Key Generation for Internet of Things: A Contemporary Survey

WEITAO XU, City University of Hong Kong, Hong Kong SAR China
JUNQING ZHANG, University of Liverpool, UK
SHUNQI HUANG, Shenzhen University, China
CHENGWEN LUO, Shenzhen University, China
WEI LI, The University of Sydney, Australia

Key generation is a promising technique to bootstrap secure communications for the Internet of Things (IoT) devices that have no prior knowledge between each other. In the past few years, a variety of key generation protocols and systems have been proposed. In this survey, we review and categorise recent key generation systems based on a novel taxonomy. Then, we provide both quantitative and qualitative comparisons of existing approaches. We also discuss the security vulnerabilities of key generation schemes and possible countermeasures. Finally, we discuss the current challenges and point out several potential research directions.

CCS Concepts: • **Computer systems organization → Sensors and actuators**; • **Human-centered computing → Ubiquitous and mobile devices**; • **Security and privacy → Network security**.

Additional Key Words and Phrases: IoT, Key generation, Device pairing, Authentication

ACM Reference Format:
Weitao Xu, Junqing Zhang, Shunqi Huang, Chengwen Luo, and Wei Li. 2020. Key Generation for Internet of Things: A Contemporary Survey. *ACM Comput. Surv.* 1, 1, Article 1 (January 2020), 35 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

The last decades have witnessed the rapid growth of the Internet of Things (IoT) from a theoretical concept to a reality. A wide range of smart IoT devices have penetrated into our daily life. These devices can be broadly classified into three classes: portable/wearable devices such as smart watch and Fitbit, smart home/building devices such as Amazon Alexa and Google Assistant, general network devices such as Wi-Fi router and 5G end device. We are entering a new era where every thing/device will be connected together to form a smart world. Fig. 1 shows the growth of the number of IoT devices in the past decade as well as the predictions of the growth until 2025. It is estimated that the number of IoT devices connected to the Internet will surge to 75 billion by 2025 [116].

With the prevalence of IoT devices, secure device-to-device (D2D) communication is becoming more and more crucial because IoT devices often need to be paired together for the purpose of file transferring, synchronisation, and data sharing. Cryptographic key agreement is a fundamental requirement for secure D2D communications to achieve confidentiality [135]. Key generation, also called key agreement or establishment, refers to the process of generating

Authors' addresses: Weitao Xu, weitaoxu@cityu.edu.hk, City University of Hong Kong, Hong Kong SAR China; Junqing Zhang, University of Liverpool, UK, junqing.zhang@liverpool.ac.uk; Shunqi Huang, Shenzhen University, China, huangshunqi2019@email.szu.edu.cn; Chengwen Luo, Shenzhen University, China, chengwen@szu.edu.cn; Wei Li, The University of Sydney, Australia, weiwilson.li@sydney.edu.au.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2018 Association for Computing Machinery.
Manuscript submitted to ACM

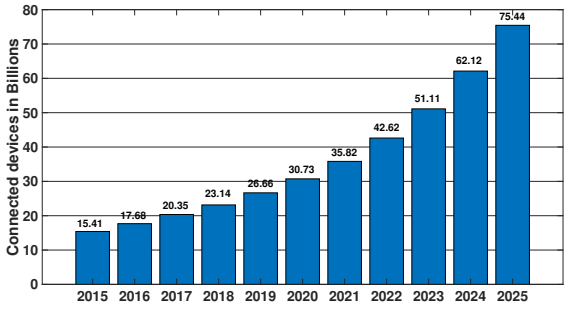


Fig. 1. Number of IoT devices from 2015 to 2025 [116].

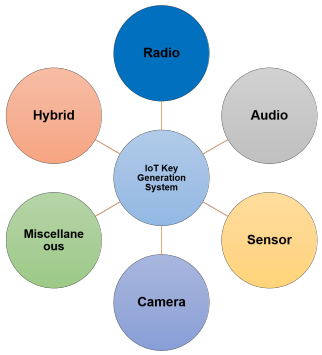


Fig. 2. Taxonomy of our survey.

the same cryptographic key between two devices that have no prior secret. Alternative terminologies, such as device association, device pairing, or device binding, have the same meaning but are adopted by other literature [19]. Essentially, the underlying concept remains the same, i.e., to establish a secure communication channel among multiple IoT devices. In the following, we will use key generation, key agreement, key establishment and device pairing interchangeably in spite of the minor differences in some contexts [30]. Broadly speaking, key generation can be divided into two classes: authenticated key generation and unauthenticated key generation. In the authenticated key generation, one of the communication parties can verify the identity of the other device. While in the unauthenticated key generation, they simply generate a pair of key without authenticating each other.

Secure key establishment between two parties can be completed by public key cryptography (PKC) [114]. PKC schemes require a public key infrastructure (PKI) and are computationally expensive as they usually rely on complicated mathematical problems, e.g., discrete logarithm algorithm. Hence, PKC solutions may not be suitable to resource-constrained devices operating in pervasive environments due to both the absence of PKI and the required high computational overhead. Another solution is pre-shared key (PSK) scheme. However, PSK scheme lacks scalability which makes them inappropriate especially in the cases of large-scale sensor deployments and mobile scenarios.

The resource constraints and the absence of common trust infrastructure motivate researchers to seek alternative key generation approaches by exploring the features and functions integrated in IoT devices themselves. Existing key generation systems are based on a common principle: if multiple devices can observe a common signal (e.g, sound, temperature, or motion) from a specific channel, their observations can be used as materials to generate random keys. Prior researches have yielded a massive number of technically sound systems relying on various auxiliary out-of-band (OOB) channels such as visual channel [82], acoustic channel [107] and sensing channel [81].

The concept of IoT device pairing is not new and there already exist several literature surveying this area [30, 84, 110, 155]. However, with the advent of new wireless technologies such as Long Range communication technology (LoRa) and new hardware such as bio-sensors, many novel secure device pairing schemes have been proposed recently [97, 101, 104, 142]. Unfortunately, these surveys do not capture the recent advances in IoT device pairing. Therefore, the aim of our survey is to bridge this gap in the current literature. Moreover, the taxonomies used in previous surveys have some weaknesses. For example, Shahab et al. [84] categorised device pairing systems into three classes: weak, public, and private channels. However, the difference between these three categories are unclear because bias is unavoidable when using subjective metrics. In a more recent survey [30], Fomichev et al. analysed secure pairing schemes from three aspects: physical channel, human-computer interaction (HCI) and application classes. However, when we review the literature we find this systematisation is not easy to use in practice because a large portion of systems actually lie in

Table 1. Comparison of prior surveys/reviews with this survey (❍–none, ◗–moderate, ●–comprehensive).

	Year	Radio	Audio	Sensor	Camera	Miscellaneous	Hybrid	Security Analysis	Performance Comparison
[61]	2009	◗	◗	❍	◗	❍	❍	❍	●
[84]	2014	●	●	◗	●	❍	❍	●	❍
[20]	2014	●	●	●	●	❍	❍	❍	●
[110]	2015	◗	❍	❍	❍	❍	❍	❍	❍
[155]	2016	●	❍	❍	❍	❍	❍	❍	❍
[30]	2017	●	●	●	●	◗	❍	❍	❍
Ours	2020	●	●	●	●	●	●	●	●

the intersection of different categories. For instance, many schemes belonging to application classes in [30] also involve physical channel and HCI.

In comparison with prior works, our survey presents two novel contributions. First, our survey complements the previous surveys in terms of recent key generation approaches and systems. Second, our survey summarises and compares existing works in a new perspective. Specifically, we use a novel taxonomy to organise this survey, as shown in Fig. 2. The rationale for introducing this new taxonomy is to classify approaches by the hardware used by different approaches, contrasting previous surveys that were organised from the perspective of HCI [20, 30]. We argue that a classification based on the hardware interface is an important complement to previous survey works, as the fundamental difference of materials or information used to generate keys is they originate from different hardware interfaces such as radio, audio, and sensor. Table 1 compares the coverage of our survey against previously published ones. For topics well studied in the prior works, we only provide a brief summary in this paper for the benefit of the readers and for the sake of completeness, while the details are referred to those references for additional information.

The rest of the paper is organised as follows. In Section 2, we classify the state-of-the-art IoT devices by examining their features and functions and derive a taxonomy based on the analysis. Section 3 surveys representative key generation systems based on the used hardware and technologies. Then, a comparison of existing key generation schemes is given in Section 4. Section 5 reviews the security vulnerabilities of key generation schemes and discusses countermeasures. Current challenges and future directions are discussed in Section 6. Finally, Section 7 concludes the paper.

2 A BRIEF SURVEY OF IOT DEVICES

In this section, we present a brief survey of existing IoT devices/products. The aim of this section is not to provide a comprehensive analysis and categorisation of IoT devices, but to give readers a general idea regarding the features and resources that can be provided by different types of devices. For a comprehensive survey of IoT systems, the readers are referred to [6, 108].

IoT devices are essentially smart devices that support internet connectivity and are able to communicate over the internet with other devices and provide a user with remote access to control the device according to their needs. These devices generally integrate sensing, processing, and communication to facilitate autonomous awareness of the context of a device. Wireless connectivity is introduced to allow sharing such context among IoT networks. Based on application scenarios, we classify the commonly used IoT devices into three categories: mobile/wearable devices, smart home/building devices, and network devices. Table 2 presents the details of devices discussed in this paper.

Portable/wearable devices. Portable/wearable devices are smart electronic devices that are worn close to and/or on the surface of the skin or carried by a user. These devices are often called wearables for short and examples of such devices include smart glass, smart watch, and smart clothing. Here we also classify mobile phone into this category

Table 2. A summary of common IoT devices.

Category	Subcategory	Example products	Common Features	Application Scenarios
Portable/Wearable Devices	Smart phone	Apple phone Samsung phone Huawei phone	Sensors: camera, accelerometer, gyroscope, geomagnetic sensor, barometer, proximity sensor, ambient light sensor Wireless Connectivity: Bluetooth 5.0, Wi-Fi, GPS, LTE, GSM, NFC, iBeacon Microphone, Speaker: Yes	Health monitoring Activity detection Localisation Entertainment AR/VR
	Smart watch	Apple Watch Huawei Watch	Sensors: accelerometer, gyroscope, geomagnetic sensor, optical heart rate sensor, ambient light sensor, air pressure sensor, capacitive sensor, Wireless Connectivity: Bluetooth, BLE, NFC, GPS Microphone, Speaker: Yes	
	Smart glass	Google Glass Vuzix Smart Glass Magic Leep One	Sensors: camera, accelerometer, gyroscope, geomagnetic sensor, multi-touch gesture touchpad, IR eye tracking, depth sensor Wireless Connectivity: Bluetooth, Wi-Fi Microphone, Speaker: Yes	
	Smart clothing	Mercury Intelligent Jacket Nadi X Yoga Pants	Sensors: accelerometer, internal and external temperature sensor Wireless Connectivity: Bluetooth Output component: a smart thermostat, haptic feedback (vibration) Microphone, Speaker: No	
	Smart shoes	Nike Adapt BB 2.0 Shoes	Sensors: accelerometer, gyroscope, capacitive touch controller Wireless Connectivity: BLE Microphone, Speaker: No	
Smart home/Building Devices	Smart speaker	Google Assistant Amazon Echo	Sensors: No Wireless Connectivity: Bluetooth 5.0, Wi-Fi Microphone, Speaker: Yes	Surveillance Intrusion detection Environmental monitoring Smart meter Building automation Smart parking
	Smart display	Google Nest Hub Lenovo Smart Display	Sensors: capacitive touch screen, ambient light sensor Wireless Connectivity: Bluetooth 5.0, Wi-Fi Microphone, Speaker: Yes	
	Smart bulb	Philips Hue Lifx Z LED Strip	Sensors: No Wireless Connectivity: Bluetooth, Wi-Fi, ZigBee Microphone, Speaker: No	
	Miscellaneous	Bosch BCC50 Google Nest Secure System	Sensors: thermostat, motion sensor, vibration sensor, humidity sensor, PIR sensor, proximity sensor, etc Wireless connectivity: Bluetooth, Wi-Fi, NFC, ZigBee, Cellular Microphone, Speaker: depending on specific device	
Network Devices	Wi-Fi	Google Nest Wifi TP-Link Deco X60	Sensors: No Wireless connectivity: Yes, depending on the specific communication technology Microphone, Speaker: No	Smart city Smart farm Smart transportation
	ZigBee	Sangsung SmartThings Hub Hive Hub		
	LoRa	Arduino MKR WAN 1300 Cisco IR 910		
	Bluetooth	Wink Hub		
	RFID	LANMU RFID Card Reader		
	5G	HTC 5G Hub		

because many so-called mobile devices are not mobile themselves, it is the host that carries these devices is mobile. As shown in Table 2, these devices are usually equipped with a variety of sensors that can monitor, detect, analyse and transmit information about user's context such as location, motion, heart rate etc. They also have built-in microphone, speaker and different wireless connectivity functionalities. Therefore, compared to the other two types of devices, wearable devices can provide more information to generate keys. Indeed, a large portion of existing key generation systems are based on wearable devices [51, 109, 112, 138, 141, 145].

Smart home/building devices. There are a variety of smart home/building devices ranging from smart sensors (e.g., proximity sensor and vibration sensor) to smart appliances (e.g., Bosch BCC50). Although several smart home applications have built-in sensors, a large majority of them do not have sensors, microphone and speaker. Key generation systems for smart home/building devices usually exploit the common context information that can be measured by heterogeneous sensors [38, 83].

Network devices. Network devices are physical devices that are needed on a computer network to communicate and interact with hardware. Network device usually do not have built-in sensors, microphone and speaker. Moreover, each network device is usually equipped with single wireless communication interface. Key generation systems for these devices are usually based on wireless channel physical layer characteristics such as Received Signal Strength Indicator (RSSI), Channel State Information (CSI) etc.

The variety of IoT devices compounds the complexity of key generation systems for two reasons. First, the hardware capabilities available, such as wireless radio interfaces, sensing functionality, and computing capacity, vary greatly across different platforms as can be seen in Table 2. Secondly, the patterns of interaction between the systems and between human operators and machines have become more complex. Therefore, to identify existing studies and encourage further work on this subject, we are motivated to propose a new taxonomy to systematise information in this area. As shown in Fig. 2, we categorise existing key generation systems based on the adopted hardware interface. The reason of introducing this new taxonomy is that the hardware interface manifests the fundamental difference between different material/information used to generate keys. With the proposed taxonomy, users can easily identify the most suitable method for their application scenarios. For example, for wearable devices which are equipped with rich sensors, users can select Inertial Measurement Unit (IMU) sensor-based or audio-based key generation techniques. For network devices which are equipped with wireless modules only, the radio-based key generation system is the best option.

3 KEY GENERATION SYSTEMS FOR IOT DEVICES

In this section, we survey the key generation systems for IoT devices based on the taxonomy in Fig. 2. Specifically, we discuss key generation systems based on the hardware or the channel used to collect information for generating keys. We divide them into six categories: radio, audio, IMU sensor, camera, miscellaneous hardware and hybrid approaches. We will survey the representative works of each category in turn.

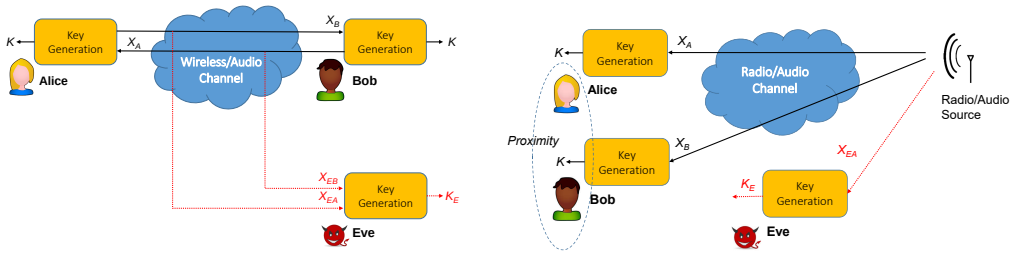
3.1 Overview of Threats

Before discussing key generation systems, we first give a brief overview of potential attacks. This is because security systems always come along with attacks. With attacks in mind, readers can better understand the vulnerabilities of different approaches. Without loss of generality, we adopt the notations commonly used in this field: Alice and Bob represent two legitimate devices that aim to generate the same key, and Eve represents an attacker trying to obtain the same key via different types of attacks. The goal of Eve is always to undermine the device pairing system and she can launch attacks on authenticity, confidentiality and integrity. The formulation of a detailed adversary model is beyond the scope of this article. In this paper, we focus on some common attacks such as Man-in-the-Middle (MITM) attack, replay attack, eavesdropping attack. These attacks will have different degrees of threats to different schemes described below. A detailed discussion of attacks and countermeasures is given in Section 5.

