Harnessing the Ambient Radio Frequency Noise for Wearable Device Pairing

Wenqiang Jin
wenqiang.jin@mavs.uta.edu
The University of Texas at Arlington

Ming Li
ming.li@uta.edu
The University of Texas at Arlington

Srinivasan Murali
srinivasan.murali@mavs.uta.edu
The University of Texas at Arlington

Linke Guo
linkeg@clemson.edu
Clemson University

ABSTRACT

Wearable devices that capture user's rich information regarding their health conditions and daily activities have unmet pairing needs. Today's solutions, which primarily rely on human involvement, are cumbersome, error-prone, and do not scale well. Despite some prior efforts trying to fill this gap, they either rely on some sophisticated sensors, such as electromyogram (EMG) or electrocardiogram (ECG) pads that may not universally exist, or non-trivial design of communication transceivers that cannot be found easily on current commercial devices. Therefore, a pairing scheme for wearable devices that is secure, practical, and convenient is in dire need. In this paper, we propose a novel approach that leverages ambient radio frequency (RF) noise. Our design is based on a key observation that received RF noise power measured in the logarithmic scale at different parts of a human body surface experience the same variation trend, whereas those from different human bodies or off the body are distinct. Wearables make use of the observed noise as the entropy source for the proposed pairing protocol. Extensive experiments show that our scheme has an equal error rate (EER) as low as 1.4% for pairing. Its key generation rate reaches 138 bits/sec, which beats so-far existing pairing schemes. Besides, our scheme can be efficiently executed within 0.97 s. Its incurred energy consumption is as low as 0.27 J for the entire pairing procedure.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**.

KEYWORDS

Wearable device pairing; radio frequency noise; body-as-a-conductor

ACM Reference Format:
Wenqiang Jin, Ming Li, Srinivasan Murali, and Linke Guo. 2020. Harnessing the Ambient Radio Frequency Noise for Wearable Device Pairing. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20), November 9–13, 2020, Virtual Event, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3372297.3417288

CCS '20, November 9–13, 2020, Virtual Event, USA

ACM ISBN 978-1-4503-7089-9/20/11…$15.00
https://doi.org/10.1145/3372297.3417288

1 INTRODUCTION

Recently, we are witnessing a remarkable growth in the number of smart wearable devices. According to recent market reports [17], it is forecasted that the yearly shipment of wearable devices will reach 279 million in the year 2023. Moreover, the wearable technology market is expected to reach a value of $58 billion by 2022, which is almost three times of that in 2015 ($19 billion) [44]. With the high penetration to people's daily life, smart wearable devices (e.g., wrist bands, earbuds, heartbeat meters, and step counter) have been gradually recognized as a compelling paradigm for e-healthcare and fitness applications. Sensitive information such as health conditions and physiological data are shared among wearables or synchronized from wearables to personal hubs [42]. Audio streaming is carried between earbuds and a smartwatch for better living and exercising experience [3, 22]. Securing their wireless communications is of critical importance to the wide deployment of wearable devices. In particular, newly deployed wearables must be able to securely associate and establish cryptographic key pairs with existing devices, also known as pairing, in a way that protects against man-in-the-middle (MitM) and protocol manipulation attacks. For devices on the Internet, pairing can be achieved by relying on certificate authorities to certify the device identities, providing a root of trust when establishing the identity of a communicating party. Unfortunately, many wearables lack direct Internet accesses. Instead, they often use short-range radio technology (e.g., Bluetooth or Zigbee) as their first hop to connect to other existing wearables or personal hubs that are to pair. Conventional solutions typically rely on a human to certify the device validity when pairing, for example, by visually comparing short strings on a screen, or by typing a number displayed by one device into the other. These pairing protocols are cumbersome, error-prone, and do not scale well. More importantly, many wearables do not have a user interface, rendering password entry or management extremely challenging.

Efforts to reduce human involvement from the wearable device pairing process have brought the emergence of the idea *touch-to-access* [11, 45, 46, 54, 56, 59]. Two devices are allowed to be paired if and only if they are attached to the same human body at the same time. The rationale behind this idea is that if a wearable has direct physical contact with the human body, it is deemed as a legitimate device validated by the wearer. Under this policy, some existing schemes utilize dedicated sensors to extract physiological signals from the human body, such as ECG [46], EMG signals [59], and body movements [11, 54], and translate them to common randomness, forming the basis of a symmetric key agreement protocol.

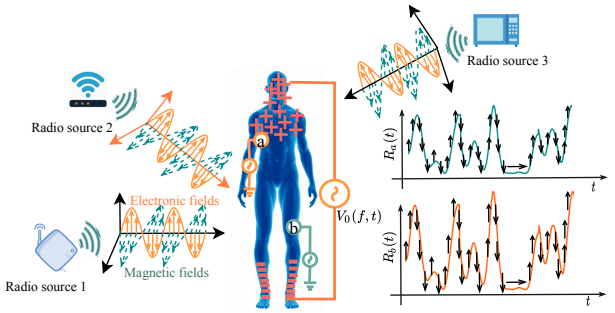


Figure 1: Physical basis of our design.

These approaches are based on the principle that the physiological signals captured from the same human body have similar features, whereas those collected from different human bodies are distinct. Apparently, their success relies on a common, properly calibrated sensing capability across all devices. In contrast, a wide diversity of sensing capabilities are present in commercial wearables; it is impractical to assume arbitrary two wearables equip with a common sensor.

In this work, we aim to develop an automatic pairing scheme for wearable devices without user involvement. Our design follows the touch-to-access policy. Rather than relying on any dedicated sensors, we propose to utilize the RF transceiver, one of the basic electronic components of wearables that are capable of data synchronization/transmission. For devices without this capacity, i.e., stand-alone wearables, there is no need of pairing. Ambient radio frequency (RF) noise is captured from open air and turned into ingredients for secure pairing. RF noise is mainly a combination of natural electromagnetic atmospheric noise and manmade radio interference. Typical sources include lightning discharges, FM/AM radio stations, power systems, a wide variety of electronic equipment, and wireless transmissions. Due to the source diversity and the electromagnetic disturbance originating in a large number of discrete distances with unpredictable occurrences in time and amplitude, RF noise is highly random and unpredictable in temporal, frequential, and spatial domains. Thus, RF noise could be an ideal entropy source for key generation during pairing. Additionally, as RF noise is ubiquitously present, such a source is easily accessible almost everywhere.

Despite these promising features of RF noise, utilizing them for device pairing still faces a significant challenge. Essentially, under the touch-to-access policy, wearables on the same human body should be capable of extracting the same secret, even when they are separately mounted, say one on the wearer's wrist and the other on the chest. Such requirement, however, is primarily hindered by the noise dynamics exhibited in the spatial domain. As pointed out by Xi et al. [53], RF signals received at two locations are independent when they are more than half of the wavelength apart (6.25 cm@2.4 GHz). Thus, how to harvest correlated noise readings from open space at two remotely positioned wearables resides at the heart of our design.

This work is based on a key observation that RF noise, measured in logarithmic scale, experiences the same variation trend even at different parts of a human body surface (as shown in Figure 1). From the perspective of electrostatics, the human body can be viewed as a low-impedance conductor. Thus, placing an induced human body in electromagnetic fields will build up a charge distribution over the body surface to reach an electrostatic equilibrium [41]. As a result, an electrical potential is formed between an arbitrary part of a human body and the ground. Since radiation waves generate time-variant electromagnetic fields, the body surface electrostatic equilibrium distribution varies accordingly, so does the induced on-body potentials. Then, by creating physical contact between the wearable transceiver and the human body, the former can readily access RF noise, reflected as instant variant potentials, captured by the latter from open air. Besides, due to the above-mentioned phenomenon that variations of RF noise readings from the same body surface are highly synchronous, RF noise can be transformed into a common entropy source for key generation.

In practice, due to the uneven charge distribution over the skin surface, variation tendencies of RF noise measures at different parts of the body surface may not be perfectly the same. Directly applying them for device pairing would result in a high error rate. To address this issue, our scheme adopts the framework of *fuzzy commitment* [13, 25, 39]. It is able to correct at most t mismatched bits during paring, with t a tunable parameter that balances between security and usability.

To evaluate the proposed paring scheme, we build a prototype based on a CC2500 transceiver [21] and Arduino board [19]. Extensive experiments show that our scheme has an equal error rate (EER) as low as 1.4%. Its key generation rate reaches 138 bits/sec, which beats so-far existing pairing schemes. Tests also show that our scheme is robust against various attacks such as imitation attacks, MitM attacks, and synthesis attacks. Besides, our scheme can be efficiently executed within 0.97 s. Its incurred energy consumption is also negligible, as low as 0.27 J for the entire pairing procedure. We summarize the contributions of this paper as follows.

- While most of the previous studies focus on avoiding RF noise to improve the performance of wireless communication systems, we propose a novel and practical wearable device pairing scheme by harnessing ubiquitously present RF noise.
- We show analytically and experimentally that the log-scale RF noise measures at different parts of body surface experience the same variation tendency, which serves as the basis for our pairing scheme.
- We develop a prototype and perform extensive experiments to evaluate the security and usability of our scheme. It outperforms the state-of-art solutions in terms of key generation rate, time consumption, and energy cost.

2 SYSTEM OVERVIEW

2.1 Problem Definition

We consider two wearables, Alice and Bob, who intend to establish a secure channel over a publicly accessible wireless media without any pre-shared secret. We focus on the problem of pairing between them. First of all, pairing must be established only between intended peers, i.e., wearables owned/admitted by the same user, which is referred to as *secure association*. Second, a secure symmetric key pair needs to be established between Alice and Bob that facilitates their secure communications in a later stage. Our discussion pertains to wearables attached to the body surface. The pairing for implantable devices is not covered in this work.

Our design follows the *de facto* paring policy for wearables, "touch-to-access" [11, 45, 46, 54, 56, 59]: A new wearable device is admitted to the system if and only if it has significant physical contact with the wearer's body. An important facet of touch-to-access is forward security. The authenticity to the system vanishes once the device loses physical contact with the wearer.

