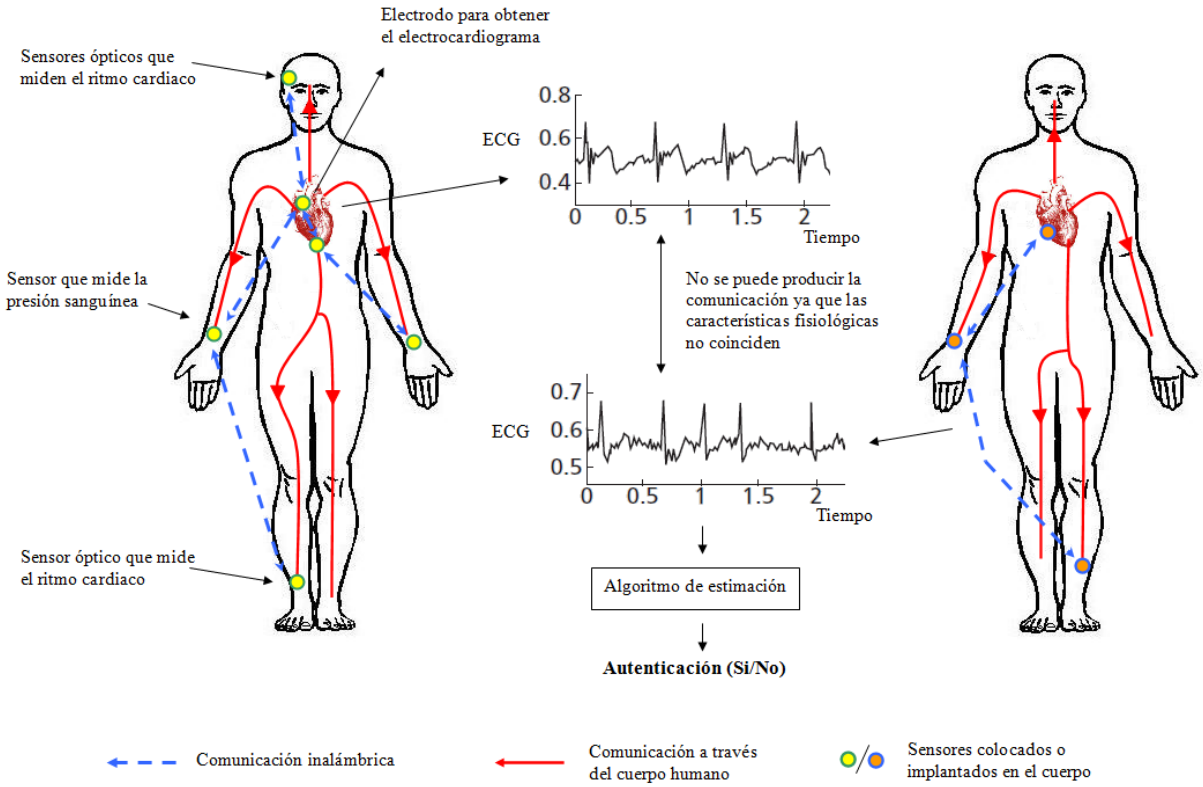

Ilustración 19. Autenticación mediante la comparación de ECG. Fuente: Propia.

Una autenticación segura y eficiente debe constar de una serie de fases. Inicialización, registro, identificación y autenticación mutua [32], [33]. Una identificación eficiente, confidencialidad directa o la actualización de una contraseña segura proporcionadas en [32], a través de un esquema de establecimiento de canales entre el servidor de autenticación del paciente en el hospital y el servidor de autenticación del propio servidor, hacen que este tipo de esquemas resistan de una forma más efectiva los ataques criptográficos. Basándose también en una autenticación a través de canales multisalto, Shi *et al* en el año 2015, consiguieron reducir la tasa de falso positivo. Con su

esquema integrado en la capa física y que se basa en los movimientos corporales se reduce el hardware subyacente mejorando su simplicidad [34].

Por otro lado, poco a poco las redes BSN están empezando a formar parte de la nueva era de las tecnologías y de la información, lo que está llevando a adaptar estos esquemas de autenticación a este tipo de usos. Debido al amplio uso de los teléfonos móviles, que cada vez son más utilizados en aplicaciones sanitarias e incluso en las redes BSN, es fundamental un buen esquema que proporcione una autenticación segura entre el teléfono móvil y los nodos de una BSN. Cuando un nodo sensor médico conecta por primera vez a una BSN debe registrarse en el teléfono enviándole un mensaje encriptado, y gracias a un Código de Autenticación de Mensajes (MAC) éste podrá verificar su identidad [35]. En otras ocasiones la monitorización se realiza a través de capsulas ingeridas por el paciente, la mayor parte de las veces en estos casos es necesario además el envío de imágenes y videos, por lo que se necesita una autenticación multimedia y en tiempo real [36].

4.1.4. Integridad de los datos.

La integridad de los datos asegura la originalidad de los datos cuando viajan a través de una comunicación inalámbrica entre los nodos de una BSN. Las señales fisiológicas recogidas por los sensores se envían a un servidor personal, que recoge todas las señales de los sensores, y, después, a una red externa para diagnóstico remoto. La importancia de la privacidad en estas redes radica en que al ser información médica personal es necesario proteger estos datos fisiológicos de escuchas indebidas, inserción de información no autorizada y modificaciones.

La mayoría de los autores afirman que una buena integridad de los datos forma parte del sistema de encriptación, por lo que estos esquemas funcionan globalmente proporcionando tanto la autentificación, la integridad de los datos, la confidencialidad y la encriptación. Otros autores apuestan por un concepto conocido como esteganografía para las redes BSN [37], [38]. Mientras que el objetivo de la criptografía es proteger el contenido de los mensajes, la esteganografía intenta ocultar el mensaje secreto cuando es colocado en el medio de transmisión encubriéndolo y así evitar que sea detectado, por ejemplo en una imagen encubierta. Por otro lado, Miao *et al* (2009) proponen un diagrama de bloques [39] en el que se utiliza el modo de cifrado de flujo del estándar de encriptación avanzada (AES) generando un código de autentificación de mensajes (MAC) para la protección de la integridad de los datos, que además minimiza el consumo de energía y el tamaño de memoria.

Debido a que los nodos sensores donde se almacenan los datos son susceptibles de ataques contra su integridad física, en [40] se muestra un diseño en el que una buena integridad debe proporcionarse desde el mismo lugar de almacenamiento de los datos. Su objetivo es proporcionar un diseño que garantice la integridad física de la información

fisiológica de una forma dinámica, es decir, que la integridad de los datos de los pacientes pueda ser revisada por los propietarios de los datos compartidos o por los usuarios autenticados dinámicamente.

Siguiendo este concepto y sin dejar de tener en cuenta los nuevos sistemas de almacenamiento que han surgido en los últimos años algunos autores ya ha comenzado a investigar el sistema del almacenamiento en la nube. Es un método muy efectivo para el almacenamiento de datos de forma que estos sean accesibles en cualquier momento y lugar. He *et al* [41] en el año 2015 proporcionaron una solución efectiva para chequear la integridad de los datos de forma remota en la nube sin necesidad de descargarlos.