3.2 Radio

Radio communication modules have been pre-installed in many consumer electronics. For example, all the smartphones have cellular, Wi-Fi and Bluetooth connectivities. Fitbits are usually equipped with Bluetooth. Most of the IoT wireless techniques operate at the unlicensed industrial, scientific, and medical (ISM) band. For instance, Wi-Fi runs at 2.4 GHz or 5 GHz; ZigBee and Bluetooth work at 2.4 GHz; LoRa operates at the sub GHz and its frequency plan depends on the regions, e.g., 868 MHz in EU and 902-928 MHz in the US.

Radio communications are used to exchange information between devices. At the same time, they can also be exploited for generating secret keys. Key generation with radio communications has received extensive interests in the last decades [155, 160]. Depending on the locations of Alice and Bob, radio-based key generation can be categorised into channel reciprocity-based and proximity-based schemes, as illustrated in Fig. 3. In the channel reciprocity-based scheme, Alice and Bob wish to generate the same key from their common wireless channel and prevent the key secure



(a) Channel reciprocity-based (b) Proximity-based

Fig. 3. System model for radio and audio-based key generation.

against eavesdroppers. On the other hand, in the proximity-based scheme, Alice and Bob are located very close to each other and receive signals from a common third user.

3.2.1 Principle. Radio-based Key generation, also referred to as physical layer key generation, relies on three principles, namely temporal variation, channel reciprocity and spatial decorrelation, which will be explained in detail below.

- *Temporal Variation.* The signal propagation is subject to reflection, refraction and scattering and hence the channel effects will be temporally varying in a mobile environment. These effects will be unpredictable and their randomness can be extracted as cryptographic keys.
- *Channel Reciprocity.* When the uplink and downlink transmissions operate at the same carrier frequency, the channel effects at both ends of the link will be reciprocal. This feature ensures that Alice and Bob can obtain highly correlated channel measurements and generate the same keys.
- *Spatial Decorrelation.* When Eve is located more than half-wavelength away from either of the legitimate users, she experiences uncorrelated channel effects according to the communication theory. This property is essential to guarantee that the keys generated by Alice and Bob cannot be guessed by Eve hence the keys are secure.

The radio-based key generation principles have been modelled and analysed in [156] and experimentally validated in [162]. There has been extensive work evaluating these principles, e.g., by using Wi-Fi [162], ultrawideband (UWB) [37].

3.2.2 Protocol. As shown in Fig. 4, a typical channel reciprocity-based key generation protocol consists of the following four steps: channel probing, quantization, information reconciliation and privacy amplification.

Channel Probing. This step requires bidirectional transmissions between Alice and Bob. In particular, Alice first transmits a signal to Bob who will measure the channel information via some channel parameters, e.g., RSSI, channel impulse response (CIR) and channel frequency responses (CFR). Bob will then reply a signal to Alice who will measure the same parameter. This completes a pair of measurements. Alice and Bob keep probing until they collect sufficient measurements, X_A and X_B, respectively.

The selection of the channel parameter depends on the adopted wireless technologies. While RSSI is almost provided in all the wireless standards, CIR and CFR are only available in wideband systems. For example, UWB systems are able to estimate the CIR [12, 133] while IEEE 802.11 Orthogonal Frequency-Division Multiplexing (OFDM) can obtain the CFR [72, 135, 154, 159].

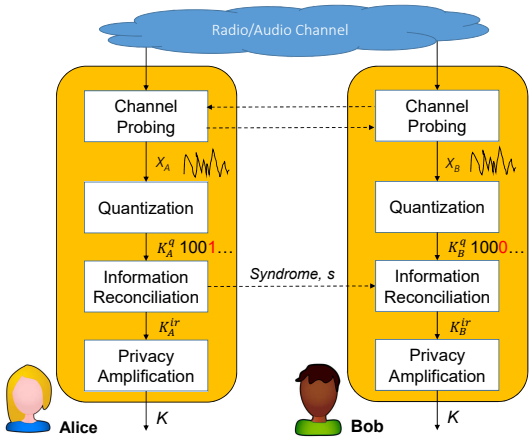


Fig. 4. Work flow of channel reciprocity based key generation.

Quantization. As cryptographic algorithms require binary input, the analog measurements, X_u, should be converted into binary sequence K_u, which can be completed by comparing X_u to thresholds and assign bit sequences. The thresholds can be determined based on the mean value and variance as well as cumulative distribution functions (CDF).

Mean and standard deviation-based quantizer [46, 80] chooses the thresholds based on the mean value and the variance of the channel measurements. Specifically, the bit assignment can be completed as follows:

$$K_u(i) = \begin{cases} 1, \text{ when } X_u(i) > \mu_u + \alpha \times \sigma \\ 0, \text{ when } X_u(i) < \mu_u - \alpha \times \sigma \end{cases} \tag{1}$$

where μ_u is the mean value and σ is the standard deviation. This quantizer is very easy to implement. However, it is not robust to burst error.

CDF-based quantizer [88] calculates the thresholds based on the CDF of the channel measurements, $F(x)$. CDF-based quantizer can be implemented as a multi-bit quantizer. The thresholds can be calculated as

$$\eta_n = F^{-1}(\frac{n}{2^{QL}}) \tag{2}$$

where $n = 1, 2, ..., 2^{QL} - 1$, QL is the quantization level, and $F^{-1}(\cdot)$ is the inverse function of the CDF. We can assign Gray code b_n to the range $[\eta_{n-1}, \eta_n]$. Finally, the keys can be generated as

$$K_u(i, QL) = b_n, \text{when } \eta_{n-1} \leq X_u(i) < \eta_n. \tag{3}$$

Compared to the mean and standard deviation-based quantizer, the CDF quantizer can generate multiple bits from one measurement, which is more efficient. However, it is more complex as it requires to calculate the CDF and its inverse function. A detailed comparison between different quantizers can be found in [35, 152].

Information Reconciliation. There will probably be key mismatch between Alice and Bob after the quantization, due to the channel variation, hardware asymmetry and noise. The mismatch can be quantified by the key disagreement rate (KDR), given as

$$KDR = \frac{\sum_i |K_A(i) - K_B(i)|}{l_K} \tag{4}$$

where l_K is the key length.

Information reconciliation is thus employed to make Alice and Bob agree on the same keys, which can be achieved using error correction codes (ECCs). Secure sketch [24] is a popular algorithm, which has been widely used in the wireless key generation to correct the mismatch [129, 158, 159]. Alice first randomly selects a codeword c from the codeset of ECC. She calculates the syndrome by $s = c \oplus K_A$ and sends it to Bob. Assuming Bob receives the syndrome successfully without error, he then obtains $c_B = s \oplus K_B$. If the hamming distance between c_B and c is within the correction capacity of the ECC, Bob will be able to decode c from c_B. Finally, Bob can calculate $K_B^{ir} = c \oplus s$, which should be the same as the key generated at Alice.

Privacy Amplification. There will be information leaked to eavesdroppers during the information reconciliation, hence privacy amplification is adopted to mitigate the threat of information leakage. In the literature, this is done by extractor [129], universal hashing functions [46], or cryptographic hash functions [157]. After this step, key generation is completed. Alice and Bob get the same secure key and they can use this key with symmetric encryption algorithms such as AES-128 to secure their subsequent communications.

3.2.3 Channel Reciprocity-based Approaches. Channel reciprocity-based key generation has received extensive research interests and been applied with several wireless technologies, such as ZigBee, Wi-Fi, LoRa, etc. As shown in Fig. 3(a), Alice and Bob are located with a certain distance between them. They will then leverage the reciprocal channel between them for key generation. Below, we introduce several representative systems for each wireless technology.

ZigBee. ZigBee is a popular communication technology for wireless sensor networks and wireless body area networks. It uses the IEEE 802.15.4 as the physical and Media Access Control (MAC) layer protocols. ZigBee operates at the 2.4 GHz and has a communication range about 100 meters. RSSI is available in ZigBee systems.

To the best of the authors' knowledge, Aono et al. [4] proposed the first ZigBee-based key generation protocol in 2005, which is also the first practical key generation system. The authors designed an electronically steerable parasitic array radiator (ESPAR) antenna, which can be dynamically configured to introduce channel fluctuation. Patwari et al. [88] proposed high-rate uncorrelated bit extraction (HRUBE), which is a framework incorporating interpolating, transforming for decorrelation and multi-bit quantization. They constructed a testbed using the TI CC2420 sensor nodes. Their system can achieve 22 bit/s at a KDR of 2.2% or 10 bit/s at a disagreement of 0.54%. Ali et al. [1] investigated key generation in body area communications. The sensors were worn on the arm of a person and tested with scenarios including high activity (subject working and walking), low activity (subject seating and working) and dynamic environment (surrounding environment variation due to walking pedestrian). They used a Savitzky-Golay filter to improve the signal noise ratio (SNR) of the received signals. They demonstrated that it is feasible to leverage the existing communication packets for key generation, though it took about 15 to 35 minutes to generate a 128-bit key.

Recently, Li et al. [67] proposed an RSSI trajectory-based secret key generation system for wearable devices. A bloom filter-based error correction scheme was proposed to correct the mismatches and Karhunen- Loeve Transform (KLT) [25] was used to enhance the randomness of the final key. The authors used both Universal Software Radio Peripheral (USRP) N210 [28] and CC2530 [44]. Evaluation results showed that their system is robust to eavesdropping attack and can generate a 128-bit key within 1s.

Wi-Fi. Wi-Fi is one of the most successful wireless technologies, which has been widely installed in almost all laptops, tablets, smartphones, and many other consumable devices. Wi-Fi is based on the IEEE 802.11 technologies, hence we use Wi-Fi and IEEE 802.11 interchangeably in this paper. Since IEEE 802.11 is first introduced in 1997, several amendments

have been released, including IEEE 802.11a/b (1999), IEEE 802.11g (2003), IEEE 802.11n (2009) and IEEE 802.11ac (2013). Because there are numerous off-the-shelf Wi-Fi platforms, they have become the ideal testbed for key generation.

The work by Mathur et al. [80] is probably the first Wi-Fi based key generation system. They used both the RSSI and the peak of the CIR. They designed a level-cross algorithm, which can achieve a high key agreement, hence information reconciliation is not required. Their algorithm was evaluated both theoretically and experimentally.

However, since RSSI and the peak of CIR can only provide coarse-grained information about wireless channels, the key generation rate of previous systems is largely limited even with the help of multi-bit quantization. To break this barrier, researchers started to explore fine-grained channel information that can be extracted from OFDM. Luckily, researchers find that CSI contains rich information about multiple sub-carriers of OFDM. Especially the release of tools that can extract CSI from commodity Wi-Fi devices [36] open the door for CSI-based key generation systems which later shows significant performance improvement compared to its counterparts. In particular, Liu et al. [75] carried out the first theoretical analysis for CSI-based key generation when there is a multipath channel. Then, Liu et al. [72] proposed the first practical CSI-based key generation system which achieved key generation rate of 60-90 bit/packet. Since then, numerous studies have been conducted to investigate CSI-based key generation systems from different application scenarios and perspectives [135, 154, 159, 162, 164].

Zhang et al. [159] modelled and analysed the time and frequency correlation of the OFDM by using Wi-Fi as a case study. Zhang et al. [154] took a step further by extending key generation to multiple users. In particular, they leveraged the Orthogonal Frequency-Division Multiplexing Access (OFDMA) for enabling the access point to communicate with multiple users simultaneously. However, Xi et al. [135] found that CSI measurements from adjacent subcarriers have strong correlations and hence the generated keys may have low randomness. To solve this problem, they proposed a key generation scheme, named KEEP, which adopted a validation recombination mechanism to generate secret keys from CSI measurements of all subcarriers.

LoRa. LoRa is a new IoT wireless technique, which features low power, low data rate and long range. The first LoRa-based key generation works were in 2018 [104, 142, 158]. Compared to the short range communications-based key generation, LoRa-based key generation has yet received less attention. LoRa protocol only provides RSSI information.

Ruotsalainen et al. [104] investigated the effects of LoRa setup on the key generation performance. They carried out extensive experiments with different configurations of spreading factors and bandwidths. These parameters will affect the airtime of LoRa packets hence the sampling delay between bidirectional transmissions between Alice and Bob. They also applied key generation with LoRaWAN specification and carried out experiments in indoor and outdoor suburban environments. They demonstrated that their system can even work when there was no significant channel variation. Xu et al. [142] designed a complete LoRa key generation protocol. They carried out extensive experiments with static and mobile modes including walking, biking and driving in indoor and outdoor environments. They employed several signal processing algorithms to improve the key generation rate. They also designed a compressive sensing-based reconciliation framework to reduce the KDR. Their experiment results demonstrated key generation rates of 18 bit/s and 31 bit/s in stationary and mobile scenarios, respectively. Zhang et al. [158] designed a differential value-based key generation protocol. They found the received power varied significantly when the LoRa devices moved in a large scale environment. In this circumstance, the threshold-based quantizer would produce non-random keys. In contrast, they quantized keys based on the trend of the received power. They carried out experiments in an indoor building and outdoor urban environment. The experimental results validated the differential value-based protocol can produce random keys.

Bluetooth. Although Bluetooth has been widely installed in smartphones and wearable devices, there are very few key generation explorations with Bluetooth and the first work is in 2014 by Premnath et al. [91]. Bluetooth operates at the 2.4 GHz ISM band, which is shared with Wi-Fi, ZigBee and microwave, etc. Bluetooth uses frequency hopping to find the free spectrum and avoid collision with other techniques. Premnath et al. [91] adopted this feature and their system can still work even under heavy Wi-Fi traffics.

5G:. The fifth-generation (5G) will be available very soon and has adopted a number of new and advanced physical layer modulation techniques, e.g., massive Multiple-input and Multiple-output (MIMO), millimeterwave (mmWave) communications, full duplex. These techniques provide new approaches to exploit channel randomness more efficiently. A tutorial on key generation with 5G can be found in [66].

Jiao et al. [48] investigated key generation performance for a mmWave MIMO system, which exploited the virtual angle of arrival (AoA) and angle of departure (AoD) characteristics. A new channel estimation method was proposed to exploit the sparsity of the mmWave MIMO channel. Their simulation achieved above 99% bit agreement ratio under very low SNR (-10dB), which can significantly decrease the reconciliation cost. Chen et al. [16] proposed a pilot reused key generation protocol for multi-user massive MIMO systems. Specifically, they designed two algorithms, namely beam domain-based channel probing and interference neutralization-based multi-user beam allocation, in order to reduce the channel dimension and reuse pilots. Their simulation results demonstrated a significant reduction of the channel estimation overhead. Vogt et al. [124] employed full duplex communications for the channel probing to improve key generation performances. Full duplex can decrease the sampling timing and significantly improve the key generation rate. However, the residual self-interference of the full duplex will impact channel measurements [125]. The authors also found that full duplex channel probing can downgrade the eavesdropping attack because of the superposition of probing signals.

3.2.4 Proximity-based Approaches. All the systems described in Section 3.2.3 depend on channel reciprocity to generate keys. There is another research direction that exploits the co-location property of mobile devices to generate keys. As shown in Fig. 3(b), when two devices are physically co-located, their radio signals will be very close to each other. Below, we review several representative works using the co-location property of IoT devices.

Amigo [121] is one of the earliest studies that use a common radio environment to authenticate mobile devices without explicit user involvement. It adopted Diffie-Hellman protocol (also known as D-H protocol) to establish keys followed by a commitment scheme to address Man-in-the-Middle (MITM) attack. Finally, the similarity between the radio signals measured by two devices is used to verify if they are in close proximity. The authors claimed that Amigo is secure against MITM attack, eavesdropping attack and spoofing attack.

