Cleveland State University

EngagedScholarship@CSU

Electrical Engineering & Computer Science Faculty Publications

Electrical Engineering & Computer Science Department

2023

A Survey of Wearable Devices Pairing Based on Biometric Signals

Jafar Pourbemany
Cleveland State University

Ye Zhu
Cleveland State University, y.zhu61@csuohio.edu

Riccardo Bettati
Texas A & M University

Follow this and additional works at: https://engagedscholarship.csuohio.edu/enece_facpub

Part of the Electrical and Computer Engineering Commons

How does access to this work benefit you? Let us know!

Repository Citation

Pourbemany, Jafar; Zhu, Ye; and Bettati, Riccardo, "A Survey of Wearable Devices Pairing Based on Biometric Signals" (2023). *Electrical Engineering & Computer Science Faculty Publications*. 512.
https://engagedscholarship.csuohio.edu/enece_facpub/512

This Article is brought to you for free and open access by the Electrical Engineering & Computer Science Department at EngagedScholarship@CSU. It has been accepted for inclusion in Electrical Engineering & Computer Science Faculty Publications by an authorized administrator of EngagedScholarship@CSU. For more information, please contact library.es@csuohio.edu.

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 January 2023, accepted 2 March 2023, date of publication 8 March 2023, date of current version 20 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3254499

SURVEY

A Survey of Wearable Devices Pairing Based on Biometric Signals

JAFAR POURBEMANY[1,2], **(Member, IEEE), YE ZHU**[1], **(Senior Member, IEEE), AND RICCARDO BETTATI**[3], **(Senior Member, IEEE)**

[1]Department of Electrical Engineering and Computer Science, Cleveland State University, Cleveland, OH 44115, USA
[2]Department of Quantitative Health Sciences, Cleveland Clinic, Cleveland, OH 44195, USA
[3]Department of Computer Science and Engineering, Texas A&M University, College Station, TX 77843, USA

Corresponding author: Jafar Pourbemany (pourbemany@ieee.org)

This work was supported in part by the National Science Foundation under Grant DGE-1821775.

ABSTRACT With the rapid growth of wearable devices, more applications require direct communication between wearable devices. To secure the communication between wearable devices, various pairing protocols have been proposed to generate common keys for encrypting the communication. Since the wearable devices are attached to the same body, the devices can generate common keys based on the same context by utilizing onboard sensors to capture a common biometric signal such as body motion, gait, heartbeat, respiration, and EMG signals. The context-based pairing does not need prior information to generate common keys. As context-based pairing does not need any human involvement in the pairing process, the pairing also increase the usability of wearable devices. A wide range of context-based pairing approaches has been proposed with different sensors and different biometric signals. Given the increasing popularity of wearable devices and applications of wearable devices, we believe that it is necessary to have a comprehensive review and comparison on the context-based pairing approaches for future research on the pairing. In this paper, we compare context-based pairing approaches and review common techniques used in pairing based on various biometric signals.

INDEX TERMS Authentication, biometrics, body area network, the Internet of Things, network security, pairing, security, sensor, spontaneous pairing, wearable device.

I. INTRODUCTION

Smart wearable devices can collect a variety of information about human activities and behaviors which makes them popular in clinical medicine and health care, health management, workplace, education, and scientific research. The wearable market is diversified with hundreds of products, including smartwatches, smart wristbands, smart glasses, smart jewelry, smart straps, smart clothes, smart belts, smart shoes, smart gloves, skin patches, and even implanted medical devices (IMD) [1], [2], [3], [4], [5], [6], [7], [8]. As Fig. 1 illustrates, there are many diverse types of wearable devices for different body parts that collect various physiological data and possibly make intelligent decisions based on the collected physiological data. Wearable devices are exploited in a wide range of applications [6]. For example, wearable devices can be used as health monitoring systems and health treatment systems. They can monitor vital signs like heart rate [9], [10], [11], respiratory rate [12], [13], [14], [15], body temperature [16], [17]. Others collect parameters like blood pressure [18], blood oxygen [19], blood glucose [20], to detect disorders. Some wearable devices also can help disabled patients to recover certain physical functions [21], [22], [23]. Wearable devices are applied beyond healthcare. For example, wearable devices can be used to recognize daily physical activities [24], [25], [26], [27], [28], [29], [30] or the activities that are related to specific sports [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47]. Other applications areas for wearable devices include payment management [4], [48], unlocking vehicles [49], keeping sensitive information (like passwords) [49], controlling paired devices [50], subject tracking [51], [52], fall detection [53], [54], [55], [56], [57], drowsiness detection [58],

The associate editor coordinating the review of this manuscript and approving it for publication was Eyuphan Bulut.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

[59], [60], environment monitoring [61], [62], virtual and augmented reality [63], [64], and spying [48].

Based on their applications, the wearable devices collect, analyze, and store the data. In some cases, the wearable device (e.g., pacemaker) may be equipped with actuators, which it may use to control important physiological functions of the wearer. Often, they need to share data or commands with the base station or other wearable devices. Data/command shared between wearable devices are usually sensitive, like stored credentials of the user or commands to adjust an IMD. Therefore, the communication should be protected by encryption, and the devices need to have a common key for encryption to ensure that the process has not been compromised by an attacker.

Many wearable devices use Bluetooth or Wi-Fi to connect to other smartphones, other wearables, or the Internet. To be able to send and receive data the new wearable device must establish a connection with the other device; this process is called pairing (also known as binding, coupling, bonding, or association [3]). For example, the user initially needs to pair a new smartwatch with their smartphone over Bluetooth or NFC channel before use. Some wearable medical devices, such as IMDs need to be paired to their external controllers to receive updates.

Traditional pairing techniques often require user actions, which can take various forms. A common approach is used in Bluetooth pairing: the user selects a target device from a list of available devices and then possibly uses a PIN for additional authentication [65]. However, the approaches that require an initial stage of network setup are not scalable as the number of wearables increases [66]. PIN-based approaches need interaction with the display, which may either be inconvenient or even impossible in many wearables [66], [67]. Furthermore, PIN-based pairing is vulnerable to observation attacks such as shoulder surfing [66]. Public key cryptography (PKC), on the other hand, cannot be used to create a secure key on wearable devices because it requires a public key infrastructure (PKI) [68]. In addition, it requires expensive computing methods that are not suitable for resource-limited IoT devices. To mitigate these limitations, various techniques have been proposed that take advantage of common features in different wearable devices. Pairing based on biometric signals is a natural choice because wearable devices are attached to the same body. Both behavioral biometrics (e.g., step counts) and physiological biometrics (e.g., heart rate) are used for wearable device pairing and authentication.

In this article, we survey context-based techniques that can be used to achieve automatic wearable pairing based on them. In Section II, we review a selection of survey papers on biometric-based approaches. Section III discusses the signals used for pairing smart wearables. In Section IV, different steps of a biometric-based pairing mechanism are surveyed. In Section V, we explore the most common adversary models. Limitations and challenges are presented in Section VI. Finally, Section VII concludes the paper.

II. RELATED STUDIES ON BIOMETRIC-BASED APPROACHES

Biometric signals are widely used for device authentication. A variety of context-based approaches are used in device authentication to verify user identity [69] on a unique device.

There are several surveys that have investigated different aspects of the security and authentication in the wireless body area network (WBAN) [70], [71]. In Table 1, we summarize the topics raised in surveys over the last ten years. Security essentials and existing attacks against WBAN have been addressed in Javadi and Razzaque [72]. They also discussed the significant constraints and challenges of security mechanisms. A detailed review of authentication schemes is conducted by Masdari and Ahmadzadeh [73]. The authors provided a taxonomy for authentication modalities that classifies them into three categories: biometric-based, channel-based, and cryptography-based. Mainanwal et al. [74] summarized the pros and cons of several security and privacy techniques and discussed the threats and challenges. Naik and Samundiswary et al. [75] surveyed the views on security and privacy essentials for WBAN. Keystroke dynamics are addressed in [76] and [77]. Abuhamad et al. [78] investigated the authentication protocols and OS-related security of smartphone users using behavioral biometrics.

The survey by Al-Janabi et al. [79] reviewed the major security and privacy problems in WBAN for healthcare applications, along with their state-of-the-art security solutions. The paper provides significant highlights on open issues and future research directions in WBANs. Zou et al. [80] explored the security problems of ubiquitous healthcare (U-Healthcare) related work. The survey by Narwal and Mohapatra [81] focuses on the analysis of authentication schemes in terms of main outcomes, strengths, and limitations. In addition to this, the authors discuss the architecture of WBAN, security essentials, and security attacks are discussed in detail. A taxonomy is proposed by Usman et al. [82] that classifies entities involved in healthcare systems. Security challenges at all WBAN tiers have been studied. The authors also identified open issues and highlighted future research directions. In another work, the cryptographic solutions have been reviewed by Malik et al. [83]. They provided a general survey on major security essentials and conceivable assaults at different layers.

Considering the security view of the complete WBAN system, Morales et al. [84] focused on various protocols in the WBAN architecture and provided a detailed review of security requirements such as confidentiality, integrity, privacy, authentication, and authorization. Komapara and Hölbl [85] reviewed the security and key agreement of Intra-BAN communication. They classified the existing key agreement schemes into traditional, physiological value-based, secret key-based, and hybrid key-based schemes. Furthermore, the authors provided a description of each class and analyzed the security strength of BAN against attacks. Nidhya and Karthik [86] emphasized the security attacks and

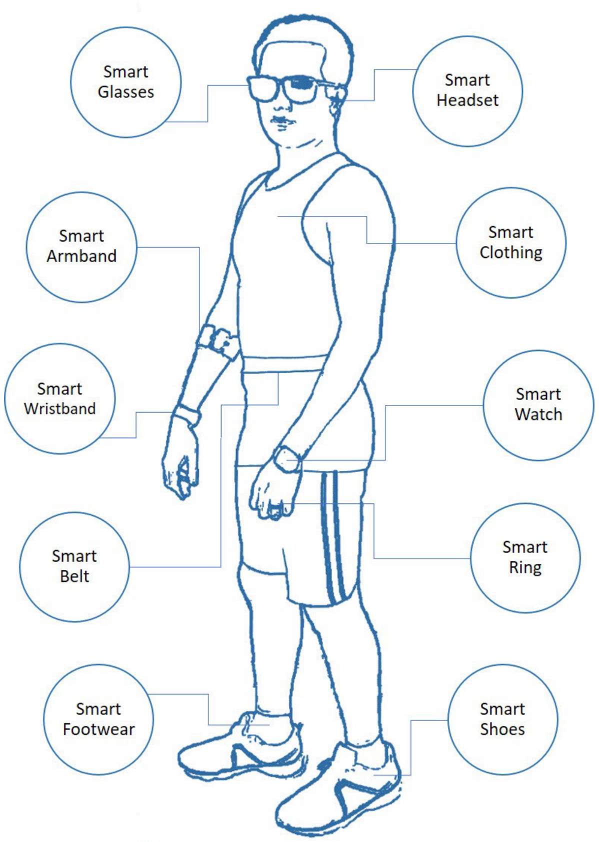

FIGURE 1. Different types of wearable devices.

security models at the data collection, transmission, and storage levels. Also, they assessed the privacy requirements and reliability of healthcare systems. Joshi and Mohapatra [87] investigated the design, functionalities, and workflow of the existing authentication schemes. They described the structure of authentication schemes and provided a detailed view on communication standards and design issues in WBAN. The paper also suggests methods to safeguard the key during key management.

