Towards Touch-to-Access Device Authentication Using Induced Body Electric Potentials

Zhenyu Yan
Nanyang Technological University
zyan006@ntu.edu.sg

Qun Song
Nanyang Technological University
song0167@ntu.edu.sg

Rui Tan
Nanyang Technological University
tanrui@ntu.edu.sg

Yang Li*
Shenzhen University
yli@szu.edu.cn

Adams Wai Kin Kong
Nanyang Technological University
adamskong@ntu.edu.sg

ABSTRACT

This paper presents TouchAuth, a new touch-to-access device authentication approach using induced body electric potentials (iBEPs) caused by the indoor ambient electric field that is mainly emitted from the building's electrical cabling. The design of TouchAuth is based on the electrostatics of iBEP generation and a resulting property, i.e., the iBEPs at two close locations on the same human body are similar, whereas those from different human bodies are distinct. Extensive experiments verify the above property and show that TouchAuth achieves high-profile receiver operating characteristics in implementing the touch-to-access policy. Our experiments also show that a range of possible interfering sources including appliances' electromagnetic emanations and noise injections into the power network do not affect the performance of TouchAuth. A key advantage of TouchAuth is that the iBEP sensing requires a simple analog-to-digital converter only, which is widely available on microcontrollers. Compared with existing approaches including intra-body communication and physiological sensing, TouchAuth is a low-cost, lightweight, and convenient approach for authorized users to access the smart objects found in indoor environments.

*This work was completed while Yang Li was with Advanced Digital Sciences Center, Illinois at Singapore.

MobiCom '19, October 21–25, 2019, Los Cabos, Mexico

ACM ISBN 978-1-4503-6169-9/19/10…$15.00
https://doi.org/10.1145/3300061.3300118

CCS CONCEPTS

• **Human-centered computing** → **Ubiquitous and mobile computing**; • **Computer systems organization** → **Embedded and cyber-physical systems**; • **Networks** → *Mobile and wireless security*.

KEYWORDS

Device authentication, wearables, induced body electric potential

ACM Reference Format:
Zhenyu Yan, Qun Song, Rui Tan, Yang Li, and Adams Wai Kin Kong. 2019. Towards Touch-to-Access Device Authentication Using Induced Body Electric Potentials. In *The 25th Annual International Conference on Mobile Computing and Networking (MobiCom '19), October 21–25, 2019, Los Cabos, Mexico.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3300061.3300118

1 INTRODUCTION

The indoor environments are increasingly populated with smart objects. It is estimated that by 2022, a typical family home could contain more than 500 smart devices [13]. Managing the access with many objects, including accessing the information on them or granting them to access certain information, becomes challenging. Typing password is tedious and infeasible for the objects without a keyboard or touchscreen. Biometrics-based user authentication suffers various shortcomings. Fingerprint scanning requires a well positioned finger press. Moreover, due to cost factor, small objects will unlikely have fingerprint scanners. Face recognition solutions require face positioning and are costly [26]. Voice recognition-based access can be disturbing in certain environments, e.g., an open-plan office with colleagues, a bedroom with sleeping buddies, etc. Moreover, defining a separate voice passphrase for each smart object to avoid incorrect invoking may result in too many passphrases.

In this paper, we aim to develop a low-cost and convenient *touch-to-access* scheme that can be easily implemented on smart objects found in indoor environments. Specifically,

a simple touch on an object allows an authorized user to access the object. This scheme will not require non-trivial interferences for user interactions, e.g., touchscreen. Different from integrating user identification (e.g., fingerprint scanning) into the objects, we resort to a *device authentication* approach that offloads the user's identity to a personal *wearable token* device (e.g., a smart watch or bracelet) and uses the token to access a touched object that has been previously paired with the token. This touch-to-access device authentication approach can greatly improve the user's convenience and experience in interacting with the smart objects. For instance, in a home with multiple residents, when a user wearing his token turns on a TV set using a smart remote control, the control obtains the user identity from the token and instructs the TV set to list the user's favorite channels. The user can also touch other smart objects to personalize them, e.g., touch a music player for the favorite music, switch on a light that automatically tunes to the user's favorite color temperature or hue, etc.

If the user can protect the personal wearable token well, the touch-to-access device authentication can also be used in more access-critical scenarios. For example, a touch on a smartphone or tablet unlocks the device's screen automatically, allows in-app purchases, passes the parental controls, etc. Beyond the above use scenarios for improved convenience in access control, the touch-to-access scheme can also enhance the security of various systems. For instance, it can be used with fingerprint scanning to form a two-factor authentication against fake fingerprints. A wireless reader can access a worn medical sensor only if the reader has a physical contact with the wearer's skin. The contact enforces the wearer's awareness regarding the access and prevents remote wireless attacks with stolen credentials [16]. Thus, the touch-to-access scheme will be more secure than the existing hardware token approaches such as Duo [9].

The essence of the touch-to-access scheme is the detection of whether the wearable token and the smart object in question have physical contact with the same user's body. Existing studies tackle this same-body contact detection problem by intra-body communication (IBC) [2, 18, 25, 29, 36, 43, 52] and physiological sensing such as electrocardiography (ECG) [19, 31, 37, 41, 46], photoplethysmogram (PPG) [19, 31, 41], and electromyogram (EMG) [51]. IBC requires either non-trivial customized transceivers [2, 25, 29, 36, 52] or a touchscreen as the receiver [18, 43], resulting in increased cost or reduced applicable scope. The physiological sensing approaches are based on a *body-area property*, i.e., the physiological signals captured from the same human body have similar values or features, whereas those collected from different human bodies are distinct. However, the physiological sensors are often bulky due to the required physical distances among a sensor's electrodes [3, 51]. Furthermore, they often need careful placement and may perform poorly in daily life settings [4].

Different from IBC and physiological sensing, in this paper, we investigate the feasibility and effectiveness of using *induced body electric potential* (iBEP) due to the *body antenna effect* for touch-to-access device authentication. As a non-physiological phenomenon, the body antenna effect refers to the alteration of the intensity of the mains hum captured by an analog-to-digital converter (ADC) when the ADC has a physical contact with a human body. The mains hum induced by the building's electrical cabling is ubiquitous. In addition, ADC is a basic electronic component that is widely available on microcontrollers. Recent studies have exploited the body antenna effect for key stroke detection [10], touch sensing [8], motion detection [6], gesture recognition [7], and wearables clock synchronization [48]. These studies leverage several characteristics of iBEP, such as signal intensity alteration [10] and periodicity [48], or feed iBEP signals to machine learning algorithms for motion and gesture recognition [6–8]. Differently, to use iBEP for device authentication, its body-area property and the underlying physical mechanism need to be well understood. To the best of our knowledge, these issues have not been studied.

In this paper, we discuss in detail the physical mechanism of the iBEP's generation and its body-area property. The iBEP measurement by an ADC is the difference between the electric potentials of the ADC pin and the ground[1] of the sensor, respectively. From electrostatics, a human body, which can be viewed as an uncharged conductor, will alter its nearby electric field (EF) emitted from the electrical cabling of the building due to electrostatic induction. As a result, the iBEP measurement by a sensor will be affected by the presence of a nearby human body. In particular, we make the following two hypotheses based on the above understanding. First, the iBEP signals measured by two sensors that are on the same human body and close to each other will be similar. This is because 1) the two sensors' ADC pins will have the same potential due to their connections to the equipotential human body, and 2) their grounds will most likely have similar potentials as they are close to each other in the EF. Second, the iBEP signals collected from different human bodies will be different. This is because different human bodies will most likely have different potentials and thus affect nearby EFs differently since they build up different surface charge distributions in the electrostatic induction.

Our extensive measurement results are consistent with the above two hypotheses. Based on the results, we design a prototype system called *TouchAuth* that performs touch-to-access device authentication based on iBEP signals. We implement the same-body contact detection algorithm based

[1]Throughout this paper, "ground" refers to the floating ground of a device.

on two similarity metrics, i.e., absolute Pearson correlation coefficient (APCC) and root mean square error (RMSE). Extensive experiments show that the APCC-based TouchAuth achieves true acceptance rates of 94.2% and 98.9% subject to a false acceptance rate upper bound of 2% when one and five seconds of iBEP signal is recorded, respectively. In contrast, ECG/PPG approaches [19, 31, 41] need to record the signal(s) for tens of seconds to achieve comparable detection accuracy (cf. §8). Our experiments also show that various possible interfering sources including appliances' electromagnetic emanations and noise injections into power networks do not affect TouchAuth.

In summary, TouchAuth is a low-cost, lightweight, and convenient approach for the authorized users to access smart objects in indoor environments. To implement TouchAuth, the smart object's and the wearable token's microcontroller ADCs are to be wired to their conductive exteriors. Compared with the near-field communication (NFC) approach that enforces a proximity requirement on device authentication, the touch requirement of TouchAuth is more intuitive and clearer. Moreover, compared with the ADCs that are widely available on microcontrollers, the NFC chips are more costly and need to be integrated into the smart objects to read the wearable tags.

The contributions of this paper are summarized as follows:

- We explain the generation mechanism of iBEP and show that iBEP is an effective signal for devising a touch-to-access device authentication approach.
- We design an iBEP-based device authentication approach called TouchAuth. It uses iBEPs to detect whether two devices are in proximity on the same human body.
- Extensive experiments under real-world settings are conducted to evaluate the performance of TouchAuth.

The rest of this paper is organized as follows. §2 presents the system and threat models, and the approach overview. §3 presents the electrostatics of iBEP generation and states the objective of this paper. §4 presents the measurement study. §5 and §6 design and evaluate TouchAuth, respectively. §7 discusses several issues. §8 reviews related work. §9 concludes the paper.

