8-2010

Is Bluetooth the Right Technology for Mhealth?

Shrirang Mare
Dartmouth College

David Kotz
Dartmouth College

Is Bluetooth the right technology for mHealth?

Shrirang Mare
Computer Science
Dartmouth College
Hanover, NH, USA

David Kotz
Computer Science; ISTS
Dartmouth College
Hanover, NH, USA

Abstract

Many people believe mobile healthcare (mHealth) would help alleviate the rising cost of healthcare and improve the quality of service. Bluetooth, which is the most popular wireless technology for personal medical devices, is used for most of the mHealth sensing applications. In this paper we raise the question – Is Bluetooth the right technology for mHealth? To instigate the discussion we discuss some shortcomings of Bluetooth and also point out an alternative solution.

1 Introduction

Today there is a broad interest in electronic medical records and in the potential for mobile healthcare (mHealth) to provide more accurate, more pervasive health data. As a general model for personal medical monitoring systems, users either have on-body or in-body sensors that send the data wirelessly to an aggregator device, which usually is envisioned as a mobile phone. Users can then share that data with their doctor by sending it directly or by uploading the data to a server.

In many mHealth sensing applications Bluetooth is used for collecting data from sensors into mobile phones. One of the main reasons for using Bluetooth is because it has a large user base, as it is available in most modern cellphones. Any solution that uses Bluetooth is easily adoptable.

Bluetooth was developed to replace cables and is a commonly used wireless technology for a Personal Area Network (PAN). But is it the right technology for mHealth? In this paper we wish to stimulate a discussion by suggesting that Bluetooth might not be the best technology for a Body Area Network (BAN)[1] and encourage researchers to improve Bluetooth or look for better alternatives. We do so by pointing out some shortcomings of Bluetooth in a mobile health context. We also touch upon an alternative to Bluetooth that is in primitive stages but looks promising.

Presented at HealthSec, August 2010.

Funded in part by NSF Trustworthy Computing award 0910842.

[1] Sensors and an aggregator device used for mHealth sensing together form a BAN.

2 Problems with Bluetooth

Bluetooth transmits data in the 2.4GHz frequency band – a communication band also used by other wireless technologies and which can be monitored by an attacker. This makes it hard to provide security, privacy, and resistance to interference. We have several concerns about Bluetooth.

Secure pairing is important, as during pairing two devices share a key that is used to secure communication between them for a session. Bluetooth supports four pairing models – Numeric Comparison, Just Works, Out of Band and Passkey Entry. The 'Just Works' (JW) model is designed to support devices that do not have any input-output capabilities. Unless medical sensors can be equipped with a display or an input capability or some other out-of-band channel, which Bluetooth can use for pairing, the sensors will have to use the JW model for pairing. Unfortunately, with JW model an attacker can falsify the input-output capabilities of his device and use this association model to launch man-in-the-middle attacks [6]. Furthermore, Bluetooth uses a stream cipher called E_0 for encrypting the payload; NIST considers the stream cipher E_0 to be a weak encryption algorithm and recommends use of a more robust algorithm [8]. Some other security weaknesses include negotiable key length, allowed repeated authentication attempts, and battery depletion attacks [3, 8].

Medical data is highly sensitive. Even the disclosure of the type of sensor a person is using, let alone the sensor data, can have privacy implications. So ***privacy*** is an important aspect of mHealth sensing. Bluetooth devices, when in discoverable mode, respond to queries by disclosing information such as their name, address, local clock and other characteristics needed to connect to it. Bluetooth devices have a 48-bit unique Bluetooth Device Address (BD_ADDR) that can be used to identify the manufacturer and hence may be used to identify the type of sensor. These unique addresses can be used to link all sensor data back to one device and maybe to one user. It can also be used for tracking location of the device, if the device's BD_ADDR is observed by several Bluetooth base stations in different locations. For these reasons it is recommended that Bluetooth devices be operated in non-discoverable mode, however, even in non-discoverable mode it is possible to identify the de-

vice address using software defined radio or commercial scanning tools [7].

Most Bluetooth devices operate in Class 2 mode, which has a range of 10 meters. Although a shorter-range Class 3 (1 meter) is possible, its lower transmission power can make communication lossy due to the attenuation caused by human body.[2]. In either case, an attacker can use range extension techniques to eavesdrop on Bluetooth communication even kilometers away [4].

As a wireless technology, Bluetooth has to deal with ***interference***. It uses Adaptive Frequency Hopping (AFH) to detect channels with interference and removes them from its hopping sequence. This works well against interference from sources such as Wi-Fi and Zigbee, but it does not make Bluetooth resistant to interference from other Bluetooth piconets that cause interference on different channels. Thus, interference can be a problem in crowded places, such as hospitals and subways, affecting the quality of service of a BAN.

