Touch-to-Access Device Authentication For Indoor Smart Objects

Zhenyu Yan, Qun Song, and Rui Tan, *Senior Member, IEEE*

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 network. 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 the existing approaches including intra-body communication and physiological sensing, TouchAuth is a low-cost, faster, and easy-to-use approach for authorized users to access the smart objects found in indoor environments.

1 Introduction

The indoor environments are increasingly populated with smart objects. Accesses with some of these objects (e.g., obtaining information on them or granting them to access certain external resources) need to be managed. However, such management 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. 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 explicit user actions. 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's 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. The touch-to-access scheme can also enhance the security of various systems. For instance, 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 [1]. In another hospital use case, the nurses can wear a token device and authenticate themselves before operating medical apparatuses. For instance, the pill dispensers can adopt the touch-to-access scheme for medication safety and backtracking.

The essence of the touch-to-access scheme is the detection of whether the wearable token and the smart object have physical contact with the same user's body. Existing studies tackle this same-body contact detection problem by intra-body communication (IBC) [2], [3], [4], [5], [6], [7], [8] and physiological sensing such as electrocardiography (ECG) [9], [10], [11], [12], [13], photoplethysmogram (PPG) [9], [11], [12], and electromyogram (EMG) [14]. IBC requires either non-trivial customized transceivers [2], [3], [4], [5], [8] or a touchscreen as the receiver [6], [7], 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, physiological sensing approaches may have respective limitations. For instance, EMG sensing requires certain physical distances among a sensor's electrodes [14], which enlarge the sensor form factor. The approaches using ECG and PPG signals require long sensing times of more than 10 seconds and up to 90 seconds [9], [11], [12]. The study [15] also pointed out that ECG sensing requires careful sensor placement and may perform poorly in daily life settings.

• *Z. Yan, Q. Song, and R. Tan are with School of Computer Science and Engineering, Nanyang Technological University (NTU), Singapore. Q. Song is also with the Energy Research Institute, Interdisciplinary Graduate School, NTU.*

Manuscript received December 19, 2020; revised April 27, 2021.

Different from IBC and physiological sensing, this paper investigates the feasibility and effectiveness of using *induced body electric potential* (iBEP) due to the *body antenna effect* for touch-to-access device authentication. 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 network 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 [16], touch sensing [17], motion detection [18], gesture recognition [19], and wearables clock synchronization [20]. These studies leverage several characteristics of iBEP, such as signal intensity alteration [16] and periodicity [20], or feed iBEP signals to machine learning algorithms for motion and gesture recognition [17], [18], [19]. Differently, to use iBEP for device authentication, its body-area property needs to be understood.

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 network 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. Our extensive measurements[2] confirm in positive the following two properties. First, the iBEP signals measured by two sensors that are on the same human body and in close proximity 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.

Based on the above two properties, 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 using the absolute Pearson correlation coefficient as the similarity metric. Extensive experiments show that the 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. 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 a metal area or their conductive exteriors. This requires a simple hardware design of the smart object. For instance, the metal area can be placed at the back of a smart watch. 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.

Paper organization: §2 presents the system and threat models, approach overview, and research objective; §3 presents the measurement study; §4, 5, and §6 show TouchAuth's design, resilience, and evaluation, respectively. §7 discusses several issues; §8 reviews related work. §9 concludes the paper.

2 System Overview & Research Objective

2.1 System Model and Threat 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 the $s'(t)$ received from the authenticatee for same-body contact detection. Before the authentication process, TouchAuth applies clock synchronization approach presented in §5 that is resilient to the attacks of delaying synchronization messages. The synchronization approach also uses the iBEP signals captured by the authenticator and authenticatee.

We now discuss the roles of different devices in the scenarios discussed in §1. When the user with a wrist wearable token touches a smart remote control, the wearable token is the authenticator, whereas the smart remote control 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. If the detection result is positive, the wearable token transmits the user's identity to the remote control for personalization. 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.

We adopt the same threat model that is used for an ECG-based device authentication system in [13]. Specifically, we consider an adversary who fully controls the

1. In this paper, "ground" refers to the floating ground of a device.

2. The data collection from volunteers was approved by NTU IRB (reference numbers: IRB-2018-09-051 and IRB-2019-05-001).

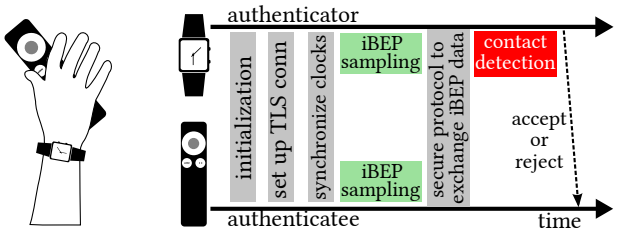


Fig. 1. Left: A use scenario where the smart watch personalizes a remote control and the associated media system by a touch; Right: authentication process.

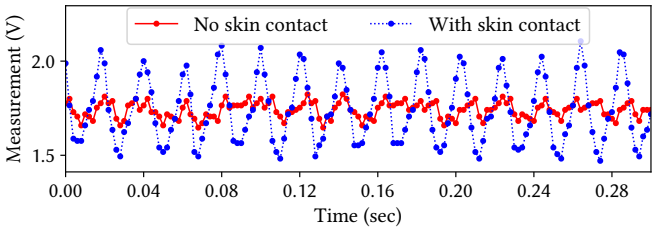


Fig. 2. The body antenna effect.

communication channel between the authenticator and any valid authenticatee and aims at impersonating the valid authenticatee. The channel control includes eavesdropping, dropping, delaying, modifying, and forging messages as desired. The adversary can corrupt neither the authenticator nor the valid authenticatee. Beyond the above adversary model that can be provably addressed by TouchAuth, this paper also evaluates the resilience of TouchAuth against two other attacks, i.e., the mimicry attack in which the adversary tries to approximate $s'(t)$ and the message delay attack in which the adversary tries to subvert the clock synchronization between the two devices.

