Enabling On-Body Transmissions with Commodity Devices

Mehrdad Hessar[1], **Vikram Iyer**[1], **Shyamnath Gollakota**
University of Washington
[1]Co-primary Student Authors
{mehrdadh, vsiyer, gshyam}@uw.edu

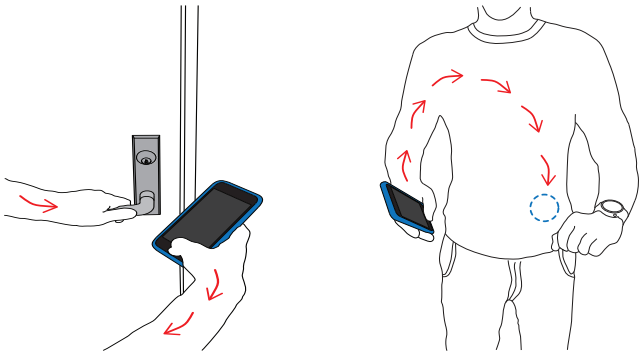
Abstract
We show for the first time that commodity devices can be used to generate wireless data transmissions that are confined to the human body. Specifically, we show that commodity input devices such as fingerprint sensors and touchpads can be used to transmit information to only wireless receivers that are in contact with the body. We characterize the propagation of the resulting transmissions across the whole body and run experiments with ten subjects to demonstrate that our approach generalizes across different body types and postures. We also evaluate our communication system in the presence of interference from other wearable devices such as smartwatches and nearby metallic surfaces. Finally, by modulating the operations of these input devices, we demonstrate bit rates of up to 50 bits per second over the human body.

ACM Classification Keywords
C.2.1. Network Architecture and Design: Wireless Communication; B.0. Hardware: General

Author Keywords
On-body communication; fingerprint sensor; touchpad; capacitive coupling; physical layer security

INTRODUCTION

In this paper, we explore the following question: can we use sensors on commodity devices such as smartphones and laptops to generate wireless data transmissions that are confined to the human body? A positive answer would enable a form of physical layer security that is currently non-existent on commodity devices. Specifically, a communication primitive that transmits information directly through the body would create links immune to eavesdropping or man in the middle attacks. For example, by simply touching a doorknob, a user could transmit secret credentials from their smartphone through their body to open the door, without leaking secret information over the air. It can also be used to create secret keys that are necessary for establishing secure wireless connections for wearable devices [37, 31]. For instance, instead of manually typing in a secret serial number or password for wirelessly pairing medical devices such as glucose or blood pressure monitors with smartphones [12, 33], a smartphone could directly transmit arbitrary secret keys through the human body.



(a) Authenticating door locks (b) Secret keys for wearables

Figure 1: Example applications for on-body communication using the fingerprint sensors on smartphones. The smartphone can securely send information to doorknobs or glucose sensors over the body.

The challenge in achieving this is that mobile devices like smartphones and laptops currently rely on radios such as Bluetooth and Wi-Fi for communication. These radios are designed to do the opposite of restricting a transmission to the body, and hence are inherently insecure. Specifically, Bluetooth and Wi-Fi chipsets are designed to transmit data as far as possible over air; an attacker familiar with the communication standard can easily intercept these wireless transmissions. In fact, researchers have raised security and privacy concerns about the vulnerability of even custom radio protocols for wearable and implantable devices [17, 21].

To achieve our goal of transmitting over the body, we look beyond traditional radios and examine other components found on mobile devices. The requirements for on-body communication are three-fold: 1) the component should be in direct contact with the body, 2) it should reliably produce electromagnetic (EM) signals required to implement the physical layer of a body-coupled communication system and, 3) since EM signals above tens of megahertz do not propagate well through the body [5], it should generate EM signals below these frequencies.

In this paper we show that fingerprint sensors and touchpads that are common on smartphones and laptops satisfy the above three constraints. Specifically, inherent to being input devices, they are in direct contact with the body. Further our analysis shows that while these devices are not designed to be active radio transmitters, during normal operation they produce characteristic EM signals, which are consistent and at frequencies

UbiComp '16, September 12-16, 2016, Heidelberg, Germany
 ISBN 978-1-4503-4461-6/16/09…$15.00
DOI: http://dx.doi.org/10.1145/2971648.2971682

below 10 MHz. Finally, we show experimentally that these low frequency signals propagate well on the human body but degrade significantly over air, enabling our goal of secure on-body data transmissions.

Building on our observations, we design an on-body communication system that modulates the EM signals produced by fingerprint sensors and touchpads. We design receiver algorithms to filter the EM signals and decode the data transmitted by these input devices. To evaluate our design, we first characterize the signal propagation on the human body using fingerprint sensors on the iPhone 5s, the iPhone 6s and the Verifi P5100 USB fingerprint scanner as well as a Lenovo T440s touchpad and the Adafruit touchpad. We provide an extensive empirical analysis of how the signals generated by these devices are affected by a user's posture and motion, as well as the user's height and weight.

Finally, by modulating the scanning operation on a Verifi fingerprint scanner in software, we demonstrate bit rates up to 25 bps over the body. We also show that by power cycling an Adafruit touchpad we can achieve on-body communication at bit rates of up to 50 bps. We believe that these rates can enable our target applications of transmitting secret keys and establishing secure connections.

While capacitive and galvanic coupling mechanisms have been demonstrated for on-body communication [48, 35], to the best of our knowledge, existing solutions require custom transmitter hardware to send data over the body. This significantly raises the bar for adoption since it requires integrating yet another custom radio into smartphones just for the purpose of on-body communication. Further, such a transmitter has to be located on the phone such that it is in contact with the user and couples well with the body. In contrast, our contributions are:

1. We show for the first time that commodity devices can be used to generate wireless data transmissions that are confined to the human body. To achieve this, we reuse fingerprint sensors and touchpads that are increasingly common on mobile devices, and thus, lower the bar for enabling on-body communication applications.
2. We demonstrate that by reusing devices designed for human touch, we achieve good coupling to the body. We analyze the channel properties of the resulting transmissions across the whole human body and empirically analyze the effect of different body postures as well as the effect of interference from other wearable devices.
3. Finally, we present a receiver design that can reliability decode our data transmissions and demonstrate bit rates of 50 bps by modulating the operations of these input devices.

APPLICATION SCENARIOS

We outline three key application scenarios that motivate the system described in this paper.

Authenticating electronic locks using touch. A compelling application is to use the transmissions created by a fingerprint sensor to send authentication codes through the body to a doorknob. In this way, a system capable of securely transmitting digital keys through the body could also be used to open physical doors. Specifically, rather than relying on keypads or cards that could be easily lost or stolen, such a system could add biometric security to a door using fingerprint sensors on phones. For instance, sending a numerical code with four numbers over the body requires less than 16 bits which can be sent in less than a second using the techniques described in this paper. The feedback for such a system is implicit, as the door will unlock if the code is successfully accepted at the receiver. We note that our approach would not require storing sensitive fingerprint information at the doorknob, which is necessary for conventional biometric based electronic lock systems.

Secure pairing for wearables. Security is of particular concern in the field of wearable medical devices used for patient monitoring or chronic disease treatment. In order to securely communicate over wireless links, these devices encrypt data based on a secret key or password. For example, continuous glucose monitors [12] require patients to enter the sensor's serial number for pairing. We can envision that a user would touch their fingerprint sensor, which would in turn transmit a secret key to medical devices on the body. Once the secret key is transmitted, an encrypted pairing process can be used to establish a traditional wireless communication link, allowing the wearable device to communicate with smartphones or other devices. For instance, a 256-bit key can be sent on the body to a wearable medical device from the fingerprint sensor in less than 15 seconds using the system in this paper. If the key is accepted by the receiver, the medical device can send an acknowledgment using either Wi-Fi or Bluetooth back to the phone and thereby establish a secure wireless connection without the need for manually entered passwords.