Mathur et al. [79] proposed Proximate, a system that generated a secret key for two mobile devices nearby from their measured wireless radio signal. Proximate adopted the conventional key generation process mentioned in the last subsection: quantization, reconciliation and privacy amplification. It removed the reliance on Diffie-Hellman protocol, but its bit generation was very low (only 1-3.5 bit/s).

To overcome the low bit rate problem, Xi et al. [136] proposed a CSI-based authentication and key generation system called The Dancing Signals (TDS) for two devices in close proximity. Although TDS used CSI to generate keys, it presented a novel key generation method. The keys were generated randomly and encoded by the CSI features. Only the other device that had similar features can decode the key. Therefore, both devices can agree on the same key. By not generating keys from CSI directly, TDS improved key generation rate significantly. According to their evaluation, TDS can achieve a bit rate of hundreds of bit/s. Moreover, TDS can be extended to support a group of users.

Some other proximity-based schemes are based on another observation. That is, if a nearby sender moves very close to one of the antennas on the receiver, the receiver can observe a large RSSI variation. Instead, if a faraway sender moves close to the receiver, the two antennas will not see a large RSSI difference. Some representative works are Neighbor [13], Wanda [89] and Move2Auth [161]. Good Neighbor is the first device pairing scheme based on this idea. Wanda was built on Good Neighbor but expanded to generate secret keys based on the channel reciprocity. Move2Auth borrowed the idea from Good Neighbor and Wanda and used for a smartphone to authenticate a nearby IoT device.

Co-location based approaches take advantage of the physical proximity to authenticate devices. However, these approaches suffer from a common problem: the distance between two legitimate devices should be close, e.g., 1.25 cm in Proximate [79], 5 cm in TDS [136] and 20 cm in Move2Auth [161]. Therefore, the practicability of such approaches is low because the wireless transceivers are embedded in mobile devices and in some scenarios it is hard to put two antennas in such short distance.

3.3 Audio

Currently, microphones and speakers are integrated in many IoT devices such as smartphone, Google assistant, Amazon Echo and laptops. Acoustic waves, as a form of wave, possess many similar properties as radio waves such as fading, multi-path, reflection and diffraction. Accordingly, a large portion of existing work have studied how to use audio signals to pair IoT devices. We describe several representative systems that achieve device pairing by audio signals. Same as radio-based key generation, the majority of works can be divided into two classes: channel reciprocity-based and proximity-based.

3.3.1 Channel Reciprocity-based Approaches. Researchers also demonstrated that acoustic channel holds reciprocity [76]. Therefore, several acoustic channel reciprocity-based device pairing systems have been proposed recently.

Lu et al. [76] conducted the first study to verify the reciprocity of acoustic channel. In order to not disturb users, FREE used the inaudible frequency range 18k-22kHz. FREE works as follows. To estimate the acoustic channel, FREE transmits a pre-defined sequence, which is modulated to the symbols of Gaussian Filtered Minimum Shift Keying (GMSK). The generated signal is stored in a Waveform Audio (WAV) file and then transmitted by the speaker. After two devices exchange a number of messages, they use channel taps [120] as acoustic channel features to generate keys. The authors implemented FREE on several smartphones and evaluated its performance in four environments: indoor static environment, indoor mobile environment, outdoor static environment and outdoor mobile environment. The results showed that FREE worked well when two devices were within 60 cm distance. They validated the randomness of the generated keys by National Institute of Standards and Technology (NIST) test and also analysed the security of FREE against possible attacks.

Bala et al. [5] also proposed a key agreement system based on acoustic channel reciprocity. The proposed system adopted the conventional key generation procedure in wireless key generation: channel probing, quantization, reconciliation and privacy amplification. Different from FREE, the proposed system used sound pressure levels as acoustic channel physical layer characteristics. The authors implemented the proposed system on Samsung Galaxy On5 pro smartphone and conducted evaluation in different environments including classroom, conference room and hallway. By carefully tuning parameters, they can achieve a key generation rate of 80 bits/sec and a bit error rate of 25% before reconciliation. They also conducted NIST test [102] and the generated keys pass the test.

3.3.2 Proximity-based Approaches. As shown in Fig. 3(b), the idea of proximity-based scheme is that sound recorded by microphones do not vary too much within close proximity, but significantly differ when two devices are far away from each other.

Schürmann and Sigg [107] proposed a system to establish a common cryptographic key for devices in the same context based on ambient audio patterns. The system works as follow. First, both devices need to perform a Network Time Protocol (NTP)-based synchronisation method to establish sufficient synchronisation. This is because synchronisation among devices plays a significant role in their approach. The extracted fingerprints will be totally different if the start time of audio signal differs several hundreds milliseconds. Second, both devices extract a binary representation of their recorded audio which is called audio fingerprint. The binary sequences of two devices will be highly similar to each other if they are in close proximity. Finally, they use fuzzy commitment scheme to account for the errors between the binary sequences to generate the same key.

The authors verified the feasibility of the proposed approach in several realistic environments including office environment, canteen environment and outdoor environment. The results showed that their protocol works well in an office environment. In the crowded canteen environment, the matching rate will decrease if there is not a dominant audio source. In the outdoor environment (a heavily trafficked road), it is hard to establish a secure communication channel based on ambient audio only. They also analysed the security of the proposed pairing scheme against various potential attacks such as eavesdropping, brute force attack, MITM, Denial-of-Service (DOS) and audio amplification attack. The analysis showed that these threats can be eliminated by a careful choice of the fingerprint mechanism.

Following the same idea, Karapanos et al. [56] proposed Sound-proof, a two-factor authentication scheme based on ambient sound. The idea of Sound-proof is that if a smartphone is close to a computer, they will record similar sound signals. So the similar sound signals can be used as the second factor to verify user's identity. The authors implemented Sound-proof on many platforms. The browsers include Google Chrome, Mozilla Firefox, and Opera. The smartphone platforms include Samsung, Google Nexus, Sony, Motorola, and different iPhone models. The evaluation in both indoor and outdoor environments showed that Sound-proof can achieve an Equal Error Rate (EER) of 0.002. EER is the crossing point of false rejection rate and false acceptance rate. It means, out of 100 trials, only 0.2% of genuine user's attempts are rejected and 0.2% of attacker's attempts are accepted. Sound-proof can complete verification within 5 seconds and work well at different locations and distances.

The primary limitation of the above two systems is that both devices need an accurate synchronisation which is sometimes unrealistic especially for devices that meet each other for the first time. AudioKey proposed by Shang and Wu [109] aims to pair two smart watches when two users shake their hands together. It adopts the same idea as the above work but eliminates the requirement of synchronisation. The working flow of AudioKey is as follows. The pairing process is triggered by detecting the fist negative peak during the handshake process. The observation is the acceleration signals measured by two smart watches should follow the same pattern and reach peak almost at the same time because two hands are held together tightly. AudioKey extracts binary key sequence from both time domain features and frequency domain features. The Golay code G(24, 12) is then employed to correct the errors between two smartwatches.

The authors recruited nine volunteers whose ages were from 22 to 29 to evaluate the performance of AudioKey. The results showed that it can achieve a bit generation rate of 13.4 bit/s and key agreement rate of 96.7% for a 128-bit key. They also analysed the security against mimicking attacker. If an attacker located 1.2 m away started key generation at the same time as the genuine user, his matching rate can be as high as 73.25%. Although the authors claim that the

location of the mismatched bits are unknown to the attacker, the entropy of the key is decreased significantly, and the security needs further validation.

Genewave proposed by Xie et al [137, 138] is also based on acoustic signal proximity. Their idea is that the acoustic channel response is unique for a given device at a given location. The proposed system includes two major steps: bidirectional initial authentication and key agreement. In the first step, they use the round-trip time of acoustic signal between two devices to authenticate each other. Specifically, if the response interval is larger than a pre-defined threshold, the device will be regarded as an attacker. In the second step, Alice and Bob first build the features of the acoustic channels. Then, the bits '1' and '0' are encoded in the acoustic signal based on a novel sine wave-based pulse coding method. Suppose Alice encodes bit sequence in an acoustic signal and transmit the modulated signal to Bob. Bob can decode the same symmetric key based on the acoustic channel response between Alice and Bob. So both Alice and Bob establish the same key to secure their communication.

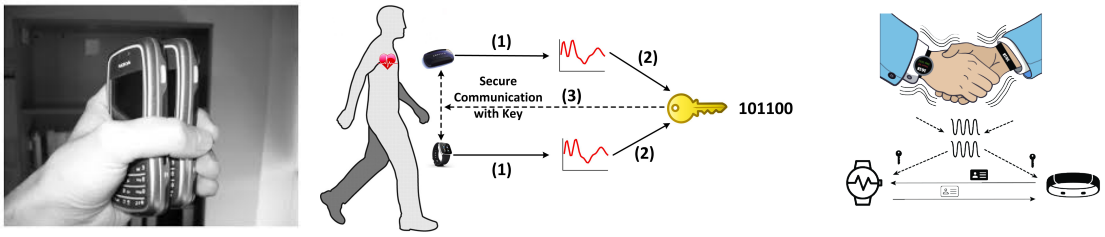
The authors implemented GeneWave on Nexus smartphone and conducted evaluation in three environments: line-of-sight (LOS) meeting room, non line-of-sight (NLOS) meeting room and coffee shop. However, they cleared all human activity in meeting room to mitigate the influence of environment changes. The evaluation results showed the proposed system can achieve high matching rate in the above three environments. Moreover, GeneWave can complete authentication and generate a 2048 bits key in 2 s, which is 10× faster than TDS [136]. Although the evaluation showed GeneWave can pair two devices quickly, the evaluation is conducted in a well controlled environment. First, Alice and Bob need to be very close to each other (<3cm) to achieve high matching rate. Second, there should be no activities in the nearby environment to avoid multi-path changes. Therefore, the usability of GeneWave in a realistic environment still requires further study.

Although the systems above can achieve high performance as demonstrated in the evaluation, they can only achieve D2D pairing. It is desirable that a group of IoT devices can be paired together based on the sound if there are a number of devices present. Motivated by this, Gu et al. [33] proposed a group audio-based authentication scheme for IoT devices which is called GAB-IoT. In GAB-IoT, there is a central device who broadcasts audio signal to nearby IoT devices. All the devices in an audio-reachable distance can observe similar audio signal, based on which they can generate the same key using fuzzy extractor [24].

3.4 IMU Sensors

In this subsection, we review representative device pairing systems based on sensors embedded in IoT devices. The on-board sensors in IoT devices provide them capabilities to collect information about the ambient environment. Thus the sensory information can be used to complement the limitation that two devices have no pre-shared secret. So far, a variety of sensory signals have been used as common knowledge to assist IoT device authentication and key generation. In the following, we survey this type of work based on their sensor types.

A large number of device pairing systems have been proposed by utilising the built-in IMU sensors. IMU sensors include 3-axis accelerometer, 3-axis gyroscope and 3-axis magnetometer. Among these three types of sensors, accelerometer is the most widely used sensor to design a device pairing system. This is because it provides a good source of entropy for bootstrapping a secure communication channel in autonomous and spontaneous interactions between mobile devices that share a common context but were not previously associated. The shared common context is usually a daily activity such as shaking, walking, hand gesture etc. Next, we discuss this category of work based on the type of motion used in each scheme.



(a) Shake well before use [81] (b) Walkie-Talkie [145] (c) Shake-n-Shack [112]

Fig. 5. Representative works of accelerometer-based device pairing system.

3.4.1 Shaking-based scheme. The idea of shaking two devices together to pair them was first proposed by Holmquist et al. [41]. To verify this idea, the authors implemented a prototype called *Smart-Its Friends*, which is a small embedded artefact that can be associated when a user holds and shakes them together. *Smart-Its Friends* pairs two devices without explicitly generating keys. Since then, a large body of studies based on this idea have emerged.

The Martini Synch proposed by Kirovski et al. [58] is the first protocol that generates a common key between two accelerometer-equipped devices shaking together. It adopted a simple fuzzy quantizer and an off-the-shelf cryptographically secure hash function, which they called joint fuzzy hashing protocol. By implementing a prototype using off-the-shelf components, they showed that their method can produce between 9–20 bits of entropy per second.

Mayrhofer and Gellersen [81] designed the first complete pairing protocol, Shake well before use. Specifically, they proposed two schemes ShaVe and ShaCK. ShaVe first used Diffie-Hellman protocol to establish an insecure channel. It is known that standard Diffie-Hellman protocol is susceptible to MITM attack. So the authord used the Interlock protocol [96] for protecting against MITM to exchange the acceleration data. Finally, two series of acceleration data measured by two devices were compared to each other based on coherence. If it passes check (the coherence exceed a predefined threshold), the key generated by D-H protocol is used as session key to secure their subsequent communications. ShaCK adopted a direct key generation method. First, the FFT features were calculated from the captured acceleration data. Then, the FFT features were quantized to binary keys based on candidate key protocol which accumulated matched parts of the keys until it reached sufficient entropy.

In addition to the systems above, there are also a number of key generation systems based on shaking motion, e.g., Shake on it (Shot) [117], Shakeunlock [29], ShakeMe [150], and iShake [113]. They essentially use the same idea but different methods to generate keys. For example, Shakeunlock uses coherence similarity to determine whether two devices are shaking together while ShakeMe extracts discriminative features from the accelerometer data to derive keys.

Recently, another daily activity, handshaking, has also attracted researchers' interest. Handshaking is a common practice when two persons meet to express trust and respect. The motion pattern during this process can be captured by the motion sensors in user's wrist-worn wearables and then employed to extract secret keys for establishing a secure communication channel. The first idea was proposed and demonstrated in Shake-n-Shack [112]. The evaluation results showed that Shake-n-Shack can generate 128-bit keys around 1 s with success rate >99%. Motivated by Shake-n-Shack, Jiang et al. [47] proposed another acceleration-based pairing scheme for wrist-worn devices. They enhanced the efficiency of Shake-n-Shack by using an improved fuzzy cryptography scheme [3]. But their result was obtained from Matlab simulation in a laptop rather than implementing the system on real wrist-worn devices.

Shaking is an intuitive movement with natural variance. Additionally, it is easy to learn and perform. However, the usability of shaking-based approaches is restricted by the shape, size, and weight of the involved devices [18, 19].

3.4.2 Walking-based scheme. Shaking devices is intuitive, vigorous, and varying but only applies to wearable devices that can be held in the hand or worn on the wrist. In recent years, researchers have found another common daily activity that can be used to generate keys, i.e., gait. Gait refers to people's walking patterns. Like other biometrics such as face and fingerprint, gait is a biometric characteristic and studies from psychology and biometrics have shown that different people have distinguished and unique walking patterns [93, 141, 163]. Therefore, mobile devices worn on the same user's body can measure the same gait pattern while devices on other user's body have different measurements. This fact lays the foundation for walking-based key generation schemes.

Lester et al. [64] first proposed to use low-cost accelerometer to determine whether two devices are carried by the same person or not by analysing the coherence of the walking data. Their method worked well when two devices were carried in the same location on the body. However, there are two limitations in their study. First, there were only two subjects involved in the experiment so the results did not fully demonstrate the feasibility. Second, their method only achieved approximately 87% accuracy if two devices were carried at different locations on the body.

Later, Cornelius and Kotz [21] extended the work of Lester et al. to sensors carried at different locations on the body including wrist, ankle, and waist. They first extracted seven features that are commonly used in activity classification. Then they employed supervised machine learning method, namely support vector machine (SVM), to determine whether two devices were carried on the same body. They used a dataset of seven subjects walking for 22 minutes to evaluate their approach and showed that their approach outperformed the work of Lester et al. [64] when devices were on the different locations on the body.

Motivated by these two pioneering works, Xu et al. [145] proposed the first gait-based key generation protocol for on-body mobile devices Walkie-Talkie. It followed the traditional key generation process as in radio-based key generation introduced in Section 3.2: quantization, reconciliation and privacy amplification. It can generate a 128-bit key within 5 seconds (≈26 bit/s). The performance was further improved in their extension paper Gait-key [141]. Gait-key utilised a multi-bit quantization approach to improve key generation rate and further employed error-correction code to correct the mismatch between the initial keys. The time required to generate a 128-bit key was reduced from 5 seconds to 3.5 seconds (≈ 36.6 bit/s). The authors also implemented Walkie-Talkie and Gait-key on MoTo E2 smartphone to evaluate the system cost. Their results showed that the computation time of Walkie-Talkie and Gait-key is 316.8 ms and 419.2 ms, respectively. They analysed the security of Walkie-Talkie and Gait-key by asking attackers to mimick genuine user's walking patterns. They found that a mimicking attack can at most achieve about 50% agreement rate indicating that their systems are resilient to active mimicking attack.

