# Communication and Security in Health Monitoring Systems -- A Review (Comunicación y Seguridad en los Sistemas de Vigilancia de la Salud: Una Revisión)

**Abstracto:**

El rápido desarrollo de dispositivos de detección y radios permite sistemas remotos de monitoreo de salud más potentes y flexibles. Teniendo en cuenta la visión futura de Internet de las cosas (IoT), muchos requisitos y desafíos surgen para el diseño e implementación de dichos sistemas. Cerrar la brecha entre los nodos de sensores en el cuerpo humano e Internet se convierte en una tarea desafiante en términos de comunicaciones confiables. Además, los sistemas no solo tendrán que proporcionar funcionalidad, sino que también serán altamente seguros. En este documento, proporcionamos una encuesta sobre los protocolos de comunicación existentes y los problemas de seguridad relacionados con el monitoreo generalizado de la salud, describiendo sus limitaciones, desafíos y posibles soluciones. Proponemos un diseño genérico de pila de protocolos como primer paso hacia el manejo de la interoperabilidad en redes heterogéneas de área de cuerpo inalámbrico de baja potencia.

**Publicado en:**[40a Conferencia Anual de Aplicaciones y Software Informático 2016 de IEEE (COMPSAC)](https://ieeexplore.ieee.org/xpl/conhome/7551592/proceeding)

**Fecha de la conferencia:** 10-14 de junio de 2016

**Fecha de adición a IEEE *Xplore* :** 25 de agosto de 2016

**Información del ISBN:**

**ISSN electrónico:** 0730-3157

**Número de acceso de INSPEC:** 16253104

**DOI:**[10.1109 / COMPSAC.2016.8](https://doi.org/10.1109/COMPSAC.2016.8)

**Editorial:**IEEE

**Lugar de la conferencia:** Atlanta, GA, EE. UU.

**SECCIÓN I.**

## **Introducción**

Los avances en el hardware de la radio y los protocolos de comunicación inalámbrica permiten cambios tremendos en las mediciones del sensor de transmisión. Varias aplicaciones están ganando en dispositivos de detección inalámbrica para fines de monitoreo y control. El monitoreo remoto de la salud es una de las aplicaciones emergentes que ha atraído a los diseñadores de sistemas para diseñar protocolos de comunicación eficientes y confiables.

Si consideramos las predicciones de que la población mundial de personas mayores (65 años o más) se duplicará en 2025, en comparación con las cifras de 1990 [1] , entonces es obvio que proporcionar una atención médica eficiente y confiable, a un precio más bajo o al mismo precio que hoy se convierte en un gran desafío. Casi el 30% de todas las muertes en todo el mundo están relacionadas con enfermedades cardiovasculares que se pueden detectar y prevenir fácilmente mediante sistemas de monitoreo de salud remotos confiables y oportunos. En consecuencia, los sistemas de monitoreo de la salud están a punto de revolucionar la vida humana al proporcionar detección rápida y monitoreo en tiempo real de los pacientes. Sin embargo, al emplear las tecnologías habilitadoras, debemos tener en cuenta el bienestar de los pacientes, ya que es inaceptable emplear soluciones que no coincidan con los estándares de las mejores prácticas actuales en el cuidado de la salud.

En este documento, investigamos investigaciones recientes relacionadas con los sistemas de monitoreo de salud, centrándonos en la comunicación inalámbrica y los requisitos de seguridad relevantes. Nos enfocamos en redes inalámbricas de baja potencia (LPWN) para el monitoreo de signos vitales humanos. Para ser completamente funcional, el sistema debe ser flexible y escalable, al tiempo que proporciona niveles suficientes de confiabilidad y oportunidad. Proporcionar interoperabilidad entre diferentes redes también es un tema desafiante. La seguridad, la privacidad y la confianza son otros temas clave que afectan la funcionalidad de los sistemas de monitoreo de salud. Con un número cada vez mayor de dispositivos conectados a Internet en los sistemas de monitoreo de salud, aumenta la posibilidad de amenazas de seguridad y ataques adversos. Además, las LPWN tienen el precio de las capacidades computacionales, de memoria limitada y de baja potencia, que limita el uso de soluciones de seguridad ya existentes. Para ser conciso, nuestras contribuciones incluyen:

* Investigar tecnologías de comunicación relevantes e identificar desafíos.
* Revisión de problemas de seguridad y privacidad dentro de las tecnologías LPWN, junto con algunas de las soluciones existentes.
* Diseñar un sistema genérico de monitoreo de la salud, considerando las limitaciones y la posible solución, centrándose en el diseño de una pila de protocolos genéricos para LPWN heterogéneos.
* Resumen de los marcos de comunicación de última generación, diseñados para aplicaciones de monitoreo de salud.

El documento está organizado de la siguiente manera. La Sección II describe las principales tecnologías y estándares de comunicación inalámbrica, utilizados en aplicaciones de monitoreo de salud. La Sección III proporciona detalles sobre los problemas de seguridad en LPWN. Proponemos un marco de vigilancia de la salud genérica en la Sección IV , seguido de la revisión de la salud conocido marcos de supervisión en la Sección V . Las observaciones finales se dan en la Sección VI .

**SECCION II.**

## **Redes de comunicación en sistemas de monitoreo de salud**

Hay dos tipos de sensores corporales no invasivos; clasificados como *sensores implantables* (p. ej., biosensores que miden los niveles de metabolitos para la diabetes [2] , marcapasos y cápsulas de endoscopio) y *sensores portátiles* (p. ej., *sensores de* presión arterial, ECG, SpO2 y aliento). Los requisitos y requisitos previos de comunicación dependen del tipo de sensores. En este trabajo, nos enfocamos en una red inalámbrica de área corporal (WBAN), ya que es el tipo de red más común dentro de un sistema de monitoreo de salud, responsable de recolectar mediciones de sensores con radios de baja potencia utilizando comunicación de corto alcance a través de enlaces poco confiables. También describimos brevemente las redes de alta potencia dentro de un sistema de monitoreo de salud.