Synchronization applications. Additionally, networks of sensors on the body often require time synchronization to implement efficient MAC protocols [47, 44, 29]. Current solutions require transmitting periodic beacon signals from wireless devices or using measurements of physiological parameters such as heart rate for synchronization [28]. Considering an eavesdropper can intercept or interfere with wireless beacons and that signals like heart rate are highly variable, there exists a need for novel synchronization solutions that address these issues. Our system is capable of securely transmitting information through the body with precise timing control.

COMMUNICATION SYSTEM DESIGN

Our goal is to create a communication system that enables wireless transmissions on the body using commodity sensors. These transmissions are then decoded on a wireless receiver that is also in contact with the body. To do this, we first analyze the physical characteristics of the human body itself and its behavior as a communication channel. Next, we explain in detail how touchpads and fingerprint sensors operate, and design a transmission mechanism to send data through the body. Finally, we explain how to design a receiver to decode these data transmissions.

Human body as a wireless channel

We begin by explaining the electrical properties of human tissue. The epidermis, which is the outermost layer of the skin, has a high impedance as it is composed of dead cells and

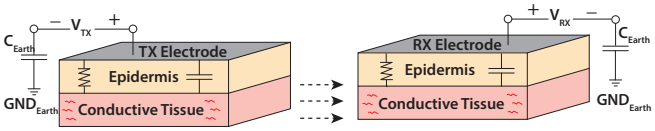


Figure 2: **Capacitively coupled body communication.** Circuit diagram illustrating the signal path through the body and capacitive coupling to earth ground. The outermost layer of the skin has high impedance below which is conductive tissue. The transmitter and receiver do not have an explicit ground connection they are capacitively coupled to earth ground.

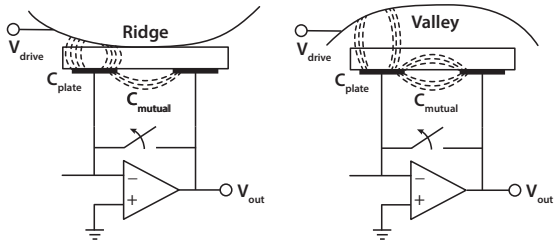
cells with non-conductive fatty membranes [50, 46]. On the other hand, the extracellular fluid in tissue beneath the skin found in muscles and blood vessels is highly conductive. For frequencies in the range of 100 kHz to 10 MHz, the complex combinations of tissue and fluids within the body can be approximated as a lattice of lumped elements such as resistors and capacitors [3].

Our design leverages capacitive coupling [50] to enable transmissions on the body. Specifically, the single metal contact of fingerprint sensors can be thought of as one plate of a capacitor, while the conductive body tissue beneath the skin is another, as shown in Fig. 2. These two conductors are separated by the epidermis, which acts as a dielectric. The receiver electrode also makes a similar connection to the body. In the case of the touchpads that do not have a metal contact touching the skin, the non-conductive material of the touchpad can be thought of as an additional dielectric layer.

Using this model of the body as a large capacitor separating the transmitter and receiver, signals produced by the transmitting devices effectively charge this capacitor and place the body at a higher potential. Typically this potential would be measured at the receiver as a voltage with respect to a common ground reference explicitly connected to the transmitter to complete the circuit. We note that in our target application scenarios the fingerprint sensor and the wireless receiver are battery-powered and worn on separate hands, and therefore do not share an explicit common ground. The lack of a shared reference with the transmitter affects the voltage recorded at the receiver. Although the transmitter and receiver grounds each have a different potential, there still exists a weak electric field between these terminals and the "earth ground", which may be modeled with a small capacitor C_{earth} that provides a return path [50]. This capacitance affects the voltage seen by the wireless receiver. One of the contributions of this paper is to observe that commodity fingerprint sensors and touchpads emit high voltage signals that can propagate over the whole body despite the losses due to the lack of a common ground.

Transmitter design

Our design uses fingerprint sensors and touchpads to transmit signals through the body. Specifically, we show that these input devices generate signals below 10 MHz and hence are ideal for transmitting data over the body. In the remainder of this section, we first understand the source of the EM signals on these input devices. We then analyze the properties of these signals and finally describe how we can transmit data using these input devices.



(a) Finger Ridge (b) Finger Valley

Figure 3: **Circuit diagram of a fingerprint sensor in which a drive signal is applied directly to the finger.** The effect on the capacitance values for a ridge and valley are shown in a) and b). A drive signal V_{drive} is applied to the finger, which results in an output V_{out} that changes between ridges and valleys.

Understanding the source of EM signals

Both fingerprint sensors and touchpads are sensing devices which operate by applying an excitation signal to the finger and measuring voltage differences caused by changes in the electric field due to touch. In the rest of this section, we first outline the operations of a touchpad and then describe in detail how commodity fingerprint sensors operate.

Touchpads. At a high level, capacitive touchpads typically consist of a 2-D array of electrodes capable of measuring capacitance at each intersection point. The presence of a finger affects the electric field at the point of touch and therefore changes the capacitance. The capacitive sensing technique used in touchpads can be classified as either being self capacitance or mutual capacitance based sensors [10, 6]. Self-capacitance sensors measure the capacitance at a single electrode with respect to ground by analyzing its response to an AC signal. As previously described, the body consists of the nonconductive epidermis overlaying various conductive tissue and thereby provides an additional path for the AC current flow and reduces the current at the receiver. Touching the electrode therefore increases impedance at the node and can be modeled by adding another capacitor to ground in parallel with the electrode. Mutual capacitance on the other hand uses the coupling between a row and a column to determine finger location. When either the row or column is driven with an input drive signal, an electric field is created at intersections between rows and columns. When a finger is placed at this intersection, part of the electric field is instead coupled to the body and the mutual capacitance between the row and column decreases. Both methods apply a strong drive signal to the sensor that creates the EM signals we leverage in our design. We modulate the drive signals used by these devices to transmit data over the body.

Fingerprint sensors. At a high level, capacitive fingerprint sensors use similar operating principles to the touchpads described above. However, to achieve the high resolution necessary for fingerprint sensing the entire grid of sensors is implemented on a custom integrated circuit (IC). Rather than detecting the presence of the whole finger, this dense array of sensors instead detects the presence of the ridges or valleys of fingerprints. A problem for fingerprint sensors is that the IC must be protected against electrostatic discharge from the human body consid-

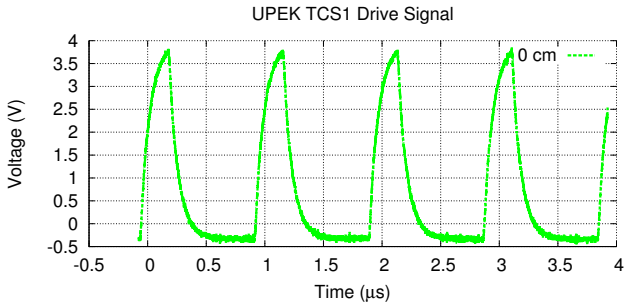


Figure 4: The figure shows the voltage signal measured on the metal contact on the Verifi P5100 during a fingerprint reading.

ering they are repeatedly touched during normal use. Adding a thicker protective layer makes the sensor more robust to electrostatic discharge, but also increases the distance between the sensor and the finger. Because capacitance is inversely proportional to distance, a thicker protective coating makes it more difficult to sense the subtle differences in capacitance caused by ridges and valleys on the finger. In order to address this, a number of capacitive fingerprint sensors use a metal contact at the edge of the sensor to apply a drive signal directly to the body.

