Towards Secure Device Pairing via Vibration Detection

Zhenge Guo[1](✉), Zhaobin Liu[2](✉), Jizhong Zhao[1](✉), Hui He[1],
and Meiya Dong[3]

[1] Xi'an Jiaotong University, Xi'an 710049, China
guozhenge@stu.xjtu.edu.cn, zjz@mail.xjtu.edu.cn, huihe@xjtu.edu.cn
[2] Suzhou Vocational University, Suzhou 215104, China
zbliusz@126.com
[3] Taiyuan University of Technology, Taiyuan 030024, China
dongmeiya@163.com

Abstract. Multi-party applications are becoming popular due to the development of mobile smart devices. In this work, we explore PVKE (Physical Vibration Keyless Entry), a novel pairing mechanism, through which users are able to utilize smart devices to detect a vibration from the smart watch, so as to use information from the vibration to deconstruct security keys. Thus, we perform device pairing without complicated operations. We show that the recognition accuracy of vibration key detection achieves 95% through solid experiments.

Keywords: Device pairing · Vibration detection · Key extraction

1 Introduction

With the recent improvements in modern technology, as well as the popularization of smart phones, smart devices like smart watches and other many multi-party applications have become more popular. In these application, smart devices often need to establish pairing relationships, and transfer data among one another via wireless communication, like Wi-Fi [9] and RFID [6]. As we know, wireless networks are more vulnerable to third party attack, as wireless channels are in a public wireless transport protocol. Hence, it is highly desirable to enforce secure communication channel between the smart devices.

Take automobile door locks system as an example, the Remote Keyless Entry System (RKE) [2] emerged after the Traditional Mechanical Key System. RKS is also know as remote central locking, refers to a lock that uses an electronic remote control as a key which is activated by a handheld device or automatically connect by proximity sensor. It can be used to remote control door lock and unlock requests. The system sends a stream through a specially coded data,

Supported by the NSFC program under Grants No. 61672372 and Shaanxi NSF under Grant No. 2017JM6109.

X. Sun et al. (Eds.): ICCCS 2018, LNCS 11068, pp. 177–186, 2018.
https://doi.org/10.1007/978-3-030-00021-9_17

the receiver in car gets the data and decodes with encrypt algorithm. After decrypting the key information, the vehicle performs lock or unlock request.

Hands-free Passive Keyless Entry (PKE) [5] is quickly becoming mainstream in automotive remote keyless entry applications and is a common option on new auto-mobile models. Instead of pressing a transmitter button to unlock or lock a car door, it is possible to gain vehicle access simply having a valid transponder in your possession.

In these applications, smart devices often need to establish pairing relationships, and transfer data among one another via wireless communications, like Bluetooth, RFID and Wi-Fi. There are two main problems with those methods: Firstly, information is easily intercepted by third parties. Secondly, information is vulnerable to "man-in-the-middle" attacks.

To solve the above problems, we propose PVKE, a new hands-free passive keyless entry based on physical vibration. This system contains two parts: base station system (bodywork) and transponder (smart wristband/watch). The user generates the key by the vibration of the personal smart device and passes the key to the base station receiving system when touching the door lock. The receiving system opens the device to unlock the door according to the key information. The main contributions of this design are as follows:

Firstly, we design a new intelligent unlocking system PVKE, which transfers the key by physical vibration, and avoiding the lack of interference by third parties in wireless transmission.

Secondly, we study the coding mechanism of key transfer via physical vibration without adding additional equipment. In order to adjust the duration of the vibration of the mechanical motor to key, the encoding is divided into two kinds depending on the coding principle: time dimension based and binary-based.

Thirdly, the feasibility of realizing intelligent unlock by physical vibration transmission key is verified through experiments.

The rest of this paper is organized as follows. Section 2 discusses the related work. In Sect. 3, we describe the overall design of the system, and introduce the details of PVKE on how to detect the vibration in real time and how to extract and negotiate the key. We report the experimental settings and results in Sect. 4. Section 5 concludes the paper.