Surveying security and privacy issues in WBAN, Chaudhary et al. [88] classified authentication schemes into four categories: physiological value-based, channel-based, proximity-based, and cryptographic-based. Furthermore, they summarized various schemes from different categories in a tabular form to highlight the features of each scheme effectively. The survey by Hussain et al. [89] was conducted to provide greater insight into authentication schemes. All in all, the survey presented a detailed discussion on security features, security attacks, strengths, limitations, and performance of the authentication schemes. Roy et al. [90] reviewed the major security and privacy issues in wireless sensor networks (WSNs) and WBANs. They conducted a comparative analysis of both networks based on their features, architecture, applications, and threats. In another work, Narwal and Mohapatra [91] explored the authentication schemes in different categories.

All the aforementioned studies surveyed a variety of methods using sensory signals to assist Internet of Things (IoT) device authentication. However, sensor data, especially biometric signals, can be used for pairing wearable devices as well. Indeed, biometric signals are the common point between wearable device authentication and pairing, whereas the goals and applications are different. This survey focuses on sensor-based pairing in wearable devices to provide more details about the challenges and limitations of sensors in such devices.

III. SIGNALS USED FOR PAIRING

Various types of sensors collect a variety of information from the human body and the environment. As Fig. 2 shows, several signals are used for context-based pairing, including motion, gait, electrocardiogram (ECG), photoplethysmogram (PPG), electromyogram (EMG), and seismocardiogram (SCG). Indeed, these sensors can provide auxiliary out-of-band (OOB) channels [95] as a feasible option to facilitate device pairing. We categorize and describe the signals used for wearable device pairing in recent papers in this section.

A. MOTION AND POSITION

Magneto-Inertial Measurement Unit (MIMU) sensors, including accelerometers, gyroscopes, and magnetometers, are the most common sensors in today's wearable devices. These sensors detect the user's motion and the heading of the device with respect to the Earth's magnetic north pole. The accelerometer measures acceleration in three orthogonal spatial dimensions, x, y, and z, where each axis denotes either the vertical, forward-to-backward, or left-to-right dimensions in meters per second squared [96]. The gyroscope measures the angular rotation about each of these axes in radians per second [97]. The magnetometer measures the strength of the local magnetic field along three orthogonal axes [98]. The user's body movement can be modeled using the information provided by these sensors. Hence, a variety of methods have been proposed to use such sensory data for authentication and pairing purposes.

For instance, in [99] and [100], the authors proposed to shake the two mobile devices held in one hand; in this way, the accelerometer reading could be used to generate matched keys on either frequency domain [99] or time-domain [100]. The authors demonstrate that the simultaneous shaking motion of two devices generates unique accelerometer readings that an adversary cannot easily mimic at a close distance. Shen et al. [101] proposed a method in which, using a similar motion pattern of handshaking, two devices on different bodies can be paired. Similarly, in [102], a handshake-based pairing scheme between wrist-worn smart devices is developed based on the observation that, by shaking hands, both wrist-worn smart devices conduct similar movement patterns. Hash functions and heuristic search trees were leveraged in [103] to propose a key exchange protocol based on accelerometer data while the user shakes devices together.

TABLE 1. Survey papers on the WBAN authentication - Content comparison.

Scheme	Year	Methods classifications	Knowledge-based methods	Motion	Gait	ECG	PPG	Advantages and disadvantages	Attack senarios	Future works
[77]	2011	■	■							
[72]	2013		■						■	
[76]	2013	■	■							
[74]	2015		■							
[73]	2016	■	■			■		■	■	
[75]	2016		■							
[92]	2016	■	■					■		
[93]	2016		■							
[94]	2016	■	■	■	■			■		
[80]	2017	■	■			■				■
[79]	2017		■						■	
[81]	2018		■			■		■	■	
[82]	2018	■							■	■
[83]	2018		■			■			■	
[84]	2018		■						■	
[85]	2018	■	■	■		■	■		■	
[86]	2019		■			■			■	
[87]	2019	■	■						■	
[88]	2019	■	■			■				
[89]	2019	■	■			■	■	■	■	
[90]	2020		■						■	
[91]	2021	■	■			■		■	■	■
[78]	2021	■	■	■	■			■		

In another work, Yüzugüzel et al. [104] propose to derive a shared key based on finding a small set of effective features from the shaking of two devices that are held together in one hand. Groza et al. [105] investigated the pairing of mobile devices based on shared accelerometer data under various transportation environments. Using multiple sensors (accelerometer and microphone), Cao et al. [106] presented a device-to-device (D2D) communication in which the user needs to hold two devices in one hand and randomly shake them for a few seconds. Jin et al. [98] proposed a scheme to pair smartphones at close distances by exploiting correlated magnetometer readings.

Table 2 shows a summary of features of several papers in the field of motion- and position-based device pairing.

B. GAIT

Gait recognition is the process of identifying an individual based on how he or she walks based on wearable sensor data, especially motion sensors (e.g., accelerometer and gyroscope) [109]. Due to the different properties of an individual's muscular-skeletal structure, gait patterns are fairly unique among individuals [110]. Hence, it can be determined if two devices are carried by the same person [111].

Various techniques exploit different features of gait to generate a common key for pairing wearable devices. Sun et al. [112] proposed a method to generate a symmetric key based on the timing information of gait. The authors used the Inter-Pulse-Interval (IPI) of consecutive gait as a common feature between the two devices. Schürmann et al. [113] presented a secure spontaneous authentication scheme that exploits correlation in acceleration sequences from devices worn or carried together by the same person to extract always-fresh secure secrets. In their method, BANDANA, they utilized instantaneous variations in gait sequences with respect to the mean. Walkie-Talkie [114] is another shared secret key generation scheme that allows two legitimate devices to establish a common cryptographic key by exploiting users' walking characteristics (gait). The authors exploit independent component analysis (ICA) for blind source separation (BSS) to separate accelerometer signals from different body movements such as arm swings and walking. In Gait-Key [115] Xu et al. extended their method in Walkie-Talkie to examine the effect of multi-level quantization on the pairing success rate. In [116] the same authors also proposed using spatial alignment instead of using BSS. A usability analysis of four gait-based device pairing schemes [103], [112], [113], [114] are presented in [117]. A summary of features of several gait-based pairing papers is shown in Table 3.

C. ECG AND PPG

The heart-beat is a promising option for wireless body area networks (WBANs) authentication and key generating schemes because its properties are unique, and their features differ from person to person [118]. Heart-beat signals can be easily collected, and they are hard to copy by other people in comparison to simple pin codes. It is more secure than traditional methods because it requires a user to be available at the time of authentication and pairing process [119], [120]. Heart-beat signals can usually be collected by ECG and PPG sensors. ECG sensors collect the electrical activity

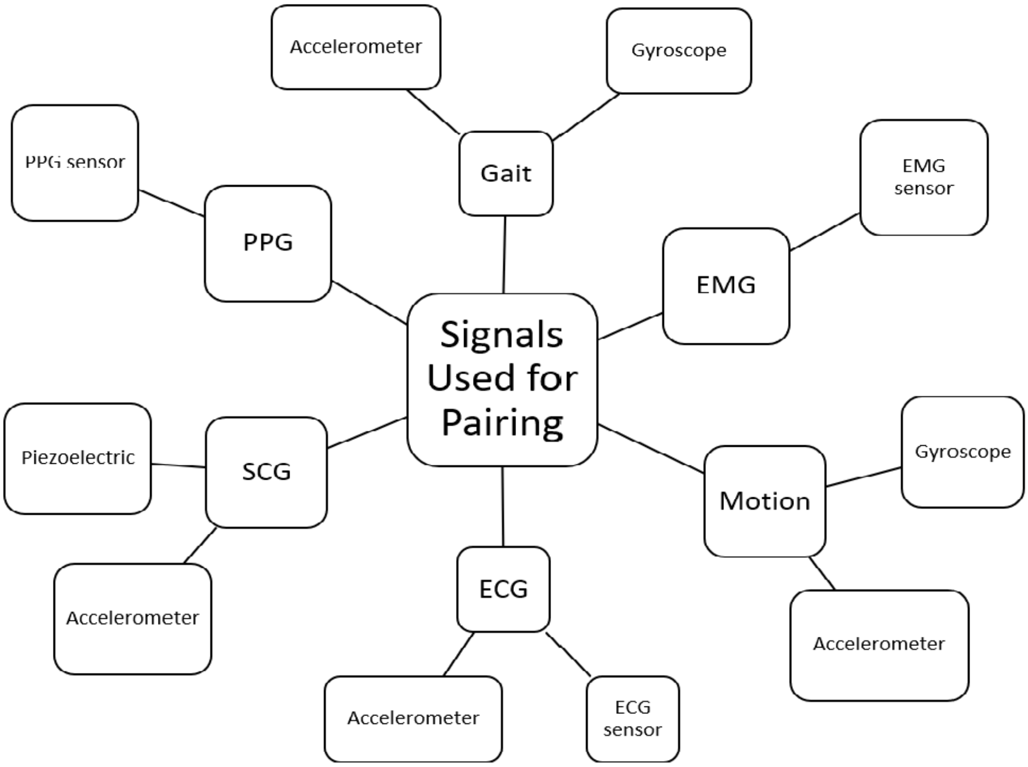

FIGURE 2. **Signals used for pairing.**

of heart muscles through electrodes attached to the body. PPG sensors which can be attached to different parts of the body like the ear and finger, detect the blood level transforms in the microvascular cot of tissue [121]. It illuminates the body and measures transforms in light absorption as blood circulates in the body. The heartbeat signal can also be measured by a seismocardiogram (SCG), which is the chest movement in response to the heartbeat. Accelerometers and piezo vibration sensors in wearable devices can measure SCG as well [122], [123], [124].

Various features extracted from heart-beat signals can be used for authentication and key generating purpose. The most important feature used in WBANs is heart rate variability (HRV) or R-R interval or inter-beat interval (IBI) or Inter-pulse Interval (IPI) [125], [126], [127] indicates the time interval between consecutive heart-beats [128]. Indeed, the fluctuations of heart rate around an average rate are shown by HRV [125]. As has been proven by several studies [129], [130], [131], HRV is highly random and can be used as a random source to generate keys. Since HRV is a unique characteristic for each person, it can be used as an authentication method to pair devices on the same body.

Rostami and Juels [130] proposed an HRV-based pairing method to authenticate external medical device controllers and programmers to IMDs. The authors introduce a touch-to-access policy using a time-varying physiological value (PV) by ECG readings. They utilized the statistical characterization of ECG for pairing wearable devices. Another pairing system called H2B is presented by Lin et al. [122], which utilizes piezo sensors to detect heartbeat signals and generate a secret key.

D. RESPIRATION

The respiratory signal is employed for key generation in [132]. The authors proposed Breathe-to-Pair (B2P) which is a pairing protocol for wearable devices that uses the wearer's breathing activity to confirm that the devices are in the same body-area network. The authors hypothesized that the gadgets extract and process the respiration signal using several types of sensors. They demonstrated B2P for the instance of two devices that extract shared dynamics from the wearer's breathing activity using respiratory inductance plethysmography (RIP) and accelerometer sensors. According to the authors, the B2P protocol can create a safe 256-bit key every 2.85 seconds (about one breathing cycle) and is resistant to impersonation attempts.

E. EMG

The EMG or electromyogram signals are the electrical signals generated by contractions of human muscles. According to

TABLE 2. Motion-based pairing papers and their features.