We categorize the communication strategies in health monitoring systems into: intra-WBAN communication (i.e., data exchange between sensing devices and the coordinator, located on the human body), and beyond-WBAN communication (i.e., communication from the WBAN coordinator, located on the body of primary end-user towards the secondary end-user). In this section, we consider the possible wireless standards/technologies for intra-WBAN and beyond-WBAN communications. We also explain some of the quality of service (QoS) communication requirements, followed by the main challenges from a communication architecture point of view.

### A. Intra-WBAN Communication Networks

Intra-WBAN communication, which is also known as WBAN, covers a wide variety of applications, such as health- care, fitness, and entertainment. It is usually used for collecting, processing and forwarding the data over a long period of time. Each WBAN consists of a number of sensing devices with processing and communication capabilities. Even if WBANs share many challenges with wireless sensor networks (WSNs), there are several specific design questions that require a new line of research.

**Table I:**Comparing different standard wireless technologies in terms of network topology, transmission range, frequency band, data rate, transmission power and their security support

Los sensores portátiles que se colocan en el cuerpo humano generalmente se usan para monitorear la salud a largo plazo y pueden prevenir eventos que amenazan la vida. Los principales estándares de LPWN para la comunicación en el cuerpo son: IEEE 802.15.4 [3] , IEEE 802.15.6 [4] y Bluetooth [5] . Sin embargo, la radio IEEE 802.15.6 no está disponible para ser utilizada dentro de las aplicaciones WBAN. La Tabla I resume las características principales de estos estándares y tecnologías, comparándolos con algunas redes inalámbricas de mayor consumo de energía, como WiFi y WiFi de baja potencia [6] .

**IEEE 802.15.4**[3] define capas físicas (PHY) y de control de acceso medio (MAC) para LPWN. Proporciona tres bandas de frecuencia de 868 MHz, 915 MHz y 2.4 GHz, con una velocidad de datos de 250 kbps. La banda industrial, científica y médica (ISM) de 2,4 GHz está disponible en todo el mundo y, por lo tanto, se usa con mayor frecuencia. IEEE 802.15.4 define dos topologías: topología en estrella (todos los nodos sensores se comunican directamente con el coordinador (salto único)) y topología punto a punto (cualquier nodo sensor puede comunicarse con otro nodo sensor), donde la topología estrella es más común en aplicaciones de monitoreo de salud.

*ZigBee*[7] es una especificación abierta que complementa el estándar IEEE 802.15.4 con capas de red y seguridad, así como perfiles de aplicaciones. ZigBee admite la topología de malla, donde cada nodo puede comunicarse con cualquier otro nodo, a través de un salto único o múltiple, retransmitiendo la transmisión a través de múltiples nodos adicionales. La red puede extenderse en un área más grande. Para proteger los datos transmitidos, las redes ZigBee utilizan el algoritmo de cifrado del estándar de cifrado avanzado (AES), que es uno de los algoritmos más seguros, robustos y confiables que cifra bloques de datos de 128 bits, utilizando múltiples operaciones de sustitución y permutación.

6 *LoWPAN*[8] es un estándar abierto, desarrollado por IETF (RFC 6282) para admitir IPv6 para LPWN, que se ha integrado en el protocolo estándar IEEE 802.15.4. Básicamente, adapta el direccionamiento IPv6 largo en una trama abstracta y corta adecuada para el formato de paquete estándar IEEE 802.15.4. 6LoWPAN proporciona un modelo de adaptación que proporciona administración de red, estrategia de enrutamiento, seguridad, interfaz de aplicaciones y descubrimiento de redes. Este estándar abierto también se está integrando en otras redes, incluidas las radios de baja potencia Sub-1 GHz, como BLE y WiFi de baja potencia [9] .

**IEEE 802.15.1 o Bluetooth**[5] , está diseñado e implementado para comunicaciones inalámbricas de corto alcance. Admite diferentes bandas de frecuencia, como 13.56 MHz, 2.4 GHz y 2.5 GHz, con una velocidad de datos de 1 a 2.1 Mb / s. Se han definido dos tipos de topologías: *piconet* y *scatternet.*. Una piconeta está formada por el nodo maestro y uno o más dispositivos Bluetooth como esclavos. El nodo maestro establece un reloj para obtener la sincronización, y se aplica el salto de frecuencia para reducir la probabilidad de interferencia. Los esclavos tienen comunicación punto a punto con su nodo maestro. Sin embargo, un nodo maestro puede unicast o multicast a esclavos dentro de la piconet. Una red de dispersión es una colección de algunas piconets. Una unidad Bluetooth puede ser miembro de diferentes piconets, es decir, puede ser esclava en muchas piconets.

*Bluetooth low energy (BLE*) [10] was introduced as a part of the Bluetooth Core Specification version 4.0. BLE expands the functionality and applicability of Bluetooth, and makes it a suitable choice for health monitoring systems. BLE involves several changes compared to traditional Bluetooth. It operates in the spectrum band 2402–2480 MHz, divided as 40×2 MHz channels instead of 79×1 MHz channels in Bluetooth. In BLE, three advertising channels are dedicated to broadcast messages, using frequencies 2402, 2426, and 2480 MHz to mitigate interference from other technologies working in same frequency band. BLE employs a frequency hopping mechanism that reduces the risk of eavesdropping on transmitted packets. In BLE, timing requirement in frequency hopping is more relaxed due to the longer stay in each channel. Security requirements are covered by advanced encryption standards, pairing to create shared secrets, and bonding to enable trusted device pair and device authentication.

**IEEE 802.15.6** [4] defines a MAC layer that supports several PHY layers, such as narrowband (NB) with frequencies 400, 800 and 900 MHz, ultra-wideband (UWB) with frequencies 2.3 and 2.4 GHz, and human body communication (HBC) with 10–50 MHz, while the data rate varies from 75.9 kb/s to 15.6 Mb/s. Selecting a proper PHY layer with accompanying frequency band should be influenced by the application requirements and limitations. With 802.15.6, sensor nodes are organised in a one- or two-hop star topology, communicating to a single coordinator or hub. In a two-hop topology, special nodes with relay capability are supposed to be placed in order to forward the data from sensor nodes towards the coordinator. The IEEE 802.15.6 standard divides the time into beacon periods or super frames with the equal length. The coordinator defines boundaries of the super frame that is separated into a number of slots, used for data transmission. Beacons are transmitted periodically for synchronisation purposes among all sensor nodes [11]. The IEEE 802.15.6 supports three security levels with different security properties, protection levels, and frame formats, which are known as (i) unsecured communication level (low security level), (*ii*) authentication level (medium security level), and (*iii*) authentication and encryption (high security level).

