TouchHBC: Touch-Based Human Body Communication via Leakage Current

Dian Ding, Hao Pan, *Member, IEEE*, Yongzhao Zhang, *Member, IEEE*, Yijie Li, Yu Lu, *Graduate Student Member, IEEE*, Yi-Chao Chen, *Member, IEEE*, and Guangtao Xue

***Abstract*—Wearable devices, including smartwatches, are increasingly popular among consumers due to their user-friendly services. However, transmitting sensitive data like social media messages and payment QR codes via commonly used low-power Bluetooth exposes users to privacy breaches and financial losses. This study introduces *TouchHBC*, a secure and reliable communication scheme leveraging a smartwatch's built-in electrodes. This system establishes a touch-based human communication system utilizing a laptop's leakage current. As the transmitting device, the laptop modulates this current via the CPU. Simultaneously, the smartwatch, equipped with built-in electrodes, captures the current traversing the human body and decodes it. The modulation and decoding processes involve techniques such as amplitude modulation, variational mode decomposition, channel estimation, and retransmission mechanisms. *TouchHBC* facilitates communication between laptops and smartwatches. Real-world tests demonstrate that our prototype achieves a throughput of 19.83 bps. Moreover, *TouchHBC* offers the potential for enhanced interaction, including improved gaming experiences through vibration feedback and secure touch login for smartwatch applications by synchronizing with a laptop. Furthermore, the system can be integrated with high-throughput communication protocols such as Bluetooth, enhancing its scalability while maintaining a strong foundation of security.**

***Index Terms*—Human body communication, laptop, leakage current, smart watch.**

I. Introduction

THE smartwatches, renowned for user-friendly services like health monitoring and sports management, saw global spending reach 31.3 billion in 2022 [1]. However, these devices predominantly rely on limited communication methods, with low-power Bluetooth being the most common. This protocol is vulnerable as attackers can simulate low-volume devices to circumvent its encryption and authentication processes, potentially leading to information theft [2]. Although some models support cellular networks, they tend to be more costly.

Researchers have explored enhancing the communication capabilities of smartwatches using bypass channels, such as electromagnetic signals [3], [4], [5], acoustic signals [4], [6], [7], vibration signals [8], [9], [10], and visual signals [11], [12], [13]. Visual communication, however, requires the screen to be aligned with the camera and keep the path unobstructed. Due to the non-directionality of acoustic signals, acoustic signal-based methods present the risk of information leakage. On the other hand, the magnetic signal-based communication system with devices such as laptops has a strict limitation on the communication distance (less than 3 cm); vibration communication is impractical for wearable devices due to its reliance on vibration propagation media such as wooden desks.

Unlike devices such as smartphones, smartwatches typically receive smaller texts, such as prompting messages from social software logged into other devices. In addition, with the growing popularity of mobile payments, smartwatches can synchronize QR codes from payment software for transactions. While these transmissions do not demand high communication rates, communication security is critical. Information leakage will bring non-negligible risks to the user's financial security and personal privacy.

This paper focuses on *developing a secure and efficient communication system utilizing smartwatch's inherent components*. Based on this, we propose a new smartwatch communication solution, *TouchHBC*, facilitating a touch-based human body communication system using the leakage current of a laptop. As shown in Fig. 1, a user simply needs to touch the metal casing of the laptop with the hand, enabling the smartwatch's built-in electrodes to capture the leakage current flowing through the human body. This system can synchronize social media messages and authenticate information like accounts, passwords, and payment QR codes without hindering the laptop's normal functions. The system offers a secure and reliable method for protecting sensitive user information. Moreover, it can be integrated with high-throughput communication systems, such as Bluetooth. By leveraging the enhanced security of *TouchHBC* for initial authentication and key exchange, and utilizing Bluetooth or similar protocols for higher data transfer rates in subsequent communications, it creates a secure, efficient, and

Received 4 November 2024; revised 24 April 2025; accepted 2 May 2025. Date of publication 12 May 2025; date of current version 3 September 2025. This work was supported in part by the National Natural Science Foundation of China under Grant 61936015 and Grant 6240071246, in part by the Natural Science Foundation of Shanghai under Grant 24ZR1430600, and in part by the Shanghai Key Laboratory of Trusted Data Circulation and Governance, and Web3. Recommended for acceptance by A. A Nayak. *(Corresponding authors: Yi-Chao Chen; Guangtao Xue.)*

Dian Ding, Hao Pan, Yu Lu, Yi-Chao Chen, and Guangtao Xue are with the School of Computer Science, Shanghai Jiao Tong University, Shanghai 200240, China, and also with the Shanghai Key Laboratory of Trusted Data Circulation and Governance, and Web3, Shanghai 200240, China (e-mail: dingdian94@sjtu.edu.cn; panh09@sjtu.edu.cn; yulu01@sjtu.edu.cn; yichao@sjtu.edu.cn; gt_xue@sjtu.edu.cn).

Yongzhao Zhang is with the Department of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: zhangyongzhao@uestc.edu.cn).

Yijie Li is with the School of Computing, National University of Singapore,, Singapore 117417 (e-mail: yijieli@nus.edu.sg).

Digital Object Identifier 10.1109/TMC.2025.3569282

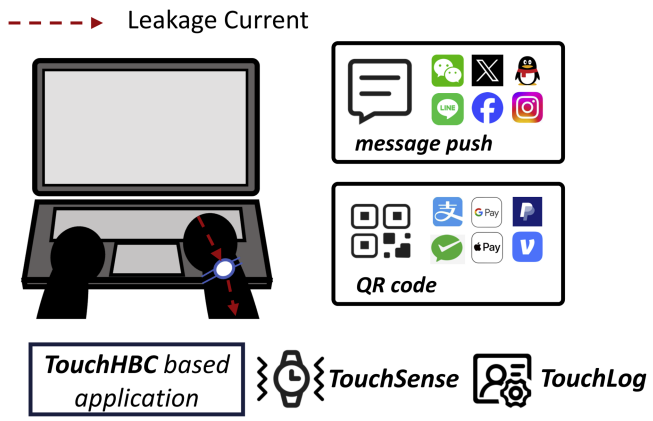


Fig. 1. Human body communication based on leakage current.

scalable communication system that balances both security and performance.

The leakage current, serving as the communication medium, originates from a safety capacitor in the laptop's adapter [14], [15] and varies with the laptop's operation [16], [17]. By modulating the high-consumption components of the laptop, such as the CPU, the system can modulate the spectral characteristics of the leakage current for data transmission. Recent studies [18], [19], [20] have demonstrated the feasibility of human-body communication between devices, where wearable devices with built-in electrodes can receive electrical signals coupled to the human body. Unlike other bypass signals, leakage currents transmit signals with the help of the user's torso and do not rely on the unobstructed channel required for visual communication. Moreover, human-body communication is more secure compared to acoustic signals. While the CPU's modulation process emits collectible magnetic signals in the near field, it predominantly facilitates short-range information theft (less than 3 cm) [3], [5], [21].

Although touch-based communication is limited to laptops with metal casings, such casings are preferred by consumers and major manufacturers for their durability and thermal properties. Major brands such as Apple, HP, Xiaomi, and Huawei have launched laptops with metal casings, which hold a significant market share. Meanwhile, electrodes are widely configured in wearable devices such as smartwatches, smart glasses, etc., enabling functionalities like heart rate monitoring [22], emotion recognition [23], and gesture recognition [24], [25]. Therefore, leakage current-based human communication systems have a wide range of applications.

In this study, we introduce a touch-based human body communication system *TouchHBC* that consists of two components: a transmitter and a receiver. The transmitter modulates the leakage current through the power consumption of the laptop CPU and employs a retransmission mechanism to improve the reliability of the communication. The receiver consists of leakage current pre-processing and decoding.

Developing a communication system based on leakage current imposed several challenges. First, we ensured the safety of the system regarding the ICNIRP guidelines [26]. The leakage current is well below the current strength limit and, therefore, does not cause discomfort or even harm to the human body. Second, it is complex to precisely control the leakage current using the operating system's job scheduling. We experimentally analyzed the characteristics of the leakage current and chose On-Off Keying modulation as the basic solution. Next, for the leakage current's low amplitude and fluctuating characteristics, we utilized signal processing techniques such as variational mode decomposition (VMD), spectral subtraction, and logarithmic short-time energy function (log-STE) to achieve stable decoding. Finally, considering the interference caused by other applications running in the operating system during the transmission process, which could misdirect the modulation of the leakage current. We adopted a retransmission mechanism based on CPU usage to retransmit the current packet when a corrupted symbol is detected.

We designed the *TouchHBC* prototype to implement the touch-based human body communication on a commercially available smartwatch (Apple Watch S6) [22]. Experimental results show that the prototype can achieve a throughput of 19.83 bps. The main contributions of this study can be summarized as follows:

- We explored the relationship between the leakage current and the working state of the laptop and verified the feasibility of a human-body communication system based on the leakage current.
- We built the transmitter by modulating the leakage current with the job scheduling of the operating system, On-Off Keying modulation, and using the retransmission mechanism to resolve interference from other applications running in the laptop;
- We screened the characteristic frequencies of laptop leakage currents by VMD and built the receiver using spectral subtraction, logarithmic short-time energy function to preprocess and decode the leakage current;
- We conducted the experiments in real-world environments, and the results demonstrated the feasibility of *TouchHBC* in human body communication.

The remainder of this paper is organized as follows: In Sec. II, we present the related works about the communication methods based on the bypass signals. In Sec. III, we introduce the principles of the leakage current from the laptop, verify the feasibility of the communication system, and describe the various noises present in the communication process. The design of the communication system is detailed in Sec. IV, including the transmitter and receiver. Sec. V outlines the experimental setup and experiments used to evaluate the proposed system. Sec. VI presents the potential application of *TouchHBC*. In Sec. VII, we discuss the limitations and the future work of *TouchHBC*. Finally, conclusions are presented in Sec. VIII.

II. Related Works

Recent researchers have developed numerous communication methods using various media to establish different communication systems based on bypass signals.

A. Communication Methods Based on Bypass Signals

1) Visual Communication: Communication methods based on the screen-camera channel can deliver information without affecting the viewing experience of the user [12], [13]. ChromaCode [12] improved the invisibility of the code by modifying the luminance of the uniform color space to adapt to pixel luminance and area texture and achieved full imperception. mQRCode [13] improved the security of QRCode by exploiting the nonlinearity of the spatial frequency of light. However, communication methods based on visual signals limit the application scenarios of the systems. Users have to keep good control of the camera and screen alignment and maintain obstacle-free access. TextureCode [11] utilized unobtrusive visual features such as edges and textures for communication and developed content adaptive coding techniques to improve the average throughput of existing methods.