4.1.5. Encriptación.

Inicialmente se desarrollaron nuevos sistemas de encriptación debido a que los que existían para las redes inalámbricas de área personal (WPAN) y las WSN no cumplían los requisitos para las BSNs, en cuanto a seguridad, tamaño y peso. Se necesitan en los sensores mecanismos de seguridad ligeros que mejoren la seguridad, reduzcan el espacio de almacenamiento y disminuyan el consumo de energía, sobre todo en los sensores implantados.

Según la HIPAA (la ley de responsabilidad y de la portabilidad de la seguridad de la salud), la encriptación puede ser opcional en las comunicaciones con una red segura, sin embargo cuando la información es transmitida por una red abierta como Internet debe ser encriptada.

Existen dos tipos de encriptación y ambos son estudiados para su utilización en las redes BSN, la criptografía simétrica y asimétrica. En la mayoría de los esquemas en los que la distribución de la clave se produce de manera simétrica los sensores necesitan pre compartir secretos, lo que no es nada conveniente cuando los secretos necesitan ser actualizados. Por otro lado, aunque se pueden utilizar la criptografía asimétrica en las redes de sensores es complicado distribuir las claves públicas de forma segura.

A continuación se van a ver los esquemas de encriptación con mayor aceptación en las BSN para el cuidado de la salud

4.1.5.1. Criptografía de curva elíptica (ECC).

La criptografía de curva elíptica (ECC) surgió como una opción viable para la criptografía de clave pública en las redes inalámbricas de sensores gracias a su rápida computación, a su pequeño tamaño y a su baja carga computacional. Sin embargo, más tarde se vio que no era la mejor opción para las BSN debido a que los requerimientos de energía necesarios eran mucho más altos que los sistemas simétricos [32].

Sin embargo, gracias a su alta seguridad se sigue implementando para la

autenticación, generación y mantenimiento de la clave. En la ECC la clave pública es un punto en la curva y la clave privada es un número aleatorio. La clave pública se obtiene de multiplicar la clave privada con el punto generador *G* en la curva, los parámetros de la curva del punto generador *G* junto a una serie de constantes forman el principal parámetro de la ECC [39]. Este protocolo consta de una cuatro de fases, la primera es la fase de inicialización constituida principalmente por cuatro entidades, la autoridad de certificación (CA), el sensor, el acumulador de datos y el doctor o experto que utilizará esos datos. La CA se utiliza para la inicialización del sistema, elige la curva elíptica *E* para generar *P* a partir de un *E* de orden *n* y un entero aleatorio *d*. Se construye la clave pública del CA de forma $Q=dP$. El acumulador de datos es el dispositivo móvil que se utiliza para el almacenamiento de los datos de los paciente y que realiza la operación $Q_i = d_iP$, donde Q_i es la clave pública y *d* es la clave privada. Y el doctor es el que realiza la operación $Q_u=d_uP$, donde Q_u es su clave pública y d_u es su clave privada. Por lo que resultaría imposible obtener las claves privadas de cada uno tanto para el otro sensor como para un intruso.

En la fase de registro o de asociación con un nodo seguro, el acumulador de datos muestra su código de identificador Id a la CA para registrarse, es en esta fase donde se produce la autenticación. La tercera fase es la verificación e intercambio de la clave, donde el acumulador de datos ya puede intercambiar información con doctor o enfermero. Y por último la fase de administración de miembros, en el que se pueden añadir nuevos nodos, eliminar algún nodo (cuando esto ocurre la clave de grupo debe ser regenerada teniendo en cuenta el nodo que fue borrado) y actualizar la representación compacta de la cadena, ocurre por ejemplo al añadir un nuevo nodo [31].

- ECDH – Curva elíptica de Diffie Hellman [42].

  Es un protocolo para el establecimiento de la clave en el que dos partes que quieren intercambiar datos pueden utilizar la clave pública para crear la clave privada. Ambas parte comparten alguna información pública y usan esos datos públicos y sus propios datos privados para calcular el secreto compartido.

  1. A calcula $K=(X_K,Y_K)=d_A * Q_B$
  2. B calcula $L=(X_L,Y_L)=d_B * Q_A$
  3. Como $d_AQ_B = d_Ad_BG = d_Bd_AG = d_BQ_A$, entonces $K=L$ y por lo tanto $X_K=Y_K$
  4. El secreto compartido es X_K

  Es prácticamente imposible averiguar la clave privada a partir de la clave pública, lo que también hace imposible que una tercera parte descubra el secreto

compartido.

- ECDSA – Curva elíptica con el algoritmo de firma digital [42].

  Se utiliza el algoritmo de la firma digital para autenticar un dispositivo o un mensaje enviado por un dispositivo. Al igual que el ECDH como está basado en curva elíptica, cada nodo tiene dos claves, una privada d_A y una pública Q_A. Consta de dos etapas, la generación de la firma, en la que además de la clave pública y privada utiliza la función *hash*, y la verificación de la firma, en la que para que B pueda autenticar la firma de A, éste debe conocer la clave pública de A.

4.1.5.2. Esquema Fuzzy Vault.

El esquema Fuzzy Vault es el más ampliamente utilizado por su simplicidad y a la vez su alto grado de seguridad proporcionado en la redes BSN. Está basado en la idea de que las señales biométricas que genera en un momento dado una persona son altamente similares, mientras que las que señales que se generan en otro momento o por otro individuo son significantemente distintas. Con los esquemas de encriptación tradicionales un sensor que pertenezca a la misma BSN pero por la distancia o los propios movimientos corporales reciba una señal cuya medida no sea exactamente igual a la medida del resto de sensores no será aceptado en esa BSN. Lo que nos proporciona este esquema es un es un cierto grado de tolerancia y flexibilidad para así reducir en gran medida la falsa probabilidad de rechazar un sensor que pertenezca a la misma BSN.

El funcionamiento de encriptación del Fuzzy Vault que inicialmente se propuso consiste en "cerrar" (de forma que quede oculto) un conjunto de los datos medidos de manera que este secreto solo pueda ser abierto por otro conjunto de datos que coincida en gran parte con el primer conjunto de datos. Este esquema muy utilizado en los sistemas biométricos tenía algunos puntos débiles al aplicarlos a las redes BSN. En el 2010, Miao *et al* propusieron una modificación a este esquema para reducir las pequeñas diferencias producidas por los patrones aleatorios entre los identificadores biométricos [43], de forma que la información transmitida contiene versión transformada pero nunca una copia exacta de la señal biométrica, lo que impide escuchas indebidas. En contra de este estudio, Cao *et al* (2011) en [44] afirma que en [43] se consigue reducir la tasa de error de falsa aceptación y de falso rechazo a costa de reducir el nivel de seguridad, algo que es inaceptable cuando se trata del cuidado de la salud.