2 SYSTEM OVERVIEW

2.1 System Model

We consider an authentication system with two devices that have been previously paired, i.e., an *authenticator* and an *authenticatee*. We assume that the two devices have a wireless communication channel, e.g., Wi-Fi, Bluetooth (Low Energy), Zigbee, etc. The pairing enables them to communicate. The authenticator is a trustworthy device that can sense the iBEP signal $s(t)$, $\forall t$, at a location $\mathcal{L}$ on the body of a user $\mathcal{U}$. To be authenticated, the authenticatee presents its sensed iBEP signal $s'(t)$, $t \in [t_1, t_2]$, to the authenticator. The $\ell = t_2 - t_1$ is called *signal length*. The authenticatee is *valid* only if it has physical contact with a location $\mathcal{L}'$ on $\mathcal{U}$ which is close to $\mathcal{L}$ such that $s'(t) \approx s(t)$, $\forall t \in [t_1, t_2]$; otherwise, it is *invalid*. The valid authenticatee will be granted a certain access; the invalid authenticatee will be denied the access. We assume that the clocks of the authenticator and the authenticatee are synchronized, such that the authenticator can select a segment of $s(t)$ in the time duration $[t_1, t_2]$ to check the similarity between $s(t)$ and $s'(t)$ for same-body contact detection. Before the authentication process, clock synchronization can be achieved using existing approaches [23, 24, 48].

We now discuss the roles of different devices in the scenarios discussed in §1. When the user with a wrist wearable token touches a smartphone to unlock its screen, the wearable token is the authenticator, whereas the automatic unlock program on the phone is the authenticatee. On detecting human touch (by either button/touchscreen press or increased iBEP intensity), the unlock program presents its captured iBEP signal to the wearable token that will perform the same-body detection. A positive detection result allows the program to unlock the smartphone; otherwise, the program should not unlock the phone. In the example of worn medical sensor access, the medical sensor is the authenticator, whereas the wireless reader is the authenticatee. Only the reader that has physical contact with the sensor wearer will receive a one-time password to access the data on the sensor. In the less access-critical examples of personalizing smart objects, the wearable token (i.e., the authenticator) transmits the user's identity to the touched smart object (i.e., the valid authenticatee) for personalization.

2.2 Threat Model

We adopt the same threat model that is used for an ECG-based device authentication system in [37]. Specifically, we consider an adversary who fully controls the communication channel between the authenticator and any valid authenticatee and aims at impersonating the valid authenticatee. The channel control includes eavesdropping, dropping, modifying, and forging messages as desired. The adversary can corrupt neither the authenticator nor the valid authenticatee.

2.3 Approach Overview

Fig. 1 illustrates an authentication process of our approach. The authentication process can be initiated by the authenticatee upon it detects a human touch based on iBEP. After a handshake with a nearby authenticator, a Transport Layer Security (TLS) connection is set up between the authenticator and the authenticatee to ensure data confidentiality, integrity, and freshness of consequent communications. TLS is feasible on mote-class platforms [12, 38]. Because the authenticatee's

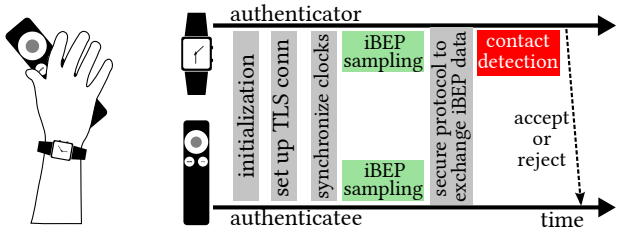


Figure 1: Left: A use scenario where the smart watch personalizes a remote control and the associated media system by a touch; Right: authentication process.

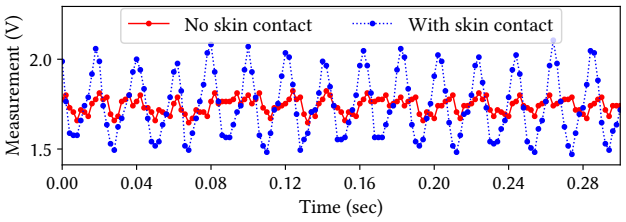


Figure 2: The body antenna effect.

certificate presented during the TLS setup needs not to be validated by the authenticator, our approach does not involve a cumbersome public key infrastructure (PKI). Then, the two parties synchronize their clocks and sample their respective iBEPs $s(t)$ and $s'(t)$ synchronously for ℓ seconds. After that, following an existing protocol H2H [37] that is designed for ECG-based device authentication, the two parties perform a commitment-based data exchange to ensure the security of the system against the threat defined in §2.2. Note that, without using H2H, a naive approach of transmitting $s'(t)$ from the authenticatee to the authenticator over the TLS connection for contact detection is vulnerable to a man-in-the-middle attack based on full channel control [37]. After obtaining $s'(t)$, the authenticator runs a same-body contact detection algorithm with $s(t)$ and $s'(t)$ as inputs to decide whether the authenticatee is valid. Lastly, the authenticator notifies the authenticatee of acceptance or rejection.

Note that in the less security-critical use scenarios such as smart object personalization, the TLS connection setup can be skipped and the commitment-based data exchange procedure can be replaced with a normal data exchange procedure. This reduces overhead.

3 BASIS AND RESEARCH OBJECTIVE

In this section, we discuss the physical basis of TouchAuth (§3.1) and the research objective (§3.2).

3.1 Body Antenna Effect

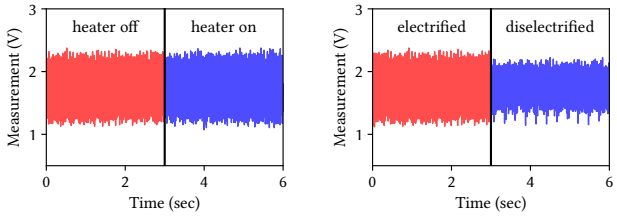
First, we illustrate the body antenna effect. The two curves in Fig. 2 are the measurement traces of a mote-class sensor placed at a fixed position, with an ADC pin floating in the air or pinched by a person, respectively. More details of the sensor will be presented in §4.1. Without body contact, the sensor captures the mains hum with weak amplitude and a frequency of about 50 Hz (i.e., the nominal grid frequency in our region). With body contact, the signal has greater amplitude and exhibits more clearly the frequency of 50 Hz. The above result shows that the human body affects the reception of mains hum. Several recent studies [7, 10, 48] exploited this human body antenna effect for various applications. However, they do not provide an in-depth explanation of the effect. This section explains this effect in detail, which will guide our experiments and the design of TouchAuth.

3.1.1 Electric field (EF) from electrical cabling. A line of charge emits an EF, whereas a current through the line generates a magnetic field. Thus, a charged wire carrying alternating current (ac) will generate both time-varying electric and magnetic fields. However, since the magnetic fields generated from the two close-lying current-carrying wires within a single power cable tend to cancel each other, the overall magnetic field around a power cable is normally very weak [42].[2] At the nominal frequency of the ac power grid, i.e., 50 or 60 Hz, the power cable's EF is an extremely low frequency (ELF) radiation with a wavelength of thousands of miles. At such a wavelength scale, we do not need to consider the magnetic field excited by the time-varying EF. Thus, EF is the main emanation from a power cable.

Modern buildings often have complex electrical cabling. Permanent power cables run above ceilings, below floors, on walls, etc. There are also power extension cords installed by residents. As the EF from a cable is a vector field with intensity attenuating with the distance from the cable, the combined EF caused by all the cables in a building is a vector field with a complex intensity distribution over the space. In normal homes with 220 V power supply, the intensity of the combined EF is often between 3 V/m and 30 V/m [42]. The EF is the superposition of the EFs emitted by surrounding electrified power cables and appliances. Due to the spatial distribution of the power cables and appliances, the gradients of the EF at different locations are generally different.

Note that if an appliance is powered off, the intensity of the EF from the power cable supporting the appliance will remain unchanged. This is due to the fact that most switches only break the connection in one wire, while the wires will still have the same service voltage as when the appliance

[2]The low-intensity net magnetic field due to a small mismatch between the two wires' currents, which is caused by the vagabond currents effect, is sensible using special devices such as hall effect sensors and tank circuits tuned to the power grid frequency.



(a) Heater powered on and off.

(b) Cord (dis)electrified.

Figure 3: Mains hum measured by a sensor (without human body contact) placed close to a power cord supporting a 2 kW heater.

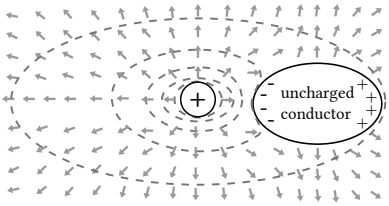


Figure 4: Impact of an uncharged conductor (e.g., human body) on an EF from a point charge. Arrows represent the directions of the electric field; dotted curves represent equipotential lines.

is powered on. We conduct an experiment to verify this. Fig. 3(a) shows the mains hum measured by a sensor that has a conductor wire connected to an ADC pin to improve EF sensing and is placed close to a power cord supporting a 2 kW heater. From the figure, the operating status of the heater does not affect the measurements. Fig. 3(b) shows the sensor's measurements when the heater remains off and the power cord is connected to or disconnected from the wall outlet. We can see that the intensity of the sensor readings is weaker when the power cord is diselectrified. The remaining intensity is caused by the EFs from other electrified power cables in the building. The above results suggest that (i) the ambient field is an EF caused by the ac voltages, (ii) the ac current changes caused by appliances' operating status changes have little impact on the ambient field.

3.1.2 Interactions among EF, sensor, and human body. First, we discuss the situation without a human body. Our discussions below concern a time instant only. As a typical sensor's ADC has high input impedance (hundreds of kΩ up to a few MΩ), the ADC pin and the ground of the sensor can be considered insulated for simplicity of discussion. The ADC and ground will have different potentials in the building's ambient EF due to their physical distance. The potential difference is the measurement of the sensor. For instance, in an EF with an intensity up to 30 V/m, if the equivalent distance between the ADC pin and the ground is 1 cm, the measurement can be up to 0.3 V. This is consistent with our results in Figs. 2 and 3.