2) Acoustic Communication: Endophasia [4] implemented silent speech commands on the smartphone using GSM signals. MagicInput [7] achieved handwriting recognition based on 1-dimensional tracking using acoustic signals. MuDis [27] proposed an air nonlinear-based multidirectional loudspeaker that utilizes parametric arrays to produce highly concentrated sound beams in multiple directions. VISAR [28] proposed a device-free virtual sound point projection system using air nonlinearity, enabling simultaneous tracking and sound point generation under acoustic augmented reality. Since sound propagation does not have a clear direction, it can pose a significant threat to the information security of communication in the effective communication range.

3) Magnetic Communication: MagneComm [3], [29] regulated the magnetic induction signal from the CPU and enabled near-field communication via magnetometer sensing on the device. MagView [4] achieved magnetic communication by changing the video packet type and reducing the quantization parameter to effectively control the CPU utilization of video decoding. MagAttack [5] and MagThief [21] used the built-in magnetic sensor of the smartphone to steal behavior information while using a laptop and a smartphone. However, research on magnetic communication has imposed strict limitations on the communication distance, requiring that the receiving device be placed in a specific location (less than $3cm$). In contrast, *TouchHBC* enables the communication between a laptop and a smartwatch through the simple action of touching the metal casing of a laptop.

4) Vibration Communication: Ripple [8] explored the possibility of using physical vibrations as a mode of wireless communication. VibWriter [9] used the built-in accelerometer of the smartphone to identify the handwriting on the same table. However, these methods rely on human bones [8], tables [9], and other vibration propagation media, thus limiting the application scenarios.

B. Human Capacitance

1) Human Body Communication: Human Body Communication (HBC) is an emerging communication technology that uses the human body as a medium for signal transmission, offering advantages such as low power consumption, high security, and stealthiness. Behailu Kibret [30] proposed a simplified equivalent circuit model that explores the calculation of electrode-skin contact impedance, providing a theoretical foundation for the design of body-area communication systems. mHBC [31] introduced a body capacitive communication technology based on magnetic resonance coupling, addressing the path loss issues encountered in traditional electric field-based body capacitive communication. EQS-HBC [32] proposed a concealed body area network technology based on capacitive quasi-static human body communication, successfully confining signals within the human body and reducing signal leakage through low-frequency, carrierless signal transmission. Sub-μWRComm [33] introduced a capacitive quasi-static human body communication system that ensures physical security while combining AES-256 encryption to provide mathematical security.

Meanwhile, researchers have further evaluated the communication performance of body communication systems. TouchCom [19], based on capacitive coupling technology, utilizes propagated current signals and has verified data transmission across the full body. Varga [20] proposed a wearable capacitive coupling communication system, assessing the impact of different frequencies, body positions, and user configurations on signal strength. Body-Guided Comm [18] implemented a security token based on human body communication from the customized smartwatch. Furthermore, BodyWire-HCI [34] introduced touch-based human body capacitive communication technology and validated the system's effectiveness in addressing signal leakage and short-range interference issues.

TouchHBC harnesses the leakage current from a laptop to enable communication between the human body and wearable devices such as smartwatches. The system does not rely on a specific signal generator, instead leveraging the inherent security and stealth advantages of human body capacitive communication systems. Using techniques like On-Off keying modulation, active retransmission, and channel estimation, the system performs encoding and decoding of the leakage current. By utilizing the leakage current from a laptop adapter as the transmission medium, communication is established through the user's touch with the laptop's metal casing, making the system more universally applicable. Additionally, the system can simultaneously capture human body capacitive characteristics and authenticate the user in real-time, further enhancing its security.

Despite its strong security performance, which makes it ideal for high-security applications such as secure login, payment systems, and device pairing, the system does have certain limitations. These include its dependence on metal-cased laptops, its charging status, and its unsuitability for long-duration transmission of large files. However, it provides a more universal solution compared to existing systems that rely on customized signal transmitters.

2) User Authentication: Recent research [35], [36], [37] has demonstrated the feasibility of using the body capacitance for user identification. Bioamp [35] used 12 pairs of electrodes on a wristband to read user capacitance information and transmitted the identity information from the touch point to the device when

the user taps the touch screen. Carpacio [36] reads the user's capacitive information using a pathway of electrode strokes on the touchscreen and car seat to authenticate the user. TouchAuth [37] explored the effect of ambient electric fields on the human body to identify users based on different electrical potentials on the surface of the body. Bioamp [38] developed a wrist-worn signal transmitter, enabling biometric data transmission between the user and mobile smart devices through finger touches on the screen, based on human body capacitive communication. Nguyen [39], on the other hand, achieved synchronized user feature extraction during the process of body communication. LeakPrint [15] used the leakage current of the laptop to extract the human capacitive feature for user identification.

3) Emotion or Gesture Recognition: Memento [23] enabled user emotion recognition on smart glasses using EEG sensors. HandSense [24] used the capacitive coupling between the electrodes on the fingertips of the glove to infer the real-time spatial relationships of the fingers and thus recognize fine and low-effort finger gestures. HandPad [40], [41] implemented a touch-based interactive interface on the back of the hand based on intrinsic capacitive modulation. LeakThief [17] validated the effect of the device operation state on the leakage current for laptop operation recognition.

III. Background

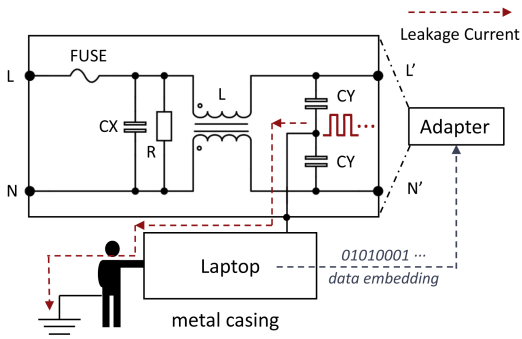
In this section, we outline the principles of leakage current in laptops and examine the feasibility of communication.

A. Leakage Current

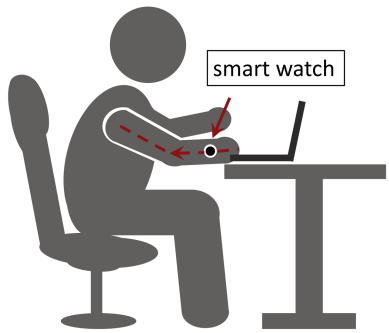
As a laptop with a metal casing (such as a MacBook) is connected to a power source, the metal casing of the laptop carries the leakage current from the adapter [14]. The leakage current comes from the Y-capacitor (safety capacitor) of the adapter, which is part of the EMI (electromagnetic interference) filtering circuit of the SMPS (switch mode power supply) to eliminate common mode interference and improve electromagnetic compatibility, and is usually configured on both the high and low voltage sides of the SMPS. As a common mode capacitor, grounding of the Y capacitor generates the leakage current [15], [42], [43]. The leakage current in the metal casing can be written as:

$$I = 2\pi f C_h U_h + k C_l U_l + I_{cmi} \tag{1}$$

where $2\pi f C_h U_h$ describes the leakage current generated by the capacitive coupling on the high-voltage side. f refers to the mains frequency, C_h indicates the size of the capacitor, and U_h indicates the voltage. On the low-voltage side, k is the leakage current constant (about 0.01 to 0.03 depending on the manufacturer), C_l and U_l denote the corresponding Y capacitor and voltage. The Y capacitors used in laptop adapters are typically around $5nF$. I_{cmi} represents the common mode interference (high-frequency harmonics) in the SMPS and contains a disturbance signal generated by the fluctuations of loading states [16], such as the high computing rate of the CPU. Therefore, a laptop powered by the 220 V/50 Hz mains generates roughly 0.3 mA of leakage current at the casing ($U_l = 12$ V).



(a) The leakage current from the adapter.



(b) The electrode-based system.

Fig. 2. Fundamental principle of leakage current.

B. Collection of Leakage Current

When using the laptop naturally, the user's hand is placed on the laptop in contact with the metal casing, and the feet are placed on the ground. The leakage current flows from the laptop through the human body and eventually into the ground, as shown in Fig. 2(a). The electrodes on the skin can perceive weak current flowing through the human body [18], [19], [20]. We, therefore, use the built-in electrode of the smartwatch to capture the leakage current, as shown in Fig. 2(b).

However, applying leakage current to the human body may involve certain safety risks, such as the current may induce localized thermal stresses in the human body and other hazards [19]. Therefore, we must ensure the safety of leakage current applications. The leakage current is about 0.3 mA, and the human body can be considered as a conductor with low impedance (a few $k\Omega$) [44]. Thus, the average SAR (Specific Energy Absorption Rate) of the human body is about 0.5 mW/kg.

To ensure the safety of the proposed system, we evaluate its compliance with international safety standards for leakage current and electromagnetic exposure. The leakage current of the system complies with IEC 60950-1, which limits the current on accessible metal parts to below 0.5 mA under normal conditions and 3.5 mA in the event of a fault, preventing electric shock or discomfort. Additionally, the system's electromagnetic exposure is well below the limits set by ANSI C95.1, which specifies a maximum specific absorption rate (SAR) of 0.4 W/kg, with the system's leakage current being only 0.5 mW/kg. Finally, the system adheres to ICNIRP guidelines, which set human

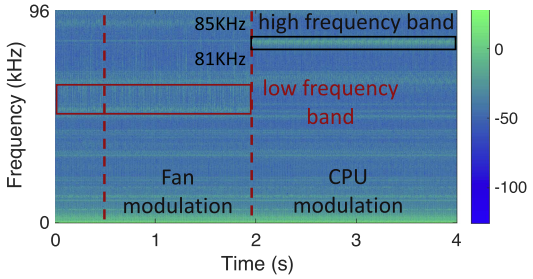
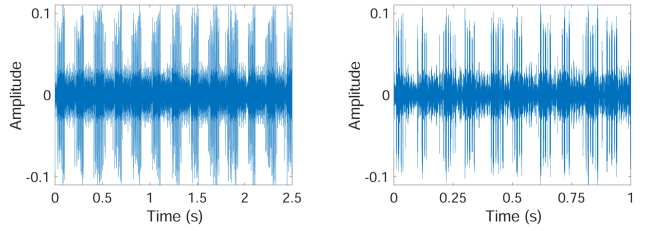


Fig. 3. Leakage current as CPU power consumption increases.



(a) Modulate the CPU at $10Hz$. (b) Modulate the CPU at $20Hz$.