Next, we describe the operations of a Verifi P5100 USB fingerprint scanner. The Verifi P5100 is based on the UPEK TCS1 fingerprint sensor [11] which is surrounded on all sides by a conductive metal plate and recessed such that the user's finger will necessarily be in contact with the metal during scans. Although documentation for the TCS1 is not publicly available, a patent filed by UPEK describes in detail this method of applying a drive signal to the body in order to improve sensitivity [26], which we outline below.[1]

As shown in Fig. 3, the sensing circuit is an inverting amplifier in which the feedback path is comprised of a switch in parallel with the two unconnected sensor electrodes spaced apart by less than the width of a fingerprint ridge or valley. An electrode forms one side of a capacitor C_{plate}, and the other is formed by the finger. When the sensor is below a ridge, the distance between the plates of capacitor C_{plate} is simply the thickness of the protective coating above the sensor; in contrast, a valley will have an additional air gap between the electrode and the skin causing C_{plate} to be lower. Additionally, an electric field between the two electrodes creates a capacitor, C_{mutual}, similar to the mutual capacitance case described above. A ridge which directly touches the surface of the protective coating is analogous to a finger touch in the mutual capacitance touchpad as it decreases C_{mutual} by disturbing the electric field. In contrast, the additional air gap in a valley causes less change in capacitance.

[1] Although implementation details about iPhone fingerprint sensors are scarce, we believe that a similar method to the UPEK sensors is most likely used. The company UPEK merged with another fingerprint sensor company AuthenTec [18], which was later acquired by Apple to develop a fingerprint sensor for the iPhone 5s. A patent application filed by Apple in 2013 [23] suggests that like the UPEK TCS1, the iPhone fingerprint sensor actively drives the conductive metal ring surrounding the sensor. Later models such as the iPhone 6s also appear to have the same conductive metal ring.

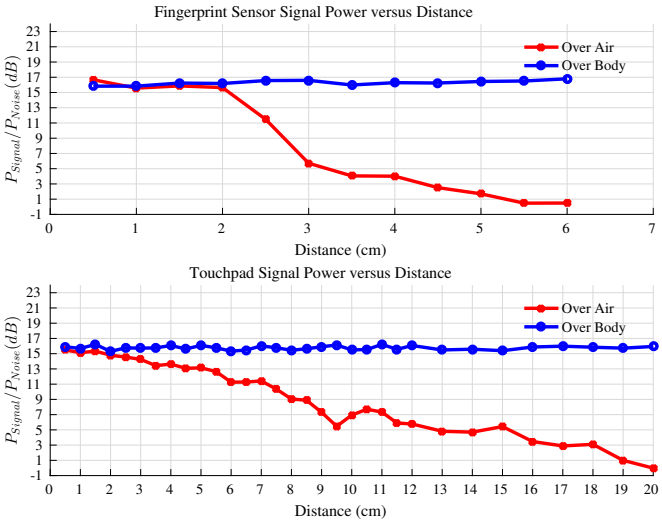


Figure 5: **Experimental Analysis 1.** We compare the strength of the EM signals generated over the body versus air at different distances between the wireless receiver and the input device. When the ratio between the power of the EM signal and ambient noise is below 0 dB, the EM signals are weaker than ambient noise.

In the sensing phase, the switch is opened and a drive signal V_{drive} is applied to the finger. Based on the equations for the gain of this switched capacitor amplifier, the output voltage can be written as, $V_{out} = -V_{drive}\frac{C_{mutual}}{C_{plate}}$. The voltage V_{out} therefore varies depending on whether the sensor is below a ridge or a valley and scales with V_{drive}. The dependence of the output on V_{drive} demonstrates the fingerprint sensor should necessarily transmit a high amplitude signal to the body. To validate this, we use an oscilloscope to measure the voltage of the metal contact on the Verifi P5100 during a fingerprint reading (sensing phase). Fig. 4 suggests that V_{drive} is an 800 kHz 4 V peak-to-peak signal. Our design leverages this high amplitude signal applied to the finger to transmit data on the body.

Analyzing the generated EM signals

To better understand the EM signals generated by our input devices, we run experiments with the following setup: we use a PCB coil antenna connected to a software-defined radio (SDR) as our wireless receiver. The SDR is composed of a USB TV tuner based on the RTL2832u chipset preceded by a 125MHz upconverter to translate the low frequency signal to be within the receiver's bandwidth. To avoid having a common ground reference between the devices, the transmitter and receiver are battery-powered. We run experiments with both the Adafruit touchpad and Verifi fingerprint sensor to analyze the EM signals they produce.

Experimental Analysis 1. We first compare the propagation of the EM signals over the body versus air. Specifically, we place the input device at a fixed location and move the receiver along a straight line from the input device. We run experiments in two different scenarios: 1) the input device and the wireless receiver are separated by air and 2) the input device and the wireless receiver are in contact with an outstretched arm. We measure the strength of the EM signals and of the ambient noise as observed at the wireless receiver at various distances

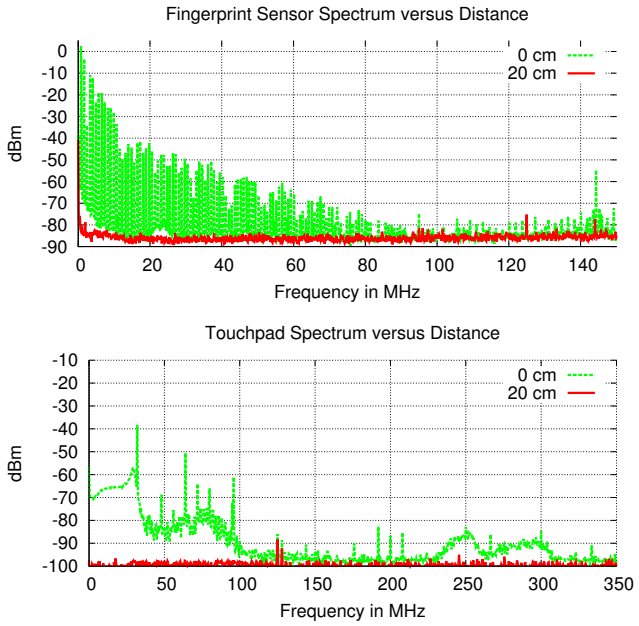


Figure 6: **Experimental Analysis 2.** The plots show the frequency spectrum of the EM signals from the fingerprint sensor and the touchpad at a receiver placed at two different distances over air.

from the input device. For each device we analyze a 10kHz bandwidth about the frequency at which the device produces the maximum amplitude signal. Fig. 5 shows the results for both the fingerprint sensor and the touchpad. The plots show that the signal strength is fairly uniform over the body as the distance between the input device and the wireless receiver increases. In contrast, over air, the signal strength rapidly decreases and the EM signal approaches the noise floor at distances of 6 cm and 20 cm for the fingerprint sensor and the touchpad respectively. This both confirms that our approach is secure considering an eavesdropper would have to be conspicuously close to a user to receive the EM signals, and that the signal propagates well through the body as predicted by the model described above.

Experimental Analysis 2. Next, we measure the frequency response of the input device across a bandwidth of 100-350 MHz to show that it does not produce additional strong signals at other frequencies that could be exploited by an attacker. To check this, we run two sets of experiments for each of our input devices. In the first set of experiments, we place an antenna directly above the input device and measure the spectrum using a Tektronix MDO4054B-3. In the second set of experiments, we place the antenna 20 cm from the input device and again measure the same spectrum. Fig. 6 shows the results for both the fingerprint sensor and the touchpad. The plots show the following:

- The EM signal has a number of higher frequency harmonics. This is because of the time-domain properties of the signal generated by these devices. For instance, as depicted in Fig. 4 the signal generated by the fingerprint sensor is similar to a square wave which in turn generates harmonics in addition to the primary frequency of the square wave.

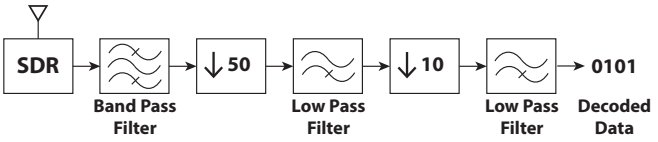


Figure 7: Block diagram of the receiver.