Now, we discuss the situation with a human body. A body can be viewed as a conductor due to its low impedance (a few kΩ [35]). From electrostatics, an uncharged conductor in an EF will build up a surface charge distribution to reach an electrostatic equilibrium, where the EF inside the conductor is zero and the conductor's surface is an equipotential surface [34]. The surface charge distribution will generate an EF. As a result, the EF combining that from the original source (i.e., electrical cabling) and the electrostatically induced conductor (i.e., the human body) is different from the EF in the absence of the conductor. In other words, the human body affects its nearby EF. The change of field intensity results in the change of potential difference between the sensor's ADC and ground, i.e., the sensor's measurement.

We use an electrostatics example as shown in Fig. 4 to illustrate the human body's impact on ambient EF. When an uncharged conductor is in the field from a point charge, negative/positive surface charges will be built up. As a result, the EF intensity, which is characterized by the density of the equipotential lines, will change in the space close to the electrostatically induced conductor. For instance, in Fig. 4, the EF between the charge and the conductor is intensified. The reading of a sensor in this area will increase if its ADC and ground are arranged in the direction of the field. In practice, the indoor EF will be much more complex than the one shown in Fig. 4. Nevertheless, the example provides a basic understanding of the body antenna effect.

3.2 Research Objective

As discussed in §3.1.2, the human body in an EF is an equipotential conductor. Considering two sensors with their ADC pins connected to the same human body, the potentials of their ADC pins will be the same. If they are close to each other, their grounds will have similar potentials. Thus, their readings will be similar. If the two sensors are attached to two locations on the human body which are far from each other, their grounds will have different potentials. As a result, though their ADC pins have the same potential due to the human body contact, their readings will be different.

Now, we discuss the case where the two sensors are on different human bodies. The human bodies will most likely have different potentials. Moreover, even if we ignore the impact of the two human bodies on the EF, because the two sensors are at two different locations, the gradients of the indoor EF at the two locations will be most likely different. As a result, the two sensors' measurements will be different. This difference will be further intensified by the different impacts of the two human bodies on their nearby EFs.

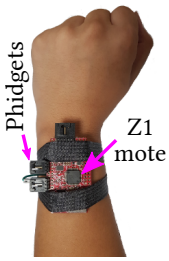


Figure 5: Z1.

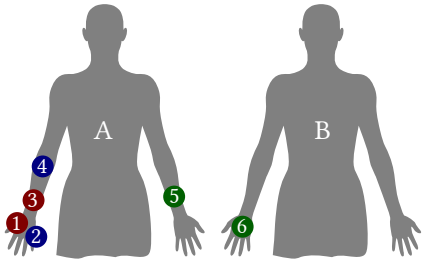
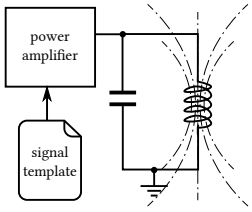


Figure 6: Sensor placements.



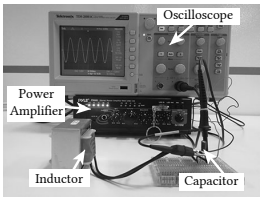


Figure 7: Time-varying magnetic field generator.

Our research objective is two-fold. First, we aim to verify the above inferences from the iBEP electrostatics via an extensive measurement study, which is the subject of §4. If the measurement results are supportive of the inferences, we will inquire whether iBEP sensing can be exploited to implement the desirable touch-to-access scheme. This will be addressed in §5 and §6.

4 MEASUREMENT STUDY

4.1 Measurement Setup

Our experiments are conducted using several Zolertia Z1 motes [53] and a Kmote [20]. Both types of motes are equipped with MSP430 microcontroller and CC2420 802.15.4 radio. The Z1 motes are used to collect iBEP data from human bodies, whereas the Kmote is used as a base station to synchronize the Z1 motes' clocks and collect their iBEP data over wireless. Each Z1 mote is powered by a lithiumion polymer battery; the Kmote base station is connected to a desktop computer through a USB cable. Each Z1 mote has two Phidgets sensor ports connected to several ADC pins of its microcontroller. We use a conductive wire as an electrode to create a physical contact between a pin in one Phidgets sensor port and the skin of the Z1 wearer. Fig. 5 shows a Z1 worn on a wrist. The motes run TinyOS 2.1.2. The program running on the Z1 mote samples the ADC at a rate of 500 sps. The samples are timestamped using the Z1's clock. The program uses a reliable transmission protocol called Packet Link Payer [27] to stream the samples to a Kmote base station. It also integrates the Flooding Time Synchronization Protocol (FTSP) [24] to synchronize the Z1's clock to the Kmote base station.

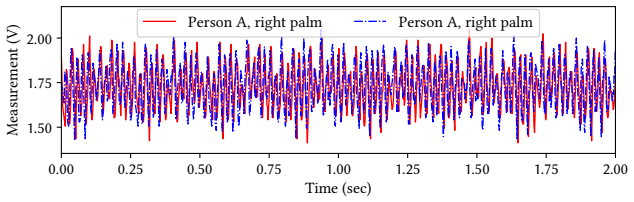
4.2 Measurement Results

We conduct three sets of experiments in a lab office.

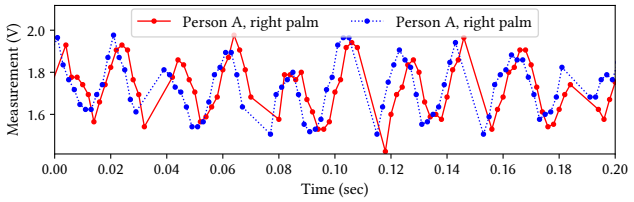
4.2.1 Insensitivity to time-varying magnetic field (MF). To verify that the body antenna effect is mainly caused by EF, rather than MF, we build an MF generator and examine its impact on iBEP sensing. Fig. 7 shows the schematic and the implemented MF generator. It consists of a *power amplifier* that weighs 2.6 kg, a 320 mH inductor, and a 1 μF capacitor. The power amplifier admits a specified signal waveform and outputs the corresponding current to induce the inductor to generate time-varying MF. The capacitor is used to smooth the output signal during the induction. In this experiment, the specified signal is a 85 Hz sinusoid. The choice of this frequency has two reasons: a) As 85 Hz is close to the grid frequency of 50 Hz in our region, the iBEP sensor will have similar signal reception performance as for the 50 Hz signal from powerlines; b) The choice of 85 Hz is also to avoid the harmonics of the grid frequency, i.e., 100 Hz, 150 Hz and so on. We configure the power amplifier to use its maximum gain. From our tests, this generator causes strong interference to nearby tank circuits that can sense MF changes. However, from our experiments, it generates little impact on nearby on-body Z1-based iBEP sensors. From a frequency analysis, the power density of the iBEP signal at 85 Hz is 66 times weaker than that at 50 Hz when the on-body iBEP sensor is only 2 cm away from the inductor. The intensity of the signal at 85 Hz is similar to that of the ambient noise. The reason is that the iBEP sensor (i.e., an ADC with floating ground) is an open circuit, which cannot be induced by the time-varying magnetic field. This result confirms that the body antenna effect is mainly caused by EF.

4.2.2 iBEPs on the same body. First, Person A sits in a chair and uses his right hand palm to hold two Z1 sensors steadily. The ADCs of both sensors have direct contact with the palm skin. In Fig. 6, the nodes numbered ❶ and ❷ illustrate the placement of the two sensors. Fig. 8(a) shows the iBEPs captured by the two sensors over two seconds. Fig. 8(b) shows a zoomed-in view of Fig. 8(a). From the two figures, we can see that the two iBEP signals are synchronous and of the same amplitude level. This shows that, when the two sensors are in proximity on the same human body, their measurements are similar.

Second, we investigate the impact of spatial location on iBEP. As discussed in §3.1, the indoor EF has an intensity distribution over space. Thus, the potential difference between the human body and the ground of the sensor will vary with location. In this experiment, Person A holds a sensor in his palm with skin contact and stands at two spots in the lab. Fig. 9(a) and Fig. 9(b) show the iBEPs at the two spots that are

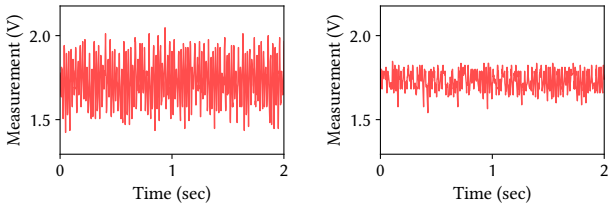


(a) Measurements of two sensors in two seconds.



(b) Zoomed-in view.

Figure 8: iBEPs measured by two sensors in the same palm when the holder sits in a chair.

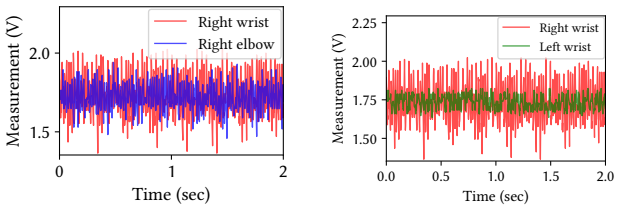


(a) Spot X. (b) Spot Y.

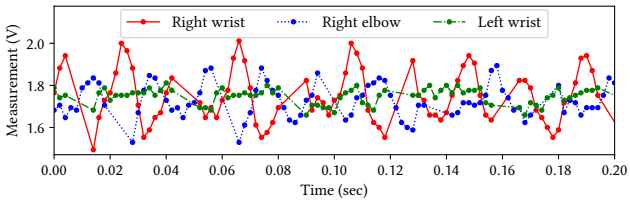
Figure 9: iBEPs measured by a sensor in the same palm when the wearer stands at different spots in the lab.

about one meter apart. From the two figures, the amplitude of the iBEP at Spot X is larger than that at Spot Y. Note that Spot X is closer to a cubicle with a number of electrified power cables and power extensions.