2.2 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. Because the authenticator does not need to validate the authenticatee's certificate presented during the TLS setup, our approach does not involve a cumbersome public key infrastructure (PKI). Then, the two parties synchronize their clocks using the approach presented in §5 and sample their respective iBEPs $s(t)$ and $s'(t)$ synchronously for ℓ seconds. After that, following an existing protocol H2H [13] 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 §2.1. 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 [13]. After obtaining $s'(t)$, the authenticator runs a same-body contact detection algorithm presented in §4 that uses $s(t)$ and $s'(t)$ as inputs. Lastly, the authenticator notifies the authenticatee of acceptance or rejection.

2.3 Research Objective

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 §3.1. 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. Our prior work [21] explained in detail the generation mechanism of iBEP from the powerline. First, iBEP is mainly induced by electric field (EF) instead of magnetic field; Second, the ADC's reading is the potential difference between the input and ground pin, which capture the potential of the body's surface and the ambient, respectively. From electrostatics, the equipotential human body affects the gradients of its nearby EF. Third, most ADCs can sense the iBEP because the human body impedance is in general within the ranges of the external impedance required by the ADCs.

Based on the above iBEP electrostatics, we have the following inferences. 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.

Our research objective is two-fold. First, we aim to verify the above inferences via an extensive measurement study, which is the subject of §3. 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 §4, §5, and §6.

3 Measurement Study

3.1 Measurement Setup

Our experiments are conducted using several Zolertia Z1 motes [22] and the Kmote [23]. 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

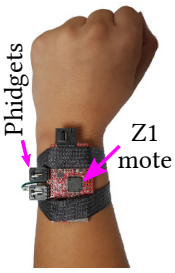


Fig. 3. Z1.

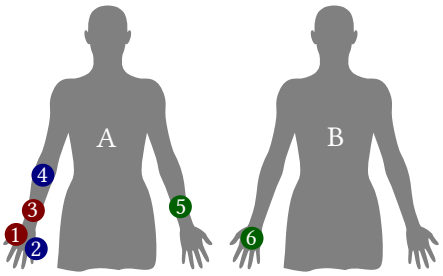
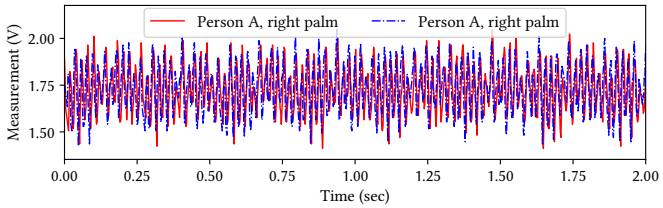
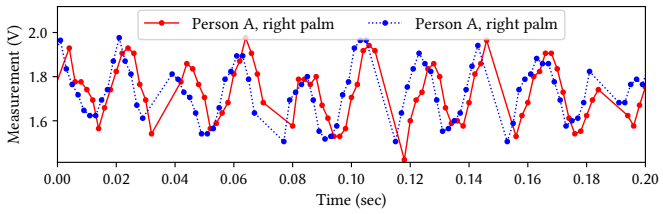


Fig. 4. Sensor placements.

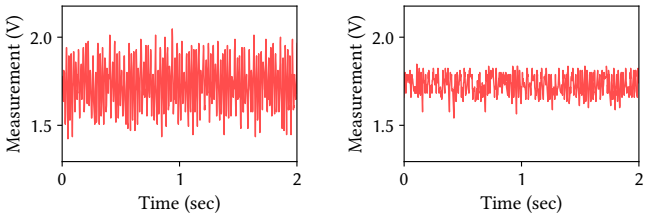


(a) Measurements of two sensors in two seconds.



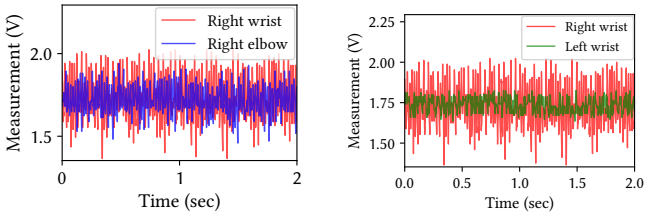
(b) Zoomed-in view.

Fig. 5. iBEPs measured by two sensors in the same palm when the holder sits in a chair.

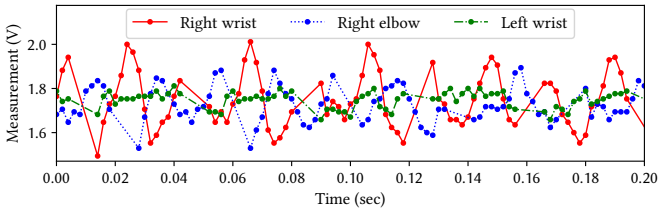


(a) Spot X. (b) Spot Y.

Fig. 6. iBEPs measured by a sensor in the same palm when the wearer stands at different spots in the lab.



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



(c) Zoomed-in view.

Fig. 7. iBEPs at different locations of Person A.

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. 3 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 [24] to stream the samples to a Kmote base station. It also integrates the Flooding Time Synchronization Protocol (FTSP) [25] to synchronize the Z1's clock to the Kmote base station.

3.2 Measurement Results on the Same Body

We conduct experiments in a lab office. 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. 4, the nodes numbered ❶ and ❷ illustrate the placement of the two sensors. Fig. 5a shows the iBEPs captured by the two sensors over two seconds. Fig. 5b shows a zoomed-in view of Fig. 5a. 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 the indoor EF has an intensity distribution over space, 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. 6a and Fig. 6b show the iBEPs at the two spots that are 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. 4, 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. 7 shows the iBEP signals collected from the three sensors in the same time period. Fig. 7a shows the iBEPs measured by the two sensors on the right arm. Fig. 7b shows the iBEPs measured by two sensors on different arms. Fig. 7c shows the zoomed-in view for the signals in Figs. 7a and 7b. From the results, we can see 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,

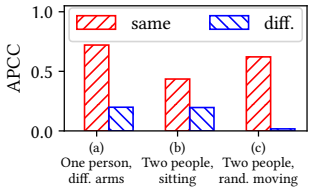


Fig. 8. APCC vs. placement.