### B. Beyond-WBAN Communication Network

In a health monitoring system, measurements are usually forwarded from a WBAN through a gateway towards the cloud. The gateway is used to bridge two different network technologies, from low-power to high-power wireless network, or from a wireless network to a wired network. The high-power networks are out of the scope of this work, as they provide more reliable and secure way of data communication. The possible high-power wireless networks are described below.

**IEEE 802.11 or WiFi** that operates in the 2.4 and 5 GHz bands is the most popular wireless technology for indoor environments. The main features of WiFi are: high data rate, easy deployment, low cost and high power consumption (compared with LPWNs)1 . Due to the increasing demands for ubiquitous devices with low-power consumption, low power WiFi (IEEE 802.111ah) [6] was designed. This radio that works at 780, 868, 915 and 950 MHz is a potential solution for relaying data from body sensors towards the cloud. IEEE 802.11ah is scalable, supporting more than 8,000 devices, and it brings seamless connectivity with WiFi. In general, WiFi enables security via WiFi Protected Access that includes both access control and privacy for the communication.

**Cellular networks** unlike LPWNs have a fixed infrastructure of base stations, which are connected through wires and have unlimited power. There are various cellular network technologies, such as GSM, UMTS, LTE and LTE advanced. Each one has its own features and they are progressing in terms of data rate, reliability, connectivity and more importantly security. This network guarantees reliability and security issues for beyond-WBAN communications.

### C. QoS Requirements

In terms of QoS, a health monitoring system should provide a long-term collection and analysis of physiological data to ensure comprehensive feedback to professionals. In order to provide a good diagnosis, the system should be dependable in the sense that it especially offers reliable, timely and secure services.

**Dependability** can be defined as a systems capability to consistently perform the expected behaviour in order to provide a service, while minimising the fault [12], meaning that patient-related data must be available in case of any individual node failure, sensor compromises or adversary attacks. It is one of the most critical concerns in WBANs, due to the fact that failure to retrieve correct data when needed, might cause life critical events. In order to be able to say that a system satisfies the dependability requirements, the following attributes should be guaranteed: reliability, availability, maintainability, safety, confidentiality, and integrity [13]. However, one has to bear in mind that the overall dependability in systems like this, is under huge impact of error sources, such as; failures of complex softwares existing in the system, network size that is in the constant increase due to the number of small sensor devices and technological solutions involved, and the overall complexity of the system. Additionally, knowing the fact that WBANs are designed to integrate various solutions such as; different types of communication, communication protocols, and security mechanisms, it is important to be able to assess their impact on system's properties (i.e., reliability, security, availability). In order to enable the satisfying level of dependability in complex systems such as WBANs, we have to agree on certain trade-offs (i.e., by integrating technological solutions aiming at increasing one of the properties of the system; one might minimise failures of the system, while increasing the dependability, or ensuring another property, while having negative impact on the dependability).

**Reliability** of a message transmission is defined as the probability of successfully delivery of a message from the sender (sensor node) to the receiver (server). Considering the existence of unreliable links in LPWNs employed in WBAN, achieving reliable data transmission is very challenging. Also, the presence of the human body, and frequent node mobility are recognized as two major sources of interference that affect link quality.

**Timeliness** is defined as collecting data in real-time, which is crucial in critical applications such as health monitoring, where human life might be in danger. Hence, emergency data that requires predictable feedback from the health service provider, should be delay bounded. The message transmission delay is defined as the amount of time needed to transfer a message from the source to the sink, and it is measured from the time the message is passed down to the MAC layer, traveling through multi-hops, until it reaches the upper layers at the sink node. The transmission delay includes queuing delay, MAC delay, propagation delay and processing delay at the link layer. Timeliness is particularly difficult to achieve in WBAN due to the unreliable wireless links with time-varying quality.

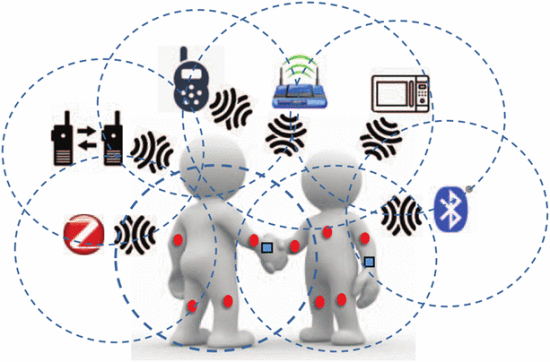
**Security** requirements for health monitoring are described in Section III.

### D. Communication Challenges

Modelling a transmission channel is imperative when it comes to wireless devices. There have been some effort to model the human body as a communication channel for WBANs [14]. In communication through the human body, the signal is transmitted through galvanic coupling, which is so-called *inductive coupling*. The transmitter injects the signal into the body such that an electromagnetic field is generated in the body. At the remote end, the receiver senses this electromagnetic field. In this channel, the data rate is low in the kbps range as the body effectively attenuates the signal. RF communication is also used to collect data from implantable sensors. Since the human body as a medium poses numerous wireless challenges, the results may vary according to different human body situations, such as age, gaining/losing weight and changing posture. Implanting sensing devices in a good location during surgery drastically improves the link reliability.

En este artículo, sin embargo, nos enfocamos principalmente en sensores portátiles para comunicaciones en el cuerpo, lo que implica intra-WBAN. Describiremos algunos desafíos de comunicación, como la interferencia, la escalabilidad y la gestión de recursos.