Scheme	Year	Sensor and Tools	Key Length (bit)	Duration (sec.)	Success Rate	Equal Error Rate (EER)	FAR	FRR	Bit Agreement	Computation Time	Energy Consumption	Frequency	Subjects	Device
[99]	2007	Acc	128	3			✓	✓				600	51 (32m 19f)	ADXL202JE accelerometers
[100]	2007	Acc	140		80%							200	10	
[103]	2012	Acc	64		75%							80-90		WiiMotes
[104]	2015	Acc	40	5	76%	4%	✓	✓				100	10 (5m 5f)	
[98]	2016	Magnetometer	128	4.5	>= 90%		✓					50		Various kinds of smartphones
[101]	2018	Acc	128	1	>99%	1.60%	✓	✓		✓	✓			Wrist-worn smart wearables
[102]	2019	Acc	128		close to 100%	1.5%	✓	✓		✓		100	16 (8m 8f)	iPhone6 and iPhone8
[106]	2019	Acc, Mic, Speaker					<5%	<2%	>90%	✓	✓	100	10 (6m 4f)	HUAWEI MATE8
[107]	2020	Acc	128	2.33						✓	✓	25		LaunchPad CC1350
[105]	2020	Acc	448	90						✓		5		LG Optimus L7 P700, Samsung J5
[108]	2020	Acc, Vibration	12.5	1	85.90%	5.00%						500	12 (5m 7f)	Arduino, accelerometer MPU-6050

TABLE 3. Gait-based pairing papers and their features.

Scheme	Year	Sensor and tools	Key length (bit)	Duration (sec.)	Success rate	Bit agreement	Computation Time	Energy Consumption	Frequency	Subjects	Device
[114]	2016	Acc	128	5		✓	✓	✓	100	20	Motorola E2
[112]	2017	Acc			79%	✓			100	5	iPhone
[115]	2017	Acc	128	4.6	98.30%	✓	✓	✓	100	20 (14m 6f)	Motorola E3
[113]	2018	Acc	16	12	>=75%				50	482 and 15	
[116]	2019	Acc	128	5		✓	✓	✓	100	21 (14m 6f)	Motorola E4

medical research [133], [134], the EMG signal is a quasi-random process, i.e., the average value of the EMG is correlated to the generated force of the muscle, but it has a random amplitude variation under a given force. In other words, there are stochastic variations of EMG amplitude for a unique gesture and force. Therefore, the EMG signals can be used as a secure source to generate secret keys in physically close contact for some wearable devices like the Myo armband [135], Athos gear [136], and Leo smart band [137]. Since detecting this kind of signal requires physical contact in close proximity, it is extremely difficult for an adversary to perform an eavesdropping attack. EMG-KEY is an EMG-based method proposed by Yang et al. [138] that leverages the EMG variation signal to generate a secret key for pairing two wearable devices.

A summary of different signals and sensors used for wearable device pairing is shown in Table 4.

IV. BIOMETRIC-BASED PAIRING MECHANISM

As Fig. 3 shows, a sequence of signal processing is needed to separate sources (signal and noise), detect and extract features/events, quantize features/segments, correct errors, amplify bit string, and create a shared key in the different devices. We explain these sequences in the following paragraphs.

TABLE 4. Different types of signals and sensors used for pairing.

Scheme	Name	Year	Signal	Sensor and tools	Description	Technique	Attack senarios
[132]	B2P	2022	Respiration	RIP, Acc	Extracting common dynamics from the user's respiration activity. The user needs to wear a smart shirt and attach a smartphone to his/her chest	Detecting respiration activity by chest movement	Impersonation, Video attack
[105]	Multi-Modal Transport	2020	Motion	Acc	Pairing of mobile devices based on accelerometer data under various transportation environments	Detecting the same variation in different devices	Full control of the communication channel
[108]	VibeRing	2020	Motion	Acc, vibration	Use of vibration, generated by a custom Ring, as an out-of-band communication channel to unobtrusively share a secret with a Thing	Detecting vibration of ring	Impersonating, eavesdropping
[102]	Shake to Communicate	2019	Motion	Acc	A secure handshake acceleration-based pairing mechanism for wrist-worn devices	Handshaking	Passive attack, active attacks
[106]	Sec-D2D	2019	Motion	Acc, Mic, speaker	Device-to-Device (D2D) communication by using multiple sensors, acceleration, and microphone by holding two devices in one hand and randomly shaking over a period of time	Shaking together	Impersonation
[116]		2019	Gait	Acc	Gait-based shared key generation system that assists two devices to generate a common secure key by exploiting the user's unique walking pattern	Using rotation matrix	Eavesdropping, adversary
[122]	H2B	2019	SCG	Piezo Vibration Sensors	Using piezo sensors to detect heartbeat signal and generate a secret key	Detecting piezo-based IPI	Passive eavesdropping attacks, Active presentation attacks, Active video attacks
[101]	Shake-n-Shack	2018	Motion	Acc	Enabling secure data exchange between smart wearables via handshakes	Handshaking	Mimicking attacks
[113]	BANDANA	2018	Gait	Acc	A secure spontaneous authentication scheme that exploits correlation in acceleration sequences from devices worn or carried together by the same person to extract always-fresh secure secrets.	Utilize instantaneous variations in gait sequences with respect to the mean	MITN, Mimic Gait, Video Recording, Attach Malicious Device
[112]		2017	Gait	Acc	Symmetric key generation scheme based on the timing information of gait	Inter-pulse Intervals (IPI) of consecutive Gait	
[115]	Gait-Key	2017	Gait	Acc	A shared secret key generation scheme that allows two legitimate devices to establish a common cryptographic key by exploiting users' walking characteristics (gait)	Using independent component analysis (ICA) for Blind Source Separation (BSS)	Impersonation attack, passive eavesdropping adversary, active spoofing attack
[98]	MagPairing	2016	Motion	Magnetometer	Pairing smartphones in close proximity by exploiting correlated magnetometer readings	Detecting correlated magnetometer readings	Passive attacks MITM attacks, replay attacks reflection attacks
[114]	Walkie-Talkie	2016	Gait	Acc	A shared secret key generation scheme that allows two legitimate devices to establish a common cryptographic key by exploiting users' walking characteristics (gait)	Using independent component analysis (ICA) for Blind Source Separation (BSS)	Impersonation attack, passive eavesdropping adversary, active spoofing attack
[138]	Secret from Muscle	2016	EMG	EMG	A system that can securely pair wearable devices by leveraging the electrical activity caused by human muscle contraction, Electromyogram (EMG), to generate a secret key	Detecting muscle contraction	Impersonation
[104]	ShakeMe	2015	Motion	Acc	Finding a small set of effective features from shaking of two devices which are held together in one hand	Shaking together	
[130]	H2H	2013	ECG	ECG	A system to authenticate external medical device controllers and programmers to Implantable Medical Devices (IMDs)	Detecting ECG-based IPI	Active adversaries, MITM
[103]	SAPHE	2012	Motion	Acc	Shake devices together, key exchange protocols based on accelerometer data that use only simple hash functions combined with heuristic search trees	Shaking together	MITM
[99]	Shake Well Before Use	2007	Motion	Acc	A method for device-to-device authentication that is based on shared movement patterns that a user can simply generate by shaking devices together.	Shaking together	MITM, online attack , offline attack
[100]		2007	Motion	Acc	Establish a secure connection between two devices by shaking them together	Shaking together	

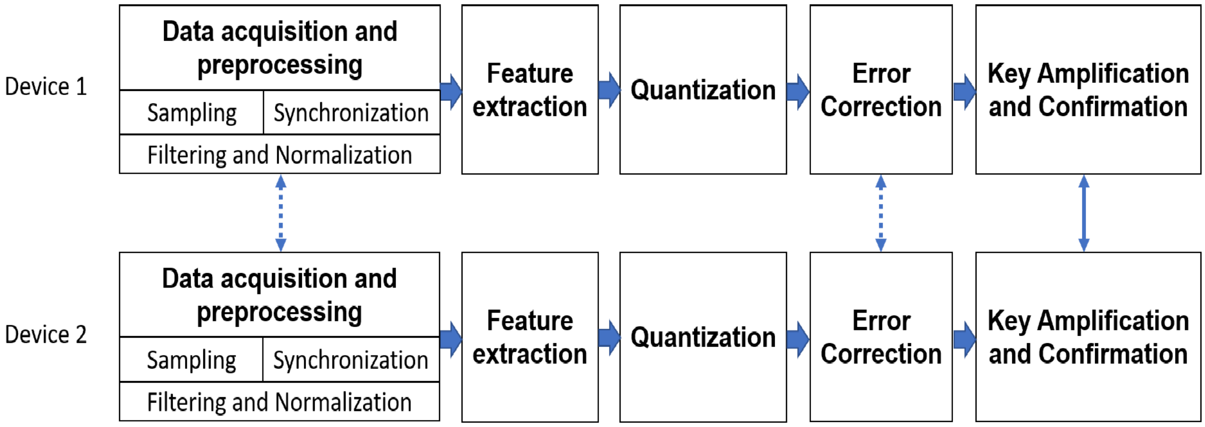
Device 1
Data acquisition and preprocessing
Sampling
Synchronization
Filtering and Normalization
Feature extraction
Quantization
Error Correction
Key Amplification and Confirmation
Device 2
Data acquisition and preprocessing
Sampling
Synchronization
Filtering and Normalization
Feature extraction
Quantization
Error Correction
Key Amplification and Confirmation

FIGURE 3. Context based pairing steps.

A. DATA ACQUISITION AND PREPROCESSING

1) SAMPLING

Sampling is the basic stage in which raw data is collected through various sensors, from the accelerometer to the ECG sensor. The speed and quality of data acquisition can directly affect key generation. Ambient noise and system noise cause the bit currents of both devices to mismatch and lead to unsuccessful pairing. On the other hand, the amount of sampling affects the amount of entropy extracted from the sensors' values. This is because the sampling rate determines the accuracy of the measurement: the higher the sampling rate, the more accurate the measured signal, and the more noise [139]. Therefore, as the sampling rate increases, the measurements will have more entropy.

2) SYNCHRONIZATION

Synchronization is required to ensure all legitimate devices capture samples at the same time. Since devices are unsynchronized by default, they must agree on a common starting point. Time asynchrony would result in a high bit string mismatch rate between devices after bit quantification, which would decrease the probability of successful key distribution. Since both smartphones are unsynchronized initially, they need user interaction for synchronizing the starting points of recording the shaking process. This task can be realized through direct user input, such as pressing a button. Alternatively, synchronization can be done by using a coordinator server [101], [140]. Hence, upon receiving the coordinator's synchronization signal, all the sensor nodes in the same network will start recording data [112]. However, we cannot ensure this kind of synchronization is always available for users. The wireless communication technique can also be exploited for synchronization purposes, e.g., a time-slotted channel hopping-based (TSCH) communication leads to temporal alignment between devices [141]. Synchronization can be at a sample level, i.e., within less than half the sample width, or at the event level, i.e., based on the onset of detected (explicit or implicit) events with the respective device. Depending on the sensors used for pairing, different events can be considered anchor points. For instance, the event can be a heel-strike [115], bumping the devices or shaking them together in one hand [104]. Although better synchronization reduces the bit mismatches at the next stage, the pairing protocol should support devices without a screen and keyboard and not impose strict synchronization on pairing devices when collecting ambient context information [138].

