WIRELESS MOBILE MEDICAL DEVICES

Abstract

Rapid developments in wireless technologies have ushered in a new era of medical devices that are improving patient quality-of-life and lowering costs for both healthcare providers and owners. Diagnostic, monitoring, and treatment systems are becoming wearable and implantable, which give them numerous advantages over bulky medical equipment. However, the wireless connectivity and programmability of these devices and applications creates an enormous vulnerability that can be exploited by malicious hackers. This paper will discuss the advantages of wireless mobile medical devices in terms of both functionality and efficiency, presenting examples to support the claim. It will then transition to assess the diversity and severity of security threats inherent to these devices. Finally, current research on potential security solutions will be presented.

Introduction

Rapid developments in electrical engineering disciplines such as flexible electronics and miniaturized, wireless technologies have ushered in a new era of medical devices that are improving the quality of life for patients suffering from a wide variety of afflictions. Diagnostic, monitoring, and treatment systems are becoming portable, wearable, and even implantable, which give them numerous advantages over bulky medical equipment, including minimized patient discomfort and lower costs for both healthcare providers and owners. However, the wireless nature of these electronic biomedical devices presents a new set of concerns from previous generations of medical equipment. The main concern regarding wireless operation of these devices is an enormous security vulnerability that can be exploited by malicious hackers. This paper will discuss the advantages of wireless mobile medical devices in terms of both functionality and efficiency, presenting examples to support the claim. It will then transition to assess the diversity and severity of security threats inherent to these devices. Finally, current research on potential security solutions will be presented.

Advantages of Wireless Mobile Medical Devices

As analog and digital electronics become increasingly fast with ultra-low power consumptions, miniaturized electronic systems are becoming viable in previously uninhabitable markets. One market that shows huge potential is the medical space. With micro-sized, ultra-thin, flexible, and biocompatible electronic systems being developed at leading research institutions and corporations, a new era of medical care is burgeoning. Biomedical devices that previously required bulky read-out equipment, large

assortments of wires, and importable displays are giving way to wearable and implantable devices that can achieve the same functionality at greatly reduced patient discomfort. In addition, wireless medical solutions are often much more affordable for patients and lower cost for healthcare providers.

Bluetooth Low Energy and other Wireless Protocols

A crucial aspect of this technological shift is the ability to achieve reliable wireless communications with biomedical devices at very low power consumptions, such that the devices can be remotely operable and data can be remotely accessed. Bluetooth technologies epitomize recent advances in wireless technologies that allow for the remote operation of mobile medical devices. In 2010, Bluetooth released its latest wireless platform: Bluetooth Low Energy (BLE), aimed at creating wireless applications in numerous fields including healthcare. The intention of BLE is to provide devices with wireless communications at aggressive power metrics and low costs without sacrificing performance relative to other wireless standards. Table 1 summarizes the relevant performance specifications of BLE chipsets that make them suitable for wireless medical devices.

Table 1

Bluetooth Low Energy Specifications. Source: Bluetooth 4.0: Low Energy (2010, p. 8).

Parameter	Value	Unit
Open Field Transmission Range	150	m
Output Power	10	dBm
Max Current Draw	15	mA
Sleep Current	1.0	µA
Carrier Frequency	2.4	GHz
Data Throughput	1.0	Mbps

The transmission range, output power, and power consumption are all outstanding, making BLE a suitable wireless protocol for use in wireless mobile medical platforms. The sacrifice for achieving transmission at such low power is the limit in data throughput – 1 Mbps (Decuir, 2010). However, the data rate is sufficient for achieving reliable discrete data transfers, such as those required for transmitting data from a sensor node in a biomedical application. BLE systems are designed to run for years on standard 3-volt coin cell batteries, eliminating the concern of constant power-supply replacement for a wearable or implantable medical device (ibid). BLE is just one of many wireless protocols that work reliably at low power consumptions. The use of ANT, ZigBee, and other wireless communications standards are also

being explored for use in the medical space. Furthermore, the “internet of things” gives the mobile medical space much more viability in a complex healthcare system: wireless devices can autonomously update electronic medical records by connecting to the internet themselves, or by transmitting data to an internet capable device such as a computer or a smart phone.