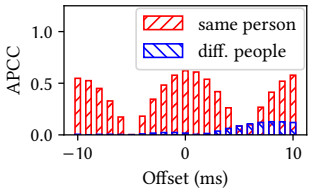
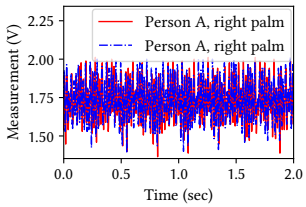
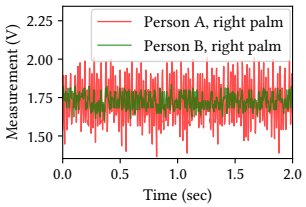


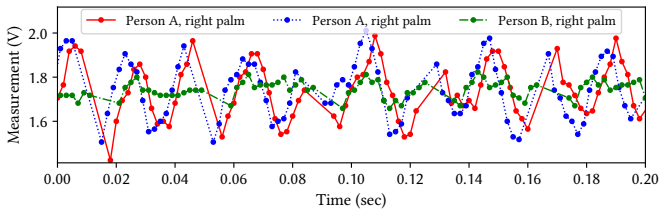
Fig. 9. APCC vs. clock offset.



(a) Two nodes in A's right palm.

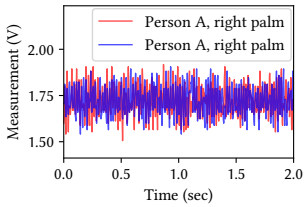


(b) Two nodes on two persons.

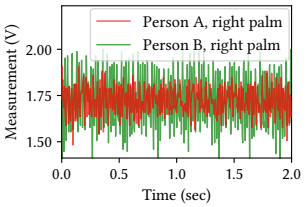


(c) Zoomed-in view.

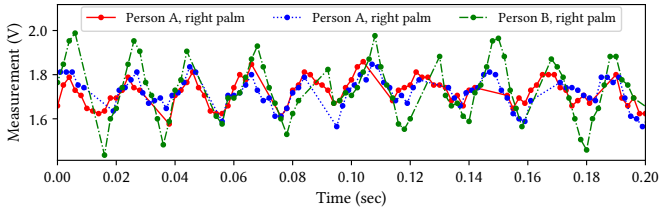
Fig. 10. iBEPs measured by three sensors on two persons who sit steadily 1 m apart.



(a) Two nodes in A's right palm.



(b) Two nodes on two persons.



(c) Zoomed-in view.

Fig. 11. iBEPs measured by three sensors on two persons who sit 1 m apart and perform random hand movements.

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. 5b.

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. 8 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 §2.3.

3.3 Measurement Results on Different Bodies

In the first experiment, we place two sensors in the palm of Person A and another sensor in the palm of Person B. The two persons sit steadily 1 m apart. This 1 m distance is consistent with the typical personal distances during social interactions, i.e., 46 cm to 122 cm [26]. In Fig. 4, the nodes numbered ❶, ❷, and ❻ illustrate the placement of the three sensors. Fig. 10a and Fig. 10b show the iBEPs measured by the two sensors in Person A's palm and the two persons' palms, respectively. Fig. 10c 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. 8 show the APCCs for the cases shown in Figs. 10a and 10b. Clearly, the iBEPs from the same body exhibit higher correlation than those from different bodies. This result is supportive of our discussion in §2.3.

In the second experiment, we investigate whether movements will affect the distinctiveness. We ask the two persons to perform some random hand movements when sitting 1 m apart. Fig. 11 and the third bar group labeled (c) in Fig. 8 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 may have milliseconds clock synchronization errors. 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. 9 shows the APCC under different simulated clock offsets among the signals in Fig. 11. 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. The attack-resilient clock synchronization approach presented in §5 that uses iBEP can maintain the synchronization errors below 3 ms. Such errors will not subvert the APCC as an effective similarity metric.

3.4 Summary

The above measurements show that iBEP signals measured in proximity on the same person show higher APCC similarity than those measured from two persons, regardless of the body movements. Thus, the APCC similarity of two

iBEP signals is promising for determining whether they are collected from the same person in proximity. This key observation drives the design of a same-body contact detection approach, which is presented in the next section.

4 Same-Body Contact Detection

From §3.2, iBEP is promising for touch-to-access device authentication. In this section, we present two same-body contact detection algorithms (§4.1 and §6.6) and discuss a *mimicry attack* that aims at subverting the algorithms (§4.3).

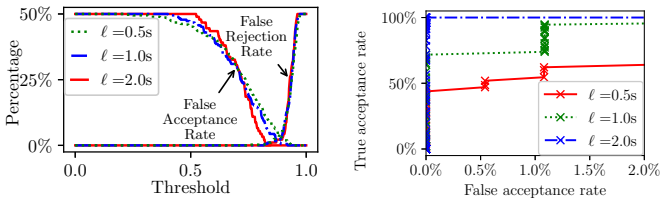
4.1 One-Shot Same-Body Contact Detection Algorithm

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 $0.06\,\text{V}$ is a good setting for the Z1 platform. Similar offline tests can be performed for other platforms. In what follows, we present the one-shot same-body contact detection algorithm. The detection performance will be evaluated in §6.

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 absolute Pearson correlation coefficient (APCC) as our similarity metric. The Pearson correlation coefficient measures the linear correlation between two variables. As shown in Fig. 7, 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 that represent the lowest and the highest similarity values, respectively.

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. 12 shows the detection performance of TouchAuth assessed by using the data shown in Fig. 11. Fig. 12a shows



(a) FAR & FRR vs. threshold η. (b) ROC curves.

Fig. 12. Detection performance of TouchAuth when ℓ is $0.5\,\text{s}$, $1\,\text{s}$, and $2\,\text{s}$, respectively.

the α and the false rejection rate (FRR) versus the detection threshold η when ℓ is $0.5\,\text{s}$, $1\,\text{s}$, and $2\,\text{s}$, respectively. Note that FRR $= 1 - \beta$. Fig. 12b 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 $\ell = 2\,\text{s}$, 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 TouchAuth can achieve a very high detection accuracy. From Fig. 12b, 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.