Fig. 4. Leakage current under different modulation rates of the CPU.

exposure limits for current at 20 mA and SAR at 80 mW/kg, ensuring its safety in practical applications. Moreover, the effect of leakage current on the human body is lower than that of previous studies [19], [20]. Taken together, we can use the leakage current for communication, and the leakage current does not pose a safety risk to users.

C. Feasibility of Leakage Current Based Communication

As the leakage current is related to the working state of the laptop [16], we try to control the electronic units of the laptop (e.g., CPU, electronic fan, etc.) to modulate it. Compared to the CPU, units such as the electronic fan have a very weak effect on the working state of the laptop. For example, under normal operating conditions, the CPU draws between 20 W to 90 W of power. On the other hand, the electronic fan has a power of about $3W$.

We modulated the fan and CPU separately, and the leakage currents collected by the built-in electrode are shown in Fig. 3; we calculated the spectrogram of the leakage current using Short-Time Fourier Transform (STFT). In the preliminary experiments, we set the sampling rate of AD2 at 192 KHz to extend the bandwidth. We first increased the power consumption of the laptop fan and then the CPU. It can be seen that the leakage current is significantly enhanced when modulating the CPU to high power consumption, whereas modulating the fan has a negligible effect on the leakage current.

Therefore, we chose to modulate the CPU to verify the feasibility of communication based on leakage current. The advantage of using the CPU is that the CPU can be easily controlled by *loop* and *sleep* commands, which are available for most programming languages and operating systems. In addition, it is easy to monitor CPU usage in real time to estimate channel conditions [3].

It can be seen that the signal in the high-frequency band (black box in Fig. 3) of the leakage current is significantly increased (concentrated between 82 KHz and 84 KHz) when the CPU is at high power consumption. There is a corresponding attenuation of the signal in the low-frequency band (red box in Fig. 3).

To further validate the feasibility of communication based on leakage current, we attempted to modulate the power consumption of the laptop CPU at different frequencies (10 Hz and 20 Hz). We extracted the high-frequency band signal of the leakage current using a band-pass filter due to the high signal-to-noise ratio. As shown in Fig. 4, the leakage current can modulate at the same frequency. Therefore, a communication system based on leakage current is feasible, and it is possible to embed the data bits in the leakage current.

D. CPU Noise From Other Applications

During data transmission, we have to consider the situation that the CPU is used by the user and the operating system. The CPU usage by other applications can generate a corresponding noise in the leakage current. We attempted to characterize this type of noise by capturing the leakage current while the user is performing different applications, including watching videos (offline and online), browsing websites, playing games, using office software, and doing nothing at all. Fig. 5 presents the leakage current received while running different applications. When watching the video, we found that the resolution and codec have little effect on the leakage current. Therefore, we omitted this due to space limitations. The samples collected show that the noise generated by the CPU has a severe impact on data transmission when performing complex applications. A retransmission mechanism is necessary to improve the reliability of the data transmission. Besides, the operating system generates corresponding noise even if the user does not perform other operations.

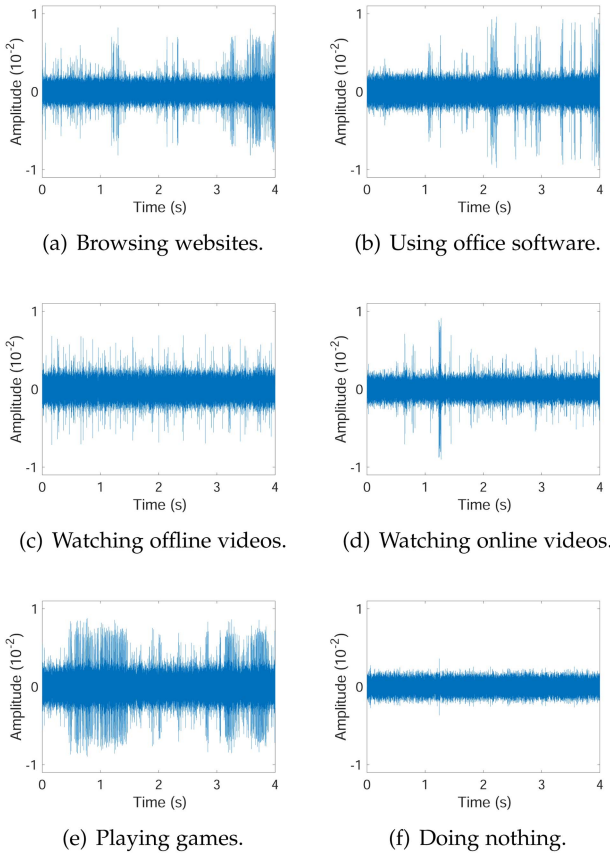
IV. System

A. System Overview

TouchHBC is designed and deployed on the smartwatch and laptop. Fig. 6 illustrates the system architecture, which comprises two parts: a transmitter and a receiver. We used the metal casing of the laptop as the transmitter and varied the power consumption of the CPU to modulate the leakage current. A retransmission mechanism can detect the corrupted symbol and retransmit the packet. At the receiver side, we perceived the leakage current with the built-in electrode of the smartwatch. Finally, we preprocessed and decoded the leakage current to extract the transmitted data. The details of each step in the two parts are detailed in this section.

B. Transmitter Design

Controlling the operating and idle states of the CPU can vary the power consumption of the CPU, thus enabling modulation



(a) Browsing websites. (b) Using office software. (c) Watching offline videos. (d) Watching online videos. (e) Playing games. (f) Doing nothing.

Fig. 5. The leakage current when performing different applications.

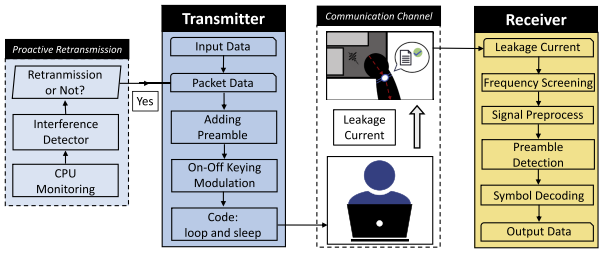
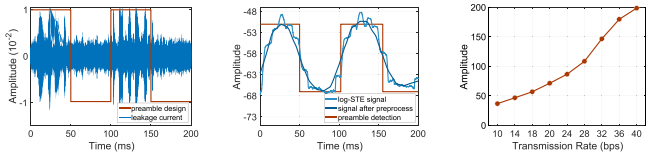


Fig. 6. System architecture of the *TouchHBC* system.

of the leakage current. We illustrate the modulation of data bits based on leakage current in the transmitter and introduce the retransmission mechanism to achieve reliable transmission under the noise caused by other applications.

1) Preamble: The insertion of a preamble at the beginning of a packet serves two main purposes. First, the preamble can synchronize the transmitter and receiver. *TouchHBC* sets a unique pattern of the leakage current for the preamble at the start of each data packet so that the system can use cross-correlation to locate the start time of the transmission. Second, the system can perform an initial estimation of the channel using the preamble. The range of change in the magnitude of the leakage current varies when communicating under different conditions. The receiver must be aware of the amplitude of the leakage current corresponding to the symbols 1 and 0 to decode the leakage current. As shown in Fig. 7, we take the example of the



(a) Preamble design. (b) Preamble detection. (c) The precision of modulation.

Fig. 7. Preamble design and detection: Fig. 7(a) The preamble is designed (red) and embedded in the leakage current (blue); Fig. 7(b) The leakage current is calculated the log-STE signal (light blue), processed with a mean window (dark blue) and transformed into a step signal for preamble detection (red); Fig. 7(c) The precision of leakage current control.

electrode-based communication system where the preamble is designed as a $[1, 0, 1, 0]$ sequence.

2) Modulation: We chose On-Off Keying for the modulation of the data bits. The choice of transmission rate depends on the precision of the leakage current control. Fig. 7(c) shows the leakage current control precision for different modulation frequencies. The control precision is defined as $P_{control} = \frac{1}{n}\sum_{i=1}^{n}(U_{real_i} - U_{desired_i})^2$, where $U_{desired}$ is the desired leakage current amplitude and U_{real} is the actual amplitude generated. Instead of setting the amplitude of the leakage current, we calculate the desired range of amplitude variation based on the preamble of each data packet. Besides, considering that the fluctuations of the leakage current interfere with the evaluation of the control accuracy, we evaluate the preprocessed signal. We test the control accuracy of the electrode-based system at different transmission rates, and a lower value for $P_{control}$ means that we can control the leakage current more precisely. From Fig. 7(c), we can see that the higher transmission rate reduces the precision of the control. Therefore, taking into account the results of the current control and the requirements for the communication rate, we choose a transmission rate of 20 bps.

The precision of the leakage current monitor: The transmitter requires continuous monitoring of the leakage current to ensure reliable data transmission. The monitor precision also constrains the choice of a transmission rate. However, it is difficult for a laptop to obtain its own leakage current directly. We use the CPU to modulate the leakage current, so we achieve an assessment of the communication quality by monitoring the usage of the CPU core: $P_{monitor} = |U_{current} - U_{monitor}|$, where $U_{current}$ is the actual received leakage current amplitude and $U_{monitor}$ is the CPU core usage monitored by the operating system (Fig. 7(c)). Therefore, combining the results of current control and monitoring and taking into account the requirements for the communication rate, we choose a transmission rate of 20 bps.

3) Proactive Retransmission: Considering that the transmitter (laptop) does not have access to its leakage current and does not have access to the reception condition of data packets from the receiver, we need a corruption detection mechanism at the transmitter to improve the reliability of the one-way communication. The main noise of the leakage current comes from other applications running in the system. Therefore, continuous monitoring of CPU usage allows the transmitter to assess whether the currently transmitted data packets are corrupted by noise. After a data packet has been sent, we determine whether

Algorithm 1: Proactive Retransmission.

Input: CPU usage
  while packet x is sent **do**
    $SymbolNoise_j \leftarrow \sum_{Core_i} Usage_i$
    $ReTran_x \leftarrow \sum_{Symbol_j} Rule(SymbolNoise_j)$
    if $ReTran_x = 0$ **then**
      Transmit packet $x+1$
    else
      Retransmit packet x
    end if
  end while

there is interference during transmission by monitoring the CPU. Suppose the usage of two or more non-transmitter CPU cores exceeds 30% . In that case, the transmitter will determine that there is interference with the symbol currently being sent, and the transmitter will re-transmit the entire data packet if there is a corrupted symbol in the packet. Algorithm 1 shows our active retransmission mechanism.

C. Receiver Design

The receiver performs preamble detection for synchronization and signal strength estimation. The signal is also preprocessed and demodulated to extract the data bits.