2.2 Threat Model

The goal of an adversary is to deceive the system as a legitimate device that is attached to the wearer's body. An adversary is assumed to be present during a pairing session. It is powerful in a sense to control the channel via, for example, eavesdropping and replaying signals through public wireless channels. It is also possible to forge MAC addresses to falsely claim as a valid device. In particular, we mainly consider the following three kinds of attacks that are severe to our scenarios.

Imitation attack. The adversary exploits physical co-presence with the wearer and tries to obtain similar RF measurements and thus extract the same secret keys as legitimate on-body devices. Depending on where the attacking device is placed, we further classify it into two types. It is called type-I attack if placed in free space, say on a desk, a floor, a stand, etc. It is called type-II attack, if attached to another wearer.

Synthesis attack. More advanced than simply generating random bit sequence, the adversary is able to observe and model the radio environment around the wearer in advance. Then it fabricates synthetic signals and tries to extract from them the same secret keys as legitimate devices.

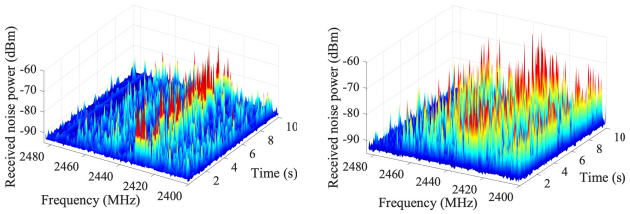
MitM attack. The adversary tries to actively participate in pairing phases of two wearables. Its goal is to either get paired with a learned key or mess the pairing procedure by tampering the exchanged messages but still make one/both of them believe the pairing protocol has completed successfully. The adversary can relay and alter messages on the wireless channel.

We assume that the adversary cannot compromise the end devices; otherwise, it renders the secure pairing impossible. Besides, the scenarios that it seeks to jam the wireless channels or by any other means of destroying communications such as Denial-of-Service (DoS) attacks are out of the scope of this work.

3 BACKGROUND AND ANALYTIC STUDY

3.1 Ambient Radio Frequency Noise

Ambient RF noise is mainly a combination of natural electromagnetic atmospheric noise and manmade radio frequency interference. Typical sources include lightning discharges, FM/AM radio stations, automobile ignition systems, power systems, and a wide variety of electronic equipment such as computers, personal devices and microwave ovens. Due to the source diversity and the electromagnetic disturbance originating in a large number of discrete distances with unpredictable occurrences in time and amplitude, RF noise is highly random in temporal, frequnencial, and spatial domains, which is desirable as an entropy source. We did some prior study to show the distribution of RF noise in these three domains. Figure 2 plots the received noise by two CC2500 transceivers [21] over 2.4 GHz. The data are collected over the same time duration at two different locations separated by 10 cm. Since existing wearables, with their radio interfaces such as Bluetooth, ZigBee, or WiFi, operate over the 2.4 GHz ISM frequency band, we thus pertain our discussion to this band in this study. As a note, our idea can be easily extended to RF noise in other frequencies.



(a) Location 1 (b) Location 2

Figure 2: RF radio noise heat map over the 2.4 GHz ISM band. RF noise is highly dynamic and randomly distributed over time, frequency, and space.

3.2 Body-as-A-Conductor

As suggested by [43, 56], a human body can be treated as a conductor with low impedance (a few $k\Omega$). Placing the induced human body in the electromagnetic fields will build up a charge distribution over the body surface to reach an electrostatic equilibrium [41]. From the perspective of electrostatics, a radio source creates electromagnetic waves at its propagation direction. Such electromagnetic waves from multiple radio sources overlap with each other that generate time-variant electromagnetic fields. In accordance, the electrostatic equilibrium distribution on the body-conductor surface will also vary. Then, by creating a physical contact (e.g., using an electrode or electrical conductor) between body skin and the wearable transceiver, the latter can access RF noise harvested by the wearer from the open air, as shown in Figure 3. Here, the transceiver is a common component of commercial off-the-shelf (COTS) wearables with data transmission capacity.

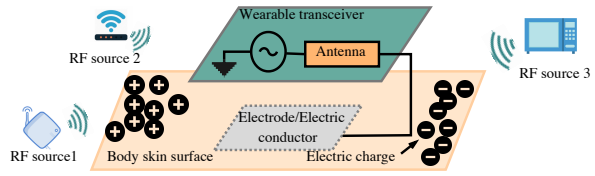


Figure 3: Illustration of how a wearable's transceiver accesses RF noise harvested by human body from open air.

Our design relies on a key observation that the received RF noise power measured in a logarithmic scale at different parts of a human body surface at the same frequency band and time instance experiences the same variation trend. We summarize the observation as the following theorem.

THEOREM 3.1. *Denote by $R_a(f,t)$ and $R_b(f,t)$ the measured RF noise power (in dBm) at two arbitrary positions on a wearer's skin, we have* $\frac{\partial R_a(f,t)}{\partial t} = \frac{\partial R_b(f,t)}{\partial t}$.

We provide a proof sketch as follows. According to prior results on bio-electricity characterization [1, 12, 28], the human body can

be deemed as a monopole cylinder conductor illuminated by waves from multiple radio sources. As mentioned above, the induced human body in electromagnetic fields builds up a charge distribution over the body surface. Assume that the axial current induced by the electric field is dominant. As shown in Figure 1, we denote $V_0(f,t)$ the voltage drop from the human head to the foot base of the body conductor. $V_0(f,t)$ is a complex value and variant with respect to f and t. Let $V(f,t)$ be the voltage at an arbitrary position of the human body. It can be expressed as $V(f,t) = \alpha V_0(f,t)$, where α is complex-valued coefficient with $|\alpha| \in [0,1]$. As indicated by [27, 43], the skin impedance Z at a given body position is positively correlated with its relative distance to the ground. Apparently, the closer the position to the foot base, the smaller $|\alpha|$ is. Moreover, Z is not only dependent on body height, but also the human biometric features, including weight, shape, body mass density, etc.

To obtain received RF noise power, most RF transceivers measure the average of the *apparent power* of RF signals in logarithmic scale [33, 51], which is expressed as

$$R(f,t) = 10\lg(|\frac{V^2(f,t)}{2Z}|/1\ mW) \tag{1}$$
$$=10\lg|\frac{(|\alpha|^2|V_0(f,t)|^2 e^{2j(\theta_\alpha+\theta_0(f,t))})}{2|Z|e^{j\theta_Z}}| = 10\lg\frac{|\alpha|^2|V_0(f,t)|^2}{2|Z|}$$

with its unit as dBm. In practice, the average of the apparent power is calculated based on the in-phase and quadrature (I/Q) components of received discrete samples. Here, we express the apparent power in its analog form for analysis simplicity. θ_α, $\theta_0(f,t)$, and θ_z stand for the corresponding phases of the α, $V_0(f,t)$, and Z, respectively. Let $R_a(f,t)$ and Z_a be the received RF noise and impedance at position a on body skin. Then, the partial derivative of $R_a(f,t)$ with respect to t is

$$\frac{\partial R_a(f,t)}{\partial t} = \frac{\partial}{\partial t}(10\lg\frac{|\alpha_a|^2|V_0(f,t)|^2}{2|Z_a|})$$
$$=10\frac{\frac{|\alpha_a|^2}{2|Z_a|}\frac{\partial|V_0(f,t)|^2}{\partial t}}{\frac{|\alpha_a|^2|V_0(f,t)|^2}{2|Z_a|}\ln 10} = \frac{10}{\ln 10}\frac{1}{|V_0(f,t)|^2}\frac{\partial|V_0(f,t)|^2}{\partial t} \tag{2}$$

where α_a is the fractional coefficient to $V_0(f,t)$. Similarly, we have

$$\frac{\partial R_b(f,t)}{\partial t} = \frac{10}{\ln 10}\frac{1}{|V_0(f,t)|^2}\frac{\partial|V_0(f,t)|^2}{\partial t} = \frac{\partial R_a(f,t)}{\partial t}$$

which ends the proof.

Theorem 3.1 states that the first order derivative of $R_a(f,t)$ and $R_b(f,t)$ over t are the same. Essentially, the first derivative reflects the direction the function is going, increasing or decreasing. It can be interpreted as an instantaneous rate of change. $R_a(f,t)$ and $R_b(f,t)$ are not necessarily exactly the same in their different amplitudes. Hence, rather than comparing the exact shape of received RF noise, we look into their variations. Besides, the equality in Theorem 3.1 exists only when noise power is measured in its logarithmic form, as otherwise $\frac{\partial R_a(f,t)}{\partial t} = \frac{|\alpha_a|^2|V_0(f,t)|}{|Z|}\frac{\partial|V_0(f,t)|^2}{\partial t} \neq \frac{\partial R_b(f,t)}{\partial t} = \frac{|\alpha_b|^2|V_0(f,t)|}{|Z|}\frac{\partial|V_0(f,t)|^2}{\partial t}$.

It is worth mentioning some prior works on establishing intra-body communication (IBC) between wearable devices [15, 48, 58]. The body serves as a transmission medium to host peer-to-peer communications. As these works focus on how to achieve high-speed low-energy data transmission, their goal and basis are quite different from ours. Given that IBC can provide covert inter-body channels, Roeschlin et al. [45] proposed to utilize these channels for key pairing between wearables. However, there are at least two restrictions. First, they need to design their own transceivers for IBC. Second, covert channels only exist for low-frequent electromagnetic signals. Signals above 100 MHz can be easily radiated to the environment, rendering the whole procedure vulnerable to eavesdropping attacks. Unfortunately, most wearables operate over 2.4 GHz nowadays.