3) FILTERING AND NORMALIZATION

The sensor data must pass a filtering step to eliminate the relative effect of ambient and artificial noise and extract the desired signal (motion, gait, PPG, ECG, EMG, etc.) from the raw data. Depending on the signal type, the filtering stage involves using a high-pass filter, a mid-pass filter, or a low-pass filter. For best results, the cut-off frequency of these filters should be in the range of the minimum and maximum frequency of the desired signal; for example, 3 Hz can be a suitable cut-off frequency for a low-pass filter for a gait signal because the normal step frequency lies between 1.6-2.8 Hz [116]. In fact, by filtering the raw signal, the unwanted frequency components are removed. Since the magnitude ranges of sensors are quite different, after filtering, the signal is usually normalized to have a mean of zero and a variance of one.

B. FEATURE EXTRACTION

Similar raw signals lead to similar feature signals. The feature extraction process maintains the user's desired characteristics (for example, heartbeats IPI, respiration rate, gait, and movement) and eliminates irrelevant noises [142]. Feature extraction is one of the most important steps in a pairing that significantly affects the bit-generation process and its performance. In particular, selecting the appropriate features plays a key role in pairing because authentication is done by comparing the bits generated based on the extracted features. Features can be selected from both time and frequency domains [143]. Time domain features can be a wide variety of features including statistical characteristics [144], [145], [146] such as mean; standard deviation; variance; median; root mean square; maximum; minimum; Skewness; kurtosis; crest factor; the number of peaks; Peak-to-peak amplitude; zero crossing rate [147]; signal magnitude area [148]; interquartile range [149], [150]. In the frequency domain, we can select features like energy, entropy [151], maximum frequency index, mean frequency, and fast Fourier transform coefficients [152], to name but a few.

C. QUANTIZATION

Quantization represents a source's output with a large (possibly infinite) alphabet with a small alphabet. It is a many-to-one mapping and, therefore, irreversible. Quantization can be performed on a sample-by-sample basis or on a group of samples (by dividing the signal into segments). Quantizer encodes each sample/segment by specifying the range value at multiple levels. In this process, the raw signals or features will be quantized into bit vectors. The quantizer has a significant role in the security of the generated key. By making a biased quantization, a brute-force attack would become feasible. On the other hand, the quantizer can change the length of the final key. The quantizer maps each sample to a bit string whose length depends on the quantization levels. A quantizer that has 2^m quantizing levels can map each sample to m bits [139].

The bit representation can also affect security. The quantizer can map samples to either binary code or Gray code [153]. A Gray code encodes numbers so that adjacent numbers have a single digit differing by one. Therefore, in some cases, the Gray code can perform better in detecting noise in two consecutive samples [130]. In the recent pairing methods, various type of quantization approaches has been exploited, including pairwise nearest neighbor (PNN) quantization [100], standard decimal-to-binary quantizer [98], [104], decimal-to-Gray-code quantizer [122], [130], uniform quantizer [112], sigma-delta quantizer [105], and exploiting multiple thresholds [99], [101], [102], [103], [106], [107], [108], [113], [114], and [116].

D. ERROR CORRECTION

Due to the measured noise, there are usually mismatches in the quantized bits between the bit vectors produced by the two devices. Therefore, in the reconciliation stage, devices exchange a certain amount of information to correct all mismatches and generate a bit-by-bit matching key. We describe some of the most important error correction approaches used in wearable device pairing in the following.

1) INDEX CHECKING

This technique exchanges the index of the valid bit positions to reach a mutual agreement on which bits will be used in the final keys. For example, suppose the key generated by Alice's devices is [$110xx11x00$], while the key for Bob is [$1100x11xx0$], where x means the position where no valid bit is presented. Then both Alice and Bob inform each other of the positions of the valid bits, i.e., Alice sends $P_{Alice} = \{1, 2, 3, 6, 7, 9, 10\}$, and Bob sends $P_{Bob} = \{1, 2, 3, 4, 6, 7, 10\}$. Upon receiving the positions, they compare the received vector with the local one and agree that only the bits that are valid according to both vectors should be used. In this example, the agreed positions should be $\{1, 2, 3, 6, 7, 10\}$ so that the final symmetric keys are [110110]. This error correction technique is utilized in [101], [114], [116].

2) ERROR CORRECTION CODE (ECC)

Error correction code (ECC) is commonly used to control data errors through unreliable or noisy communication channels [154]. The central idea is that the sender encodes the message with additional information in an ECC form. The redundancy allows the receiver to detect a limited number of errors that may occur anywhere in the message, and often to correct these errors without retransmission [155]. Bose–Chaudhuri–Hocquenghem (BCH) [156], Reed-Solomon (RS) [157], Hamming [158], and binary Golay Codes [159] are some of the most common ECC used in the recent pairing methods [106], [108], [112], [113], [115], [138]. BCH codes form a class of cyclic error-correcting codes constructed using polynomials over a finite field (also called a Galois field). One of BCH codes' key features is that there is precise control over the number of symbol errors that can be corrected by the code during code design. Specifically, it is possible to design binary BCH codes can be designed that can correct multiple bit errors [160]. Reed-Solomon codes are the subset of BCH codes among the most powerful known classes of linear, cyclic block codes. Reed Solomon describes a systematic way of building codes that could detect and correct multiple random symbol errors. By adding t check symbols to the data, the RS code can detect any combination of up to t erroneous symbols or correct up to $t/2$ symbols. In addition, RS codes are suitable as multiple-burst bit-error correcting codes because a sequence of $b + 1$ consecutive bit errors can affect up to two symbols of size b [161]. Hamming code is a block code that can detect up to two simultaneous bit errors and correct single-bit errors. Binary Golay code is another linear error-correcting code in which a codeword is formed by taking 12 information bits and appending 11 check bits.

3) FUZZY CRYPTOGRAPHY

The fuzzy cryptographic scheme enables the compatibility of a certain amount of tolerable noise between the keys extracted from different devices by changing the error correction parameters and the length of the samples used. "Fuzzy," in this context, refers to the fact that the fixed values required for cryptography will be extracted from values that are close to but not identical to the original key, without compromising the security required [162], [163]. Jiang et al. [102] used this technique for error-correcting in their pairing algorithm. In [112], Sun et al. exploited fuzzy cryptography and BCH to provide the superior performance of false acceptance rate (FAR).

4) COMPRESSIVE SENSING

Compressed sensing theory has shown that sparse signals can be reconstructed exactly from remarkably few measurements [164]. Hence, it can be exploited as an error correction method [165], [166]. Compressed sensing is a technique where a signal x is multiplied by an $M \times N (M < N)$ sampling matrix to be sampled and compressed in a single operation. The signal x is recovered by finding the $l1$ norm of the sparse version of x, represented by the received samples y. In other words, out of the infinite signals that could have been used to create the received y, the sparsest one is recovered as the original signal. As long as x is "sparse enough," it can be recovered exactly using this technique. Lin et al. used this method in their error correction method [122].

E. KEY AMPLIFICATION

In the reconciliation phase, the devices may send some information to each other through a public wireless channel. Besides, some slightly different samples/segments may have the same bit string due to error correction. Thus, an adversary can infer some private information about the secret sequence. The privacy amplification process solves this issue. Key amplification helps to increase the final key's randomness to eliminate information leakage and increase entropy. Typically, two methods are used to combine keys generated from different segments and eliminate the correlation between them: the bitwise XOR function [114], [115], [116] and the hash function MD5 and SHA-256 [99], [100], [106], [107], [113], [130].

F. PERFORMANCE METRICS

The ultimate objective of pairing is to generate the same key on different devices independently. On the other hand, due to wearable devices' hardware limitations, all the operations in such devices are expected to use as little memory and computational power as possible and communicate the smallest amount of data with the fewest number of messages to achieve the lowest overall energy consumption. There are several evaluation metrics for evaluating pairing system performance, of which we have provided a brief description in the lines below [78], [167], and [85].

- *Bit generation rate:*
  The number of bits generated from the sensor readings per second.
- *Key generation rate:*
  The major performance metric for symmetric key generation is the success rate, or the probability that two keys generated by Alice and Bob can completely agree with each other (The probability of 100% matching). In other words, it is the percentage of identical keys generated by two devices in one second.
- *Bit agreement rate:*
  Bit Agreement Rate denotes the percentage of the matching bits of the two cryptographic keys generated by two devices
- *Computational cost:*
  The next important performance indicator is computational cost. It is important for schemes to be as computationally efficient as possible, because sensor nodes do not pose much processing power and because more computing uses up more of the very limited energy supply. The most common method to analyze computation costs is by measuring the amount of time it takes for the necessary operations to finish processing.
- *Energy consumption:*
  Energy consumption was measured by how much energy is spent on every bit of information produced.
- *Communication cost:*
  Measuring communication costs is very important because it is the most energy-consuming operation of them all. The most common ways of determining the communication cost are by the size of the sent data
- *False positive ratio:*
  The false positive ratio (FPR), also known as the false accept rate (FAR), is defined as the percentage of pairing attempts that incorrectly generate common keys among all the expected unsuccessful attempts. The metric indicates the likelihood of the adversary successfully pairing with a legitimate device by the adversary. The FPR can be computed as:$FPR = \frac{FP}{EN}$, where FP is the number of incorrectly generated keys, and EN is the expected number of unsuccessful attempts.
- *False negative ratio:*
  The false negative ratio (FNR), also known as the false reject rate (FRR), is defined as the percentage of incorrectly unsuccessful pairing attempts among all the expected successful pairing attempts. It indicates the probability that two legitimate devices attached to the same body can not pair successfully. FNR is computed as $FNR = \frac{FN}{EP}$, where FN is the number of incorrectly missed keys, and EP is the number of expected successful attempts.
- *Equal/crossover error rate (EER/CER):*
  Equal or crossover error rate (EER/CER) is the rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the intersection point between the FAR and the FRR curves. Equal Error Rate (EER) measures the trade-off between FAR and FRR and it is the value of FAR or FRR when the two false rates are equal.
- *Entropy:*
  Another important security metric in the pairing schemes is the entropy estimation. Entropy is the measure of uncertainty or randomness in the bit string generated from the measured signals. Higher entropy means more randomness in the generated bit string, or, in other words, fewer dependencies between the bits. Some papers use the NIST test suite [168] to estimate the entropy.

TABLE 5. Processes and techniques utilized in wearable device pairing studies.