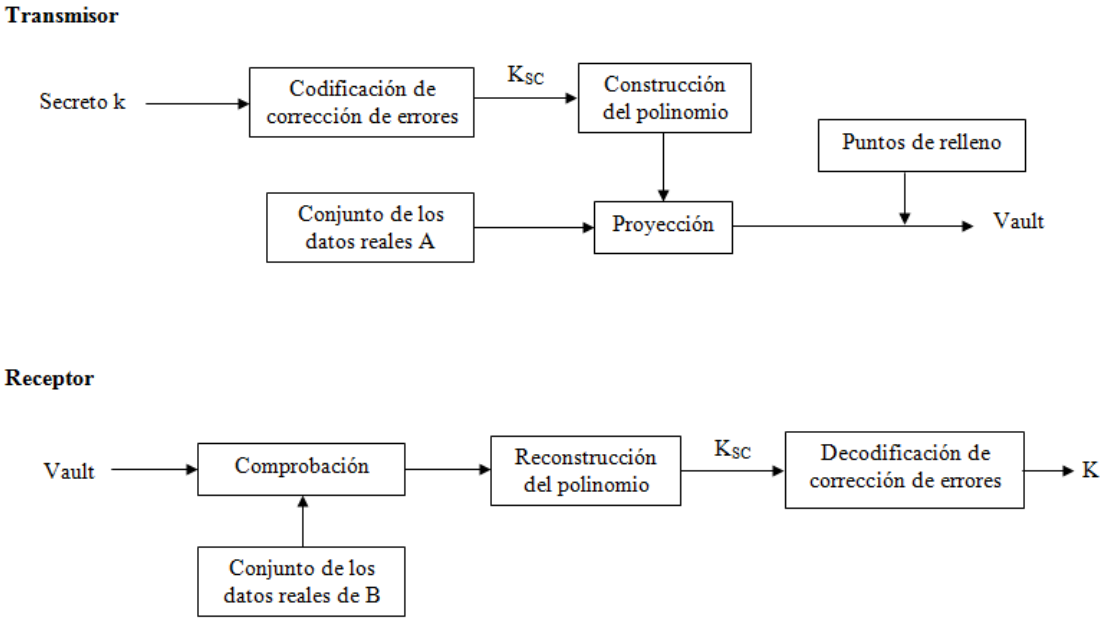

Ilustración 20. Diagrama de bloques del esquema Fuzzy Vault. Fuente: [45].

El funcionamiento de este esquema consiste en la codificación de la clave secreta *K* para formar la clave secreta codificada *Ksc*. Con los coeficientes obtenidos de esta clave se construye el polinomio con el que se construirá la proyección formada por el polinomio y un conjunto de los datos reales. Por último se le añaden unos puntos de relleno generados aleatoriamente y ya estaría generado el vault. Para poder acceder a los datos se debe reconstruir el polinomio con el conjunto de datos del receptor, solo se podrá descodificar la clave si el conjunto de datos del receptor coincide en gran parte con el conjunto de datos del emisor [45], cuantos más puntos de relleno se utilicen en la construcción del vault mayor será la seguridad. En [46] se muestra un método de reconocimiento de nodos para mejorar la seguridad de una BSN, en el que el diseño del vault se realiza en el espacio de dos dimensiones con la codificación código Gray.

La biométrica más utilizada, como ya se explicó en el apartado de autenticación, es el IPI, puesto que la información se puede obtener fácilmente de múltiples señales fisiológicas, como puede ser de un electrocardiograma o una fotopletismografía (PPG), con los que se pueden generar los identificadores de entidad (EIs) con el objetivo de mejorar la seguridad, el reconocimiento de los nodos y la protección de la clave.

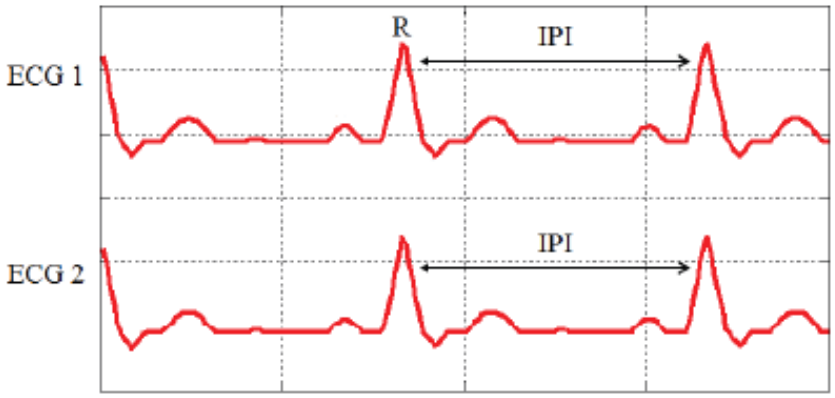

Ilustración 21. Intervalo inter-pulsos (IPI) generado por la distancia entre dos picos R consecutivos [45].

El requerimiento fundamental que debe tener todo EI utilizado en la seguridad de las BSN es su completa aleatoriedad, aunque también es importante tener en cuenta la singularidad del identificador a tiempo real y la similitud síncrona [43].

El estudio de Zheng *et al* (2015) compara el esquema Fuzzy Vault, en el que la biométrica utilizada es directamente el valor IPI, con el esquema Fuzzy Commitment, en el que la biométrica se obtiene de la generación de secuencias binarias aleatorias de los valores IPI de un ECG [45] . Por un lado, el fuzzy commitment es un esquema más complicado a la hora de obtener las medidas de EGC, pero por el otro la ocultación y revelación de la clave es mucho más sencillo que el fuzzy vault. Un aspecto fundamental que tratan estos esquemas y no puede dejarse de lado, es la FAR y la FRR. Mientras que la FRR es comparable en ambos esquemas, la FAR es superior en el fuzzy commitment frente al fuzzy vault. Este estudio llega a la conclusión que desde el punto de vista del cálculo y reconstrucción del polinomio es más adecuado el fuzzy vault, mientras que desde la perspectiva de la complejidad computacional el esquema fuzzy commitment es más adecuado sensores ligeros de una BSN.

4.1.5.3. Señal fisiológica basada en acuerdos de claves (PSKA).

Este esquema utiliza la información de las señales fisiológicas en el dominio de la frecuencia para generar los EIs, y junto con el esquema fuzzy vault implementa la distribución de la clave en una BSN. El propósito de PSKA es facilitar la comunicación segura entre sensores permitiendo que dos sensores se comuniquen a través de una clave simétrica acordada entre ellos procedente de las señales fisiológicas [44], [47]. Por un lado utiliza el esquema fuzzy vault para la codificación de la clave y generación del polinomio. Por otro utiliza su propio esquema para el intercambio del vault y confirmación de las fases, lo que complica la obtención de la clave a los adversarios. Si un sensor malicioso

intenta intercambiar un mensaje vault, replicando intercambios anteriores o creando su propio vault utilizando características fisiológicas anteriores, será descartado por el MAC en el receptor. El número de puntos de relleno que utiliza es mucho mayor que el conjunto de datos reales (un 3%), por lo que sin la clave resultará imposible desbloquear el mensaje [47].

