Prevailing over Wires in Healthcare Environments: Benefits and Challenges

David Cypher, Nicolas Chevrollier, Nicolas Montavont, and Nada Golmie, National Institute of Standards and Technology

ABSTRACT

The objectives of this article are to survey the benefits and challenges posed by the deployment and operation of wireless communications in support of healthcare networks. While the main advantage of wireless communications remains to provide ubiquitous connectivity, thus allowing greater physical mobility and interoperability, a number of engineering issues need to be addressed before this vision is realized. Our intent in this article is to explore some of these issues, including deployment, interference, and mobility, and provide insights for potential solutions.

INTRODUCTION

The reliance on network technologies in healthcare and clinical environments for monitoring, diagnosis, surgery, and treatment stresses the need for universal and wireless network interfaces that provide reliable connectivity and untethered access to information.

The main argument in the case for wireless stems from the need to provide better access and enable greater physical mobility. Other considerations that may arise include the cost of deploying and maintaining a wired network and the interoperability between networked devices. Currently, most network connections are based on RS-232 port interfaces, which are made permanently to stationary monitors. In addition to the cost and time required to rewire buildings and hospitals in order to plug more devices into the network, severe incompatibility issues arise because each device manufacturer defines its own data-link communication method. Therefore, proprietary drivers must be loaded every time a different device is plugged into the network, making it unrealistic to plug in mobile devices several times during the day.

The IEEE 1073 Medical Device Communications standards organization is currently developing specifications for wireless interface communication. The main objective for this effort is to develop universal and interoperable interfaces for medical equipment that are

- Transparent to the end user
- Easy to use
- Quickly (re)configurable

Since designing wireless technologies from scratch in order to satisfy the needs of the healthcare industry may not be a viable or economical option, the group is focusing instead on evaluating the suitability of currently available and emerging technologies developed by the IEEE 802 Local Area Network/Metro Area Network standards organization.

Part of this evaluation work consists of matching medical device application requirements with the appropriate wireless technology. While reliable connectivity constitutes a requirement for all healthcare applications, additional constraints imposed on the timeliness and the criticality of information delivery, such as bandwidth, delay, and loss, depend on the specifics of the application considered. Given the nature and the diversity of the applications envisioned for healthcare, let alone the many constraints imposed by the environment, it is most likely that different medical applications will use different wireless technologies. Therefore, a number of questions arise with respect to deployment and operation issues. For example, are there any pitfalls that can be avoided in the deployment of such systems? Does simultaneous and proximal operation lead to interference? What are the mobility requirements of such systems? What are the effects on the application's performance?

Our objectives in this work are to provide a survey of some of the benefits provided by the use of wireless technologies in healthcare, and also capture the challenges that may affect the deployment and the operation of wireless network technologies in the healthcare environment. The remainder of this article is structured as follows. First, we list a few example medical applications. We then survey candidate wireless technologies and show how to find adequate pairings between the medical applications and currently available wireless technologies. The article next explores wireless network deployment issues ranging from coverage area through frequency allocation and network architecture to transmitted power. Part of the article is then devoted to discussing interference issues in the 2400 MHz band. We go over an illustrative scenario consisting of multiple medical applications using different wireless technologies. This example is intended to show the impact of interference on performance and the extent of the resulting performance degradation. We discuss the implications related to supporting physical and network mobility in healthcare. Concluding remarks are given in the last section.

WHAT ARE HEALTHCARE APPLICATIONS?

In this section, medical applications are discussed and several examples are given. In order to understand some of the network requirements posed by applications, the Electrocardiogram (ECG) is selected as an example medical application. A similar approach is applicable to all other medical applications.

MEDICAL APPLICATIONS

There are two broad categories of healthcare applications. There are those that are specific to medical data and those of general purpose, but used in a medical environment, also known as healthcare informatics.

Medical data healthcare applications are usually specific to the medical device that collects or generates medical data. Some examples of these medical devices are: infusion devices, vital signs monitor (VSM), ventilator, pulse oximeter, defibrillator, electrocardiogram (ECG), blood pressure, temperature, airway flowmeter, cardiac output, capnometer, hemodynamic calculator, respirator, weigh scales, and dialysis devices.

Patient records, Internet access, and other administration information are considered healthcare informatics, since they are similar to general applications such as database manipulation. Video conferencing and remote device control (e.g., a camera) are other examples of general-purpose applications that are used in the medical environment. However, in some of these cases, there may be additional application requirements, such as whether the remote control was used during a critical operation or for the delivery of the dosage of a medication.