**Enlace no confiable** . Hay tres razones principales para la falta de fiabilidad de los enlaces en LPWN. Primero, la naturaleza de los dispositivos sensores que generalmente están equipados con antenas de baja ganancia. Estas antenas, que a menudo son omnidireccionales, tienen un patrón irregular durante la radiación. Por lo tanto, tienen rangos de comunicación no uniformes y enlaces asimétricos. En segundo lugar, los factores ambientales, como la temperatura y la humedad, afectan drásticamente la calidad de los enlaces. Tercero, hardware de radio inexacto que causa un enlace asimétrico y eventualmente afecta el rendimiento de la red.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/7551592/7551973/7552069/7552069-fig-1-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/7551592/7551973/7552069/7552069-fig-1-source-large.gif)

**Figura 1:**

Todo tipo de interferencia en una WBAN, que consiste en la coexistencia de otra WBAN, dispositivos bluetooth, dispositivos zigbee, horno microondas, punto de acceso wifi, walkie talkie y monitores para bebés.

[Ver todo](https://ieeexplore.ieee.org/document/7552069/all-figures)

**Interferencia** . Los LPWN comparten la misma banda de frecuencia (2,4 GHz) con muchos otros dispositivos inalámbricos, como WiFi, Bluetooth, IEEE 802.15.4, monitores para bebés, walkie-talkies y hornos de microondas. **Todos** los dispositivos externos además de los dispositivos WBAN que usan la misma frecuencia son fuentes de *interferencia cruzada*2 , la Figura 1 muestra todas las posibles fuentes de interferencia para un WBAN. Las WBAN vecinas también se consideran como otras fuentes importantes de interferencia, especialmente en algunos entornos como hospitales, donde muchos pacientes son monitoreados de forma remota. La interferencia generada por otros dispositivos WBAN se conoce como *interferencia mutua* .

**La escalabilidad** es uno de los principales desafíos en las aplicaciones de monitoreo de salud remoto. Para algunos pacientes, es necesario controlar varios signos vitales y recopilar diferentes parámetros de diferentes sensores. Además, en algunos casos para recopilar un parámetro fisiológico, se requiere emplear más que un nodo sensor. En algunos casos, los parámetros de detección pueden aumentar según la condición. La tecnología inalámbrica debe ser escalable y capaz de autoorganizarse en la red incluso después de aumentar el número de nodos dentro de una WBAN.

**La gestión de recursos** en LPWNs con energía de batería limitada y ancho de banda de canal debe considerarse al diseñar un sistema de monitoreo de salud. Para el monitoreo a largo plazo del paciente, una solución inteligente sería informar rápidamente los mensajes de emergencia y alta prioridad, pero ingresar los ciclos de sueño cuando no hay datos para transmitir. Los mensajes de baja prioridad se pueden almacenar y transmitir con intervalos bajos.

**SECCION III.**

## **Seguridad en el Sistema de Monitoreo de Salud**

In case of health monitoring systems, security threats might endanger the health state of a patient, or in the most extreme cases cause a death. In order to prevent this, strict and scalable security mechanisms are required to prevent any malicious interaction in the system. An efficient security framework for health monitoring applications must therefore ensure basic security services, such as privacy, confidentiality, authentication, authorization, availability, etc. These security services are imposed and required by different legal directives including European directive 95/46 on data protection [15] and **HIPAA** [16] in the United States, and should guarantee patient safety and privacy. To establish foundations for development and use of different types of WBAN applications, including medical applications, in a secure way, IEEE 802 working group for standardisation of WBANs, has produced the IEEE 802.15.6 standard [4]. Additionally in WBAN, the security mechanisms must operate fast to avoid any latency and at the same time enable high-level of scalability.

In the following, we focus on security requirements related to privacy and data access security, network communication security and data storage security as the main potential targets for security attacks.

### A. Application Data Security Requirements

*Data confidentiality* means that the collected, transmitted, and stored medical information is kept strictly private, and therefore can be accessed by authorised people only. On the other hand, an adversary can monitor the communication within the system and eavesdrop the transmitted information. Data confidentiality is usually achieved by en-cryption/decryption. *Data access control* defines a privacy policy and prevents possible unauthorised access to patient information. In WBAN, patient records could be accessed by physicians, nurses, or insurance companies. For example, based on the health condition described in a patient record, an insurance company might offer an expensive premium for health insurance [17]. Therefore, data access roles should be defined at the application level, enforcing different access privileges [18]. Besides role-based access control, one has to ensure a comprehensive set of control rules applicable within the communication framework. *Non-repudiation* is a way to guarantee that a participant in the communication network cannot deny sending or receiving a message. A common way to ensure non-repudiation is the use of digital signatures while communicating.

### B. Network Communication Security Requirements

When developing a secure WBAN, one should account for secure network communications. In this section, we describe some of the requirements related to security at this level.

*Data integrity* ensures that no data changes have been done by any adversary before reaching the storage. In WBANs, a failure to obtain correct data might lead to incorrect medical treatment that can have disastrous consequences. One of the mechanisms to achieve data integrity is to use a message authentication code, employed at the sender and receiver sides to verify that the data is not modified by an adversary. *Data authentication* should guarantee that the data is sent by a trusted sender. In case of absence of such a mechanism, it might happen that a false sender, appearing as a legitimate one, sends false data to the storage or gives incorrect treatment instructions to a patient, possibly causing harm to the patient. Similarly as with data integrity one can use a message authentication code with a shared secret key. *Data freshness* guarantees that all received data is fresh, i.e., **all** data frames are in correct order, and not replicated for disruption purposes. There are two types of data freshness guarantees, both needed in WBANs; weak and strong freshness. The first guarantees just the ordering of frames, not tackling possible delays, while the latter makes guarantees on both order and delay. Weak freshness in WBANs is required by low-cycle body sensors, such as blood pressure, while strong freshness is required during synchronising measurements with higher duty cycle, for instance in ECG [19]. *Availability* enables patient data to always be available to the physician. In case of loss of availability of one node in the system, redundancy that enforces switching operation from a disabled node to an available node can be used. In this case, it is important to use forward and backward secrecy. The first makes sure that a node leaving a network will no longer be able to read future messages, while the second ensures that the new node joining the network should not be able to read previously transmitted messages.