Scheme	Synchronization	Filtering	Feature Extraction	Quantization	Bit Presentation	Error Correction	Amplification	Confirmation	Encryption
[101]	First peak		Dominant motion features, PCA	Thresholds	Binary	Index exchange			AES
[107]	Using gateway	Low-pass filter 2 Hz, mean filter		Hysteresis thresholding	Binary	Error correction code	Hash function	Challenge-Response (CR) mechanism	
[102]	First sample with magnitude of 0	Low-pass filter 5Hz	Acceleration magnitude of 0	Thresholds	Binary	Fuzzy cryptography		MAC (message authentication code)	
[105]	Exchange time message by an insecure channel	Low-pass filter and High-pass	Sign of each sample	Sigma-delta	Binary				EKE and SPEKE
[106]	First extreme point	Filtering Algorithm (EPEFA)	Extreme points extracting	Thresholds	Binary	BCH	Hash function MD5	Verify over audio and RF	AES
[104]	Bumping both devices	Low-pass FIR filter	10 statistics features	Decimal-to-binary	Binary				
[108]		Band-pass filter	5 statistics features	Thresholds	Binary	Hamming			AES
[103]				Thresholds	Binary	Hashed heuristic tree			
[99]	Onset of detected events		Coherence and quantized FFT coefficient	Thresholds	Binary		Hash function	DH, CKP	AES
[100]	Peak of cross-correlation function	Low-pass filter	Weight vector of segments, PCA	Pairwise nearest neighbor	Binary		Hash function		
[98]	Tap two devices			Decimal to binary	Binary			Diffie-Hellma	AES
[112]		Low-pass filter	Peaks of signal - IPIs	Uniform quantizer with q levels	Gray	Fuzzy commitment and BCH			
[113]		Madgwick and Chebyshev bandpass filter	Gait cycle detection	Threshold	Binary	BCH	Hash function	Password Authenticated Key Exchanges (PAKE), fuzzy cryptography	SHA-256
[114]	First heel-strike event	Low-pass filter		Thresholds	Binary	Index exchange	Bit-wise XOR function	MAC	AES
[115]	First heel-strike event	Low-pass filter		M-ary quantization	Binary	Reed-Solomon (RS)	Bit-wise XOR function	MAC	AES
[116]	First heel-strike event	Low-pass filter		Thresholds	Binary	Index exchange	Bit-wise XOR function	MAC, HMAC-MD5	AES
[130]		Discarding four bits of IPI	Inter-pulse interval (IPI)	Decimal to Gary code	Gray		Hash function	Neyman Pearson Lemma	AES-128, RSA
[122]	Time-slotted channel hopping-based (TSCH)	Savitzky-Golay (SG) filter, discarding the least 3 bits of IPI	Inter-pulse interval (IPI)	Decimal to Gary code	Gray	Compressive Sensing (CS)			
[138]		High-pass filter, notch filter, Chebyshev IIR filter	Rectified EMG signal	Fast dynamic time warping with three levels	Binary	Binary Golay Code			

A list of various processes and techniques used in wearable device pairing techniques is shown in the Table 5.

V. ADVERSARY MODEL/WWWWW/ATTACK SCENARIOS

Wearable device pairing can face various attacks, largely due to the broadcast nature of wireless communication between wearable devices. We must consider the presence of a strong attacker during key generation. Eve is fully aware of the system and control of the communication channel, meaning that she may monitor, jam, and modify messages at will. Various attacks on wearable device pairing can be categorized into passive and active attacks [91], [169], [170]. In this section, we provided a brief description of these attacks and discussed some common countermeasures.

A. PASSIVE ATTACKS

A passive attacker monitors the network for information but does not affect the target network. Passive attacks are performed as a preliminary act for the active attack [171]. Data Sniffing/Eavesdropping: Data Sniffing or Snooping attack is an old security issue. Sniffing is an incursion that involves a weak connection between the WBAN node and the server. The attacker passively accesses the data traffic (important health data, routing updates, node ID numbers, etc.) for later analysis by sitting between the unsecured network paths. Detecting a passive attack is exceedingly difficult and impossible in many cases because it does not involve any changes. However, protective measures can be implemented to stop it, including: Avoid posting sensitive information publicly, using random key distribution and strong encryption techniques to scramble messages, making them unreadable for any unintended recipients.

B. ACTIVE ATTACKS

An active attack involves using information gathered during a passive attack to compromise a user or network. Active attackers can cause devastation to the system as they attempt to intercept the wireless communication to change the information present on the target or en route to the target. There are several types of active attacks. In an impersonation/spoofing attack, an attacker pretends to be another user to access the system's restricted area. In a replay attack, the intruder steals a packet from the network and forwards that packet to a service or application as if the intruder were the user who originally sent the packet. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks are also examples of active attacks, both of which work by preventing authorized users from accessing a specific resource on a network or the internet (for example, flooding a device with more traffic than it can handle).

Unlike a passive attack, an active attack is more likely to be discovered quickly by the target upon execution. For instance, we can stop the attacker from impersonating the nodes by using authentication mechanisms and intrusion detection. To defend against reply attacks, nonces and time tokens can be used to introduce fresh data [172]. Authentication and anti-replay protection are the solutions suggested for avoiding denial of service [173], [174].

VI. LIMITATIONS AND CHALLENGES

The wearable device pairing methods should be lightweight, with fast computation, low storage, and low transmission overhead. Otherwise, the power and storage space of the body sensors could be quickly drained. There are different limitations and challenges when trying to pair devices using sensors' data. The main limitations of the current approaches are that they require the user to do a specific action (e.g., walking, handshake, gesture), and some devices should be placed on a certain part of the body (e.g., wrist, arm, head) to collect the desired signal. Also, some techniques need special sensors like ECG and EMG sensors, which are not used in common wearable devices. These requirements can limit the usability of the proposed techniques. On the other hand, some other challenges can affect the accuracy of the proposed methods; the user's motion artifact and health condition can challenge the pairing's success rate. In some pairing methods, users must remain static during the data collection phase. Furthermore, a recent study [117] revealed that gait-based pairing approaches are vulnerable to video attacks.

VII. CONCLUSION

Various context-based pairing protocols have been proposed in recent years. In this paper, we review the pairing research by classifying the pairing protocols according to biometric signal types, comparing pairing approaches, and reviewing common techniques used in context-based pairing. We also compare adversary models and countermeasures to common attacks on context-based pairing. We end the survey with a discussion on current challenges and limitations in context-based pairing. This survey is expected to be helpful for further research on context-based pairing.

REFERENCES

[1] K. Guk, G. Han, J. Lim, K. Jeong, T. Kang, E. K. Lim, and J. Jung, "Evolution of wearable devices with real-time disease monitoring for personalized healthcare," *Nanomaterials*, vol. 9, no. 6, p. 813, 2019.

[2] S. Vhaduri and C. Poellabauer, "Multi-modal biometric-based implicit authentication of wearable device users," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 12, pp. 3116–3125, Dec. 2019.

[3] M. K. Chong, R. Mayrhofer, and H. Gellersen, "A survey of user interaction for spontaneous device association," *ACM Comput. Surv.*, vol. 47, no. 1, pp. 1–40, Jul. 2014.

[4] S. Seneviratne, Y. Hu, T. Nguyen, G. Lan, S. Khalifa, K. Thilakarathna, M. Hassan, and A. Seneviratne, "A survey of wearable devices and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2573–2620, 4th Quart., 2017.

[5] A. Bianchi and I. Oakley, "Wearable authentication: Trends and opportunities," *it-Inf. Technol.*, vol. 58, no. 5, pp. 255–262, Oct. 2016.

[6] F. John Dian, R. Vahidnia, and A. Rahmati, "Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: A survey," *IEEE Access*, vol. 8, pp. 69200–69211, 2020.

[7] T. Poongodi, R. Krishnamurthi, R. Indrakumari, P. Suresh, and B. Balusamy, *Wearable Devices and IoT*. Cham, Switzerland: Springer, 2020, pp. 245–273.

[8] A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis," *IEEE Trans. Syst., Man, Cybern., C (Appl. Rev.)*, vol. 40, no. 1, pp. 1–12, Oct. 2010.

[9] S. Jayanth, M. B. Poorvi, R. Shreyas, B. Padmaja, and M. P. Sunil, "Wearable device to measure heart beat using IoT," in *Proc. Int. Conf. Inventive Syst. Control (ICISC)*, Jan. 2017, pp. 1–5.

[10] A. Majumder, Y. A. ElSaadany, R. Young, and D. R. Ucci, "An energy efficient wearable smart IoT system to predict cardiac arrest," *Adv. Hum.-Comput. Interact.*, vol. 2019, Feb. 2019, Art. no. 1507465.

[11] A. Brezulianu, O. Geman, M. D. Zbancioc, M. Hagan, C. Aghion, D. J. Hemanth, and L. H. Son, "IoT based heart activity monitoring using inductive sensors," *Sensors*, vol. 19, no. 15, p. 3284, Jul. 2019.

[12] S. Milici, J. Lorenzo, A. Lázaro, R. Villarino, and D. Girbau, "Wireless breathing sensor based on wearable modulated frequency selective surface," *IEEE Sensors J.*, vol. 17, no. 5, pp. 1285–1292, Mar. 2017.

[13] S. T. U. Shah, F. Badshah, F. Dad, N. Amin, and M. A. Jan, "Cloud-assisted IoT-based smart respiratory monitoring system for asthma patients," in *Applications of Intelligent Technologies in Healthcare*. Cham, Switzerland: Springer, 2019, pp. 77–86.

[14] I. Mahbub, S. A. Pullano, H. Wang, S. K. Islam, A. S. Fiorillo, G. To, and M. Mahfouz, "A low-power wireless piezoelectric sensor-based respiration monitoring system realized in CMOS process," *IEEE Sensors J.*, vol. 17, no. 6, pp. 1858–1864, Mar. 2017.

[15] D. Naranjo-Hernández, A. Talaminos-Barroso, J. Reina-Tosina, L. Roa, G. Barbarov-Rostan, P. Cejudo-Ramos, E. Márquez-Martín, and F. Ortega-Ruiz, "Smart vest for respiratory rate monitoring of COPD patients based on non-contact capacitive sensing," *Sensors*, vol. 18, no. 7, p. 2144, Jul. 2018.

[16] J. Wan, M. A. A. H. Al-awlaqi, M. Li, M. O'Grady, X. Gu, J. Wang, and N. Cao, "Wearable IoT enabled real-time health monitoring system," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, pp. 1–10, Dec. 2018.

[17] S. Yoshida, H. Miyaguchi, and T. Nakamura, "Development of tablet-shaped ingestible core-body thermometer powered by gastric acid battery," *IEEE Sensors J.*, vol. 18, no. 23, pp. 9755–9762, Dec. 2018.

[18] F. Lamonaca, E. Balestrieri, I. Tudosa, F. Picariello, D. L. Carni, C. Scuro, F. Bonavolonta, V. Spagnuolo, G. Grimaldi, and A. Colaprico, "An overview on Internet of Medical Things in blood pressure monitoring," in *Proc. IEEE Int. Symp. Med. Meas. Appl. (MeMeA)*, Jun. 2019, pp. 1–6.

[19] D. Murali, D. R. Rao, S. R. Rao, and M. Ananda, "Pulse oximetry and IoT based cardiac monitoring integrated alert system," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2018, pp. 2237–2243.

[20] B. Sargunam and S. Anusha, "IoT based mobile medical application for smart insulin regulation," in *Proc. IEEE Int. Conf. Electr., Comput. Commun. Technol. (ICECCT)*, Feb. 2019, pp. 1–5.

[21] C. Nave and O. Postolache, "Smart Walker based IoT physical rehabilitation system," in *Proc. Int. Symp. Sens. Instrum. IoT Era (ISSI)*, Sep. 2018, pp. 1–6.

[22] G. Yang, J. Deng, G. Pang, H. Zhang, and J. Li, "An IoT-enabled stroke rehabilitation system based on smart wearable armband and machine learning," *IEEE J. Translational Eng. Health Med.*, vol. 6, 2018, Art. no. 2100510.

[23] M. O. Agyeman and A. Al-Mahmood, "Design and implementation of a wearable device for motivating patients with upper and/or lower limb disability via gaming and home rehabilitation," in *Proc. 4th Int. Conf. Fog Mobile Edge Comput. (FMEC)*, Jun. 2019, pp. 247–252.

[24] J. Qi, P. Yang, M. Hanneghan, S. Tang, and B. Zhou, "A hybrid hierarchical framework for gym physical activity recognition and measurement using wearable sensors," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1384–1393, Apr. 2019.