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 $\text{SDR} = 10\log_{10}\frac{P[s(t)]}{P[s(t)-s'(t)]}$ dB. A high SDR suggests high-quality iBEP sensing.

4.2 Sequential Detection with Early Stopping

This detection approach performs sequential detections based on a series of short signals and yields a positive detection result once sufficient confidence about the same-body contact is achieved. Thus, it may reduce the sensing time compared with the one-shot detection approach presented in §4.1. Specifically, the authenticatee transmits iBEP data to the authenticator in small data blocks. Once a new data block is received by the authenticator, TouchAuth compares the similarity of the two iBEPs from the first data block to the latest data block. When the similarity score is larger than η, TouchAuth accepts the authenticatee, notifies it, and terminates the sequential detection process. Otherwise, when the signal length ℓ reaches a specified maximum signal length ℓ_{max}, TouchAuth rejects the authenticatee. The sequential detector, compared with the one-shot detector that adopts a signal length of ℓ_{max}, can terminate the authentication process early and thus reduce the communication overhead. In §6.6, we evaluate the signal length required by TouchAuth based on the sequential detection approach and its detection performance. We note that this sequential detection approach incurs lower computation overhead compared with the one-shot detector if ℓ_{max} is the same as the signal length used by the one-shot detector.

4.3 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, this attack 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 §2.1 that only concerns the security of data communications between the authenticator and the authenticatee. Thus, our approach described in §2.2, 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.

5 Resilience against Message Delays

As discussed in §2.1, the threat model of TouchAuth assumes that the attacker can fully control the communication channel between the authenticator and the authenticatee. Since TouchAuth requires that the iBEP traces from the authenticator and authenticatee are time-aligned, the attacker may seek to delay the synchronization messages used in the clock synchronization process to introduce synchronization errors. Due to the TLS protection, we assume that the attacker can only delay the transmissions of the messages and cannot tamper with the messages. Note that this message delay attack is feasible in practice and its impact has been studied in [27]. Should the attack successfully introduce clock synchronization errors, a valid authenticatee may be wrongly rejected, forming a denial of service (DoS) effect. This message delay attack remains largely an open issue to clock synchronization protocols based on message passing [28]. In this paper, we study the resilience of a clock synchronization protocol [20] designed based on iBEPs against the message delay attack. Note that the work [20] does not consider the security of the designed protocol. If the protocol is shown resilient to the message delay attack, TouchAuth can adopt it to prevent the DoS effect caused by the attack. This section reviews the iBEP-based clock synchronization protocol. Then, we conduct extensive numeric experiments to investigate the impacts of several attack strategies on TouchAuth. The results show that the message delay attacks can only induce TouchAuth to use longer time for clock synchronization.

5.1 Clock Synchronization Using iBEP Signals

Our measurements in §3 show that iBEP signals exhibit good synchrony since they are induced by the same periodic source. We reuse an approach presented in [20] that exploits this synchrony to synchronize the clocks of the authenticator and authenticatee. In the approach, both devices extract the zero crossing points from their iBEP signals to obtain series of periodic impulses. In a synchronization session shown in Fig. 13, the two devices exchange a `request` packet and a `reply` packet. The packet transmissions and arrivals are

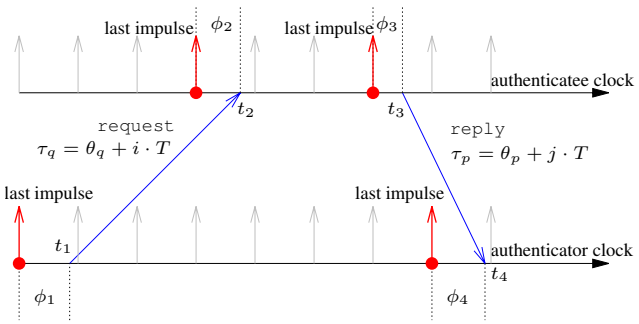


Fig. 13. A clock synchronization session.

timestamped as t_1, t_2, t_3, t_4 using the devices' local clocks. Meanwhile, for each timestamp, each device records the elapsed time from the last impulse (LI) of iBEP signals, which are denoted as ϕ_1, ϕ_2, ϕ_3, ϕ_4, respectively. Then, we compute the *rounded phase differences* θ_q and θ_p of the `request` and `reply` packets:

$$\theta_q = \begin{cases} \phi_2 - \phi_1, & \text{if } \phi_2 \geq \phi_1; \\ \phi_2 - \phi_1 + T, & \text{otherwise.} \end{cases} \quad \theta_p = \begin{cases} \phi_4 - \phi_3, & \text{if } \phi_4 \geq \phi_3; \\ \phi_4 - \phi_3 + T, & \text{otherwise.} \end{cases}$$

Note that T is iBEP's nominal period, i.e., 20ms. When the transmission time is longer than T, the phase difference can be negative and we round the phase difference by adding T. We use two non-negative integers, i.e., i and j, to represent the number of periods elapsed within the fly time of `request` and `reply`. We use τ_q and τ_p to represent the transmission time of `request` and `reply` packet, respectively. Hence, $\tau_q = \theta_q + i \cdot T$ and $\tau_p = \theta_p + j \cdot T$. By definition, the round trip time (RTT) can be measured as $RTT = (t_4 - t_1) - (t_3 - t_2)$. From the above analysis, RTT can be expressed as

$$RTT = \tau_q + \tau_p = \theta_q + \theta_p + (i + j) \cdot T. \quad (1)$$

If the i and j can be determined, the estimated clock offset δ between the two devices' clocks can be computed as $\delta = t_1 - (t_2 - \tau_q) = t_1 - t_2 + \theta_q + i \cdot T$. However, from Eq. (1), we can only determine $i + j$. Thus, Eq. (1) gives a finite number of possible values for δ, which forms a *candidate set*. We perform multiple clock synchronization sessions until the intersection of the resulted candidate sets contains only one candidate value for δ, which is then used to adjust the iBEP timestamps generated by the authenticator for synchronization purpose. We call the above process of reducing the cardinality of the candidate sets intersection as *synchronization convergence*. Once converged, the synchronization accuracy will be in the level of the iBEP's synchrony, which is in general milliseconds.