1) Frequency Screening: The modulation of leakage current with the CPU is mainly reflected in specific frequency bands, as shown in Fig. 3. However, the safety capacitors on the high and low-voltage sides of the adapter are affected by the current from the mains and the laptop. Besides, even for the same model of laptop, the capacitors will have different frequency characteristics due to process differences. Given that the frequency bands containing various high-frequency noises in the two states remain relatively stable, we employ the Variational Mode Decomposition (VMD) method [45] to extract different components of the leakage current corresponding to different CPU power consumption states.

The VMD decomposes the leakage current in two operating states into k components $(IMF_1, IMF_2, \ldots, IMF_k)$. These components are then grouped based on their center frequencies, as the frequency bands where the noise is located are relatively stable. Among these groups, the frequency bands where the amplitude is higher in the high power state than in the low power state can indicate the CPU operating state. To improve the signal-to-noise ratio, we select the frequency band with the largest amplitude difference, as shown in Fig. 8. It is noteworthy that for the same device, the system only needs to perform the VMD once to identify the characteristic frequency.

VMD separates the leakage current (S_{lc}) into k narrow band signals (u_k) with different values for the estimated central frequency ω_k and shifts each u_k signal from passband to baseband:

$$\min_{u_k(\omega_0)} \left\{ || \sum_k u_k(\omega_0) - S_{lc}(\omega_0)||_2^2 + \alpha \sum_k ||j\omega u_k(\omega_0 - \omega_k)||_2^2 \right\}$$

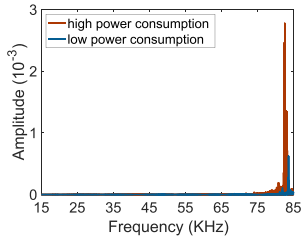


Fig. 8. FFT of different CPU power consumption.

$||j\omega u_k(\omega_0 - \omega_k)||_2^2$ is equal to $||j(\omega_0 - \omega_k)u_k(\omega_0)||_2^2$ in the frequency domain. The constrained variational model corresponding to the decomposition process of the response signal $S_{lc}(\omega)$ is as follows:

$$\min_{u_k(\omega_0)} \left\{ || \sum_k u_k(\omega_0) - S_{lc}(\omega_0)||_2^2 + \alpha \sum_k ||j(\omega_0 - \omega_k)u_k(\omega_0)||_2^2 \right\}$$
$$\text{s.t.} \sum_k u_k(\omega_0) = S_{lc}(\omega_0)$$

The optimal solution of the VMD can be obtained using the Lagrange multiplier, and the saddle point can be found using the ADMM algorithm [45].

2) Signal Preprocessing: Then, we use a band-pass filter to extract the signal in this band of the leakage current. Consider the noise present in the leakage current, even if the user is not running another application. We denoise the signal using spectral subtraction [46] based on the noise samples taken at idle moments as follows:

$$\|Y(k)\|^2 = \|S(k)\|^2 - \alpha \|N(k)\|^2 \tag{2}$$

where k represents the frequency range of the band, $S(k)$ and $N(k)$ represent filtered signal and noise signal respectively. α is the ratio of the signal strength of each frequency corresponding to symbol 0in the current channel to the signal strength of the noise sample. To reduce the effect of signal fluctuations, we set a processing window of 0.02 s and calculate the logarithmic short-time energy (log-STE) of the processing window as follows:

$$E(j) = 10\ log \sum_{i=j}^{j+0.02\times F_s} y(i)^2 \tag{3}$$

where $y(i)$ represents the leakage current signal and F_s represents the sampling rate of the receiver. To further smooth out the fluctuations in the signal, the signal was processed with a mean window of 0.02 s in duration.

3) Signal Decoding: After pre-processing, we can identify the symbols corresponding to different signal segments. First, we need to detect the preamble to synchronize the transmitter and receiver and calculate the signal amplitude corresponding to different symbols. Considering that there is an unstable delay in the change of the amplitude, which may affect the time duration corresponding to each symbol in the leakage current. As shown

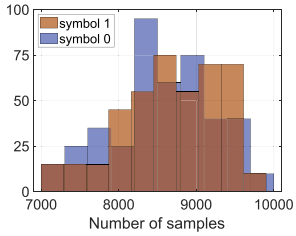
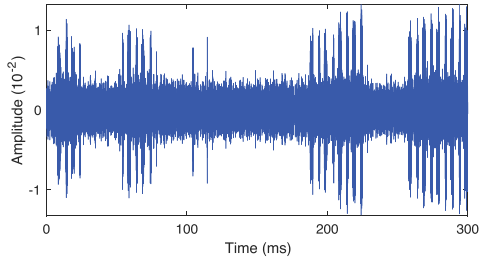
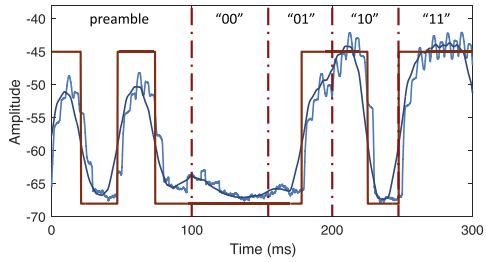


Fig. 9. Distribution of the sample sizes in symbols.



(a) Modulate the leakage current with the preamble and the binary sequence.



(b) Preprocess and decode the leakage current.

Fig. 10. Transmission example: Fig. 10(a) Modulate the leakage current at the transmitter; Fig. 10(b) Preprocess and decode the leakage current at the receiver.

in Fig. 9, with a transmission rate of 20 bps and a duty cycle of 0.5, we counted the number of samples corresponding to 800 symbols of 1 and 0. It can be seen that stable data bit embedding can be achieved based on the leakage current.

We further validated the system by two-bit binary coding. We added the preamble at the beginning of the example and modulated the leakage current for communication. The received leakage current is shown in Fig. 10(a), and the leakage current is preprocessed and decoded as shown in Fig. 10(b).

V. Evaluation

A. Evaluational Setup

The prototype of *TouchHBC* is adopted on a laptop (MacBook Pro) as a transmitter, as shown in Fig. 11. The laptop is placed on the desk and kept in charge. We verify the system in two real-world environments to test the effect of other electrical appliances in the circuit [47]: office (more electrical interference) and conference hall (less electrical interference).

We collected the leakage current using the built-in electrodes of the smartwatch (Apple Watch S6), which is worn on the left wrist, as shown in Fig. 11. Due to sensor permission issues,

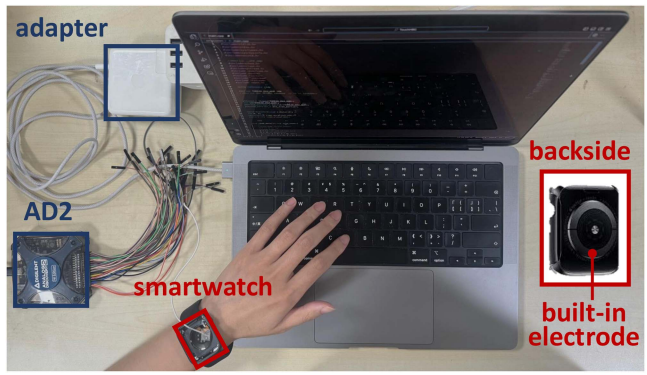
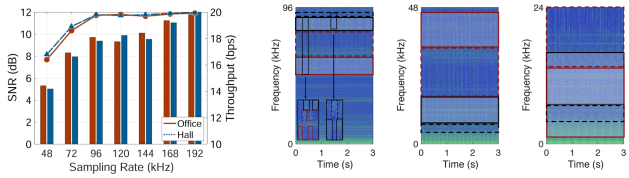


Fig. 11. Evaluational Setup of the *TouchHBC* system.



(a) Influence of sampling rate. (b) The aliasing effect of electrode-based.

Fig. 12. Evaluation of the *TouchHBC* system.

we used an external AD2 [48] to collect data. The laptop on the receiving side is kept ungrounded to simulate the scenario where a user wears a wearable device. The user can communicate with the smartwatch by touching the metal casing of the laptop. We set the sampling rate of the AD2 to 192 kHz. The transmission rate and duty cycle of the laptop leakage current are 20 bps and 0.5.

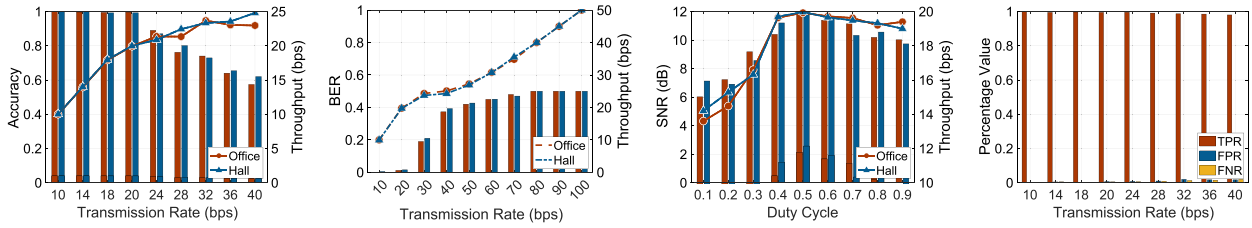
B. Micro Benchmark

1) Sampling Rate: In the feasibility experiment, the sampling rate of the AD2 was set to 192 KHz, and we were able to use the leakage current of the laptop for communication. We seek to sample the leakage current based on the aliasing effect [49], thus reducing the limitation of the sampling rate. The aliasing effect can be written as:

$$f_a = min|f_o - Nf_s| \tag{4}$$

where N is an integer, f_a, f_o, and f_s indicate the aliasing frequency, the signal frequency, and the sampling rate, respectively. For example, with the sampling rate of 48 KHz, the 80 KHz signal corresponds to an aliasing frequency of 16 KHz. In this experiment, we evaluate the throughput and signal-to-noise ratio of *TouchHBC* in two environments at various sampling rates from 48 KHz to 192 KHz. We keep the transmission rate and duty cycle as 20 bps and 0.5, and the performance of the system is shown in Fig. 12(a).

The throughput and signal-to-noise ratios are greater than 19.76 bps and $9.38dB$, respectively, and remain stable at sampling rates greater than 96 KHz. When the sampling rate is below this standard, both are significantly reduced. Since the



(a) Influence of transmission rate. (b) Influence of transmission rate. (c) Influence of duty cycle. (d) Corruption Detection.

Fig. 13. Evaluation of the *TouchHBC* system.

leakage current collected by the built-in electrode has different spectral characteristics and the bandwidths of both the high and low-frequency bands (red and black boxes) increase when the modulation rate (i.e., transmission rate) is $20Hz$, as shown in Fig. 12(b). Besides, the signals in the other frequency bands are also affected by CPU modulation, with the band in the red dashed box dominating. However, the signals in this band cannot clearly reflect the changes in CPU power consumption.