[25] D. Castro, W. Coral, C. Rodriguez, J. Cabra, and J. Colorado, "Wearable-based human activity recognition using an IoT approach," *J. Sensor Actuator Netw.*, vol. 6, no. 4, p. 28, Nov. 2017.

[26] H. Huang, X. Li, S. Liu, S. Hu, and Y. Sun, "TriboMotion: A self-powered triboelectric motion sensor in wearable Internet of Things for human activity recognition and energy harvesting," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4441–4453, Dec. 2018.

[27] W. Lu, F. Fan, J. Chu, P. Jing, and S. Yuting, "Wearable computing for Internet of Things: A discriminant approach for human activity recognition," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2749–2759, Apr. 2019.

[28] L. Atallah, B. Lo, R. King, and G.-Z. Yang, "Sensor positioning for activity recognition using wearable accelerometers," *IEEE Trans. Biomed. Circuits Syst.*, vol. 5, no. 4, pp. 320–329, Aug. 2011.

[29] A. M. Nasrabadi, A. R. Eslaminia, P. R. Bakhshayesh, M. Ejtehadi, L. Alibiglou, and S. Behzadipour, "A new scheme for the development of IMU-based activity recognition systems for telerehabilitation," *Med. Eng. Phys.*, vol. 108, Oct. 2022, Art. no. 103876.

[30] A. M. Nasrabadi, A. R. Eslaminia, A. M. S. Enayati, L. Alibiglou, and S. Behzadipour, "Optimal sensor configuration for activity recognition during whole-body exercises," in *Proc. 7th Int. Conf. Robot. Mechatronics (ICRoM)*, Nov. 2019, pp. 512–518.

[31] E. Mencarini, A. Rapp, L. Tirabeni, and M. Zancanaro, "Designing wearable systems for sports: A review of trends and opportunities in human–computer interaction," *IEEE Trans. Human-Mach. Syst.*, vol. 49, no. 4, pp. 314–325, Aug. 2019.

[32] Z. Wang, M. Guo, and C. Zhao, "Badminton stroke recognition based on body sensor networks," *IEEE Trans. Human-Mach. Syst.*, vol. 46, no. 5, pp. 769–775, Oct. 2016.

[33] A. Raina, T. G. Lakshmi, and S. Murthy, "CoMBaT: Wearable technology based training system for novice badminton players," in *Proc. IEEE 17th Int. Conf. Adv. Learn. Technol. (ICALT)*, Jul. 2017, pp. 153–157.

[34] J. C. Maglott, J. Xu, and P. B. Shull, "Differences in arm motion timing characteristics for basketball free throw and jump shooting via a body-Worn sensorized sleeve," in *Proc. IEEE 14th Int. Conf. Wearable Implant. Body Sensor Netw. (BSN)*, May 2017, pp. 31–34.

[35] S. Bogers, C. Megens, and S. Vos, "Design for balanced engagement in mixed level sports teams," in *Proc. CHI Conf. Extended Abstr. Hum. Factors Comput. Syst.*, May 2017, pp. 994–1002.

[36] Z. Wang, H. Zhao, S. Qiu, and Q. Gao, "Stance-phase detection for ZUPT-aided foot-mounted pedestrian navigation system," *IEEE/ASME Trans. Mechatronics*, vol. 20, no. 6, pp. 3170–3181, Dec. 2015.

[37] Z. Wang, J. Wang, H. Zhao, N. Yang, and G. Fortino, "CanoeSense: Monitoring canoe sprint motion using wearable sensors," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2016, pp. 000644–000649.

[38] J. Pansiot, B. Lo, and G.-Z. Yang, "Swimming stroke kinematic analysis with BSN," in *Proc. Int. Conf. Body Sensor Netw.*, Jun. 2010, pp. 153–158.

[39] M. Bächlin, K. Förster, and G. Tröster, "SwimMaster: A wearable assistant for swimmer," in *Proc. 11th Int. Conf. Ubiquitous Comput.*, 2009, pp. 215–224.

[40] J. Häkkilä, M. Alhonsuo, L. Virtanen, J. Rantakari, A. Colley, and T. Koivumäki, "Mydata approach for personal health—A service design case for young athletes," in *Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2016, pp. 3493–3502.

[41] J. Haladjian, M. Reif, and B. Brügge, "VIHapp: A wearable system to support blind skiing," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput. ACM Int. Symp. Wearable Comput.*, 2017, pp. 1033–1037.

[42] E. Niforatos, A. Fedosov, I. Elhart, and M. Langheinrich, "Augmenting skiers' peripheral perception," in *Proc. ACM Int. Symp. Wearable Comput.*, Sep. 2017, pp. 114–121.

[43] H. Sharif, A. Eslaminia, P. Chembrammel, and T. Kesavadas, "Classification of activities of daily living based on grasp dynamics obtained from a leap motion controller," *Sensors*, vol. 22, no. 21, p. 8273, Oct. 2022.

[44] M. Pan, S. Salvi, and E. Brady, "Designing auditory feedback from wearable weightlifting devices," in *Proc. Extended Abstr. CHI Conf. Hum. Factors Comput. Syst.*, Apr. 2018, pp. 1–6.

[45] H. Havlucu, I. Bostan, A. Coskun, and O. Özcan, "Understanding the lonesome tennis players: Insights for future wearables," in *Proc. CHI Conf. Extended Abstr. Hum. Factors Comput. Syst.*, 2017, pp. 1678–1685.

[46] M. Lapinski, E. Berkson, T. Gill, M. Reinold, and J. A. Paradiso, "A distributed wearable, wireless sensor system for evaluating professional baseball pitchers and batters," in *Proc. Int. Symp. Wearable Comput.*, Sep. 2009, pp. 131–138.

[47] H. Ghasemzadeh, V. Loseu, E. Guenterberg, and R. Jafari, "Sport training using body sensor networks: A statistical approach to measure wrist rotation for golf swing," in *Proc. 4th Int. ICST Conf. Body Area Netw.*, 2009, pp. 1–8.

[48] C. Wang, J. Liu, X. Guo, Y. Wang, and Y. Chen, "WristSpy: Snooping passcodes in mobile payment using wrist-Worn wearables," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2019, pp. 2071–2079.

[49] T. Nguyen and N. D. Memon, "Smartwatches locking methods: A comparative study," in *Proc. SOUPS*, 2017.

[50] R. Kumar, V. V. Phoha, and R. Raina, "Authenticating users through their arm movement patterns," 2016, *arXiv:1603.02211*.

[51] R. C. Shit, S. Sharma, D. Puthal, and A. Y. Zomaya, "Location of things (LoT): A review and taxonomy of sensors localization in IoT infrastructure," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2028–2061, 3rd Quart., 2018.

[52] Y. Kim, H. Shin, and H. Cha, "Smartphone-based Wi-Fi pedestrian-tracking system tolerating the RSS variance problem," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun.*, Mar. 2012, pp. 11–19.

[53] W. Saadeh, S. A. Butt, and M. A. B. Altaf, "A patient-specific single sensor IoT-based wearable fall prediction and detection system," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 27, no. 5, pp. 995–1003, May 2019.

[54] W. Saadeh, M. A. Bin Altaf, and S. A. Butt, "A wearable neuro-degenerative diseases detection system based on gait dynamics," in *Proc. IFIP/IEEE Int. Conf. Very Large Scale Integr. (VLSI-SoC)*, Oct. 2017, pp. 1–6.

[55] L. Ren and Y. Peng, "Research of fall detection and fall prevention technologies: A systematic review," *IEEE Access*, vol. 7, pp. 77702–77722, 2019.

[56] N. Otanasap, "Pre-impact fall detection based on wearable device using dynamic threshold model," in *Proc. 17th Int. Conf. Parallel Distrib. Comput., Appl. Technol. (PDCAT)*, Dec. 2016, pp. 362–365.

[57] M. N. Nyan, F. E. Tay, and E. Murugasu, "A wearable system for pre-impact fall detection," *J. Biomech.*, vol. 41, no. 16, pp. 3475–3481, 2008.

[58] P. Choudhary, R. Sharma, G. Singh, and S. Das, "A survey paper on drowsiness detection & alarm system for drivers," *Int. Res. J. Eng. Technol.*, vol. 3, no. 12, pp. 1433–1437, 2016.

[59] W.-J. Chang, L.-B. Chen, and Y.-Z. Chiou, "Design and implementation of a drowsiness-fatigue-detection system based on wearable smart glasses to increase road safety," *IEEE Trans. Consum. Electron.*, vol. 64, no. 4, pp. 461–469, Nov. 2018.

[60] S. R. Dhole, A. Kashyap, A. N. Dangwal, and R. Mohan, "A novel helmet design and implementation for drowsiness and fall detection of workers on-site using EEG and random-forest classifier," *Proc. Comput. Sci.*, vol. 151, pp. 947–952, Jan. 2019.

[61] F. Wu, J.-M. Redoute, and M. R. Yuce, "A self-powered wearable body sensor network system for safety applications," in *Proc. IEEE SENSORS*, Oct. 2018, pp. 1–4.

[62] M. Serbanescu, V. M. Placinta, O. E. Hutanu, and C. Ravariu, "Smart, low power, wearable multi-sensor data acquisition system for environmental monitoring," in *Proc. 10th Int. Symp. Adv. Topics Electr. Eng. (ATEE)*, 2017, pp. 118–123.

[63] A. G. Perez, D. Lobo, F. Chinello, G. Cirio, M. Malvezzi, J. S. Martin, D. Prattichizzo, and M. A. Otaduy, "Optimization-based wearable tactile rendering," *IEEE Trans. Haptics*, vol. 10, no. 2, pp. 254–264, Apr. 2017.

[64] M. Maisto, C. Pacchierotti, F. Chinello, G. Salvietti, A. De Luca, and D. Prattichizzo, "Evaluation of wearable haptic systems for the fingers in augmented reality applications," *IEEE Trans. Haptics*, vol. 10, no. 4, pp. 511–522, Oct. 2017.

[65] M. Fomichev, F. Álvarez, D. Steinmetzer, P. Gardner-Stephen, and M. Hollick, "Survey and systematization of secure device pairing," 2017, *arXiv:1709.02690*.

[66] J. A. Unar, W. C. Seng, and A. Abbasi, "A review of biometric technology along with trends and prospects," *Pattern Recognit.*, vol. 47, no. 8, pp. 2673–2688, Aug. 2014.

[67] Y. Zeng, A. Pande, J. Zhu, and P. Mohapatra, "WearIA: Wearable device implicit authentication based on activity information," in *Proc. IEEE 18th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2017, pp. 1–9.

[68] K.-A. Shim, "A survey of public-key cryptographic primitives in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 577–601, 1st Quart., 2016.

[69] N. D. Sarier, "A survey of distributed biometric authentication systems," in *BIOSIG: Biometrics and Electronic Signatures*. IEEE, 2009, pp. 1–10.

[70] R. Cavallari, F. Martelli, R. Rosini, C. Buratti, and R. Verdone, "A survey on wireless body area networks: Technologies and design challenges," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1635–1657, 3rd Quart., 2014.

[71] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1658–1686, 3rd Quart., 2014.

[72] S. S. Javadi and M. A. Razzaque, "Security and privacy in wireless body area networks for health care applications," in *Wireless Body Area Networks: Technology, Implementation, and Applications*. CRC Press, 2013, pp. 165–187.

[73] M. Masdari and S. Ahmadzadeh, "Comprehensive analysis of the authentication methods in wireless body area networks," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4777–4803, Nov. 2016.