Before a type of transport medium can be chosen, such as cable or wireless, several factors have to be considered in the transport of medical data from the collection device to the display device. These factors include the type, amount, and frequency of the data generated, and constitute the application requirements. In the following section, we use the electrocardiogram (ECG) application as an example of an application requirement that comes into play for designing a medical data transport.

ELECTROCARDIOGRAM

The ECG application is a recording of the electrical signals from the heart (Fig. 1a). These electrical signals are continuous and must be periodically sampled in order to be digitized

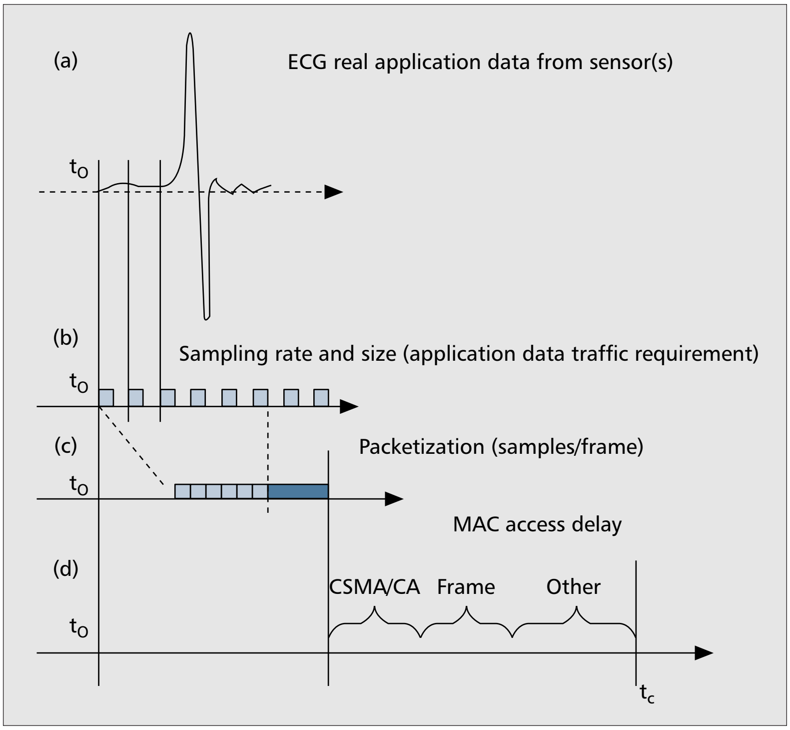

Figure 1. *From heart beats to digital bits.*

(Fig. 1b). The sample frequency and digitization method play a critical role in determining the traffic characteristics for transport. There are a number of sampling and digitizing methods to choose from, as well as various compression techniques.

For example, if the electrical signals from the heart were sampled and digitized at a rate of 500 samples per second with a sample size of 8 bits (1 byte), then the resultant ECG application data traffic requirement would be 4000 bit/s (500 byte/s). The user expects the data to be displayed instantly.

In the next section we use this application's data traffic and timing requirements to select a wireless technology for its transport.

HEALTHCARE APPLICATION WIRELESS TRANSPORT

This section considers several candidate wireless technologies that may be used for the transport of medical applications. After a brief introduction of the wireless technologies available, an example is given of pairing the ECG application with the candidate wireless technologies considered.

CANDIDATE WIRELESS TECHNOLOGIES

The candidate wireless technologies that we investigate are standards developed by IEEE 802. The wireless local area network (WLAN) defined in the IEEE 802.11 [1] family of standards uses a single media access control (MAC) sublayer with many different physical layers (e.g., 802.11a [2] and 802.11b [3]).

The wireless personal area network (WPAN) is also a family of standards, but unlike 802.11, each defines its own MAC sublayer and physical

Technology	802.15.4	802.15.1	802.11b
Network type	WPAN	WPAN	WLAN
Modulation	DS	FH	DS
Number of channels	16	79	11
Channel width (MHz)	2	1	22
Coverage area (m)	< 10	< 10	< 100
Data rate (Mb/s)	0.25	1	11
Data service	Unack, ack	Acknowledged	Acknowledged
Medium access	CSMA/CA	TDMA	CSMA/CA

Table 1. *The candidate wireless technologies.*

layers. Covered here are IEEE 802.15.1 [4], which is designed as a cable replacement and includes the lower layers of the Bluetooth specification developed by the Bluetooth Special Interest Group (SIG) and the IEEE 802.15.4 [5], which is designed for low data rates, low power consumption, and low usage applications and is promoted by the Zigbee Alliance.