Para mejorar la resistencia del esquema PSKA contra ataques a la seguridad, surgió el esquema llamado Características fisiológicas ordenadas basada en acuerdos de claves (OPFKA) [48]. Es un protocolo seguro, eficiente y viable que consigue un alto nivel de seguridad con una baja carga computacional, que además ofrece un consumo de energía menor en comparación con PSKA. Las características generadas por cada sensor son ordenadas en un vector y solo el sensor que recoge los datos sabe el orden, éste envía los datos con una gran cantidad de ruido al receptor, que genera una clave de acuerdo con las características comunes y devuelve los índices de dichas características. Por último el emisor identifica las características comunes en su propio vector y calcula la clave acordada.

4.1.5.4. Comunicaciones de luz visible (VLC).

VLC es una avanzada tecnología de comunicación óptica inalámbrica que utiliza el espectro de luz visible como medio de transmisión de los datos. VLS es menos peligroso para la salud de los humanos y proporciona una mayor seguridad puesto que la luz no puede atravesar las paredes. Este protocolo tiene muchas ventajas en cuanto a las BSN dedicadas al ámbito de la salud puesto que se pueden utilizar sin ninguna condición extra ya que es soportado por la mayor parte de las BSN, y además no necesita intercambiar secretos pre compartidos [49].

La modulación preferida en este tipo de esquemas en la modulación *on-off keying* (OOK) [50], también conocida como modulación en amplitud. El funcionamiento básico es el siguiente. Primero se transmiten las claves de seguridad a través de unos canales de radio inalámbricos, sin embargo los atacantes pueden bloquear la comunicación y modificar esas claves. Para prevenir los ataques que puedan ocurrir se utilizan las VCLs para verificar esas claves, por ejemplo transmitiendo una representación compacta de los mensajes transmitidos por los canales, como los usuarios pueden ver de dónde procede una comunicación VLC a los atacantes les será más complicado bloquear y modificar el resumen del mensaje transmitido. Utilizando en el receptor el resumen del mensaje se puede verificar que las claves de seguridad no han sido modificadas.

Este esquema tiene muchas expectativas de vista a un futuro en las BSN, puesto que los LEDs, los sensores de luz y las cámaras necesarios para las VLC se encuentran en la mayoría de los teléfonos móviles y los nodos sensores.

4.1.5.5. Encriptación basada en atributos (ABE).

El esquema de encriptación basada en atributos es muy adecuado para encriptar los mensajes cuando no se conoce con exactitud la identidad del receptor. Por ejemplo en una emergencia médica es posible que el paciente no sepa que doctor, enfermero o incluso hospital le va a atender. Este diseño proporciona un esquema de control de acceso detallado, en el que los datos médicos son encriptados por atributos y únicamente los atributos que satisfagan la estructura de acceso de la clave podrá descifrarlos. Los atributos son las identidades. A pesar de no conocer el personal médico por el que va a ser atendido, el paciente puede especificar los atributos para satisfacer la estructura de acceso y así puedan tener acceso a los datos.

La estructura del control de acceso se crea mediante un árbol de acceso y al texto cifrado se le asocian unos los atributos. Cada nodo no-hoja tiene asignado un nivel umbral y cada nodo hoja se etiqueta con atributos. Un usuario solo podrá descifrar el texto encriptado y acceder a los datos médicos si tiene asociado atributos para ese nivel o superior. Solo podrán tener acceso a los datos si los atributos asociados con el texto cifrado satisfacen la estructura de acceso de los usuarios [51].

Shanthi propone una nueva versión de este esquema en el que se toma en cuenta la información almacenada en un servidor a parte como puede ser un servidor en la nube [52]. Utiliza un registro personal de la salud (PHR) que decide cómo encriptar la información y que grupo de usuarios puede tener acceso a esa información. De esta forma cada usuario puede tener diferentes privilegios de acceso en relación con el PHR al que pertenezcan.

Tipo de criptografía	Tipo de clave	Esquema	Ventajas	Desventajas
Simétrica	Clave privada	Fuzzy Vault	Obtención sencilla de las medidas de ECG. Proporciona una alta seguridad.	Mayor complejidad computacional que otros esquemas.
Simétrica	Clave privada	PSKA	Se suele utilizar el electrocardiograma para medir la señal. No necesita inicialización ni un despliegue previo.	No es capaz de reordenarse ante la presencia de nuevos sensores.
Simétrica	Clave privada	OPSKA	Obtiene el vector de sensores de forma dinámica. No necesita inicialización ni distribución de la clave.	Los sensores maliciosos no detectados pueden comprometer a los sensores de una BSN.
Asimétrica	Clave pública	ECC	Puede conseguir el mismo nivel de seguridad que RSA con claves más pequeñas.	Muy complejo. La implementación práctica provoca un gran gasto computacional.
Asimétrica	Clave pública	VLC	Minimiza las interferencias y el consumo de energía a través de canales de luz invisibles.	Posible fallo si algo obstaculiza la comunicación entre fotodetectores (sombras). Absorción atmosférica.
Asimétrica	Clave pública	Sistemas biométricos	Mejora la seguridad. No existe el error ni el fraude a la hora de autenticarlos.	No es fácil su utilización en cualquier lugar.

Tabla 4. Comparativa de los diferentes tipos de encriptación. Fuente: Propia.

4.2. Tolerancia ante fallos

Las BSNs a menudo requieren un alto grado de fiabilidad y unos requerimientos mínimos de latencia para algunos mensajes específicos respecto a la monitorización a tiempo real de la salud. Cuando ocurre un fallo en una BSN, la mayoría de las aplicaciones esperan que una buena fiabilidad les permita seguir operando con normalidad. El sistema debe tener la capacidad de seguir recogiendo información y, más tarde, enviar el aviso al nodo correspondiente para solucionar el fallo. Si por el contrario los datos no pueden ser enviados, debido a una congestión en la red o a un cambio en la topología, el sistema debe ser capaz de tomar una rápida decisión y redirigir la información por un camino seguro, si no el paciente se podrá ver perjudicado o dañado. El número de errores en cuanto a la

adquisición de datos, por lo tanto, debe ser lo más pequeño posible, así como el retardo de propagación.

Por otro lado nodos tan pequeños implican baterías de menor tamaño que los sensores utilizados habitualmente en otros tipos de redes, lo que provoca estrictas limitaciones de la energía que se consume en el procesamiento de los datos, en el almacenamiento y en los recursos de la comunicación. El resultado de la pérdida de paquetes en la trasmisión de datos, debido a que la capacidad de almacenamiento de un biosensor suele ser muy limitada, implica que los datos a menudo tengan que ser reenviados, algo que consume mucha energía y provoca que el nodo comience a fallar. Todo ello hace que en algunos casos los datos críticos no puedan ser transmitidos a los nodos de control a tiempo, lo que posiblemente provocará fallos en el diagnóstico de los pacientes por parte de los doctores.