Scalability is also a concern for Bluetooth. A Bluetooth device can talk to only seven other devices at a time and so this limits the number of sensors a person's BAN can use concurrently. This number seems adequate for now, but it may be a constraint in the future. ***Power*** consumption is another concern for existing Bluetooth devices. Bluetooth v3.0 or earlier versions are inefficient in terms of their power utilization. Bluetooth v4.0, also called 'Bluetooth Low Energy', was released recently. How quickly it will be adopted remains to be seen.

A majority of cell phones in use today have older versions of Bluetooth (v2.0 or earlier). In addition to the security concerns mentioned above, these older versions have many security flaws that can be exploited by an attacker to gain access to the data in the device or even gain control of the device [4, 8]. Bluetooth v2.1, released in 2007, provides an improvement in terms of security by introducing the Secure Simple Pairing models and Security Mode 4 (service level enforced security) [1], but it is still not secure enough. In addition to the vulnerabilities listed by NIST [8], the JW model is the weak link in the security design of Bluetooth (including v4.0).

Later versions of Bluetooth focus on higher data rate and data reliability (v3.0), and power (v4.0). For Bluetooth v4.0 the overall Bluetooth stack is optimized for power efficiency: the PHY design is changed so that radios will consume less power. As a result, v4.0 divides the 2.4GHz band in 40 channels instead of 79 channels [9], which might be more prone to interference.

3 Proposed solution

With some changes to the Bluetooth specifications, Bluetooth could be more secure and privacy preserving. Adopting protocols such as Sly-Fi [5], which are designed for preserving privacy, and using standard encryption algorithms such as AES for encrypting payload, can help make Bluetooth a better wireless technology for mHeath sensing.

As an alternative technology for a BAN, it may be possible to establish a communication channel through the body itself. One form of Body Coupled Communication (BCC) [2], for example, uses a 23 MHz channel through the skin. Since the range of such a channel is limited to the body, it inherently provides better security and privacy, and there may be less interference compared to a wireless radio channel. It also resolves the problem of secure pairing of devices, which is one of the security weaknesses of Bluetooth, and makes it easier (compared to radio) to identify whether sensors are on the same body. There is much to study about such body-based communications, such as their effects on the human body, before they can be widely adopted. Furthermore, many such techniques require skin contact, which may be difficult or impossible for certain kinds of devices. Nonetheless this technology looks promising.

4 Conclusion

Older versions of Bluetooth, still present in a majority of deployed devices, have serious security flaws. The newer versions of Bluetooth still have some security flaws, pose privacy risks, and hence are not ideal for mHealth sensing applications. Alternative technologies such as body-coupled communication look promising but would need extensive experimentation before they are ready to use.

5 References

[1] Bluetooth specifications. Online at http://www.bluetooth.com/English/Technology/Building/Pages/Specification.aspx Last accessed April 9, 2010.

[2] A. T. Barth, M. A. Hanson, H. C. Powell, D. Unluer, S. G. Wilson, and J. Lach. Body-coupled communication for body sensor networks. In *BodyNets 2008*.

[3] T. Buennemeyer, M. Gora, R. Marchany, and J. Tront. Battery exhaustion attack detection with small handheld mobile computers. In *IEEE International Conference on Portable Information Devices*, pages 1–5, 2007.

[4] J. Dunning. Taming the Blue Beast: A Survey of Bluetooth Based Threats. *IEEE Security & Privacy*, 8(2):20 –27, March-April 2010. DOI 10.1109/MSP.2010.3.

[5] B. Greenstein, D. McCoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In *Mobisys 2008*, pages 40–53. ACM. DOI 10.1145/1378600.1378607.

[6] K. Haataja and P. Toivanen. Two practical man-in-the-middle attacks on Bluetooth secure simple pairing and countermeasures. *IEEE Transactions on Wireless Communications*, 9(1):384–392, January 2010.

[7] K. Munro. Breaking into Bluetooth. *Network Security*, pages 4 – 6, 2008. DOI 10.1016/S1353-4858(08)70074-6.

[8] K. Scarfone and J. Padgette. Guide to Bluetooth Security. *NIST Special Publication*, 800:121, 2008.

[9] K. H. Torvmark. Bluetooth low energy frequency hopping. Bluetooth Special Interest Group, 2009.

[2]The human body attenuates radio communications in 2.4Ghz band, used by Bluetooth.