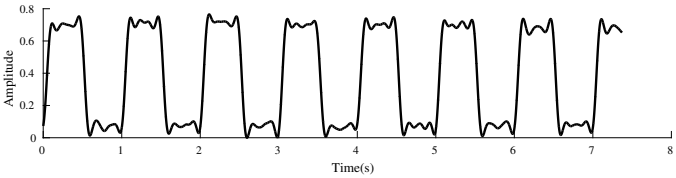


Figure 8: Example processed signal corresponding to an alternating sequence of zeros and ones.

- As the distance increases to 20 cm, signals across the whole spectrum are close to ambient noise; this demonstrates that these signals follow a near-field propagation on the air and hence are secure from far-field adversaries.

Transmitting data using input devices

Unlike a traditional radio, the signals produced by fingerprint sensors and touchpads are not designed to be modulated for data transmission. We can however amplitude modulate the EM signals they generate by starting and stopping operation of these devices. Specifically, we represent a one bit by the presence of the EM signals and a zero bit by their absence. By continuously modulating these signals, we can transmit sequences of bits on the human body.

On the Verifi P5100 USB fingerprint sensor, such a data transmission can be triggered in software. Specifically, to transmit a one bit, we set the fingerprint sensor to perform its scanning operation; to transmit a zero bit, we do not perform the scanning operation. To control the duration of each bit, we set time out values in software that allows us to terminate the scan operation before completing the full fingerprint scan. We note that Apple devices currently do not allow this level of control in software and rather abstract the use of the fingerprint sensor into the Local Authentication framework. Thus, the above bit modulation requires sleep cycling the whole phone, severely limiting the data rate. Our proof-of-concept with the Verifi USB device however demonstrates that similar hardware has the capability to be controlled at a finer grained time resolution.

To enable transmissions on the touchpad, we power cycled the touchpad device to either start or stop the EM signal generation. In our implementation, we automate this procedure by using an ATmega328p microcontroller to switch the touchpad ON and OFF at a specified rate. We however believe that with finer-grained control of the touchpad, one can achieve higher data rates than the 50 bps demonstrated in this paper.

Receiver design

A simple way to receive the above signals is to connect an antenna to an oscilloscope or other standard test equipment connected to a power outlet. The problem however is these devices have a connection earth ground which provides a low impedance return path from the transmitter to the receiver.

Figure 9: Velcro wrist strap covered in conductive copper tape used to couple the SDR receiver to the body.

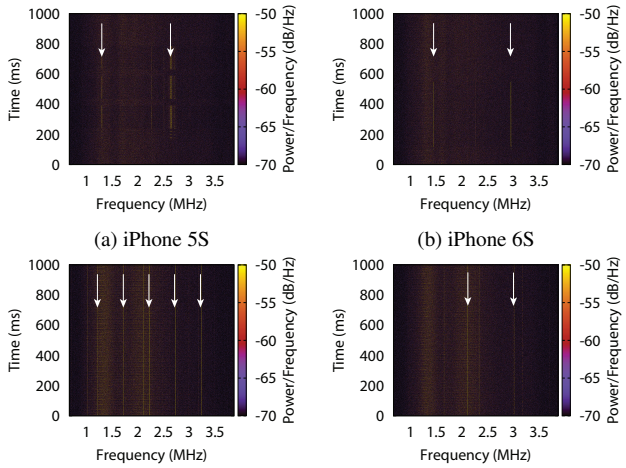
This causes a higher current at the receiver and as a result skews the results such that they would not be representative of a realistic use case in which both transmitter and receiver are battery powered and have no explicit ground connection. To prevent this, we implement our design on a software-defined radio running on a battery with no explicit connection to earth ground. Rather than designing a custom receiver circuit, we use the RTL2832U based SDR platform [1] to implement our receiver in software. The receiver is composed of a USB TV tuner based on the RTL2832u chipset preceded by a 125MHz upconverter to translate the low frequency signal to be within the receiver's bandwidth. To avoid a common ground reference, we connect the SDR to a battery powered laptop. In addition to providing the flexibility to be used with the various input devices tested, this SDR provides a convenient small form factor platform for performing measurements across the body. We connect the input of the SDR to a velcro wrist strap covered in conductive copper tape shown in Fig. 9 that can be attached tightly at different points on the user's body.

At a high level our receiver first bandpass filters the received signals to isolate the frequencies at which the EM signals have the highest amplitude. The parameters for this are determined based on the transmitting devices, as they each produce a different characteristic signal. After isolating the strongest frequency range the resulting signal is low pass filtered to remove the carrier frequency and decode the amplitude-modulated data.

To efficiently process the raw data generated, the processing steps described above are split into multiple blocks and the data is down-sampled in between. Fig. 7 shows a block diagram of the steps used for decoding data transmissions. Specifically, the raw sampled data is first passed through a finite impulse response band pass filter 14 kHz bandwidth. The output of the band pass filter is then down sampled by a factor of 50. We then apply a 1 kHz FIR low pass filter on the resulting signal. We then again down sample the resulting signals by an additional factor of 10. Finally, we apply a low pass filter with a cutoff frequency four times the data rate. This results in the signal as shown in Fig. 8 which represents an alternating sequence of zeros and ones transmitted from our fingerprint sensor. To decode the bits from this signal, we compare the output to a threshold value and output a one bit whenever the received signal is greater than the threshold and a zero bit otherwise.

EVALUATION

We run experiments with commodity fingerprint sensors and touchpads. We use the fingerprint sensors on Apple iPhone 5s and 6s as well as the Verifi P5100 USB fingerprint sensor. We also run experiments with the Lenovo Thinkpad T440s trackpad and the Adafruit capacitive touchpad. To receive and analyze the transmissions from these sensors, we use our software defined radio (SDR) implementation described earlier. We set the low noise amplifier gain for the SDR to 36.4 dB and keep this value consistent across our experiments. All our devices including the touchpads, fingerprint sensors and the SDR-based wireless receiver were battery-operated to ensure that they do not share a common ground.



(a) iPhone 5S (b) iPhone 6S

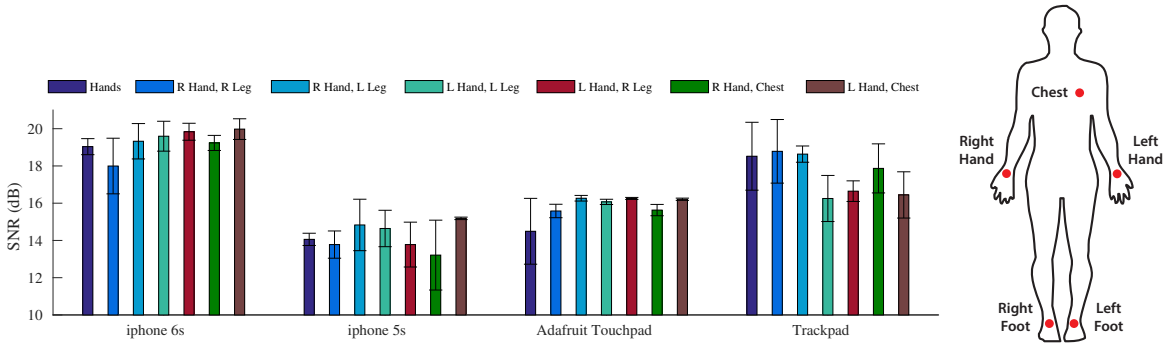
(c) Adafruit Touchpad (d) Lenovo Trackpad

Figure 10: **Spectrograms of the four input devices.**The white arrows are shown in the graphs for emphasis.

In the rest of this section, we first show the frequency response of the signals generated by these devices. We then analyze how these signals propagate throughout the body as well as the effects of posture, movements and body size on the signal strength. We then evaluate the effect of interference from other wearable devices on the reliability of our communication system. Finally, we provide results for different data rates we achieved using our input devices.