Third, we investigate the impact of the sensor placement on the received iBEP signal. We place three sensors on Person A, two on the right arm and the remaining one on the left arm. The two sensors on the right arm are separated by about 15 cm, one of which is close to the wrist and the other is close to the elbow. In Fig. 6, the nodes numbered ❸, ❹, and ❺ illustrate the placement of the three sensors. In this experiment, the person stands and keeps a side lateral raise posture. Fig. 10 shows the iBEP signals collected from the three sensors in the same time period. Fig. 10(a) shows the iBEPs measured by the two sensors on the right arm. Fig. 10(b) shows the iBEPs measured by two sensors on different arms. Fig. 10(c) shows the zoomed-in view for the signals in Figs. 10(a) and 10(b). From the results, we can see



(a) Two nodes on the right arm. (b) Two nodes on different arms.



(c) Zoomed-in view.

Figure 10: iBEPs at different locations of Person A.

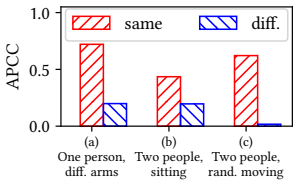


Figure 11: APCC in different placements.

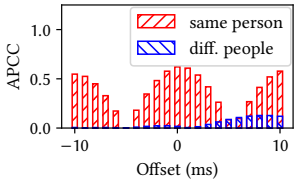
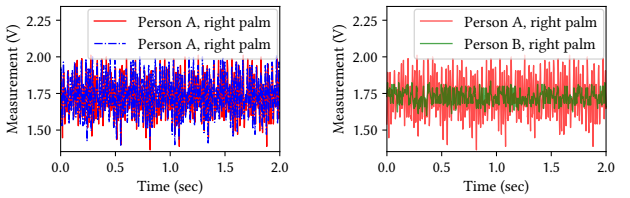


Figure 12: APCC under different clock offsets.

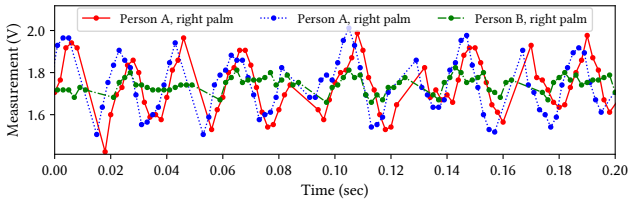
that the signals measured by the two sensors on the right arm have similar amplitudes, but a phase shift of about 180°. This can be caused by that the ADC-to-ground directions of the two sensors in the EF are different. Ignoring the phase shift, the signals measured by the two sensors 15 cm apart on the same arm exhibit higher similarity than those measured by the two sensors on different arms, but lower similarity than those measured by the two sensors in the same palm as shown in Fig. 8(b).

We use the absolute Pearson correlation coefficient (APCC) to quantify the similarity between two iBEP signals. The two bars in the first bar group labeled (a) in Fig. 11 show the APCCs between two iBEP signals collected from the same and different arms on the same person, respectively. The above results suggest that the correlation between the iBEPs is affected by the distance between the sensors. When the two sensors are closer, their iBEPs exhibit higher correlation. This is supportive of our discussion in §3.2.

4.2.3 iBEPs on different bodies. In the first experiment, we place two sensors in the palm of Person A and another sensor

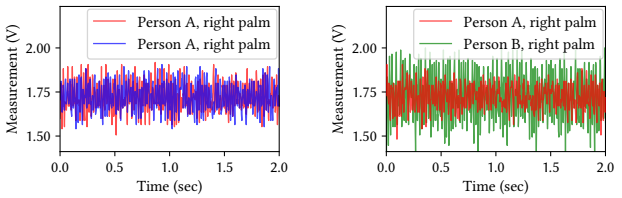


(a) Two nodes in A's right palm. (b) Two nodes on two persons.

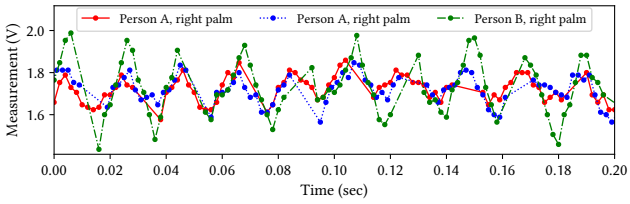


(c) Zoomed-in view.

Figure 13: iBEPs measured by three sensors on two persons who sit steadily 1 m apart.



(a) Two nodes in A's right palm. (b) Two nodes on two persons.



(c) Zoomed-in view.

Figure 14: iBEPs measured by three sensors on two persons who sit 1 m apart and perform random hand movements.

in the palm of Person B. The two persons sit steadily 1 m apart. In Fig. 6, the nodes numbered ❶, ❷, and ❻ illustrate the placement of the three sensors. Fig. 13(a) and Fig. 13(b) show the iBEPs measured by the two sensors in Person A's palm and the two persons' palms, respectively. Fig. 13(c) shows the zoomed-in view. From the results, we can see that the iBEP on Person B is clearly different from that on Person A, in terms of both signal amplitude and waveform. In contrast, the iBEPs on Person A are very similar. The two bars in the second bar group labeled (b) in Fig. 11 show the APCCs for the cases shown in Figs. 13(a) and 13(b). Clearly, the iBEPs from the same body exhibit higher correlation than those from different bodies. This result is supportive of our discussion in §3.2.

In the second experiment, we investigate whether movements will affect the distinctiveness. We ask the two persons to perform some random hand movements. Fig. 14 and the third bar group labeled (c) in Fig. 11 show the results. We can see that, in the presence of movements, the iBEPs from the same body still exhibit higher correlation than those from different bodies.

In the above experiments, the clocks of the sensors are tightly synchronized using FTSP that uses MAC-layer timestamping to achieve microsecond-level synchronization accuracy. Platforms without MAC-layer timestamping can achieve millisecond-level synchronization accuracy [23]. We now assess the impact of a clock synchronization error of up to 10 ms on the APCC. As our collected iBEP signals are tightly synchronized, we simulate the clock synchronization error by offseting an input iBEP signal. Fig. 12 shows the APCC under different simulated clock offsets among the signals in Fig. 14. We can see that, in the presence of clock synchronization error, the APCC for the signals from the same person is generally higher than that for different persons. Moreover, when the synchronization error is around −5 ms or 5 ms, the APCCs are nearly zero. This is because the two signals have a phase difference of 90°, resulting in near-zero correlations. Our earlier study [48] shows that by using iBEP, wearables on the same person or two nearby persons can maintain the synchronization errors below 3 ms. Such synchronization errors will not subvert the APCC as an effective similarity metric.

5 SAME-BODY CONTACT DETECTION

From §4.2, iBEP is promising for touch-to-access device authentication. In this section, we present the design of the same-body contact detection algorithm (§5.1) and discuss a *mimicry attack* that aims at subverting the algorithm (§5.2).

5.1 Detection Algorithm

Before TouchAuth detects the same-body contact, it checks the iBEP signal strength. Specifically, if the standard deviation of either $s(t)$ or $s'(t)$ is below a predefined threshold, TouchAuth rejects the authentication request without performing same-body contact detection. This ensures that the detection is made based on meaningful iBEP signals. From our offline tests, a standard deviation threshold of 0.06 V is a good setting for the Z1 platform. Similar offline tests can be

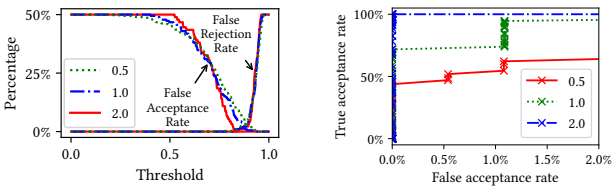
performed for other platforms. In what follows, we present the same-body contact detection algorithm. The detection performance will be evaluated in §6.

5.1.1 Similarity-based detector. The detector compares a similarity score between $s(t)$ and $s'(t)$, $\forall t \in [t_1, t_2]$, with a threshold denoted by η. If the similarity score is larger than η, TouchAuth accepts the authenticatee; otherwise, it rejects the authenticatee. We adopt the reciprocal of the root mean square error (RMSE) and the absolute Pearson correlation coefficient (APCC) as our similarity metrics. The RMSE is a variant of the Euclidean distance which has been used as a dissimilarity metric by physiological sensing approaches [31]. The Pearson correlation coefficient measures the linear correlation between two variables. As shown in Fig. 10, the iBEP signals collected from the same arm have a phase shift of 180°, resulting in a Pearson correlation of about −1. However, the authenticatee on the same arm as the authenticator may be accepted. This motivates us to use the APCC as the similarity metric that ranges from 0 to 1, with 0 and 1 representing the lowest and the highest similarity values, respectively. In the rest of this paper, the TouchAuth based on the RMSE and APCC is called *RMSE-TouchAuth* and *APCC-TouchAuth*, respectively.

Dynamic time warping distance (DTWD) is also a widely adopted dissimilarity metric that can address time-varying phase shift. From our experiments, it may wrongly help the invalid authenticatee who is spatially close to the authenticator. Thus, we do not adopt DTWD.

5.1.2 Assessment metrics. This paper uses the false acceptance rate (FAR or simply α) and the true acceptance rate (TAR or simply β) as the main detection performance metrics. The α and β are the probabilities that an invalid or valid authenticatee is wrongly or correctly accepted, respectively. The detection threshold η and the signal length ℓ are two important parameters. The receiver operating characteristic (ROC) curve of β versus α by varying η depicts fully the performance of a detector under a certain ℓ. The signal length ℓ characterizes the sensing time needed by the authentication process. In this paper, we use the ROC curves to compare the detection performance of various detectors. In practice, the settings of η and ℓ can follow the Neyman-Pearson lemma to enforce an upper bound for α. A stringent α is often required by authentication. For instance, with $\alpha = 1\%$, an invalid authenticatee needs to repeat the authentication process 100 times on average to be successful, which is frustrating if some after-rejection freeze time is enforced. Moreover, an authenticatee device can be banned if it is continuously rejected for many times.

