Interoperability in heterogeneous low-power wireless networks for health monitoring systems

Hossein Fotouhi, Aida Čašević, Maryam Vahabi, Mats Björkman
Mälardalen University, Västerås, Sweden
{hossein.fotouhi, aida.causevic, maryam.vahabi, mats.bjorkman}@mdh.se

Abstract—Ensuring interoperability in the future Internet of Things applications can be a challenging task, especially in mission-critical applications such as Health Monitoring Systems. Existing low-power wireless network architectures are designed in isolated networks, and ensure a satisfying level of performance in homogeneous networks. However, with co-existence of different low-power networks, the interoperability related problems arise. To bridge this gap in this paper, we study various protocol stacks (i.e., Bluetooth, Bluetooth Low Energy, IEEE 802.15.4, ZigBee, 6LoWPAN and IEEE 802.15.6), and explain their specific features. Furthermore, we provide a generic protocol stack design that facilitates multiple radios with different protocol stacks, regardless of being IP-based or non-IP-based networks. We see this approach as a possibility to enhance network performance in terms of reliability, timeliness, and security, while providing higher levels of scalability and connectivity.

I. INTRODUCTION

The wireless technologies are changing dramatically, and we are facing with a demand to accommodate different architectures, protocols, services, and applications, running and interconnecting to each other [1]. Such requirements imply the use of heterogeneous networks, while operating with existing legacy solutions. A Health Monitoring System (HMS) is an example of the future Internet of Things (IoT) applications, where various networks, wireless technologies, and devices are employed at the same time.

According to the United Kingdom’s National Heath Services report, two-third of patients coming to hospitals are over 65, and it makes hospitals unable to provide a good quality of services to all patients [2]. Additionally, today’s workforce is not proportional to the number of old people and according to the UN report only in developed countries, the population of elderly people will increase from 15% in 2014 to around 30% in 2030 [3]. Therefore we need to invest into design of autonomous systems, able to facilitate the remote patients monitoring to increase the quality and efficiency of the healthcare. The main driver to enable such shift in healthcare systems is the development of wireless communication.

There exists an extensive research on developing HMSs that rely on wireless communication for collecting medical data [4]–[6]. The collected data is used to enhance HMSs by fast detection of a possible health deterioration. The collection of data is done using wearable physiological sensors attached at the human body, as well as environmental sensors attached at the surrounding area. The design of an HMS that employs wireless communications needs to address requirements, such as: reliability, connectivity, scalability, data privacy, and timeliness.

In an HMS, different types of physiological sensor devices are needed to collect sufficient information on patients. According to the nature of the vital signs being monitored, some sensors should report their readings periodically within long intervals, while some others have to enable collection of the data continuously. Therefore, it is essential that the HMS is able to accommodate different sensor nodes with diverse sampling intervals, while providing reliability. Additionally, there are various conditions where early reporting of sensor measurements is mandatory. For instance, measurements that reflect epileptic seizures, a heart attack, or a stroke should be reported to the physicians and nurses in real-time. An HMS needs to be intelligent to detect these extreme cases and assign higher priority to these measurements to deliver them faster. A scalable network design should be able to answer questions regarding increasing (or decreasing) number of sensors, changing network topology, and data quality in terms of sampling rate, sensor sensitivity, and amount of the data.

The vision of IoT implies a seamless connectivity between different networks, which is one of the major concerns of HMSs. In HMS applications, it might be required to employ various low-power wireless networks such as Bluetooth [7], Bluetooth Low Energy (BLE) or Bluetooth smart[8], IEEE 802.15.4 [9], IEEE 802.15.6 [10], ZigBee [11], and 6LoWPAN [12], and it is a requirement for an HMS to enable interconnectivity between different technologies.

Moreover, the collected data in an HMS includes a personal information about a patient, and it is prone to malicious attacks. The privacy factors should be considered in all stages of an HMS, such as data collection, data transmission, and data storage, which becomes more challenging in heterogeneous networks, where each network has its specific level of security.