Examples of Wireless Mobile Medical Devices

To achieve patient diagnosis, monitoring, and treatment, medical devices from previous generations require probes and sensors which attach to the patient with long wires leading off the probes to a bulky, non-portable display / user interface. The wires and bulky nature of the devices tether the patient to a hospital bed, during which their hospital visits are expensive and in many cases unaffordable. The technology of these generations simply did not allow for wireless mobile medical devices to compete with the performance of cumbersome, importable medical systems. But with the aforementioned advances in electrical engineering, in particular in wireless communications, research-level prototypes for wireless mobile medical devices are emerging across all sectors of medicine. Examples of autonomous wearable or implantable medical devices that are already being employed in the field include pacemakers, defibrillators, glucose monitors, insulin pumps, and neuro-monitoring systems. But this is just the beginning; researchers are working to develop the next generation of wireless medical devices that will revolutionize healthcare on all fronts.

Current Research: Smart Wound Dressing

One example of promising research that combines the use of miniaturized sensor systems, microprocessors, and low-power wireless communications in a biomedical application is an intelligent wound dressing platform. Researchers at Tufts University, Purdue University, and Harvard University are developing a wearable bandaging with integrated sensors, read-out electronics, and wireless communications that can autonomously monitor the process of a healing wound. An early stage prototype was created over the summer of 2014: a wireless flexible smart bandage for continuous monitoring of wound oxygenation (Mostafalu, 2014). Embedded in the bandage is an oxygen sensor as well as an electronic readout system with wireless data transmission for autonomous, real-time, remote monitoring of oxygen concentration at the wound site. Figure 1 shows a 3D rendering of the smart wound dressing,

which serves as an exemplary template for wearable medical technologies.

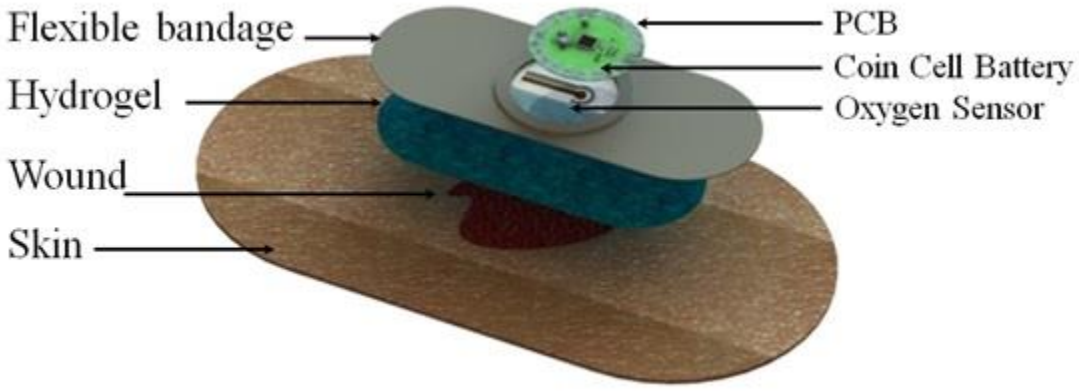

Figure 1

3D Rendering of Wearable Smart Wound Dressing. Source: Wireless Flexible Smart Bandage for Continuous Monitoring of Wound Oxygenation (2014).

A flexible, galvanic oxygen sensor on the order of 100 μm in diameter with a highly linear sensitivity was fabricated and integrated into the bandage (ibid). The oxygen sensor is interfaced via a flexible conductor to an analog-front-end circuit for amplification (ibid). The front end circuit contains a fully programmable, variable-gain, trans-impedance amplifier, allowing for monitoring of a wide variety of oxygen concentrations with oxygen sensors of various sensitivities (ibid). The output of the analog-front-end is read into a microcontroller through an analog-to-digital converter, where the data is converted back to a voltage value and wirelessly transmitted to a nearby computer or smartphone via a Bluetooth Low Energy radio (ibid). Once the data is captured to the smart phone or computer, it can, of course, be uploaded to a server for remote access by a caregiver or physician. The sensors and readout electronics are assembled in a conformal packaging that is sufficiently compact to be embedded in a wearable bandage without causing discomfort to the user. Furthermore, the entire configuration is powered by a single 3-volt coin cell battery (ibid). The smart bandage demonstrates the imminent arrival of wireless medical diagnostic and therapeutic tools that are wearable or implantable across a multitude of healthcare domains.