2 Related Work

How to achieve secure and rapid pairing between devices is a matter of concern for all multi-party applications. We classify the existing approaches as follows:

Wireless Channel-Based Technology. RFID is used for non-contact communication using radio city [16]. NFC (Near Field Communication) [8] is another wireless technology for short-range communication with a maximum communication range of 20CM based on the RFID technology. While Wi-Fi Bluetooth [1], and ZigBee [7] are widely available for longer range communication than NFC, eavesdropping without the knowledge of the user is possible [3] and private communication cannot be guaranteed.

Acoustics Based Technology. The authors in [10,11,14,15] generate keys by sound. According to a devices position background sound, it got the key from the frequency domain information and completed the pairing through the changing of FFT (Fast Fourier Transform). Schürmann [12] realizes a safe channel through the sound, Dhwani [13] further uses sound signals to imitate the hardware NFC to reach the goal of communicating in the near field. It uses a microphone and speaker to realize safe communication and the pairing in a near field on the cellphones without the pairing hardware NFC. However, the limitations of the microphone lead to a lot of inconsistent information and low security in the key. In order to improve the security, we need to increase the sampling time, which increases the difficulty of matching.

Light Based Technology. Komine et al. [4] proposed a new communication method using LED lights. This has an advantage in the sense of privacy over the other radio-based wireless communication method. However, it requires a line of sight between communicating devices and one-to-many communication is not possible without an extra apparatus.

3 System Design

3.1 System Overview

Based on the vibration detection [17], PVKE mainly consists of two parts: base station system and transponder system. The base station is used to receive the key and decide whether to open the entrance guard according to the correctness of the password. The transponder is used for generating physical vibration according to the cipher after receiving the instruction from the base station and releasing the key information. The base station part is the main body of the vehicle and continuously sends low frequency messages to activate transponders within the effective communication range. The message is sent in broadcast format in plain code and can be received by all transponders within the signal range. When the transponder enters the communication area and receives the message, it begins to transmit the key in the form of vibration. It is difficult for the base station to decode the sensing data after receiving the vibration information. If the verification is successful, the control instruction executive mechanism opens the door and sends the information to the responder to stop the vibration.

3.2 Key Generation Mechanism

Software/API limitations in smartphones and smartwatch prevent fully exploiting the vibro-motors and accelerometers. It limits the vibration intensity and vibration frequency of the mechanical motor, therefore, we can only adjust the start time and end time of the vibration.

Vibration Detection. Modern accelerometers sense the movement of the seismic mass along 3 orthogonal axes, and report them as an (X, Y, Z) tuple. The gravitational acceleration appears as a constant offset along the axis pointed towards the floor. When using accelerometer to sense data, we ignore the spatial direction of acceleration. The value of the acceleration three directions is computed by vector knowing, and the vector sum is compared with the threshold value to judge whether the vibration has taken place, and then the key is received further. The basic formula is shown in Eq. (1):

$$svm = \sqrt{x^2 + y^2 + z^2} \tag{1}$$

How to set the start and end times of a key word in the transmission process? There are two ways to do this:

The first method: as long as the base station detects the vibration, it is assumed that the key has started to pass. This method is simple and easy to operate. However, in the actual delivery process, the key transfer in this form is easy to generate string code, which leads to the failure of verification. Because the transmission mechanism determines that the intelligent device begins to transfer the key through vibration after receiving the base station activation information. So, under normal circumstances, in order to guarantee the integrity of the transmitted key, the intelligent device must transmit more than one set of keys continuously. If the key is decoded simply by recording continuous vibration data, the wrong string code is easily generated. For example, the responder passes two sets of keys, 213 and 213. Since the base station receives the vibrator from the second encoding in the first group, the key identified by the base station is likely to be 132.

This problem can be solved as follows: Set the threshold value of key transfer interval, the vibration interval of the digital single in the same group of keys is less than that of different groups of keys.

The second method: set a special transmission vibration mode to represent the beginning and the end of the key transmission. Before transferring the key, we set a special vibration to let the base station system know that we will start to transfer the key and to know when we will stop transferring.

Encoding Mechanism. In this paper, in order to adjust the duration of the vibration of the mechanical motor to key, the encoding is divided into two kinds depending on the coding principle: Time Dimension based and Binary-based.