In this paper, in Section II, we motivate the need to employ heterogeneous networks for HMSs. We review the most relevant low-power radios in Section III and explain main features of their protocol stack designs in Section IV. Moreover, we highlight the limitations of conventional communication techniques and propose a generic protocol stack for heterogeneous Low-Power Wireless Networks (LPWNs) in Section V. Finally, we conclude the paper in Section VI with discussion and some future directions.

II. HETEROGENEOUS HMS

Let’s assume an HMS system that includes various types of wireless sensor nodes such as physiological sensor nodes, attached at the body of a patient, leading to a set of mobile sensor nodes, and environmental sensor nodes attached at home appliances, creating a static sensor network infrastructure as illustrated in Figure 1. Static sensor nodes are used as an
access point for the mobile body sensors to deliver their data. Moreover, additional access points (i.e., AP in Figure 1) are used to guarantee wireless connectivity all over the indoor environment.

We assume sensor nodes being equipped with the most suitable wireless radios based on their required data rate. For instance, BLE radio [8] can be used for body sensor nodes that support higher data rates, while ZigBee radios [11] can be considered for the environmental sensor nodes that have lower data rates. Mobile sensor nodes are able to send their data through either (i) an access point, or (ii) a coordinator\(^2\) (by forming a star Wireless Body Area Network (WBAN)). Considering the latter case, a conventional way to interconnect these two networks (WBAN and static infrastructure) is to employ a gateway node (e.g., smart phone) that provides seamless communication between networks with different radio technologies. However, the former case is only possible when the access points are equipped with multi-radio hardware.

Various wireless technologies have been proposed in the literature that take into account special requirements of the higher level applications. Thus, each legacy solution is designed to respond to a set of requirements, such as reliability, timeliness, scalability, security, and connectivity. For instance, in IEEE 802.15.4 MAC protocol, both TDMA and CSMA protocols are developed to accommodate both sporadic and periodic traffic in a single channel, WirelessHART [13] and ISA100.11a [14] use time slotted channel hopping MAC protocols to enhance the reliability. The IEEE 802.15.4e working group have redesigned the IEEE 802.15.4 to improve the reliability, while maintaining low duty cycles through time synchronisation and channel hopping. The frequency hopping approach is also implemented in Bluetooth, but on the other hand has provides low scalability and high power consumption. The BLE standard provides improvements in power consumption, but it lacks backward compatibility and seamless connectivity with other Bluetooth devices. Considering the aforementioned requirements in each protocol design, interconnecting these technologies would reduce the overall network performance. The reason is that each solution has been devised for a specific purpose, developed by different communities. Merging these standard protocols inherits the common features, while drops the add-on features during data delivery from one network to another network.

Integrating technologies with different capabilities and

\(^2\)A coordinator consist of a sensor, or a set of sensors that collect data from other sensors attached at the human body.

functionalities is a complex process that involves issues from all protocol layers. To obtain ubiquitous computing, a lot of work has been done to integrate various wireless platforms, such as Cellular and WiFi [15], [16], using the benefits of software-defined and cognitive radio technologies to make multi-interface and environmental aware solutions. One example is the seamless migration of a connection during downloading a large video file, while switching from Cellular network with low-data rate and high-cost to WiFi with high-data rate and low-cost. Solutions for integrating these technologies consider WiFi devices working within the Cellular networks as part of the architecture, and thus not addressing a heterogeneous architecture and services [17].

There are two main solutions to interconnect devices in a heterogeneous network [18]. Mobile IP-based techniques are used as a network architecture to integrate different networks [19], [20]. However, this approach requires fundamental changes in non-IP-based network protocol stacks, since most of Commercial-Off-The-Shelf (COTS) products prohibits using IP-based approaches in LPWNs. Using gateway devices is another solution to establish connection between different networks. These devices are intermediate nodes that transfer information between different networks. However, relying only on gateway devices would degrade the system performance, since they may become a bottleneck, delaying the transmission of critical messages.