Security Risks of Wireless Mobile Medical Devices

Mobile medical devices are advantageous for both healthcare providers and recipients. Patients can reduce the burden of frequent hospital visits and bulky medical equipment tethering them to hospital beds, while the cost of care is dramatically reduced for both hospitals and patients. But for all these advantages, the security risks presented by wireless mobile medical devices are significant. A typical mobile medical

device will have a low-power wireless communications system, such as a BLE or ZigBee radio. The use of low power radios requires an intermediate base station in close proximity to the user (e.g. 150 meters maximum for BLE) where data can be dumped and subsequently uploaded to a "secure" server through a wireless network such as Wi-Fi. The transmission of data across a wireless network presents a glaring security vulnerability if malicious hackers can penetrate the network security and gain access to confidential patient information. Furthermore, if the medical device itself can directly be accessed or programmed from a remote location, such as the previously discussed smart wound dressing, malicious hackers could actually hijack operation of the device to steal private information or cause device malfunction.

Flavors of Security Breaches

Rushanan et al. break the variety of security threats for implantable medical devices (IMD's) into three general categories: telemetry interface breaches, software threats, and hardware / sensor threats (Rushanan, 2014). The most commonly considered and most feasible security vulnerability is the telemetry interface. Usually, a wireless network requires knowledge of a network identifier to access the information communicated through the network, much the way many Wi-Fi networks require a password for admittance. If a remote adversary could somehow infiltrate the wireless network by obtaining the network identifier or through other network vulnerabilities, the adversary can pose threats in one of two forms: passive and active (ibid). A passive adversary will eavesdrop on information from the medical device, which compromises patient confidentiality and privacy (ibid). An active adversary can jam, modify, or forge the information exchange, corrupting the data readout from the medical device, or even terminate wireless access to the device altogether (ibid). Active adversaries compromise confidentiality and privacy like a passive attacker, but also threaten the integrity and safety of the medical device. Malicious hackers can also pose more immediate threats to the medical device if they are within range of its remote operation. Familiarity of the embedded software of an IMD would allow the adversary to alter the logic and functionality of the device without having to establish physical contact (ibid). Furthermore, knowledge of the hardware and sensor structure of an IMD would enable an attacker to potentially introduce remote interference that directly compromises sensor operation, sensor read-out, and actuation of treatment (ibid).

How to Breach a Wireless Insulin Pump, For Dummies

Jerome Radcliffe outlines a shockingly feasible scenario in which a wirelessly operable insulin pump using supervisory control and data acquisition (SCADA) could be breached and in turn used for malicious purposes (Radcliffe, 2011). SCADA refers to any system sending coded signals over a wireless

communications channel for sensing and actuation, such as those utilized in wireless mobile medical devices. The frequency of wireless communication for the insulin pump in this theoretical attack (916.5 MHz) and the modulation scheme used for wireless transmission from the device (On / Off Keying) is readily available information provided by the device manufacturer (ibid). There are myriad wireless chipsets available in commercial markets that broadcast across all frequency ranges and are programmable to allow for various modulation types, meaning they could be programmed to communicate with this insulin pump. These include wireless radios utilizing the protocols previously discussed (Bluetooth, ZigBee, etc.). In this scenario, Radcliffe used the CC1101 radio transceiver from Texas instruments (TI), which can be directly purchased from TI's website or through a third party distributor such as Digi-Key. The command codes for wireless operation of the medical device were found to be published in multiple online locations, though not released directly by the insulin pump manufacturer (ibid). The indirect availability of this information calls into question the intentions of those who made it publicly available. Additionally, a dedicated attacker could purchase the same insulin pump and likely gain the necessary knowledge to stage an effective attack through the information provided with the product. Thus the relevant information and hardware needed to hack this insulin pump would be readily accessible to an adversary. With this information, Radcliffe postulates many serious threats, including the ability of the adversary to change the amount of insulin delivered by the pump to the patient (ibid). Although this would require close proximity to the device (100 to 200 feet for the wireless transceiver used on this insulin pump), it would only take seconds to reprogram its functionality, which could potentially result in patient hospitalization or even fatality (ibid).