Frequency response of input devices

As described above, fingerprint sensors and touchpads have unique frequency responses measurable through the human body that we repurpose to enable on-body communication. In this section, we characterize the frequency response of our input device. Specifically, we evaluate the fingerprint sensors on an Apple iPhone 5s and iPhone 6s, as well as an Adafruit capacitive touchpad and a Lenovo Thinkpad T440s trackpad. To do this, we run experiments with a single participant who is a co-author of this paper; later we demonstrate that our results generalize across multiple participants. We ask the participant to touch the fingerprint sensor on the phone or the touchpad as they would during normal use, and place our SDR receiver on the opposite wrist. We note that the frequency response is similar throughout the body, which we later confirm with additional experiments. We compute a spectrogram showing the frequency response of the transmitting devices as a function of time. Specifically, we apply a Hamming window and compute



(a) SNR for Different Locations on Body

(b) Locations on Body

Figure 11: **Signal strength across the body.** The plot shows the SNR measured when the transmitting device was touching fingers on the right or left hand and the receiver was placed at the different marked locations.

a 1024 point DFT over one second intervals to generate the spectrogram.

Fig 10 (a) and (b) show the spectrogram over a period of one second for the fingerprint sensors on the iPhone 5s and 6s. Apple's Local Authentication Framework, which controls the fingerprint sensor, does not allow repeated scanning, but rather prompts a user for fingerprint verification. In order to test the fingerprint sensor we instructed users to repeatedly scan their finger while the phone was locked to trigger multiple scans. The plots indicate that both of the fingerprint sensors create distinct signals at specific frequencies as well as what appear to be weaker harmonics of the signals at adjacent frequencies. We note that frequency response of phones do not differ between different phones of the same model. However iPhone 5s and 6s do have a different response, most likely due to improvements made to the fingerprint sensor [41].

Next we show the spectrograms for the Adafruit touchpad and the Lenovo trackpad in Fig. 10 (c) and (d). The plots show that these devices create more harmonics than the fingerprint sensors. Further, these devices continuously create these EM signals on the body while they are powered on. Finally, the spectrograms confirm that both the touchpads and fingerprint sensors create signals with distinctive frequency responses.

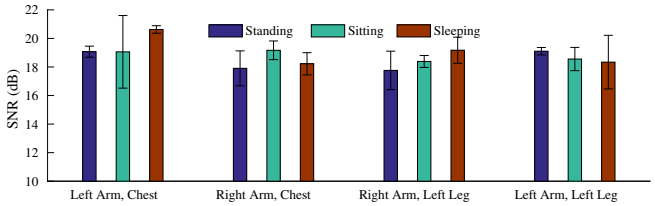
Signal strength across the body

In practice, the physical distance between the finger print sensor and wireless receiver will vary for different applications as well as the receiver's location on the body. We evaluate how well the signals from these input devices propagate to different locations on the body. To do this, we again run experiments with the fingerprint sensors on the iPhone 5s and 6s as well as the Adafruit touchpad and the Thinkpad trackpad. With each of these sensors we compute the signal to noise ratio (SNR) defined as follows:

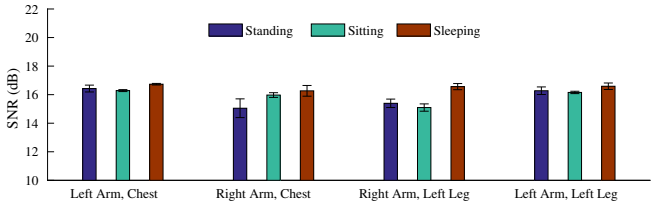
$$SNR = 10log_{10}\left(\frac{P_{ON}}{P_{OFF}}\right)$$

Here P_{ON} and P_{OFF} are defined as the average measured power when the input device is ON (performing its operation) and OFF respectively. To compute P_{ON} and P_{OFF}, we band pass filter the incoming signal to isolate frequencies between 2.642 to 2.652 MHz. We then average the signal power over a symbol period to obtain P_{ON} and P_{OFF}. We repeat the above measurements five times for each of these computations.

We run experiments to test the effect of placing the wireless receiver at different locations on the body. Specifically, we place the wireless receiver at the locations shown in Fig. 11b including the wrist, ankle and the chest. The participant holds the touchpad in either their left or right palm. In the case of the fingerprint sensor, the participant places their thumb on the sensor while for the touchpad the participant places all the fingers except the thumb on the touchpad. We run these experiments with a participant who is 68.1 inches tall and weighed 154 lbs. The experiments were run in a lab setting with a number of other machines and computers on the desk nearby including a desktop, multiple mobile phones and a laptops. Fig. 11a shows the SNR computed for various positions for the wireless receiver and the input device. The plots show the results for all our four input devices. The graphs show negligible differences in attenuation of 2-3 dB across the body. This result indicates that devices placed anywhere on the surface of the body can receive transmissions from fingerprint sensors and touchpads.



(a) iPhone 6S



(b) Adafruit Touchpad

Figure 12: Signal strength for different body postures and locations of the wireless receiver and input device.

Effect of Posture

Next, we evaluate whether the signal propagation through th body changes with the subject's posture. To do this, we pe form measurements when the subject is standing, seated, an lying down. We test the scenario in which the participant seated in a typical office desk chair and lying down horizo tally on their back on a leather couch. We run experimen with the iPhone 6s fingerprint sensor and the Adafruit touch pad. For each posture we place the input device at the user right or left palm and the wireless receiver on their chest legs. Figs. 12 (a) and (b) show the measured SNR valu as a function of different posture with the iPhone 6s and th touchpad. The figure shows a minimal change of 1–2 d across postures demonstrating that the system is applicable f a variety of different use cases.

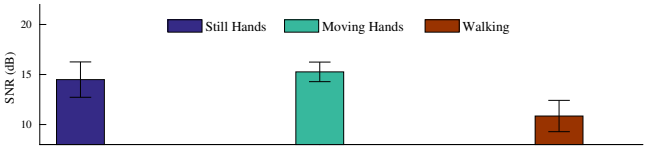


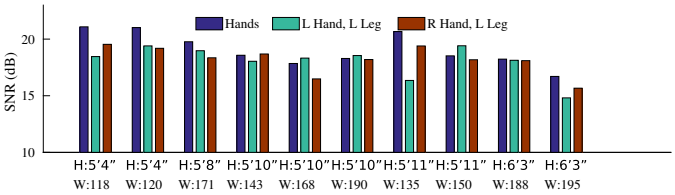
Figure 13: Signal strength for different movement scenarios with the Adafruit touchpad.

Effect of motion

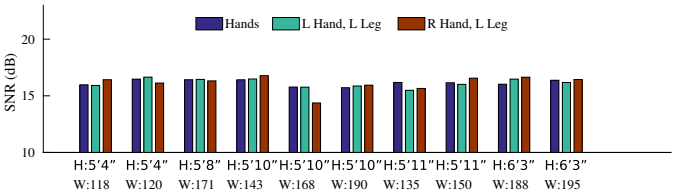
We evaluate how the signal propagation is affected by motion. In order to characterize the effect of motion we compare the propagation of the signal between a user's hands when stationary, when only the hands are in motion, and when the user is walking. Specifically, the subject touches the Adafruit touchpad with four fingers on their right hand and wears our wireless receiver on the wrist of the left hand. We measure the SNR values using the same method described above in these different mobility scenarios. Specifically, we ask the subject to move both arms in a continuous marching motion at the maximum speed of around 0.11 meter per second as the first mobility scenario. For the second mobility scenario, the subject walks while moving their arms. We also perform the experiments in the absence of motion, as a baseline. Fig. 13 shows the SNR measurements across these scenarios. The plots show that hand motion does not significantly affect the observed SNR values; however, walking causes more attenuation than just arm motion. This is likely due to inconsistent contact with the touchpad or receiver electrode while walking. The key observation is that the SNR is greater than 10 dB across all the tested scenarios, which is sufficient for communication. For comparison, Wi-Fi requires an SNR of 3-5 dB to operate at its lowest bit rate of 1 Mbps.