5.2 Message Delay Attacks

We consider three attack scenarios: the `request` packet is delayed, the `reply` packet is delayed, and both packets are delayed. We assume that the integrity of the packets is not compromised due to cryptographic protection. The attacker aims to prolong the synchronization convergence process or even disable the convergence. If the attacker can precisely control τ_q and τ_p, the attack will disable the convergence.

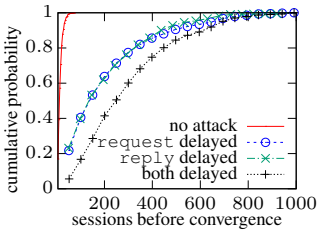


Fig. 14. CDFs of the number of sessions before convergence under message delay attacks.

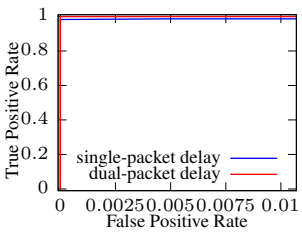


Fig. 15. ROC curves of detecting message delay attacks.

However, as the authenticator and the authenticatee performs timestamping in the application layer, the τ_q and τ_p contain uncertain delays due to operating system overhead and wireless media access control. These uncertain delays are unmeasurable and uncontrollable to the attacker. As a result, it is impossible for the attacker to precisely control τ_q and τ_p. Therefore, a practical attack method is to introduce random delays to τ_q and τ_p.

We conduct numeric experiments to evaluate how the three attack scenarios affect the synchronization convergence speed. We assume the intact τ_q and τ_p are two independent random variables that are uniformly distributed between 0 and 200ms. The message delay also follows uniform distribution from 0 to 200ms. For each attack scenario, we perform 1,000 clock synchronization processes to generate the cumulative distribution function (CDF) of the number of synchronization sessions needed before convergence. Fig. 14 shows CDFs in the absence of attack and in the presence of the three attack scenarios. When there is no attack, most clock synchronization processes can converge within tens of sessions. The average number of synchronization sessions is 14. As each synchronization session takes about 150 ms, the synchronization convergence needs around 2 seconds. When either the `request` or the `reply` packet is delayed, the average number of sessions for convergence is 200 and 191, respectively. The convergence takes about 30 seconds. When both packets are delayed, the average number of sessions is 291. In addition, within 600 synchronization sessions, the synchronization process can converge with a probability of 90%. The convergence time is in the order of one minute. Note that once convergence is achieved, the clock synchronization accuracy will be the same as that in the absence of the attack. The above results show the resilience of the iBEP-based clock synchronization approach against the message delay attacks.

5.3 Detecting Message Delay Attacks and Other DoS Attacks

In this subsection, we present an approach to detect the message delay attacks and other DoS attacks based on the observation that the attacks add extra delays to RTTs. By setting a threshold ρ for RTT, when the measured RTT is longer than ρ, the detector outputs a positive result indicating the existence of attack. If all RTTs are smaller than ρ throughout a synchronization process, the detector outputs a negative result. The threshold value ρ can be set based on the 90th percentile of RTTs in previous clock synchronization sessions that are detected attack-free. To evaluate the performance of our detection approach, we create two sets of data traces corresponding to two attack scenarios, i.e., delay attack on a single packet or both packets. Each set contains 2,000 synchronization processes. For each set of data traces, 1,000 out of 2,000 synchronization processes are subject to delay attacks. Fig. 15 shows the ROC curves of the attack detection, where the points on a curve are obtained by varying the threshold ρ. The blue curve is the ROC when the random malicious delay is added to either `request` packet or `reply` packet. The red curve is the ROC when both packets are subject to malicious random delays. From Fig. 15, the detector can effectively detect the message delay attacks. When both packets are subject to attacks, the detector performs slightly better, because the attacks introduce more delays. Note that when other DoS attacks like jamming occur, the measured RTT will be always larger than ρ. Thus, TouchAuth can detect the attacks. When a DoS attack is detected, TouchAuth can switch to an alternative wireless communication channel. TouchAuth can also rely on the used wireless communication technology's mitigation strategy. For instance, Bluetooth can mark and avoid using bad channels that may be affected by jamming.

6 Evaluation Experiments

We conduct a set of experiments to evaluate TouchAuth's same-body contact detection under a wide range of settings including different wearers, various indoor environments, multiple possible interfering sources, device proximity, skin moisture, and heterogeneous devices. By default, we use the detection algorithm in §4.1.

6.1 Performance across Different Wearers

We collect a set of data traces 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. In addition to the APCC similarity metric introduced in §4.1, we also compute the reciprocal of the root mean square error (RMSE) for comparison. The RMSE is a variant of the Euclidean distance which has been used as a dissimilarity metric by physiological sensing approaches [9]. In the rest of this paper, the TouchAuth based on the RMSE and APCC is called *RMSE-TouchAuth* and *APCC-TouchAuth*, respectively.

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.

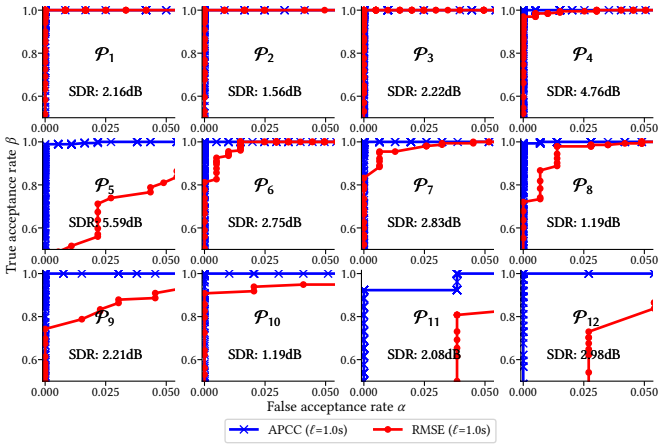


Fig. 16. ROCs for 12 different wearers with the invalid authenticatee device. The x-axis and y-axis of each subfigure are α and β, respectively.