The main characteristics of these are shown in Table 1. The importance of these will be covered in subsequent sections as appropriate.

Pairing ECG to Candidate Wireless Technologies

This pairing focuses on the packetization (framing and the sample accumulation delay, Fig. 1c). Considering just the ECG data-rate traffic requirements (4 kb/s) with the wireless raw data rates (i.e., capacity), it appears that 802.15.4 (250 kb/s) is more appropriate than 802.11b (11 Mb/s) or 802.15.1 (1 Mb/s). From an analytical perspective, when using IEEE 802.15.4 for ECG, the maximum payload size allows up to 118 sample/frame bringing the accumulation delay to 236 ms. The minimum data sampling rate of 1 sample/frame results in an accumulation delay of 2 ms.

Now that a frame size is determined, we consider the method for accessing the medium that also contributes to the end-to-end delay. The 802.15.4 uses carrier sense multiple access with collision avoidance (CSMA/CA), which produces a random access delay for each frame. This access delay is shown generically in Fig. 1d. For 802.15.4 and ECG, the medium access delay ranges from 1.024 to 5.216 ms as the number of samples per frame varies from 1 to 118 when there is success on the first attempt to transmit the frame. When multiple attempts to transmit are needed due to varying the load on the network, this can increase to a maximum of 36.8 ms before the packet is dropped. Dropping a frame (packet loss) is another application requirement to consider.

IEEE 802.15.4 supports two types of data services: acknowledged and unacknowledged, which contribute to delay and overhead. Since the ECG application is more sensitive to time delays than to packet loss, the unacknowledged data service is used [6].

At this point only packetization, framing, and medium access delay are considered for pairing an application to a wireless technology. In later sections, other factors such as deployment, interference, errors, and mobility are considered.

Deployment Issues

In the previous section several considerations (packetization, framing, access delay, and data service) for pairing ECG's requirements to the IEEE 802.15.4 wireless technology were described. We continue with this example by considering deployment issues such as coverage area, network architecture, frequency allocation, and output power and their associated challenges, in order to determine whether the pairing choice is still acceptable.

Figure 2 describes a basic user case for the potential use of wireless technologies in a healthcare environment. Several ECG leads on a patient's body collect the medical information, which is displayed on a monitor located at the patient's bedside. This information is also transmitted to another hospital location for remote monitoring (e.g., a nurses' station). In case of emergency, when the patient is moved from his/her room to the intensive care unit, these communications need to be maintained. We are interested in investigating the various issues associated with the wireless communications in this scenario.

Coverage Area

Designed coverage areas vary from the body area (< 1 m), personal area (< 10 m), local area (< 100 m), to wide area (> 100 m). The 802.15 family is designed for communications in the personal area while the 802.11 covers the local area. In reality, coverage areas vary widely based on radio frequency used and the physical environment. For the personal area this is an advantage, since it allows for the signal to be constrained within its limited usage area, while for the local area it is a detriment, since its goal is to cover larger distances. Since the ECG's communicating devices are in close proximity to each other, a personal area wireless technology (e.g., 802.15.4) is a likely choice. However, for further relaying the ECG data to the nurses' station, a local area wireless technology may be needed.

Network Architecture

Some wireless technologies are designed with infrastructure, while others are designed for ad hoc communications. The IEEE 802.11 was designed for both. Its infrastructure mode assumes a fixed access point (AP), which attaches to the established fixed network infrastructure and thus provides a communication portal for stations (STA) in range of the AP. Its ad hoc (or self-organizing) mode permits devices to dynamically communicate with other peer devices. IEEE 802.15 uses this ad hoc mode. The ad hoc nature is convenient for quick deployment, but potentially disastrous for static RF management control, which will be discussed below. For the

ECG application where the sensors are communicating with the bedside monitor, an ad hoc mode is more appropriate.

FREQUENCY ALLOCATIONS

The radio frequency spectrum covers a wide range (3 kHz to 300 GHz). In the United States, this range is divided into numerous usage bands by the Federal Communications Commission (FCC). In this respect, the RF allocation is outside the control of the medical environment's management. There are several of these usage bands such as Industry, Scientific, Medical (ISM) available for medical usage, but they are shared with other users. The selection of which ISM band to use is the first consideration. For the three candidate wireless technologies considered (i.e., 802.11b, 802.15.1, and 802.15.4), all use the 2400 MHz ISM band. IEEE 802.11a and IEEE 802.15.4 have some channels in other bands, which may be an option when the 2400 MHz band is overcrowded. After selecting the RF allocation, the next step is to determine how the wireless technology uses the band.