4.2.1. Fallo en el diagnóstico.

Diferentes movimientos del cuerpo humano no tienen por qué tener el mismo desplazamiento ni consumir la misma energía. Por ejemplo andar o correr implica un desplazamiento coordinado de los brazos y las piernas, sin embargo levantarse o sentarse implica un desplazamiento vertical de los brazos, de la cabeza y de las piernas, así que comparar la energía de cada nodo para detectar nodos defectuosos no es lo más adecuado. Otro escenario en el que es difícil detectar un nodo defectuoso se produce cuando la mayoría de los nodos tienen una actividad muy baja mientras que otros son altamente activos, por ejemplo un paciente que esté tumbado o en una posición de descanso pero en un momento dado mueva un brazo o el pecho provocará que unos nodos transmitan una gran actividad, siendo datos correctos, mientras que otros transmitirán muy baja o ninguna actividad, lo cual también son datos correctos. Asegurar una buena tolerancia ante fallos en este tipo de escenarios requiere un gran número de nodos desplegados por el cuerpo humano, lo que dificultaría la vida diaria del paciente, además de necesitar una batería mayor y del incremento de las interferencias por la gran cantidad de sensores [53].

A su vez, diferentes tipos de datos fisiológicos tienen diferentes requerimientos de fiabilidad. Como ya se explicó en el apartado 3.3.1., los sensores que miden la frecuencia cardiaca se suelen considerar más importantes que los sensores de temperatura o de presión sanguínea, por consiguiente el nivel de fiabilidad debe considerarse de forma dinámica en función del estado en el que se encuentre el paciente. Mientras las lecturas del sensor se encuentren en un rango en el que se consideren normales, la presión sanguínea puede tener un nivel de fiabilidad bajo, pero cuando el sensor indica hipotensión o hipertensión los biosensores deben ser capaces de proporcionar un nivel de fiabilidad mucho más riguroso para que se pueda realizar un diagnóstico adecuado.

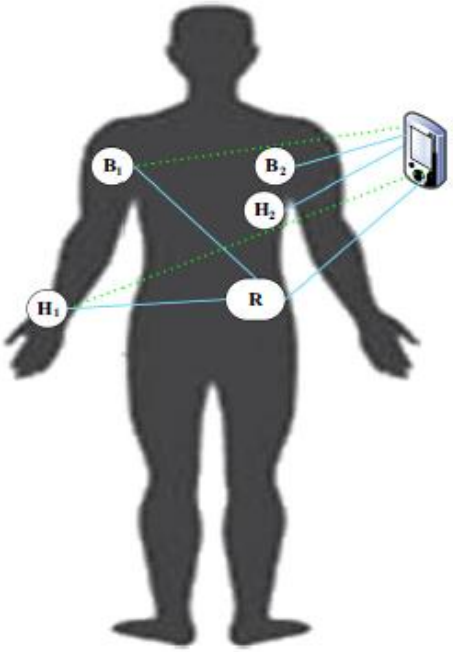

Ilustración 22. Ejemplo de un sistema BSN para la monitorización de pacientes. Fuente: [54].

En la ilustración 22 se puede ver un ejemplo de un sistema BSN para la monitorización de un paciente. En este caso la presión sanguínea se mide a través de los nodos B_1 y B_2, y el ritmo cardiaco a través de los nodos H_1 y H_2. El nodo de transmisión (R) se utiliza para transmitir los datos obtenidos por los sensores B_1 y H_1 al dispositivo desde donde más tarde el doctor o centro médico podrá acceder a los datos [54]. En este ejemplo para poder realizar un diagnóstico correcto se requieren tanto las medidas de la presión sanguínea como el del ritmo cardiaco y así evitar que con solo una de las medidas se obtenga un diagnóstico erróneo.

Para reducir las falsas alarmas y prevenir fallos en el diagnóstico se debe detectar las medidas defectuosas que se hayan producido en los sensores, todo ello antes de que los datos sean transmitidos. Sin embargo no es posible distinguir si los datos están bien o son erróneos si sus valores están dentro del rango normal, únicamente se podrán detectar fácilmente aquellos que tengan errores obvios. En [55] se puede advertir, al igual que en el ejemplo anterior, como diferentes señales fisiológicas del cuerpo humano llegan a tener cierta relación, por lo que los datos recogidos por los diferentes tipos de sensores deben satisfacer esas relaciones.

4.2.2. Fallo en los sensores.

La mayoría de los sensores son micro sistemas electro-mecánicos que pueden fallar y llevar a diferentes tipos de errores. Las salidas erróneas procedentes de los nodos que han fallado pueden llevar a una interpretación equivocada o a falsas alarmas innecesarias.

La presencia de anomalías, ya sean intermitentes, transitorias o permanentes, y la posibilidad de que estos fallos estén relacionados entre sí hace que se deban considerar dos tipos de fallos en los componentes de una BSN.

- ✓ Fallos importantes. Incluyen la presencia de nodos defectuosos, la pérdida de la comunicación inalámbrica o una batería agotada.
- ✓ Fallos ligeros. Son causados por un ruido excesivo seguramente provocado por un mal contacto o un mal funcionamiento de los componentes de un sensor.

En la mayoría de los sistemas reales, el 80% de los fallos son fallos intermitentes. Los fallos intermitentes son un caso especial de los fallos transitorios cuando estos se originan desde dentro del sistema debido a que el software o el hardware es defectuoso. Después de su primera aparición suelen volver a producirse con cierta frecuencia, e incluso algunas veces se llega a hacer permanente. Por otro lado los fallos transitorios suelen ser causados por agentes externos como la radiación electromagnética o el calor, y normalmente sus efectos desaparecen relativamente rápido. La mayor parte el mal funcionamiento de los sistemas suele venir de fallos transitorios, así que reemplazar los nodos sensores implicados no suele ser la mejor solución si esto no ocurre de manera muy frecuente.

4.2.3. Pérdida de datos.

Hay una gran cantidad de factores que pueden causar el retardo o la pérdida de una pequeña parte de los datos medidos, los defectos de hardware, las interferencias de comunicación o las condiciones medioambientales son algunos de ellos. Para que ocurra una comunicación con éxito es muy importante que los nodos sensores no alteren el comportamiento de los pacientes que los llevan. El tamaño y la portabilidad producen grandes limitaciones de hardware, como resultado los nodos suelen disponer de una pequeña batería con una cantidad de energía de procesamiento y memoria limitada y una comunicación inalámbrica a corta distancia. Por lo tanto se puede definir el tiempo de vida de una red en términos de consumo de energía. Es preferible disminuir la cantidad de energía consumida por los nodos sensores e incrementar el tiempo de vida del sistema tanto en su funcionamiento normal como en la recuperación ante fallos. Otra manera de prolongar el tiempo de vida de un nodo sensor es activar únicamente el número de sensores que sean necesarios en cada momento para la monitorización.

Lo principal es preservar la integridad computacional, esto se realiza gracias a las copias de seguridad de los datos cuando el enlace que ha fallado restablece la comunicación. La copia de seguridad de los datos se puede almacenar localmente o en otros nodos de manera inalámbrica. A nivel de consumo de energía almacenar los datos de

forma local implica un gasto menor que de forma inalámbrica.