In the next section, we provide some basic knowledge on the existing low-power radios, followed by description of their own protocols in Section IV.

III. BASICS ON LOW-POWER RADIOS

In this paper, we focus on the two most commonly used, and commercially available radio technologies that fit our target HMS application: CC2420 IEEE 802.15.4 [9] and Bluetooth. Both radios operate in the 2.4 GHz frequency band, while Bluetooth has 79 channels with bandwidth of 1 MHz, and IEEE 802.15.4 has 16 channels with bandwidth of 2 MHz.

The IEEE 802.15 working group has been initially established to create standard protocols for LPWNs. IEEE 802.15.4 has been designed for low data rate networks, while IEEE 802.15.1 or Bluetooth targets the medium data rate networks. Unlike Bluetooth, which offers the whole protocol stack from physical layer to application layer, IEEE 802.15.4 specifies only physical and data link layers. The ZigBee Alliance has proposed a standard, called ZigBee, that is the most widely deployed enhancement to the IEEE 802.15.4 standard. IEEE and ZigBee Alliance work closely to provide the whole protocol stack for LPWNs. The ZigBee standard enables the network and application-layers functionalities for the IEEE 802.15.4. The IEEE 802.15.6 [10] is standardised for WBANs and defines physical and MAC layers. Since the IEEE 802.15.6 radio hardware is unavailable for experiments, thus we skip describing its radio features, and focus on its protocol stack design in this paper.

Bluetooth low energy (BLE) is an enhanced standard Blue- tooth protocol that provides energy efficiency by adding sleep cycles when node is inactive, which makes it suitable for HMS applications. It operates in the 2.4 GHz ISM band and defines 40 channels with 2 MHz channel spacing. Three channels that have the minimum overlap with WiFi (1, 6 and 11) are the advertising channels for the broadcast purposes, and the remainder are the data channels for the unicast communication.
An adaptive frequency hopping mechanism is used for the data channels to switch the channel in case of interference and propagation issues. BLE and Bluetooth define two types of devices: a master (manages multiple connections with different slaves) and a slave device.

6LoWPAN [12] is an open standard, developed by IETF (RFC 6282) for supporting IPv6 for LPWNs, which has been integrated within IEEE 802.15.4 standard protocol. It basically adapts the long IPv6 addressing into an abstract and short frame suitable for IEEE 802.15.4 standard packet format. 6LoWPAN provides an adaptation model that supports network management, routing strategy (e.g. RPL routing), security, application interface, and network discovery (inherited from IPv6). This open standard is also under integration within other networks, including Sub-1 GHz low-power radios, such as BLE, power line control (PLC), and low-power WiFi [21].

The aforementioned standard protocols have major differences with each other, which comes from the protocol design and hardware limitations. We describe two major differences in terms of packet size and security issues.

Packet size in LPWNs. The duration of packet transmission in wireless medium depends on the packet size and the radio data rate. In IEEE 802.15.4 networks with the maximum packet size of 127 Bytes and the data rate 250 kbps, the packet transmission duration is 512–4256 µs [9]. The Bluetooth packet has three main parts: access code (72 bits length), packet header (18 bits length), and payload (0 - 2745 bits). Considering the 1 Mb/s data rate with the packet size of 90 to 2835 bits, the shortest and longest packet transmission duration varies from 90 µs to 2835 µs [22]. The transmitted packet in BLE has 1 byte of preamble, 4 bytes of access codes, 3 bytes of cyclic redundancy code, and a protocol data unit size of 2 to 39 bytes. This implies the shortest packet size of 80 Bytes and the longest 376 bytes, which concludes to the packet transmission duration between 80 µs to 300 µs by considering the 1 Mb/s data rate [23].