Fig. 15 shows the detection performance of APCC-TouchAuth assessed by using the data shown in Fig. 14. Fig. 15(a) shows the α and the false rejection rate (FRR) versus the detection threshold η when ℓ is 0.5 s, 1 s, and 2 s, respectively. Note that FRR $= 1 - \beta$. Fig. 15(b) shows the ROC curves when α is from 0 to 2%. Note that the α and β values of each point on the ROC are measured based on 500 tests. From the figure, we can see that when $\ell = 2$ s, APCC-TouchAuth achieves a β value of 100% (i.e., correctly accepts all 500 tests when the authenticatee is valid) while keeping $\alpha = 0\%$ (i.e., correctly rejects all 500 tests when the authenticatee is invalid). This suggests that APCC-TouchAuth can achieve a very high detection accuracy. From Fig. 15(b), the ROC curve under a smaller ℓ setting becomes lower, suggesting lower detection accuracy. §6 will extensively evaluate the detection performance of TouchAuth under a wider range of settings among a larger group of users.



(a) FAR & FRR vs. threshold η.

(b) ROC curves.

Figure 15: Detection performance of APCC-TouchAuth when ℓ is 0.5 s, 1 s, and 2 s, respectively.

In addition to the ROC that characterizes detection performance, we also use the *signal-to-difference ratio* (SDR) to assess the quality of iBEP sensing. Specifically, let $P[x(t)]$ denote the average power of a signal $x(t)$. Ideally, if the authenticator and the valid authenticatee are very close to each other on the same human body, their iBEP signals $s(t)$ and $s'(t)$ should be very similar. Thus, we define the SDR in decibel as SDR $= 10 \log_{10} \frac{P[s(t)]}{P[s(t)-s'(t)]}$ dB. A high SDR suggests high-quality iBEP sensing.

5.2 Mimicry Attack

We now discuss a *mimicry attack* that attempts to obtain the authenticator's $s(t)$. Due to the complex spatial distribution of the indoor ambient EF, it is generally difficult for the attacker to estimate the authenticator's $s(t)$. In this attack, the attacker wearing an iBEP sensor mimics the body movements of the victim user wearing the authenticator. To be effective, the mimicry attacker should stay as close as possible to the victim user to sense the same/similar ambient EF. Thus, it is unrealistic in practice, because the strange mimic behavior in proximity can be easily discerned by the user. Note that this attack is beyond the threat model defined in §2.2 that concerns the security of data communications between the authenticator and the authenticatee. Thus, our

approach described in §2.3, which is based on the secure protocol H2H, does not guarantee security against this mimicry attack. In §6, we will show the ineffectiveness of this attack experimentally.

6 EVALUATION

We conduct a set of experiments to evaluate TouchAuth's same-body contact detection performance under a wide range of settings including different wearers, various indoor environments, multiple possible interfering sources, device proximity, skin moisture, and heterogeneous devices.

6.1 Performance across Different Wearers

We collect a set of data involving a wearer $\mathcal{R}$ and 12 other wearers $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_{12}$. The experiments are conducted in a computer science lab. In the ith experiment ($i = 1, \ldots, 12$), $\mathcal{R}$ holds an authenticator device and a valid authenticatee device in his palm, whereas $\mathcal{P}_i$ holds an invalid authenticatee device in his palm. Thus, in this set of experiments, we evaluate the detection performance of TouchAuth for a certain user with a valid authenticatee against different users with invalid authenticatees. In each experiment, $\mathcal{R}$ and $\mathcal{P}_i$, which are about 0.5 m apart, are allowed to perform some uncoordinated and random hand movements. The data collection of each experiment lasts for two minutes. We measure the detection performance of APCC-TouchAuth and RMSE-TouchAuth as follows. Let N_L, or N_I, denote the total number of tests between the authenticator and the valid authenticatee, or between the authenticator and the invalid authenticatee. Accordingly, let N_{TA} and N_{FA} denote the total numbers of true acceptances and false acceptances, respectively. The β and α are measured by N_{TA}/N_L and N_{FA}/N_I, respectively.

Fig. 16 shows the APCC- and RMSE-TouchAuth's ROC curves for different wearers with the invalid authenticatee device when the signal length ℓ is 1 s. Different data points on an ROC represent the results under different detection threshold η. The SDR assessed using the authenticator's and the valid authenticatee's iBEP signals in each experiment is included in the corresponding subfigure. We can see that across different wearers with the invalid authenticatee, APCC-TouchAuth is comparable or superior to RMSE-TouchAuth in terms of the detection performance. This is because that APCC inherently captures the correlation between the iBEP signals on the same moving hand. In contrast, as the RMSE captures sample-wise differences between two signals, two uncorrelated signals with similarly small amplitudes can give a small RMSE value, leading to a false acceptance. Note that the RMSE has been adopted as a dissimilarity metric for physiological sensing [31]. However, it is ill-suited for iBEP sensing because the iBEP signal amplitude has a large

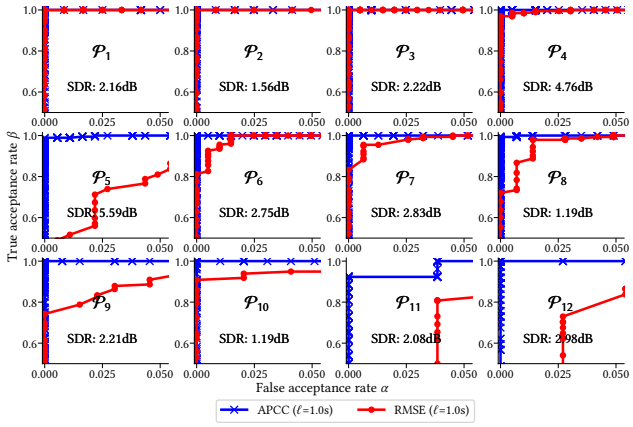


Figure 16: ROCs for 12 different wearers with the invalid authenticatee device. The x-axis and y-axis of each subfigure are α and β, respectively.

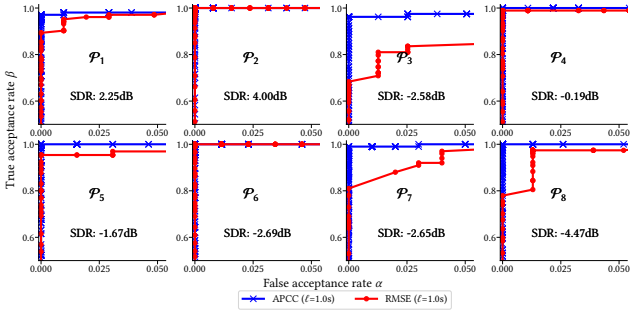


Figure 17: ROCs for 8 different wearers with the valid authenticatee device. The x-axis and y-axis of each subfigure are α and β, respectively.

dynamic range depending on the ambient EF's gradient. This is different from physiological signals that often have stable ranges of signal amplitude. From Fig. 16, we can see that APCC-TouchAuth achieves a high β value (100%) subject to an α upper bound of 1%, except for the wearer $\mathcal{P}_{11}$. For $\mathcal{P}_{11}$, APCC-TouchAuth achieves a β value of 100% subject to an α upper bound of 4%.

We collect another set of data, where $\mathcal{R}$ wears an invalid authenticatee and $\mathcal{P}_i$ holds an authenticator and a valid authenticatee. Thus, this set of experiments evaluate the detection performance of TouchAuth for different users wearing the valid authenticatee against a certain user wearing the invalid authenticatee. Fig. 17 shows the ROCs for eight different wearers with the valid authenticatee. Similar to the results in Fig. 16, APCC-TouchAuth achieves high-profile ROCs and outperforms RMSE-TouchAuth. The results in Figs. 16 and

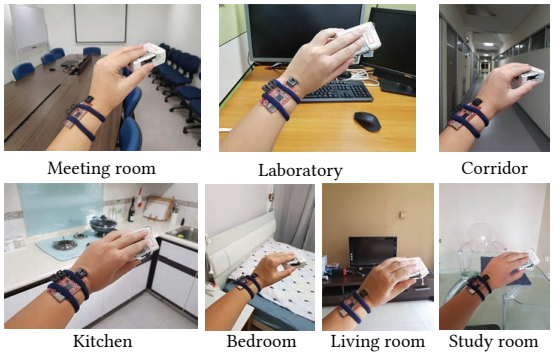


Figure 18: Experiments in indoor environments.

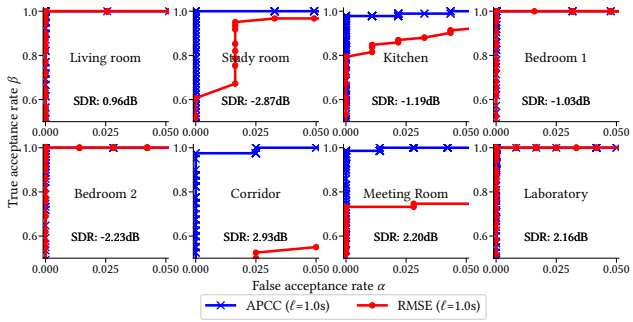


Figure 19: ROCs in various environments.

17 show that the detection performance of TouchAuth is not wearer-specific.

6.2 Various Indoor Environments

Two wearers conduct experiments in eight different indoor environments as shown in Fig. 18, which include a living room, a study room, a kitchen, two bedrooms, a corridor, a meeting room, and an open area of a lab. One wearer carries the authenticator and a valid authenticatee and the other carries the invalid authenticatee. Fig. 19 shows the snapshots of some environments and the measured SDRs and ROCs in the eight environments. We can see that in certain environments, the RMSE-TouchAuth performs poorly. Investigation on the raw iBEP signals shows that in these environments, the iBEP signals of the authenticator and the invalid authenticatee have similar amplitudes. In all the eight environments, APCC-TouchAuth achieves high β values ($\geq$ 97%) subject to an α upper bound of 1%. If the α upper bound is relaxed to 4%, the β value of 100% can be achieved.