Effect of height and weight

The above experiments were performed on a single subject for consistency. Next, we evaluate the efficacy of our design across ten different adult subjects with varying heights and weights. Specifically, we place the wireless receiver and the input devices at different points on the subject's body and measure the SNR values as described before. We run experiments with the fingerprint sensor on iPhone 6s as well as the Adafruit touchpad. Fig. 14 (a) and (b) show the results for each of the ten subjects along with their heights and weights



(a) iPhone 6s



(b) Adafruit Touchpad

Figure 14: Measurements of signal propagation across different body types.

for different locations of the wireless receiver on the body. The plots show that despite a standard deviation of 3.57 inches and 27.25 pounds in height and weight respectively of the subjects, the resulting SNR measurements have a maximum standard deviation of 0.7 dB when measured from the arm to leg for the touchpad and 1.43 dB for the corresponding measurements using the iPhone 6s. While these values would have been significant at very low SNRs, since the observed signal to noise values are above 10 dB, it does not impact the performance of our communication system.

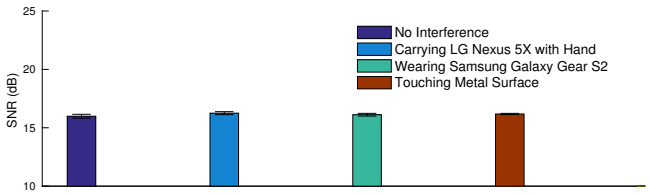


Figure 15: Impact of various interference scenarios on SNR using the Adafruit Touchpad.

Impact of interference

Although our design does not interfere with high frequency radio transmissions such as Wi-Fi and Bluetooth, we notice that devices with LCD screens or touchscreens/touchpads are known to produce low frequency EM signals. Fig. 16 shows the frequency spectrum measured when a LG Nexus 5X phone screen is ON versus OFF using our SDR receiver connected to a wire coil placed in contact with the phone screen. To evaluate how this noise can affect our communication system we run experiments with an LG Nexus 5X smartphone and a Samsung Galaxy Gear S2 smartwatch. Additionally we evaluate the impact of large metal objects such as tabletops that could potentially reflect or radiate signals from the environment [2] by touching a 1.72 ft^2 steel surface. We place the user's right wrist in contact with the interfering object and place the Adafruit touchpad on the same arm 20 cm above the wrist. We place the receiver on the user's left wrist positioned

50 cm away from their right arm to guarantee the signal was propagating through the body and not coupling directly to the receiver through the air.

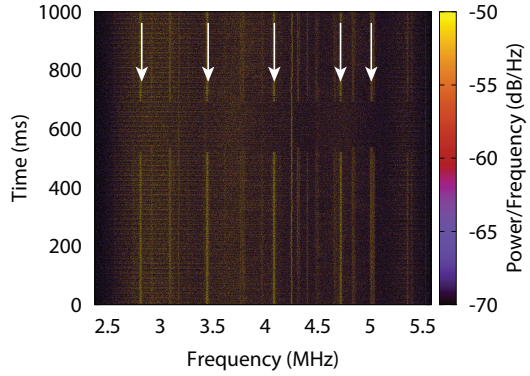


Figure 16: EM signals from the screen of a Nexus 5X smartphone captured by an antenna placed on top of the phone.

Fig. 15 shows the results for each of these scenarios. The plots show high SNR indicating that signals from the environment or other wearable devices do not couple as well to the body We confirm this by measuring the EM signals of the LG Nexus 5X phone screen over the body. While the signals were clear on an antenna placed right on top of the phone, we could not see any signal over the body. Thus, the EM signals generated by the screens of such devices do not propagate well over the body and hence do not cause interference. This not only suggests that the system is robust to interference from existing devices, but also suggests that it would be difficult for an attacker to transmit an external signal on the air to either jam transmissions or send false information. This experiment also confirms that the dominant source of noise in the system will be from the receiver circuit rather than outside interference.

Different data rates

Finally, we analyze the data rates achieved by our communication system using the Adafruit touchpad and the Verifi fingerprint sensor. As noted earlier, on the Verifi P5100 USB fingerprint sensor such a data transmission can be triggered in software. Specifically, to transmit a one bit, we set the fingerprint sensor to perform its scanning operation; to transmit a zero bit we do not perform the scanning operation. We note that the API for the device does not allow direct control of the drive signal and rather is designed for discrete high level tasks such as fingerprint verification. In order to use the sensor to transmit information, we utilize the timeout functionality exposed by the API to begin and terminate fingerprint scans rapidly. We observe however only specific time delays could be realized achieving bit rates of 0.92, 1.7, 2, 3.6, 5.8 and 25 bps. To transmit bits using the touchpad, we power cycled it to either start or stop the EM signal generation and generate different bit rates between 1 and 50 bps.

We run experiments where we place the input device on the palm of the right hand and attach the wireless receiver to the left arm. We measure the SNR values at different bit rates as observed by the receiver. Fig. 17 shows the measured SNR values as a function of the bit rates used for both the fingerprint sensor and the touchpad. The plot shows that for the touchpad, as the bit rate increases the SNR slightly decreases. This is most likely because as the bit rate increases the touchpad has less time to power up the circuit. Given a finite rise time for the circuit, the signal strength slightly reduces as the bit transitions occur at a higher rate. For the fingerprint sensors on the other hand, the SNR is consistently between 16 and 20 dB across the bit rates. This demonstrates that we can achieve data rates between 25–50 bits per second using commodity fingerprint sensors and touchpads. We emphasis here that the achievable bit rates are currently limited by the API provided in software and are not fundamentally limited to the values we demonstrate. With an API that provides a more fine-grained access to the hardware, we believe that one could achieve even higher data rates.

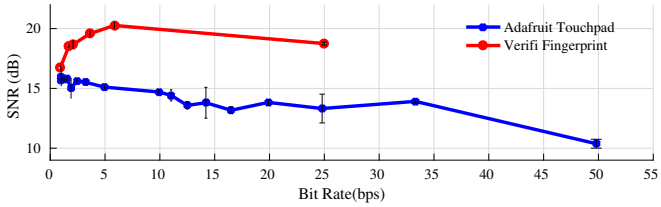


Figure 17: **SNR as a function of bit rate.** We can achieve 25 and 50 bps with the fingerprint sensor and touchpad respectively.

RELATED WORK

Related work falls in three main domains.

Body-coupled communication. Researchers have explored a variety of approaches to send information through the human body [4, 24, 7]. Detailed models and measurements of the human body as a communication channel have been developed in [25, 50, 3, 5]. The focus of these works, however, has been to characterize the transmission properties of the body in order to build custom transceiver solutions. This paper builds on this foundational work to show instead that commodity input devices with fingerprint sensors or touchpads produce EM signals that propagate on the human body and can be repurposed to transmit data through the body. Below we describe the prior work in this domain in greater detail.

It is known that signals can be transmitted through the body in one of three ways: galvanic coupling, capacitive coupling, and magnetic resonant coupling. [25] developed a detailed model of the body for galvanic coupling based on tissue characteristics. Zimmerman et. al [50] first introduced the concept of communication through the body with capacitive coupling in which the environment is used as the return path. Following this work, [7] presents an experimental characterization of the human body channel for capacitive coupling. [3] improves upon this work and gives a detailed explanation of galvanic and capacitive coupling including careful experimental characterization of attenuation through this channel in which grounding effects are isolated. [48, 14, 49] demonstrates custom transmitter and receiver hardware that can stream information through the body in a capacitively coupled system. Applications of body coupled communications have been outlined in [30], which presents a wrist worn system based on capacitive coupling for use as a personalized key with custom designed

transmitters and receivers. [35] explores pulse width modulation for body coupled communication schemes. Additional work has also modeled propagation loss through the body channel including fading due to motion [32]. [40] designs a custom transmitter-receiver pair that use electro-optic effect and laser light to achieve a sensitive electric field sensor for on-body communication. [36] briefly explores magnetic resonant coupling, but to date a communication system using this method has not been demonstrated.