Security issues in LPWNs. Wireless protocols are vulnerable to security attacks in various protocol layers. Each protocol design and wireless technology provides some level of security in the specific protocol layers. In the following, we describe some of the main security features of LPWNs below.

Bluetooth and BLE have three basic security services to address issues related to authentication, authorisation, data protection, privacy, and confidentiality, using built in mechanisms to determine who is at the other end of a Bluetooth link and, whether this device is authorised to get the message. All data is encrypted, and it is possible to decrypt it only by approved devices. The address of the Bluetooth device can be encrypted, and it is very hard for an intruder to track the device. Moreover, Bluetooth provides flexibility for users to decide on the level of security to be employed. All nodes and hubs in IEEE 802.15.6 have to choose one of the three security levels that are: unsecured communication, authentication level, and authentication and encryption level, where the first level can be seen as the low security level, while the latter, as the high security level. It has been shown that all protocols have some security issues [24], such as lack of forward secrecy or key-compromise impersonation attack. Moreover, some of them have shown vulnerabilities to impersonation attack, and offline dictionary attack. To enable a secure data transmission, ZigBee networks use the advanced encryption standard (AES) encryption algorithm that is assumed as one of the most secure, robust, and reliable algorithms that encrypts 128-bit blocks of data, using multiple substitution and permutation operations [25]. ZigBee security services include: key establishment through the day centre, key transport via pre-configured TC link key, frame protection using AES-CCM with a low-cost implementation, and a device authorisation. 6LoWPAN nodes can operate in either secure or non-secure mode. So called higher-layer processes, are able to specify keys to perform symmetric cryptography in order to protect the payload and restrict it to a group of devices or just a point-to-point link. It also computes freshness checks between successive receptions to ensure that old frames, are no longer available.

IV. PROTOCOL STACKS IN LOW-POWER NETWORKS

In the following, we explain the main features of different protocol stacks, considering the standard layers and adaptations layers.

Bluetooth protocol stack. The Bluetooth protocol stack has three main parts that are grouped into: (i) Transport Protocol Group, (ii) Middleware Protocol Group, and (iii) Application Group, as in Figure 2. The first group corresponds to the Physical and Data Link layers, where it manages the communication with higher layers as well. It comprises of radio, baseband, link manager, logical link control and application (L2CAP) layers, and the host controller interface (HCI). The middleware group provides interoperability with other standard protocols and Bluetooth Special Interest Group (SIG) protocols, for instance, point-to-point protocol (PPP), Internet protocol (IP), transmission control protocol (TCP), serial port emulator (RFCOMM), and service discovery protocol (SDP). The application group consists of legacy applications that use Bluetooth-aware protocols.

The choice of radio is basically related to the design of Bluetooth transceivers. The baseband defines how devices connect to each other, based on master-slave communication strategies and frequency hopping mechanism. It manages the packet transmission policy in a specific pre-defined time-slots, error detection and correction, encryption and re-transmissions. It supports synchronous and asynchronous communications. The asynchronous communication supports sending packets.
The interoperability concern has been considered within the Bluetooth stack design, where it has been designed in to enable interoperability between Bluetooth devices manufactured by different companies. This has been achieved by matching various applications in remote devices to run over identical protocol stacks. Thus, existence of additional radios and backward compatibility with the oldest versions of Bluetooth has not been tackled.

**BLE and IPv6-enabled BLE protocol stack.** The BLE protocol stack is layered in such a way to facilitate IP communications. Generally it has three main groups of controller, host, and applications [23]. Figure 3 illustrates the BLE and IPv6-based BLE protocol stacks. The controller is responsible for physical and data link layers. Similar to Bluetooth, the HCI unit separates the controller part from the host part. In BLE, the host implements the functionalities of the upper layers, which includes attribute protocol (ATT), generic attribute profile (GATT), generic access profile (GAP) and a security manager (SM). GAP defines procedures for discovering BLE devices and managing their connectivity. ATT allows attribute server to expose attributes and their associated values to an attribute client. GATT describes a service framework using ATT to discover services. SM is responsible for a device pairing and a key distribution, while it also implements a resource management policy. In IPv6-based BLE that is under the development, the host consists the transport layer, suitable for IoT devices. The IP support inserts a 6LoWPAN adaptation layer, where it enables the coexistence of the native and IPv6-based BLE within the same network [8]. To add 6LoWPAN layer, the L2CAP layer should be customised for IPv6 support.

