# MedMon: Securing Medical Devices Through Wireless Monitoring and Anomaly Detection

Meng Zhang, Anand Raghunathan, *Fellow, IEEE*, and Niraj K. Jha, *Fellow, IEEE*

***Abstract*—Rapid advances in personal healthcare systems based on implantable and wearable medical devices promise to greatly improve the quality of diagnosis and treatment for a range of medical conditions. However, the increasing programmability and wireless connectivity of medical devices also open up opportunities for malicious attackers. Unfortunately, implantable/wearable medical devices come with extreme size and power constraints, and unique usage models, making it infeasible to simply borrow conventional security solutions such as cryptography. We propose a general framework for securing medical devices based on wireless channel monitoring and anomaly detection. Our proposal is based on a medical security monitor (MedMon) that snoops on all the radio-frequency wireless communications to/from medical devices and uses multi-layered anomaly detection to identify potentially malicious transactions. Upon detection of a malicious transaction, MedMon takes appropriate response actions, which could range from passive (notifying the user) to active (jamming the packets so that they do not reach the medical device). A key benefit of MedMon is that it is applicable to existing medical devices that are in use by patients, with no hardware or software modifications to them. Consequently, it also leads to zero power overheads on these devices. We demonstrate the feasibility of our proposal by developing a prototype implementation for an insulin delivery system using off-the-shelf components (USRP software-defined radio). We evaluate its effectiveness under several attack scenarios. Our results show that MedMon can detect virtually all naive attacks and a large fraction of more sophisticated attacks, suggesting that it is an effective approach to enhancing the security of medical devices.**

***Index Terms*—Anomaly detection, medical devices, monitor, personal healthcare systems, security, wireless.**

## I. Introduction

In recent years, medical advances as well as innovations in ultra low-power computing, networking, and sensing technologies have led to an explosion in implantable and wearable medical devices (IWMDs). IWMDs are currently used to perform cardiac pacing, defibrillation, insulin delivery and glucose monitoring, deep brain stimulation, intrathecal drug infusion, and many other diagnostic, monitoring, and therapeutic functions [1]. IWMDs commonly include wireless communication interfaces through which they can be connected to external diagnostic or programming equipment, or to body area networks (BANs) to form personal healthcare systems (PHSs). Fig. 1 shows a generic architecture for how IWMDs can be connected to form a PHS. A PHS typically consists of sensors for physiological data collection, actuators for therapy delivery, remote controllers for reconfiguration, and a hub for logging, compressing, and analyzing the raw health data.

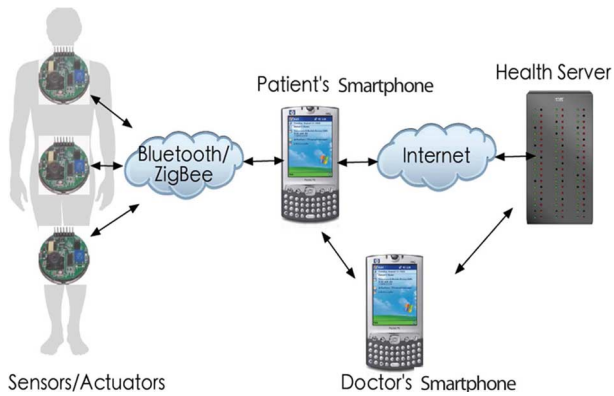


Fig. 1. Generic architecture of a personal healthcare system.

Since the functions performed by IWMDs and PHSs are frequently life-critical, any malfunction in their operation is of utmost concern. An incessant trend in IWMDs has been towards increased functional complexity, software programmability, and network connectivity. While these advances are desirable from the viewpoint of the improvements that they engender in diagnostic/therapeutic effectiveness and convenience to patients, they also collude to greatly increase the risk of security vulnerabilities and malicious attacks [2]. Ensuring the security of IWMDs and PHSs is a *sine qua non* since the functions that they perform are frequently life-critical (e.g., cardiac pacing, continuous blood glucose monitoring and insulin delivery [3] and brain-machine interfacing [4], [5]). Unfortunately, the very tight power and size budgets that are inherent to IWMDs virtually rule out the use of conventional security solutions such as cryptography. Inductive charging [6]–[8] offers the possibility of relaxing the energy constraints and avoiding the complications and costs associated with replacing batteries for medical implants. However, wireless charging for IWMDs is still in the research phase and must go through rigorous testing to ensure safety before commercial use. In addition to resource constraints, the need for emergency responders to communicate with medical devices (in the absence of any mechanism, such as

Manuscript received February 25, 2012; revised June 27, 2012 and October 22, 2012; accepted January 06, 2013. Date of publication April 24, 2013; date of current version January 28, 2014. This work was supported by NSF under Grant CNS-0914787. This paper was recommended by Associate Editor E. Jovanov.

M. Zhang and N. K. Jha are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: mengz@princeton.edu; jha@princeton.edu).

A. Raghunathan is with the School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907 USA (e-mail: raghunathan@purdue.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TBCAS.2013.2245664

public key infrastructure, for shared key establishment) is also cited as a factor preventing the use of encryption. In summary, the current generation of IWMDs typically does not employ cryptographic protection for their radio-frequency (RF) wireless communications.

Due to the absence of cryptographic protection, the wireless channel has been identified as the Achilles' heel of medical devices. Recent demonstrations of successful RF wireless attacks on cardiac pacemakers [9] and insulin pumps [10], [11] have placed medical device security under great scrutiny. To better understand how wireless channels can be used to compromise medical devices, we provide a brief overview of the attack described in [10] on a glucose monitoring and insulin delivery system. This attack exploits the wireless channels between the device and controller, and between medical devices. The attacker first eavesdrops on the wireless packets sent from a remote control to an insulin pump. From the captured packets, the attacker reverse-engineers the device PINs associated with the remote control and glucose meter. By mimicking the remote control, the attacker can configure the insulin pump to disable or change the intended therapy, stop the insulin injection, or inject a much higher dose than allowed. By mimicking the glucose meter, the attacker can send bogus data to the insulin pump, causing the pump to adjust insulin delivery based on the false data. In addition, the attacker can snoop on the packets to infer sensitive patient data.

The above attack is hard to defend against, especially because it is hard to differentiate the attacker's forged wireless transmissions from legitimate ones. In this paper, we propose a medical security monitor (called MedMon) that detects such wireless attacks and protects PHS integrity and patient safety. MedMon's is based on the observation that although the attacker's transmissions may conform to the communication protocol, they are likely to deviate from legitimate transmissions either in the physical signal characteristics or in the behavior or underlying content. MedMon is an external monitor that tracks all wireless communications to/from medical devices and identifies potentially malicious transactions using multi-layered anomaly detection. When anomalies are captured, the monitor can warn the patient and jam the suspicious transmission before it changes the state of the target device. MedMon can be implemented as a dedicated device or built into an existing personal device such as a smartphone.

The summary of our contributions is as follows:

- We propose a new defense method based on wireless monitoring and anomaly detection to defend against wireless attacks on IWMDs.
- The proposed approach is truly non-invasive in that it does not require any hardware or software modifications and can hence be applied to existing medical devices that are on the market or in use by patients.
- We demonstrate the feasibility and effectiveness of the proposed approach by developing a prototype implementation for a glucose monitoring and insulin delivery system, and using it to prevent a wide range of wireless attacks.

We note that, while MedMon addresses what we believe to be the most pressing issue in medical device security, namely the loss of integrity that may result in endangerment of a patient's health or life, it does not address the loss of privacy since the attacker may passively listen to transmissions to/from the medical device. MedMon also does not address the attacks on availability, since attackers may simply jam the wireless channel, rendering any communication impossible, or intentionally send invalid packets to drain the device's battery life.