6.3 Various Possible Interfering Sources

From our discussion in §3 and the measurement results in §4.2.1, the iBEP measurement is mainly caused by the ambient EF. The MFs generated by the operating currents of electric appliances will have little impact on the iBEP sensing.

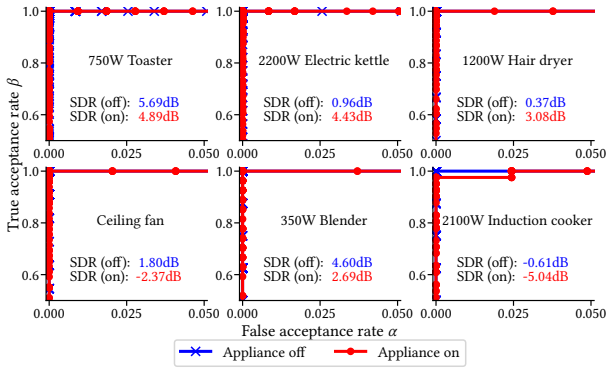


Figure 20: ROCs with various nearby appliances.

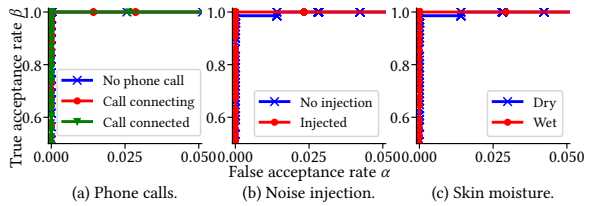


Figure 21: ROCs with interference and skin moisture.

However, some appliances, especially those based on motors and high-frequency switched-mode power, may generate interference to the iBEP sensing. This is because that unlike the 50 Hz current-induced MF that generates little/no EF, the high-frequency currents caused by the frictions between the motor's brush and stator as well as the switched-mode power may generate propagating electromagnetic waves. As a result, the EFs generated by the appliances and powerlines may weaken each other, making the overall EF weaker. Thus, we conduct a set of experiments with various home appliances including toaster, electric kettle, hair dryer, ceiling fan, blender, and induction cooker. Specifically, two wearers, one with a valid authenticatee and the other with an invalid authenticatee, stand close to a certain appliance to collect iBEP traces. Fig. 20 shows the SDR and the APCC-TouchAuth's ROCs for various appliances when the appliance is on and off. We can see that, for a certain appliance, the SDR may increase or decrease when the appliance is switched on. This is because that the interference from the appliance may be constructive or destructive to the EF generated by the building's power cabling. The operating status of the induction cooker causes the largest SDR change of more than 5 dB. This is due to the high-frequency switched-mode current in the cooker's internal inductor. As a result, the ROC drops slightly when the induction cooker is switched on. However, APCC-TouchAuth still achieves a high β value (100%) subject to an α upper bound of 2.5%.

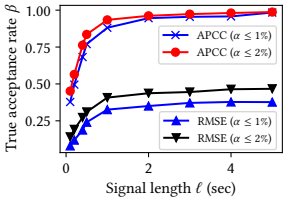


Figure 22: β versus ℓ.

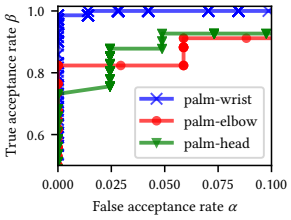


Figure 23: Sensor proximity.

The signaling phase of a cell phone call often interferes with audio systems because of the intermittent wireless power pulses. Thus, we also evaluate the impact of cell phone calls on APCC-TouchAuth. In the experiments, the wearer holds a smartphone, a valid authenticatee, and the authenticator in one palm. Another wearer holding an invalid authenticatee stands 0.5 m away. Fig. 21(a) shows the ROCs at different phases of a phone call. We can see that the phone call does not affect the detection performance of APCC-TouchAuth.

Secondly, we use a circuit seeker (Greenlee CS-8000) that is capable of up to 4 miles circuit tracing [5] to inject noises into the power network serving the lab in which we conduct experiments. The injector of CS-8000 is plugged into a power outlet, injecting a 15 kHz signal into the power network; the seeker can detect the 15 kHz electromagnetic emanation from the powerlines. We conduct experiments in proximity of a powerline close to the injector. Fig. 21(b) shows the ROCs when the injector is in operation or not. We can see that the noise injection does not affect TouchAuth.

Lastly, we evaluate the impact of the skin moisture conditions on TouchAuth. We conduct two experiments, in which the user holds the authenticator using a wet hand. He also holds a valid authenticatee. Another user stands 0.5 m away holding an invalid authenticatee. Fig. 21(c) shows the ROCs for dry and wet skin moisture conditions. We can see that the skin moisture has little impact on the performance of TouchAuth.

6.4 Impact of Signal Length ℓ

We evaluate the impact of the signal length ℓ on the detection performance of TouchAuth. We combine the data collected from 12 different wearers in §6.1 into a single dataset. Based on the combined dataset, Fig. 22 shows the β achieved by APCC-TouchAuth and RMSE-TouchAuth versus ℓ when $\alpha \leq 1\%$ or $\alpha \leq 2\%$. APCC-TouchAuth's β increases sharply when $\ell \leq 1$ s. When $\ell > 1$ s, its β increases with ℓ slowly. This suggests that a setting of $\ell = 1$ s well balances the detection performance and sensing time. The β-ℓ curves for RMSE-TouchAuth exhibits a similar pattern. Moreover, consistent with the results in §6.1 and 6.2, RMSE-TouchAuth is inferior to APCC-TouchAuth.

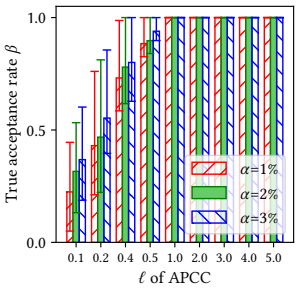


Figure 24: β vs. ℓ under mimicry attack.

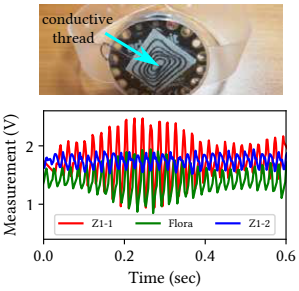


Figure 25: A Flora as the valid authenticatee.

6.5 TouchAuth Devices' Proximity

In the previous subsections, the authenticator and the valid authenticatee are in the same palm. In this set of experiments, they are placed at different locations on the user's body. Fig. 23 shows APCC-TouchAuth's ROC curves. When the two devices are on the palm and the wrist of the same hand, respectively, a high-profile ROC is achieved. When the two devices are on (i) the right palm and the right elbow, respectively, or (ii) the right palm and the head, respectively, the detection performance is degraded. This shows that TouchAuth is applicable to the example use scenarios discussed in §1 where the two devices are in proximity on the same body. In §7, we will further discuss the impact of the proximity requirement on the usability of TouchAuth.

6.6 Mimicry Attack

We follow the data collection methodology described in §6.1 to collect another dataset in the lab, except that each wearer $\mathcal{P}_i$ with the invalid authenticatee mimics the hand movements of the wearer $\mathcal{R}$ with the authenticator and the valid authenticatee. The $\mathcal{R}$ performs simple and repeated hand movements, such that $\mathcal{P}_i$ can follow easily. The distance between $\mathcal{R}$ and $\mathcal{P}_i$ is about 0.5 m. Fig. 24 shows the APCC-TouchAuth's β versus ℓ subject to various α upper bounds. The error bars show the minimum, maximum, and mean of the β values among different $\mathcal{R}$-$\mathcal{P}_i$ pairs in the dataset. Compared with Fig. 22, when ℓ is small (e.g., 0.1 s), the mimicry attack degrades APCC-TouchAuth's detection performance. However, the attack impact can be fully mitigated by adopting a larger ℓ setting (e.g., $\ell = 1$ s).

6.7 Heterogeneous Devices

In this set of experiments, the authenticator and the invalid authenticatee are based on Z1 motes (denoted by Z1-1 and Z1-2); the valid authenticatee is based on an Adafruit's Flora [1], an Arduino-based wearable platform. The top part of Fig. 25 shows a Flora-based TouchAuth prototype device with a 3D-printed insulating wristband and a conductive

thread creating the body contact. We use a laptop computer to relay the communications between the Bluetooth-based Flora and the Zigbee-based Z1. The bottom part of Fig. 25 shows the zoomed-in view of the signals captured by the three devices. We can see that although the Z1 and Flora have different direct current lines, the Z1-1 authenticator and the Flora authenticatee are highly correlated. Based on this setup, with $\ell = 1$ s, APCC-TouchAuth achieves a β value of 100% subject to an α upper bound of 1%. This result shows that TouchAuth can be applied on heterogeneous devices.

7 LIMITATIONS AND DISCUSSIONS

This section discusses limitations and the applicable scope of TouchAuth.

Applicability to outdoors: The outdoor naturally occurring EF is too weak to be exploited by TouchAuth. Thus, TouchAuth is not applicable outdoors, where it will reject all authentication requests due to too weak iBEP signal strength (cf. §5.1). As most smart objects are indoors and we spend most of our time indoors (e.g., 87% on average for Americans [21]), TouchAuth gives a satisfactory availability. Note that the wide availability of the iBEP signals in indoor environments has been shown in existing studies [6–8, 48].