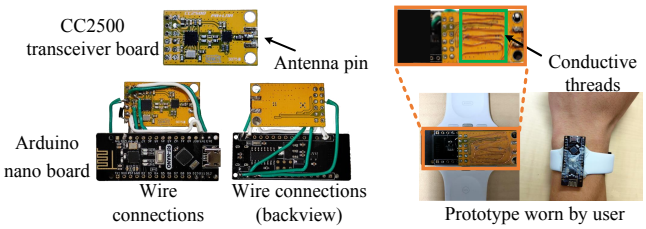


Figure 4: System setup.

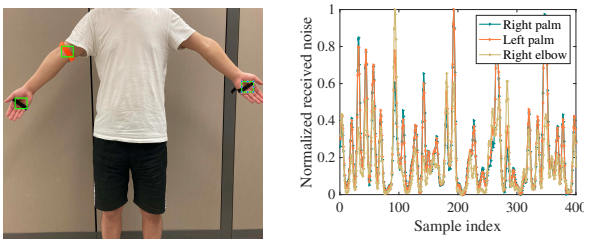
4 FEASIBILITY STUDY

The objective of this section is to investigate the feasibility of leveraging ambient RF noise for wearable device paring via extensive measurement studies. Essentially, we need to validate two substrates. First, on-body and thus legitimate devices should be capable of extracting from RF noise common features. Second, it is infeasible for an adversary to do so.

4.1 Measurement Setup

Our experiments are conducted using Arduino nano boards and CC2500 radio chips [21]. Several watch-like wearables have been built as shown in Figure 4. CC2500 is an RF transceiver that operates over the 2.4 GHz ISM band and designed for very low-power wireless applications. Its role here is to collect and sample RF noise captured by the human body. A conductive wire is wound back of CC2500 to create physical contact between the CC2500's antenna and the wearer's skin. In this way, RF noise, which is first captured by the human body from the open air, is then conducted to the wearable transceiver through the wire, as demonstrated in Figure 3. Each CC2500 is associated with an Arduino nano that plays as a microcontroller to store and process the received noise. Arduino nano is powered by a lithiumion polymer battery. The system samples the noise at a rate of 7000 samples/sec. Samples are timestamped using the system clock. A classical flooding time synchronization protocol (FTSP) [36] is implemented for clock synchronization between devices. We build a prototype for the measurement study instead of using COTS wearables. As they seal their transceiver chips inside of the out-shell case, it is challenging to create direct contact between a wearer's skin and transceiver chips, more specifically, antennas.

Although our prototype does not involve any dedicated sensors, such as accelerometer [11, 54], ECG, and EMG sensors [46, 59], we do need a minor modification on hardware. As mentioned above, a conductive wire or an electrode is needed to connect between the body skin and the wearable antenna.



(a) Experiment setup (b) Received RF noise after filtering and normalization

Figure 5: RF noise measures at different parts on body surface.

4.2 Measurement Results

Devices on the same body. This part verifies the theoretical result of Theorem 3.1 that wearables attached to different parts of the body surface sense the same RF noise variation tendency. Three prototypes are used; two of them are held in the wearer's right and left hand palm, respectively, while the third one is attached to the right elbow (shown in Figure 5(a)). To examine noise variation tendencies, the raw signal is first fed into a Gaussian filter to remove low-frequency noise caused by, for example, loose skin contact or imperfect measurements. As our design does not rely on signal amplitudes, normalization is further applied. Figure 5(b) depicts the received RF noise over a frequency band of 2400.0–2400.4 MHz. We observe that the three signals are synchronous across most samples, even when the right palm is about 125 cm away from the left palm. Such a phenomenon validates the basis of our pairing scheme: Wearables can observe almost identical RF noise variations when attached to the same body surface, regardless of their inter-device distance.

One on-body device and one off-body device. This part further shows that measures at an adversary, a device has no physical contact with the wearer, are distinct from the ones obtained at legitimate on-body devices. In the experiment, one device is placed on a table, while the other is held in the wearer's right palm (shown in Figure 6(b)). To evaluate the correlation between two measures, we examine their *Pearson correlation coefficients* [40]. Figure 6(d) plots the Pearson correlation coefficients by tuning the distance between two devices. We find that the average coefficient is merely 0.53 even when the distance is as short as 1 cm. As a comparison, the value is around 0.75 when both devices are on the same body (shown in Figure 6(a)). Besides, the correlation drops quickly as the distance grows. As revealed in Section 6.1, the success rate of imitation attacks under an inter-device distance of 1 cm is only 5.8%. Therefore, the off-body adversary cannot extract meaningful information for key forgery even within close proximity to the wearer.

Devices on different bodies. We now demonstrate that an adversary, a device attached to an outlier, is incapable of extracting the same secret as a legitimate device. The setting is shown in Figure 6(c). Like above, we first examine the Pearson correlation coefficient of RF noise received at the two devices. Figure 6(e) shows that their correlation is relatively low throughout all inter-device distances. Specifically, when two wearers stand as close as 1 cm, the corresponding coefficient is merely 0.47, even lower than the

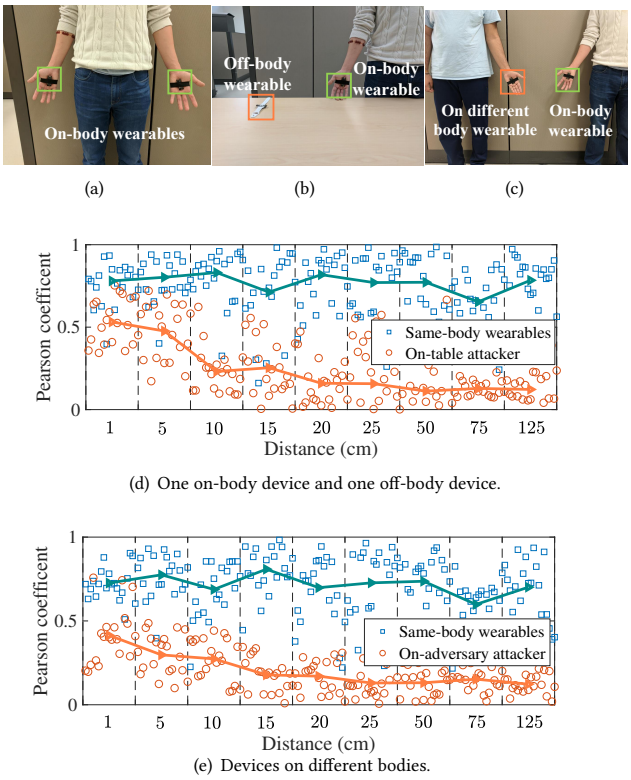
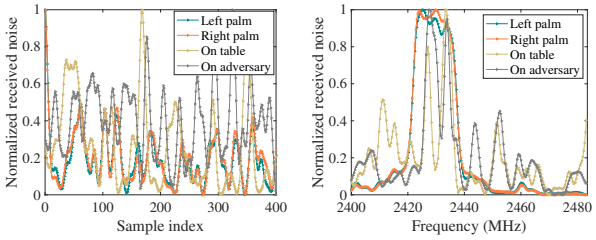


Figure 6: Pearson correlation coefficients of RF noise received at wearables under various placement settings.



(a) RF noise in temporal domain (b) RF noise in frequential domain

Figure 7: RF noise properties in time and frequency domains.

value when the adversary is placed on the table. This is because the unique biometrics of different human bodies introduce another dimension of diversity to RF noise measures.

Figure 6 indicates that the adversary cannot generate the same pairing key as the legitimate device due to a lack of common entropy source. In contrast, some prior pairing schemes [32, 34, 35, 38, 49, 53, 60], which rely on propagation characteristics of wireless signals in free space, only work if the adversary is at least half the wavelength (6.25 cm@2.4 GHz) away from the legitimate device, as otherwise wireless signals highly correlate. Apparently, our approach is free from such a restriction.

RF noise properties in time and frequency domains. Figure 7 shows the normalized RF noise in both time and frequency domains. Four devices are used, two on wearer's left and right palms,

one on a table, and the last one on a second wearer's left palm. We observe in Figure 7(a) that measures from devices on wearer's left and right palms match well in the time domain. Besides, they are well separated from measures from the other two devices. We further show in Figure 7(b) RF noise measures across different spectrum bands around 2.4 GHz. A similar relation between these four measures is obtained. Interestingly, a surge is observed from all four measures at the frequency band between 2416 MHz and 2440 MHz, which is exactly the operating frequency of IEEE 802.11 WiFi router in the test room.

The properties of RF noise discussed above are essential for our pairing scheme. Since devices on the same wearer share RF noise measures of high similarity, common secret keys can be extracted. The details of key generation and device pairing will be discussed in Section 5. Besides, readings from an adversary, either placed off-body (denoted as type-I imitation attack) or worn by another wearer (denoted as type-II imitation attack), are distinct from the ones measured at the legitimate device even they are in close vicinity. Thus, it is extremely challenging for an adversary to extract a valid pairing key. Moreover, the above properties are consistent across time and frequency domains. It provides an ample choice of time slots and frequency bands from which pairing keys can be extracted.

5 DEVICE PAIRING

5.1 Overview

As a key component, Alice and Bob seek to produce common secret keys from their RF noise readings. A naive approach is *reciprocal quantization* [35, 52]. Setting two adaptive thresholds q_+ and q_-, sample readings above q_+ are mapped to 1's and those smaller than q_- are mapped to 0's. However, this approach imposes stringent requirement over device synchronization. If two devices are misaligned even by a single bit, the mismatch will be accumulated and result in high error rate eventually. Instead, we propose to utilize the noise variation tendency for key generation. By dividing samples into blocks, we examine the variation of samples in each block so as to tolerate the misalignment over a couple of individual samples. Besides, our scheme adopts the framework of *fuzzy commitment* [13, 25, 39] for key establishment. It is able to transform a secret value s into a commitment/opening value pair (σ, λ), such that σ does not reveal any information about the secret s. Another pair (σ, λ') will reveal s if the Hamming distance $\texttt{Ham}(\lambda, \lambda') \leq t$. It is computationally infeasible to find λ' with $\texttt{Ham}(\lambda, \lambda') > t$ that decommits σ. Due to the employment of Reed-Solomon (RS) codes [50], two devices are able to agree on a common key, if the opening values generated from their received RF noise differ in t bits at most. The value of t depends on the parameterization of the RS code and is tunable to strike a balance between security and usability. Its discussion is provided in Section 6.3.