Figure 3 shows the channelization or the segmentation of the 2400 MHz ISM band. The sharing of the wireless channels causes interference. The significance of interference, the need to avoid it, and interference mitigation techniques are described in the next section. For now, we concentrate on the configuration of the channels to avoid or reduce interference by planning for no overlapping of channels. Channel configuration may occur statically (manual) or dynamically and for a single wireless technology or multiple wireless technologies. For IEEE 802.11b, only three nonoverlapping channels can be manually selected out of the 11 channels available. For IEEE 802.15.4's 16 channels and IEEE 802.15.1's 79 channels, none overlap. However, for IEEE 802.15.1, since it uses frequency hopping (FH) rather than direct sequence (DS), all 79 channels are used by every communicating device at some point in time. Thus, manual channel configuration is only applicable to DS technologies, not FH technologies. Continuing with manual configuration given one wireless technology, is it possible to configure channels from another wireless technology? For 802.11b and 802.15.4, there exists channels in both that will permit nonoverlapping channels. The trade-off is a reduction in available channels. However, if IEEE 802.15.1 (or any FH wireless technology) is added to any of these individually or in combination, no manual configuration exists. Dynamic allocation is when the devices determine the channel or channels to use based on some criteria, for example, interference mitigation.

OUTPUT POWER

The amount of output power used to generate the wireless signal affects not only the coverage area, but also affects the power consumption of the wireless device. For WLANs the assumption is that the devices will be powered by mains, while the assumption for WPANs is that the devices will the powered by batteries. IEEE 802.15.4 specifies a number of ways to reduce the power consumption and still maintain its coverage area. Since the incentive for wireless is to remove wires, the ECG sensors are battery powered.

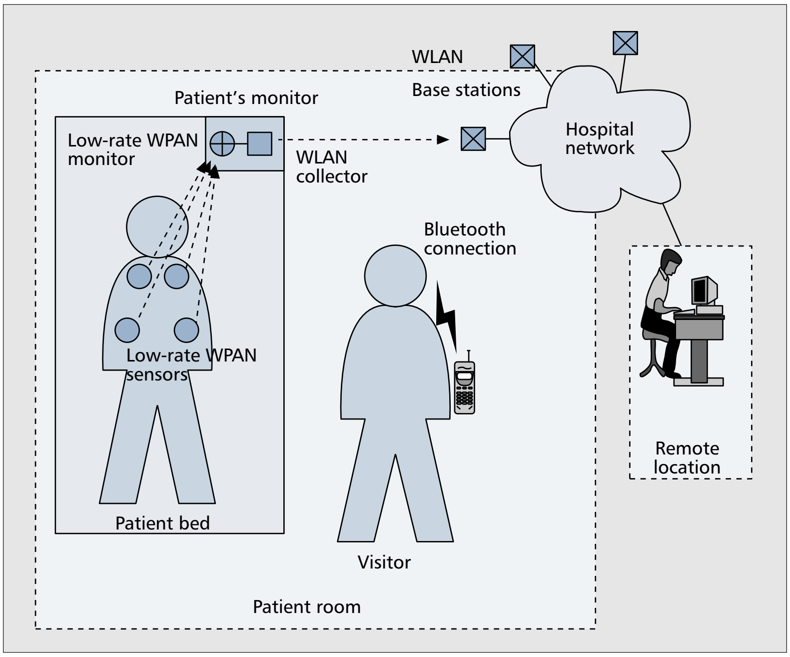

Figure 2. *Room topology.*

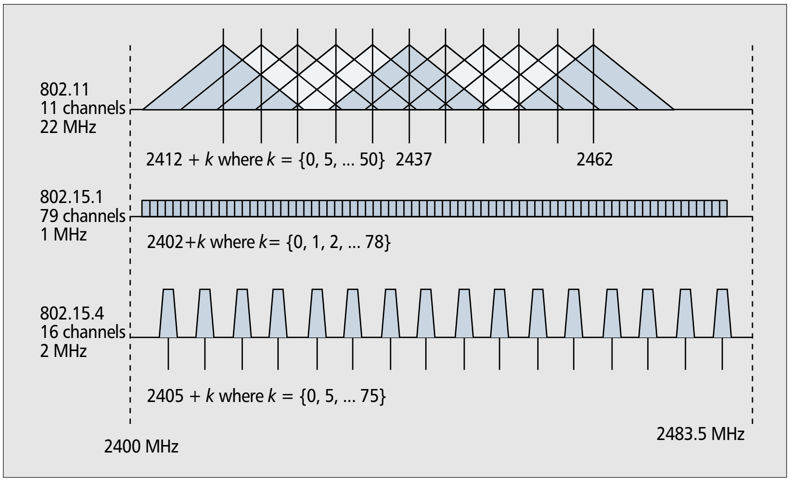

Figure 3. *Frequency map for select IEEE 802 specifications in the 2400 MHz band.*

LOCATION MANAGEMENT

A method used for location management involves managing the physical locations for using these technologies. However, this method may not be practical if one cannot prevent the inherent mobile natural of wireless capable equipment or when patients move from one facility to another, such as from the emergency room to the operating room, to intensive care, or to a regular patient's room.