Se pueden encontrar dos tipos de fallos.

- ✓ Fallos de corto alcance. Este tipo de fallos en el enlace de transmisión pueden ser resueltos por los nodos locales sin que sea necesario transmitir ningún tipo de dato a la red de almacenamiento.
- ✓ Fallos de largo alcance. Son los fallos que los nodos locales no pueden tratar y es necesario reenviar la copia de seguridad de los datos a un destino alternativo para preservar la integridad de los datos.

Todos los fallos se clasifican inicialmente como fallos de corto alcance y los datos se almacenan al comienzo del enlace que falla. Si se produce el caso de que se agota la memoria del nodo, el enlace se clasifica como fallido y comienza el proceso de recuperación del enlace mientras el resto de la red sigue funcionando con normalidad. Cuando un nodo ya no puede recuperar la copia de seguridad de los datos, el fallo es reclasificado como un fallo de largo alcance. En estas situaciones los nodos necesitan colaborar para encontrar la mínima cantidad de datos que deban ser almacenados en los destinos alternativos con el menor coste en la comunicación.

4.2.4. Fallo en el medio de transmisión.

Cuando se produce un fallo en la transmisión, Wang *et al*, en el año 2015, demuestra que se puede aislar los sensores implicados en la transmisión con una cierta probabilidad, dependiendo de si la energía restante puede permitir al nodo transmitir directamente al dispositivo encargado de recoger toda la información medida de los sensores, también conocido dispositivo de acumulación [54]. Un sensor biomédico puede transmitir la información fisiológica percibida al dispositivo de acumulación o entregar la información a través del nodo de transmisión, dependiendo de la distancia entre el sensor y el dispositivo de acumulación. Cuando el nodo de transmisión sufre un fallo, el sensor biomédico puede ser aislado de la transmisión (por ejemplo llegando a ser aislado del resto del sistema BSN) con una cierta probabilidad, dependiendo de si la energía restante del último nodo le permite alcanzar largas distancias, transmitiendo directamente al dispositivo de acumulación. Según este estudio todos los sensores biomédicos que transmiten información a través del nodo de transmisión tienen una dependencia probabilística funcional con el nodo de transmisión.

Hay dos tipos de fallos que pueden ocurrir entre los componentes de una BSN, los fallos locales y los fallos de propagación. Un fallo local no solo causa daños al componente que ha fallado sino que también se extienden a otros componentes de la BSN. Este tipo de fallos puede inutilizar la transmisión y la función de percibir del sensor. Cuando se produce

un fallo de propagación que hace que el sistema entero falle se le considera un fallo de propagación con efectos globales. Este último tipo de fallo puede ocurrir tanto en sensores biomédicos como en los nodos de transmisión y se dan en situaciones en las que se producen ataques de interferencias que hacen que el sistema entero falle.

Al igual que en [54] en [56] se demuestra como los fallos están sujetos a un cierta probabilidad. La diferencia en este caso está en que toma el intervalo de tiempo transcurrido entre dos muestras para calcular la probabilidad de detectar si la transmisión ha fallado o no. Si este periodo es demasiado grande la probabilidad de que se produzca más de un fallo aumenta, y si es demasiado pequeño los sensores medirán con más frecuencia lo que incrementará el gasto de energía. Gracias a este esquema se pueden detectar los sensores que están defectuosos, además muestra cómo afecta el diseño del parámetro del intervalo de tiempo al sistema y cómo se minimiza la sobrecarga al ejecutar el algoritmo de diagnóstico propuesto.

Wu *et al*(2010), en el artículo [57], propone un esquema adaptativo llamado AFTCS en el que estudia una estrategia para la reserva del ancho de banda del canal cuando se produce un fallo en el canal de transmisión y así mantener la fiabilidad en la trasmisión de los datos. La reserva del ancho de banda se realiza a partir de la información percibida del estado fisiológico de la persona, el entorno que le rodea y del estado del sistema.

Este esquema tiene en cuenta tres aspectos, los fallos relacionados con la información recogida, la tolerancia ante fallos en el tratamiento de la prioridad de la cola y la reserva de recursos del canal basado en la prioridad de la cola. Los biosensores recogen los datos fisiológicos y los fallos que se produzcan relativos a esa información (fallo hace referencia a toda aquella medida que no se encuentre en rango establecido como normal) y los envían al nodo de control. El nodo de control analiza esos fallos y cambia dinámicamente la prioridad de los sensores encargados de la tolerancia ante los fallos, que se encarga de distribuir los recursos del canal entre los sensores para reducir los desperfectos del canal. Para garantizar la prioridad a los sensores críticos cuando los recursos del canal son escasos la prioridad de los fallos de tolerancia se ajusta dinámicamente. El nodo de control mide el ancho de banda disponible constantemente, y cuando se produce una deficiencia en el canal la reserva de éste la realiza en tres pasos, el primero consiste en medir el ancho de banda efectivo, el segundo en el cálculo de los requerimientos del ancho de banda y por último la distribución del ancho de banda en función de la prioridad. Este esquema proporciona una menor latencia y pérdida de paquetes para sensores que requieren una gran fiabilidad.

5. CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones.

5.1.1. Conclusiones generales.

Tras finalizar el trabajo de fin de grado son varios los aspectos a tener en cuenta en el apartado de conclusiones en cuanto al estado actual de las redes de sensores corporales, sobre todo en el largo camino que aún les queda por recorrer.

En primer lugar cabe destacar cómo en los últimos años ha crecido la confianza de las personas en las nuevas tecnologías, tanto en los dispositivos como la cantidad de opciones que nos proporcionan en nuestra vida diaria. Algo con gran relevancia debido al envejecimiento que se está produciendo en la sociedad actual, a los malos hábitos de vida e incluso a la gran contaminación de las ciudades que lleva un importante aumento del número de enfermedades crónicas. Unido a esta situación también se encuentra una sociedad joven sumergida en el mundo de las aplicaciones móviles que cada día se preocupa más por el cuidado de su salud.

En segundo lugar es importante mencionar el gran futuro que tienen este tipo de redes en el ámbito sanitario, tanto en el control y diagnóstico de las enfermedades como en la forma de proceder en los novedosos tratamientos que van apareciendo cada día. Con su interoperabilidad y su ubicuidad facilitan el diagnóstico a los médicos y reducen el número de desplazamientos de los pacientes proporcionándoles una gran libertad en su vida diaria.

Por último, no se puede dejar de lado el gran reto que presentan aún estas redes en cuanto a la reducción del tamaño de los sensores y de la red en su conjunto, sin perder parte de su funcionalidad ni de su calidad.

Con este trabajo se ha querido dar una visión actualizada y demostrar la gran viabilidad que tienen las redes BSN en el ámbito sanitario de manera que sirva como punto de partida en el desarrollo y mejora de los dispositivos, nodos y sistemas de comunicaciones personales y portátiles que existen en la actualidad.