DiamondTouch [13] presents an interactive touch surface that transmits capacitively coupled signals through the human body. The authors use a custom built table embedded with antennas to transmit the signals. Microchip Technology's Bodycomm system is a commercial version of a capacitive human body communication system [43], however it requires integration of a separate custom radio chip into the transmitting device. In contrast to all the above work, we demonstrate for the first time that input devices such as fingerprint sensors and touchpads available on commodity devices can be used to send information on the human body.

Finally, prior work [22, 45] has shown that touchscreens can be used to *receive* signals through the body. However, these design still require custom transmitter hardware. In contrast, we show for the first time that one can use commodity devices to *transmit* through the body. We also note that the custom transmitter hardware in [22, 45] was worn on the same arm as the hand using the touch screen and has not been demonstrated to work across the whole body. In contrast, we demonstrate that the transmissions generated by our design can propagate across the whole body.

EM emanations. Prior work has demonstrated that the EM signals radiated from devices such as power supplies and computer monitors can be used to extract cryptographic keys [15] as well as recognize gestures [9, 8]. [20] demonstrate that these signals can be modulated to transmit information over the air. [27] classifies the EM noise emitted by electrical and electromechanical objects to identify kitchen appliances, computing devices, power tools and automobiles. In contrast, we show that commodity fingerprint sensors and touchpads can be used to transmit data and that they effectively propagate throughout the human body.

Secure wireless pairing. Wirelessly pairing two devices has been an active area of research in the security community. The simplest approach involves a physical wired connection between the devices, however such an approach is cumbersome and impractical for sensors worn on the body. Visual and gesture based approaches [38, 39, 31] are susceptible to eavesdropping by a person or camera with line of sight to the user. Acoustic solutions [19, 42] and far field wireless transmitters [37] face similar challenges. Near field wireless transmitters such as NFC or RFID require a central device in close proximity to each sensor for pairing. In contrast, our solution simply requires devices to be in contact with the body. Physical layer techniques [16] use measurements of the devices' communication channel to establish secret keys. [34] uses biometric measurements such as heart rate to agree on the keys and for synchronizing devices on the human body, however such a solution would be difficult for patients with cardiovascular diseases affecting their heart rhythm. Using a device such as a touchpad or fingerprint sensor has similar security advantages to biometric methods, but has the advantage of being able to send arbitrary data bits over the human body.

DISCUSSION AND CONCLUSION

We show that commodity fingerprint sensors and touchpads can be used to generate wireless data transmissions that are confined to the human body. We present a receiver design that can reliability decode our data transmissions and demonstrate bit rates of up to 50 bps by modulating the operations of these input devices. We now discuss some of the potential directions for improving the design presented in this paper.

High data rates. While the data rates demonstrated in this paper are sufficient for our target application scenarios, we believe that with better access to the hardware functionality of fingerprint sensors and touchpads, one can achieve higher data rates. In the case of the fingerprint sensor for example, the existing API was not designed with our communication application in mind and therefore it arbitrarily restricts the minimum transmission length, thereby limiting our data rate. Our measurements show that these devices are clearly capable of applying the pulses of the drive signal at a faster rate; enabling finer grained software control over this would greatly increase the achievable data rates.

Custom versus commodity receivers. The focus in this paper is to enable on-body transmissions using commodity fingerprint sensors and touchpads. We use a custom receiver to decode these transmissions. This is acceptable for our target applications since the wireless receiver can be integrated into doorknobs or medical devices, while allowing the users to use ubiquitous mobile devices such as smartphones to transmit data on the body. We note that even with only the ability to broadcast data to all receiving nodes on the body, our system does provide a means to receive feedback from these devices. For example, in the case of pairing, a device could use a different channel to indicate failure or success by sending acknowledgment over Wi-Fi/Bluetooth or even blinking an LED. In the case of the door application, the user gets an implicit feedback when the door successfully opens. Future work could also explore the possibility of receiving feedback from sensors on the body or from touching objects in the environment using touchscreens or other sensors designed to measure changes in electric fields, without the need for custom receivers.

Secure MAC protocols. We demonstrate a secure physical communication link through the body and discuss how such signals could be used to provide time synchronization in a secure MAC protocol for body area networks. Building such secure MAC protocols to enable a network of sensors on the body to be synchronized using signals from a phone is an interesting direction that is worth exploring in the future.

ACKNOWLEDGMENTS.

We thank Joshua Smith and Vamsi Talla for their feedback on the paper. This work was funded in part by the Intel Science and Technology Center for Pervasive Computing, a Google faculty award and National Science Foundation grants.

REFERENCES

1. 2016. About RTL-SDR. http://www.rtl-sdr.com/about-rtl-sdr/. (2016). Accessed:2016-03-31.
2. Occupational Health & Safety Administration. 1990. Electromagnetic Radiation and How It Affects Your Instruments. Near field vs. Far field. (May 1990).
3. G. S. Anderson and C. G. Sodini. 2013. Body coupled communication: The channel and implantable sensors. In *Body Sensor Networks (BSN), 2013 IEEE International Conference on*. 1–5.
4. A. R. Ansari and Sunghyun Cho. 2014. Human body: The future communication channel for WBAN. In *Consumer Electronics (ISCE 2014), The 18th IEEE International Symposium on*. 1–3.
5. J. Bae, H. Cho, K. Song, H. Lee, and H. J. Yoo. 2012. The Signal Transmission Mechanism on the Surface of Human Body for Body Channel Communication. *IEEE Transactions on Microwave Theory and Techniques* 60, 3 (March 2012), 582–593.
6. Gary Barrett and Ryomei Omote. 2010. Projected-capacitive touch technology. *Information Display* 26, 3 (2010), 16–21.
7. W. c. Wang, Z. d. Nie, F. Guan, T. f. Leng, and L. Wang. 2011. Experimental Studies on Human Body Communication Characteristics Based Upon Capacitive Coupling. In *Body Sensor Networks (BSN), 2011 International Conference on*. 180–185.
8. Gabe Cohn, Daniel Morris, Shwetak Patel, and Desney Tan. 2012. Humantenna: Using the Body As an Antenna for Real-time Whole-body Interaction. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. ACM, New York, NY, USA, 1901–1910.
9. Gabe Cohn, Daniel Morris, Shwetak N. Patel, and Desney S. Tan. 2011. Your Noise is My Command: Sensing Gestures Using the Body As an Antenna. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 791–800.
10. 3M Company. 2013. Projected Capacitive Technology. (2013). multimedia.3m.com/mws/media/7884630/tech-brief-projected-capacitive-technology.pdf Accessed:2016-03-31.
11. Crossmatch. 2010. TouchChip TCS1. (2010). http://www.crossmatch.com/tcs1-sensor/ Accessed:2016-03-31.
12. Dexcom. 2010. Dexcom G4 User's Guide. (2010). http://www.dexcom.com/sites/dexcom.com/files/dexcom-g4/docs/dexcomG4-UsersGuide-English-mmol24hr.pdf
13. Paul Dietz and Darren Leigh. 2001. DiamondTouch: A Multi-user Touch Technology. In *Proceedings of the 14th Annual ACM Symposium on User Interface Software and Technology (UIST '01)*. ACM, New York, NY, USA, 219–226.
14. Ericsson. 2012. When the body becomes the network. (2012). https://www.ericsson.com/res/thecompany/docs/press/media_kits/infographics_connected_me.pdf
15. Daniel Genkin, Adi Shamir, and Eran Tromer. 2014. RSA key extraction via low-bandwidth acoustic cryptanalysis. In *Advances in Cryptology–CRYPTO 2014*. Springer, 444–461.
16. Shyamnath Gollakota, Nabeel Ahmed, Nickolai Zeldovich, and Dina Katabi. 2011a. Secure In-Band Wireless Pairing.. In *USENIX security symposium*. San Francisco, CA, USA, 1–16.
17. Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. 2011b. They Can Hear Your Heartbeats: Non-invasive Security for Implantable Medical Devices. *SIGCOMM Comput. Commun. Rev.* 41, 4 (Aug. 2011), 2–13.
18. Dan Goodin. 2012. Confirmed: Apple-owned fingerprint software exposes Windows passwords. (Oct. 2012). http://arstechnica.com/security/2012/10/confirmed-fingerprint-reader-owned-by-apple-exposes-\windows-passwords/ Accessed:2016-03-31.
19. M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun. 2006. Loud and Clear: Human-Verifiable Authentication Based on Audio. In *Distributed Computing Systems, 2006. ICDCS 2006. 26th IEEE International Conference on*. 10–10.
20. Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici. GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies. In *24th USENIX Security Symposium (USENIX Security 15)*. USENIX Association, Washington, D.C., 849–864.
21. D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. 2008. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*. 129–142.
22. Christian Holz and Marius Knaust. 2015. Biometric Touch Sensing: Seamlessly Augmenting Each Touch with Continuous Authentication. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology (UIST '15)*. ACM, New York, NY, USA, 303–312.
23. S.P. Hotelling, J.M. Bussat, and B.B. Lyon. 2013. Capacitive Sensing Array Modulation. (Oct. 17 2013). https://www.google.com/patents/US20130271422 US Patent App. 13/842,635.
24. S. j. Song, S. J. Lee, N. Cho, and H. j. Yoo. 2006. Low Power Wearable Audio Player Using Human Body Communications. In *Wearable Computers, 2006*.