REVISITING THE ECG AND THE WIRELESS TECHNOLOGY PAIRING

For the topology depicted in Fig. 2 and based on different considerations described in this section, Interference mitigation techniques can be divided into two main categories: collaborative and noncollaborative mechanisms. Collaborative mechanisms require communication between heterogeneous protocol stacks; noncollaborative mechanisms do not require direct communication between heterogeneous protocol stacks.

IEEE 802.15.4 can still support the ECG traffic and usage scenario. WLAN is preferred to establish a wireless connection between the central monitor device at the patient's bedside and the hospital network because of its large coverage area and its infrastructure mode, which enables access to the hospital network and supports mobility. From an RF perspective, as described above, it is possible to select nonoverlapping channels (for example, 2410 MHz for low-rate WPAN and 2462 MHz for WLAN) to avoid any interactions between the two technologies. In this user case, wireless technologies peacefully coexist thanks to pertinent network design.

However, not everything can be anticipated and the fundamental nature of wireless devices allows them to appear anytime, anywhere. In this heterogeneous wireless environment, two critical issues arise. The first issue is: How significant will the interference be among the various wireless technologies? This is the topic of the next section. The second issue is: Will there exist a need to have devices access whichever wireless technology is available in order to maintain communications? This is covered subsequently.

Interference in the 2400 MHz Band

As described in the previous section, a proactive network design can anticipate potential interference among wireless technologies. However, inherent to the wireless technology characteristics, a device can appear anytime, anywhere. These unpredictable appearances challenge the viability of a preplanned wireless network configuration. In fact, how well these wireless devices are able to operate in close proximity to each other, especially those employing the same 2400 MHz ISM frequency band, will be discussed in this section along with potential mitigation techniques.

Effects of Interference in a Walk-In Usage Scenario

The usage scenario described in Fig. 2 illustrates an ideal network design. Low-rate WPAN channels are manually chosen in order to avoid overlapping with WLAN channels, thus guaranteeing coexistence between the two technologies. We extend this basic scenario by adding an individual entering the patient's room using devices equipped with the Bluetooth technology (e.g., doctors exchanging data between PDAs, a visitor using his cell phone via a Bluetooth earset). As explained in the previous section, Bluetooth technology uses a frequency-hopping technique. Consequently, during a communication, a Bluetooth device's FH spans the entire frequency band. Thus, in our extended scenario, overlapping between Bluetooth channels and WLAN or low-rate WPAN channels is inevitable.

We simulate this walk-in user case where the low-rate WPAN sensors carry ECG traffic. The collection of this traffic is transmitted via the WLAN connection to a remote hospital location and, in the meantime, a visitor carrying a Bluetooth device enters the patient's room. In this walk-in user case, we look at the packet loss at the MAC sublayer of the low-rate WPAN monitor to characterize performance.

In this particular wireless environment, communications are deeply impacted. As the Bluetooth piconet gets closer to the patient's bed, the packet loss at the low-rate WPAN monitor is up to 60 percent at very close range (i.e., 0.5 m) and is still significant (i.e., 18 percent) when the Bluetooth piconet and the low-rate WPAN monitor are 2 m apart. With respect to the topology chosen, the transmission power of each technology, and the traffic characteristics, the impact on the WLAN devices and the Bluetooth pair is less significant. Additional studies [7, 8] have shown that, in different scenarios, most of the time there is a mutual impact between DS spread spectrum technologies (e.g., WLAN and low-rate WPAN) and FH technologies (e.g., Bluetooth). With this simple and likely walk-in user case, one can see that unexpected appearances of wireless devices can severely impact the existing surrounding wireless environment. In order to tackle this issue, interference mitigation techniques need to be in place, since administrative means seem to be doomed to failure.

Interference Mitigation Techniques

Interference mitigation techniques can be divided into two main categories: collaborative and noncollaborative mechanisms. On one hand, collaborative mechanisms require communication between heterogeneous protocol stacks. One wireless technology is then aware of the communication of another, thus delaying or adapting its transmission accordingly as it has been developed in [9] to enable peaceful coexistence between WLAN and Bluetooth devices.