Fig. 12(b) presents the aliasing signals generated by the different frequency bands as the sampling rate decreases. When the sampling rate is 192 KHz, two frequency bands (red and black boxes) can be used for communication. The signal enhancement in the red box corresponds to low CPU power consumption, and the signal enhancement in the black box corresponds to high CPU power consumption. When the sampling rate is 96 KHz, we chose the signal band with lower noise interference (red box) for communication. When the sampling rate is reduced to 48 KHz, there is a significant overlap in the aliasing signals of the two frequency bands (red and black boxes). This part of the signal cannot be used for communication during the switching of CPU power consumption. We can only communicate via the frequency band in the red dashed box.

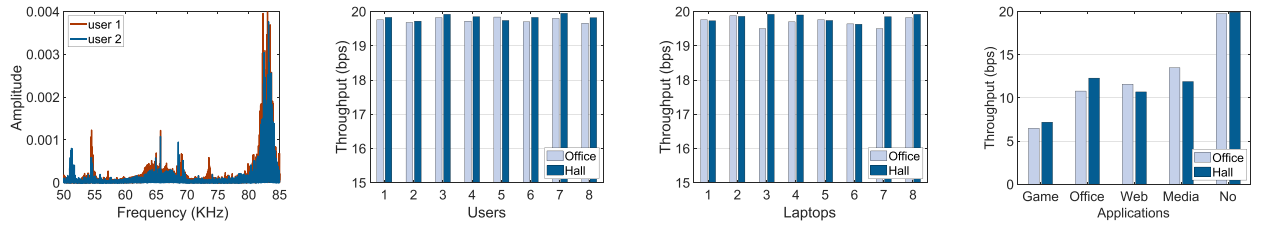
Therefore, when the sampling rate is higher than 96 KHz, the leakage current collected by the built-in electrode of the smartwatch has a high signal-to-noise ratio and throughput. In addition, even if the sampling rate is only 48 KHz, the system can still achieve a throughput of 16.8 bps, which proves the feasibility of applying *TouchHBC* to the communication between smartwatches and laptops. We will further discuss the sampling rate issue of wearable devices such as smartwatches in Sec.VI.

2) Transmission Rate: As a bypass signal generated during laptop operation, the leakage current is related to the operating state of the laptop [16]. However, similar to temperature variations, there is an upper limit to the frequency of switching between operating states [50]. We adjust the transmission rate of the leakage current to test the transmission rate of the system. We increased the transmission rate from 10 bps to 40 bps and measured the accuracy and throughput of the communication. We keep the sampling rate and duty cycle as 192 kHz and 0.5. As shown in Fig. 13(a), the transmission rate is increased from 10 bps to 20 bps, and the communication accuracy remains above 99.1%, meaning that throughout can be able to increase steadily. When the transmission rate is higher than 20 bps, the communication accuracy decreases significantly. Although throughout rises with the transmission rate, low accuracy can seriously affect the reliability of the communication system.

To further evaluate the system's performance at higher transmission rates, we conducted additional tests measuring throughput and bit error rate (BER) at transmission rates ranging from 40 bps to 100 bps. As shown in Fig. 13(b), when the transmission rate reaches 40 bps, the system's BER approaches 40% and continues to increase as the transmission rate rises. This is primarily due to the inherent latency in leakage current modulation based on CPU workload, which stems from the charging and discharging characteristics of the Y capacitor inside the adapter. The RC time constant of this capacitor prevents instantaneous changes in leakage current. Additionally, CPU workload modulation is subject to delays introduced by the operating system's scheduling and power management system (PMS), leading to millisecond-level response lag when adjusting power output. Consequently, when the transmission rate increases to 60 bps, brief transitions to low-power CPU states no longer effectively modulate the Y capacitor's behavior, causing the CPU-based modulation to fail.

To demonstrate practicality, we conducted experiments transmitting 64, 96, and $160-bit$ messages, corresponding to 8-, 12-, and 20-character strings, respectively. The average transmission times over 100 trials were 3.52 s, 5.29 s, and 8.77 s. These results suggest that *TouchHBC* can reliably transmit short messages within an acceptable delay.

3) Duty Cycle: The duty cycle reflects the number of samples occupied by the two different symbols (0 and 1). Whether a duty cycle is too short or too long can affect the decoding of the leakage current. We increase the duty cycle from 0.1 to 0.9 and keep the sampling rate and transmission rate at 192 KHz and 20 bps in the process. As shown in Fig. 13(c), with a duty cycle of 0.5, the system can achieve the maximum throughput and SNR. As the duty cycle increases or decreases, both throughout and SNR decrease, especially as the duty cycle decreases. As shown in Fig. 10(a), when the modulated leakage current is symbol 1, the current signal is sparse in the time domain. Therefore, at a lower duty cycle, the actual number of samples contained in symbol 1in the leakage current is lower, resulting in the corresponding signal being more likely to be swamped. The duty cycle above 0.5 can achieve better communication performance with throughput above 18.9 bps.



(a) Influence of users. (b) Influence of users. (c) Influence of laptops. (d) Influence of applications.

Fig. 14. Evaluation of the *TouchHBC* system.

To achieve an efficient and stable communication system based on the leakage current, we set the sampling rate, transmission rate, and duty cycle to 192 KHz, 20 bps, and 0.5, respectively.

C. Macro Benchmark

1) Corruption Detection: To further guarantee the reliability of *TouchHBC*, one-way communication requires the transmitter to accurately detect and retransmit the data bits. We set the sampling rate and duty cycle to 192 KHz and 0.5 and increased the transmission rate from 10 bps to 40 bps. The results are shown in Fig. 13(d). The true positive rate (TPR) represents the number of symbols that were corrupted and detected as corrupted versus the number of symbols that were corrupted. The false positive rate (FPR) represents the ratio of the number of symbols that were correct but detected as corrupted to the number of correct symbols. The False Negative Rate (FNR) represents the ratio of the number of symbols that were corrupted but detected as correct to the number of symbols that were corrupted. At transmission rates below 20 bps, the TPR is 99.5% or higher, while the FNR is 0.05% or lower, indicating that our corruption detection algorithm on the transmitter can correctly detect corrupted symbols.

2) Different Users: We invited 8 users to evaluate both prototypes of *TouchHBC*, with an average age of 25.6. Different biometric characteristics of the users, such as muscle, fat, and bone, can produce different capacitive characteristics [35], [36], [37]. When the leakage current flows through different users, the spectral characteristics of the signal collected by the electrode of the smartwatch may change. We compared the leakage currents collected from two users with the same electrode. During this process, we modulated the CPU to high power consumption and calculated the spectral information corresponding to the 1 s sample of leakage current using Fast Fourier Transform (FFT), as shown in Fig. 14(a). Although the capacitance characteristics vary between different users at specific frequencies, the signal in the high-frequency band of the leakage current is significantly enhanced when the laptop is in a high power consumption state.

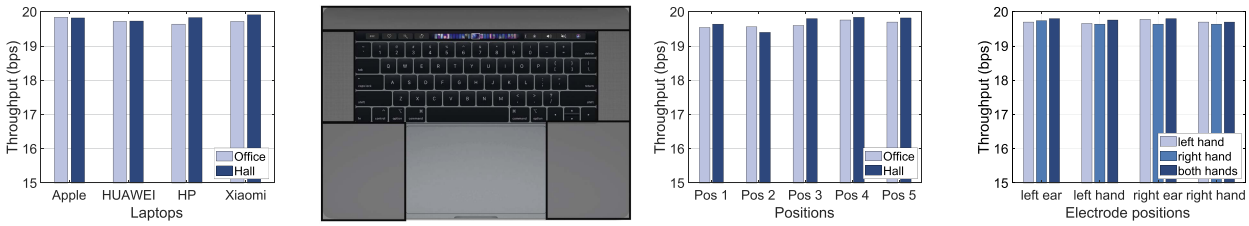
As shown in Fig. 14(b), the system maintains a throughput of approximately 19.74 bps and 19.81 bps for different users in two environments. This demonstrates the communication performance of *TouchHBC* is not influenced by the user.

3) Different Laptops: Leakage current comes from the safety capacitors in the adapter and may differ even between devices of the same model due to the process [51]. In this experiment, we evaluated *TouchHBC* on different laptops running Windows, Ubuntu, or MacOS, including three Apple laptops, two HP laptops, two HUAWEI laptops, and one XiaoMi laptop. We modulated the CPUs using loop and sleep instructions, so the different operating systems would not influence the communication performance. As shown in Fig. 14(c), the system can maintain throughputs of approximately 19.69 bps and 19.73 bps in two environments, indicating that the system can be deployed on most laptops with metal casings. Furthermore, given the excellent strength and thermal performance of the metal casing, companies such as Apple, HP, HUAWEI, and XiaoMi all produce laptops with a metal casing that is favored by a wide range of consumers. Therefore, we believe *TouchHBC* has high promotion prospects.

4) Other Applications: In addition to the active modulation of the leakage current by the CPU, other applications running on the laptop can also affect the leakage current collected by the electrode of the smartwatch. We selected common application operations of laptops, including browsing the website, using office software, watching videos, and playing games. To ensure the normal operation of other applications on the laptop while minimizing the impact on the communication system, a priority scheduling mechanism is employed. This mechanism assigns a lower priority to *TouchHBC* through the operating system's scheduling algorithm, ensuring the smooth operation of other critical programs.

Based on the corruption detection mechanism, the system excluded symbols disturbed by other applications during the communication. As shown in Fig. 14(d), we evaluated the throughput of the system under the influence of different applications. We tested 4 laptops with metal casing running different operation systems: Apple (Mac OS), HUAWEI (Windows), HP (Ubuntu), and XiaoMi (Windows), and presented the average throughput. It can be seen that running other applications can affect the throughput of *TouchHBC* and is related to the CPU usage of the application.

5) Laptop Battery: In addition to different applications running in the laptop, the state of the laptop's battery may also have an impact on the leakage current, as the charging current of the adapter varies depending on the state of the laptop's battery (i.e., fully charged or not fully charged). Therefore, we evaluated *TouchHBC* with the battery in various states of charge. As shown in Fig. 15(a), we validated the system on different laptops running different operation systems. As can be seen, the



(a) Influence of laptop battery. (b) Different positions of laptop. (c) Influence of touch mode. (d) Influence of electrode positions.

Fig. 15. Evaluation of the *TouchHBC* system.