The rest of the paper is organized as follows. Section II discusses related defense solutions that can enhance IWMD and PHS safety. Section III provides an overview of the proposed defense framework, describes the metrics used for anomaly detection, and discusses the design of security policies. Section IV evaluates our prototype implementation of MedMon for a glucose monitoring and insulin delivery system. Finally, Section V concludes the paper.

## II. Related Work

This section introduces several existing solutions against RF wireless attacks and discusses their merits and drawbacks.

Cryptography is the best approach for securing the wireless communication channel and preventing unauthorized access. It can protect device integrity as well as data confidentiality. However, conventional cryptographic methods, such as symmetric- and asymmetric-key cryptography, are not directly applicable as the problem of distributing keys to legitimate parties remains a hindrance. For example, encryption prevents medical professionals from accessing the patient's health data in emergency situations. As a possible solution, a universal key may be preloaded in devices of the same model that the ambulance staff can request from the manufacturer or patient's doctor in emergencies. However, this scheme is inherently unsafe as attackers can discover the secret key of a particular model through side-channel attacks or by hacking into the doctor's computer. Another straightforward key-distribution solution is to ask patients to carry cards or bracelets imprinted with the secret keys of their devices. To prevent the imprints from being lost or damaged, the keys could be printed into the patient's skin using ultraviolet-ink micropigmentation [12]. These "tattoos" only become visible under ultraviolet light, which is how the ambulance staff can find the keys and access the devices. To some extent, this approach protects the patient from close-range attacks as well, since although the attacker may be in close proximity, it is unlikely that the attacker can lift up the patient's sleeves while shining ultraviolet light without raising suspicion.

IMDGuardian [13] is a cryptographic scheme for implantable cardiac devices. It utilizes the patient's electrocardiography signals for key extraction so that no pre-distributed secrets are required and rekeying is easy. However, attackers may be able to extract the key through physical contact with the patient. Cryptographic methods cannot defend IWMDs against denial-of-service attacks that repeatedly request communication with the IWMD. To preserve battery power, the verification of incoming requests can be offloaded to a trusted external device. One such device, called Communication Cloaker, is described in [14]. The Cloaker mediates communications between the IWMD and pre-authorized parties, causing the IWMD to ignore incoming communications from all unauthorized programmers. Cloakers are wearable. If the Cloaker is missing or broken,

the IWMD accepts and responds to all incoming communications. Therefore, in emergency situations, the medical staff can remove the Cloaker in order to access the IWMD. Since the burden of computation is offloaded to the external device, this approach can protect the IWMD against battery-draining attacks. Unlike IWMDs, the external device can be easily recharged.

Another external device, a personal base station called the "Shield," is described in [15]. The shield works as a relay between the IWMD and external programmer. It is designed to receive and jam the IWMD messages at the same time, so that others cannot decode them. It then encrypts the IWMD message and sends it to the legitimate programmer. The shield also protects the IWMD from unauthorized incoming commands by jamming all the messages sent directly to the IWMD. All commands must be encrypted and sent to the shield first. The shield then sends legitimate commands to the IWMD. Therefore, the shield does not require any change in commercial IWMDs, but requires changes in all programmers. Since the messages from the IWMD are jammed and the communication between the programmer and the shield is encrypted, the confidentiality of IWMD messages is protected. However, when the shield sends programmer's commands to the IWMD, the commands are not encrypted and the confidentiality of the commands is not protected. The shield can defend against both close-range and long-range wireless attacks. In our defense framework, the active response of jamming and use of an external device are similar to the design of the shield. However, unlike the shield, MedMon passively monitors the communication and only interferes when an anomaly is detected. Although the shield may work well for PHSs consisting of an implantable medical device (IMD) and an external programmer, it does not suit PHSs in which IWMDs communicate with each other, because changes must be made to any device that needs to communicate with the IWMD under protection. On the contrary, MedMon does not require any change in existing communication protocols, and therefore requires no change in other devices in the PHS.

Alternatively, limiting the communication range is a simple and intuitive way of limiting wireless attacks. A radio frequency identification (RFID)-based channel between medical devices and external controllers is often proposed in this context [16]. However, an attacker with a strong enough transmitter and a high-gain antenna can attack the wireless channel even if the channel is only for RFID-based communication. For an RFID channel, the attacker can access the IWMD from up to ten meters away [17], [18]. A better alternative, perhaps, is near-field communication (NFC), an extension to RFID, which is gaining increasing attention, especially due to its integration on mobile phones [19]. The typical working distance for NFC is up to twenty centimeters. However, there is no guarantee that an attacker with a high-gain antenna cannot read the signal from outside the intended range, e.g., one meter away [20]. Another technology that can help limit the communication range is body-coupled communication (BCC). In contrast to conventional wireless communication, BCC uses the human body as the transmission medium. The communication range is limited to the proximity of the human body [21]. Experimental results in [10] show a promising attenuation in signal strength measured from some distance when comparing the BCC channel signal to the air channel signal.

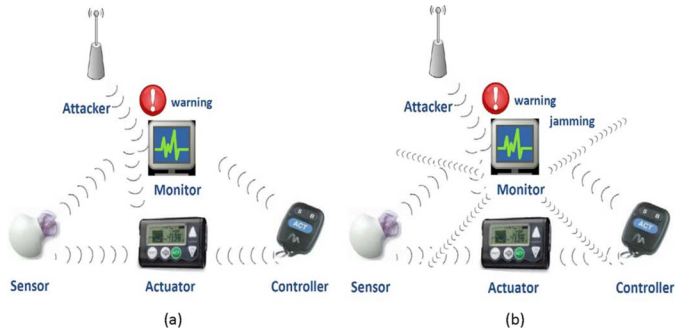


Fig. 2. Upon identifying an attack, MedMon (a) just provides a warning in the passive mode. (b) Provides a warning and jams the communication in the active mode.

In addition to communications that are designed to be inherently short-range, measures can be taken to enforce close-range communication. An access control scheme based on ultrasonic distance-bounding is introduced in [22]. In this scheme, an IWMD grants access to its resources to only those devices that are close enough. However, limiting the communication range is only effective against attacks launched beyond a certain distance. It is quite possible that an attacker can approach within a small distance of the patient and even make physical contact without raising suspicion (e.g., in a crowded subway station).

## III. Our Defense Framework

In this section, we first discuss the generic scheme employed in our defense framework against RF wireless attacks. We then describe various anomalies and discuss the design of security policies. We also discuss the limitations of the proposed framework.

### A. Overview

In our defense framework, security is delivered by MedMon, a wearable external device added to the BAN of a PHS. To accommodate different devices and patient needs, the monitor needs to be trained and configured first in order to learn the characteristics of normal behavior. For both training and actual use, it must be placed at a fixed position relative to the IWMD. When in use, the monitor quietly monitors communications among the different components of a PHS. It searches for anomalies in transmitted signals to determine whether a wireless attack is being launched against the PHS.

The operation of MedMon is illustrated in Fig. 2. When anomalies are identified, indicating a possible attack, the monitor can respond passively or actively, depending on its configuration for this type of anomaly or attack. The monitor is set to the passive (active) mode for a particular anomaly if the potential damage is low (high). In the passive mode, it provides a warning to the patient through an alarm or vibration, without interfering with ongoing communication. In the active mode, in addition to alerting the patient, it interferes with the transmission by sending jamming signals, so that the suspicious

transmission is blocked before it can complete and succeed in altering the state of the devices.