On the other hand, noncollaborative mechanisms do not require direct communication between heterogeneous protocol stacks. Instead, they rely on channel or network measurements to detect the presence of other wireless devices. Such measurements range from the bit or frame error rate to the signal strength or the signal-to-interference ratio. Based on these measurements, techniques are implemented to avoid a simultaneous use of the same frequency. Two basic strategies are envisaged, namely, time-division multiplexing (TDM) and frequency-division multiplexing (FDM). In TDM, transmissions are postponed while waiting for an interference-free channel. Such a mechanism can significantly reduce the packet loss at the cost of some additional delay due to the transmitter having to wait for an error-free channel. An application of this technique was used in [8] to enable coexistence between the Bluetooth and DS technologies. On the other hand, FDM techniques allocate different portions of the frequency band to a specific group of communicating devices. In Bluetooth, a unique random FH pattern is derived for each piconet in order to limit the interference between neighboring piconets.

It is evident that neither the TDM nor the FDM technique can totally eradicate interference. Also, as in the case of most reactive measures, the communication has to be impacted first before an adaptive mechanism is triggered.

One can envision that for the healthcare environment, where interference cannot be tolerated, a strict monitoring and control of spectrum usage is put in place in order to constantly detect spectrum usage and direct the choice of which technology to use.

Handling Inherent Mobility of Wireless Transport

One of the main advantages of using wireless technologies in healthcare environments is to enable devices to move. As depicted in Fig. 2, mobility in the healthcare environment is everywhere. From the patient's bed network, moving to an intensive care unit and to the visitor using his Bluetooth earset with a cellular phone, wireless technologies will certainly imply devices in motion at some point of time, even during an ongoing communication. Mobility includes various concepts that are detailed in this section.

Enabling Motion

The wireless nature of the technologies makes user motion common. Geographical motion of the user follows different mobility patterns, according to the environment of the user, the means of transportation, and the application used. In a healthcare environment (e.g., inside a hospital building), we assume a user's mobility to be walking speed. Users may transport their wireless devices from room to room, or between different floors of a hospital.

- If the communication between two wireless devices does not use any intermediate hop, the devices need to remain in their common coverage area to maintain communication. For example, this is the case for the Bluetooth communication between a cell phone and a corresponding earset, or for the communication between the low-rate WPAN sensors and their monitor. These devices need to move together in order to stay connected.
- If wireless nodes are communicating through a wireless AP, mobility management is needed when devices are moving out of range of their point of attachment. Basically, these devices need to perform a handover to another AP. Still, considering the scenario depicted in Fig. 2, a handover is needed if the patient's bed together with the patient's monitor are moving out of the coverage area of their current WLAN AP.

In both cases, the geographical mobility of devices implies many issues, such as interference effects when several devices operating in the same frequency get closer to each other or mobility management across wireless APs and/or networks. Mechanisms such as mobile IP allow flow persistence after a handover, but communication disruption may occur to the applications. In the remaining subsections we focus on an infrastructure mode, where each mobile node needs to be connected to a point of attachment (i.e., IEEE 802.11 model). We explain the handover issue and describe current solutions to minimize the interruption time observed by mobile nodes.

Handover Management

The handover process is the operation of changing the point of attachment to the infrastructure. Two different levels of handover can be distinguished, according to the topology of the network. If the old and new APs share the same subnet, only a layer 2 handover is needed. The mobile node only needs to associate with the new AP. In addition, if the two APs are connected to a different subnet, a layer 3 handover must take place as well. A layer 3 handover consists of determining a valid address on the new subnet, and updating the address to use on correspondent node(s).

When a mobile node loses its connection with its current AP, it switches to a promiscuous mode and engages a layer 2 handover. The layer 2 handover consists of three stages [10]: the discovery phase, the authentication phase, and the association phase. The discovery phase may be accomplished by using either passive or active scanning. If the mobile node uses passive scanning, it only waits for a beacon message, which is periodically sent by the access point. This beacon contains the necessary information for the mobile node to choose its future AP.

In the active scanning mode, the mobile node aggressively requests responses from the AP(s) by sending *Probe Request* messages. APs in range reply with a *Probe Response* message, which basically contains the same information as the beacon frame.

Different algorithms and timers may be used by mobile nodes to scan for available APs. For example, one can choose to attach to the first AP found, while another could first scan all channels before selecting the target AP. These various algorithms result in different latencies in the layer 2 handover. Simulation studies [11] have shown that the handover latency range from about 10 to 80 ms, depending on the number of channels that the mobile node has to scan before selecting a new AP.