### C. Security Requirements on Data Storage

In WBANs, it is important to address data confidentiality and integrity, as well as dependability of data storage security. *Dependability* is one of the most critical properties when it comes to storage accessed by WBANs. It ensures quick retrieval of patient data, even in case of individual node failure and malicious modifications. So far, in the literature, dependability has been given limited attention. However, some works propose error correcting code techniques [17] that add redundancy to the original source data, while they increase network overhead in terms of packet payload size, but enhance data reliability for LPWNs with unreliable links.

### D. Security Challenges

Due to the resource constrains, a WBAN is required to be highly efficient. Wearable sensors are small and come at the price of low-power supply, making them incapable to carry out larger computations and to store larger amounts of data. Thus, cryptographic mechanisms used by sensors should be as light-weight as possible, in terms of computation and low storage overhead. Additionally, a denial of service attack might overwhelm the WBAN if the authentication protocol is not sufficiently fast.

The safety of a patient can be endangered if their records are not available at any time. In case of too strict data access control being introduced, providing a prompt medical care might be a problem. On the other hand, having a loose access control makes more room for malicious attacks.

If we assume that sensing devices in the health monitoring system would be used by non-expert patients, then we should make it as easy to use as possible, but at the same time provide an acceptable level of security. Possible problems might occur in cases when the patient has to give an access to his/her data to an emergency physician that has not been initially authorised, even though the strong security mechanism is used at the device. Sensor nodes might origin from different manufactures, and therefore, it might be a problem to share cryptographic materials. Consequently, it becomes very difficult to establish data security mechanisms and provide common settings compatible with a wide range of WBAN devices.

### E. Existing Security Solutions

There are several techniques available to secure communications in WBANs based on the use of *biometrics*. Such techniques use the unique features of the human body to generate and maintain cryptographic keys used in the system. The cryptographic keys are obtained using electrocardiogram (ECG) signals, timing of the heartbeat, or using a group of similar random numbers obtained from a combination of biometrics of the human body and further distributed throughout the network [20], [21][22]. Another suitable approach for WBANs is proposed by Shanthini et al. [23]. Their approach uses the receiver's fingerprint to generate cryptographic keys and preserve data integrity and patient's privacy. These approaches usually require less memory and computational power and thus makes them suitable for WBANs.

More traditional approaches to obtain a secure sensor network is based on the public key *cryptography*. The main disadvantage of this method is a high resource consumption, making it unsuitable for WBANs. Therefore a number of novel light-weight approaches have been proposed. The authors in [24] present a light-weight approach that includes key management, random number generation, and a three step security model. The approach is based on using a bio-channel in combination with a wireless channel to establish secure communications, as well as on the usage of physiological data to establish a secure system. In [25], a light-weight secure sensor association and key management scheme for WBANs was proposed. A group of sensor nodes establish an initial trust via group device pairing (GDP) without prior secret sharing before the meeting. The GDP protocol does not require any extra hardware devices, supports batch deployment, and relies on symmetric key cryptography. A secure sensor allocation for WBANs is described in [26]. Nodes in the system are equipped with public key-based authentication one-by-one, by a central controller, and are verified by the user through a comparison among LED blinking patterns. The disadvantage of this approach is the long time period needed for association and lack of batch deployment. Additionally, nodes with pre-distributed public keys from a trusted authority are often not practical. Authors in [27] present a secure, lightweight user authentication scheme, called Securing User Access to Medical Sensing Information (SecMed). The approach is based on elliptic curve cryptography (ECC), and provides an authentication protocol between physicians and nurses and a sensor node or PDA device. The approach uses public key codes that makes it highly scalable, requires less memory in comparison with other symmetric key-based schemes, and has good performance. Another approach based on ECC is presented in [28]. The scheme consist of setup, registration, verification and key exchange, and use of the patient's phone SIM card number as an identification code. To prevent the replay attack, they provide a counter number at every process of authenticated message exchange to resist.

**SECTION IV.**

## **Proposed Health Monitoring Framework**

In Sections II and III, we stated that the main features of LPWNs (i.e., low-power radios, link unreliability, low-processing capability, single radio, and limited bandwidth) imply reliability and timeliness guarantees, while application-specific requirements (i.e., health monitoring applications) demand security support. We also need to provide the following issues while designing a health monitoring system: (i) interoperability to support IoT applications, (*ii*) scalability, (*iii*) light-weight security on the application, network and storage levels, and finally (*iv*) it should work in any environment, indoors, as well as outdoors, and thus, requires intra- and beyond-Wban communications.

In this section, we propose a generic system model for health monitoring systems that provides reliable, timely and wireless secure communications and considers the future IoT demands, scalability issues, and suitability for any environment, indoors as well as outdoors. Figure 2 illustrates our proposed system design, with classification based on the limitations of each wireless technology and its security demands.

**Figure 2:**

A generic health monitoring system, consisting of three tiers with respect to the possible wireless technologies.

[View All](https://ieeexplore.ieee.org/document/7552069/all-figures)

### A. System Design Considerations

As can be concluded from Section II, selecting a wireless network technology affects system performance in terms of *reliability, timeliness* and *security*. The system architecture should be designed based on the type of sensor devices, location of sensors, and the number of sensor nodes. Sensor devices record data periodically with low or high sampling rate. High sampling rate requires a radio that supports higher data rate (e.g., Bluetooth). Large attenuation of the signal during communication with the implanted sensor requires a radio that overcomes channel restrictions (e.g., UWB and IEEE 802.15.6). Increasing the number of sensor nodes on the human body requires a radio that is scalable (e.g., IEEE 802.15.4 and ZigBee). In environments where patients are more prone to security threats and attacks, it is important to employ wireless networks that guarantee some security levels (e.g., 6LoWPAN on top of IEEE 802.15.4). A multi-standard radio module is useful for supporting connectivity in different environments based on the existing wireless infrastructure [29]. Moreover, this radio module supports various data rates based on the frequency of measurements and application specific requirements. Hence, to enable data collection from a range of different sensors, a health monitoring framework should support at least IEEE 802.15.4, IEEE 802.15.6, UWB and Bluetooth to enable enough flexibility.