Similar to Bluetooth, the BLE protocol stack ensures interoperability among Bluetooth-, and BLE-enabled devices implementing different specifications. Additionally, HCI allows interoperability between hosts and controllers produced by different companies.

**IEEE 802.15.4 and ZigBee protocol stack.** The IEEE 802.15.4 protocol defines the physical and data link layers. ZigBee Alliance standardised the higher layers of the protocol stack, which are network and application layers [26]. Figure 4 illustrates the protocol stack of both IEEE 802.15.4 and ZigBee standards. The network layer provides routing in a multi-hop network and it is responsible to support joining and leaving of nodes in the network. It applies a security mechanism to frame packets and then routes them to their intended destination. The application layer has three sub-layers, which are defined as follows:

- the application objects (AOs) that are manufacturer-defined objects based on the requirements of the applications and users;
- the application support sub-layer (APS), which is responsible for communication with other applications, maintaining binding tables and sending messages between nodes;
- the ZigBee device object (ZDO) that defines functions for network operation. The role of devices as a coordinator or router is defined by ZDO.

**6LoWPAN protocol stack.** Figure 5 illustrates the 6LoWPAN protocol stack, which has been inherited from the typical IP protocol stack and IEEE 802.15.4 [12]. In this architecture, the physical and data link layer are based on the IEEE 802.15.4 implementation. The higher layers are the abstract version of

---

**Fig. 3:** BLE protocol stack, including application, host and controller groups.

**Fig. 4:** IEEE 802.15.4 and ZigBee standards protocol stack.

**Fig. 5:** The 6LoWPAN protocol stack.
IP protocol stack, which have been simplified for low-power networks. Usually, 6LoWPAN is known as an adaptation layer that is bridged between the data and the network layer. The IETF routing protocol is called RPL, which communicates with the 6LoWPAN and the transport layer. The most common transport layers used in 6LoWPAN are user datagram protocol (UDP) and the Internet control message protocol v6 (ICMPv6).

IEEE 802.15.6 protocol stack and frequency bands. The IEEE 802.15.6 is a task group concentrating on standardising WBANs. This standard defines two OSI layers: data link and physical layers (Figure 6(a)). The design of its MAC sub-layer permits using various radios; such as narrowband (NB), ultra-wideband (UWB) and human body communications (HBC) as illustrated in Figure 6(b). It means that all the radios working in the ISM band are allowed to work within this standard protocol. Due to the lack of a network layer, this network supports one-hop star topologies, where a special relay node is used to enable two-hop networks.

V. ENVISIONED GENERIC PROTOCOL STACK

With the increasing number of low-power radios and the future vision of the IoT providing seamless connectivity between devices, the communication networks have to be able to intelligently manage interoperability within heterogeneous networks. Therefore, we propose a generic protocol stack that focuses on all layers and reuses advantages of the existing protocol stack designs.

A conventional generic protocol stack consists of a multiple physical layers, data link layers, and MAC layers, but only one network, transport, and application layer [18]. Based on the requirements, a specific combination of lower layers is selected, while all networks are supposed to have similar upper layer protocol designs. In our proposed protocol stack, we define layers in such a way to provide the common constructs of all LPWN protocol stacks, while adaptation layers are supposed to add extra features to provide a reasonable network performance.

Figure 7 illustrates the proposed stack with three major parts, as in (i) IEEE 802.15.4 and IEEE 802.15.6 standards, (ii) Bluetooth and BLE specifications, and (iii) IETF implementations.