As shown in Figure 8, the pairing protocol consists of three phases, initialization, key agreement, and key confirmation.

Initialization phase. Alice broadcasts her identifier ID_A to its vicinity. If a new wearable Bob wishes to pair with Alice, he sends a "RQST_TO_PAIR" message with his identifier ID_B. Alice confirms this request by replying with "RSP_TO_PAIR" and the specification of noise measurement duration T and frequency channel CH.

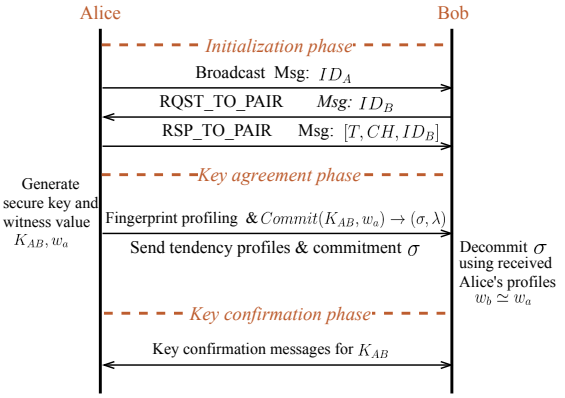
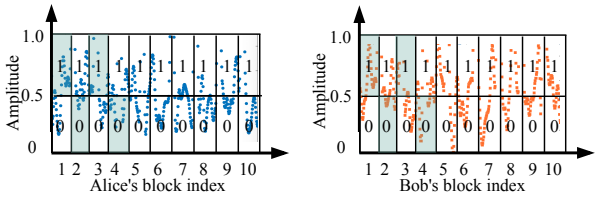


Figure 8: Pairing protocol.



(a) Fingerprinting with $w_a = 1010$ (b) Recover *witness* as $w_b = 1010$

Figure 9: Fingerprint profiling.

Key agreement phase. Denote by R_a and R_b the noise measurements collected by Alice and Bob, respectively. Alice generates a secret key $K_{AB} \in \{0,1\}^k$ and a *witness* $w_a \in \{0,1\}^k$ using her pseudo-random number generator (PNG). She then turns them into a commitment/opening pair $(\sigma, \lambda) \leftarrow \texttt{comit}(K_{AB}, w_a)$. The opening value λ is calculated as the codeword for K_{AB} using Reed-Solomon (RS) encoding, $\lambda = \texttt{RS}(K_{AB})$. The commitment σ is then calculated as the difference of w_a and λ, $\sigma = w_a \ominus \lambda$, where $\ominus$ denotes a subtraction in a finite field (analogous to an XOR operation). Then, Alice applies the proposed fingerprint profiling mechanism (discussed in Section 5.2) to derive her selected fingerprint profile, denoted by P. Alice releases σ and P to Bob. Neither K_{AB} nor w_a can be revealed from the transmitted message by any adversary. Unlike some prior works on device pairings [46, 56], which assume the existence of some secure (but unauthenticated) channel (e.g., TLS) to exchange messages, our protocol does not need such an assumption and is thus more practical for implementation.

Upon receiving the message, Bob produces another *witness* w_b based on P and his received RF noise R_b via the fingerprint profiling mechanism. If Bob is a legitimate device, then $w_b \simeq w_a$. Bob's opening value is calculated as $\lambda' = w_b \ominus \sigma$. If $\texttt{Ham}(\lambda, \lambda') \leq t$, K_{AB} is retrieved by decoding λ' as $K_{AB} = \texttt{RSD}(\lambda')$ using the RS decoding function $\texttt{RSD}()$. It means w_a and w_b can differ in t bits at most, the maximum number of mismatch bits the RS coding can correct.

Key confirmation phase. The aim of this phase is for peers to determine if their established keys are identical. We employ the classic challenging-and-replying protocol [13, 14]. Two devices use their established keys to encode a nonce and send both the nonce and its ciphertext to each other. The key is confirmed if its decoded ciphertext is the same with the nonce.

5.2 Fingerprint Profiling Module

This module enables Alice to select her fingerprint profile P that hides the information of *witness* w_a and Bob to recover *witness* w_b from P. A success design ensures $w_b \simeq w_a$ if Bob is a legitimate device. This module consists of components at both Alice and Bob. Our idea is inspired by [53] but different in several ways. For example, the scheme [53] employs instant channel state information (CSI) amplitude as device's fingerprint features. Singular value decomposition is applied to avoid RF noise interference for feature extraction. Instead, RF noise is treated as ingredients for key generation in this work. Besides, the noise variation, rather than its amplitude, is considered. As a result, the corresponding feature extraction algorithm will be different.

For Alice, she first segments RF noise samples R_a into a sequence of blocks. Denote by n the size of each block; it stands for the number of successive samples contained in a block. Then, the samples in a block is further divided into two groups G_0 and G_1 by a threshold which is set to 0.5 in this work. Particularly, samples with normalized amplitude above 0.5 belong to G_1; the rest belong to G_0. Figure 9(a) illustrates the formulation of blocks and groups. Alice applies the PRG to produce a pseudo-random number $w_a \in \{0,1\}^k$, called *witness* under the framework of fuzzy commitment. Then, the corresponding group is selected in each block sequentially. In the example shown in Figure 9(a), given $w_a = 1010$, it indicates that G_1 is selected at the first and third blocks, while G_0 is selected at the second and fourth blocks, all marked in green.

As discussed in Section 3 and 4, the variation tendency of RF noise at two legitimate devices shares high similarity. Therefore, by applying the regression analysis over the samples from the same group given the same underlying model, Alice and Bob are able to derive the same set of parameters that characterize the model. For computation efficiency, in this work we apply the *linear regression* model, which is fitted using the least squares approach [5]. Once Alice derives a linear function to fit samples in each of her selected groups, she then gathers their slopes and sample statistics as her selected fingerprint profile, denoted by P.

The operations executed at Bob are similar to Alice. Blocks and groups are constructed based on his R_b. The same linear regression model is applied to derive linear functions and thus their slopes for both G_0 and G_1 in each block. Upon receiving P from Alice, for each element Bob decides which group, G_0 or G_1, in a block produces the closest slope by applying the t-test similarity comparisons [16]. If it is G_0, then a bit 0 is recorded, and 1 otherwise. This step can be viewed as the reverse of operations executed at Alice. Eventually, *witness* w_b is obtained at Bob. In the given example, w_b is equal to 1010 if Bob is a legitimate device.

If Alice intends to deliver a k-bit key K_{AB}, she constructs at least k blocks. The block size n influences the performance of key generation. A small n results in high bit error rate, while a large n reduces the key generation rate. Section 6.3 provides detailed discussion over the choice of n.

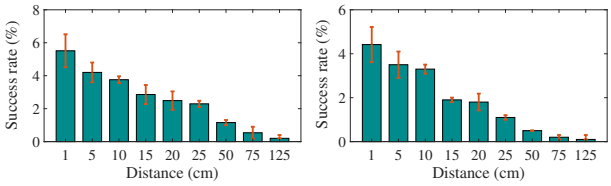
6 EVALUATION

The experiments are conducted using our prototype devices described in Section 4. As human subjects are involved, the entire research has been approved by IRB. Since the prototype is built on a commercial transceiver that follows the FCC regulations, it poses a minimal risk to human health. During the data collection, the transceiver only passively measures the RF noise without injecting any current flow through the body. Subjects are fully informed before voluntarily participating in the experiments. Their discomfort anticipated in the research is not greater than those ordinarily encountered in daily life. All collected data are de-identified and properly stored locally from potential leakage.

The goal is to evaluate both the security and usability of the proposed mechanism. A wide spectrum of impact factors are thoroughly examined, such as system parameters, wireless environments, wearer motion status, and device types. Comprehensive performance comparison is also made with existing works. A total of 6 volunteers, 4 males and 2 females between 25 to 28 years old, are recruited for data collection. Before each experiment, detailed instructions regarding experimental procedures are provided.

6.1 Robustness Against Attacks

Imitation attack. In type-I imitation attacks, the adversary aims to derive a valid pairing key from its RF noise measurement for being at the vicinity of the wearer. Since RF noise is highly diverse in the spatial domain, its electromagnetic features are distinct even at two geographic locations with close proximity, as illustrated in our feasibility study. Thus, it is impossible for the adversary to extract an accurate *witness* to decode the session key K_{AB}. In the experiment, we test the adversary's success rate by varying its distance to the wearer. Figure 10(a) shows that the maximum success rate of type-I imitation attack is upper-bounded by 5.8% which is achieved at the closest distance to the wearer of 1 cm. The success rate further drops to 0.2% when the distance becomes 125 cm. This phenomenon is consistent with the result of Figure 6(d).



(a) Type-I imitation attack (b) Type-II imitation attack

Figure 10: Success rate of imitation attacks.

In type-II imitation attacks, the adversary is attached to another wearer's body. The experiment is carried following the same setting in Section 4.2 for our feasibility study. As shown in Figure 10(b), type-II attacker's success rate, 4.3% the maximum, is even lower than type-I attacker. This is because body biometric characteristics introduce an additional layer of uniqueness to the RF noise measures. Therefore, the adversary, attached to an outlier, is also unlikely to extract the same *witness* as a legitimate device to derive the valid session key.

Some existing schemes [34, 37, 53] that rely on wireless signals for device pairing typically assume the adversary no less than half of the signal wavelength away from the legitimate device; otherwise, their received signals will be highly correlated and thus fail the scheme. To be specific, the adversary gains a success rate of 93% at a distance of 5 cm [53], while this value is only 4.2% of our scheme.