The active response of jamming and use of an external device are similar to the design of the shield [15]. However, unlike the shield, MedMon passively monitors the communication and only interferes when an anomaly is detected. Although the shield may work well for PHSs consisting of an IWMD and an external programmer, it is not suitable for PHSs in which IWMDs communicate with each other, because changes must be made to any device that needs to communicate with the IWMD under protection. On the contrary, MedMon does not require any change in existing communication protocols and therefore requires no change in other devices in the PHS.

### B. Anomaly Detection

Anomaly detection techniques are commonly used in diverse domains [23], but have not been explored in the context of medical devices. In our scenario, MedMon infers the legitimacy of a packet using a sequence of checks. Transmission is allowed only if it passes these checks. We classify potential anomalies into two categories: physical and behavioral, as discussed next.

*1) Physical Anomalies:* MedMon starts its examination by observing the physical characteristics of the transmitted signal. Such characteristics may include the received signal strength indicator (RSSI), time of arrival (TOA), differential time of arrival (DTOA), and angle of arrival (AOA), all of which are well-known indicators from the area of radio location [24], [25]. In radiolocation, RSSI, TOA, and DTOA are used to estimate the distance of a transmitter from the receiver, and AOA is used to determine the transmitter's direction in relation to the receiver. Knowing these characteristics of the transmitter will allow the monitor to verify its legitimacy with high confidence. However, the relative positions of the PHS components and the monitor may not always stay the same. For example, the patient may hold the remote control at different angles relative to the monitor. Fortunately, the monitor does not have to precisely locate the transmitting device used in the attack. For legitimate transmitting devices in the PHS, some of the above-mentioned metrics have relatively steady values. Thus, thresholds can be used to demarcate boundaries between normal and abnormal values, as discussed next.

- **RSSI:** If the distance between the monitor and each transmitting device is known and expected to remain relatively constant, the signal strength from the device can be expected to fall within a specific range. An anomaly is detected if the signal allegedly sent by the device has unusually high or low strength.
- **TOA:** If a transmission is scheduled to occur at specific points in time, the occurrence of the transmission at a non-scheduled time reveals an anomaly.
- **DTOA:** If a transmission is scheduled to occur periodically at certain time intervals, early arrival of the transmission signal is recognized as an anomaly.
- **AOA:** Assuming the monitor is carried at a fixed location on the patient, e.g., attached to the right side of the patient's belt, a transmitting device, e.g., a sensor on the patient's back, will have a fixed angle relative to MedMon. In such cases, AOA could be used to examine whether the signal is arriving from the correct direction. For example, the monitor will report an anomaly if it receives sensor signals from the front, when it expects them to come from the back.

*2) Behavioral Anomalies:* An examination of physical indicators cannot guarantee all attacks will be caught. For example, attack signals might have the physical characteristics that satisfy all requirements by chance or through sophisticated design. However, although an attack signal may be physically indistinguishable from a normal signal, the underlying information (commands or data) can typically be distinguished due to its intention to cause harm to the patient, e.g., a malicious command that orders repeated or large-dose drug injections, or forged data that feign sudden changes in vital signs to induce unnecessary drug delivery.

We define anomalies in the underlying information to be behavioral anomalies. The monitor keeps a record of the historical data and commands. When new command/data arrive, it compares them to the historical record to decide whether the new command/data constitute a behavioral anomaly.

When a command anomaly is detected, such as for repeated drug injections, the monitor prevents the new command from being executed by jamming the command signal, in order to protect patient health and safety. If the command is authorized by the patient, the patient can simply revise the command or change the anomaly definition in the monitor's configuration.

When a data anomaly is detected, such as a sudden change in the patient's vital signs, the monitor raises a warning. Abnormal data may be generated by an attacker or may actually represent a deteriorating patient condition. In either case, the monitor's warning alerts the patient to an attack or a health condition that he/she should be concerned about.

The firmware on some devices may provide functionality similar to that of behavioral checking, which verifies whether measured values are within bounds and raises an alarm if they are not. However, not all device firmware do so. For devices on which such a functionality or parameter reconfigurability is absent, firmware updates may require device recalls and may be limited by the capacity of existing hardware. MedMon provides behavioral checking without requiring any changes to the IWMDs. If the firmware already provides the same protection, behavioral checking can be turned off on MedMon.

*3) Protection Layers:* The examination process is analogous to peeling off the layers of an onion. We refer to these layers as protection layers. They are shown in Fig. 3. The outer layers, i.e., the physical indicators, are examined first. If the transmitted signal passes the examination in the outer layers, the monitor searches for data or command anomalies in the signal's underlying content. If no anomaly is found, the signal is deemed to be safe and granted access to the target device.

An implicit assumption in the above scenario is that the signal under examination is transmitted or allegedly transmitted from a registered device (the device PIN is known to other devices in the PHS and to the monitor). If the transmitted signal carries a PIN from an unregistered device, e.g., the controller of another patient nearby, the monitor does not need to perform any examination of the signal, since the signal will be ignored by IWMDs in the PHS anyway. Needless to say, it should not

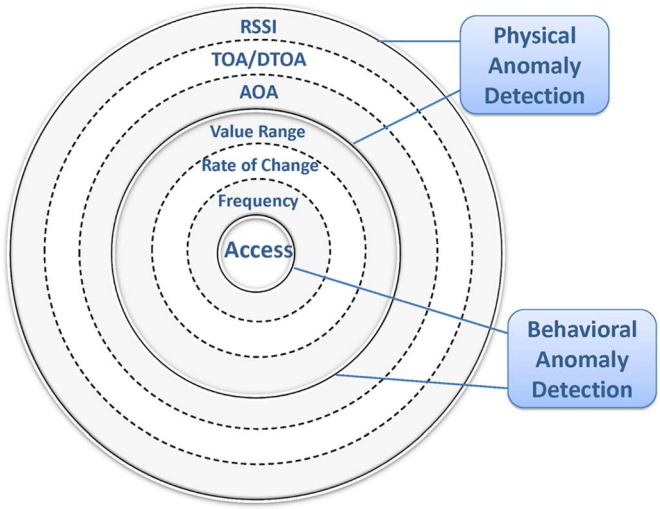


Fig. 3. Layers of protection.

TABLE I
EXAMPLES OF SECURITY POLICIES

| Type | Anomaly | Response |
|---|---|---|
| Physical | RSSI is greater than $A_h$ or smaller than $A_l$ | Raise warning, jam |
| | TOA does not fall in any of the time ranges $(t_l(m), t_h(m))$ | Raise warning, jam |
| | DTOA is greater than $\Delta t_h$ or smaller than $\Delta t_l$ | Raise warning, jam |
| | AOA is greater than $\alpha_h$ or smaller than $\alpha_l$ | Raise warning, jam |
| Behavioral | Data value is greater than $D_h$ or smaller than $D_l$ | Raise warning |
| | Rate of change of data value is greater than $r_{th}$ or smaller than $-r_{th}$ | Raise warning |
| | Injection dose is larger than $D_{th}$ | Raise warning, jam |
| | Repeated $n$ injections in the past $\Delta T$ | Raise warning, jam |
| | Total injected dose greater than $V_{th}$ in the past $\Delta T$ | Raise warning, jam |

try to jam communications in a nearby patient's BAN. Therefore, MedMon first examines the PIN carried by the transmitted signal before taking any further action.

### C. Security Policies

Anomalies can be defined within security policies. Security policies define what the monitor's response should be to each detected anomaly. Each transmitting device has its own set of security policies. The monitor is guided by the security policies of the transmitting device when snooping on its transmission.