In general, the generic protocol stack has to provide interoperability at different aspects, such as: (i) physical integration that focuses on interconnecting different devices, (ii) application integration that considers executing different applications concurrently, and generating packets independently, and (iii) business integration that coordinates various business processes.

The main features of the proposed protocols stack are:

1) Supporting IP-based (with 6LoWPAN implementation - adaptation layer between the L2CAP and transport layer) and non-IP-based protocols to facilitate various protocol designs. In this protocol stack, networks are not obliged to add transport layer to support Internet connection, since the adaptation layers are supposed to bridge the gap and provide an abstract IP addressing.

2) Supporting all types of a low-power radio hardware. All the existing radios within NB, HBC and UWB can be used and simply communicate with the higher layers. The physical layer is similar to one in IEEE 802.15.6.

3) Re-configurability and maintainability of the network by managing data communication and routing path.

With this we achieve the main requirements for a heterogeneous HMS system, including seamless connectivity, reliability, timeliness, security and scalability. Providing adaptation layer for IP-based addressing enables seamless connectivity and security. Scalability is provided by adding the mesh networking concept within the transport layer. Reliability and timeliness are dependent on the various situations, such as external interference and network collision. An enhanced MAC design eliminates packet collision, while a channel hopping algorithm reduces the chance of interference, and thus packet losses. As it comes to security, the use of the generic protocol stack might enable means for a security insurance through one robust and efficient security framework, instead of focusing on separate technologies, as it is the case now.

Let us assume an example depicted in Figure 1, and employing the generic protocol stack in all devices. The devices are able to communicate directly with the coordinator, APs, home appliances and gateways that are equipped with multi-radios (e.g., using CC2650 radio [27]). A message generated by the BLE radio is reachable by a multi-radio with generic protocol stack. The L2CAP adaptation layer transfers the message from the data link towards the 6LoWPAN adaptation.

---

3The CC2650 device is an ultra-low power wireless microcontroller, targeting BLE, ZigBee and 6LoWPAN applications.
layer, to ensure abstract IPv6 that brings into the picture an additional security level. Furthermore, the message reaches the application layer with multiple services, such as REST-full [28] and CoAP [29] web services that support interoperability at the application layer.

The same process with message reconfiguration at the intermediate nodes is applied to a message generated by the ZigBee radio when it reaches at any multi-radio node. The ZigBee radio will be enriched by a proper MAC protocol, since its protocol stack lacks this layer. The HCI layer implements the main features needed for the Bluetooth hardware driver. Thus, the message will be meaningful for other devices with Bluetooth radio that receives the same message. This makes it possible to activate communication between two WBANs through intermediate multi-radio nodes, while WBANs are equipped with different radios, such as Bluetooth and ZigBee. This approach opens new possibilities to design various generic stacks based on the proposed structure, while tuning the standard and adaptation layers based on the system specific requirements.

VI. CONCLUDING REMARKS

In this paper, we address one of the major challenges for an HMS, known as interoperability, required for heterogeneous networks. In an HMS, with various radio technologies and network designs available, providing inter-connectivity is a complex task. We propose a generic protocol stack that inherits the common features of all LPWAN protocol stacks, and implements adaptation layers to enable extra features missing in some of the existing network protocols. With this approach, we provide a network performance, while addressing network connectivity and interoperability. Our future work includes implementation of the basic primitives of the protocol stack within one of the existing operating systems for sensor networks.

ACKNOWLEDGMENTS

Authors would like to thank to associate professor Elisabeth Uhlemann for discussions and valuable comments on the early versions of the paper. This work is funded by the Swedish Knowledge Foundation (KKS) throughout research profile Embedded Sensor System for Health (ESS-H), the distributed environments Ecare@Home, and Research Environment for Advancing Low Latency Internet (READY).

REFERENCES