[74] V. Mainanwal, M. Gupta, and S. K. Upadhayay, "A survey on wireless body area network: Security technology and its design methodology issue," in *Proc. Int. Conf. Innov. Inf., Embedded Commun. Syst. (ICIIECS)*, Mar. 2015, pp. 1–5.

[75] M. R. K. Naik and P. Samundiswary, "Wireless body area network security issues—Survey," in *Proc. Int. Conf. Control, Instrum., Commun. Comput. Technol. (ICCICCT)*, Dec. 2016, pp. 190–194.

[76] S. Bhatt and T. Santhanam, "Keystroke dynamics for biometric authentication—A survey," in *Proc. Int. Conf. Pattern Recognit., Inform. Mobile Eng.*, Feb. 2013, pp. 17–23.

[77] M. Karnan, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review," *Appl. Soft Comput.*, vol. 11, no. 2, pp. 1565–1573, Mar. 2011, doi: 10.1016/j.asoc.2010.08.003.

[78] M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, "Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 65–84, Jan. 2021.

[79] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Inform. J.*, vol. 18, no. 2, pp. 113–122, 2017.

[80] S. Zou, Y. Xu, H. Wang, Z. Li, S. Chen, and B. Hu, "A survey on secure wireless body area networks," *Secur. Commun. Netw.*, vol. 2017, May 2017, Art. no. 3721234.

[81] B. Narwal and A. K. Mohapatra, "A review on authentication protocols in wireless body area networks (WBAN)," in *Proc. 3rd Int. Conf. Contemp. Comput. Informat. (IC3I)*, Oct. 2018, pp. 227–232.

[82] M. Usman, M. R. Asghar, I. S. Ansari, and M. Qaraqe, "Security in wireless body area networks: From in-body to off-body communications," *IEEE Access*, vol. 6, pp. 58064–58074, 2018.

[83] M. S. A. Malik, M. Ahmed, T. Abdullah, N. Kousar, M. Nigar, and M. Awais, "Wireless body area network security and privacy issue in E-healthcare," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 4, pp. 209–215, 2018.

[84] L. V. Morales, D. Delgado-Ruiz, and S. J. Rueda, "Comprehensive security for body area networks: A survey," *Int. J. Netw. Secur.*, vol. 21, pp. 342–354, Mar. 2019.

[85] M. Kompara and M. Hölbl, "Survey on security in intra-body area network communication," *Ad Hoc Netw.*, vol. 70, pp. 23–43, Mar. 2018, doi: 10.1016/j.adhoc.2017.11.006.

[86] R. Nidhya and S. Karthik, "Security and privacy issues in remote healthcare systems using wireless body area networks,"in *Body Area Network Challenges and Solutions*. Springer, 2019, pp. 37–53.

[87] A. Joshi and A. K. Mohapatra, "Authentication protocols for wireless body area network with key management approach," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 2, pp. 219–240, Feb. 2019.

[88] S. Chaudhary, A. Singh, and K. Chatterjee, "Wireless body sensor network (WBSN) security and privacy issues: A survey," *Int. J. Comput. Intell.*, vol. 2, no. 2, pp. 515–521, 2019.

[89] M. Hussain, A. Mehmood, S. Khan, M. A. Khan, and Z. Iqbal, "Authentication techniques and methodologies used in wireless body area networks," *J. Syst. Archit.*, vol. 101, Dec. 2019, Art. no. 101655, doi: 10.1016/j.sysarc.2019.101655.

[90] M. Roy, C. Chowdhury, and N. Aslam, "Security and privacy issues in wireless sensor and body area networks," in *Handbook of Computer Networks and Cyber Security*. Springer, 2020, pp. 173–200.

[91] B. Narwal and A. K. Mohapatra, *A Survey on Security and Authentication in Wireless Body Area Networks*, vol. 113. Amsterdam, The Netherlands: Elsevier, 2021, doi: 10.1016/j.sysarc.2020.101883.

[92] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, "Continuous and transparent multimodal authentication: Reviewing the state of the art," *Cluster Comput.*, vol. 19, no. 1, pp. 455–474, Mar. 2016.

[93] R. Spolaor, Q. Q. Li, M. Monaro, M. Conti, L. Gamberini, and G. Sartori, "Biometric authentication methods on smartphones: A survey," *PsychNology J.*, vol. 14, nos. 2–3, pp. 87–98, 2016.

[94] T. Neal and D. Woodard, "Surveying biometric authentication for mobile device security," *J. Pattern Recognit. Res.*, vol. 11, no. 1, pp. 74–110, 2016.

[95] R. Mayrhofer and I. Ion, "UACAP: A unified auxiliary channel authentication protocol," *IEEE Trans. Mobile Comput.*, vol. 12, no. 4, pp. 710–721, Apr. 2013.

[96] R. Ferrero, F. Gandino, B. Montrucchio, M. Rebaudengo, A. Velasco, and I. Benkhelifa, "On gait recognition with smartphone accelerometer," in *Proc. 4th Medit. Conf. Embedded Comput. (MECO)*, Jun. 2015, pp. 368–373.

[97] A. L. Fantana, S. Ramachandran, C. H. Schunck, and M. Talamo, "Movement based biometric authentication with smartphones," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Sep. 2015, pp. 235–239.

[98] R. Jin, L. Shi, K. Zeng, A. Pande, and P. Mohapatra, "MagPairing: Pairing smartphones in close proximity using magnetometers," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1306–1320, Jun. 2016.

[99] A. LaMarca, M. Langheinrich, and K. N. Truong, "Pervasive computing," in *Proc. Int. Conf. Pervasive Comput.*, Toronto, ON, Canada, May vol. 4480, May 2007, pp. 73–90, doi: 10.1007/978-3-540-72037-9_5.

[100] D. Bichler, G. Stromberg, M. Huemer, and M. Löw, "Key generation based on acceleration data of shaking processes," in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Lecture Notes in Computer Science), vol. 4717. 2007, pp. 304–317.

[101] Y. Shen, F. Yang, B. Du, W. Xu, C. Luo, and H. Wen, "Shake-n-shack: Enabling secure data exchange between smart wearables via handshakes," 2018, *arXiv:1801.07555*.

[102] Q. Jiang, X. Huang, N. Zhang, K. Zhang, X. Ma, and J. Ma, "Shake to communicate: Secure handshake acceleration-based pairing mechanism for wrist Worn devices," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5618–5630, Jun. 2019.

[103] B. Groza and R. Mayrhofer, "SAPHE: Simple accelerometer based wireless pairing with heuristic trees," in *Proc. ACM Int. Conf.*, no. 2, 2012, pp. 161–168.

[104] H. Yuzuguzel, J. Niemi, S. Kiranyaz, M. Gabbouj, and T. Heinz, "ShakeMe: Key generation from shared motion," in *Proc. IEEE Int. Conf. Comput. Inf. Technol.; Ubiquitous Comput. Commun.; Dependable, Autonomic Secure Comput.; Pervasive Intell. Comput.*, Oct. 2015, pp. 2130–2133.

[105] B. Groza, A. Berdich, C. Jichici, and R. Mayrhofer, "Secure accelerometer-based pairing of mobile devices in multi-modal transport," *IEEE Access*, vol. 8, pp. 9246–9259, 2020.

[106] M. Cao, L. Wang, H. Xu, D. Chen, C. Lou, N. Zhang, Y. Zhu, and Z. Qin, "Sec-D2D: A secure and lightweight D2D communication system with multiple sensors," *IEEE Access*, vol. 7, pp. 33759–33770, 2019.

[107] E. Bejder, A. K. Mathiasen, M. De Donno, N. Dragoni, and X. Fafoutis, "SHAKE: SHared acceleration key establishment for resource-constrained IoT devices," in *Proc. IEEE 6th World Forum Internet Things (WF-IoT)*, Jun. 2020, pp. 1–6.

[108] S. Sen and D. Kotz, "VibeRing: Using vibrations from a smart ring as an out-of-band channel for sharing secret keys," in *Proc. 10th Int. Conf. Internet Things*, 2020, pp. 1–8.

[109] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition," in *Proc. 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Oct. 2010, pp. 306–311.

[110] Y. Zhong and Y. Deng, "Sensor orientation invariant mobile gait biometrics," in *Proc. IEEE Int. Joint Conf. Biometrics*, Sep. 2014, pp. 1–8.

[111] J. Lester, B. Hannaford, and G. Borriello, "'Are you with me?'—Using accelerometers to determine if two devices are carried by the same person,"in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2004, pp. 33–50.

[112] Y. Sun, C. Wong, G.-Z. Yang, and B. Lo, "Secure key generation using gait features for body sensor networks," in *Proc. IEEE 14th Int. Conf. Wearable Implant. Body Sensor Netw. (BSN)*, May 2017, pp. 206–210.

[113] D. Schürmann, A. Brüsch, N. Nguyen, S. Sigg, and L. Wolf, "Moves like jagger: Exploiting variations in instantaneous gait for spontaneous device pairing," *Pervas. Mobile Comput.*, vol. 47, pp. 1–12, Jul. 2018.

[114] W. Xu, G. Revadigar, C. Luo, N. Bergmann, and W. Hu, "Walkie-talkie: Motion-assisted automatic key generation for secure on-body device communication," in *Proc. 15th ACM/IEEE Int. Conf. Inf. Process. Sensor Netw. (IPSN)*, Apr. 2016, pp. 1–12.

[115] W. Xu, C. Javali, G. Revadigar, C. Luo, N. Bergmann, and W. Hu, "Gait-key: A gait-based shared secret key generation protocol for wearable devices," *ACM Trans. Sensor Netw.*, vol. 13, no. 1, pp. 1–27, 2017.

[116] W. Xu and G. Lan, "Gait-based smart pairing system for personal wearable devices," in *Medical Internet of Things (m-IoT)-Enabling Technologies and Emerging Applications*. Rijeka, Croatia: IntechOpen, 2019.

[117] A. Bruesch, L. Nguyen, D. Schürmann, S. Sigg, and L. C. Wolf, "Security properties of gait for mobile device pairing," *IEEE Trans. Mobile Comput.*, vol. 19, no. 3, pp. 697–710, Mar. 2019.

[118] K. M. S. Thotahewa, J. M. Redoute, and M. R. Yuce, *Ultra Wideband Wireless Body Area Networks*, vol. 9783319052878. Springer, 2014,

[119] S. Sujatha and R. Govindaraju, "A secure crypto based ECG data communication using modified SPHIT and modified quasigroup encryption," *Int. J. Comput. Appl.*, vol. 78, no. 6, pp. 27–33, Sep. 2013.

[120] W. Wang, H. Wang, M. Hempel, D. Peng, H. Sharif, and H. H. Chen, "Secure stochastic ECG signals based on Gaussian mixture model for *e*-healthcare systems," *IEEE Syst. J.*, vol. 5, no. 4, pp. 564–573, Dec. 2011.

[121] J. Pourbemany, A. Essa, and Y. Zhu, "Real-time video-based heart and respiration rate monitoring," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*, Aug. 2021, pp. 332–336.

[122] Q. Lin, W. Xu, J. Liu, A. Khamis, W. Hu, M. Hassan, and A. Seneviratne, "H2B: Heartbeat-based secret key generation using piezo vibration sensors," 2019, *arXiv:1904.00750*.

[123] L. Wang, K. Huang, K. Sun, W. Wang, C. Tian, L. Xie, and Q. Gu, "Unlock with your heart: Heartbeat-based authentication on commercial mobile phones," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 2, no. 3, pp. 1–22, 2018.