Synthesis attack. In this attack, the adversary first models the statistic distribution of RF noise by collecting samples from the radio environment surrounding the wearer for a period of time. Then it fabricates synthetic measurements from the distribution to launch pairing attempts.

In the experiment, Gaussian process is adopted. For each noise sample $R(f,t), t \in T, f \in CH$, the synthetic value is randomly chosen following $\mathcal{N}(\mu, \delta)$. It estimates from collected RF noise measurements to get μ and δ. We generate 10,000 forgery noise samples to attack 120 pairing processes. As shown in Table 1, the attacker's success rate is relatively low, 3.2% the maximum. Besides, it gains no advantage for a longer observation period. Since RF noise is highly dynamic, demonstrating memoryless property in the time domain, historical statistics are of little help to predict its future values. Thus, it is unlikely for this type of adversary to extract useful information from historical data analysis. It is noteworthy that some existing approaches use cable radiations [56] and human movements [11, 54] as common entropy for pairing. As these signals exhibit certain patterns, they are vulnerable to synthesis attacks. For example, cable radiations follow a sinuous waveform at the frequency of 50Hz/60Hz. Such a pattern is easily predictable.

Table 1: Success rate of synthesis attacks.

Observation duration	10 min	15 min	20 min	30 min
Success rate (%)	2.9	1.8	3.2	2.1

MitM attack. In order to place between Alice and Bob, the adversary must either run the protocol with each of them or interfere, for example, replace or modify at least one of the key agreement messages, in an ongoing pairing session between Alice and Bob. As discussed above, the adversary cannot successfully complete the protocol alone with either Alice or Bob. Besides, any modification of the key messages will also cause Alice and Bob to disagree on the key. For example, if the adversary replaces Alice's commitment σ with its own commitment σ', then Bob derives a different opening value $\lambda' = w_b \ominus \sigma' \neq w_b \ominus \sigma$. The decoded symmetric key $K'_{AB} = \mathtt{RSD}(\lambda')$ is different from K_{AB} generated by Alice. It results in a failure during the key confirmation phase. Now the only remaining option for the adversary is to initiate two sessions simultaneously with both Alice and Bob, and then rely on them for key establishment. To succeed, the adversary must correctly guess K_{AB} generated by Alice. The probability is $1/2^{128}$ given $k = 128$, which is negligible.

6.2 Key Generation Performances

Source entropy. Entropy characterizes the uncertainty associated with an information source. It is more difficult for an adversary to predict and deduce secrets from high-entropy sources. We examine the *spectral entropy* of RF noise in the experiment. It is calculated by applying the Shannon entropy concept over the power distribution of a given signal. This metric has been widely employed to quantify signal randomness and irregularities in the domain of speech recognition.

Figure 11 shows the spectral entropy of RF noise at different time instances. We observe its value is above 0.9 mostly with its average around 0.94. Hence, RF noise demonstrates satisfactory randomness to defend against brute force attacks and guessing

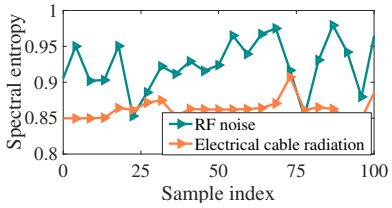


Figure 11: Spectral entropy.

attacks on device pairing. For comparison, Figure 11 further shows the spectral entropy of electrical cable radiation. Its randomness has been recently explored for paring and wearable device on-body/off-body detection (e.g., [31]). We find that the electrical cable radiation exhibits a much lower spectral entropy around 0.85. As mentioned above, this is because cable radiations mainly follow a sinuous waveform at the frequency of 50Hz/60Hz. Thus, it bears much less uncertainty than RF noise.

Table 2: Bit generation rate (bits/sec)

TDS	KEEP	ASBG	Telepathy	Proposed
96	28	13	12	138

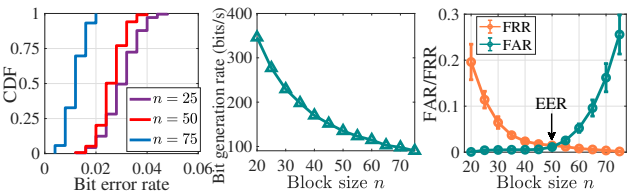
Bit generation rate. Bit generation rate is defined as the number of bits of the key over the time for the entire pairing process. Table 2 compares this metric between our scheme and other four schemes, including TDS [53], KEEP [52], ASBG [23], and Telepathy [38]. Specifically, TDS and KEEP leverage the common CSI measurements at two closely located devices for key pairing. ASBG and Telepathy rely on the reciprocity of radio wave propagation for transmission peers to extract common secret keys. For the sake of fairness, we copy the performance of these four schemes from their own papers. We notice that our scheme has the highest rate of 138 bits/sec. KEEP, ASBG and Telepathy have relatively low rates among the five. This is because they employ the *reciprocal quantization* mechanism when converting radio samples into bits. As the mechanism drops a large amount of samples to resolve the quantization ambiguity, it slows down the bit generation process. Although the rate has been improved significantly by TDS, it suffers from a time-consuming information reconciliation process, which is used to reconcile bit mismatch caused by imperfect clock synchronization. Since our scheme utilizes RF noise variation tendency for common secret extraction, imperfect clock synchronization imposes a rather limited impact on key agreement. Take Figure 9 as an illustration. Even if clocks at pairing devices are asynchronous by one-sample time duration, it is unlikely to change the slope and the corresponding bit derived from the entire samples in one block. Thus, the tedious information reconciliation process can be avoided.

6.3 Impact of Settings

Impact of key parameters. We first examine the impact of block size n on the performances of bit error rate, bit generation rate, and pairing accuracy. Specifically, bit error rate is defined as the number of mismatched bits over the number of all bits generated. False rejection rate (FRR) and false acceptance rate (FAR) are employed to characterize the pairing accuracy. FRR is the probability that a legitimate device is treated as an adversary. It is the ratio between

the number of times that a legitimate device is wrongly classified and the total attempts. FAR is the probability that an adversary is treated as a legitimate device. In the experiment, two legitimate wearables are attached to a wearer while an adversarial device locates 20 cm away from the wearer.

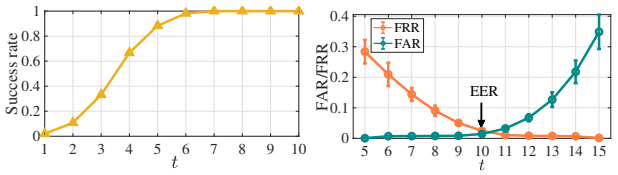
Figure 12(a) shows the cumulative distribution function (CDF) of the bit error rate for generating 128-bit pairing keys. We observe that a larger n associates with a lower error rate. This is because a larger group size can better tolerate tendency mismatches caused by measurement errors. On the other hand, as shown in Figure 12(b), a larger n brings down the bit generation rate. This is because it takes a longer time for collecting enough samples for key generation. We further observe in Figure 12(c) that a larger n leads to a lower FRR but a higher FAR. This is because a smaller-size block contains fewer samples. The derived fingerprint profile P becomes sensitive to measurement errors. Thus, legitimate devices become easier to be wrongly rejected. Meanwhile, it renders adversaries even less likely to pair. On the contrary, a larger block size better tolerates measurement errors with a lower FRR. Since it indicates a loose detection rule, FAR increases accordingly. We observe that the EER, the point at which FRR and FAR are equal, is 1.4% when $n = 50$. Figure 12 provides insights for selecting proper n that strikes a balance among the metrics of bit error rate, bit generation rate, and pairing accuracy.



(a) CDF of bit error rate (b) Bit generation rate (c) Pairing accuracy

Figure 12: Impact of block size n.

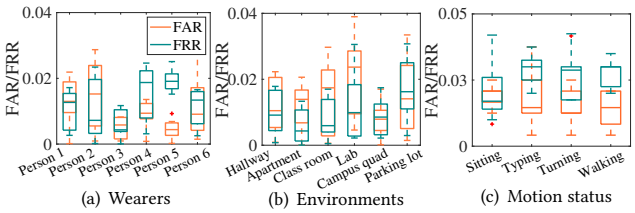
We then investigate the selection of parameter t for the fuzzy commitment. Recall that t is the maximum Hamming distance between two opening values λ and λ' that recover the same key K_{AB}. Figure 13(a) depicts the pairing success rate with respect to t. It is observed that the success rate increases as t grows. It meets our expectation as a larger t tolerates a larger amount of bit mismatches in opening values. It also accounts for why FAR increases as t grows shown in Figure 13(b); an adversary becomes easier to get paired. On the other hand, a larger t effectively brings down FRR. EER is equal to 1.6%, when $t = 10$. Combining the results of Figure 13, we find $t = 10$ as a suitable setting for implementation, as it produces 96.8% pairing success rate and a low EER of 1.6%.



(a) Pairing success rate (b) Pairing accuracy

Figure 13: Impact of fuzzy commitment parameter t.

Impact of wearers. Figure 14(a) shows the pairing accuracy across six different wearers. While each individual exhibits slightly different FAR/FRR, the overall performance is relatively consistent, with the average FAR and FRR both under 2.0%.



(a) Wearers (b) Environments (c) Motion status

Figure 14: Impact of usage settings.

Impact of environments. We further test the scheme at six different types of locations, including hallway, apartment, lab, classroom, campus quad, and parking lot. Figure 14(b) shows that the pairing accuracy performance is promising both indoors and outdoors. Since RF noise is ubiquitously accessible, our scheme does not impose any restrictions on its usage environment. In contrast, [56] relies on electrical cable radiation and thus is inapplicable in outdoors due to the unavailability of its signal sources.