25. B. Kibret, M. Seyedi, D. T. H. Lai, and M. Faulkner. 2014. Investigation of Galvanic-Coupled Intrabody Communication Using the Human Body Circuit Model. *Journal of Biomedical and Health Informatics* (2014).

26. A. Kramer. 2001. Enhanced fingerprint detection. (Oct. 4 2001). https://www.google.com/patents/US20010025532 US Patent App. 09/753,344.

27. Gierad Laput, Chouchang Yang, Robert Xiao, Alanson Sample, and Chris Harrison. 2015. EM-Sense: Touch Recognition of Uninstrumented, Electrical and Electromechanical Objects *(UIST '15)*.

28. H. Li and J. Tan. 2010. Heartbeat-Driven Medium-Access Control for Body Sensor Networks. *IEEE Transactions on Information Technology in Biomedicine* 14, 1 (Jan 2010), 44–51.

29. G. Lu, B. Krishnamachari, and C. S. Raghavendra. 2004. An adaptive energy-efficient and low-latency MAC for data gathering in wireless sensor networks. In *Parallel and Distributed Processing Symposium, 2004. Proceedings. 18th International*. 224–.

30. N. Matsushita, S. Tajima, Y. Ayatsuka, and J. Rekimoto. 2000. Wearable key: device for personalizing nearby environment. In *Wearable Computers, The Fourth International Symposium on*. 119–126.

31. R. Mayrhofer and H. Gellersen. 2009. Shake Well Before Use: Intuitive and Secure Pairing of Mobile Devices. *IEEE Transactions on Mobile Computing* 8, 6 (June 2009), 792–806.

32. Nafiseh Seyed Mazloum. 2008. *Body-Coupled Communications: Experimental characterization, channel modeling, and physical layer design*. Ph.D. Dissertation. Chalmers University of Technology.

33. A&D Medical. 2016. UA-767PC Instruction Manual. (2016). http://www.andonline.com/uploads/documents/I-MAN-UA-767PC.pdf

34. Samira Mesmoudi and Mohammed Feham. 2011. BSK-WBSN: biometric symmetric keys to secure wireless body sensors networks. (2011).

35. Miltiadis Moralis-Pegios, Pelagia Alexandridou, and Christos Koukourlis. 2015. Applying Pulse Width Modulation in Body Coupled Communication. *Journal of Electrical and Computer Engineering* 2015 (2015), 1–6.

36. J. Park and P. P. Mercier. 2015. Magnetic human body communication. In *Engineering in Medicine and Biology Society (EMBC), 2015 37th Annual International Conference of the IEEE*. 1841–1844.

37. T. J. Pierson, X. Liang, R. Peterson, and D. Kotz. 2016. Wanda: securely introducing mobile devices. In *INFOCOM WKSHPS*.

38. N. Saxena, J. E. Ekberg, K. Kostiainen, and N. Asokan. 2006. Secure device pairing based on a visual channel. In *IEEE Security and Privacy, 2006*. 6 pp.–313.

39. Mohit Sethi, Elena Oat, Mario Di Francesco, and Tuomas Aura. 2014. Secure Bootstrapping of Cloud-managed Ubiquitous Displays *(UbiComp '14)*. New York, NY, USA, 739–750.

40. M. Shinagawa, M. Fukumoto, K. Ochiai, and H. Kyuragi. 2003. A near-field-sensing transceiver for intra-body communication based on the electro-optic effect. In *Instrumentation and Measurement Technology Conference, 2003.*, Vol. 1. 296–301.

41. Chris Smith. 2015. iPhone 6s: How fast is the new Touch ID fingerprint sensor? (2015). http://bgr.com/2015/09/25/iphone-6s-touch-id-fingerprint/ Accessed:2016-03-31.

42. Claudio Soriente, Gene Tsudik, and Ersin Uzun. 2008. *Information Security: 11th International Conference, ISC 2008, Taipei, Taiwan, September 15-18, 2008. Proceedings*. Springer Berlin Heidelberg, Berlin, Heidelberg, Chapter HAPADEP: Human-Assisted Pure Audio Device Pairing, 385–400.

43. Microchip Technology. 2013. Bodycom Tehcnology. (Feb. 2013). http://ww1.microchip.com/downloads/en/DeviceDoc/30685a.pdf Accessed:2016-03-31.

44. Tijs van Dam and Koen Langendoen. 2003. An Adaptive Energy-efficient MAC Protocol for Wireless Sensor Networks. In *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys '03)*. ACM, New York, NY, USA, 171–180.

45. Tam Vu, Akash Baid, Simon Gao, Marco Gruteser, Richard Howard, Janne Lindqvist, Predrag Spasojevic, and Jeffrey Walling. 2012. Distinguishing Users with Capacitive Touch Communication. In *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking (Mobicom '12)*. ACM, New York, NY, USA, 197–208.

46. Marc Simon Wegmüller. 2007. *Intra-Body Communication for Biomedical Sensor Networks*. Ph.D. Dissertation. Massachusetts Institute of Technology.

47. Wei Ye, J. Heidemann, and D. Estrin. 2002. An energy-efficient MAC protocol for wireless sensor networks. In *INFOCOM 2002*, Vol. 3. 1567–1576 vol.3.

48. H. J. Yoo and N. Cho. 2008. Body channel communication for low energy BSN/BAN. In *Circuits and Systems, 2008. APCCAS 2008.* 7–11.

49. Hoi-Jun Yoo, Seong-Jun Song, Namjun Cho, and Hye-Jeong Kim. 2007. *Low Energy On-Body Communication for BSN*. Springer Berlin Heidelberg, Berlin, Heidelberg, 15–20.

50. Thomas G. Zimmerman, Joshua R. Smith, Joseph A. Paradiso, David Allport, and Neil Gershenfeld. 1995. Applying Electric Field Sensing to Human-computer Interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '95)*. ACM Press/Addison-Wesley Publishing Co., New York, NY, USA, 280–287.