5.1.2. Conclusiones sobre la seguridad de las BSNs.

Tras realizar el estudio de cómo los problemas respecto a la seguridad afectan a las redes BSN y a los esquemas y soluciones propuestos por diferentes autores podemos llegar a las siguientes conclusiones:

- En cuanto al tipo de seguridad, hay una gran diferencia en el número de autores que han estudiado la seguridad en la encriptación que los autores que buscan una mejora de la tolerancia de la red ante fallos, lo que se aprecia en la gran cantidad de artículos propuestos de cara a la encriptación.

- Dentro de la seguridad proporcionada por la encriptación de la red, el principal

objetivo es buscar esquemas de comunicación en los que los datos estén seguros de manera que solo puedan ser accesibles por la persona o personas que el paciente desee.

- En cuanto a la funcionalidad del sistema, la seguridad pasa por una buena recuperación del sistema cuando ocurren ciertos fallos que pueden provocar que la información no llegue a su destino.

En el ámbito personal, este Trabajo Fin de Grado me ha ayudado a descubrir la importancia de la telemedicina y cómo las nuevas tecnologías pueden estar muy ligadas al ámbito sanitario y a ver cómo esta unión puede facilitar la vida de tantas personas.

5.2. Líneas futuras.

Al concluir este trabajo he visto ciertos aspectos de mejora de las BSN, como es el desarrollo de redes menos invasivas para el cuerpo humano, además de cuál es la mejor topología de forma que si se produce un fallo de la red el sistema no quede aislado y todos los nodos puedan seguir comunicándose o la difícil elección cuando se produce una emergencia para detectarla o decidir si únicamente es un movimiento corporal para no provocar un fallo de diagnóstico.

Por otro lado, faltan mecanismos de seguridad para el almacenamiento de los datos en la nube. Es un sistema de almacenamiento cada vez más utilizado ya que evita ocupar espacio físico de los dispositivos y, actualmente, un significante número de personas ya poseen una cuenta en algún sistema de almacenamiento de este tipo. Esto implica mejorar la seguridad de encriptación y de autenticación, puesto que si la información no se encuentra en el dispositivo transportado por el paciente los datos son más vulnerables.

Como ya he visto durante la realización de este trabajo, almacenar los datos de forma inalámbrica aumenta el consumo de energía respecto al almacenamiento local. Para que el punto anterior sea más factible, este gasto de energía debe ser disminuido de manera que la duración de la batería no se vea afectada. De esta forma se evitarán fallos en la transmisión que afecten a la fiabilidad de la red.

Con los avances tecnológicos los sensores tienden a ser cada vez más microscópicos y adaptables al cuerpo humano, estos sensores y dispositivos algún día formarán parte de nuestra rutina diaria, y lo que actualmente nos parece algo utópico espero que en pocos años llegue a ser algo común para todos.

6. REFERENCIAS

[1] Informe mundial sobre la diabetes http://bit.ly/22esx2d (Último acceso 25/04/2016)
[2] ¿Qué son las enfermedades cardiovasculares? http://bit.ly/1DH8jUT (Último acceso 25/04/2016)
[3] P. Honeine, et al "Wireless Sensor Networks in biomedical: Body Area Networks," 7th International Workshop on Systems, Signal Processing and their Applications (WOSSPA), pp. 388-391, 2011
[4] Diseñan un tatuaje digital que controla el flujo sanguíneo de forma constante http://bit.ly/1NLtXuu (Último acceso 15/04/2016)
[5] J. H. Kurunathan, "Study and overview on WBAN under IEEE 802.15.6", U.Porto Journal of Engineering, pp. 11-21, 2015
[6] IEEE 802.15 WPAN™ Task Group 6 (TG6) Body Area Networks http://bit.ly/1py95k0 (Último acceso 07/02/2016)
[7] IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks http://bit.ly/1rcD2Yk (Último acceso 07/02/2016)
[8] Campaña Bastidas, Sixto Enrique, and Jorge Mario Londoño Peláez. Estudio De Redes De Sensores Y Aplicaciones Orientadas a La Recolección Y Análisis De Señales Biomédicas. Universidad Industrial de Santander, 2013
[9] E. Jovanov, A. Milenkovic , C. Otto, PC. de Groen," A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation", Journal of NeuroEngineering and Rehabilitation, 2005
[10] X. Lai, Q. Liu, X. Wei, W. Wang, G. Zhou and G. Han, "A Survey of Body Sensor Networks", Sensors (Basel), pp. 5406–5447, 2013
[11] R. de Francisco and A. Pandharipande, "Spectrum occupancy in the 2.36–2.4 GHz band: Measurements and analysis", Proc. 16th EW Conf., pp. 231-237, 2010
[12] S. L. Chen , H. Y. Lee , C. A. Chen , C. C. Lin and C. H. Luo , "A Wireless Body Sensor Network System for Healthcare Monitoring Application" , IEEE Biomedical Circuits and System Conf. , pp.243 -246 , 2007
[13] M. R. Yuce , S. W. P. Ng , N. L. Myo , C. H. Lee , J. Y. Khan and W. Liu, "A MICS band wireless body sensor network", Proc. IEEE WCNC, pp. 2473-2478, 2007
[14] G. Z. Yang, "Body Sensor Networks", 2007
[15] S. Kim, C. Brendle, H. Y. Lee, M. Walter, S. Gloeggler, S. Krueger, S. Leonhardt, "Evaluation of a 433 MHz band body sensor network for biomedical applications.", Sensors (Basel), pp. 898-917, 2013
[16] A. Taparugssanagorn, A. Rabbachin, M. Hämäläinen, J. Saloranta and J. Iinatti, "A Review of Channel Modelling for Wireless Body Area Networks in Wireless Medical Communications," in Proc. 11
[17] Motoyama, S. "Flexible polling-based scheduling with QoS capability for Wireless Body Sensor Network", Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference on, On page(s): 745 – 752
[18] Pontes Gomes, M.; Motoyama, S. "Performance Analysis of an Access Scheme Based on Weighted Polling for WBAN", Computer-Based Medical Systems (CBMS), 2015 IEEE 28th International Symposium on, On page(s): 157 – 162
[19] L. Huaming and T. Jindong, "Heartbeat-driven medium-access control for body sensor networks," IEEE Transactions on Information Technology in Biomedicine, Vol. 14, No. 1, January 2010, pp. 44-51.
[20] Z. Yan and B. Liu, "A context aware MAC protocol for medical wireless body area network," in Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International, pp. 2133-2138
[21] Hossain, M.U.; Dilruba; Kalyan, M.; Rana, M.R.; Rahman, M.O. "Multi-dimensional traffic adaptive energy-efficient MAC protocol for Wireless Body Area Networks", Strategic Technology (IFOST), 2014 9th International Forum on, On page(s): 161 – 165
[22] Marinkovic S, Popovici E. Ultra low power signal oriented approach for wireless health monitoring.Sensors (Basel) 2012;12(6):7917–37. doi: 10.3390/s120607917
[23] http://ieeexplore.ieee.org (Último acceso 11/04/2016)