Proximity requirement: From the measurement study in §4 and the evaluation results in §6.5, our approach requires that the authenticator and the authenticatee are in proximity on the same human body. For instance, in the example of personalizing smart objects, the user should use the hand with the wrist wearable to touch the objects. A wireless reader needs to be placed close to a worn medical sensor to be authenticated. We believe that this proximity requirement introduces little overhead of using TouthAuth-based devices. Nevertheless, TouchAuth offers a low cost and small form factor solution based on ubiquitous ADCs only. Although exiting IBC and physiological sensing approaches may not have this proximity requirement, they generally require non-trivial sensing devices that are more costly and of larger form factors. In particular, the proximity requirement increases the barrier for active attackers to steal the iBEP signals, since they have to place a sensor close to the authenticator. In contrast, if the body-area property is effective for the whole body like for ECG/PPG, the attackers may attach a miniature sensor to the clothing of the victim to steal the signal.

iBEP injection attack: If an attacker can generate a strong ac EF that overrides the ambient EF, the attacker can infer the $s(t)$ sensed by the authenticator and spoof it to accept an invalid authenticatee. However, the strong EF generation is non-trivial and inevitably requires bulky equipment. Overriding the power grid voltage is generally impossible unless the building's power network is disconnected from the mains grid and supplied by a power generator controlled by the attacker. Another possible approach is to surround the victim TouchAuth devices with two metal plates connected with an ac generator. The bulky setting of the EF generation renders the attack easily discernible by the TouchAuth user and costly, unattractive to the attacker. Another possible attack is to generate power surges in the power network by frequently switching on and off high-power appliances like space heaters. However, the surges will also generate easily discernible disturbances to other appliances such as lights and audio systems. Thus, we believe that the iBEP injection attack, though possible, is unrealistic or easily discernible.

Other interferences: TouchAuth is based on the instantaneous similarity of the iBEP signals in close proximity induced by the ambient EF. Hence, the similarity does not depend on the user's physiological state. Certain limited scenarios may affect the iBEP. For example, a temporary charging caused by taking off a sweater may override the iBEP in a short time. However, such situations do not happen frequently.

Applicability to implantable medical devices (IMDs): Our measurement study (§4) and evaluation (§6) are based on iBEPs collected from skins. We now discuss the applicability of TouchAuth to devices implanted into human bodies. From our discussion in §3.1, an electrostatically induced human body is an equipotential body. Thus, the ADC pin and the ground of an IMD that is fully implanted into the human body will have the same potential. As a result, the iBEP measurement will be zero. We conducted a set of experiments to verify this. We bought two types of homogeneous meat from a supermarket. We wrapped a Z1 mote using cling film but leaved its ADC-connected electrode out of the wrap. We *fully* and *partially* implanted the mote into the meat. Under both settings, the electrode has significant contact with the meat. The partial implanting means that a small portion of the cling film was still visible. The peak-to-peak amplitudes of the iBEP signals measured by the Z1 mote fully and partially implanted are about 0.05 V and 0.1 V, respectively. The peak-to-peak amplitude of the latter case is comparable to some of our measurement results on human skins (cf. §4). Frequency analysis shows that the former is close to white noise and the latter clearly exhibits a frequency of 50 Hz. These results suggest that TouchAuth is applicable to partially implanted devices, such as insulin pumps, cochlear implants, foot drop implants, etc.

8 RELATED WORK

Device authentication and key generation: Various physiological signals have been exploited for contact-based *device authentication* and *key generation*. Key generation establishes

Table 1: Comparison with existing approaches.

Ref.	Signal	Sensing time (s)	α (%)	β (%)
TouchAuth		**1**	**2.0**	**94.2%**
		5	**2.0**	**98.9%**
[31]	ECG+PPG	~60 (67 IPIs)	2.1	93.5
		~30 (34 IPIs)	4.5	90.5
[41]	PPG	12.8	0.1	99.9
[19]	ECG	~90 (90 IPIs)	~0*	~100*

* [19] fuzzily states that its FAR and FRR are almost zero.

a secret symmetric key for a pair of nodes on the same human body. Using ECG and PPG for the above two tasks has received extensive research. An early work [31] encodes the interpulse intervals (IPIs) of ECG or PPG into a bit sequence and performs authentication by comparing the Hamming distance of two bit sequences with a threshold. The study [46] generates IPI-based symmetric key for an IMD and an external device. PSKA [41] and OPFKA [19] generate keys from certain ECG/PPG features. Rostami et al. [37] quantify ECG's randomness in terms of entropy and design the H2H authentication protocol. However, ECG/PPG sensors often have large form factors due to the required physical distances between electrodes. Moreover, ECG/PPG sensing can be vulnerable to video analytics [30, 45]. Table 1 compares the performance of APCC-TouchAuth (from Fig. 22) and several ECG/PPG device authentication approaches. TouchAuth achieves comparable detection accuracy within shorter sensing times. Recent studies have also exploited EMG [51] and gait [47] for key generation. However, the multi-electrode EMG sensor [51] is sizable and must be placed close to muscles. Walking to generate keys [47] may be inconvenient and the used inertial measurement units (IMUs) may be vulnerable to remote acoustic attack [40].

Human body coupled capacitive sensing: The iBEP sensing belongs to a broader area of capacitive sensing. A recent survey [15] provides a taxonomy of capacitive sensing. We review those on passively sensing the mutual impact between the human body and ambient EF. The iBEP has been used for touch [8] and motion sensing [6], keyboard stroke detection [10], gesture recognition [7], wearables clock synchronization [48]. Several studies use a single off-body electrode to sense the change of ambient EF due to human's electrophysiological signals [33] and body movement [32, 39]. Platypus [14] uses an EF sensor array on the ceiling to localize and identify a human walker. The EF change is due to the triboelectric effect and changes in capacitive coupling between the walker and the environment. Wang et al. [44] use an external sound card as the ADC and three magneto-inductive coil sensors to collect the electromagnetic interference (EMI) radiated from various devices. The signatures contained in the EMI are used for identifying the device the user is touching. Laput et al. [22] attach a modified software-defined radio to the human body for sampling iBEP. When the user touches an object, the class of the object can be recognized based on the sampled iBEP signal. Yang et al. [49] develop a follow-up research of [22] to recognize the identity, rather than the class, of the touched object. However, the needed training phase of [22, 44, 49] introduces overhead.

The human body can be used as a communication channel. Early studies [2, 25, 29, 52] build customized transmitter and receiver for intra-body communication (IBC). Vu et al. [43] design a wearable transmitter to convey identification data to a touchscreen as the receiver. Holz et al. [18] use a wrist wearable and touchscreen to measure bioimpedance and identify the user. Hessar et al. [17] uses fingerprint scanner and touchpad as the transmitter and a software-defined radio attached to skin as the receiver. Yang et al. [50] show that the transmitters can be LEDs, buttons, I/O lines, LCD screens, motors, and power supplies. Roeschlin et al. [36] design an IBC approach that estimates the body channel characteristics to pair on-body devices. Although IBC can be used for contact-based device authentication, it often requires non-trivial transmitter/receiver devices. In contrast, our approach requires a ubiquitous low-speed ADC only.

Other related studies: VAuth [11] uses a wearable token device to sense the vibrations caused by the speech of the wearer and match the vibration signal with the received voice signal. The matched vibration and voice signals are further used to verify that the voice signal received by a voice assistant is really from the token wearer. Nyemkova et al. [28] study the distinguishability of various electronic devices based on the fluctuations of their internal EMI.

9 CONCLUSION

This paper explained the electrostatics of iBEP with supporting measurement results. Based on the understanding, we designed TouchAuth and evaluated its same-body contact detection performance via extensive experiments under a wide range of real-world settings. Results show that TouchAuth achieves comparable detection accuracy as existing physiological sensing approaches, but within much shorter sensing times. Moreover, the uni-electrode iBEP sensor can be miniaturized. TouchAuth offers a low-cost, lightweight, and convenient approach for the authorized users to access the smart objects found in indoor environments.

ACKNOWLEDGMENTS

The authors wish to thank our shepherd Dr. Alanson Sample and the anonymous reviewers for providing valuable feedback on this work. This research was funded by a Start-up Grant at Nanyang Technological University.

REFERENCES

[1] Adafruit. 2018. Adafruit FLORA. Retrieved November 21, 2018 from https://www.adafruit.com/category/92

[2] Heribert Baldus, Steven Corroy, Alberto Fazzi, Karin Klabunde, and Tim Schenk. 2009. Human-centric connectivity enabled by body-coupled communications. *IEEE Communications Magazine* 47, 6 (2009), 172–178.

[3] T Barill. 2003. *An ECG primer*. Nursecom Educational Technologies, Vancouver, BC, Canada, 63–100.

[4] Sang-Yoon Chang, Yih-Chun Hu, Hans Anderson, Ting Fu, and Evelyn YL Huang. 2012. Body Area Network Security: Robust Key Establishment Using Human Body Channel. In *The 3rd USENIX Workshop on Health Security and Privacy (HealthSec '12)*. USENIX, Bellevue, WA, 1–10.

[5] Emerson Electric Co. 2018. Greenlee CS-8000 Circuit Seeker. Retrieved November 21, 2018 from https://www.greenlee.com/catalog/product.aspx?product_id=19199

[6] Gabe Cohn, Sidhant Gupta, Tien-Jui Lee, Dan Morris, Joshua R Smith, Matthew S Reynolds, Desney S Tan, and Shwetak N Patel. 2012. An ultra-low-power human body motion sensor using static electric field sensing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12)*. ACM, Pittsburgh, PA, USA, 99–102.

[7] 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, Austin, TX, USA, 1901–1910.

[8] 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, Vancouver, BC, Canada, 791–800.

[9] Duo. 2018. Using Duo With a Hardware Token - Guide to Two-Factor Authentication · Duo Security. Retrieved November 21, 2018 from https://guide.duo.com/tokens

[10] HM Elfekey and Hany Ayad Bastawrous. 2013. Design and implementation of a new thin cost effective ac hum based touch sensing keyboard. In *IEEE International Conference on Consumer Electronics (ICCE '13)*. IEEE, Las Vegas, NV, USA, 602–605.

[11] Huan Feng, Kassem Fawaz, and Kang G. Shin. 2017. Continuous Authentication for Voice Assistants. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (MobiCom '17)*. ACM, Snowbird, UT, USA, 343–355.