[124] J. Ramos-Castro, J. Moreno, H. Miranda-Vidal, M. A. Garcia-Gonzalez, M. Fernandez-Chimeno, G. Rodas, and L. Capdevila, "Heart rate variability analysis using a seismocardiogram signal," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Aug. 2012, pp. 5642–5645.

[125] W. B. A. Karaa, *Biomedical Image Analysis and Mining Techniques for Improved Health Outcomes*. Hershey, PA, USA: IGI Global, 2015.

[126] F. Sufi, I. Khalil, and J. Hu, "ECG-based authentication," in *Handbook of Information and Communication Security*. Springer, 2010, pp. 309–331.

[127] E. Okoh, "Biometrics solutions in e-health security: A comprehensive literature review," *Spine*, vol. 19, p. 2274S–2278S, Jan. 2015.

[128] R. McCraty and F. Shaffer, "Heart rate variability: New perspectives on physiological mechanisms, assessment of self-regulatory capacity, and health risk," *Global Adv. Health Med.*, vol. 4, no. 1, pp. 46–61, Jan. 2015.

[129] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Proc. Int. Conf. Parallel Process. Workshops*, 2003, pp. 432–439.

[130] M. Rostami and A. Juels, "Authentication for implanted medical devices categories and subject descriptors," in *Proc. CCS*, 2013, pp. 1099–1111.

[131] P. A. Obrist, *Cardiovascular Psychophysiology: A Perspective*. Springer, 2012.

[132] J. Pourbemany, Y. Zhu, and R. Bettati, "Breathe-to-pair (B2P): Respiration-based pairing protocol for wearable devices," in *Proc. 15th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, New York, NY, USA, 2022, pp. 188–200, doi: 10.1145/3507657.3528545.

[133] R. Merletti and P. J. Parker, *Electromyography: Physiology, Engineering, and Non-Invasive Applications*, vol. 11. Hoboken, NJ, USA: Wiley, 2004.

[134] S. R. Devasahayam, *Signals and Systems in Biomedical Engineering: Signal Processing and Physiological Systems Modeling*. Springer, 2012.

[135] T. Labs. *Myo Armband*. Accessed: Mar. 10, 2023. [Online]. Available: https://www.myo.com

[136] Athos. *Athos Gear*. Accessed: Mar. 10, 2023. [Online]. Available: https://www.liveathos.com

[137] Leo. *Leo Smartband*. Accessed: Mar. 10, 2023. [Online]. Available: http://leohelps.com

[138] L. Yang, W. Wang, and Q. Zhang, "Secret from muscle: Enabling secure pairing with electromyography," *Proc. 14th ACM Conf. Embedded Netw. Sensor Syst. (SenSys)*, 2016, pp. 28–41.

[139] K. M. Iftekharuddin and A. Awwal, "Sampling and quantization," in *Field Guide to Image Processing*, no. 1. SPIE, 2012, p. 5.

[140] D. Schürmann and S. Sigg, "Secure communication based on ambient audio," *IEEE Trans. Mobile Comput.*, vol. 12, no. 2, pp. 358–370, Feb. 2013.

[141] A. Elsts, S. Duquennoy, X. Fafoutis, G. Oikonomou, R. Piechocki, and I. Craddock, "Microsecond-accuracy time synchronization using the IEEE 802.15.4 TSCH protocol," in *Proc. IEEE 41st Conf. Local Comput. Netw. Workshops (LCN Workshops)*, Nov. 2016, pp. 156–164.

[142] M. B. del Rosario, S. J. Redmond, and N. H. Lovell, "Tracking the evolution of smartphone sensing for monitoring human movement," *Sensors*, vol. 15, no. 8, pp. 18901–18933, 2015.

[143] M. N. Malik, M. A. Azam, M. Ehatisham-Ul-Haq, W. Ejaz, and A. Khalid, "ADLAuth: Passive authentication based on activity of daily living using heterogeneous sensing in smart cities," *Sensors*, vol. 19, no. 11, p. 2466, May 2019.

[144] Y.-P. Chen, J.-Y. Yang, S.-N. Liou, G.-Y. Lee, and J.-S. Wang, "Online classifier construction algorithm for human activity detection using a triaxial accelerometer," *Appl. Math. Comput.*, vol. 205, no. 2, pp. 849–860, 2008.

[145] Y. He and Y. Li, "Physical activity recognition utilizing the built-in kinematic sensors of a smartphone," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 4, 2013, Art. no. 481580.

[146] U. Maurer, A. Rowe, A. Smailagic, and D. Siewiorek, "Location and activity recognition using ewatch: A wearable sensor platform," in *Ambient Intelligence in Everyday Life*. Springer, 2006, pp. 86–102.

[147] J. Saunders, "Real-time discrimination of broadcast speech/music," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. Conf.*, vol. 2, May 1996, pp. 993–996.

[148] C. V. C. Bouten, K. T. M. Koekkoek, M. Verduin, R. Kodde, and J. D. Janssen, "A triaxial accelerometer and portable data processing unit for the assessment of daily physical activity," *IEEE Trans. Biomed. Eng.*, vol. 44, no. 3, pp. 136–147, Mar. 1997.

[149] J. Parkka, M. Ermes, P. Korpipaa, J. Mantyjarvi, J. Peltola, and I. Korhonen, "Activity classification using realistic data from wearable sensors," *IEEE Trans. Inf. Technol. Biomed.*, vol. 10, no. 1, pp. 119–128, Jan. 2006.

[150] A. Moncada-Torres, K. Leuenberger, R. Gonzenbach, A. Luft, and R. Gassert, "Activity classification based on inertial and barometric pressure sensors at different anatomical locations," *Physiol. Meas.*, vol. 35, no. 7, p. 1245, 2014.

[151] M. Ehatisham-ul-Haq, J. Loo, K. Shuang, S. Islam, U. Naeem, and Y. Amin, "Authentication of smartphone users based on activity recognition and mobile sensing," *Sensors*, vol. 17, no. 9, p. 2043, Sep. 2017.

[152] T. Huynh and B. Schiele, "Analyzing features for activity recognition," in *Proc. Joint Conf. Smart Objects Ambient Intell., Innov. Context-Aware Services: Usages Technol.*, Oct. 2005, pp. 159–163.

[153] K. Sayood, *Introduction to Data Compression*. San Mateo, CA, USA: Morgan & Kaufmann, 2017.

[154] S.-Y. Ho and D. J. Kleitman, "An odd kind of BCH code," *Discrete Appl. Math.*, vol. 161, no. 9, pp. 1216–1220, Jun. 2013, doi: 10.1016/j.dam.2012.08.021.

[155] *Error Correction Code, Wikipedia, the Free Encyclopedia*. [Online]. Available: https://en.wikipedia.org/wiki/Error_correction_code

[156] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Inf. Control*, vol. 3, no. 1, pp. 68–79, Mar. 1960.

[157] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *J. Soc. Ind. Appl. Math.*, vol. 8, no. 2, pp. 300–304, Jun. 1960.

[158] R. W. Hamming, "Error detecting and error correcting codes," *Bell Syst. Tech. J.*, vol. 29, no. 2, pp. 147–160, Apr. 1950.

[159] M. J. Golay, "Notes on digital coding," *Proc. IEEE*, vol. 37, no. 5, p. 657, 1949.

[160] Wikipedia. *Bch Code, Wikipedia, the Free Encyclopedia*. Accessed: Mar. 10, 2023. [Online]. Available: https://en.wikipedia.org/wiki/BCH_code

[161] P. Shrivastava and U. P. Singh, "Error detection and correction using Reed Solomon codes," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 8, pp. 1–5, 2013.

[162] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Springer, 2005, pp. 457–473.

[163] A. Anees and Y.-P.-P. Chen, "Discriminative binary feature learning and quantization in biometric key generation," *Pattern Recognit.*, vol. 77, pp. 289–305, May 2018.

[164] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2016.

[165] R. Chartrand, "Nonconvex compressed sensing and error correction," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, vol. 3, Apr. 2007, pp. III-889–III-892.

[166] H. Zoerlein, M. Shehata, and M. Bossert, "Concatenated compressed sensing-based error correcting codes," in *Proc. 9th Int. ITG Conf. Syst., Commun. Coding (SCC)*, Jan. 2013, pp. 1–5.

[167] M. Hosseinzadeh, B. Vo, M. Y. Ghafour, and S. Naghipour, *Electrocardiogram Signals-Based User Authentication Systems Using Soft Computing Techniques*, vol. 54, no. 1. Amsterdam, The Netherlands: Springer, 2021, doi: 10.1007/s10462-020-09863-0.

[168] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-Allen Hamilton Inc., McLean VA, USA, Tech. Rep., 2010.

[169] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[170] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)*, Feb. 2017, pp. 32–37.

[171] J.-C. Kao and R. Marculescu, "Eavesdropping minimization via transmission power control in ad-hoc wireless networks," in *Proc. 3rd Annu. IEEE Commun. Soc. Sensor Ad Hoc Commun. Netw.*, vol. 2, Sep. 2006, pp. 707–714.

[172] S. Malladi, J. Alves-Foss, and R. B. Heckendorn, "On preventing replay attacks on security protocols," in *Proc. Int. Conf. Secur. Manage.*, Jun. 2002.

[173] Y.Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2–23, 2006.

[174] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," in *Security in Distributed, Grid, Mobile, and Pervasive Computing*, vol. 1, no. 367, 2007, p. 6.

JAFAR POURBEMANY (Member, IEEE) received the B.Sc. degree in electronics and the M.Sc. degree in telecommunications from Yazd University, in 2009 and 2014, respectively. He is currently pursuing the joint Ph.D. degree in computer science with the Network Security and Privacy Research Laboratory, Cleveland State University, and the Dr. Tereshchenko's Laboratory, Cleveland Clinic, USA. He is currently a Research Assistant with the Dr. Tereshchenko's Laboratory, Cleveland Clinic. His research interests include multidisciplinary, focusing on network security, body area networks, wireless sensor networks, and machine learning in healthcare, with a particular focus on cardiac data analysis.

YE ZHU (Senior Member, IEEE) received the B.Sc. degree from Shanghai Jiao Tong University, in 1994, the M.Sc. degree from Texas A&M University, in 2002, and the Ph.D. degree from the Department of Electrical and Computer Engineering, Texas A&M University. He is currently a Professor with the Department of Electrical and Computer Engineering, Cleveland State University. His research interests include network security, traffic engineering, and wireless sensor networks. He is a member of the IEEE Computer Society.

RICCARDO BETTATI (Senior Member, IEEE) received the Diploma degree in informatics from the Swiss Federal Institute of Technology (ETH), Zürich, Switzerland, in 1988, and the Ph.D. degree from the University of Illinois at Urbana–Champaign, in 1994. From 1993 to 1995, he held a postdoctoral position with the International Computer Science Institute, Berkeley, and the University of California at Berkeley. He is currently a Professor with the Department of Computer Science, Texas A&M University, where he has been leading the Real-Time Systems Research Group and until 2015, the Center for Information Assurance and Security. His research interests include traffic analysis and privacy, real-time distributed systems, real-time communication, and network support for resilient distributed applications. He shares the best paper awards with his collaborators and students at the IEEE National Aerospace and Electronics Conference and the Euromicro Conference on Real-Time Systems. He was the Program Chair and the General Chair of the IEEE Real-Time and Embedded Technology and Applications Symposium, in 2002 and 2003, respectively.