In another work BANDANA [106], the authors also used gait to authenticate devices on the same body. Different from Walkie-Talkie, BANDANA proposed a novel quantization method and utilised fuzzy commitment scheme [53] to account for the errors. Compared to the fuzzy vault scheme, fuzzy commitment is less complex and computationally expensive in terms of key locking and unlocking. Their evaluation results showed that BANDANA can achieve 80% similarity between devices on the same body. Because they only used the acceleration data along gravity direction to generate keys, the key generation rate was very slow: it took approximately 96 s to generate a 128 bit key (≈ 1.3 bit/s).

The authors in [118] followed the same idea and simply combined the advantage of Walkie-Talkie and BANDANA together. Their method used 3-axis acceleration data to generate keys and employed fuzzy commitment scheme with BCH code to correct errors. However, their key agreement rate can only reach 79%.

In a more recent work Auto-Key [134], Wu et al. proposed to use autoencoder to speed up the key generation rate of gait-based scheme. Instead of exchanging additional error correction information, one device uses an autoencoder to predict the gait measurements at another device attached to the same body. Then the key was generated based on the

predicted accelerometer data. The evaluation results showed that Auto-Key can improve matching rate by 16.5% while speeding up bit rate by 1.9×.

However, the systems mentioned above suffer the same limitation: they can only pair two devices and fail to pair a group of devices. To solve this problem, Revadigar et al. [95] proposed a group key generation scheme for wearable devices based on user's walking patterns. The system works as follow. First, a hub device generates a random key using random number generator (RNG). Then, it uses fuzzy vault scheme [52] to construct a vault based on the measured acceleration data. Afterwards, it broadcasts this vault to nearby devices. The other devices can recover the random key by unlocking the vault using their own gait measurements. According to fuzzy vault scheme, only highly similar gait signal can be used to unlock the vault. Therefore, their approach ensures that the random key hidden in the vault can only be recovered by the devices on the same user's body. Because the gait signal is not used to generate keys directly, the key generation rate is up to 750 bit/s.

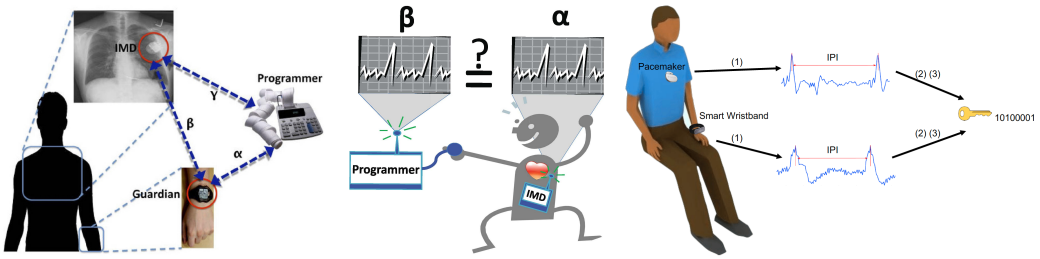
Since walking is a daily activity, walking-based key generation systems provide an autonomous and spontaneous way to pair wearable devices that are worn on the same user's body. Although all the authors above claimed that their approaches can generate keys with high randomness, a recent study revealed that there is a bias in the generated binary bit strings [10]. They also pointed out that the attacker can generate a highly similar key by video analysis. Unfortunately, there has not been any work in the literature that can prevent this kind of attack. Therefore, it would be an interesting future research topic.

3.4.3 Others. Apart from the motions above, other motions are also utilised to facilitate secure device pairing. Synchronous gestures such as bumping was utilised to pair two mobile devices equipped with accelerometers. The intuition is bumping generates equal and opposite hard contact forces that are simultaneously sensed by the accelerometer. Hence, the accelerometer signal can provide enough information to determine whether two devices are physically interacting or not. Example of such systems include Hinckley et al. [40] and BUMP [119].

Wang et al. [130] introduced Touch-and-Guard (TAG), a system that used hand resonant to associate a wrist-worn wearable with an external device equipped with accelerometers. TAG is based on the observation that the hand and the external device form a vibration system of which resonant properties measured by two devices attached to hand or wrist are highly correlated. The authors demonstrated the feasibility of TAG by implementing a prototype on Arduino development board and conducted experiments involving 12 subjects. Evaluation results showed that TAG can achieve a key generation rate of 7.84 bit/s, which is faster than commonly used PIN authentication scheme. They also analysed the security of TAG and found that it is resilient to passive acoustic eavesdropper but vulnerable to visual eavesdropper using high-speed cameras.

Han et al. [39] proposed to use road bumpiness and traffic conditions as a common context to detect trucks in the same platoon. Convoy (the name of their system) exploited the fact that trucks in the same platoon experience similar road (e.g., bumps and cracks) and traffic (e.g., acceleration and steering) conditions. By using the embedded accelerometers, Convoy used the traditional fuzzy commitment scheme [53] to establish the same key for the trucks in the same platoon. The authors implemented and tested the Convoy protocol with real-world driving data. Evaluation results demonstrated that vehicles moving in neighbouring lanes can be differentiated adequately by their context, and Convoy can counter platoon ghost attacks.

3.4.4 A Summary of Motion-based Schemes. In this subsection, we have discussed various motion-based device pairing schemes. These methods require users to perform an explicit action (i.e., shake devices together). Because it explicitly involves users, it increases their perception of the association while it executes. The motions researchers have explored



(a) IMDGuard [139] (b) H2H [145] (c) H2B [69]

Fig. 6. Representative works of IPI-based key generation systems.

are common daily activities such as shaking, walking, bump and touch. Therefore, these schemes are intuitive and easy to learn. Nevertheless, their usability is limited by the shape and form factor of the involved IoT devices [19].

3.5 Miscellaneous Hardware

Advances in microelectronics, embedded system and wireless technology, have led to a rapid development of new types of miniature sensors in IoT devices which in turn create many new opportunities for context-based IoT device pairing. In this subsection, we survey recent related work using new hardware. It should be noted that due to the diversity of miscellaneous hardware, we categorise these works based on the signal they used to pair devices.

3.5.1 Heartbeat Signal. The concept of using human biometrics to secure body area network communication was first proposed by Cherukuri et al. [17]. Conventionally, biometrics is a technique commonly known as the automatic identification or verification of an individual by his or her physiological or behavioural characteristics [45]. The concept described here, however, is different from conventional biometrics cryptography systems. In the context of key generation, biometrics traits are used as keying materials to generate random keys. To this end, the biometrics should fulfil the following two requirements as noted in [90].

- Distinctiveness. The trait should be sufficiently distinctive on two individuals, so that the keys generated from different subjects will be different.
- Time variation and invulnerability. The trait should change over time and have a high degree of randomness so that the biometric characteristics recorded at different times would not generate the same key even they are obtained from the same person.

The motion-based systems described in the last subsection are essentially based on behavioural characteristics. Despite their user friendliness, they still pose some burdens on users. A desirable device pairing system should reduce user involvement as much as possible. Moreover, the feasibility of such behavioural-based device pairing system is validated on a small-scale dataset under controlled environment. It is still elusive whether they apply to large-scale population. However, another human physiological biometrics, heartbeat, does not have such problem because they have been validated on large datasets [17, 86]. Specifically, researchers have found that inter-pulse interval (IPI), i.e., the interval between heartbeat signal peaks, is highly random and can be used as a random source to generate keys [100]. Fig. 6 illustrates the idea of heartbeat signal-based key generation system. Below, we discuss several representative works utilising IPIs to pair wearable devices.

The first practical key generation system based on IPIs was proposed by Poon et al. in their pioneering work [90]. The suggested system was validated on a dataset of 99 subjects, and the results showed that it can achieve a total

error rate of 2.58% when the IPIs were coded into 128-bit key. Later, the same group of authors proposed a more advanced system which improved the system performance significantly [7]. The proposed system works as follows. To begin with, a series of IPIs were captured by biosensors located at different body locations. Then, multiple IPIs were accumulated to achieve better performance followed by a modulo operation to randomise the monotonically increasing multi-IPIs. Finally, the mapped IPIs were represented by their corresponding Gray code to form the final binary sequence. Compared to their previous scheme [90], the error rate with 64-bit key generated was reduced from 6.98% is 2.83%. Meanwhile, the improved system required less IPIs to generate the same length of key. In both systems, the IPIs were obtained from biosensor signals that can record electrocardiogram (ECG) and photoplethysmogram (PPG).

However, Xu et al. [139] found that previous work did not properly extract the randomness of IPI. Specifically, as the average IPI of most people is about 850 ms, the 7th and 8th digits of the ending time are not random at all. For example, suppose the first IPI value is 860 ms and its Gray code representation is "1011110010". If there is another IPI whose value is 840 ms, then its Gray code representation is "1011101100". It is clear that the first 5 digits are exactly the same. The randomness of IPI data lies in the least significant bits, so does the error. To tackle this problem, Xu et al. [139] proposed the first comprehensive secure protocol for ECG-based key agreement system, IMDGuard. IMDGuard solved this issue by proposing an algorithm that can transform raw IPI data from normal distribution to uniform distribution. Then, the least 4 bits were used to generate keys. Finally, IMDGuard used parity check to discard the mismatched bit blocks to generate the final key. The authors implemented IMDGuard on TelosB board which utilised the CC2420 transceiver for wireless communication. Evaluation results showed that IMDGuard required 61 IPIs, corresponding to 45 seconds or so, to generate a 128-bit key. The author also validated the randomness of the extracted keys by NIST test suite [102].

Venkatasubramanian et al. [122, 123] proposed to use fuzzy vault to account for the measurement errors between different biosensors. The difference between these two works is in [122] they used PPG only while in [123] they utilised the combination of PPG and electrocardiogram (EKG). However, the security level of these two systems is not high due to the limited feature size and high computational overhead. To overcome this limitation, Hu et al. [42] proposed IPI-based key agreement protocol termed OPFKA. In comparison with the work of Venkatasubramanian et al. [122, 123], OPFKA is more secure and energy efficient. OPFKA is based on the observation that secret features generated by a sensor are ordered and only the sensor itself is aware of the order of the features. But this way is controversial because the authors assume only Alice and Bob know the order of features which is actually a pre-shared secret. It contradicts the normal assumption that two devices meet for the first time have no pre-shared secret between them.

However, as discussed in [99], IMDGuard and OPFKA have serious security flaws. For instance, by performing a simple MITM attack to IMDGuard, the effective key length is reduced from 189 bits to 86 bits. To solve this problem, Rostami et al. [100] proposed their ECG-based authentication protocol, Heart-to-Heart (H2H). H2H is a novel cryptographic device pairing protocol that uses the randomness of IPI to protect against active attackers, while meeting the requirement of lightweight implementation and noise tolerance in ECG readings. The authors implemented H2H in an ARM-Cortex M-3 microcontroller to demonstrate the practicality of H2H in current implantable medical device (IMD) hardware. The authors claimed that H2H is the first physiologically-based IMD device pairing protocol with a rigorous adversarial model and protocol analysis.

With the emergence of new sensors, researchers started to investigate the feasibility of using these sensors to detect heartbeat signals. Lin et al. [69] proposed the first piezoelectric sensor-based key generation system H2B for on-body wearable and implantable devices. H2B is based on the observation that the minor vibrations caused by heartbeats can be detected by piezoelectric sensors on different body locations. The evaluation results showed that H2B can pair two

wearable devices on the same user's body with a success rate of 95.6%. Security analysis of H2B also demonstrated that it is secure against passive attack, active presentation attack and active video attack.

Compared to walking and shaking, heartbeat signal-based key generation systems can ease the burden on users, i.e., users do not need to walk a few steps or shake devices. Additionally, several large dataset are publicly available online. For example, the dataset used in [42, 122, 123, 139] is PhysioBank database [1], and the dataset used in [100] includes MIT-BIH Arrhythmia Database [85], PTB Database [9], and MGH/MF Waveform Database [132]. However, due to the limited entropy of information source, this kind of scheme cannot achieve high key generation rate. For instance, the state-of-the-art heartbeat signal-based system H2B can generate keys at the speed of 3 bit/s, which is several order-of-magnitude lower than walking-based scheme (750 bit/s in Revadigar et al. [95]) and shaking-based scheme (128 bit/s in Shake-n-Shack [112]).

3.5.2 Gait Signal. The aforementioned walking-based device pairing schemes use accelerometer to record user's walking patterns. However, the main problem of accelerometer-based sensing systems is continuously sampling accelerometer will quickly drain the battery of resource-constrained IoT devices. To address this problem, a recent trend is to use kinetic energy harvesting (KEH) device to replace accelerometer. KEH is the process of converting motion and vibrations into electrical energy to power electronic devices. Human activities are the most relevant sources because wearable devices can harvest energy directly from user activities. Therefore, KEH is a promising technology for applications where batteries are impractical, such as wearable and implantable sensors [59].

Initially, this idea is proposed in the field of activity [57], gait [143, 144] and transport mode classification [62, 63] for the purpose of power saving by not sampling accelerometer. The first piezoelectric energy harvesting-based key generation system based on user's walking pattern was proposed by Qi et al. [68] until very recently. The principle of KEHKey (the name of their system) is the same as walking-based key generation schemes such as Walkie-Talkie [145], i.e., the energy patterns harvested by multiple KEH devices on the same user's body are highly correlated while it is not accessible to outsiders.

KEHKey consists of the following three stages: sampling and smoothing, quantization, and information reconciliation. First, Alice and Bob harvest energy from user's walking independently. Then, they quantize the measurements into binary key sequence which contains '1's and '0's only. Finally, they apply the compressive sensing-based reconciliation method as [69] to correct the mismatches between their keys.

The authors implemented the proposed system using off-the-shelf piezoelectric energy harvesting products and evaluated its performance with data collected from 24 subjects wearing the devices on different body locations including head, torso and hands. The results showed that KEHKey was able to generate keys at a speed of 12.57 bit/s while reducing energy consumption by 59% compared to accelerometer-based approaches. Additionally, they demonstrated that KEHKey can successfully withstand typical adversarial attacks. Particularly, KEHKey is found to be more resilient to video side channel attacks than its accelerometer-based counterparts.

3.5.3 Magnetometer. Jin et al. [50, 51] proposed magnetometer-based system MagPairing to pair two smartphones in close proximity. When two smartphones are in close proximity, their magnetometer readings are highly correlated. The working flow of MagPairing is very similar to ShaVe proposed in Shake well before use [81] . First, Alice and Bob use D-H protocol to establish an unauthenticated communication channel and Interlock protocol to counter MITM attack. Then, they exchange their magnetic fields readings. If their similarity is higher than a threshold, the DH key will be

[1] http://www.physionet.org/physiobank

used to secure the communication. In the evaluation, the authors implemented MagPairing on several smartphones such as Google Nexus 5 and GALAXY 3. Evaluation results showed that MagPairing can pair two devices within 4.5 s with more than 90% success rate.

3.5.4 Electromyogram (EMG). Yang et al. [146] proposed an EMG-based pairing system which is called EMG-KEY. EMG-KEY utilised the electrical activity caused by human muscle contraction (i.e., EMG) to generate secret keys for two wearable devices. MEG-KEY works as follows. First, two wearable devices record raw EMG signal independently when the user performed a random gesture. Then, the EMG signal was rectified and converted into binary bits based on a shape-based key generation method. Finally, the same key was obtained by using Golay Code G(23, 12) in the reconciliation to correct the mismatches. Evaluation results on 10 subjects suggested that EMG-KEY can reach a high bit rate of 5.51 bit/s with a success rate of 88.84%.

3.5.5 Electrode. Roeschlin et al. [97] proposed a device pairing protocol for two devices that can be physically attached to the body. The suggested protocol is built on the unique body channel: the body channel is used as a part of the pairing protocol to allow two legitimate devices agree on the same secret. Any external devices have no knowledge of the body channel characteristics, and thus cannot guess the secret. In the evaluation, the authors implemented a proof-of-concept and recruited 15 volunteers to verify their idea. Evaluation results showed that the system can achieve 94.3%-99.6% accuracy.