The Authentication phase follows the Discovery phase. It allows the mobile node and the AP to exchange their identity and possibly a key for further data exchange. However, this mechanism has been shown to be very weak and most of the time is not used anymore, especially in sensitive environments.

IEEE 802.11i [12] and IEEE 802.1x [13] have defined a new authentication mechanism that takes place after the association with the target AP. Once the association is made, only control packets exchanged between the mobile node and an authentication, authorization, and accounting (AAA) server can traverse the AP. Once authentication and key exchange are completed, data packets can be sent and received by the mobile node on the new AP.

The association only consists of the exchange of two frames, mainly in order to allocate an association identifier to the mobile node.

If the old and the new APs are not connected to the same subnet, a layer 3 handover is needed. Once the new connection with the new AP is done, the mobile node has to discover the layer 3 information of the link. For example in IPv6, this information is advertised in *Router Advertise-*

The wireless nature of the technologies makes user motion common. Geographical motion of the user follows different mobility patterns, according to the environment of the user, the means of transportation, and the application used. In a healthcare environment, we assume a user's mobility to be walking speed.

The process of pairing medical application to a wireless transport requires a thorough understanding of the medical application considered, the detailed functions and capabilities of the wireless technology, and the deployment environment.

ment periodically sent over the IPv6 link by routers. Mobile IPv6 proposes that Router Advertisement should be sent between 30 and 70 ms in order to meet the trade-off of minimizing the bandwidth used to send Router Advertisement and minimize the discovery time. Moreover, if the mobile node is aware that its IPv6 link has changed (e.g., via L2 triggers), it can explicitly solicit a Router Advertisement by sending a *Router Solicitation*.

Once the mobile node knows the new parameters associated with the new link, a mechanism is needed to update its location with its correspondent. Mobile IPv6 [14, 15] proposes a mechanism to redirect packets to a temporary location for the mobile node. Each node has a binding cache which contains the permanent address of the mobile node (namely, Home address) and the current, temporary address of the mobile node (known as care-of address). IPv6 headers are used to hide the temporary address from the application (i.e., the application socket is always opened through the home address of the device). When the care-of address of the mobile node changes, it sends a Binding Update with the new care-of address. If a correspondent node does not support Mobile IPv6 features, or in order to reach a mobile node while attached to a visited network, a home agent is used. The home agent is a router in the home link of the mobile node, which is in charge of redirecting packets intended to the mobile node to its current location. In [11], it is shown that layer 3 handover latencies range from 80 to 150 ms.

Impact on Deployment and Interference

As we have seen, user mobility is a benefit for the user who enjoys moving while being in communication. However, this feature requires specific management.

On the one hand, mobility management mechanisms are needed to maintain the ongoing communication of a mobile device, when moving out of the coverage area of its point of attachment. Moreover, user mobility brings the need to dynamically (re)configure each of the wireless technologies using the same frequencies. As a mobile device gets closer to other devices using the same frequencies, it may interfere with devices that have been well configured.

On the other hand, a handover can be used to mitigate interference that might be observed when several devices operating at the same frequency get closer. In the latter case, flow redirection can be done on another wireless AP operating on another channel if available, or on another technology if the device is equipped with multiple network technologies in order to free the impacted channel.

In most cases, handover will cause degradation in the user applications' performances by introducing, for example, delay or packet loss. These degradations may have different impacts, according to the requirements of the application. Some of them may be managed by the corresponding MAC sublayer via retransmission. For real-time application, or very sensitive data transfers, delay or packet loss may have dramatic consequences.

Summary

In this article, we have explored the use of wireless communications to transport medical applications. We surveyed several candidate wireless technologies, such as IEEE 802.11, 802.15.1, and 802.15.4, which can be used to support the traffic characteristics and connectivity requirements of these medical applications. ECG is used as an illustrative example in order to highlight engineering choices such as packetization and access control rules that come into play when designing a wireless transport. Key issues related to deployment are also considered ranging from coverage area, frequency allocation, network architecture, interference, and mobility. For each issue identified, we discuss how design choices affect the performance and suggest potential approaches for optimizing the overall network performance.

The process of pairing medical application to a wireless transport requires a thorough understanding of the medical application considered, the detailed functions and capabilities of the wireless technology, and the deployment environment. Since neither the deployment environment nor the availability of wireless technologies is static, this remains an iterative process subject to continuous evaluation in order to satisfy all the operation requirements.