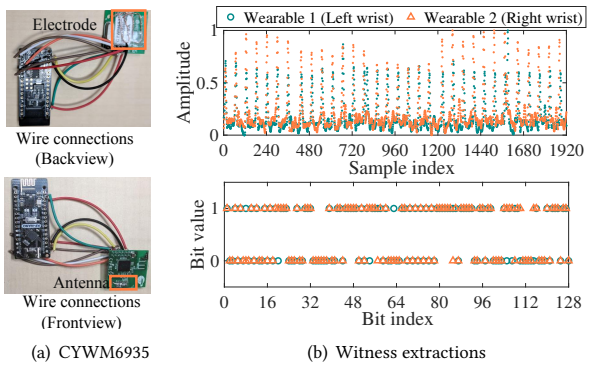
Impact of motion status. Since a human body performs various types of motions due to daily activities, it is important to show that the proposed scheme is motion-insensitive. In the experiments, volunteers are asked to perform four types of motions, including sitting, typing, turning directions, and walking. The corresponding pairing accuracy is depicted in Figure 14(c). We find that the best performance is achieved at the sitting status with averaged FAR=2.8% and FRR=3.1%, while moving actions slightly bring up the error rate. Still, the pairing accuracy is practically acceptable. Some prior works on wearable device pairing extract common secrets from body movements [11, 54]. The source entropy comes from the randomness of body movements. Their schemes do not work when users are in a relatively static status, say sleeping and sitting.

Impact of device placements. In this set of experiments, we evaluate the impact of device placements on the body surface. Several locations are examined, including user's palm, elbow, front head, wrist, and keen. Table 3 shows that the FRR is relatively stable for all locations, with the maximum value equal to 2.6%. It meets our expectations. The RF noise measures at different parts of a wearer's skin experience the same variation tendency. Therefore, the pairing performance, reflected by FRR here, is consistent. This is a desirable property. In practice, various wearables are attached to various parts of body skin to collect diverse biosignals. For instance, ECG monitors are sometimes attached to the chest. Then the above-mentioned prior designs [11, 54] that relay on body movements for key extraction do not work in this case as no significant movement is observable in the chest area.

Table 3: Impact of device placements.

Placement	R. elbow	F. head.	L. wrist	L. keen
FRR	2.1%	1.6%	1.8%	2.6%

Impact of different devices. To test the impact of different hardware, we prototype our scheme with an alternative 2.4 GHz



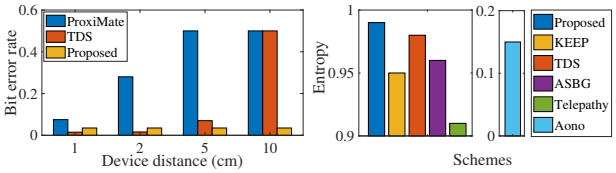
(a) CYWM6935 (b) Witness extractions

Figure 15: Impact of different devices.

ISM transceiver chip CYWM6935 [8] and Arduino board as shown in Figure 15(a). Two prototypes are used, worn on wearer's right and left wrists, respectively. The upper part of Figure 15(b) shows the normalized RF noise readings at two devices. It is observed that the two readings are highly overlapped. The lower part of the figure shows the generated random bits as *witness*. There are 8 mismatched bits in total between the two 128-bit witnesses generated at two wearables. According to the discussion over the selection of parameter t, i.e., the maximum number of tolerable mismatched bits, for fuzzy commitment, it is set to 10 empirically. Hence, despite the 8 mismatched bits, our scheme is capable of correcting them and guaranteeing the success of pairing.

6.4 Comparison with Other Pairing Schemes

In addition to the bit generation rate in Section 6.2, we present the performance comparison with prior works on bit error rate and key entropy. For the sake of fairness, we directly utilize the experimental results from these works.



(a) Bit error rate (b) Key entropy

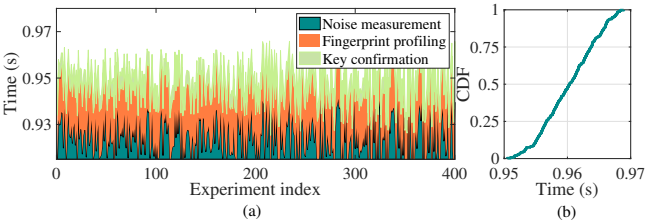
Figure 16: Comparison with other pairing schemes.

Figure 16(a) compares the bit error rate with two other schemes, ProxiMate [37] and TDS [53]. As mentioned previously, TDS leverages common CSI measurements at devices in close proximity to establish their symmetric keys, whereas ProxiMate utilizes FM radio and TV signals. The bit error rate is examined by tuning the inter-device distance. ProxiMate and TDS experience a surge in error after the distance surpasses certain thresholds. This is because the common secrets can only be extracted at two antennas within half wavelength. On the other hand, our pairing scheme is independent of the inter-device distance as long as they have physical contact to the same wearer.

Figure 16(b) compares the entropy of generated keys. Entropy reflects the randomness of keys from the perspective of uncertainty. Recall that Figure 11 shows the entropy of raw signals. We find that Aono [2] has the lowest entropy among the six, as it directly turns raw measurements into secret bits and raw signals are correlated in the temporal domain. To address this issue, KEEP, ASBG and Telepathy employ the reciprocal quantization mechanism; a certain amount of correlated signals are discarded during quantization. As shown, it effectively improves the entropy. The proposed scheme and TDS have the highest entropy, approximate to 1, since their keys are produced by PRN generators. As a note, our scheme extracts from RF noise the *witness* values instead of the key itself.

6.5 Usability

Time consumption. Figure 17(a) shows the duration for the three most time-consuming steps in the pairing protocol, including noise measurement, fingerprint profiling, and key confirmation. All results are obtained for establishing 128-bit key pairs. The noise measurement takes the longest time, with the average value of 0.924 s. For fingerprint profiling and key confirmation, their average time is 0.022 s and 0.006 s, respectively. We further depict in Figure 17(b) the CDF of the total time duration for one pairing. All trials can be accomplished within 0.97 s, which is promising for real-world application. As a reference, due to human involvement, the average duration for device pairing using numerical PIN and string PIN is about 8.6 s and 12.7 s [29], respectively.



(a) (b)

Figure 17: Computation time.

We further compare the average time consumption with other schemes in Table 4. FREE [35] leverages the acoustic CIR as the source and involves users for pairing. TouchAuth [56] explores cable radiation for authentication token generation. The entropy sources of these schemes have a much lower frequency range than RF noise; that being said, these sources exhibit much slower variations in the time domain. Thus, a high sampling rate is incompatible with these sources that produce low-entropy secret bits. TDS and KEEP utilize CSI as the entropy source, but suffer low bit generation rate as shown in Table 2.

Table 4: Comparison with existing schemes for time consumption.

TDS	KEEP	TouchAuth	FREE	Proposed
1.33 s	4.57 s	5 s	5.12 s	0.97 s

Energy consumption. Typically, wearable devices have a much shorter battery life compared with regular mobile devices. As pointed out by [18], the battery life for Apple Watch Series 3 is about 18 hours after an overnight charge under normal use, including 90 time checks, 90 notifications, 45 minutes of app use, and a 30-minute workout with music playback from Apple Watch via Bluetooth.

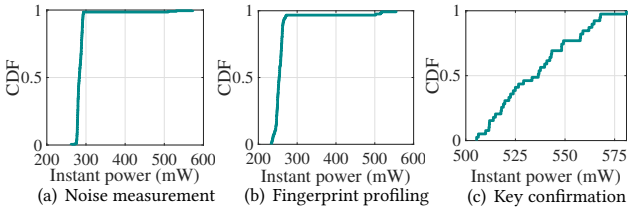


Figure 18: Power consumption of different steps.

Therefore, it is desirable to design energy-efficient pairing for wearable devices. Such an evaluation has been rarely discussed in previous literature due to the lack of readily usable energy measurement software. Instead, we measure the energy consumption of the proposed system by using dedicated hardware, Monsoon power monitor [20]. During the measurement, we first set up the prototype device in standby mode without running any programs and get the power consumption as 245.38 mW. In order to get the actual power consumption of our scheme, we subtract this baseline power from the instant power readings in the following measurements.

Figure 18 shows the CDF of power consumption during noise measurement, fingerprint profiling, and key confirmation. Their average values are 287.36 mW, 262.03 mW, and 530.88 mW, respectively. The key confirmation incurs the highest power consumption, since it involves multiple rounds of wireless transmissions. As indicated in Figure 17(a), the key confirmation can be completed within 6 ms on average. Thus, the energy consumption for key confirmation is rather limited. According to the readings, its average value is merely 1.52×10^{-3} J. Besides, the average energy consumption for noise measurement and fingerprint profiling are 0.26 J and 5.76×10^{-3} J, receptively. The entire pairing process consumes 0.27 J, which is negligible to the capacity of a wearable's battery. As a reference, the capacity of an Apple watch battery is 205 mAh, i.e., 2.73×10^{6} J.

Impact on communications. In our design, we create contact between the wearable antenna and body skin with the assistance of a conductive wire or an electrode. The goal is to facilitate the transmission of RF noise from the skin to the transceiver module, as illustrated in Figure 3. Apparently, the wearable transceiver module, which previously emits/receives wireless signals to/from open air, is now partially "blocked" by the human body. It is thus indispensable to examine the impact of coupling antenna with human skin on wearable communications. In the experiment, we examine peer-to-peer communication data rate between two prototype devices. We notice that the difference is negligible when they are closely positioned, e.g., 50 cm apart from each other. It becomes noticeable as the distance increases. For example, the data rate without body contact is 287.9 kbps, which is about 1.16 times the rate with body contact 248.6 kbps, when their distance is 185 cm. Therefore, our scheme sacrifices a small portion of communication performances, especially when devices are remotely located. Such degradation is practically acceptable for most biosignal transmissions. For example, according to [4], it takes 1 sec on average to produce an entry of realtime one-byte heart rate reading. Taking into account of 20-byte header for data transmission, the estimated data rate is about 168 bps, which is negligible compared with 248.6 kbps, the lowest achievable data rate of peer-to-peer transmission between two prototype devices with body contact given in Table 5.

Table 5: Impact on wireless data communication rate (kbps).