3.6 Camera

As camera are ubiquitous in almost all smartphones, researchers have designed many key generation approaches taking advantage of the cameras in the devices. Below, we introduce several representative works.

McCune et al. [82] proposed an authenticated key exchange scheme named Seeing-Is-Believing (SiB). One camera-equipped device can take a photo of a 2D bar code which encodes the cryptographic key of another device. By changing the roles and repeating the above process, both devices can achieve authenticated key exchange. The authors compared their scheme with other key exchange systems using other channels such as ultrasound, audio etc. They claimed that SiB is more secure and convenient to use because the user can identify the device to be paired visually.

However, SiB has several limitations. For example, both devices must be equipped with a camera to achieve mutual authentication. The application scenarios of SiB are limited when one device has limited capabilities such as small size and display. To overcome these drawbacks, Saxena et al. [105] proposed several extensions to SiB. The proposed approach can achieve mutual authentication when only one device is camera-equipped. This is done by having both Alice and Bob compute a common checksum on public data, then compare their results via a unidirectional visual channel.

Buhan et al. [11] proposed a biometrics-based secure device pairing system, SAFE. SAFE used cameras to take a picture of another user's face. Then, they applied fuzzy extractor [24] to extract secret keys from face images. By exchanging some information, both Alice and Bob can agree on the same key. The authors demonstrated that the proposed system is resilient to eavesdropping attack and MITM attack.

The above methods are restricted to two-parties key exchange. GAnGs proposed by Chen et al. [14] and SPATE proposed by Lin et al. [70] extended SiB to support group device pairing. GAnGs allows a group of devices to collect and distribute authentic information by displays and cameras equipped on each device. SPATE requires users to compare images on different devices to achieve group pairing. Compared to SiB and GAnGs, SPATE achieves better performance

in terms of efficiency, accuracy and user experience. The common feature of SiB, GAnGs and SPATE is that they all adopt the barcode format designed by Rohs and Gfeller [98].

In these methods, cameras are used as OOB visual channel to convey some secret information between intended parties. The application scenarios of these approaches, however, are limited because of the unavailability of cameras in most IoT devices. Additionally, these approaches require human computer interaction to facilitate device pairing process. For example, in the work of McCune et al. [82] and Saxena et al. [105], the authentication is completed by user answering affirmatively in the last step.

3.7 Hybrid Approaches

The above context-based pairing approaches improve the efficiency of pairing IoT devices by removing any human interference in pairing. Using on-board sensors with the same sensing modalities, it is possible to capture a specific physical background such as physical layer characteristics of the same wireless channel, the motion signal of the same user, and ambient sound from the same event. Nonetheless, due to the heterogeneity of IoT devices it is impractical to presume, in some scenarios, that all devices share a common modality of sensing. This limitation sparks some new studies that aim to pair heterogeneous IoT devices by exploiting different sensor modalities. Below, we introduce several representative works belonging to this subcategory.

Miettinen et al. [83] proposed a context-based zero-interaction pairing protocol for wearable devices by using ambient audio and luminosity. The suggested system utilises context fingerprints to evolve the generated key which is only possible when two devices are in close proximity over a long period of time. Intuitively, it is based on the fact that devices belong to the same user can observe similar context information in a longer time than other devices. Although the proposed scheme does not involve user interaction, it takes a long time to accumulate sufficient entropy to complete authentication.

Han et al. [38] proposed a novel context-based pairing scheme named Perceptio for IoT devices that are equipped with different types of sensors. Perceptio utilises time as the common factor across different types of sensors. It produces event fingerprints that can be compared across a range of IoT devices by concentrating on the event timing rather than the individual event sensor data. The principle of Perceptio is that devices co-located inside a physically protected boundary (e.g., smart home) will be able to detect more typical events over time as opposed to outsiders. The authors deployed a variety of heterogeneous IoT devices in a room such as geophone, microphone, accelerometer, motion sensor and a power meter. Evaluation results showed that the legitimate devices in the same room can achieve an average fingerprint similarity of 94.9% while an outside attacker can only yield 68.9% similarity.

Additionally, some other systems uses different combinations of sensor modalities to pair devices. To name a few, Shrestha et al. [115] designed an authentication system by using the combination of four different sensor modalities namely, ambient temperature, precision gas, humidity, and altitude. Liu et al. [71] proposed a pairing scheme for wearable devices based on sound and light. Unisense proposed by Pan et al. [87] and IDIoT proposed by Ruiz et al. [101] (the same group of people) leveraged video signals and IMU sensor signals to pair heterogeneous IoT devices.

Key generation schemes using multi-modality sensing present two advantages. On the one hand, it can be used to associate heterogeneous IoT devices that have different sensors, shapes, and sizes. On the other hand, it improves the security of pairing schemes against attackers because it requires the attacker to monitor the various physical environment properties at the same time. Meanwhile, it also has some drawbacks. First, such schemes may take a long time to complete device pairing because the frequency of some events is low (e.g., door closing in [38]). Second, due to the heterogeneity of sensor data, the processing method is usually more complex and expensive because signals

measured in different sensing state-spaces cannot be directly compared. For example, Unisense [87] and IDIoT [101] require camera calibration and coordinate transformation to obtain motion signal in the common state-space.

4 PERFORMANCE COMPARISON

Because of the diversity of different hardware and protocols, many metrics have been used in prior works. Yet, there lacks a common understanding and sound comparison of existing systems in the current literature. Although several previous works have provided comparisons of some early device pairing schemes [54, 60, 61], their studies only provide quantitative comparison by using subjective metrics such as usability [61]. In this section, we first summarise commonly used objective metrics in device pairing systems. Then, we provide a comprehensive quantitative comparison of existing schemes. Due to space limitation, we only compare the performance of representative works in each category. Finally, we define five goals of a desirable key generation scheme and provide a qualitative analysis based on this baseline.

4.1 Objective Metrics and Quantitative Comparison

Below, we summarise three commonly used metrics in key generation systems.

- Key generation rate (KGR). KGR represents the number of bits in a unit time that a system can generate. It indicates how fast a key generation system can generate or update keys. For the real-time key generation process a high KGR is desirable, as the cryptographic schemes need a certain length of keys. For instance, AES requires a key sequence with a minimum length of 128 bits.
- Key agreement rate (KAR). KAR means the number of agreed bits over the total number of generated bits. A high success rate or KAR can considerably improve the efficiency of a device pairing protocol. Ideally, it should be identical for two legitimate devices, and as low as possible for an attacker.
- Randomness. Randomness of the key is of upmost importance in a cryptographic protocol because a key with low entropy can be easily cracked by an adversary. In device pairing system, the randomness of the generated keys is evaluated by the popular NIST test suite [102]. The NIST test suite provides 15 tests to evaluate the different randomness features. For example, The purpose of Frequency (Monobit) Test is to evaluate the proportion of zeroes and ones in the key sequence. The goal of Binary Matrix Rank Test is to check for linear dependence among fixed length substrings of the binary key string. The returned result of each test is a *p-value*, which indicates whether the key pass the NIST test or not. Conventionally, if $p\text{-}value \geq 0.01$, we say the key passes the corresponding test and it has high randomness.

Table 3 summarises the performance of representative works in each category. We have the following observations.

- Some studies do not explicitly report the three metrics above, making it hard to achieve a fair comparison with other systems. For example, Shake well before use [81] used false positive rate and false negative rate in their evaluation. In Miettinen et al. [83], the authors evaluated the performance of key revolution in different scenarios but did not give a clear indication about how long it takes to generate a 128 bit key.
- Some works do not evaluate their systems properly. To be specific, some direct key generation systems do not evaluate the randomness of the extracted keys using NIST test, such as Zeng et al. [151], Shake-n-Shack [112], Touch-and-Guard [130]. While in TDS [136], the authors suggested that their key can be generated by any sophisticated key generation method but do not point out which one. Moreover, since the key is generated from a random number generator, it is not necessary to apply NIST test to validate the randomness of the key.

- For wireless key generation, CSI-based systems can improve key generation significantly compared to RSSI-based approaches. Unfortunately, some communication technologies cannot provide CSI such as LoRa. Current works on LoRa [103, 104, 142] still use coarse-grained channel information such as RSSI. Therefore, a future research direction is investigating how to extract fine-grained channel information to improve KGR.
- For behavioural and physiological traits based key generation schemes, activities involving large displacements usually produce good results such as walking and shaking. The reason is that the SNR of the measured signal is higher as motion signals overwhelm noise when user walks or shakes hands. In contrast, physiological characteristics such as ECG and EMG have limited entropy resulting in low KGR. Moreover, they are not only hard to measure but also contain much noise (i.e., low SNR), which further reduces the performance. But these protocols can be applied in certain scenarios such as implantable IoT devices.
- Although new sensors provide more possibilities and options to pair various IoT devices, the KGR and KAR is relatively lower than their counterparts such as radio-based and accelerometer-based approaches. Therefore, more research efforts are required to further improve the performance of device pairing schemes using new sensors. However, as these new sensors are not available on off-the-shelf IoT devices and usually require customised hardware or prototype, these obstacles may hinder the progress of research in this direction.

Table 3. A quantitative comparison of different key generation schemes (– not available).

Source	Communication Technology/Sensors	Features	Literature	Direct Key generation	KGR (bit/s)	KAR (%)	Randomness
Radio	ZigBee	RSSI	Patwari et al. [88]	✓	10-22	97.8-99.46	✓
	Wi-Fi	RSSI	Zeng et al. [151]	✓	10	90	×
	Wi-Fi	CIR	Radio-telepathy [80]	✓	1.17	>84.15	✓
	Wi-Fi	CSI	TDS [136]	×	90-120	96.5-98	✓
	Bluetooth	RSSI	Premnath et al. [91]	✓	–	>79	✓
	LoRa	RSSI	LoRa-Key [142]	✓	18-31	98-100	✓
	LoRa	RSSI	Ruotsalainen et al. [104]	✓	–	71 - 85	✓
Audio	Mircophone/Speaker	Channel response	GeneWave [137, 138]	×	1024	88-100	×
		Channel tap	FREE [76]	✓	100-260	97-100	✓
IMU sensors	Accelerometer	Shake	Shake well before use [81]	ShaVe × ShaKe ✓	–	–	×
		Shake	Shake-n-Shack [112]	✓	≈ 98.4	100	×
		Walk	Gait-Key [141]	✓	28	97-100	✓
		Walk	Auto-Key [134]	✓	3.84-11	90-100	✓
		Walk	Ravedigar et al. [95]	✓	750	80-100	✓
		Gesture	Touch-and-Guard [130]	✓	7.84	98-100	×
	Mag	Movement	Magpairing [50, 51]	×	–	>90	×
Miscellaneous	Piezoelectric sensor	Walk	KEHKey [68]	✓	12.57	85-100	✓
		Heartbeat	H2B [69]	✓	3	95.6	✓
	ECG	Heartbeat	IMDGuard [139]	✓	2.84	92-100	✓
	EMG	Hand resonance	EMG-Key [146]	✓	5.51	88.84	✓
	Electrode	Body channel	Roeschlin et al. [97]	×	–	94.3-99.3	×
Hybrid	Microphone Light sensor	–	Miettinen et al. [83]	×	–	–	×
	Geophone Microphone Accelerometer Infrared motion sensor Power meter	–	Perceptio [38]	×	–	94.9	×
	Camera+IMU	Gesture	IDIoT [101]	×	–	92.2	×

Table 4. A qualitative comparison of different key generation systems (❍–low, ◗–medium, ●–high).

	Robustness	Usability	Practicability	Ubiquity	Security
Radio	●	●	●	◗	◗
Audio	●	❍	◗	◗	◗
IMU sensors	●	❍	●	◗	◗
Camera	●	◗	❍	❍	●
Miscellaneous sensors	◗	❍	❍	❍	●
Hybrid approachs	❍	❍	❍	❍	●

4.2 Subjective Metrics and Qualitative Comparison

In this paper, we use the following five subjective metrics to evaluate a key generation system for IoT devices. An ideal key agreement system should achieve high performance in each metric, i.e., they should achieve high robustness, usability, practicability, ubiquity and security.

- Robustness. It refers to whether a key generation protocol can achieve a high KAR, success rate or true positive rate.
- Usability. It refers to the performance of the device pairing system in terms of KGR, completion time, the degree of user involvement and user's ease-of-use perception [61].
- Practicability. It refers to the viability of a key generation scheme and is measured by whether the system can work without replying on special hardware.
- Ubiquity. It represents the environments a key generation system is applicable to. If a system can work in a variety of environments, it has high ubiquity, and vice versa.
- Security. It measures the security of a key agreement protocol against various attacks. The more attacks a key generation system can defend, the more secure it is.

Based on the definition above, we provide a qualitative comparison for existing systems and summarise the results in Table 4. It should be noted that comparison between different systems is not straightforward and challenging, and our goal is to provide users with a general understanding of the advantages and disadvantages of each technique. From Table 4, we can arrive at a conclusion that no universal approach exists, despite that different studies analyse key generation systems from different perspectives. A system suitable for one scenario may not be applicable to another environment. Meanwhile, there is always a trade-off between different requirements such as security and usability. For instance, a system easy to use is also easy to attack in the meantime. That is to say, a user needs to make efforts to enable a more secure system by participating the key agreement process (high degree of user involvement).

Overall, radio-based key generation system is a good choice because it achieves high robustness, usability, practicability and ubiquity. Although the security of such system is medium due to the broadcast nature of wireless radio link, radio-based schemes apply to a variety of IoT devices as most devices possess wireless communication functionalities. Audio-based systems suffer from low transmission distance and depend on microphone and speaker which are not always available on IoT devices. The usability and practicability, therefore, are relatively low. The usability of IMU sensor based schemes is low because they also require users to perform some actions such as walking, shaking, bumping to create some common context information. But their practicability is high thanks to the wide availability of IMU sensors on modern IoT devices. Miscellaneous sensors based systems, due to their dependence on special hardware, suffer from low usability, practicability and ubiquity. However, the security in turn benefits from these drawbacks. This is because the signals of such miscellaneous sensors such as user's biometrics are usually hard to copy, fabricate,

mimic and eavesdrop. Similar to miscellaneous sensors, multi-modality sensing approaches also achieve low usability, practicability and ubiquity. Additionally, the survey results in Table. 4 point out some future research directions because it reveals the research gap in each category. For example, the robustness of miscellaneous sensor and multi-modality sensing approaches need more research input.

5 ATTACKS AND COUNTERMEASURES

Due to the open nature of wireless communications, attacker's ability of observing users, and side channel information leakage, there are various attacks on an IoT key generation system. In this section, we summarise these attacks and discuss possible countermeasures to address these security issues. Because of the diversity in hardware and design principles, different key generation systems face different attacks. Therefore, we only focus on attacks encountered by most key generation systems.

We omit some common attacks that have been well investigated in IoT security such as MITM attack, replay attack, DOS attack etc. These attacks have been well examined and many approaches have been proposed to detect and counter such attacks. For example, a MITM attack can be solved by interlock protocol [96] or message authentication code (MAC). A replay attack can be addressed by using nounces, timestamps or tagging each message with a session ID [78]. There are numerous studies in the literature to detect and prevent DOS attack such as [126, 131]. For a comprehensive survey of attacks in IoT, interested readers can refer to [23, 148].

5.1 Eavesdropping Attack

Eavesdropping attack is one of the typical attacking approaches in wireless networks. It has received much attention because many adversarial attacks often follow the eavesdropping activity, such as the MITM attack and the hear-and-fire attack [55]. The attacker, Eve, can simply sit somewhere in the propagation path and eavesdrop all the relevant network traffic for later analysis. Hence, it is easy to perform and hard to detect.

In a key generation protocol, Alice and Bob often need to exchange some information to correct the mismatches between their initial keys (this step is often called information reconciliation). So Eve can eavesdrop this information and utilise it to improve the success rate. There are two ways to address this issue.