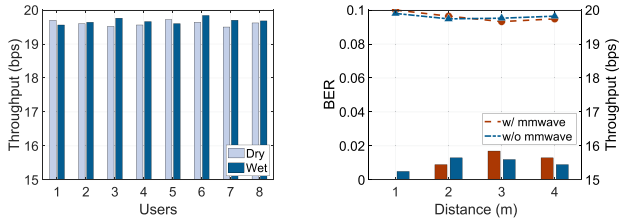
different states of the laptop battery do not affect the modulation of the leakage current.

6) Touch Modes: To avoid the influence of other variables on communication performance, we have restricted how the user touches the metal casing of the laptop in our previous experiments. For the electrode-based communication systems, the user touched the lower right corner of the C-side of the laptop using the palm of the right hand. First, we consider the effect of the different positions of the laptop on the leakage current, where we divide the C-side of the laptop into five positions as shown in Fig. 15(b). Even though the metal casing of the laptop has a very low resistance, the effect of this on the propagation of leakage current cannot be ignored.

To improve the practicality of the system, a fixed contact method may cause discomfort to the user. Therefore, we studied the different touching modes of the user, as different touching styles (e.g., finger, palm, or wrist) can change the area of the user with the laptop and thus affect the propagation of leakage current. Variables such as touch strength and angle, we do not discuss here as the effect of these factors is minimal in comparison. As shown in Fig. 15(c), we compared the differences between different touch positions of the system without the restriction of touch modes in the MacBook Pro running MacOS. As can be seen, *TouchHBC* is not affected by the different touch modes and can maintain the communication performance in all cases.

7) Electrode Positions: We proposed an electrode-based system to implement the communication system between the laptop and smartwatch via leakage current. In this experiment, we further verified the feasibility of communication between a laptop and other wearable devices. In addition to common wearable devices such as smartwatches and smart bracelets, smart glasses are also coming into the public eye. Different devices imply different contact positions of the device with the human body. Previous research [20] verified the feasibility of HBC at different locations on the human body. We attempted to verify the feasibility of communication between the laptop and different types of wearable devices, such as smartwatches (the built-in electrodes at the wrist) and smart glasses (the built-in electrode near the ear).

Furthermore, the electrode-based system has some special cases when the user touches the laptop. For example, when the user touches the laptop with his right hand while wearing the smartwatch in his left hand. In this experiment, we placed the



(a) Influence of hand moisture. (b) Influence of electromagnetic interference.

Fig. 16. Evaluation of the *TouchHBC* system.

electrodes on the wrist and behind the ear of the user, respectively, and evaluated the communication performance when the user touched the laptop with the right hand, left hand, or both hands, as shown in Fig. 15(d). The electrode position did not affect the system, and the communication system based on the leakage current is feasible for wearable devices with built-in electrodes, such as smart watches, bracelets, and glasses.

8) Hand Moisture: The skin's moisture level can affect the body's capacitance due to the electrode-skin coupling effect. This phenomenon primarily arises from changes in the skin's conductivity: when the skin is wet, its surface resistance decreases, and the contact impedance reduces, which could potentially affect the leakage current's transmission path. However, body capacitance is influenced not only by the skin's electrical properties but also by the dielectric properties of internal tissues. Therefore, variations in skin moisture may not significantly impact overall signal transmission. In this experiment, users touched the metal casing of the laptop in the same manner, first with wet hands and then with dry hands, to evaluate the influence on *TouchHBC*. As shown in Fig. 16(a), although wet skin may reduce the contact impedance, its effect on the leakage current is weak, and the impact on signal modulation and transmission stability is negligible.

9) Electromagnetic Interference: To evaluate the system's robustness against environmental interference, we simulated electromagnetic noise by deploying a millimeter-wave radar (MMWCAS-RF-EVM) near the user. The transmitter operated at a power level of 13 dBm with a frequency of 77 GHz to 80 GHz, containing 4 cascaded AWR2243 FMCW transceiver chips, while the system maintained a transmission rate of 20 bps. We then varied the distance between the millimeter-wave transmitter and the user. As the distance decreased from $4m$ to

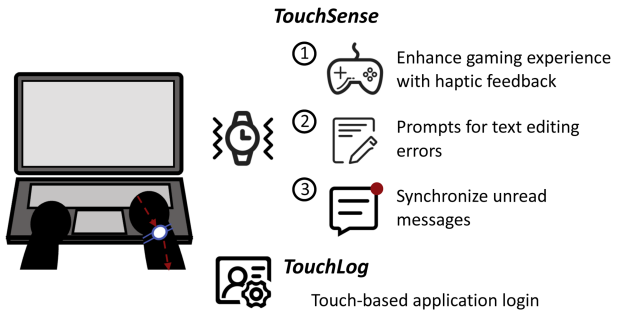


Fig. 17. Extended applications of *TouchHBC*.

$1m$, the signal-to-noise ratio (SNR) and throughput exhibited only a slight decline, indicating that the impact on communication was negligible (Fig. 16(b)). This is because common environmental electromagnetic interferences, such as Wi-Fi, typically operate at high frequencies significantly higher than the leakage current's frequency range. As a result, the system demonstrates strong robustness against electromagnetic interference from the surrounding environment.

VI. Application

In this section, we discuss several potential applications for *TouchHBC*. The system provides a safe and secure way to protect sensitive user information such as accounts and passwords. In addition, it facilitates the secure pairing of laptops with wearable devices such as smartwatches and smart glasses.

A. Touchsense

Vibration feedback is now widely used in smartphones, switch consoles, and other devices to provide more realistic and interesting interactions while playing games. However, it is difficult for laptops to provide electronic components such as motors for vibration feedback. With the built-in motors in smartwatches, we can expand smartwatches into vibration feedback modules for laptops.

The smartwatch can extract the data embedded in the leakage current and define different vibration methods to achieve different feedback. As shown in Fig. 17, *TouchSense* can achieve real vibration feedback in the process of playing games, prompting typos during text editing, as well as prompting messages without affecting the screen display when watching videos on full screen.

B. Touchlog

As the hardware performance of smartwatches improves, the types of services they support and the number of apps they offer show explosive growth. It is difficult for users to directly manage the numerous accounts and passwords, and these may contain private information, such as payment software and social software. Inspired by the Chrome browser to manage accounts and passwords for multiple websites, we can use a laptop to manage account passwords for different APPs in smartwatches and embed the information into leakage currents to log into different APPs in smartwatches and transmit information such as payment QR codes.

VII. Discussion

A. Limitation

1) Sampling Rate: Wearable devices such as smartwatches on the market are capable of achieving the sampling rate of 48 KHz [52]. Still, the built-in sensors, such as electrodes and accelerometers, are only capable of low sampling rates (below 1 KHz) [53]. First, there is a limitation of the sensor itself, whereas electrodes, in contrast to other sensors, have no limitation on the frequency of the signal collected. The second limitation comes from the kernel of the smart device, and recent research [54] has increased the sampling rate of the built-in accelerometer by adjusting the smartwatch kernel. Besides, as the demands of the application increase, hardware upgrades in smart devices, such as user demand for Hi-Fi. LG V60 [55] is capable of achieving a sampling rate of 192 KHz. We believe that the sampling rate limitation of wearable devices is surmountable. The communication between laptops and wearable devices via the leakage current could be widely used in the future.

2) Sensor Permission: Due to the lack of an API for accessing the built-in electrodes of the smartwatch, it is difficult for the system to collect the raw data directly from the sensor. In this paper, *TouchHBC* achieves communication with a laptop using an external AD2 [48] to read the leakage current captured by the built-in electrode of the smartwatch (Apple Watch S6). The laptop on the receiving side is kept ungrounded to simulate the scenario where a user wears a smartwatch and touches the laptop. We demonstrate through extensive experiments that the leakage current-based communication system is robust to variations in channel conditions, including different users and laptop models. Therefore, it is feasible to build a human capacitive communication system using a smartwatch to collect leakage current. Recent research also confirmed that the built-in electrodes of wearable devices can enable attractive applications in human-computer interaction, information security, and other areas such as emotion recognition [23], gesture recognition [24], [25], and user authentication [35], [36], [37]. Therefore, we believe that sensor permissions for wearable devices with built-in electrodes have an open trend in the future.

3) Transmission Rate: Although Bluetooth has been upgraded to enhance communication security, it remains challenging to completely eliminate the risk of information leakage. This continues to be a prevalent issue in the field of security research. The security vulnerabilities in Bluetooth protocols include attacks on the Bluetooth Passkey Entry protocol [56], Numeric Comparison [57], and Device Impersonation [58]. The continuous emergence of new attack methods highlights the ongoing challenge of optimizing and safeguarding Bluetooth protocols.

Physical-layer protections, on the other hand, offer a higher level of security. The human body communication system based on leakage current provides a more secure means of communication by restricting the range at which information can be intercepted, allowing data extraction only at distances of less than 3 cm [5]. This limitation makes leakage current-based communication systems less susceptible to remote interception,

thereby enhancing overall security compared to traditional wireless protocols.

While the data rate of *TouchHBC* is lower than that of conventional wireless technologies, it is not designed to replace high-speed communication. Rather, it serves as a complementary secure channel for the transmission of short, critical information, such as cryptographic keys, credentials, or pairing codes. In these scenarios, security takes precedence over bandwidth. Furthermore, the lower bandwidth is mitigated by the enhanced physical security and reduced attack surfaces provided by the system. *TouchHBC* offers a trade-off between speed and security, which is commonly seen in many security-critical systems (e.g., smart card readers, QR-based logins, etc.).

4) Application Scenarios: TouchHBC enables communication through the leakage current generated by the human body capacitance in a laptop, providing a more integrated and user-friendly solution. However, the system does have certain limitations in terms of application scenarios.

The primary limitation is its dependence on the conductivity of the metal casing. The system relies on the metal casing to facilitate the transmission of leakage current. Currently, major brands such as Apple, HP, Xiaomi, and Huawei have released laptops with metal casings, which dominate a significant portion of the market. Additionally, wearable devices like smartwatches and smart glasses are becoming increasingly popular among users. With the widespread adoption of metal-cased laptops and wearable devices, we believe that the *TouchHBC* system holds promising potential for future applications, offering a convenient and secure communication solution.

Secondly, the system relies on the laptop's connection to a power source to generate leakage current, which limits its portability and usability in environments without power. However, in most common usage scenarios, such as offices, homes, or other environments with access to power, the system's advantages in terms of security and ease of use can provide significant benefits. The ability to securely transmit data through the human body capacitance and the simplicity of the setup make it an attractive solution in environments where power is readily available.

Finally, the system requires users to maintain physical contact during communication. However, *TouchHBC* is not designed for large file transfers; instead, it is intended for short, secure exchanges, such as account credentials, pairing keys, or payment tokens. These interactions typically only require a few seconds of contact, which does not result in significant user fatigue. As such, *TouchHBC* provides a secure and reliable method for protecting sensitive user information, such as account details and passwords, ensuring that such data is transmitted safely in a convenient manner.