We propose a health monitoring system, which includes the following components: (*i) Coordinator* - a simple sensor node located on the human body that collects the data from all sensor nodes. Both sensing nodes and the coordinator are equipped with the same low-power radio. (*ii) Access points (APs*) - nodes that have the same radio as sensor nodes, which are static nodes attached on the walls, known as infrastructure. APs collect and forward data towards a Gateway. (*iii) Gateway* - a device that provides connection between the WBAN and the Internet, and receives the data directly from either sensor nodes or the coordinator, which is then forwarded to the cloud. We assume two types of users in these system: *primary end-user*, defined as the patient that holds sensors, and *secondary end-user*, a physician, whom analyses and makes decisions based on the processed information. We define *a three tier system architecture* for health monitoring, where low-power radios are employed in Tier 1 and Tier 2, while high-power radios are used in Tier 3. This system architectures supports various radio and network technologies that establishes a heterogeneous network.

**Tier 1** supports intra-WBAN communication, i.e., data transmission from sensor nodes toward a coordinator. This short range communication is supported by IEEE 802.15.4, ZigBee, 6LoWPAN, IEEE 802.15.6, Bluetooth, BLE and UWB.

**Tier 2** is classified as a beyond-WBAN communication, where it covers data transmission from the coordinator within WBAN to the APs, and then from APs toward the Gateway. The coordinator and APs have one of the aforementioned low-power radio technologies (i.e., 802.15.4, ZigBee, 6LoWPAN, 802.15.6, Bluetooth, BLE or UWB). This tier is beneficial for special patients and environments. Holding a smartphone as a Gateway for elderly people and patients with Alzheimer disease would be difficult and sometimes impossible. In some environments with the possibility of deploying low-cost low-power radios, it is possible to provide direct communication from the coordinator (i.e., one of the selected sensors within the WBAN) to one of the neighbour APs3 (i.e., a low-power radio node) [30]. These static APs with low-power radio provide an infrastructure to relay data toward a Gateway that supports multi-radio. In outdoor environments, due to the lack of AP infrastructure, Tier 1 and Tier 2 are merged together. Thus, person should hold the Gateway node in order to collect WBAN information and relay toward the cloud.

**Tier 3** is also considered as a beyond-WBAN communication, which covers data transmission from Gateway through cloud towards the sink node (server) [31]. The server is responsible for data processing before it reaches to the secondary end-user (physicians/nurses) for possible actions. Each of the aforementioned tiers would be sufficient to collect data from sensor nodes. However, in order to support connectivity in different indoor/outdoor environments, depending on the possible infrastructure, we assume three levels, where each of these levels may become inaccessible in special environments.

### B. Solutions for the Identified Existing Challenges

In Sections II and III, we have identified a set of challenges. The proposed generic health monitoring system design enhances network inter-operability, scalability, connectivity and security. In addition, we propose the following solutions that would further benefit the network in terms of increased QoS regarding reliability, timeliness and security.

There exists various **link quality estimators** (LQEs) for LPWNs, which are designed based on various parameters, such as packet delivery ratio, signal strength and link symmetry. However, most of them consider static nodes. In healthcare applications, the human body and mobile nodes are the two major sources that create dynamic environments, which eventually affect the **LQE** metric. Link quality directly affects packet delivery rate in wireless media.

Providing sufficient QoS levels in unreliable LPWNs requires a **mobility management framework** that considers both link quality (LQE parameters such as RSSI, SNR, LQI) and network parameters (e.g., local traffic, number of hops). There are different strategies to tackle mobility in wireless networks, such as (i) localisation algorithms, where they defines how to estimate the position or spatial coordinates of a wireless device. (*ii*) Software defined radio techniques that controls the path of a packet to an individual router. (*iii*) Handoff or hand-over4 mechanisms that select the best router for data communication [32]. For instance, in Tier 2, it supports network connectivity by selecting the best access point for data reliability based on an LQE parameter. A mobile IPv6-based (6LoWPAN) hand-off mechanism provides guarantees on data security.

There are different solutions proposed in the literature that address **interference awareness** in WBANs. [33] classifies these solutions into five groups: (i) time spacing, (*ii*) frequency spacing, (*iii*) code diversity, (*iv*) standards adaptation, and (v) hybrid solutions.

The idea of *time spacing* is to avoid simultaneous transmissions that causes collision in networks with single channel. TDMA techniques within MAC protocols are used to schedule data packet transmission. These solutions are useful for cases with interference from other WBAN devices. Thus, it will not be effective to obtain better performance with WiFi interference, where it uses a contention-based MAC protocol. Major problems with TDMA-based protocols are the large delays in dense sensing networks and the complex process of rescheduling in networks with high dynamics. The re-scheduling process have been targeted in many works, by cooperative scheduling in [34] and horse race scheduling in [35].

*En las* soluciones de *espaciado de frecuencia o salto de frecuencia* , se emplean estrategias de asignación de canales que cambian el canal después de detectar interferencia. Estas estrategias se limitan al número de canales disponibles y no son muy precisas para estimar el nivel de interferencia en cada canal. Con la selección dinámica de canales, la interferencia se detecta utilizando la tasa de error de paquete [36] . La programación de canales también se utiliza para reducir la interferencia mutua entre las WBAN adyacentes [37]. El salto de frecuencia permite la comunicación entre dos o más antenas mediante salto sincrónico a través de un conjunto de canales predefinidos que se seleccionan tradicionalmente de forma pseudoaleatoria. Esta estrategia se ha implementado en Bluetooth y BLE. Por lo tanto, se requiere un modelo de salto de frecuencia adaptativo para cambiar los canales dedicados [38] . Al aplicar una estrategia de salto de frecuencia, es posible entregar los datos a través de un enlace más confiable, lo que a su vez resulta en una mayor confiabilidad y menos demora. Además, el salto de frecuencia dificulta las escuchas y la vigilancia maliciosa, y el adversario primero necesita adquirir la secuencia de salto pseudoaleatoria correcta.