[24] http://www.sciencedirect.com (Último acceso 23/03/2016)
[25] http://www.ncbi.nlm.nih.gov (Último acceso 05/03/2016)
[26] Hackers roban datos de 80 millones de clientes de aseguradora Anthem de EEUU http://bit.ly/1YQdn2j (Último acceso 25/03/2016)
[27] C. C. Tan, H. Wang, S. Zhong and Q. Li, "Body Sensor Network Security: An Identity-Based Cryptography Approach", WiSec '08 , pp. 148-153, 2008
[28] S. D. Bao , Y. T. Zhang and L. F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems", Proc. 27th IEEE Conference on Engineering in Medicine and Biology, pp. 2455-2458, 2005
[29] C. C. Y. Poon, Y. T. Zhang and S. D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-Health", IEEE Commun. Mag., vol. 44, no. 4, pp. 73-81, 2006
[30] S.N. Ramli, R. Ahmad, M.F. Abdollah, E. Dutkiewicz," A Biometricbased Security for Data Authentication in Wireless Body Area Network (WBAN)," Advanced Communication Technology (ICACT), pp. 998-1001, Jan. 2013.
[31] J. Shen, H. Tan, S. Moh, I. Chung, Q. Liu, and X. Sun, "Enhanced Secure Sensor Association and Key Management in Wireless Body Area Networks", JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 17, NO. 5, pp 453-462 2015
[32] Y. Sil Lee, B. Ndibanje, E. Alasaarela, T. Y. Kim and H. Lee, "An Effective and Secure User Authentication and Key Agreement Scheme in m-Healthcare Systems", 7th IEEE International Symposium on Cyberspace Safety and Security (CSS), 2015
[33] M. Sarvabhatla and C.S. Vorugunti, "An energy efficient mutual authentication scheme for secure data exchange in health-care applications using wireless body sensor network", Future Information Security Workshop, COMSNETS, 2015
[34] L. Shi, J. Yuan, S. Yu and M. Li, "MASK-BAN: Movement-Aided Authenticated Secret Key Extraction Utilizing Channel Characteristics in Body Area Networks", IEEE INTERNET OF THINGS JOURNAL, VOL. 2, NO. 1, pp 52-62, 2015
[35] M. H. Salama, S. Taha and H. Elmahdy, "PMAS: A Proposed Mutual Authentication Scheme for Wireless Body Area Networks", Information and Communication Technology Convergence (ICTC), pp 636-641, 2015
[36] W. Wang, C. Wang, M. Zhao, "Resource Optimized TTSH-URA for Multimedia Stream Authentication in Swallowable-Capsule-Based Wireless Body Sensor Networks", IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, VOL. 18, NO. 2, pp 404-410, 2014
[37] V. Sankari and K. Nandhini, "Steganography Technique to Secure Patient Confidential information using ECG Signal", International Conference on Information Communication and Embedded Systems (ICICES), 2014
[38] R. Rekha, T. Gayathri Mathambigai, and Dr.R. Vidhyapriya, "Secure Medical Data Transmission in Body Area Sensor Networks Using Dynamic Biometrics and Steganography", Bonfring International Journal of Software Engineering and Soft Computing, 2012
[39] Fen Miao, Lei Jiang, Ye Li and Yuan-Ting Zhang, "A Novel Biometrics Based Security Solution for Body Sensor Networks", IEEE, 2009
[40] Fan, Rong. The new secure and efficient data storage approaches for wireless body area networks[C], 2010 International Conference on Wireless Communications and Signal Processing (Wcsp), 2010: 1-5.
[41] D. He, S. Zeadally and L. Wu, "Certificateless Public Auditing Scheme for Cloud-Assisted Wireless Body Area Networks", IEEE Systems Journal, pp 1932-8184, 2015
[42] Y. S. Lee, E.Alasaarela and H. Lee, "Secure Key management Scheme based on ECC algorithm for Patient's Medical Information in Healthcare System", The International Conference on Information Networking (ICOIN2014), pp 453 - 457, 2014
[43] F. Miao, S.-D. Bao and Y. Li, "A modified fuzzy vault scheme for biometrics-based body sensor networks security", Proc. IEEE Global Telecommun. Conf. GLOBECOM, pp. 1-5, Dec. 2010
[44] C. Z. Cao, C. G. He, S. D. Bao and Y. Li, "Improvement of fuzzy vault scheme for securing key distribution in body sensor network, "Proc. Annual Conference of IEEE-EMBS, 2011, pp. 3563-

3567.
[45] G. Zheng, G. Fang, M. A. Orgun and R. Shankaran, "A Comparison of Key Distribution Schemes Using Fuzzy Commitment and Fuzzy Vault within Wireless Body Area Networks", 26th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC): Services Applications and Business, pp 2120-2125, 2015
[46] Y. Lu and S. D. Bao, "Efficient Fuzzy Vault Application in Node Recognition for Securing Body Sensor Networks", IEEE International Conference on Communications (ICC), pp 3648 - 3651, 2014
[47] K. K. Venkatasubramanian, A. Banerjee, S. K. S. Gupta, "PSKA: usable and secure key agreement scheme for body area networks, " IEEE Transactions on Information Technology in Biomedicine, vol. 14, no. 1, 2010, pp. 60-68.
[48] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao and D. Chen, "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks", INFOCOM, 2013
[49] W. A. Cahyadi, T. Jeong, Y. H. Jim, Y. H. Chung and T. Adiono, "Patient Monitoring Using Visible Light Uplink Data Transmission", International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS) pp 9-12, 2015
[50] X. Huang, X. Gao, and Z. Yan, "Security protocols in body sensor networks using visible light communications", International Journal of Communication Systems, 2015
[51] Y. Tian,Y. Peng, X. Peng and H. Li, "An Attribute-Based Encryption Scheme with Revocation for Fine-Grained Access Control in Wireless Body Area Networks", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, 2014
[52] A. V. K Shanthi, "FINE-GRAINED ACCESS OF PERSONAL HEALTH RECORD IN CLOUD COMPUTING", ARPN Journal of Engineering and Applied Sciences, Vol 10, no. 22, 2015
[53] D.J. Kim and B. Prabhakaran, "Motion Fault Detection and Isolation in Body Sensor Networks",Proceeding of IEEE International Conference on Pervasive Computing and Communications, pp. 147-155
[54] Y. Wang, Li. Xing, H. Wang and G. Levitin, "Combinatorial analysis of body sensor networks subject to probabilistic competing failures", Reliability Engineering & System Safety, V 142, pp 388-398, 2015
[55] H. Zhang, and J. Liu, "Fault Diagnosing ECG in Body Sensor Networks Based on Hidden Markov Model", 10th International Conference on Mobile Ad-hoc and Sensor Networks, 2014
[56] A. Mahapatro and P. Mohan Khilar, "Fault Diagnosis in Body Sensor Networks", International Journal of Computer Information Systems and Industrial Management Applications. V 5, pp. 252-259, 2012
[57] G. Wu, J. Ren, F. Xia and Z. Xu, "An Adaptive Fault-Tolerant Communication Scheme for Body Sensor Networks", Sensors, 2010