5) Information Security: During CPU modulation, the laptop generates a near-field magnetic field that can be captured by nearby devices within a short range (less than 3 cm [5]). For example, smartphones or other IoT devices equipped with magnetic sensors can detect fluctuations in the magnetic signal caused by CPU modulation, potentially leading to signal leakage and posing an information security risk [3]. However, the limited sensing range mitigates this risk, as any nearby smartphone or device would likely be noticeable to the user in close proximity. Additionally, the system employs On-Off Keying (OOK) modulation to embed data into the leakage current. While this method is simple, its robustness and security could be further optimized. To enhance transmission reliability, the system incorporates an active retransmission mechanism to minimize data loss during communication.

To address these limitations, the system could adopt advanced modulation techniques, such as hybrid coding schemes that combine Low-Density Parity-Check (LDPC) coding [59] with Advanced Encryption Standard (AES) [60], improving error correction, robustness, and security in signal transmission. Furthermore, during communication, the leakage current flowing through the human body can be leveraged to extract human capacitance characteristics for user authentication [15], [37], adding an additional layer of security to the system.

6) Personal Safety: To ensure the safety of the proposed system, we evaluate its compliance with established international safety standards for leakage current and electromagnetic exposure. First, we consider the safety of leakage current. IEC 60950-1 [61], established by the International Electrotechnical Commission (IEC), is an information technology (IT) equipment safety standard that explicitly regulates leakage current to prevent electric shock risks under both normal and fault conditions. According to this standard, the leakage current on the device's exterior or accessible metal parts must not exceed 0.5 mA under normal operating conditions and must remain below 3.5 mA in the event of a single fault (e.g., ground disconnection). This ensures that users will not experience an electric shock or discomfort when touching electronic devices in daily use. The leakage current of the laptop complies with these safety requirements.

Second, ANSI C95.1 [62], developed by the American National Standards Institute (ANSI) and the Institute of Electrical and Electronics Engineers (IEEE), sets safety limits for human exposure to radio frequency (RF) electromagnetic fields. The standard specifies that the specific absorption rate (SAR) of electromagnetic signals must not exceed 0.4 W/kg. The leakage current of the proposed system is 0.5 mW/kg, which is significantly below this threshold, ensuring compliance with international electromagnetic safety standards. Finally, the ICNIRP [26] defines human exposure limits across different frequencies, stating that the current should not exceed 20 mA, and the average SAR should remain below 80 mW/kg. Therefore, the proposed system meets the necessary safety requirements outlined in these standards, ensuring its safe use in practical applications.

B. Future Work

The operating state of devices in the mains may affect the signals in the power network [47]. Therefore, we try to mine information about the operating state of other devices from the leakage current for interactions or attacks between devices.

Besides, we verified the feasibility of receiving the leakage current at different positions of the human body in Experiment V-C7. In future work, we plan to validate *TouchHBC* on commercially available smart watches and smart glasses to

enable information push from a laptop to a wearable device. In addition, based on the perception of the human body capacitance by the leakage current [15], the communication system can provide user identification to the wearable device, thus further enhancing the security of the system.

Furthermore, we aim to explore hybrid architectures that integrate *TouchHBC* for secure key negotiation, followed by high-throughput communication using conventional wireless protocols such as Bluetooth. This approach has the potential to combine the strengths of both paradigms, leveraging the enhanced security of *TouchHBC* for initial authentication and key exchange, while utilizing the higher data transfer rates of Bluetooth or similar protocols for the subsequent communication. By incorporating these complementary technologies, we can create a secure, efficient, and scalable communication system that balances both security and performance.

VIII. Conclusion

In this paper, we propose a touch-based human communication system that leverages the built-in electrodes of a smartwatch. The system embeds information into the leakage current of a laptop to enable communication, with *TouchHBC* achieving a throughput of 19.83 bps between the laptop and smartwatch. The proposed system supports rich interaction features, such as vibration feedback and account management, which can be implemented on the smartwatch. Additionally, the system can be integrated with high-throughput communication protocols like Bluetooth, offering enhanced scalability while maintaining a robust security foundation.

References

[1] G. F. G. S. on Wearable Devices to Total 81.5 Billion in 2021, 2021. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2021-01-11-gartner-forecasts-global-spending-on-wearable-devices-to-total-81-5-billion-in-2021

[2] J. Wang, F. Hu, Y. Zhou, Y. Liu, H. Zhang, and Z. Liu, "Bluedoor: Breaking the secure information flow via BLE vulnerability," in *Proc. 18th Int. Conf. Mobile Syst., Appl., Serv.*, New York, NY, USA, 2020, pp. 286–298.

[3] H. Pan, Y.-C. Chen, G. Xue, and X. Ji, "Magnecomm: Magnetometer-based near-field communication," in *Proc. 23rd Annu. Int. Conf. Mobile Comput. Netw.*, 2017, pp. 167–179.

[4] J. Zhang, X. Ji, W. Xu, Y.-C. Chen, Y. Tang, and G. Qu, "Magview: A distributed magnetic covert channel via video encoding and decoding," in *Proc. IEEE Conf. Comput. Commun.*, 2020, pp. 357–366.

[5] Y. Cheng et al., "Magattack: Guessing application launching and operation via smartphone," in *Proc. 2019 ACM Asia Conf. Comput. Commun. Secur.*, New York, NY, USA, 2019, pp. 283–294.

[6] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "Diskfiltration: Data exfiltration from speakerless air-gapped computers via covert hard drive noise," 2016, *arXiv:1608.03431*.

[7] H. Pan, Y.-C. Chen, Q. Ye, and G. Xue, "Magicinput: Training-free multi-lingual finger input system using data augmentation based on mnists," in *Proc. 20th Int. Conf. Inf. Process. Sensor Netw.*, 2021, pp. 119–131.

[8] N. Roy and R. R. Choudhury, "Ripple II: Faster communication through physical vibration," in *Proc. 13th USENIX Symp. Netw. Syst. Des. Implementation*, Mar. 2016, pp. 671–684.

[9] D. Ding, L. Yang, Y.-C. Chen, and G. Xue, "Vibwriter: Handwriting recognition system based on vibration signal," in *Proc. 18th Annu. IEEE Int. Conf. Sens., Commun., Netw.*, 2021, pp. 1–9.

[10] D. Ding, L. Yang, Y.-C. Chen, and G. Xue, "Handwriting recognition system leveraging vibration signal on smartphones," *IEEE Trans. Mobile Comput.*, vol. 22, no. 7, pp. 3940–3951, Jul. 2023.

[11] V. Nguyen et al., "High-rate flicker-free screen-camera communication with spatially adaptive embedding," in *Proc. 35th Annu. IEEE Int. Conf. Comput. Commun.*, 2016, pp. 1–9.

[12] K. Zhang et al., "Chromacode: A fully imperceptible screen-camera communication system," in *Proc. 24th Annu. Int. Conf. Mobile Comput. Netwo.*, 2018, pp. 575–590.

[13] H. Pan, Y.-C. Chen, L. Yang, G. Xue, C.-W. You, and X. Ji, "MQRCode: Secure QR code using nonlinearity of spatial frequency in light," in *Proc. 25th Annu. Int. Conf. Mobile Comput. Netw.*, New York, NY, USA, 2019.

[14] M. M. Jha, K. B. Naik, and S. P. Das, "Estimation of optimum value of Y-capacitor for reducing EMI in switch mode power supplies," *Elect. Power Qual. Utilisation, J.*, vol. 15, no. 2, pp. 47–50, 2009.

[15] D. Ding, L. Yang, Y.-C. Chen, and G. Xue, "Leakage or identification: Behavior-irrelevant user identification leveraging leakage current on laptops," *Proc. ACM Interactive, Mobile, Wearable Ubiquitous Technol.*, vol. 5, no. 4, pp. 1–23, Dec. 2022.

[16] W. Meng, "Touch current analysis for power supplies designed for energy efficient regulations," in *Proc. 2011 IEEE Symp. Product Compliance Eng. Proc.*, 2011, pp. 1–6.

[17] D. Ding, Y.-C. Chen, X. Ji, and G. Xue, "Leakthief: Stealing the behavior information of laptop via leakage current," in *Proc. 20th Annu. IEEE Int. Conf. Sens., Commun., Netw.*, 2023, pp. 186–194.

[18] V. Nguyen et al., "Body-guided communications: A low-power, highly-confined primitive to track and secure every touch," in *Proc. 24th Annu. Int. Conf. Mobile Comput. Netwo.*, New York, NY, USA, pp. 353–368.

[19] V. Varga, G. Vakulya, A. Sample, and T. R. Gross, "Enabling interactive infrastructure with body channel communication," *Proc. ACM Interactive, Mobile, Wearable Ubiquitous Technol.*, vol. 1, no. 4, pp. 1–29, Jan. 2018.

[20] V. Varga, M. Wyss, G. Vakulya, A. Sample, and T. R. Gross, "Designing groundless body channel communication systems: Performance and implications," in *Proc. 31st Annu. ACM Symp. User Interface Softw. Technol.*, 2018, pp. 683–695.

[21] H. Pan et al., "MagThief: Stealing private app usage data on mobile devices via built-in magnetometer," in *Proc. 18th Annu. IEEE Int. Conf. Sens., Commun., Netw.*, 2021, pp. 1–9.

[22] Apple Watch Series-7, 2021. [Online]. Available: https://www.apple.com/apple-watch-series-7/

[23] S. Jiang, Z. Li, P. Zhou, and M. Li, "Memento: An emotion-driven lifelogging system with wearables," *ACM Trans. Sensor Netw.*, vol. 15, no. 1, pp. 1–23, Jan. 2019.

[24] V. Nguyen, S. Rupavatharam, L. Liu, R. Howard, and M. Gruteser, "Handsense: Capacitive coupling-based dynamic, micro finger gesture recognition," in *Proc. 17th Conf. Embedded Netw. Sensor Syst.*, 2019, pp. 285–297.

[25] D. J. Matthies, C. Weerasinghe, B. Urban, and S. Nanayakkara, "Capglasses: Untethered capacitive sensing with smart glasses," in *Proc. Augmented Hum. Conf.*, 2021, pp. 121–130.

[26] A. Ahlbom et al., "Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz)," *Health Phys.*, vol. 74, no. 4, pp. 494–521, 1998.

[27] Y. Li et al., "MUDIS: An audio-independent, wide-angle, and leak-free multi-directional speaker," in *Proc. 30th Annu. Int. Conf. Mobile Comput. Netw.*, 2024, pp. 263–278.