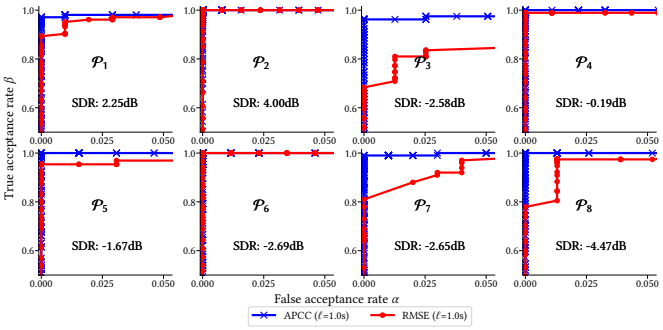


Fig. 17. ROCs for 8 different wearers with the valid authenticatee device. The x-axis and y-axis of each subfigure are α and β, respectively.

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 [9]. However, it is ill-suited for iBEP sensing because the iBEP signal amplitude has a large 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, 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

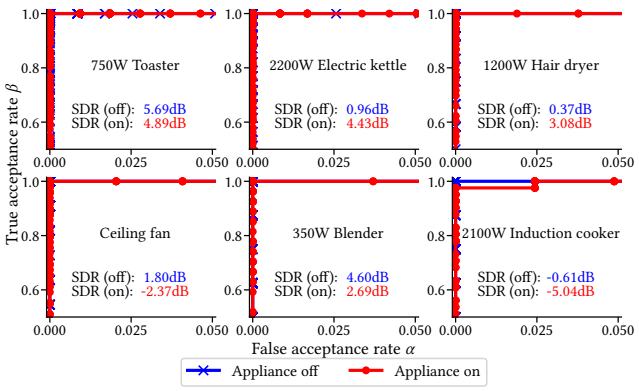


Fig. 18. ROCs with various nearby appliances.

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 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, which include a living room, a study room, a kitchen, two bedrooms, a corridor, a meeting room, and an open area of a lab. Details of the indoor environments can be found in Fig. 1 of Appendix A[3]. One wearer carries the authenticator and a valid authenticatee and the other carries the invalid authenticatee. 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. The measured SDRs and ROCs in the eight environments are shown in Fig. 2 of Appendix A. In conclusion, TouchAuth shows satisfactory performance across eight locations in laboratories and home rooms. Note that TouchAuth may not work when there is no or extremely sparse powerline installation, such as indoor sport halls and warehouses.

6.3 Various Possible Interfering Sources

As discussed in §2, the iBEP measurement is mainly caused by ambient EF. The magnetic fields generated by the operating currents of electric appliances have little impact on the iBEP sensing. 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 magnetic that generates little/no EF, the high-frequency currents caused by the frictions between the motor's brush and stator as well

3. All appendics of this paper can be found in the supplementary file.

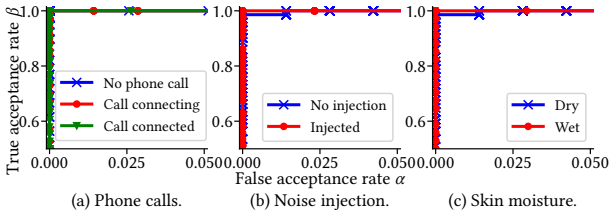


Fig. 19. ROCs with interference and skin moisture.

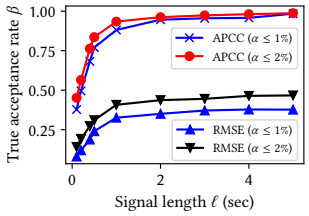


Fig. 20. β versus ℓ.

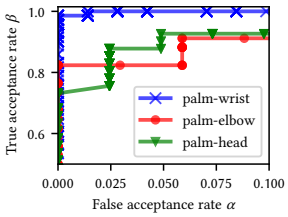


Fig. 21. Sensor proximity.

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. 18 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 network. 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%.

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. 19(a) shows the ROCs at different phases of a phone call. 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 [29] 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. 19(b) shows the ROCs when the injector is in operation or not. 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. 19(c) shows the ROCs for dry and wet skin moisture conditions. The skin moisture has little impact on 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. 20 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 exhibit a similar pattern. Moreover, consistent with the results in §6.1 and §6.2, RMSE-TouchAuth is inferior to APCC-TouchAuth.

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. 21 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. §7 will further discuss the impact of proximity requirement on usability of TouchAuth.

6.6 Performance of Sequential Detection

We evaluate the sequential detection approach presented in §4.2 in terms of ROC and the needed signal length. In this set of experiments, the authenticatee transmits the sensed iBEP signal every 100ms, which is the block size. We vary the maximum signal length ℓ_{max} from 100ms to 5s. Fig. 22 shows the ROC curves of TouchAuth using the one-shot detector ($\ell = 100$ ms or 5 s) and the sequential detector ($\ell_{max} = 5$ s). The ROC curves are generated by varying η from -1 to 1. When $\alpha \leq 2\%$, TouchAuth using the sequential detector achieves $\beta \geq 92.8\%$, which is 20% higher than TouchAuth using the one-shot detector with $\ell = 100$ ms and 7.1% lower than the one-shot detector with $\ell = 5$ s. The error bars in Fig. 23 show the signal lengths used by the TouchAuth with sequential detector under various settings of the maximum signal length ℓ_{max}. The value of η is subjected to $\alpha = 2\%$ for each ℓ_{max} setting. The bars represent the average values. The whiskers represent the 5th and 95th percentiles, respectively. The error bars

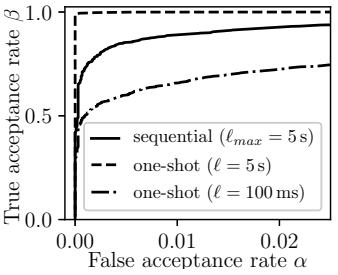


Fig. 22. ROCs of TouchAuth using different detectors.