Distance (cm)	50	70	100	125	150	185
Without body contact	308.9	298.6	294.2	292.5	289.5	287.9
With body contact	301.3	285.2	275.7	255.2	251.5	248.6

7 RELATED WORK

7.1 Pairing for Wearable Devices

To secure wireless communications among wearable devices, quite a few novel methods have been proposed to facilitate automatic device pairing without any trusted authority. The idea of *touch-to-access* is *de facto* the pairing rule followed by existing works. Two wearables are allowed to be paired if and only if they are attached to the same human body.

Body movements have been explored as an entropy source for key extraction. Since human movements are unique across individuals, readings from the same human body are considered to share significant similarity, while that on different bodies are not. Thus, prior works [11, 54] turn readings from inertial sensors into common cryptographic keys. Along this line of research, some othere existing works utilize ECG or EMG signals [46, 59] for key establishment. These solutions require a common dedicated sensor across all devices (e.g., an accelerometer or ECG monitor), which largely hinders their wide adoption. Treating human body as a transmission medium, Roeschlin et al. [45] proposed to utilize this covert channel for key pairing. Nonetheless, it requires a non-trivial design of communication transceivers. A recent study TouchAuth [56] treats human body as an antenna that captures radiation from electrical cabling. It converts the corresponding potentials measured at two devices within close proximity into their common secrets. The scheme fails if two devices are reasonably distantly located even on the same body. Besides, cable radiations are mostly unavailable outdoors.

7.2 General Device Pairing

Pairing has also been studied for general IoT devices. Existing schemes mainly fall into two categories, channel reciprocity based and context-based paring.

Channel reciprocity based paring. Channel reciprocity states that a pair of wireless transceivers observe the same channel characteristics, which are then utilized by transceivers for key pairing. Zeng et al. [60] turned RSS readings into secret bits. Realizing that RSS-based pairing bears low bit generation rate, recent works use CSI [32, 52] and Channel impulse response (CIR) [35, 38, 49] as alternative entropy sources. Due to the involvement of phase information (in addition to signal amplitudes in RSS readings), CSI/CIR measurements can be converted to secret keys at a much higher speed. More importantly, the diverse information also renders spoofing attack more difficult to launch. Meanwhile, these works impose strict requirement over channel coherence–channel reciprocity exists only within channel coherent time, which is typically at a level of 10 ms for 2.4 GHz wireless signals. Existing schemes are implemented using the probing mechanism in IEEE 802.11. Alice broadcasts a Probe frame, upon receiving which Bob replies with

an ACK. Only under the ideal case that ACK is replied immediately, i.e., the frame interval is deemed within coherence time. In practice, it is not rare that Probe or ACK is corrupted by other ongoing transmissions, especially in crowded 2.4 GHz ISM band. Consequently, the condition for channel reciprocity does not hold.

Context-based paring. This series of approaches are based on the assumption that co-present devices observe common contextual information that can be transformed into shared secrets. For example, Markus et al. [39] proposed to have devices compute a fingerprint of their ambient context using sensor modalities like ambient noise and luminosity. A similar idea is adopted in [26, 47]. Like many existing pairing schemes for wearables, [39, 47] assume the existence of commonly available sensors. To overcome this restriction, Han et al. [13] proposed a pairing scheme using heterogeneous sensor types. Their idea is that devices co-located within a physical boundary can observe more events in common over time, as opposed to devices outside. Nonetheless, sensors still need to capture certain contextual information, such as light, sound, movement, which are not accessible for many wearables. More importantly, these schemes are vulnerable to stealthy attackers that coexist with legitimate devices, say in the same room. As a result, the secret can be easily interpreted by attackers.

Another line of research also employs wireless channel characteristics for pairing. Rather than channel reciprocity, these approaches rely on the observation that received wireless signals are unique for co-presence devices. For example, Miettinen et al. [37] used the RSS to generate symmetric keys for two devices of close proximity. CSI measurements are also exploited [34, 53]. Nonetheless, these schemes only work when inter-device distance is within a certain threshold. Given a radio wave of frequency 2.4 GHz, two pairing devices should be located within 6.25 cm, as their received signals quickly de-correlate beyond the half-wavelength limit. Such a restriction is easily violated in a wearable system, for example, two devices worn on user's two wrists.

7.3 Human Body Sensing Capacity

The idea of leveraging conductive human body for sensing has been explored in various context. Pioneered by Zimmerman [62], IBC is investigated for information transmission among on-body devices by treating human body as a transmission medium. The research [15, 30, 58] also falls into this category, but with different focuses, such as propagation channel modeling and channel capacity quantification. Different from IBC, some existing works investigate the feasibility of using body electric potentials induced by power line radiation for gesture recognition [7], clock synchronization [55], object classification [57], and touch/motion sensing [6]. However, none of them is about device pairing.

8 DISCUSSION

Requirement of device wearing. Our scheme requires physical contact between the wearer's skin and the conductive wire or electrode (as shown in Figure 3). In this way, the RF noise harvested by the human body is accessible by the wearable antenna. In fact, the RF noise measured at the antenna is a mixture of RF noise from both the human body and open air. A physical contact ensures that the dominant portion is from the former. This is important, as otherwise the basis of our scheme that RF noise measures at different parts of body surface share the same variation tendency may not hold. It is because wireless signals are high dynamic when propagated through open air. The correlation between two signals vanishes quickly if their distance is beyond half of the signal wavelength.

We notice that body movement may impact the physical contact which, in turn, degrade pairing performance. In this scenario, a larger block size n or fuzzy commitment parameter t can be adopted during the pairing process to better tolerate key mismatches caused by measurement errors. We show in Figure 14(c) that such an impact to pairing accuracy is effectively avoided. Meanwhile, it will prolong the pairing duration though.

Injection attack. An adversary can inject spoofing frames or signals to the wireless environment to force Alice and Bob to agree on a common key designed by the adversary [9]. This is referred to as injection attack or spoofing attack. Quite a few countermeasures have been proposed to resist such attacks. For example, Zheng et al. [61] exploited the out of ISM band signals, e.g., cellular signals, as an additional reliable source for pairing security. Rong et al. [24] defended the attack by developing user introduced randomness (UIR) to eliminate any correlations caused by the injected signals. Song et al. [10] had the transmitter (Alice) to design a secrete key and the receiver (Bob) to obtain it by leveraging a channel manipulation technique. The adversary can only sabotage Bob's key but not Alice's. Any key disagreement will alert the participants about the presence of injection attacks. All these ideas can be adapted to our scheme to resist injection attacks.

In many cases, the wireless channel between the adversary and Alice/Bob is a multi-path transmission link due to reflectors and scatters in the environment. The multi-path channel is even time-variant because of the movement of wearers and their surrounding objects. Even slight perturbations in the environment can lead to significant differences between the received signal at Alice/Bob and the transmitted signal from the adversary. Therefore, the conventional injection attack is not easy to launch effectively in the wearable system with human involvement.

9 CONCLUSION

In this paper we propose a novel approach for wearable device pairing which builds upon the core idea of treating the human body as a conductor. Wearables can observe almost identical RF noise variations when attached to the same body surface, regardless of which part of the skin they contact. Under the touch-to-access policy, we present a protocol that allows two legitimate devices to securely agree on a mutual secret. The RF noise serves as an ideal entropy source due to its ubiquitous presence and high randomness and unpredictability. We have also implemented a prototype of our scheme. Its security is measured from the aspects of robustness against various types of attackers, key generation performances, the impact of system settings. Its usability is also evaluated in terms of time and energy consumption. Compared with prior works, our scheme does not restrict the placement of wearables on a human body; neither does it rely on any dedicated sensors. In summary, we believe that our scheme is an attractive and practical solution to the pairing problem for light-weight wearable devices.

REFERENCES

[1] JB Andersen and P Balling. 1972. Admittance and radiation efficiency of the human body in the resonance region. *Proc. IEEE* 60, 7 (1972), 900–901.

[2] Tomoyuki Aono, Keisuke Higuchi, Takashi Ohira, Bokuji Komiyama, and Hideichi Sasaoka. 2005. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. *IEEE Transactions on Antennas and Propagation* 53, 11 (2005), 3776–3784.

[3] Apple. assessed at January, 2020. Use AirPods and other Bluetooth accessories with Apple Watch. (assessed at January, 2020). https://support.apple.com/en-us/HT204218

[4] Apple. assessed at January, 2020. Your heart rate. What it means, and where on Apple Watch you'll find it. (assessed at January, 2020). https://support.apple.com/en-us/HT204666

[5] Samprit Chatterjee and DL McLeish. 1986. Fitting linear regression models to censored data by least squares and maximum likelihood methods. *Communications in Statistics-Theory and Methods* 15, 11 (1986), 3227–3243.

[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 ACM Conference on Ubiquitous Computing (UbiComp)*.

[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)*.

[8] Cypress. assessed at January, 2020. CYWM6935 Transceiver. (assessed at January, 2020). https://www.cypress.com/file/123521/download

[9] Simon Eberz, Martin Strohmeier, Matthias Wilhelm, and Ivan Martinovic. 2012. A practical man-in-the-middle attack on signal-based key generation protocols. In *Proceedings of the European Symposium on Research in Computer Security (ESCORICS)*.

[10] Song Fang, Ian Markwood, and Yao Liu. 2019. Wireless-Assisted Key Establishment Leveraging Channel Manipulation. *IEEE Transactions on Mobile Computing* (2019).

[11] Rainhard Dieter Findling, Muhammad Muaaz, Daniel Hintze, and René Mayrhofer. 2016. Shakeunlock: Securely transfer authentication states between mobile devices. *IEEE Transactions on Mobile Computing* 16, 4 (2016), 1163–1175.

[12] Mohamad Ghaddar, Larbi Talbi, Tayeb A Denidni, and Abderazik Sebak. 2007. A conducting cylinder for modeling human body presence in indoor propagation channel. *IEEE Transactions on Antennas and Propagation* 55, 11 (2007), 3099–3103.