- Design a key generation protocol that does not exchange any information. For instance, Ali et al. [2] proposed a zero reconciliation protocol for wearable devices. To eliminate reconciliation, they first proposed a filtering scheme to significantly improve RSSI correlation between the two communication parties without reducing entropy. Then, they designed an approach that can ensure near-perfect key agreement. The proposed system can achieve 99.8% key matching rate but the KGR is extremely low (only 0.057–0.141 bit/s).
- Key generation protocol needs to ensure that Eve still cannot recover the correct key even with information exchange. Most key generation systems adopt this strategy but in different ways. For example, Xu et al. [145] exchanged the indices of the samples used for key generation. With the eavesdropped information, the attacker can at most achieve 60% KAR. In [69, 142], the authors used compressive sensing to compress the generated keys into a lower dimension space. Even Eve intercepts the compressed signal, she cannot recover the original key due to the secrecy of compressive sensing theory [92].

Apart from the eavesdropper in radio-based key generation, there are other types of eavesdroppers such as accelerometer eavesdropper in accelerometer-based system [130] and audio eavesdropper in audio-based system [76]. Most studies find that if the distance between the eavesdropper and legitimate device exceeds a certain threshold, she

cannot use her measurements to generate the same key. Therefore, although eavesdropping attack is easy to perform, most key generation systems can defend it by careful design.

5.2 Predictable Channel Attack

Predictable channel attack means attackers can perform some regular actions intentionally to cause predictable changes in the received signal of legitimate devices. Jana et al. [46] first identified this attack and later it is found that the majority of RSSI-based key generation systems suffer from such attack. Unfortunately, the majority of RSSI-based key generation systems omit this attack in their evaluation such as [1, 94, 104, 142, 158, 162]. Recently, researchers found that CSI can counter this attack because it can extract channel information from different subcarriers and attacker's movement has different impact on different subcarriers [72, 136]. To counter predictable channel attack for RSSI-based key generation system, researchers have proposed a variety of methods by introducing different kinds of randomness into the channels, such as using multiple attennas [104], rotating attenna [127], transmitting random signals [128], and other schemes [15, 32, 34, 43, 77].

5.3 Mimicking Attack

In the mimicking attack, Eve has the ability to observe how the user is walking, shaking and moving. Then she can repeat user's actions with the aim of generating a similar signal, so that she can extract the same key. Mimicking attack is a major threat to motion-based key generation systems because user's motions are easy to observe and intimate. Although a large portion of these systems have verified the security against mimicking attacks such as [81, 111, 112, 141, 145]. The evaluation is conducted in a controlled environment and using small size dataset. For example, Shake well before use [81] recruited 30 participants while Walkie-Talkie [145] and Shake-n-Shack [112] recruited 20 volunteers only.

Traditionally, it is believed that user's biometrics are hard to copy and fabricate. However, recent studies found that attackers can hack a biometics-based authentication system by generating highly similar biometrics. For example, Eberz et al. [26] developed an ECG synthesise system to spoof an ECG-based authentication system. The synthetic ECG signals are very close to the ECG of a benign user and the hacking success rate is as high as 81%. The feasibility of using synthetic ECG signal to hack an ECG-based key generation system such as [69, 100] has not been investigated yet. But this technology clearly poses a threat to ECG-based key generation systems.

To mitigate the mimicking attack, we can use signals from multiple sensors such as [38, 71]. It is hard for Eve to obtain similar signals from different sensors by eavesdropping and mimicking. But the cost and practicability of using multi-modality sensing is a concern.

5.4 Side Channel Attack

Attackers are becoming more and more powerful with the development of technology. For example, Davis et al. [22] found that when an audio signal hits an object, it will cause minute vibrations which can be measured by high-speed camera. They proposed a system to recover the sound from a video. With this technology, attackers can hack vibration or acoustic based key generation systems such as [56, 76, 130]. Recent studies also showed that videos can be used to recover the motion data of people's activities [149]. Therefore, motion or vibration-based key generation schemes are vulnerable to a video analysis attack. In fact, Bruesch et al. [10] have demonstrated the feasibility of using video to estimate user's gait signals. To defend against such attacks, one solution is to introduce random signal in the key generation process as how researchers did to counter eavesdropping attack above. Another possible solution is to borrow the idea from face recognition with liveness detection system [8]. The purpose of liveness detection is to

Table 5. Vulnerability of key generation systems to different attacks. (❍–low, ◗–medium, ●–high).

	Eavesdropping Attack	Predictable Channel Attack	Mimicking Attack	Side channel Attack
Radio	●	●	◗	◗
Audio	●	❍	◗	❍
IMU sensors	●	◗	●	◗
Camera	●	◗	●	◗
Miscellaneous sensors	◗	❍	◗	❍
Hybrid approaches	◗	◗	❍	❍

detect whether a face is "alive" or just a fraudulent reproduction. Therefore, by incorporating liveness detection, a key generation system can defend such attacks when they reproduce a similar signal from side channel information.

5.5 Summary

The vulnerability of key generation systems subject to different attacks is summarised in Table 5. We can see that different key generation systems have varied vulnerability levels to attacks.

The rapid development of technology is a double-edged sword. On the one hand, it brings more opportunities for researchers to design novel IoT key generation systems by using novel algorithms (e.g., deep learning [134]) and hardware (e.g., bio-sensors [97]). On the other hand, attackers can use more powerful devices (e.g., high-speed camera [22]) to perform more advanced attacks. Therefore, in addition to the above well studied attacks, researchers should consider potential attacks especially that exploit side channel information leakage. Additionally, when we survey the literature, we find that almost all the studies focus on developing novel key generation systems but very limited work has been done to analyse the vulnerabilities of existing systems. Some challenging studies are hard to conduct but of great value. To name a few, Edman et al. [27] challenged the common assumption in physical layer key generation that if Eve is more than half wavelength away from Alice or Bob, her channel measurements have low correlation with that of Alice and Bob. Instead, they found that there is a strong correlation in Eve's channel measurements which is contradictory to previous results. Bruesch et al. [10] analysed the security of several gait-based key generation system and pointed out that there is a bias in the generated keys. Therefore, studies from the perspective of attackers need more research efforts.

In addition to the attacks above, the generated keys may also suffer from poor randomness and key collision. The poor randomness will make the key easy to be hacked, and key collision may lead to duplicated keys in the key generation process. As mentioned in Section 4.1, key randomness is evaluated by NIST test. However, Table 3 reveals that a large portion of work do not verify the randomness of the generated keys. Therefore, the usability of these schemes in real applications is still questionable. Key collision has been rarely mentioned in the previous studies because the focus of prior work is whether Eve can generate the same key as Alice and Bob rather than if Alice and Bob will generate the same key multiple times. Therefore, key randomness and key collision require more attention in the future research.

6 CHALLENGES AND DIRECTIONS

So far, we have surveyed recent advances on IoT key generation, compared their performance and analysed various security issues. A number of research challenges still require further investigation. We discuss some of them and point out several future directions in this section.

- **Key Generation for Emerging Technologies.** Previous radio-based key generation works have been mainly focused on short range communications such as Wi-Fi and ZigBee. However, limited efforts have been made in key generation using new wireless communication technologies such as Low power wide area networks (LPWAN) and 5G. LPWAN have started to prevail in the last few years, such as LoRa/LoRaWAN, NB-IoT. The key challenge for LPWAN is channel reciprocity may not hold any more for those techniques [142]. LoRaWAN protocol specifies a one-second delay between the uplink and downlink transmissions, which will significantly impact the channel reciprocity. NB-IoT employs the FDD duplex mode where the channel reciprocity may not hold at all [65]. Therefore, how to key generate keys in low channel reciprocity scenarios remains an open research problem. Another hot communication technology is 5G which uses several new features such as mmWave, massive MIMO and highly directional beamforming [147]. The current study on 5G key generation still relies on simulation and practical key generation systems have not been developed yet. These new communication technologies bring not only challenges but also opportunities. For instance, high directional beamforming can be used to thwart co-located attackers in key generation [49]. We believe that designing key generation systems for these emerging communication technologies will be a hot research direction in the future.
- **Group Key Generation.** With the growing number of IoT devices, it is more common to pair a group of IoT devices in the same network or context. Unfortunately, most existing key generation systems work in peer-to-peer communication mode. While many studies have been conducted in group key generation [33, 73, 74, 95, 129, 140], they suffer from either efficiency or practicability issues. Traditional pairwise key generation protocols cannot be directly extended to group key generation scenarios. This is because the secret information between a pair of legitimate devices cannot be efficiently and securely distributed to other IoT devices. The naive solution is first to apply pairwise key generation schemes to generate a secure channel between each pair of nodes, then exchange some information to agree on the same group key. However, the computation and communication overhead of this approach increases linearly with the group size. Some solutions are impracticable because off-the-shelf IoT devices cannot provide the channel characteristics they used (e.g., phase [129]). Therefore, how to design an efficient and practical group key generation protocol remains an open question.
- **User Friendliness.** From a user-friendliness point of view, the user needs to have minimal involvement during key generation process. Unfortunately, the majority of systems described in this paper require user in the loop. The user plays a crucial role in some key generation systems, such as introducing randomness by shaking [81, 112] or walking [141, 145], comparing results [82, 105]. Even for radio-based key generation when two devices are static, the channel variance is caused by moving subjects or objects in the environment. This is why several previous surveys classify key generation systems based on HCI [20, 148]. For example, Chong et al. [20] provided an in-depth analysis of device pairing schemes from the perspective of user involvement. A desirable key generation system requires as little user involvement as possible. However, a highly user-friendly key generation system does not come for free but it decreases the performance. For example, the zero-interaction device pairing scheme proposed by Miettinen et al. [83] does not need user interaction but requires a long time to complete authentication. Therefore, how to design a fast and practical key generation system with little user involvement requires further investigation.
- **Balancing Different Design Requirements.** While the battery life and processing capability of IoT devices have been greatly improved over the past few years, some categories of devices are still limited by on-board resources such as wearable and IMD devices. Resource constraints have been long identified as the primary challenge in designing an IoT system and researchers have made significant efforts and progress to find a

balance between performance and resource consumption. With regards to key generation protocols, this trade-off becomes more complex. As mentioned earlier, there are several requirements of a desirable IoT key generation protocol such as security, efficiency and usability. There is a fundamental tension between these goals, particularly when examining these goals in the context of realistic application scenarios. Unfortunately, finding a suitable balance between these tensions is non-trivial. Therefore, we believe that the conflicting requirements of security, reliability, and usability in IoT devices will still be a research problem in the near future and motivate more inventive works.

- **Theory vs Practice.** Many studies are based on theoretical analysis and simulation evaluation [129, 140, 154, 159], while many other studies are based on real-world measurements using off-the-shelf hardware [29, 51, 104, 112, 141, 145]. Only a small portion of studies in the literature present both theoretical analysis and practical validation such as [13, 142]. This is probably because the results obtained from theory may not apply to real-world measurements directly. For example, according to wireless communication theory [31], the channel will be statistically uncorrelated if two devices are separated by half wavelength away. In practice, however, this is not always true because of the poor multi-path conditions and interference in some environments [27, 94]. As another example, although channel phase randomness has been extensively investigated for key generation [129, 133], it is only validated in simulation. Unfortunately, off-the-shelf devices cannot provide accurate channel phase information due to noise and offset [153]. Therefore, a solid and rigorous work needs both theory support and field validation. Unfortunately, this gap has not been filled so far.

7 CONCLUSION

IoT is seen as the future of the world. Over the past decade, a large variety of IoT devices have hit the market. Therefore, ensuring secure communication in IoT system is of the upmost importance. Accordingly, the number of research articles related to secure D2D communication has been increasing exponentially. A large number of key generation systems have been proposed and designed. In this paper, we have reviewed, analysed, and compared recent solutions. Based on a novel taxonomy, we categorised existing works based on the hardware interface used in the device pairing systems. Moreover, we analysed the security of current key generation systems and pointed out several potential future research directions. Although we have reviewed more than 100 articles in this survey, the list of existing systems is by no means exhaustive but covers the majority of recent advances and directions. We hope this survey can help researchers identify research gaps and find solutions easily. We also would like to invite all researchers to broaden this exciting area and provide new insights.

ACKNOWLEDGMENTS

This work is supported by the APRC grant (Project No. 9610485) and the Start-up grant (Project No. 7200642) from City University of Hong Kong.

REFERENCES

[1] S.T. Ali, V. Sivaraman, and D. Ostry. 2014. Eliminating Reconciliation Cost in Secret Key Generation for Body-Worn Health Monitoring Devices. *IEEE Transactions on Mobile Computing* 13, 12 (December 2014), 2763–2776.

[2] Syed Taha Ali, Vijay Sivaraman, and Diethelm Ostry. 2012. Zero reconciliation secret key generation for body-worn health monitoring devices. In *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*. ACM, Tucson, Arizona, USA, 39–50.

[3] Amir Anees and Yi-Ping Phoebe Chen. 2018. Discriminative binary feature learning and quantization in biometric key generation. *Pattern Recognition* 77 (2018), 289–305.

[4] 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 (Nov. 2005), 3776–3784.

[5] Dania Qara Bala and Bhaskaran Raman. 2020. PHY-Based Key Agreement Scheme using Audio Networking. In *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*. IEEE, Bengaluru, India, India, 129–136.

[6] Sharu Bansal and Dilip Kumar. 2020. IoT Ecosystem: A Survey on Devices, Gateways, Operating Systems, Middleware and Communication. *International Journal of Wireless Information Networks* (2020), 1–25.

[7] Shu-Di Bao, Carmen CY Poon, Yuan-Ting Zhang, and Lian-Feng Shen. 2008. Using the timing information of heartbeats as an entity identifier to secure body sensor network. *IEEE transactions on information technology in biomedicine* 12, 6 (2008), 772–779.

[8] Wei Bao, Hong Li, Nan Li, and Wei Jiang. 2009. A liveness detection method for face recognition based on optical flow field. In *2009 International Conference on Image Analysis and Signal Processing*. IEEE, Taizhou, China, 233–236.

[9] R Bousseljot, D Kreiseler, and A Schnabel. 1995. Nutzung der EKG-Signaldatenbank CARDIODAT der PTB über das Internet. *Biomedizinische Technik/Biomedical Engineering* 40, s1 (1995), 317–318.

[10] Arne Bruesch, Le Nguyen, Dominik Schürmann, Stephan Sigg, and Lars C Wolf. 2019. Security Properties of Gait for Mobile Device Pairing. *IEEE Transactions on Mobile Computing* 19, 3 (2019).

[11] Ileana Buhan, Jeroen Doumen, Pieter Hartel, and Raymond Veldhuis. 2007. Secure ad-hoc pairing with biometrics: SAfE. *Proceedings of IWSSI* (2007), 450–456.

[12] M Bulenok, Iulia Tunaru, L Biard, Benoît Denis, and Bernard Uguen. 2016. Experimental channel-based secret key generation with integrated ultra wideband devices. In *Proc. 27th IEEE Int. Symp. Personal Indoor Mobile Radio Commun. (PIMRC)*. IEEE, Valencia, Spain, 1–6.

[13] Liang Cai, Kai Zeng, Hao Chen, and Prasant Mohapatra. 2011. Good Neighbor: Ad hoc Pairing of Nearby Wireless Devices by Multiple Antennas.. In *NDSS*.

[14] Chia-Hsin Owen Chen, Chung-Wei Chen, Cynthia Kuo, Yan-Hao Lai, Jonathan M McCune, Ahren Studer, Adrian Perrig, Bo-Yin Yang, and Tzong-Chen Wu. 2008. GAnGS: gather, authenticate'n group securely. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*. ACM, San Francisco, California, USA, 92–103.

[15] Dajiang Chen, Zhen Qin, Xufei Mao, Panlong Yang, Zhiguang Qin, and Ruijin Wang. 2013. SmokeGrenade: An efficient key generation protocol with artificial interference. *IEEE Transactions on Information Forensics and Security* 8, 11 (2013), 1731–1745.

[16] You Chen, Guyue Li, Chen Sun, Junqing Zhang, Eduard Jorswieck, and Bin Xiao. 2020. Beam-Domain Secret Key Generation for Multi-User Massive MIMO Networks. *Proc. ICC*, 1–6.

[17] Sriram Cherukuri, Krishna K Venkatasubramanian, and Sandeep KS Gupta. 2003. Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In *Proceedings of International Conference on Parallel Processing Workshops*. IEEE, Kaohsiung, Taiwan, 432–439.