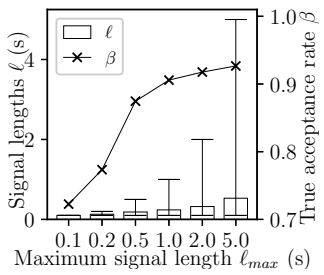


Fig. 23. Signal length ℓ and TAR β of the sequential detector.

show that the ratio of ℓ to ℓ_{max} reduces dramatically as ℓ_{max} increases. When $\ell_{max} = 100$ ms, ℓ is always equal to ℓ_{max}, which is the length of a single data block. When $\ell_{max} = 5$s, the average ℓ is just around 500 ms. The reason is that under most cases, the sequential detector accumulates enough confidence regarding the same-body contact within a few data blocks. The curve in Fig. 23 shows the true acceptance rate β of each ℓ_{max}. When $\ell_{max} = 1$ s, TouchAuth with the sequential detector achieves β larger than 90%. Meanwhile, the sequential detector only requires less than 240 ms on average. The results show that the sequential detector significantly reduces ℓ with a large ℓ_{max}, while preserves a high β. Specifically, when the ℓ_{max} of the sequential detector is identical to ℓ of the one-shot detector, TouchAuth with the sequential detector can reduce the sensing time by almost 10 times. The above results show that with the sequential detector, TouchAuth can output an accurate result within hundreds of milliseconds. Meanwhile, the system has the ability to adapt to the cases that require longer signals for accurate detection.

6.7 Heterogeneous Devices and Mimicry Attack

We deploy TouchAuth on two different hardware platforms, i.e., TinyOS-based Z1 and Arduino-based Adafruit's Flora. The result shows that, with $\ell = 1$ s, APCC-TouchAuth achieves a β value of 100% subject to an α upper bound of 1%. This shows TouchAuth's applicability to heterogeneous devices. The setup photo and results can be found in Appendix B.

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. The result shows that the mimicry attack degrades APCC-TouchAuth's detection performance when ℓ is short. However, the attack impact can be fully mitigated by adopting a larger ℓ setting (e.g., $\ell = 1$ s). Detailed results can be found in Appendix C.

7 Limitations and Discussions

This section discusses limitations of TouchAuth.

Proximity requirement: From the measurement study in §3 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. 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.

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 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 [9] 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 [10] generates IPI-based symmetric key for an IMD and an external device. PSKA [11] and OPFKA [12] generate keys from certain ECG/PPG features. Rostami et al. [13] quantify ECG's randomness in terms of entropy and design the H2H authentication protocol. Table 1 compares the performance of APCC-TouchAuth (from Fig. 20) and several ECG/PPG device authentication approaches. TouchAuth achieves comparable detection accuracy within shorter sensing times. Recent studies have also exploited EMG [14] and gait [30] for key generation. However, the multi-electrode EMG sensor [14] is sizable and must be placed close to muscles. Walking to generate keys [30] may be inconvenient.

Human body coupled capacitive sensing: The iBEP sensing belongs to a broader area of capacitive sensing. A recent

TABLE 1
Comparison with existing approaches.

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

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

survey [31] 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 [17] and motion sensing [18], keyboard stroke detection [16], gesture recognition [19], wearables clock synchronization [20]. Platypus [32] 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. [33] 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. [34] 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. [35] develop a follow-up research of [34] to recognize the identity, rather than the class, of the touched object. However, the needed training phase of [33], [34], [35] introduces overhead.

The human body can be used as a communication channel. Early studies [2], [3], [4], [5] build customized transmitter and receiver for intra-body communication (IBC). Vu et al. [6] design a wearable transmitter to convey identification data to a touchscreen as the receiver. Holz et al. [7] use a wrist wearable and touchscreen to measure bioimpedance and identify the user. Hessar et al. [36] uses fingerprint scanner and touchpad as the transmitter and a software-defined radio attached to skin as the receiver. Yang et al. [37] show that the transmitters can be LEDs, buttons, I/O lines, LCD screens, motors, and power supplies. Roeschlin et al. [8] 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.

9 Conclusion

Based on the iBEP electrostatics, this paper designed TouchAuth and evaluated its same-body contact detection performance 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 also integrates an iBEP-based attack-resilient clock synchronization approach that is a prerequisite of the same-body contact detection. 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 Dr. Yang Li, Dr. Adams Wai Kin Kong, and Dr. Hong Liang Tey for their constructive comments on this work. This research was supported by an MOE AcRF Tier 1 grant (2019-T1-001-044).

References

[1] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *SP '08*.

[2] T. G. Zimmerman, "Personal area networks (pan): Near-field intra-body communication," Ph.D. dissertation, Massachusetts Institute of Technology, 1995.

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

[4] D. G. Park, J. K. Kim, J. B. Sung, J. H. Hwang, C. H. Hyung, and S. W. Kang, "Tap: Touch-and-play," in *CHI '06*.

[5] H. Baldus, S. Corroy, A. Fazzi, K. Klabunde, and T. Schenk, "Human-centric connectivity enabled by body-coupled communications," *IEEE Communications Magazine*, vol. 47, no. 6, 2009.

[6] T. Vu, A. Baid, S. Gao, M. Gruteser, R. Howard, J. Lindqvist, P. Spasojevic, and J. Walling, "Distinguishing users with capacitive touch communication," in *Mobicom '12*.

[7] C. Holz and M. Knaust, "Biometric touch sensing: Seamlessly augmenting each touch with continuous authentication," in *UIST '15*.

[8] M. Roeschlin, I. Martinovic, and K. B. Rasmussen, in *NDSS '18*, Reston, VA.

[9] C. C. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Communications Magazine*, vol. 44, no. 4, 2006.

[10] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *INFOCOM '11*.

[11] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Pska: Usable and secure key agreement scheme for body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 1, 2010.

[12] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, "Opfka: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in *INFOCOM '13*.

[13] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (h2h): authentication for implanted medical devices," in *CCS '13*.

[14] L. Yang, W. Wang, and Q. Zhang, "Secret from muscle: Enabling secure pairing with electromyography," in *SenSys '16*.

[15] S.-Y. Chang, Y.-C. Hu, H. Anderson, T. Fu, and E. Y. Huang, "Body area network security: Robust key establishment using human body channel," in *HealthSec '12*.

[16] H. Elfekey and H. A. Bastawrous, "Design and implementation of a new thin cost effective ac hum based touch sensing keyboard," in *ICCE '13*.