Table I shows examples of security policies that could be used. These policies may be different for different PHSs. We will see an example of how a security policy can be designed in Section IV. The parameters mentioned in Table I can be set to predefined values or else tailored to the patient's condition and environment. Values of parameters associated with physical anomalies, e.g., $A_h$ and $\Delta t_h$, can be generated automatically at the end of a training period. Values of parameters associated with behavioral anomalies, e.g., $D_{\rm th}$ and $r_{\rm th}$, can be selected based on the advice of the doctor.

During the training period, the patient carries the monitor, with the PHS operating normally. After collecting a sufficient number of values for RSSI, TOA, DTOA, and AOA for each transmitting device, the monitor determines if each parameter has values that fall in a certain range and, if so, decides the thresholds for the parameter. If a parameter does not have a range of normal values, it is not included in the device's security policies.

Note that policies related to TOA and DTOA are only helpful if data transmissions occur periodically or at specific points in time. Fortunately, irregular transmissions are most likely initiated by the patient. We can therefore apply strict policies to jam or raise a warning by default, as discussed in Section IV.C. Sometimes, even if data transmissions are scheduled to occur periodically or at specific times, the actual occurrence may not exactly be in accordance with the schedule, because the communication protocol may require verifying the absence of other traffic before transmission, or retransmissions are performed after failed transmissions. In such cases, TOA and DTOA, with wider acceptable ranges, may still be quite useful, especially if the transmissions occur fairly infrequently (e.g., a few times a day) and the delay till successful transmission is relatively small (e.g., several minutes).

### D. Limitations

Among the three high-level goals of information security, i.e., confidentiality, integrity, and availability, MedMon only protects device integrity. It does not protect the confidentiality of the communication channel. For example, an eavesdropper who intercepts private health data, but does not interfere with the PHS otherwise, will not be caught. Availability of the communication channel is not ensured either. For example, an attacker may jam all communications, causing the PHS to stop functioning for the duration of the jamming signal.

The effectiveness of MedMon depends on the comprehensiveness and strictness of the security policies. Stringent policies can increase the detection rate and decrease the false negative rate (FNR). However, they may also result in an increased false alarm rate, i.e., false positive rate (FPR). Too many false alarms may annoy the user into giving up on the product. Thus, security policy design should seek a balance between security and user comfort.

## IV. IMPLEMENTATION AND EVALUATION

In this section, we discuss the prototype implementation of MedMon for a glucose monitoring and insulin delivery system. We first provide background on this PHS and our experimental setup for both launching an RF wireless attack and defending against it. We then describe a range of attack scenarios that were considered in our evaluation. Next, we discuss the design of the security policies that can protect the insulin pump from being maliciously reconfigured through the wireless link. Finally, we present experimental results demonstrating the effectiveness of MedMon in thwarting security attacks.

### A. Experimental Setup

Glucose monitoring and insulin delivery systems are used for the treatment and management of diabetes. They commonly employ wireless communication among system components to

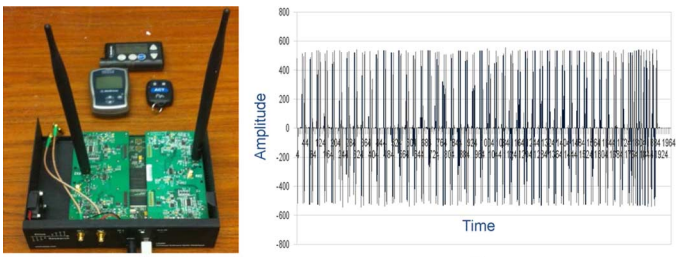


Fig. 4. (a) Experimental setup. (b) Intercepted wireless signal.

form a real-time monitoring and response loop. We analyze a popular glucose monitoring and insulin delivery system.[1] It consists of the following components:

- A glucose sensor, which samples blood glucose levels on a continuous basis, typically every few minutes.
- A manual glucose meter, which is used to manually measure blood glucose levels.
- An insulin pump, which performs autonomous administration of insulin through subcutaneous infusion.
- A remote control, which is used to program the insulin pump to reconfigure parameters or to cause the pump to inject a bolus dose (e.g., in advance of an event that will cause a surge in blood glucose levels, such as a meal).

Our experimental setup, as shown in Fig. 4(a), includes a manual glucose meter, insulin pump, remote control, and two Universal Software Radio Peripheral (USRP) [26] boards. The USRP is an off-the-shelf software radio platform. It can intercept radio communications within a frequency band and generate wireless signals with different frequency, modulation, and power configurations.

In our experiments, we use one USRP to simulate the attacker and the other one to implement MedMon. Each USRP has two transmit/receive paths that can be used independently. To perform attacks, we use one path of the attacker USRP for eavesdropping and the other path for transmitting attack signals. The passive mode of MedMon can be implemented using only one path of the USRP configured as a receiver. The active mode of MedMon requires both paths, where one acts as a receiver and the other as a transmitter to send jamming signals. On the USRP that emulates MedMon, the RF signal is down-converted to the baseband and then sampled at 64 MS/s. The samples are then decimated to 320 kS/s before being transferred to the computer via USB in the form of a stream of floats. Note that, in our prototype, the MedMon functionality is implemented in part on the USRP board, while the rest of it is implemented in the GNU Radio software framework that is run on a host PC. We observed that the data transfer over USB has a latency of around 1 ms. However, an integrated MedMon implementation will not have this latency.

Following the steps presented in [10], we were able to fully reverse-engineer the communication protocol of the remote control and use the USRP to act as an attacker and launch attacks. The intercepted and down-converted wireless signal sent by the remote control is shown in Fig. 4(b). A data packet contains a synchronizing sequence of "0"s and "1"s, device type, device PIN, command, cyclic redundancy check (CRC) bits, etc.

[1]We have withheld the identity of the product since it is currently deployed in the market.

### B. Attack Scenarios

The scope of potential attacks on the insulin delivery system can be categorized based on the wireless links being exploited and the nature of the security breach.

*1) Classification Based on Exploited Links:* In the insulin delivery system, there exist several wireless links: the link from the sensor to the pump to continuously transmit glucose data, the link from the manual meter to the pump to transmit glucose data (the messages on this link are manually triggered), and the link from the remote control to the pump to transmit control commands. All three links can be exploited by an attacker.

*2) Classification Based on Security Breaches:* By exploiting a particular wireless link, the following attacks can be launched. If the attacker does not know the device PIN of the remote control or glucose meter/sensor, some of the possible attacks are:

- Privacy attacks: Eavesdropping on any wireless link in the insulin delivery system exposes: 1) the existence of the therapy and the glucose level, and thus the medical condition of the patient, 2) the device type, and 3) the device PIN, which gives the attacker an open door to launch all the attacks discussed in the next group.
- Integrity attacks: Even without the knowledge of the device PIN, by relaying transmission signals (intercepting and replaying later), the attacker can still control the insulin pump or report an incorrect (past) glucose reading to the insulin pump.
- Availability attacks: Attackers can simply jam the communication channel, causing incorrect operation.

If the attacker knows the device PIN of the remote control, manual glucose meter or glucose sensor, either by reading the printed device PIN from the medical device or through eavesdropping, attacks can be launched by impersonating the respective device. The consequences of such attacks could include: 1) the attacker can stop insulin injection into the human body, 2) the attacker can resume insulin injection into the human body if it is currently stopped, and 3) the attacker can inject a bolus dose into the human body, which may lead to hypoglycemia and, hence, endanger the patient's life.

### C. Design of Security Policies

We observe that the signals transmitted from the manual glucose meter and the remote control are initiated by the patient. Commands allegedly sent by the remote control or data allegedly sent by the manual glucose meter, which are not authorized by the patient, must have been sent by an attacker. Based on this observation, we adopt the strictest policy for remote control and manual glucose meter data transmissions: the monitor jams any command signal by default and raises a warning for any meter or remote control data transmission by default. This is equivalent to defining all remote control and meter data packets as behavioral anomalies. By doing so, we ensure that fake commands sent by the attacker do not go through.