[18] Ming Ki Chong and Hans Gellersen. 2010. Classification of spontaneous device association from a usability perspective. In *The 2nd International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Device Use*.

[19] Ming Ki Chong and Hans Gellersen. 2012. Usability classification for spontaneous device association. *Personal and Ubiquitous Computing* 16, 1 (2012), 77–89.

[20] Ming Ki Chong, Rene Mayrhofer, and Hans Gellersen. 2014. A survey of user interaction for spontaneous device association. *ACM Computing Surveys (CSUR)* 47, 1 (2014), 1–40.

[21] Cory T Cornelius and David F Kotz. 2012. Recognizing whether sensors are on the same body. *Pervasive and Mobile Computing* 8, 6 (2012), 822–836.

[22] Abe Davis, Michael Rubinstein, Neal Wadhwa, Gautham J Mysore, Frédo Durand, and William T Freeman. 2014. The visual microphone: Passive recovery of sound from video. *ACM Transactions on Graphics* (2014).

[23] Jyoti Deogirikar and Amarsinh Vidhate. 2017. Security attacks in IoT: A survey. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, Palladam, India, 32–37.

[24] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. 2008. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.* 38, 1 (2008), 97–139.

[25] R Dony et al. 2001. Karhunen-loeve transform. In *The transform and data compression handbook*. Vol. 1. CRC Press Boca Raton, 1–34.

[26] Simon Eberz, Nicola Paoletti, Marc Roeschlin, Marta Kwiatkowska, I Martinovic, and A Patané. 2017. Broken hearted: How to attack ECG biometrics. (2017).

[27] Matthew Edman, Aggelos Kiayias, and Bülent Yener. 2011. On passive inference attacks against physical-layer key extraction?. In *Proceedings of the Fourth European Workshop on System Security*. 1–6.

[28] Ettus. 2-17. Universal Software Radio Peripheral. https://www.ettus.com/.

[29] Rainhard Dieter Findling, Muhammad Muaaz, Daniel Hintze, and René Mayrhofer. 2014. Shakeunlock: Securely unlock mobile devices by shaking them together. In *Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia*. ACM, Kaohsiung Taiwan, 165–174.

[30] Mikhail Fomichev, Flor Álvarez, Daniel Steinmetzer, Paul Gardner-Stephen, and Matthias Hollick. 2017. Survey and systematization of secure device pairing. *IEEE Communications Surveys & Tutorials* 20, 1 (2017), 517–550.

[31] Andrea Goldsmith. 2005. *Wireless communications*. Cambridge university press.

[32] Shyamnath Gollakota and Dina Katabi. 2011. Physical layer wireless security made fast and channel independent. In *Proceedings of IEEE INFOCOM*. IEEE, Shanghai, China, 1125–1133.

[33] Zhonglei Gu and Yang Liu. 2016. Scalable group audio-based authentication scheme for IoT devices. In *2016 12th International Conference on Computational Intelligence and Security (CIS)*. IEEE, Wuxi, China, 277–281.

[34] René Guillaume, Stephan Ludwig, Andreas Müller, and Andreas Czylwik. 2015. Secret key generation from static channels with untrusted relays. In *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, Abu Dhabi, United Arab Emirates, 635–642.

[35] René Guillaume, Andreas Mueller, Christian T Zenger, Christof Paar, and Andreas Czylwik. 2014. Fair comparison and evaluation of quantization schemes for PHY-based key generation. In *Proc. 18th Int. OFDM Workshop (InOWo'14)*. Essen, Germany, 1–5.

[36] Daniel Halperin, Wenjun Hu, Anmol Sheth, and David Wetherall. 2011. Tool release: Gathering 802.11 n traces with channel state information. *ACM SIGCOMM Computer Communication Review* 41, 1 (2011), 53–53.

[37] Sana Tmar-Ben Hamida, Jean-Benoît Pierrot, and Claude Castelluccia. 2010. Empirical analysis of UWB channel characteristics for secret key generation in indoor environments. In *Proc. 21st IEEE Int. Symp. Personal Indoor Mobile Radio Commun. (PIMRC)*. IEEE, Instanbul, Turkey, 1984–1989.

[38] 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 *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 836–852.

[39] 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 18th International Workshop on Mobile Computing Systems and Applications*. ACM, Sonoma, CA, USA, 73–78.

[40] Ken Hinckley. 2003. Synchronous gestures for multiple persons and computers. In *Proceedings of the 16th annual ACM symposium on User interface software and technology*. ACM, Vancouver Canada, 149–158.

[41] Lars Erik Holmquist, Friedemann Mattern, Bernt Schiele, Petteri Alahuhta, Michael Beigl, and Hans-W Gellersen. 2001. Smart-its friends: A technique for users to easily establish connections between smart artefacts. In *Ubicomp' 2001*. Springer, 116–122.

[42] Chunqiang Hu, Xiuzhen Cheng, Fan Zhang, Dengyuan Wu, Xiaofeng Liao, and Dechang Chen. 2013. OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks. In *Proceedings of IEEE INFOCOM 2013*. IEEE, Turin, Italy, 2274–2282.

[43] Pengfei Huang and Xudong Wang. 2013. Fast secret key generation in static wireless networks: A virtual channel approach. In *Proceedings of IEEE INFOCOM 2013*. IEEE, Turin, Italy, 2292–2300.

[44] Texas Instruments. 2012. CC2530 second generation System-on-Chip solution for 2.4 GHz IEEE 802.15. 4/RF4CE/ZigBee.

[45] Anil K Jain, Arun Ross, and Salil Prabhakar. 2004. An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology* 14, 1 (2004), 4–20.

[46] 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 15th annual international conference on Mobile computing and networking*. ACM, Beijing China, 321–332.

[47] Qi Jiang, Xiaohan Huang, Ning Zhang, Kuan Zhang, Xindi Ma, and Jianfeng Ma. 2019. Shake to communicate: Secure handshake acceleration-based pairing mechanism for wrist worn devices. *IEEE Internet of Things Journal* 6, 3 (2019), 5618–5630.

[48] Long Jiao, Jie Tang, and Kai Zeng. 2018. Physical Layer Key Generation Using Virtual AoA and AoD of mmWave Massive MIMO Channel. In *Proc. IEEE Conf. Commun. Netw. Security (CNS)*. IEEE, Beijing, China, 1–9.

[49] Long Jiao, Ning Wang, and Kai Zeng. 2018. Secret Beam: Robust Secret Key Agreement for mmWave Massive MIMO 5G Communication. In *2018 IEEE Global Communications Conference (GLOBECOM)*. IEEE, Abu Dhabi, United Arab Emirates, 1–6.

[50] Rong Jin, Liu Shi, Kai Zeng, Amit Pande, and Prasant Mohapatra. 2014. MagPairing: Exploiting magnetometers for pairing smartphones in close proximity. In *2014 IEEE Conference on Communications and Network Security*. IEEE, San Francisco, CA, USA, 445–453.

[51] Rong Jin, Liu Shi, Kai Zeng, Amit Pande, and Prasant Mohapatra. 2015. Magpairing: Pairing smartphones in close proximity using magnetometers. *IEEE Transactions on Information Forensics and Security* 11, 6 (2015), 1306–1320.

[52] Ari Juels and Madhu Sudan. 2006. A fuzzy vault scheme. *Designs, Codes and Cryptography* 38, 2 (2006), 237–257.

[53] Ari Juels and Martin Wattenberg. 1999. A fuzzy commitment scheme. In *Proceedings of the 6th ACM conference on Computer and Communications Security*. ACM, Singapore, 28–36.

[54] Ronald Kainda, Ivan Flechais, and AW Roscoe. 2009. Usability and security of out-of-band channels in secure device pairing protocols. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM, Mountain View, California, USA, 1–12.

[55] Jung-Chun Kao and Radu Marculescu. 2006. Eavesdropping minimization via transmission power control in ad-hoc wireless networks. In *2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*, Vol. 2. IEEE, Reston, VA, USA, 707–714.

[56] Nikolaos Karapanos, Claudio Marforio, Claudio Soriente, and Srdjan Capkun. 2015. Sound-proof: usable two-factor authentication based on ambient sound. In *24th {USENIX} Security Symposium ({USENIX} Security 15)*. 483–498.

[57] Sara Khalifa, Guohao Lan, Mahbub Hassan, Aruna Seneviratne, and Sajal K Das. 2017. Harke: Human activity recognition from kinetic energy harvesting data in wearable devices. *IEEE Transactions on Mobile Computing* 17, 6 (2017), 1353–1368.

[58] Darko Kirovski, Michael Sinclair, and David Wilson. 2007. The martini synch: Using accelerometers for device pairing. *Microsoft Research, Washington* (2007), 1–16.

[59] ME Kiziroglou and EM Yeatman. 2012. Materials and techniques for energy harvesting. In *Functional Materials for Sustainable Energy Applications*. Elsevier, 541–572.

[60] Alfred Kobsa, Rahim Sonawalla, Gene Tsudik, Ersin Uzun, and Yang Wang. 2009. Serial hook-ups: a comparative usability study of secure device pairing methods. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM, Mountain View, California, USA, 1–12.

[61] 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.

[62] Guohao Lan, Weitao Xu, Sara Khalifa, Mahbub Hassan, and Wen Hu. 2016. Transportation mode detection using kinetic energy harvesting wearables. In *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*. IEEE, Sydney, NSW, Australia, 1–4.

[63] Guohao Lan, Weitao Xu, Dong Ma, Sara Khalifa, Mahbub Hassan, and Wen Hu. 2019. EnTrans: Leveraging Kinetic Energy Harvesting Signal for Transportation Mode Detection. *IEEE Transactions on Intelligent Transportation Systems* (2019).

[64] Jonathan Lester, Blake Hannaford, and Gaetano Borriello. 2004. Are You with Me?-Using Accelerometers to Determine If Two Devices Are Carried by the Same Person. In *Pervasive computing*. Springer, 33–50.

[65] Guyue Li, Aiqun Hu, Chen Sun, and Junqing Zhang. 2018. Constructing reciprocal channel coefficients for secret key generation in FDD systems. *IEEE Communications Letters* 22, 12 (2018), 2487–2490.

[66] Guyue Li, Chen Sun, Junqing Zhang, Eduard Jorswieck, Bin Xiao, and Aiqun Hu. 2019. Physical Layer Key Generation in 5G and Beyond Wireless Communications: Challenges and Opportunities. *Entropy* 21 (2019), 497.

[67] Zi Li, Qingqi Pei, Ian Markwood, Yao Liu, and Haojin Zhu. 2017. Secret key establishment via RSS trajectory matching between wearable devices. *IEEE Transactions on Information Forensics and security* 13, 3 (2017), 802–817.

[68] Qi Lin, Weitao Xu, Guohao Lan, Yesheng Cui, Hong Jia, Wen Hu, Mahbub Hassan, and Aruna Seneviratne. 2020. KEHKey: Kinetic Energy Harvester-based Authentication and Key Generation for Body Area Network. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, 1 (2020), 1–26.

[69] Qi Lin, Weitao Xu, Jun Liu, Abdelwahed Khamis, Wen Hu, Mahbub Hassan, and Aruna Seneviratne. 2019. H2B: Heartbeat-based secret key generation using piezo vibration sensors. In *Proceedings of the 18th International Conference on Information Processing in Sensor Networks*. ACM, Montreal, Quebec, Canada, 265–276.

[70] Yue-Hsun Lin, Ahren Studer, Yao-Hsin Chen, Hsu-Chun Hsiao, Li-Hsiang Kuo, Jonathan M McCune, King-Hang Wang, Maxwell Krohn, Adrian Perrig, Bo-Yin Yang, et al. 2010. Spate: small-group pki-less authenticated trust establishment. *IEEE Transactions on Mobile Computing* 9, 12 (2010), 1666–1681.

[71] Dong Liu, Jing Chen, Qisi Deng, Arouna Konate, and Zairong Tian. 2017. Secure pairing with wearable devices by using ambient sound and light. *Wuhan University Journal of Natural Sciences* 22, 4 (2017), 329–336.

[72] Hongbo Liu, Yang Wang, Jie Yang, and Yingying Chen. 2013. Fast and practical secret key extraction by exploiting channel response. In *Proceedings of IEEE INFOCOM)*. IEEE, Turin, Italy, 3048–3056.

[73] Hongbo Liu, Jie Yang, Yan Wang, and Yingying Chen. 2012. Collaborative secret key extraction leveraging received signal strength in mobile wireless networks. In *Proceedings of IEEE INFOCOM 2012*. IEEE, Orlando, FL, USA, 927–935.

[74] Hongbo Liu, Jie Yang, Yan Wang, Yingying Jennifer Chen, and Can Emre Koksal. 2014. Group secret key generation via received signal strength: Protocols, achievable rates, and implementation. *IEEE Transactions on Mobile Computing* 13, 12 (2014), 2820–2835.

[75] 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 (October 2012), 1484–1497.

[76] 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 Twentieth ACM International Symposium on Mobile Ad Hoc Networking and Computing*. ACM, Catania Italy, 311–320.

[77] Masoud Ghoreishi Madiseh, Stephen W Neville, and Michael L McGuire. 2012. Applying beamforming to address temporal correlation in wireless channel characterization-based secret key generation. *IEEE Transactions on Information Forensics and Security* 7, 4 (2012), 1278–1287.

[78] Sreekanth Malladi, Jim Alves-Foss, and Robert B Heckendorn. 2002. *On preventing replay attacks on security protocols*. Technical Report. IDAHO UNIV MOSCOW DEPT OF COMPUTER SCIENCE.

[79] 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 9th international conference on Mobile systems, applications, and services*. ACM, Bethesda, Maryland, USA, 211–224.

[80] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. 2008. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *Proc. 14th Annu. Int. Conf. Mobile Computing and Networking (MobiCom)*. ACM, San Francisco, California, USA, 128–139.

[81] Rene Mayrhofer and Hans Gellersen. 2009. Shake well before use: Intuitive and secure pairing of mobile devices. *IEEE Transactions on Mobile Computing* 8, 6 (2009), 792–806.

[82] Jonathan M McCune, Adrian Perrig, and Michael K Reiter. 2005. Seeing-is-believing: Using camera phones for human-verifiable authentication. In *2005 IEEE Symposium on Security and Privacy (S&P'05)*. IEEE, Oakland, CA, USA, 110–124.

[83] 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 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM,

Scottsdale, Arizona, USA, 880–891.

[84] Shahab Mirzadeh, Haitham Cruickshank, and Rahim Tafazolli. 2013. Secure device pairing: A survey. *IEEE Communications Surveys & Tutorials* 16, 1 (2013), 17–40.

[85] George B Moody and Roger G Mark. 2001. The impact of the MIT-BIH arrhythmia database. *IEEE Engineering in Medicine and Biology Magazine* 20, 3 (2001), 45–50.

[86] Paul A Obrist. 2012. *Cardiovascular psychophysiology: A perspective*. Springer Science & Business Media.

[87] Shijia Pan, Carlos Ruiz, Jun Han, Adeola Bannis, Patrick Tague, Hae Young Noh, and Pei Zhang. 2018. Universense: Iot device pairing through heterogeneous sensing signals. In *Proceedings of the 19th International Workshop on Mobile Computing Systems & Applications*. ACM, Tempe, Arizona, USA, 55–60.

[88] Neal Patwari, Jessica Croft, Suman Jana, and Sneha Kumar Kasera. 2010. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *IEEE Transactions on Mobile Computing* 9, 1 (January 2010), 17–30.

[89] Timothy J Pierson, Xiaohui Liang, Ronald Peterson, and David Kotz. 2016. Wanda: securely introducing mobile devices. In *Proceedings of IEEE INFOCOM 2016*. IEEE, San Francisco, CA, USA, 1–9.

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

[91] Sriram N Premnath, Prarthana L Gowda, Sneha Kumar Kasera, Neal Patwari, and Robert Ricci. 2014. Secret key extraction using Bluetooth wireless signal strength measurements. In *Proc. 11th Annu. IEEE Int. Conf. Sensing, Commun., and Networking (SECON)*. IEEE, Singapore, 293–301.

[92] Yaron Rachlin and Dror Baron. 2008. The secrecy of compressed sensing measurements. In *2008 46th Annual Allerton conference on communication, control, and computing*. IEEE, 813–817.