[17] G. Cohn, D. Morris, S. Patel, and D. Tan, "Your noise is my command: sensing gestures using the body as an antenna," in *CHI '11*.

[18] G. Cohn, S. Gupta, T.-J. Lee, D. Morris, J. R. Smith, M. S. Reynolds, D. S. Tan, and S. N. Patel, "An ultra-low-power human body motion sensor using static electric field sensing," in *UbiComp '12*.

[19] G. Cohn, D. Morris, S. Patel, and D. Tan, "Humantenna: using the body as an antenna for real-time whole-body interaction," in *CHI '12*.

[20] Z. Yan, R. Tan, Y. Li, and J. Huang, "Wearables clock synchronization using skin electric potentials," *IEEE Transactions on Mobile Computing*, no. 12, 2019.

[21] Z. Yan, Q. Song, R. Tan, Y. Li, and A. W. K. Kong, "Towards touch-to-access device authentication using induced body electric potentials," in *MobiCom '19*.
[22] Zolertia Inc. (2018) Z1 mote. [Online]. Available: https://github.com/Zolertia/Resources/wiki/The-Z1-mote
[23] KETI. (2009) Kmote - KETI mote. [Online]. Available: http://tinyos.stanford.edu/tinyos-wiki/index.php/Kmote
[24] D. Moss and P. Levis. (2007) Packet link layer. [Online]. Available: https://github.com/tinyos/tinyos-main/blob/master/doc/txt/tep127.txt
[25] M. Maróti, B. Kusy, G. Simon, and A. Lédeczi, "The flooding time synchronization protocol," in *SenSys '04*.
[26] E. T. Hall, "The hidden dimension. anchor books," *Garden City, NY*, pp. 119–120, 1966.
[27] S. Ganeriwal, C. Pöpper, S. Čapkun, and M. B. Srivastava, "Secure time synchronization in sensor networks," *ACM Transactions on Information and System Security*, vol. 11, no. 4, 2008.
[28] M. Ullmann and M. Vögeler, "Delay attacks—implication on ntp and ptp time synchronization," in *ISPCS '09*.
[29] E. E. Co. (2018) Greenlee CS-8000 circuit seeker. [Online]. Available: https://www.greenlee.com/catalog/product.aspx?product_id=19199
[30] W. Xu, G. Revadigar, C. Luo, N. Bergmann, and W. Hu, "Walkie-talkie: Motion-assisted automatic key generation for secure on-body device communication," in *IPSN '16*.
[31] T. Grosse-Puppendahl, C. Holz, G. Cohn, R. Wimmer, O. Bechtold, S. Hodges, M. S. Reynolds, and J. R. Smith, "Finding common ground: A survey of capacitive sensing in human-computer interaction," in *CHI '17*.
[32] T. Grosse-Puppendahl, X. Dellangnol, C. Hatzfeld, B. Fu, M. Kupnik, A. Kuijper, M. R. Hastall, J. Scott, and M. Gruteser, "Platypus: Indoor localization and identification through sensing of electric potential changes in human bodies," in *MobiSys '16*.
[33] E. J. Wang, T.-j. Lee, A. Mariakakis, M. Goel, S. Gupta, and S. N. Patel, "MagnifiSense : Inferring Device Interaction using Wrist - W orn Passive Magneto - Inductive Sensors," in *UbiComp '15*.
[34] G. Laput, C. Yang, R. Xiao, A. Sample, and C. Harrison, "Em-sense: Touch recognition of uninstrumented, electrical and electromechanical objects," in *UIST '15*.
[35] C. Yang and A. P. Sample, "Em-id: Tag-less identification of electrical devices via electromagnetic emissions," in *RFID '16*.
[36] M. Hessar, V. Iyer, and S. Gollakota, "Enabling on-body transmissions with commodity devices," in *UbiComp '16*.
[37] C. J. Yang and A. P. Sample, "Em-comm: Touch-based communication via modulated electromagnetic emissions," *IWMUT*, vol. 1, no. 3, Sep. 2017.

Zhenyu Yan is a Research Fellow at Singtel Cognitive and Artificial Intelligence Lab for Enterprises, Nanyang Technological University, Singapore. He received his Ph.D. degree (2020) from Nanyang Technological University, Singapore, and his B.S. degree (2016) from University of Electronic Science and Technology of China. His research interests include the resilience of Artificial Intelligence of Things (AIoT) systems, mobile computing, and sensor networks. He is the recipient of IPSN'21 Best Artifact Award Runner-Up.

Qun Song received B.S. (2018) in Computer Science from Nankai University. Currently, she is a Ph.D. candidate at the Energy Research Institute and the School of Computer Science and Engineering, Nanyang Technological University. Her ongoing research focuses on constructing secure and efficient machine learning systems for edge devices and autonomous systems. She is the recipient of IPSN'21 Best Artifact Award Runner-Up.

Rui Tan (M'08-SM'18) is an Associate Professor at School of Computer Science and Engineering, Nanyang Technological University, Singapore. Previously, he was a Research Scientist (2012-2015) and a Senior Research Scientist (2015) at Advanced Digital Sciences Center, a Singapore-based research center of University of Illinois at Urbana-Champaign, and a postdoctoral Research Associate (2010-2012) at Michigan State University. He received the Ph.D. (2010) degree in computer science from City University of Hong Kong, the B.S. (2004) and M.S. (2007) degrees from Shanghai Jiao Tong University. His research interests include cyber-physical systems, sensor networks, and pervasive computing systems. He is the recipient of IPSN'21 Best Artifact Award Runner-Up, IPSN'17 and CPSR-SG'17 Best Paper Awards, IPSN'14 Best Paper Award Runner-Up, PerCom'13 Mark Weiser Best Paper Award Finalist, and CityU Outstanding Academic Performance Award. He is currently serving as an Associate Editor of the ACM Transactions on Sensor Networks. He also serves frequently on the technical program committees (TPCs) of various international conferences related to his research areas, such as SenSys, IPSN, and IoTDI. He received the Distinguished TPC Member recognition twice from INFOCOM in 2017 and 2020.