The lessons learned from this study point to the need for careful analysis of the trade-offs associated with using wireless networks in healthcare environments. The obvious benefits introduced by wireless technologies in terms of eliminating cumbersome wires, enabling mobility, and facilitating cheaper deployment should always be evaluated against potential side effects, including interference and deployment management.

References

[1] IEEE Std. 802.11-1999/8802-11 (ISO/IEC 8802-11:1999), "IEEE Standard for Information Technology, LAN/MAN-Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1999.

[2] IEEE Std. 802.11A-1999 8802-11, A (ISO/IEC 8802-11/Amd 1), "Information Technology: Telecommunications and Information Exchange Between Systems, LAN/MAN-Specific Requirements," 1999.

[3] IEEE Std. 802.11B-1999, "IEEE Local and Metropolitan Area Networks, Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band," 1999.

[4] IEEE Std. 802.15.1-2002, "IEEE Standard for Information Technology, Telecommunications and Information Exchange Between Systems, Local and Metropolitan Area Networks: Specific Requirements,Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks," 2002.

[5] IEEE Std 802.15.4-2003, "IEEE Standards for Information Technology Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)," 2003.

[6] N. Golmie, D. Cypher, and O. Rebala, "Performance Analysis of Low-Rate Wireless Technologies for Medical Applications," Elsevier Comp. and Commun., vol. 28, no. 10, June 2005, pp. 1255–75.

[7] N. Chevrollier and N. Golmie, "On the Use of Wireless Technologies in Healthcare Environments," *Proc. ASWN '05*, Paris, France, June 2005.

[8] N. Golmie, N. Chevrollier, and O. Rebala, "Bluetooth and WLAN Coexistence: Challenges and Solutions, *IEEE Wireless Commun.*, vol. 10, no. 6, Dec. 2003, pp. 22–29.

[9] J. Lansford, A. Stephens, and R. Nevo, "Wi-Fi (802.11b) and Bluetooth: Enabling Coexistence," *IEEE Network*, vol. 15, Sept/Oct. 2001, pp. 20–27.
[10] A. Mishra, M. Shin and W. Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Proces," *SIGCOMM Comp. Commun. Rev.*, vol. 33, no. 2, 2003, pp. 93–102.
[11] N. Chevrollier, N. Montavont, and N. Golmie, "Handovers and Interference Mitigation in Healthcare Environment," *Proc. IEEE MILCOM 2005*, Atlantic City, NJ, Oct. 2005.
[12] IEEE Std. 802.11I-2004, "IEEE Standard for Information Technology: Telecom. and Information Exchange between Systems, LAN/MAN-Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 6: MAC Security Enhancements," 2004.
[13] IEEE Std. 802.1X-2004, "IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control," 2004.
[14] D. Perkins and J. Arkko, "Mobility Support in IPv6, IETF RFC 3775, June 2004.
[15] C. Perkins and D. Johnson, "Mobility Support in IPv6," *ACM/IEEE Int'l. Conf. Mobile Comp. and Net.*, 1996.

BIOGRAPHIES

NICOLAS CHEVROLLIER received his engineering diploma from the Institut National des Telecommunications (INT), France in 2000 and is currently working toward a Ph.D. from the same institution. After an eight-month training period at Cisco Systems, Paris, he has been a guest researcher in the high-speed networks technologies group at the National Institute of Standards and Technology (NIST). His interests include mobility and QoS management in wireless networks.

DAVID CYPHER received his B.S. in mathematics from Clarion University of Pennsylvania in 1986 and his M.S. in computer science/telecommunications from The Johns Hopkins University in 1996. He is employed by NIST, Gaithersburg, Maryland, as a computer scientist in the Advanced Network Technologies Division. His research interests are networking protocols and validation of systems.

NADA GOLMIE received her Ph.D. in computer science from the University of Maryland at College Park. Since 1993 she has been a research engineer in the advanced networking technologies division at NIST. She is currently the manager of the high-speed network technologies group. Her research in media access control and protocols for wireless networks led to more than 100 papers presented at professional conferences, published in journals, and contributed to international standard organizations and industry-led consortia.

NICOLAS MONTAVONT (nicolas.montavont@enst-bretagne.fr) is an assistant professor at the ENST-Bretagne, Rennes, France, working in the RSM (network, security, and mobility) Department. He received his M.Sc. and Ph.D. degrees in computer science in 2001 and 2004, respectively, from Louis Pasteur University, France. In 2005 he was working at NIST in a post-doctoral position. His research interests are network/host mobility, IPv6, cross-layer architecture, and wireless technologies.