[93] Yanzhi Ren, Yingying Chen, Mooi Choo Chuah, and Jie Yang. 2013. Smartphone based user verification leveraging gait recognition for mobile healthcare systems. In *2013 IEEE International Conference on Sensing, Communications and Networking (SECON)*. IEEE, New Orleans, LA, USA, 149–157.

[94] Girish Revadigar, Chitra Javali, Wen Hu, and Sanjay Jha. 2015. DLINK: Dual link based radio frequency fingerprinting for wearable devices. In *2015 IEEE 40th Conference on Local Computer Networks (LCN)*. IEEE, Clearwater Beach, FL, USA, 329–337.

[95] Girish Revadigar, Chitra Javali, Weitao Xu, Athanasios V Vasilakos, Wen Hu, and Sanjay Jha. 2017. Accelerometer and fuzzy vault-based secure group key generation and sharing protocol for smart wearables. *IEEE Transactions on Information Forensics and Security* 12, 10 (2017), 2467–2482.

[96] Ronald L Rivest and Adi Shamir. 1984. How to expose an eavesdropper. *Commun. ACM* 27, 4 (1984), 393–394.

[97] Marc Roeschlin, Ivan Martinovic, and Kasper Bonne Rasmussen. 2018. Device Pairing at the Touch of an Electrode.. In *NDSS*, Vol. 18. 18–21.

[98] Michael Rohs and Beat Gfeller. 2004. *Using camera-equipped mobile phones for interacting with real-world objects*. na.

[99] Masoud Rostami, Wayne Burleson, Farinaz Koushanfar, and Ari Juels. 2013. Balancing security and utility in medical devices?. In *Proceedings of the 50th Annual Design Automation Conference*. ACM, Austin, Texas, USA, 1–6.

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

[101] Carlos Ruiz, Shijia Pan, Hae Young Noh, Pei Zhang, and Jun Han. 2020. IDIoT: Towards Ubiquitous Identification of IoT Devices through Visual and Inertial Orientation Matching During Human Activity. In *Proceedings of The ACM/IEEE International Conference on Internet of Things Design and Implementation (IoTDI)*.

[102] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, and Elaine Barker. 2001. *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. Technical Report. Booz-allen and hamilton inc mclean va.

[103] Henri Ruotsalainen and Stepan Grebeniuk. 2018. Towards Wireless Secret key Agreement with LoRa Physical Layer. In *Proc. Int. Conf. Availability, Reliability and Security*. Hamburg, Germany, 23.

[104] Henri Ruotsalainen, Junqing Zhang, and Stepan Grebeniuk. 2020. Experimental Investigation on Wireless Key Generation for Low Power Wide Area Networks. *IEEE Internet of Things Journal* 7, 3 (2020), 1745 – 1755.

[105] Nitesh Saxena, J-E Ekberg, Kari Kostiainen, and N Asokan. 2006. Secure device pairing based on a visual channel. In *2006 IEEE Symposium on Security and Privacy (S&P'06)*. IEEE, Berkeley/Oakland, CA, USA, 6–pp.

[106] Dominik Schürmann, Arne Brüsch, Stephan Sigg, and Lars Wolf. 2017. BANDANA—Body area network device-to-device authentication using natural gAit. In *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. IEEE, Kona, HI, USA, 190–196.

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

[108] Suranga Seneviratne, Yining Hu, Tham Nguyen, Guohao Lan, Sara Khalifa, Kanchana Thilakarathna, Mahbub Hassan, and Aruna Seneviratne. 2017. A survey of wearable devices and challenges. *IEEE Communications Surveys & Tutorials* 19, 4 (2017), 2573–2620.

[109] Jiacheng Shang and Jie Wu. 2020. AudioKey: a usable device pairing system using audio signals on smartwatches. *International Journal of Security and Networks* 15, 1 (2020), 46–58.

[110] Youssef El Hajj Shehadeh and Dieter Hogrefe. 2015. A survey on secret key generation mechanisms on the physical layer in wireless networks. *Security and Communication Networks* 8, 2 (2015), 332–341.

[111] Yiran Shen, Bowen Du, Weitao Xu, Chengwen Luo, Bo Wei, Lizhen Cui, and Hongkai Wen. 2020. Securing cyber-physical social interactions on wrist-worn devices. *ACM Transactions on Sensor Networks (TOSN)* 16, 2 (2020), 1–22.

[112] Yiran Shen, Fengyuan Yang, Bowen Du, Weitao Xu, Chengwen Luo, and Hongkai Wen. 2018. Shake-n-Shack: Enabling secure data exchange between smart wearables via handshakes. In *2018 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. IEEE, 1–10.

[113] Congcong Shi, Lei Xie, Chuyu Wang, Peicheng Yang, Yubo Song, and Sanglu Lu. 2019. iShake: Imitation-Resistant Secure Pairing of Smart Devices via Shaking. In *2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS)*. IEEE, Tianjin, China, 655–662.

[114] Kyung-Ah Shim. 2016. A survey of public-key cryptographic primitives in wireless sensor networks. *IEEE Communications Surveys and Tutorials* 18, 1 (2016), 577–601.

[115] Babins Shrestha, Nitesh Saxena, Hien Thi Thu Truong, and N Asokan. 2014. Drone to the rescue: Relay-resilient authentication using ambient multi-sensing. In *International Conference on Financial Cryptography and Data Security*. Springer, 349–364.

[116] IHS Statista. 2018. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). (2018).

[117] Ahren Studer, Timothy Passaro, and Lujo Bauer. 2011. Don't bump, shake on it: The exploitation of a popular accelerometer-based smart phone exchange and its secure replacement. In *Proceedings of the 27th Annual Computer Security Applications Conference*. ACM, Orlando, Florida, USA, 333–342.

[118] Yingnan Sun, Charence Wong, Guang-Zhong Yang, and Benny Lo. 2017. Secure key generation using gait features for body sensor networks. In *2017 IEEE 14th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*. IEEE, Eindhoven, Netherlands, 206–210.

[119] Bump Technologies. [n.d.]. http://bu.mp.

[120] David Tse and Pramod Viswanath. 2005. *Fundamentals of wireless communication*. Cambridge university press.

[121] Alex Varshavsky, Adin Scannell, Anthony LaMarca, and Eyal De Lara. 2007. Amigo: Proximity-based authentication of mobile devices. In *International Conference on Ubiquitous Computing*. Springer, 253–270.

[122] Krishna K Venkatasubramanian, Ayan Banerjee, and Sandeep KS Gupta. 2008. Plethysmogram-based secure inter-sensor communication in body area networks. In *Proceedings of MILCOM*. IEEE, San Diego, CA, USA, 1–7.

[123] Krishna K Venkatasubramanian, Ayan Banerjee, and Sandeep Kumar S Gupta. 2009. PSKA: Usable and secure key agreement scheme for body area networks. *IEEE Transactions on Information Technology in Biomedicine* 14, 1 (2009), 60–68.

[124] Hendrik Vogt, Zohaib Hassan Awan, and Aydin Sezgin. 2018. Secret-key generation: Full-duplex versus half-duplex probing. *IEEE Transactions on Communications* 67, 1 (2018), 639–652.

[125] Hendrik Vogt, Kevin Ramm, and Aydin Sezgin. 2016. Practical secret-key generation by full-duplex nodes with residual self-interference. In *Proc. 20th International ITG Workshop on Smart Antennas*. 1–5.

[126] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary. 2007. Wireless sensor network security: A survey. *Security in distributed, grid, mobile, and pervasive computing* 1 (2007), 367.

[127] Lin Wang, Haonan An, Haojin Zhu, and Wenyuan Liu. 2020. MobiKey: Mobility-based Secret Key Generation in Smart Home. *IEEE Internet of Things Journal* (2020).

[128] Qiuhua Wang, Mingyang Kang, Guohua Wu, Yizhi Ren, and Chunhua Su. 2020. A Practical Secret Key Generation Scheme Based on Wireless Channel Characteristics for 5G Networks. *IEICE Transactions on Information and Systems* 103, 2 (2020), 230–238.

[129] Qian Wang, Hai Su, Kui Ren, and Kwangjo Kim. 2011. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In *Proceedings of IEEE INFOCOM 2011*. IEEE, Shanghai, China, 1422–1430.

[130] Wei Wang, Lin Yang, and Qian Zhang. 2016. Touch-and-guard: secure pairing through hand resonance. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, Heidelberg Germany, 670–681.

[131] Yong Wang, Garhan Attebury, and Byrav Ramamurthy. 2006. A survey of security issues in wireless sensor networks. *IEEE Communications Surveys & Tutorials* 8, 2 (2006).

[132] J Welch, P Ford, R Teplick, and R Rubsamen. 1991. The Massachusetts General Hospital-Marquette Foundation hemodynamic and electrocardiographic database–comprehensive collection of critical care waveforms. *Clinical Monitoring* 7, 1 (1991), 96–97.

[133] Robert Wilson, David Tse, and Robert Scholtz. 2007. Channel identification: Secret sharing using reciprocity in ultrawideband channels. *IEEE Transactions on Information Forensics and Security* 2, 3 (2007), 364–375.

[134] Yuezhong Wu, Qi Lin, Hong Jia, Mahbub Hassan, and Wen Hu. 2020. Auto-Key: Using Autoencoder to Speed Up Gait-based Key Generation in Body Area Networks. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, 1 (2020), 1–23.

[135] Wei Xi, Xiangyang Li, Chen Qian, Jinsong Han, Shaojie Tang, Jizhong Zhao, and Kun Zhao. 2014. KEEP: Fast secret key extraction protocol for D2D communication. In *Proc. 22nd IEEE Int. Symp. of Quality of Service (IWQoS)*. IEEE, Hong Kong, 350–359.

[136] 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 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, Vienna, Austria, 616–627.

[137] Pengjin Xie, Jingchao Feng, Zhichao Cao, and Jiliang Wang. 2017. GeneWave: Fast authentication and key agreement on commodity mobile devices. In *2017 IEEE 25th International Conference on Network Protocols (ICNP)*. IEEE, Toronto, ON, Canada, 1–10.

[138] Pengjin Xie, Jingchao Feng, Zhichao Cao, and Jiliang Wang. 2018. GeneWave: Fast authentication and key agreement on commodity mobile devices. *IEEE/ACM Transactions on Networking* 26, 4 (2018), 1688–1700.

[139] Fengyuan Xu, Zhengrui Qin, Chiu C Tan, Baosheng Wang, and Qun Li. 2011. IMDGuard: Securing implantable medical devices with the external wearable guardian. In *Proceedings of IEEE INFOCOM*. IEEE, Shanghai, China, 1862–1870.

[140] Peng Xu, Kanapathippillai Cumanan, Zhiguo Ding, Xuchu Dai, and Kin K Leung. 2016. Group secret key generation in wireless networks: algorithms and rate optimization. *IEEE Transactions on Information Forensics and Security* 11, 8 (2016), 1831–1846.

[141] 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 (TOSN)* 13, 1 (2017), 1–27.

[142] Weitao Xu, Sanjay Jha, and Wen Hu. 2019. LoRa-Key: Secure Key Generation System for LoRa-based Network. *IEEE Internet of Things Journal* 6, 4 (2019), 6404 – 6416.

[143] Weitao Xu, Guohao Lan, Qi Lin, Sara Khalifa, Neil Bergmann, Mahbub Hassan, and Wen Hu. 2017. KEH-Gait: Towards a Mobile Healthcare User Authentication System by Kinetic Energy Harvesting. In *NDSS*.

[144] Weitao Xu, Guohao Lan, Qi Lin, Sara Khalifa, Mahbub Hassan, Neil Bergmann, and Wen Hu. 2018. KEH-Gait: Using kinetic energy harvesting for gait-based user authentication systems. *IEEE Transactions on Mobile Computing* 18, 1 (2018), 139–152.

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

[146] Lin Yang, Wei Wang, and Qian Zhang. 2016. Secret from muscle: Enabling secure pairing with electromyography. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*. ACM, Stanford CA USA, 28–41.

[147] Nan Yang, Lifeng Wang, Giovanni Geraci, Maged Elkashlan, Jinhong Yuan, and Marco Di Renzo. 2015. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Communications Magazine* 53, 4 (2015), 20–27.

[148] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao. 2017. A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal* 4, 5 (2017), 1250–1258.

[149] Guixin Ye, Zhanyong Tang, Dingyi Fang, Xiaojiang Chen, Kwang In Kim, Ben Taylor, and Zheng Wang. 2017. Cracking Android pattern lock in five attempts. In *Proceedings of the 2017 Network and Distributed System Security Symposium 2017 (NDSS 17)*. Internet Society.

[150] Hidir Yüzugüzel, Jari Niemi, Serkan Kiranyaz, Moncef Gabbouj, and Thomas Heinz. 2015. ShakeMe: Key generation from shared motion. In *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*. IEEE, Liverpool, UK, 2130–2133.

[151] 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 IEEE INFOCOM 2010*. IEEE, San Diego, CA, USA, 1–9.

[152] Christian T Zenger, Jan Zimmer, and Christof Paar. 2015. Security Analysis of Quantization Schemes for Channel-based Key Extraction. In *Workshop Wireless Commun. Security at the Physical Layer*. Coimbra, Portugal, 267–272.

[153] Dongheng Zhang, Yang Hu, Yan Chen, and Bing Zeng. 2020. Calibrating Phase Offsets for Commodity WiFi. *IEEE Systems Journal* 14, 1 (2020), 661 – 664.

[154] Junqing Zhang, Ming Ding, David López-Pérez, Alan Marshall, and Lajos Hanzo. 2019. Design of an Efficient OFDMA-Based Multi-User Key Generation Protocol. *IEEE Transactions on Vehicular Technology* 68, 9 (2019), 8842–8852.

[155] Junqing Zhang, Trung Q. Duong, Alan Marshall, and Roger Woods. 2016. Key Generation from Wireless Channels: A Review. *IEEE Access* 4 (March 2016), 614–626.

[156] Junqing Zhang, Biao He, Trung Q Duong, and Roger Woods. 2017. On the key generation from correlated wireless channels. *IEEE Communications Letters* 21, 4 (2017), 961–964.

[157] Junxing Zhang, Sneha K Kasera, and Neal Patwari. 2010. Mobility assisted secret key generation using wireless link signatures. In *Proceedings of IEEE INFOCOM 2010*. IEEE, San Diego, CA, USA, 1–5.

[158] Junqing Zhang, Alan Marshall, and Lajos Hanzo. 2018. Channel-Envelope Differencing Eliminates Secret Key Correlation: LoRa-Based Key Generation in Low Power Wide Area Networks. *IEEE Transactions on Vehicular Technology* 67, 12 (2018), 12462–12466.

[159] Junqing Zhang, Alan Marshall, Roger Woods, and Trung Q Duong. 2016. Efficient Key Generation by Exploiting Randomness from Channel Responses of Individual OFDM Subcarriers. *IEEE Transactions on Communications* 64, 6 (2016), 2578–2588.

[160] Junqing Zhang, Sekhar Rajendran, Zhi Sun, Roger Woods, and Lajos Hanzo. 2019. Physical layer security for the Internet of Things: Authentication and key generation. *IEEE Wireless Communications* 26, 5 (October 2019), 92–98.

[161] Jiansong Zhang, Zeyu Wang, Zhice Yang, and Qian Zhang. 2017. Proximity based IoT device authentication. In *Proceedings of IEEE INFOCOM 2017*. IEEE, Atlanta, GA, USA, 1–9.

[162] Junqing Zhang, Roger Woods, Trung Q Duong, Alan Marshall, Yuan Ding, Yi Huang, and Qian Xu. 2016. Experimental Study on Key Generation for Physical Layer Security in Wireless Communications. *IEEE Access* 4 (August 2016), 4464–4477.

[163] Rong Zhang, Christian Vogler, and Dimitris Metaxas. 2004. Human gait recognition. In *2004 Conference on Computer Vision and Pattern Recognition Workshop*. IEEE, Washington, DC, USA, 18–18.

[164] Jizhong Zhao, Wei Xi, Jinsong Han, Shaojie Tang, Xiangyang Li, Yunhao Liu, Yihong Gong, and Zehua Zhou. 2012. Efficient and secure key extraction using CSI without chasing down errors. *arXiv preprint arXiv:1208.0688* (2012).