La *codificación de diversidad o codificación de red se* dirige a técnicas CDMA para la comunicación de datos, donde se utilizan códigos ortogonales de las redes interferentes. Sin embargo, estas técnicas requieren una gran cantidad de intercambios de paquetes y algoritmos complejos. Una solución es una cancelación de interferencia paralela que utiliza la secuencia directa CDMA y se dirige a la interferencia mutua [39] . Otra solución es la detección multiusuario en redes CDMA para la cancelación de interferencia, donde se consideraron el ruido gaussiano y los canales de desvanecimiento de Rayleigh [40]. En la codificación de red, se selecciona más de una ruta en un protocolo de enrutamiento, pero en cambio los paquetes se combinan cuando se envían a través de enlaces individuales. Es una técnica útil para ahorrar consumo de energía y mejorar la escalabilidad de la red. Esta técnica permite que los nodos en la red realicen operaciones algebraicas, pero requiere más recursos computacionales. Por lo tanto, es probable que la codificación de red no sea posible en los sensores de baja potencia, pero en la parte Tier 2 del marco, se puede usar para aumentar la escalabilidad, la redundancia y la disponibilidad.

Con *las* soluciones de *adaptación estándar* , los protocolos MAC generalmente se revisan y reestructuran para mejorar la coexistencia de interferencia. Un ejemplo es seleccionar un esquema de modulación especial, velocidad de datos y ciclo de trabajo (períodos activos e inactivos) en función del nivel y la duración de la interferencia [41] . También hay soluciones que no modifican los estándares, que se basan en la transmisión de paquetes falsos. Por ejemplo, un paquete de datos WiFi falso con una duración de preámbulo suficiente para un WBAN [42] , o un paquete RTS falso para reservar el medio para nodos WBAN y evitar que los nodos WiFi interfieran [43] , o paquetes CTS falsos con una duración específica , que es suficiente para WBAN y evita que los nodos WiFi envíen datos a través del medio[43] .

Una combinación de las cuatro soluciones anteriores se denomina *soluciones híbridas* , que mantiene los beneficios de todos estos esquemas. En [44] , se propuso un método distribuido de mitigación de interferencia mutua basado en la transmisión de paquetes de datos y la programación de canales. En este método, basado en la información recopilada de las redes interferentes, la WBAN reprograma las transmisiones de datos o ingresa en estado inactivo hasta que finaliza la interferencia.

**La pila de protocolos genéricos** es un requisito de diseño de protocolo para los futuros sistemas de monitoreo de salud que requieren el uso de varias tecnologías de radio. Proponemos esta solución como una solución inicial para permitir LPWN heterogéneos para sistemas de monitoreo de salud. En una red homogénea tradicional, todas las entidades de red funcionan en una misma pila de protocolos, donde cada capa tiene sus características específicas. La integración de varias tecnologías con diferentes capacidades en un sistema de monitoreo de salud degradaría el rendimiento de la red, ya que los problemas de interoperabilidad se han descuidado en las pilas de protocolos. En la literatura, hay dos soluciones principales que proporcionan interoperabilidad dentro de una red heterogénea [45] :

1. Mobile IP-based techniques, which are used as network architecture to integrate different networks [46], [47]. This approach requires fundamental changes in non-IP-based network protocol stacks.
2. Gateways are used to establish connection between different networks. These devices are intermediate nodes that transfer information between different networks. However, this approach is easy to implement.

The first solution — mobile IPv6 — is a more common way to attain inter-operability in LPWNs [48], [49]. Many adaptation techniques have been defined to integrate IPv6 in different networks. For instance, 6LoWPAN was designed to carry IPv6 datagrams over the IEEE 802.15.4 and recently under development within BLE. Web services such as REST and CoAP are tailored within the application layer. A light version of XML and SOAP are under IETF implementation for the security purposes.

The aforementioned adaptation techniques based on mobile IPv6 are targeting one of the layers specifically and customised for a network design or standard. Providing a seamless communication with good performance using different devices and networks is still a challenging topic. Conventional generic protocol stacks consist multiple physical, data link and medium access control (MAC) layers, and network, transport, and application layers [45]. Thus, based on the requirement, a specific combination of lower layers is selected, while all networks are supposed to have similar upper layer protocol designs. However, these conventional protocol stacks are very heavy in terms of memory footprint. There is a need to design novel protocol stacks that provide common features of all networks, while adding additional features to obtain a reasonable network performance.

**Security enhancements**, can be addressed using a lightweight encryption solutions to prevent possible eavesdropping of the transmitted data and attacks to a patient's privacy. Unauthorised access to a patient data can be solved by strict data access roles, and enforcing access privileges. Additionally, a message authentication code can be used to prevent data modification and to guarantee that the data is sent from a trusted node, but we have to keep in mind that it does not provide guarantees on timeliness. Availability can be ensured via redundancy mechanisms that enforce mode switch in case a node becomes unavailable. So far dependability-related issues are the least addressed, but we see as a possibility to include existing error correcting code techniques to bridge this gap. Note also that redundancy mechanisms and error correcting codes not only enhance security, but also increase reliability.

**SECTION V.**

## **Health Monitoring Frameworks**

In this section, we provide a description of the most representative examples of well-known system architectures for health monitoring, including both research and commercial solutions, enlisted in a chronological order of their appearance. Table II illustrates a qualitative comparison between the most common system architectures for health monitoring applications compared with our proposed system architecture with heterogeneous LPWNs. We argue that our system model can outperform the other systems in terms of security, scalability, real-time, infrastructure, hand-off and heterogeneity. However, there is a need to provide appropriate solutions for all these issues to provide the requirements for a generic system suitable for health monitoring applications.

CodeBlue [51] is a low-power wireless infrastructure, intended for emergency medical care. It is designed to operate both with a small number of devices under almost static conditions' such as hospitals, as well as in ad-hoc deployments at a mass casualty site. CodeBlue utilises a set of medical sensors integrated with some commercial-off-the-shelf platforms (i.e., Mica2, MicaZ, and Telos motes). The sensing units measure the vital signs and transmit their data directly to APs, attached on walls. Physicians subscribe to the network by multicasting. This system architecture is very scalable with self-organising capabilities. Literature related to this monitoring system recognises the need of data security and privacy protection and suggests the use of ECC approach [52] for the key generation and TinySec [53] for symmetric encryption. However, none of the suggested approaches have never been implemented within the system. CodeBlue supports scalability, timeliness and security, but it fails in terms of reliability. The results in [51] indicate that packet delivery ratio drops drastically in a (i) multi-hop network and (*ii*) with high sampling measurements.