[13] Jun Han, Albert Jin Chung, Manal Kumar Sinha, Madhumitha Harishankar, Shijia Pan, Hae Young Noh, Pei Zhang, and Patrick Tague. 2018. Do you feel what I hear? Enabling autonomous IoT device pairing using different sensor types. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*.

[14] Jun Han, Madhumitha Harishankar, Xiao Wang, Albert Jin Chung, and Patrick Tague. 2017. Convoy: Physical context verification for vehicle platoon admission. In *Proceedings of the International Workshop on Mobile Computing Systems and Applications (HotMobile)*.

[15] Mehrdad Hessar, Vikram Iyer, and Shyamnath Gollakota. 2016. Enabling on-body transmissions with commodity devices. In *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*.

[16] David C Howell. 2009. *Statistical methods for psychology*. Cengage Learning.

[17] International Data Corporation (IDC). assessed at January, 2020. IDC Forecasts Steady Double-Digit Growth for Wearables as New Capabilities and Use Cases Expand the Market Opportunities. (assessed at January, 2020). https://www.idc.com/getdoc.jsp?containerId=prUS44930019

[18] Apple Inc. assessed at January, 2020. Apple watch battery. (assessed at January, 2020). https://www.apple.com/watch/battery/

[19] Arduino Inc. assessed at January, 2020. Arduino chips. (assessed at January, 2020). https://www.arduino.cc

[20] Monsoon Solution Inc. assessed at January, 2020. Monsoon power monitor. (assessed at January, 2020). https://www.msoon.com/online-store/High-Voltage-Power-Monitor-Part-Number-AAA10F-p90002590

[21] Texas instruments. assessed at January, 2020. CC2500 Transceiver. (assessed at January, 2020). http://www.ti.com/product/CC2500

[22] Jabra. assessed at January, 2020. Jabra Elite 75t compatible with smartwatches. (assessed at January, 2020). https://www.jabra.com/supportpages/jabra-elite-75t/100-99090000-02/faq/What-tablet-smartphone-and-smartwatch-operating-systems-are-compatible-with-Jabra-SoundPlus#/

[23] Suman Jana, Sriram Nandha Premnath, Mike Clark, Sneha K Kasera, Neal Patwari, and Srikanth V Krishnamurthy. 2009. On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Proceedings of the Annual International Conference on Mobile Computing and Networking (MobiCom)*.

[24] Rong Jin and Kai Zeng. 2015. Physical layer key agreement under signal injection attacks. In *Proceedings of the Conference on Communications and Network Security (CNS)*.

[25] Ari Juels and Martin Wattenberg. 1999. A fuzzy commitment scheme. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*.

[26] Nikolaos Karapanos, Claudio Marforio, Claudio Soriente, and Srdjan Capkun. 2015. Sound-proof: usable two-factor authentication based on ambient sound. In *USENIX Security Symposium (USENIX Security)*.

[27] Behailu Kibret, Assefa K Teshome, and Daniel TH Lai. 2014. Human body as antenna and its effect on human body communications. *Progress In Electromagnetics Research* 148 (2014), 193–207.

[28] Behailu Kibret, Assefa K Teshome, and Daniel TH Lai. 2015. Characterizing the human body as a monopole antenna. *IEEE Transactions on Antennas and Propagation* 63, 10 (2015), 4384–4392.

[29] Arun Kumar, Nitesh Saxena, Gene Tsudik, and Ersin Uzun. 2009. A comparative study of secure device pairing methods. *Pervasive and Mobile Computing* 5, 6 (2009), 734–749.

[30] Jingzhen Li, Zedong Nie, Yuhang Liu, Lei Wang, and Yang Hao. 2017. Evaluation of Propagation Characteristics Using the Human Body as an Antenna. *Sensors* 17, 12 (2017), 2878–2893.

[31] Xiaopeng Li, Fengyao Yan, Fei Zuo, Qiang Zeng, and Lannan Luo. 2019. Touch Well Before Use: Intuitive and Secure Authentication for IoT Devices. In *Proceedings of the Annual International Conference on Mobile Computing and Networking (MobiCom)*.

[32] Hongbo Liu, Yang Wang, Jie Yang, and Yingying Chen. 2013. Fast and practical secret key extraction by exploiting channel response. In *Proceedings IEEE International Conference on Computer Communications (INFOCOM)*.

[33] Wei Liu, Merima Kulin, Tarik Kazaz, Adnan Shahid, Ingrid Moerman, and Eli De Poorter. 2017. Wireless technology recognition based on RSSI distribution at sub-Nyquist sampling rate for constrained devices. *Sensors* 17, 9 (2017), 2081–2104.

[34] Yanpei Liu, Stark C Draper, and Akbar M Sayeed. 2012. Exploiting channel diversity in secret key generation from multipath fading randomness. *IEEE Transactions on information forensics and security* 7, 5 (2012), 1484–1497.

[35] Youjing Lu, Fan Wu, Shaojie Tang, Linghe Kong, and Guihai Chen. 2019. FREE: A Fast and Robust Key Extraction Mechanism via Inaudible Acoustic Signal. In *Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*.

[36] Miklós Maróti, Branislav Kusy, Gyula Simon, and Ákos Lédeczi. 2004. The flooding time synchronization protocol. In *Proceedings of the International Conference on Embedded Network Sensor Systems (SenSys)*.

[37] Suhas Mathur, Robert Miller, Alexander Varshavsky, Wade Trappe, and Narayan Mandayam. 2011. Proximate: proximity-based secure pairing using ambient wireless signals. In *Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys)*.

[38] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. 2008). Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*.

[39] Markus Miettinen, N Asokan, Thien Duc Nguyen, Ahmad-Reza Sadeghi, and Majid Sobhani. 2014. Context-based zero-interaction pairing and key evolution for advanced personal devices. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*.

[40] Reinhold Müller and Petra Büttner. 1994. A critical discussion of intraclass correlation coefficients. *Statistics in medicine* 13, 23-24 (1994), 2465–2476.

[41] Wolfgang KH Panofsky and Melba Phillips. 2005. *Classical electricity and magnetism*. Courier Corporation.

[42] Polar. assessed at January, 2020. Pair Heart rate sensor with your watch. (assessed at January, 2020). https://support.polar.com/e_manuals/vantage-v/polar-vantage-v-user-manual-english/content/pairing-sensors.htm

[43] J Patrick Reilly. 2012. *Applied bioelectricity: from electrical stimulation to electropathology*. Springer Science & Business Media.

[44] Allied Market Research. assessed at January, 2020. Wearable Technology Market by Device, by Product type and Geography - Global Opportunity Analysis and Industry Forecast, 2014-2022. (assessed at January, 2020). https://www.alliedmarketresearch.com/wearable-technology-market

[45] Marc Roeschlin, Ivan Martinovic, and Kasper Bonne Rasmussen. 2018. Device Pairing at the Touch of an Electrode.. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*.

[46] Masoud Rostami, Ari Juels, and Farinaz Koushanfar. 2013. Heart-to-heart (H2H): authentication for implanted medical devices. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*.

[47] Dominik Schürmann and Stephan Sigg. 2011. Secure communication based on ambient audio. *IEEE Transactions on Mobile Computing* 12, 2 (2011), 358–370.

[48] 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 international conference on Mobile computing and networking (Mobicom)*.

[49] Qian Wang, Kaihe Xu, and Kui Ren. 2012. Cooperative secret key generation from phase estimation in narrowband fading channels. *IEEE Journal on selected areas in communications* 30, 9 (2012), 1666–1674.

[50] Stephen B Wicker and Vijay K Bhargava. 1999. *Reed-Solomon codes and their applications*. John Wiley & Sons.
[51] Alan Wolke. assessed at January, 2020. Calculating RF Power from IQ Samples. (assessed at January, 2020). https://www.tek.com/blog/calculating-rf-power-iq-samples
[52] Wei Xi, Xiang-Yang Li, Chen Qian, Jinsong Han, Shaojie Tang, Jizhong Zhao, and Kun Zhao. 2014. KEEP: Fast secret key extraction protocol for D2D communication. In *Proceedings of the IEEE International Symposium of Quality of Service*.
[53] Wei Xi, Chen Qian, Jinsong Han, Kun Zhao, Sheng Zhong, Xiang-Yang Li, and Jizhong Zhao. 2016. Instant and robust authentication and key agreement among mobile devices. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*.
[54] Weitao Xu, Chitra Javali, Girish Revadigar, Chengwen Luo, Neil Bergmann, and Wen Hu. 2017. Gait-key: A gait-based shared secret key generation protocol for wearable devices. *ACM Transactions on Sensor Networks* 13, 1 (2017), 6–33.
[55] 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 *Proceedings of the Conference on Embedded Network Sensor Systems (SenSys)*.
[56] 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 *Proceedings of the Annual International Conference on Mobile Computing and Networking (MobiCom)*.
[57] Chouchang Yang and Alanson P Sample. 2016. EM-ID: Tag-less identification of electrical devices via electromagnetic emissions. In *Proceedings of the IEEE International Conference on RFID*.
[58] Chouchang Jack Yang and Alanson P Sample. 2017. Em-comm: Touch-based communication via modulated electromagnetic emissions. In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (Ubicomp)*.
[59] Lin Yang, Wei Wang, and Qian Zhang. 2016. Secret from muscle: Enabling secure pairing with electromyography. In *Proceedings of the ACM Conference on Embedded Network Sensor Systems (SenSys)*.
[60] Kai Zeng, Daniel Wu, An Chan, and Prasant Mohapatra. 2010. Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*.
[61] Yao Zheng, Ming Li, Wenjing Lou, and Y Thomas Hou. 2012. Sharp: Private proximity test and secure handshake with cheat-proof location tags. In *Proceedings of the European Symposium on Research in Computer Security (ESCORICS)*.
[62] Thoams Guthrie Zimmerman. 1996. Personal area networks: near-field intrabody communication. *IBM systems Journal* 35, 3.4 (1996), 609–617.