[12] Sepideh Fouladgar, Bastien Mainaud, Khaled Masmoudi, and Hossam Afifi. 2006. Tiny 3-TLS: A trust delegation protocol for wireless sensor networks. In *European Workshop on Security in Ad-hoc and Sensor Networks*. Springer, Hamburg, Germany, 32–42.

[13] Gartner. 2014. Retrieved November 21, 2018 from https://www.gartner.com/newsroom/id/2839717

[14] Tobias Grosse-Puppendahl, Xavier Dellangnol, Christian Hatzfeld, Biying Fu, Mario Kupnik, Arjan Kuijper, Matthias R. Hastall, James Scott, and Marco Gruteser. 2016. Platypus: Indoor Localization and Identification Through Sensing of Electric Potential Changes in Human Bodies. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '16)*. ACM, Singapore, 17–30.

[15] Tobias Grosse-Puppendahl, Christian Holz, Gabe Cohn, Raphael Wimmer, Oskar Bechtold, Steve Hodges, Matthew S Reynolds, and Joshua R Smith. 2017. Finding common ground: A survey of capacitive sensing in human-computer interaction. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, Denver, CO, USA, 3293–3315.

[16] Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. 2008. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In *Proceedings of the 2008 IEEE Symposium on Security and Privacy (SP '08)*. IEEE Computer Society, Oakland, CA, USA, 129–142.

[17] Mehrdad Hessar, Vikram Iyer, and Shyamnath Gollakota. 2016. Enabling On-body Transmissions with Commodity Devices. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '16)*. ACM, Heidelberg, Germany, 1100–1111.

[18] 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, Charlotte, NC, USA, 303–312.

[19] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen. 2013. OPFKA: Secure and efficient Ordered-Physiological-Feature-based key agreement for wireless Body Area Networks. In *The 32th IEEE International Conference on Computer Communications (INFOCOM '13)*. IEEE, Turin, Italy, 2274–2282.

[20] KETI. 2009. Kmote - KETI mote. Retrieved November 21, 2018 from http://tinyos.stanford.edu/tinyos-wiki/index.php/Kmote

[21] NE Klepeis, WC Nelson, WR Ott, JP Robinson, AM Tsang, P Switzer, JV Behar, SC Hern, and WH Engelmann. 2001. The National Human Activity Pattern Survey (NHAPS): a resource for assessing exposure to environmental pollutants. *Journal of Exposure Science and Environmental Epidemiology* 11, 3 (2001), 231.

[22] Gierad Laput, Chouchang Yang, Robert Xiao, Alanson Sample, and Chris Harrison. 2015. EM-Sense: Touch Recognition of Uninstrumented, Electrical and Electromechanical Objects. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology (UIST '15)*. ACM, Charlotte, NC, USA, 157–166.

[23] Zhenjiang Li, Cheng Li, Wenwei Chen, Jingyao Dai, Mo Li, Xiang-Yang Li, and Yunhao Liu. 2012. Clock Calibration Using Fluorescent Lighting. In *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking (Mobicom '12)*. ACM, Istanbul, Turkey, 463–466.

[24] Miklós Maróti, Branislav Kusy, Gyula Simon, and Ákos Lédeczi. 2004. The Flooding Time Synchronization Protocol. In *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys '04)*. ACM, Baltimore, MD, USA, 39–49.

[25] N. Matsushita, S. Tajima, Y. Ayatsuka, and J. Rekimoto. 2000. Wearable key: device for personalizing nearby environment. In *Digest of Papers. Fourth International Symposium on Wearable Computers*. IEEE, Atlanta, GA, USA, 119–126.

[26] Benjamin Mayo. 2018. Face ID deemed too costly to copy, Android makers target in-display fingerprint sensors instead. Retrieved November 21, 2018 from https://9to5mac.com/2018/03/23/face-id-premium-android-fingerprint-sensors/

[27] David Moss and Philip Levis. 2007. Packet Link Layer. Retrieved November 21, 2018 from https://github.com/tinyos/tinyos-main/blob/master/doc/txt/tep127.txt

[28] Elena Nyemkova and Zenoviy Shandra. 2018. Fluctuations of internal electromagnetic fields as the means of electronic device authentication. In *2018 XIV-th International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH)*. IEEE, Lviv, Ukraine, 81–85.

[29] Duck Gun Park, Jin Kyung Kim, Jin Bong Sung, Jung Hwan Hwang, Chang Hee Hyung, and Sung Weon Kang. 2006. TAP: Touch-and-play. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*. ACM, Montréal, Québec, Canada, 677–680.

[30] Ming-Zher Poh, Daniel J McDuff, and Rosalind W Picard. 2010. Non-contact, automated cardiac pulse measurements using video imaging and blind source separation. *Optics Express* 18, 10 (2010), 10762–10774.

[31] Carmen CY Poon, Yuan-Ting Zhang, and Shu-Di Bao. 2006. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine* 44, 4 (2006), 73–81.

[32] H Prance, P Watson, RJ Prance, and ST Beardsmore-Rust. 2012. Position and movement sensing at metre standoff distances using ambient electric field. *Measurement Science and Technology* 23, 11 (2012), 115101.

[33] RJ Prance, ST Beardsmore-Rust, P Watson, CJ Harland, and H Prance. 2008. Remote detection of human electrophysiological signals using electric potential sensors. *Applied Physics Letters* 93, 3 (2008), 033906.

[34] E.M. Purcell and D.J. Morin. 2013. *Electricity and Magnetism* (3 ed.). Cambridge University Press, Cambridge, UK.

[35] J.P. Reilly, H. Antoni, M.A. Chilbert, and J.D. Sweeney. 1998. *Applied Bioelectricity: From Electrical Stimulations to Electropathology.* Springer New York, New York.

[36] Marc Roeschlin, Ivan Martinovic, and Kasper B Rasmussen. 2018. Device Pairing at the Touch of an Electrode. In *Proceedings of 2018 Network and Distributed System Security Symposium (NDSS).* Internet Society, Reston, VA, 1–15.

[37] Masoud Rostami, Ari Juels, and Farinaz Koushanfar. 2013. Heart-to-heart (H2H): authentication for implanted medical devices. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '13).* ACM, Berlin, Germany, 1099–1112.

[38] Corinna Schmitt, Thomas Kothmayr, Wen Hu, and Burkhard Stiller. 2017. *Two-Way Authentication for the Internet-of-Things.* Springer International Publishing, Cham, 27–56.

[39] Kiyoaki Takiguchi, Takayuki Wada, and Shigeki Toyama. 2007. Human body detection that uses electric field by walking. *Journal of Advanced Mechanical Design, Systems, and Manufacturing* 1, 3 (2007), 294–305.

[40] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu. 2017. WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks. In *IEEE European Symposium on Security and Privacy (Oaklawn '17).* IEEE, Paris, France, 3–18.

[41] Krishna K Venkatasubramanian, Ayan Banerjee, and Sandeep Kumar S Gupta. 2010. PSKA: Usable and secure key agreement scheme for body area networks. *IEEE Transactions on Information Technology in Biomedicine* 14, 1 (2010), 60–68.

[42] Arnt I. Vistnes. 2001. Electromagnetic Fields at Home. In *Radiation at Home, Outdoots and in the Workplace*, Dag Brune, Ragnar Hellborg, Bertil R. R. Persson, and Rauno Pääkkönen (Eds.). Scandinavian Science Publisher, Bakkehaugveien 16, NO-0873 OSLO, Norway, Chapter 19, 286–305.

[43] 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, Istanbul, Turkey, 197–208.

[44] Edward J Wang, Tien-jui Lee, Alex Mariakakis, Mayank Goel, Sidhant Gupta, and Shwetak N Patel. 2015. MagnifiSense : Inferring Device Interaction using Wrist - W orn Passive Magneto - Inductive Sensors. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15).* ACM, Osaka, Japan, 15–26.

[45] Hao-Yu Wu, Michael Rubinstein, Eugene Shih, John Guttag, Frédo Durand, and William Freeman. 2012. Eulerian video magnification for revealing subtle changes in the world. *ACM Trans. Graph.* 31, 4 (July 2012), 65:1–65:8.

[46] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li. 2011. IMDGuard: Securing implantable medical devices with the external wearable guardian. In *The 30th IEEE International Conference on Computer Communications (INFOCOM '11).* IEEE, Shanghai, China, 1862–1870.

[47] Weitao Xu, Girish Revadigar, Chengwen Luo, Neil Bergmann, and Wen Hu. 2016. Walkie-talkie: Motion-assisted automatic key generation for secure on-body device communication. In *The 15th International Conference on Information Processing in Sensor Networks (IPSN '16).* IEEE, Vienna, Austria, 1–12.

[48] Zhenyu Yan, Yang Li, Rui Tan, and Jun Huang. 2017. Application-Layer Clock Synchronization for Wearables Using Skin Electric Potentials Induced by Powerline Radiation. In *The 15th ACM Conference on Embedded Networked Sensor Systems (SenSys '17).* ACM, Delft, Netherlands, 10:1–10:14.

[49] Chouchang Yang and Alanson P. Sample. 2016. EM-ID: Tag-less identification of electrical devices via electromagnetic emissions. In *2016 IEEE International Conference on RFID (RFID).* IEEE, Orlando, FL, USA, 1–8.

[50] Chouchang Jack Yang and Alanson P. Sample. 2017. EM-Comm: Touch-based Communication via Modulated Electromagnetic Emissions. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 3, Article 118 (Sept. 2017), 24 pages.

[51] Lin Yang, Wei Wang, and Qian Zhang. 2016. Secret from Muscle: Enabling Secure Pairing with Electromyography. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems (SenSys '16).* ACM, Stanford, CA, USA, 28–41.

[52] Thoams Guthrie Zimmerman. 1995. *Personal area networks (PAN): Near-field intra-body communication.* Ph.D. Dissertation. Massachusetts Institute of Technology.

[53] Zolertia Inc. 2018. Z1 mote. Retrieved November 21, 2018 from https://github.com/Zolertia/Resources/wiki/The-Z1-mote