TABLE II
IMPLEMENTED SECURITY POLICIES FOR THE INSULIN DELIVERY SYSTEM

| Device | Anomaly | Response |
|---|---|---|
| Remote control | Always | Jam |
| Glucose meter | Always | Raise warning |
| Continuous sensor | RSSI is greater than $A_h$ or smaller than $A_l$ | Raise warning |
| | DTOA is greater than $\Delta t_h$ or smaller than $\Delta t_l$ | Raise warning |
| | Glucose level is greater than $G_h$ or smaller than $G_l$ | Raise warning |
| | Rate of change of glucose level is greater than $r_{th}$ or smaller than $-r_{th}$ | Raise warning |

However, commands sent by the patient are jammed too (false positives), rendering the glucose meter and remote control unusable. Fortunately, this problem can be easily resolved at the cost of a slight increase in patient effort. The patient can simply disable jamming or turn off MedMon before initiating transmission from the manual glucose meter or remote control to allow the command to pass to the pump. The patient can enable jamming or turn on MedMon right after the transmission is completed. This slight inconvenience is in exchange for much greater confidence in preventing attack commands from harming the patient. In case the attacker continuously transmits forged messages, the patient should not turn MedMon off while "prolonged" warnings are reported. In addition, continuous malicious signals can interfere with normal signals. If the insulin pump does not respond to normal commands due to interference, the patient should immediately turn MedMon back on in case the interference is caused by an attack signal.

The monitor raises warnings when data transmissions from the manual glucose meter or remote control are detected. The patient should expect to receive warnings when sending data from these devices to the insulin pump. If a warning for meter data transmission arrives when the patient is not using the glucose meter, the patient knows that an attack is taking place. Furthermore, the warnings issued by MedMon also ensure that a patient does not inadvertently forget to turn off jamming before transmitting a legitimate command. Finally, the small window of vulnerability, when MedMon is disabled, can be eliminated by having MedMon operate in the passive mode and merely report successful data transmissions to the user. If the user sees more transmissions reported than he/she generated, evasive action may be taken, such as resetting the pump and its parameters.

We also observe that data transmission from the continuous sensor is automatic, and transmissions are expected to occur at fixed time intervals. In addition, the distance between the sensor and the monitor is expected to remain relatively constant as well as their relative position. Therefore, RSSI, DTOA, and AOA can be used to ascertain if there are physical anomalies pertaining to the data transmissions from the continuous sensor. In addition to these physical indicators, we also specify acceptable ranges for the glucose level and its rate of change in the security policies as examples of behavioral security policies.

The security policies that we used in our experiments are shown in Table II.

### D. Evaluation

We present various results that demonstrate the effectiveness of MedMon in detecting and averting security attacks on the glucose monitoring and insulin delivery system.

*1) Attack Detection and Reaction:* The effectiveness of MedMon is predicated upon its ability to detect and block anomalous transmissions before they can successfully reach the target device, which in our case is the insulin pump. To test this ability, we set MedMon to the active mode and use another USRP as an attacker to send command packets at random times, from varying locations, and at varying power levels. For this experiment, MedMon is programmed to determine the command type, verify the device PIN in the packet against the stored PIN(s) of devices to which the insulin pump will respond, and if a match is found, raise a warning and jam the signal to disrupt the packet from being successfully received by the insulin pump. For the studied system, the transmission of all information bits in a packet (excluding synchronization bits) takes about 2.5 ms. As the device PIN is embedded in the middle of each incoming packet, MedMon has enough information to decide whether to start jamming after receiving 65% of the packet. To enable quick reaction, the MedMon transmitter that transmits the jamming signal is always on, but its signal strength is kept at zero by default. This way, the transmitter does not need to be initiated when the jamming starts. Instead, only a command to set the signal strength is needed. The reaction latency of MedMon is therefore only constrained by the processing delay for matching the parsed PIN with the stored PIN. As shown below, in our experiments, MedMon was able to successfully meet the latency constraint.

As noted earlier, the latency of transferring samples to the host over USB dominates the MedMon reaction latency. However, this overhead will be eliminated in an integrated implementation of MedMon. Furthermore, performing even complex computations for anomaly detection should not be a bottleneck in a hardware implementation.

Fig. 5(a) shows the frequency spectrum and time domain waveform of a command packet before MedMon starts jamming. As can be seen from the spectrum (the upper graph) in Fig. 5(a), packet transmission is concentrated at around 916.68 MHz. Data are modulated with on-off keying, as shown in the lower graph in Fig. 5(a). Fig. 5(b) shows the spectrum and waveform after jamming starts. The upper graph in Fig. 5(b) shows the jamming signal frequency is approximately 916.87 MHz, slightly higher than that of the command packet. As shown in the lower graph in Fig. 5(b), the command packet is disrupted by the jamming signal. Note that the jamming signal frequency is adjustable.

Although not shown in the figure, we verified that warnings were also generated by MedMon (in our implementation, these messages are displayed on the screen of the host computer to which the USRP, which emulates MedMon, is connected).

In our experiments, the monitor successfully detects and jams all command packets, achieving a 100% detection rate (0% FNR). The jamming is always in time such that the insulin pump no longer responds to the remote control commands. One factor that contributes to the success of jamming in our