[28] J. Zhou et al., "Visar: Projecting virtual sound spots for acoustic augmented reality using air nonlinearity," *Proc. ACM on Interactive, Mobile, Wearable Ubiquitous Technol.*, vol. 8, no. 3, pp. 1–30, Sep. 2024.

[29] G. Xue, H. Pan, Y.-C. Chen, X. Ji, and J. Yu, "Magnecomm : Near-field electromagnetic induction communication with magnetometer," *IEEE Trans. Mobile Comput.*, vol. 22, no. 5, pp. 2789–2801, May 2023.

[30] B. Kibret, M. Seyedi, D. T. Lai, and M. Faulkner, "Investigation of galvanic-coupled intrabody communication using the human body circuit model," *IEEE J. Biomed. Health Inform.*, vol. 18, no. 4, pp. 1196–1206, Jul. 2014.

[31] J. Park and P. P. Mercier, "Magnetic human body communication," in *Proc. 37th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, 2015, pp. 1841–1844.

[32] D. Das, S. Maity, B. Chatterjee, and S. Sen, "Enabling covert body area network using electro-quasistatic human body communication," *Sci. Rep.*, vol. 9, no. 1, 2019, Art. no. 4160.

[33] S. Maity et al., "Sub-μWRComm: 415-nW 1–10-kb/s physically and mathematically secure electro-quasi-static HBC node for authentication and medical applications," *IEEE J. Solid-State Circuits*, vol. 56, no. 3, pp. 788–802, Mar. 2021.

[34] S. Maity, D. Yang, S. S. Redford, D. Das, B. Chatterjee, and S. Sen, "Bodywire-HCI: Enabling new interaction modalities by communicating strictly during touch using electro-quasistatic human body communication," *ACM Trans. Comput.- Hum. Interact.*, vol. 27, no. 6, pp. 1–25, 2020.

[35] C. Holz and M. Knaust, "Biometric touch sensing: Seamlessly augmenting each touch with continuous authentication," in *Proc. 28th Annu. ACM Symp. User Interface Softw. Technol.*, New York, NY, USA, 2015, pp. 303–312.
[36] E. J. Wang, J. Garrison, E. Whitmire, M. Goel, and S. Patel, "Carpacio: Repurposing capacitive sensors to distinguish driver and passenger touches on in-vehicle screens," in *Proc. 30th Annu. ACM Symp. User Interface Softw. Technol.*, 2017, pp. 49–55.
[37] 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 *Proc. 25th Annu. Int. Conf. Mobile Comput. Netwo.*, New York, NY, USA, 2019, pp. 1–16.
[38] C. Holz and M. Knaust, "Biometric touch sensing: Seamlessly augmenting each touch with continuous authentication," in *Proc. 28th Annu. ACM Symp. User Interface Softw. Technol.*, 2015, pp. 303–312.
[39] V. Nguyen et al., "Body-guided communications: A low-power, highly-confined primitive to track and secure every touch," in *Proc. 24th Annu. Int. Conf. Mobile Comput. Netw.*, 2018, pp. 353–368.
[40] Y. Lu et al., "Handpad: Make your hand an on-the-go writing pad via human capacitance," in *Proc. 37th Annu. ACM Symp. User Interface Softw. Technol.*, 2024, pp. 1–16.
[41] Y. Lu, D. Ding, R. Wang, and G. Xue, "HCMG: Human-capacitance based micro gesture for VR/AR," in *Proc. Companion ACM Int. Joint Conf. Pervasive Ubiquitous Comput.*, 2024, pp. 766–770.
[42] S. Westerlund and L. Ekstam, "Capacitor theory," *IEEE Trans. Dielectr. Electr. Insul.*, vol. 1, no. 5, pp. 826–839, Oct. 1994.
[43] D. Ding, Y. Li, H. Pan, Y. Lu, Y.-C. Chen, and G. Xue, "Enable touch-based communication between laptop and smartwatch," in *Proc. Companion ACM Int. Joint Conf. Pervasive Ubiquitous Comput.*, 2024, pp. 4–8.
[44] J. P. Reilly, *Applied Bioelectricity: From Electrical Stimulation to Electropathology*. Berlin, Germany: Springer, 2012.
[45] K. Dragomiretskiy and D. Zosso, "Variational mode decomposition," *IEEE Trans. Signal Process.*, vol. 62, no. 3, pp. 531–544, Feb. 2014.
[46] S. Kamath and P. Loizou, "A multi-band spectral subtraction method for enhancing speech corrupted by colored noise," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, 2002, vol. 4, pp. IV-4164–IV-4164.
[47] Z. Shao, M. Islam, and S. Ren, "Your noise, my signal: Exploiting switching noise for stealthy data exfiltration from desktop computers," *Proc. ACM Meas. Anal. Comput. Syst.*, vol. 4, pp. 1–39, 2020.
[48] Digilent AD2, 2021. [Online]. Available: https://digilent.com/shop/analog-discovery-2-100ms-s-usboscilloscope-logic-analyzer-and-variable-power-supply/
[49] Y. Chen, W. Gong, J. Liu, and Y. Cui, "Fine-grained ultrasound range finding for mobile devices: Sensing way beyond the 24 kHz limit of built-in microphones," in *Proc. 2017 IEEE Conf. Comput. Commun. Workshops*, 2017, pp. 845–850.
[50] M. Guri, M. Monitz, Y. Mirski, and Y. Elovici, "BitWhisper: Covert signaling channel between air-gapped computers using thermal manipulations," in *Proc. IEEE Comput. Secur. Found. Symp.*, 2015, pp. 276–289.
[51] Y. Cheng, X. Ji, J. Zhang, W. Xu, and Y.-C. Chen, "DemiCPU: Device fingerprinting with magnetic signals radiated by CPU," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, 2019, pp. 1149–1170.
[52] G. Reyes et al., "Whoosh: Non-voice acoustics for low-cost, hands-free, and rapid input on smartwatches," in *Proc. ACM Int. Symp. Wearable Comput.*, 2016, pp. 120–127.
[53] Z. Ba et al., "Learning-based practical smartphone eavesdropping with built-in accelerometer," *NDSS Symp.*, vol. 2020, pp. 1–18, 2020.
[54] G. Laput, R. Xiao, and C. Harrison, "Viband: High-fidelity bio-acoustic sensing using commodity smartwatch accelerometers," in *Proc. 29th Annu. Symp. User Interface Softw. Technol.*, 2016, pp. 321–333.
[55] SoundGuys, "Best smartphones for audio," 2020. [Online]. Available: https://www.soundguys.com/best-smartphones-for-audio-16373/
[56] M. K. Jangid, Y. Zhang, and Z. Lin, "Extrapolating formal analysis to uncover attacks in bluetooth passkey entry pairing," *NDSS*, vol. 2023, pp. 1–18, 2023.
[57] M. Von Tschirschnitz, L. Peuckert, F. Franzen, and J. Grossklags, "Method confusion attack on bluetooth pairing," in *Proc. IEEE Symp. Secur. Privacy*, 2021, pp. 1332–1347.
[58] D. Antonioli, "Bluffs: Bluetooth forward and future secrecy attacks and defenses," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2023, pp. 636–650.
[59] S. Ten Brink, G. Kramer, and A. Ashikhmin, "Design of low-density parity-check codes for modulation and detection," *IEEE Trans. Commun.*, vol. 52, no. 4, pp. 670–678, Apr. 2004.
[60] D. Selent, "Advanced encryption standard," *Rivier Academic J.*, vol. 6, no. 2, pp. 1–14, 2010.
[61] IEC 60950-1:2005, 2005. [Online]. Available: https://www.iecee.org/certification/iec-standards/iec60950-12005
[62] ANSI/IEEE C95.1, 2019. [Online]. Available: https://www.atecorp.com/compliancestandards/ieee/ieee-c95-1

Dian Ding received the PhD degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China, in 2023. He is currently a postdoctoral Researcher with the Department of Computer Science and Engineering, Shanghai Jiao Tong University. He has authored or coauthored more than 20 papers in international conferences and journals, including ACM MobiCom, EuroSys, UIST, UbiComp, SenSys, IEEE INFOCOM, *IEEE Transactions on Mobile Computing*, and *IEEE/ACM Transactions on Networking*. His research interests include mobile computing and distributed systems. His work has been recognized with nominations for WCAI 2021 Young Outstanding Paper Award and ACM UbiComp 2024 MIMSVAI Workshop Best Paper Award.

Hao Pan (Member, IEEE) received the bachelor's degree from the Yingcai Honors College, University of Electronic Science and Technology of China, Chengdu, China, in 2016, and the PhD degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2022. His research interests include networked systems and span the areas of wireless communication and sensing, human–computer interaction, and computer vision.

Yongzhao Zhang (Member, IEEE) received the BS degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2018, and the PhD degree from Shanghai Jiao Tong University, Shanghai, China, in 2023. He is currently an assistant professor with the School of Computer Science and Engineering, University of Electronic Science and Technology of China. His research interests include wireless networks and security, mobile sensing, and underwater Internet of Things (IoT).

Yijie Li received the bachelor's degree from the Hongyi Class of Computer Science, Wuhan University, Wuhan, China, in 2018, and the PhD degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China, in 2024. He is currently a postdoctoral research fellow with the School of Computing, National University of Singapore, Singapore. His research interests focus on novel mobile sensing, human-computer interaction, and IoT security.

Yu Lu (Graduate Student Member, IEEE) received the BEng degree major in IS from Shanghai Jiao Tong University, Shanghai, China, in 2022. Since 2022, he has been working toward the PhD degree with Mobile Sensing and Interaction Laboratory, Shanghai. His research interests include the Internet of Things (IoT), Big Data, mobile computing, and security.

Yi-Chao Chen (Member, IEEE) received the BS and MS degrees from the Department of Computer Science and Information Engineering, National Taiwan University, Taipei, Taiwan, in 2004 and 2006, respectively, and the PhD degree in computer science from the the University of Texas at Austin, Austin, TX, USA, in 2015. He was with Huawei Future Network Theory Laboratory, Hong Kong, where spent a year as a Researcher. He then worked as a Co-founder with Hauoli LLC. In 2018, he joined the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China, as a tenure-track assistant professor. His research interests include networked systems and span the areas of wireless networking, network measurement and analytics, and mobile computing.

Guangtao Xue received the PhD degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China, in 2004. He is currently a professor with the Department of Computer Science and Engineering, Shanghai Jiao Tong University. His research interests include wireless networks, mobile computing, and distributed computing. He is a member of the IEEE and the IEEE Communication Society.