Security Solutions for Wireless Mobile Medical Devices

If innovation in electrical engineering has enabled the feasibility of mobile medical devices, in turn generating a new set of security risks, then advances in electrical engineering and related fields such as computer science can certainly mitigate these risks as well. Researches are investigating highly advanced data encryption methods, security protocols, and trust models to help secure wireless medical instruments.

Example: Architecture for Trustworthy Data Collection from an IMD

Hu et al. used a public-key cryptography standard—IEEE 1363—in combination with a complex, probabilistic trust model to demonstrate highly trustworthy data collection from IMD's (Hu, 2010). Public-key cryptography is a scheme in which data is scrambled, or encrypted, such that it is undecipherable in its raw form. To convert the data back to the original, discernable form, two "keys" are

required—one public key and one private key. A key can be thought of as an operation which is applied to the encrypted data which uniquely produces the original, unencrypted information. The private key is mathematically related to the public key, but the mathematical relationship will typically not have a closed-form solution, so an adversary obtaining the private key from the public key is neither trivial nor likely—in fact, it is said to be computationally infeasible. <pFurthermore, in this study, a trust model was developed to quantify the level of trust for any user trying to access information through the wireless network (ibid). Instead of using a conventional binary trust quantifier, where the number 1 represents a trusted user and 0 represents an untrustworthy user, Hu et al. used a complex probabilistic framework based on numerous variables to map the level of trust to any decimal on the continuous interval form 0 to 1 (ibid). Based on the encryption scheme and the novel trust model, a protection system was implemented in hardware and shown to be highly effective against a variety of staged attacks ranging from naïve to advanced in nature (ibid). Hu et al. thus demonstrate how encryption algorithms and probabilistic models can be mapped to functionalized electronic systems to secure medical devices. This is just one example of a multitude of research efforts within the electrical engineering discipline that are intended to mitigate the vulnerabilities of wireless medical devices.

Conclusion

In summary, developments across many electrical engineering disciplines have given rise to a new generation of medical devices, ranging from diagnostic to therapeutic, that are wirelessly operable. Wireless functionality reduces patient discomfort, reduces costs for both patients and health care providers, and in many cases improves the efficacy of treatment relative to medical instrumentation from previous generations. At the heart of wearable and implantable medical devices are advances in wireless communications, specifically the ability of wireless radios to achieve sufficient data throughput with ultra-low power consumption on highly miniaturized electronic chips. A typical mobile medical device will consist of a miniaturized system worn by or embedded inside the patient, a nearby intermediate base station in range of the device's wireless radio (which can exist in the from of a computer or smartphone), and a protected data server where information from the base station can be relayed for remote access by a caregiver or physician. The channels through which the information travels to ultimately reach the remotely located care provider open up many security vulnerabilities. Malicious hackers who can penetrate the data server could obtain and / or alter information from the device, compromising the patient's confidentiality, privacy, and the integrity of treatment. Additionally, hackers within communication range of the device can alter its operation, posing serious risks for patient safety. In some scenarios, it has been shown that the information and the equipment needed to stage a malicious attack are

readily accessible to the general public. In an effort to minimize these vulnerabilities, researchers have implemented novel protection schemes, intended specifically for wireless medical systems, and demonstrated their efficacy. Mobile medical devices are advantageous for numerous reasons, and even though they pose a set of risks that were not present with previous generations of medical equipment, the ongoing effort of researchers to secure these devices will not allow their vulnerabilities to prevent them from one day saturating the medical marketplace.

Source : https://sites.tufts.edu/eeseniordesignhandbook/2015/wireless-mobile-medical-devices/