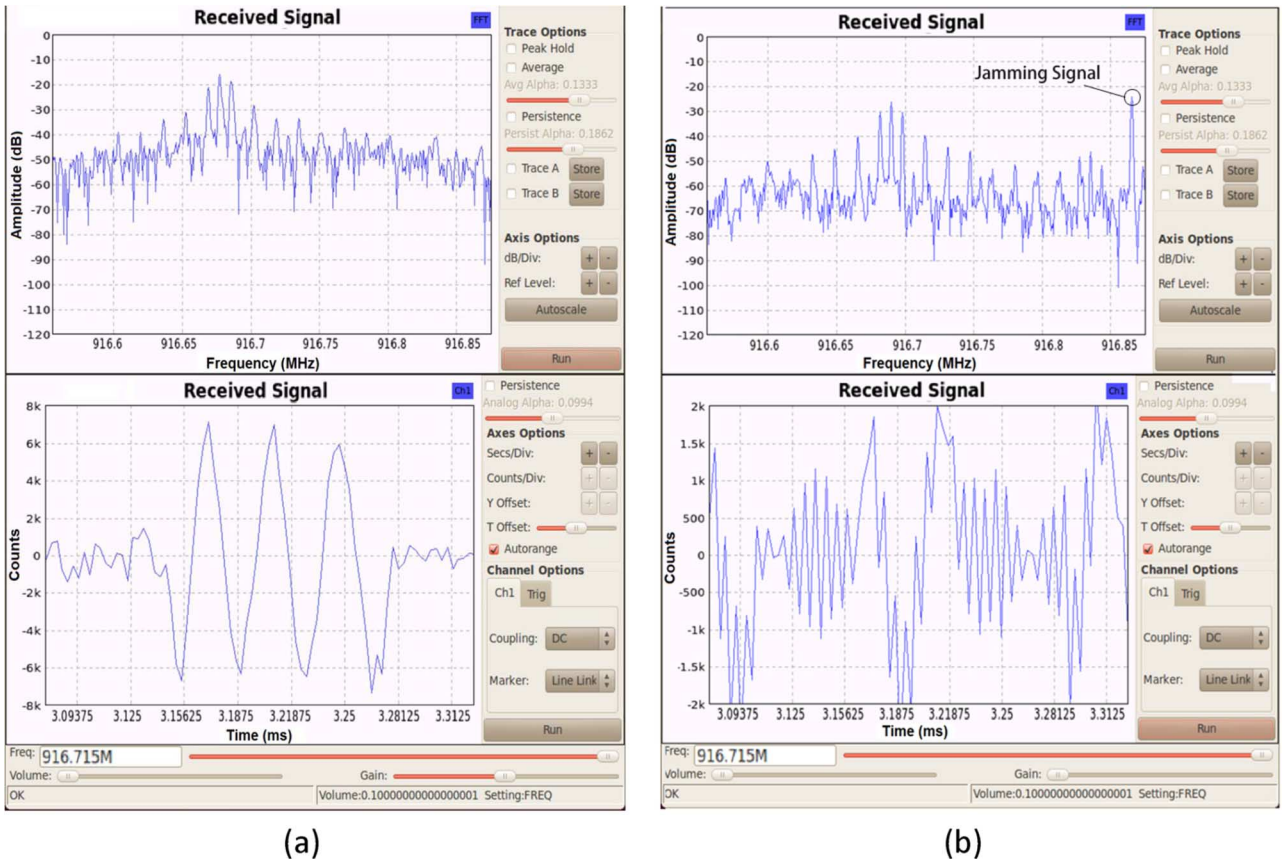


Fig. 5. Received signal in both the frequency and time domains when MedMon is in the (a) passive mode and (b) active mode. The upper graphs display the signal strengths of different frequency components. The lower graphs display how signal strength changes with time.

experiments is the slow response of the insulin pump. We suspect that the receiver on the insulin pump is turned on and off periodically in order to save power. As a result, we had to press the remote control button (resulting in repeated command packet transmissions from the remote control to the insulin pump) for more than a half second before the command can be recognized by the pump. MedMon, which snoops on the communication at all times, easily beat the insulin pump in response time. However, as described previously, MedMon can be designed to finish parsing and start jamming before receiving the entirety of a single packet.

As discussed in Section IV.C, all legitimate user commands from the remote control are jammed as well. The patient must disable jamming (or turn off MedMon) before sending legitimate commands and enable jamming (or turn on MedMon) afterwards.

*2) Parameter Determination:* Before MedMon can be put to use, it must first be trained to learn or be manually programmed with the physical characteristics of the communications between the medical devices. For example, by observing the communications between the medical devices under normal operations (in a safe physical environment), MedMon can determine the RSSI thresholds to be used in anomaly detection.

To simulate the RSSI training for the continuous sensor, we use the remote control to act as the continuous sensor and initiate transmissions at various distances up to 20 cm away from the monitor, which we consider a normal operating distance of a continuous sensor. After the training, the monitor decided the acceptable range of RSSI to be [800, 1400], i.e., $A_h = 1400$ and $A_l = 800$.

In order to demonstrate that RSSI can be used for anomaly detection, we record the measured strengths of signals sent from various distances. Fig. 6 shows that RSSI decreases as the remote control moves further away from the monitor. Each cross in Fig. 6 is an average signal strength of one received packet. Each circled dot represents the median signal strength of 168 packets collected at that distance.

Meanwhile, since every transmission from the glucose sensor is expected 60 seconds after the last one, we set the acceptable range of DTOA to be [59, 61], i.e., $\Delta t_h = 61$ and $\Delta t_l = 59$. The beginning of a transmission is recognized upon the first verification of the transmitter's device PIN. The current transmission is deemed to be complete only when consecutive zeros are received.

Our experimental setup precluded the use of AOA since it has only one receiving antenna. We conservatively assume a 60° acceptable range for incoming continuous sensor signals, since the position of the continuous glucose sensor usually remains stable with respect to the insulin pump and the monitor.

*3) Physical Anomaly Detection:* Now that we have trained and specified the physical characteristics that MedMon expects from incoming packets, we can evaluate the effectiveness of physical anomaly detection. MedMon is set to the passive mode and placed at a fixed position in an empty room. The attacker

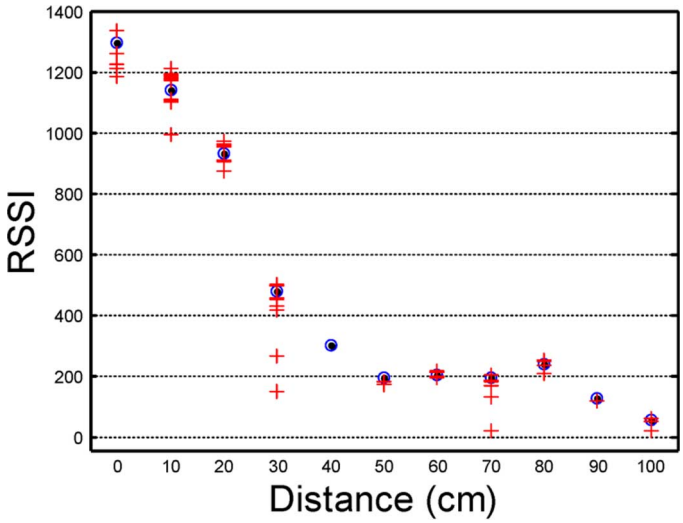


Fig. 6. Average received signal strengths as distance increases.

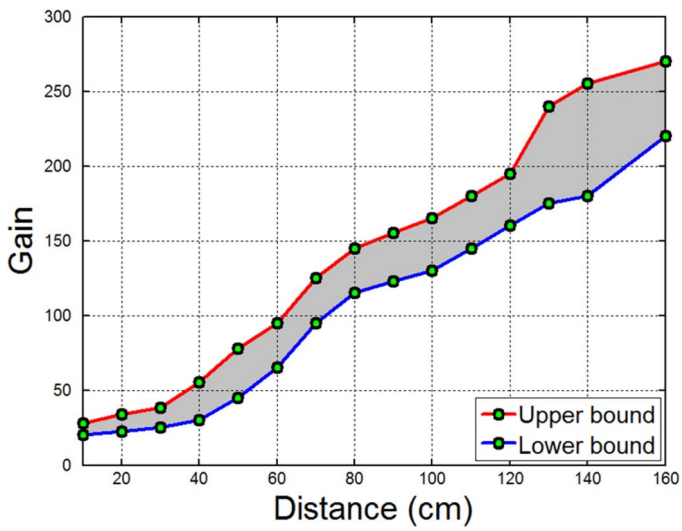


Fig. 7. Transmission power levels that result in successful attacks for different distances (MedMon uses only RSSI for detection).

USRP transmits attack signals at random times and various power levels, with changing distances and angles with respect to the monitor.

Fig. 7 shows the range of attacker transmission power that results in successful attacks at different distances from the monitor. Power levels that fall outside the boundaries lead to unacceptable RSSI as measured by the monitor. Fig. 8 further includes the AOA constraint and shows the transmission power for successful attacks at different spots on the horizontal plane when the monitor is fixed at location (0, 0).