The **AID-N** [54] health monitoring architecture is designed in three layers. Layer 1 consists of an ad-hoc network for collecting vital signs and running lightweight algorithms, able to operate on a limited memory and computing capabilities. Layer 2 includes servers that are connected to the Internet to forward information to a central server, located in Layer 3. The intermediate servers are laptops and PDAs that send the data. Intra- and beyond-WBAN communications is supported via IEEE 802.15.4 and IEEE 802.11, respectively, while a flexible security level is provided (i.e., from low to high level). AID-N is a real-time system architecture that fails in terms of reliability in LPWNs with unreliable links and also in networks with high sampling measurements.

The CareNet [55] system architecture builds a heterogenous network infrastructure and provides a two-tier wireless network for data sensing, collection, transmission, and processing. The intra-WBAN communication uses IEEE 802.15.4 wireless standard to send the data from Telos motes, while a multi-hop IEEE 802.11 wireless network provides a high performance backbone structure for packet routing. This architecture comes with a scalable software platform and built-in security communication mechanisms, which enable a reliable and privacy-preserving data transmission within the system. CareNet supports intra- and beyond-WBAN communications with a reasonable reliability, scalability and security. However, CareNet neglects the real-time issue in critical health monitoring applications.

The **MobiHealth** [56] system is designed for ambulant patient monitoring that employs cellular network (i.e., UMTS and GPRS). The patient is provided with a number of sensors, measuring the vital signs and communicating with a mobile base unit (collects the data) via Bluetooth and ZigBee. Thus this architecture supports both intra- and beyond-Wban communication, however, mechanisms for security are not provided. MobiHealth provides reliability and inter-operability issues, while it fails in terms of security and data privacy.

**MEDiSN** is a wireless sensor network used to automate the process of patient monitoring in hospitals and at disaster scenes [57], developed in a collaboration of John Hopkins University Hospital, University of Latvia, University of Maryland Medical Center and Aid Networks. The system consist of a number of a mobile sensor-based physiological monitors that collect the medical data of a patient, temporarily store the data and transmit it to the nearest relay points. Relay points are self-organised into bidirectional routing tree and they transmit the patient's medical data to gateways. In the final phase, the data is stored within the back-end databases and is available to authorised personnel only. Security protection includes encryption for each physiological monitor and authentication and user authorisation. However, the details regarding the implemented security mechanism have not been revealed in the existing literature.

**LAURA** is a wireless sensor based lightweight system for monitoring of patients within nursing institutions [58]. Architecturally, the system consist of (i) a localisation and tracking engine to locate patients based on the samples of the received signal, (ii) a personal monitoring module that classifies the movements of the patients eventually detecting hazardous situations, and (iii) a wireless communication infrastructure to deliver the information remotely. The benefit of the approach is its ability to be quickly deployed, due to adopted self-calibration method. Authors address the need of security and privacy preserving mechanisms, however they omit to provide any details on the existing implementations.

**Table II:**Qualitative comparison between the related works on system architectures for health monitoring with our proposed generic health monitoring system architecture

**eCare Companion** is a health monitoring system from Philips [59]. The system provides a patient portal, accessible via **PDA** or tablet, where patients can enter medical information such as weight, blood pressure, etc., but also to answer questionaries about their current health condition. The system is able to connect to sensor devices such as pulse oximeter, weight scale, blood pressure meter, and medicine dispenser to collect the data automatically. In the system description Philips claims that they provide security and privacy protection of the patient's data, but do not provide details on mechanisms used. In 2014, in partnership with Salesforce Philips constructed a connected, multi-point and collaborative data platform for healthcare similar to eCare Companion [60] . Es una tecnología de información basada en la nube que permite conectar diferentes dispositivos.

En [50] , los autores presentan una arquitectura de sistema distribuido para la detección de caídas mediante la identificación de posturas humanas y la detección de actividades dañinas. El sistema se compone de múltiples nodos sensores pequeños conectados al cuerpo humano con radio IEEE 802.15.4. Se definieron dos tipos de comunicación entre los nodos sensores y el servidor remoto. Para entornos interiores, los sensores se comunican con los puntos de acceso a través de radios habilitados para 802.15.4, mientras que para el entorno exterior, los nodos sensores envían datos a través de teléfonos inteligentes usando la radio Bluetooth. Por lo tanto, cada nodo sensor está equipado con dos radios de Bluetooth y 802.15.4.

**SECCION VI.**

## **Observaciones finales**

En este documento, revisamos la investigación en curso dentro de los sistemas de monitoreo de salud en términos de infraestructura de comunicación inalámbrica, requisitos de QoS, cuestiones de seguridad y protección. Identificamos los principales desafíos relacionados con las tecnologías de comunicación inalámbrica y las amenazas de seguridad. También proponemos un marco genérico, clasificado en tres niveles en función de las ventajas y limitaciones específicas de las tecnologías inalámbricas junto con las demandas de la aplicación, y ofrecemos un conjunto de soluciones a los principales desafíos de comunicación y requisitos de seguridad relacionados con estos niveles. Hemos identificado la seguridad como un punto crítico en las aplicaciones relacionadas con el monitoreo de la salud y, por lo tanto, es fundamental seleccionar LPWN que brinden suficientes garantías de seguridad.

### EXPRESIONES DE GRATITUD

Los autores desean agradecer a la profesora asociada Elisabeth Uhlemann por las discusiones y los valiosos comentarios sobre las primeras versiones del documento. Este trabajo está financiado por la Fundación Sueca del Conocimiento (KKS) a través del perfil de investigación Embedded Sensor System for Health (ESS-H), los entornos distribuidos Ecare @ Home y Research Environment for Advancing Low Latency Internet (READY).