We performed over 250 attacks with the following uniformly distributed ranges for various parameters: (i) signal amplification levels: 1–270×, (ii) distances: 10–270 cm, (iii) angles: −180–180°, and (iv) transmission intervals: 30–90 s. The monitor raised warnings for all but two attacks, yielding an FNR of less than 0.8%. It is important to note that the above measurements are performed in an empty room with no object near the transmitter/receiver or blocking the transmission paths. When a sizable object (e.g., a person) blocks the transmission path, the

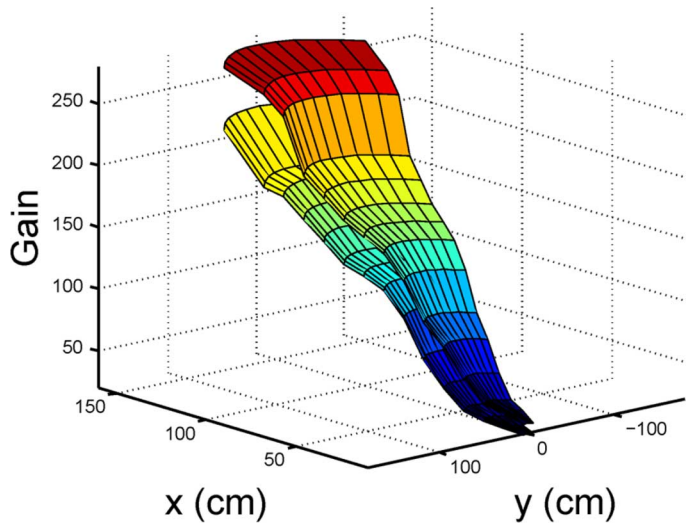


Fig. 8. Successful attack transmission power levels and locations when MedMon uses RSSI and AOA.

RSSI can drop by 10–20×. It would be quite challenging for the attacker to maintain the RSSI to within the required range in a changing channel environment with movement, obstructions, multi-path fading, etc. The RSSI of the transmissions from the glucose sensor is quite steady, since MedMon and the sensor are positioned close to each other (both are carried or worn by the patient).

We also evaluated the FPR by narrowing the distance of the continuous glucose sensor to within 10–20 cm from the monitor and initiating transmissions at 60 s intervals. In over 100 transmissions, we observed zero false alarms and thus a 0% FPR. AOA is not included in the evaluation of the FPR. We expect the false alarm induced by the 60° AOA limit to be minimal, as the relative position of the monitor and sensor vary minimally. However, FPR may increase if the relative position and distance between the monitor and sensor often change greatly, or if the transmission path is blocked. In that case, we should relax the security policies to reduce the FPR. However, that may cause the FNR to increase.

*4) Behavioral Anomaly Detection:* The evaluation of physical anomaly detection shows promising results for defending against naive attackers. However, after many trials, a sophisticated and diligent attacker may ascertain ranges of transmission parameters that lead to a high probability of success, breaking through MedMon's physical protection layers. Fortunately, the monitor can analyze the packet contents and capture "smart" attacks that are not caught by physical anomaly detection.

We implement the behavioral anomaly detection module based on the security policies listed in Table II. $G_l$ and $G_h$ are set, respectively, to 70 and 140 mg/dL, which denote the normal range of glucose levels. $r_{\text{th}}$ is set to 5 mg/dL/min, which limits the maximum rate of change in the glucose level. When an abnormal glucose level ($<G_l$ or $>G_h$) or a drastic change ($>r_{\text{th}}$) is detected, MedMon issues a warning. The behavioral anomaly may indicate an attack or a genuine sign of deteriorating glucose levels regarding which the patient should be alerted.

While the behavioral security policies described above are highly effective at detecting attacks that attempt to send grossly incorrect information to the insulin pump, it is possible that they could fail to detect attacks that are seemingly benign, e.g., attacks that slightly perturb the reported blood glucose levels. Such attacks do not immediately jeopardize the patient's health, but their accumulated effect could be harmful if the attack goes undetected for a long time. Security policies defined over long timescales can be introduced to further minimize the potential harm of such large-timescale attacks.

## V. Conclusion

Many IWMDs perform life-sustaining functions, such as cardiac pacing and defibrillation, neuromodulation, and insulin delivery and administration. They are also responsible for monitoring, recording, and storing private patient information, and making changes in response to doctors' orders. Because of the critical nature of their functionality and the fact that many implanted devices are in close contact with human organs, safety concerns must be addressed aggressively and proactively. Changes made to these devices must correspond to doctors' orders to ensure delivery of the intended therapy. Any security compromise can be life-threatening.

In this article, we introduced MedMon, a non-invasive defense framework based on anomaly detection that guards against RF wireless attacks on PHSs. This defense solution is directed at enhancing the security of existing medical devices that are already deployed or upcoming products that cannot be easily modified. MedMon snoops on all RF wireless communications to/from medical devices and uses multi-layered anomaly detection to identify potentially malicious transactions. We described two layers of anomaly detection: physical and behavioral. Physical anomaly detection targets the physical characteristics of the communications (packets) whereas behavioral anomaly detection targets the underlying information embedded in the communications.

We demonstrated the feasibility and effectiveness of MedMon through a prototype implementation for an insulin delivery system using off-the-shelf devices. Experimental results indicate that MedMon is able to thwart virtually all "naive" attacks using physical anomaly detection. Although a sophisticated attacker may evade physical anomaly detection by adapting the attacks, the most dangerous kinds of smart attacks can be captured by leveraging behavioral anomaly detection.

Besides the demonstrated insulin delivery system, MedMon can be applied to other PHSs in which the sensor, controller, and actuator are wirelessly linked, such as deep-brain stimulation or intrathecal drug delivery systems. MedMon is more suitable for communication links that are not protected by cryptographic methods. If the communication protocol includes encryption and authentication, as Bluetooth and ZigBee do, it is likely that the communication is secured against wireless attacks.

A highly desirable attribute of MedMon is that it incurs zero power overhead on the medical devices themselves, and it can be realized in a form factor that is not subject to the stringent power constraints associated with medical devices. For example, MedMon can be implemented as an add-on to a smartphone. In summary, MedMon provides an effective approach to enhancing the security of currently deployed PHSs.

## References


[1] Medtronic, 2013 [Online]. Available: http://www.medtronic.eu/our-therapies

[2] D. Arney, K. Venkatasubramanian, O. Sokolsky, and I. Lee, "Biomedical devices and systems security," in *Proc. IEEE Int. Conf. Engineering in Medicine and Biology Soc.*, Sep. 2011, pp. 2376–2379.

[3] M. Ahmadi and G. Jullien, "A wireless-implantable microsystem for continuous blood glucose monitoring," *IEEE Trans. Biomed. Circuits Syst.*, vol. 3, no. 3, pp. 169–180, Jun. 2009.

[4] A. Csavoy, G. Molnar, and T. Denison, "Creating support circuits for the nervous system: Considerations for brain-machine interfacing," in *Proc. Int. Symp. Very Large Scale Integration Circuits*, Jun. 2009, pp. 4–7.

[5] R. Sarpeshkar, W. Wattanapanitch, S. K. Arfin, B. I. Rapoport, S. Mandal, M. W. Baker, M. S. Fee, S. Musallam, and R. A. Andersen, "Low-power circuits for brain-machine interfaces," *IEEE Trans. Biomed. Circuits Syst.*, vol. 2, no. 3, pp. 173–183, Sep. 2008.

[6] P. Si, A. Hu, S. Malpas, and D. Budgett, "A frequency control method for regulating wireless power to implantable devices," *IEEE Trans. Biomed. Circuits Syst.*, vol. 2, no. 1, pp. 22–29, Mar. 2008.

[7] S.-Y. Lee, C.-J. Cheng, and M.-C. Liang, "A low-power bidirectional telemetry device with a near-field charging feature for a cardiac microstimulator," *IEEE Trans. Biomed. Circuits Syst.*, vol. 5, no. 4, pp. 357–367, Aug. 2011.

[8] A. RamRakhyani, S. Mirabbasi, and M. Chiao, "Design and optimization of resonance-based efficient wireless power delivery systems for biomedical implants," *IEEE Trans. Biomed. Circuits Syst.*, vol. 5, no. 1, pp. 48–63, Feb. 2011.

[9] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. IEEE Symp. Security and Privacy*, May 2008, pp. 129–142.

[10] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. IEEE Int. Conf. e-Health Networking, Applications and Services*, Jun. 2011.

[11] C. Purvis, Implantable Medical Devices: Hacks and Countermeasures, Aug. 2011 [Online]. Available: http://www.securitymanagement.com/news

[12] S. Schechter, Security That is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices, Microsoft Research, Tech. Rep. MSR-TR-2010-33, Apr. 2010.

[13] F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE Int. Conf. Computer Communications*, Apr. 2011, pp. 1862–1870.

[14] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder: New directions for implantable medical device security," in *Proc. Conf. Hot Topics in Security*, Jul. 2008, pp. 1–7.

[15] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *Proc. ACM Conf. Special Interest Group on Data Communication*, Aug. 2011.

[16] C. Israel and S. Barold, "Pacemaker systems as implantable cardiac rhythm monitors," *Amer. J. Cardiol.*, vol. 88, no. 4, pp. 442–445, Aug. 2001.

[17] K. Fotopoulou and B. Flynn, "Optimum antenna coil structure for inductive powering of passive RFID tags," in *Proc. IEEE Int. Conf. Radio Frequency Identification*, Mar. 2007, pp. 71–77.

[18] G. P. Hancke and S. C. Centre, "Eavesdropping attacks on high-frequency RFID tokens," in *Proc. Workshop Radio Frequency Identification Security*, Jul. 2008, pp. 100–113.

[19] What is NFC Technology [Online]. Available: http://www.rfid-nfc.eu

[20] E. Haselsteiner and K. Breitfuss, "Security in near field communication," in *Proc. Workshop Radio Frequency Identification Security*, Jul. 2006, pp. 3–13.

[21] H. Baldus, S. Corroy, A. Fazzi, K. Klabunde, and T. Schenk, "Human-centric connectivity enabled by body-coupled communications," *IEEE Commun. Mag.*, vol. 47, pp. 172–178, Jun. 2009.

[22] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proc. ACM Conf. Computer and Communications Security*, Nov. 2009, pp. 410–419.
[23] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, pp. 15:1–15:58, Jul. 2009.
[24] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero, III, R. L. Moses, and N. S. Correal, "Locating the nodes: Cooperative localization in wireless sensor networks," *IEEE Signal Process. Mag.*, vol. 22, no. 4, pp. 54–69, Jul. 2005.
[25] G. Sun, J. Chen, W. Guo, and K. Liu, "Signal processing techniques in network-aided positioning: A survey of state-of-the-art positioning designs," *IEEE Signal Process. Mag.*, vol. 22, no. 4, pp. 12–23, Jul. 2005.
[26] USRP [Online]. Available: http://www.ettus.com

**Meng Zhang** received the B.S. degree in electronics from Beijing University, Beijing, China, and the M.A. degree in electrical engineering from Princeton University, Princeton, NJ, USA, in 2008 and 2010, respectively.

Currently, he is working toward the Ph.D. degree in electrical engineering at Princeton University. His research interests include low-power system design, computer security, and body area networks.

**Anand Raghunathan** (F'12) received the B.Tech. degree in electrical and electronics engineering from the Indian Institute of Technology, Madras, India, in 1992, and the M.A. and Ph.D. degrees in electrical engineering from Princeton University, Princeton, NJ, USA, in 1994 and 1997, respectively.

Currently, he is a Professor with the School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN, USA. He was a Senior Research Staff Member with NEC Laboratories America, Princeton, where he led research projects related to system-on-chip architectures, design methodologies, and design tools. He was the coauthor of a book entitled *High-Level Power Analysis and Optimization* (A. Raghunathan, N. K. Jha, and S. Dey, Kluwer Academic, Norwell, MA, 1998) and eight book chapters. He holds 21 U.S. patents. He has presented several full-day and embedded conference tutorials.

Dr. Raghunathan was a recipient of the IEEE Meritorious Service Award in 2001 and the Outstanding Service Award in 2004. He was a recipient of eight Best Paper Awards and four Best Paper Nominations at leading conferences. He received the Patent of the Year Award (an award recognizing the invention that has achieved the highest impact) and two Technology Commercialization Awards from NEC. He was chosen by MIT's Technology Review among the TR35 (top 35 innovators under 35 years, across various disciplines of science and technology) in 2006, for his work on "making mobile secure." He has been a member of the technical program and organizing committees of several leading conferences and workshops. He was the Program and General Co-Chair of the ACM/IEEE International Symposium on Low Power Electronics and Design, the IEEE VLSI Test Symposium, and the IEEE International Conference on VLSI Design. He was an Associate Editor of the IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN, the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION SYSTEMS, the *ACM Transactions on Design Automation of Electronic Systems*, the IEEE TRANSACTIONS ON MOBILE COMPUTING, the *ACM Transactions on Embedded Computing Systems*, the *IEEE Design and Test of Computers*, and the *Journal of Low Power Electronics*. He is a Golden Core Member of the IEEE Computer Society.

**Niraj K. Jha** (S'85–M'85–SM'93–F'98) received the B.Tech. degree in electronics and electrical communication engineering from the Indian Institute of Technology, Kharagpur, India, in 1981, the M.S. degree in electrical engineering from S.U.N.Y., Stony Brook, NY, USA, in 1982, and the Ph.D. degree in electrical engineering from the University of Illinois at Urbana, Urbana, IL, USA, in 1985.

He is a Professor of electrical engineering with Princeton University, Princeton, NJ. He has coauthored or co-edited five books entitled *Testing and Reliable Design of CMOS Circuits* (Kluwer, 1990), *High-Level Power Analysis and Optimization* (Kluwer, 1998), *Testing of Digital Systems* (Cambridge University Press, 2003), *Switching and Finite Automata Theory*, 3rd edition (Cambridge University Press, 2009), and *Nanoelectronic Circuit Design* (Springer, 2010). He has authored 12 book chapters. He has authored or coauthored more than 390 technical papers. He has coauthored 14 papers that have won various awards. He holds 14 U.S. patents. He has given several keynote speeches in the area of nanoelectronic design and test. His current research interests include FinFETs, low power hardware/software design, computer-aided design of integrated circuits and systems, digital system testing, and secure computing.

Dr. Jha is a fellow of ACM. He has served as the Editor-in-Chief of the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS and an Associate Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS–I: REGULAR PAPERS, the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS–II: EXPRESS BRIEFS, the IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, and the *Journal of Electronic Testing: Theory and Applications*. He is currently serving as an Associate Editor of the IEEE TRANSACTIONS ON COMPUTERS, the *Journal of Low Power Electronics* and the *Journal of Nanotechnology*. He has served as the Program Chairman of the 1992 Workshop on Fault-Tolerant Parallel and Distributed Systems, the 2004 International Conference on Embedded and Ubiquitous Computing, and the 2010 International Conference on VLSI Design. He has served as the Director of the Center for Embedded System-on-a-Chip Design funded by New Jersey Commission on Science and Technology. He was a recipient of the AT&T Foundation Award and NEC Preceptorship Award for Research Excellence, the NCR Award for Teaching Excellence, and the Princeton University Graduate Mentoring Award. He was a recipient of the Best Paper Award at ICCD'93, FTCS'97, ICVLSID'98, DAC'99, PDCS'02, ICVLSID'03, CODES'06, ICCD'09, and CLOUD'10. His paper was selected for "The Best of ICCAD: A collection of the Best IEEE International Conference on Computer-Aided Design papers of the past 20 years," two papers by IEEE Micro Magazine as one of the top picks from the 2005 and 2007 Computer Architecture Conferences, and two others as being among the most influential papers of the last ten years at the IEEE Design Automation and Test in Europe Conference. He has coauthored six other papers that have been nominated for Best Paper Awards.