The encoding mechanism based on the time dimension: the number of strings to be transmitted is encoded by the corresponding time length of each digit. For example, the continuous vibration 1 second represents the number 1, the continuous vibration 2 seconds represents the number 2, and so on. Binary-based encoding scheme: sets the password according to binary code. Code each digit in binary.

How to set the number 0 in the key. In wireless signal transmission, color Manchester coding is usually used to transmit data. The data such as continuous 0 or

1 can be identified without clock synchronization signal. However, in the process of passing the key with vibration, if the non-vibration is represented as 0, it is easy to confuse the spatial time without data transfer with the number 0, which leads to the wrong key identification.

In the digital coding process of the vibration key, PVKE use the +1 method to experiment the coding. Use 1 for 0 and 10 for 9. For example, the number 0 is represented by 1 millisecond vibrated time in the encoding process according to the length of time described above. In binary coding, the number 0 is 11, and the number 1 is 12.

4 System Evaluation

Based on the Android Wear intelligent platform, this paper realizes the detection module. Android Wear is the new open intelligence platform that was created by Google to use for smart watches, which allows a third-party to manufacture a wide variety of devices to be compatible in Android Wear. We realize the extraction of acceleration and gyro sensor data through the API that was provided by the Android Wear system, and the adjustment of the sensor sampling frequency as well.

4.1 System Implementation

The experiment used the equipment HUAWEI watch and SAMSUNG X5, their hardware as show in Table 1.

Table 1. Hardware comparison between Galaxy S5 and HUAWEI-WATCH 2

Hardware parameter	Galaxy S5	HUAWEI-WATCH 2
Type	Smart Phone	Smart Watch
RAM	2 GB	768 mb
CPU	Qualcomm Snapdragon 801	Qualcomm Snapdragon Wear 2100
Android version	6.0.1	7.1.1
Sampling frequency	200 Hz	200 Hz

4.2 Experimental Result and Analysis

The Influence of Threshold Value for Vibration Detection Accuracy. In previous sections, we have discussed the relationship between the threshold value and the detection accuracy. PVKE collected 9 number vibration, with each number vibrations 5 times. We use the different threshold to resample in the subsequent vibration detection, finally, due to the different threshold we detect respectively, the result is shown in Figs. 1, 2 and 3. In Fig. 1, we can figure out that when the threshold is 20.05, the deviation is 358.82 ms. Since the threshold is smaller, the motion information the capture is more, making it harder to identify the error. With the increase in threshold to 20.10 in Fig. 2, the deviation is decrease to 112.73 ms. After reaching a certain degree to 20.15 in Fig. 3, however, the deviation is no longer decrease, because most of the vibration information cannot be detection. Considering the recognition accuracy, PVKE choose 20.10 as the threshold value.

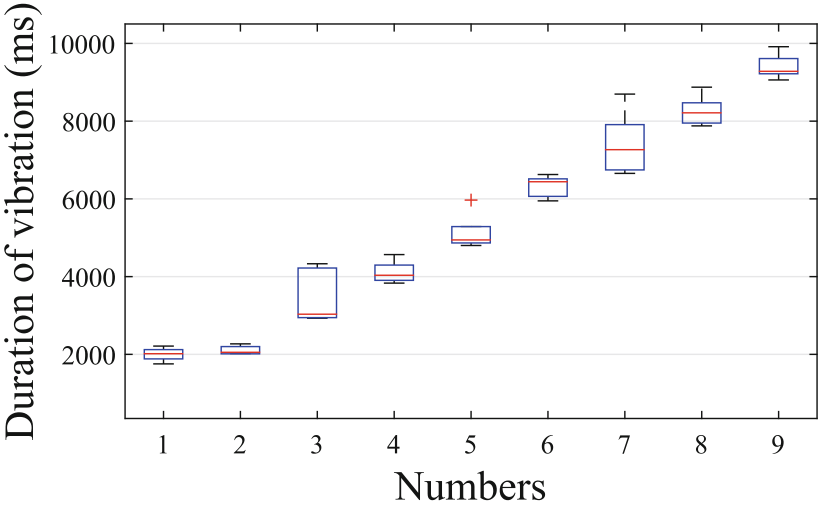

Fig. 1. The duration of vibration with SVM = 0.205

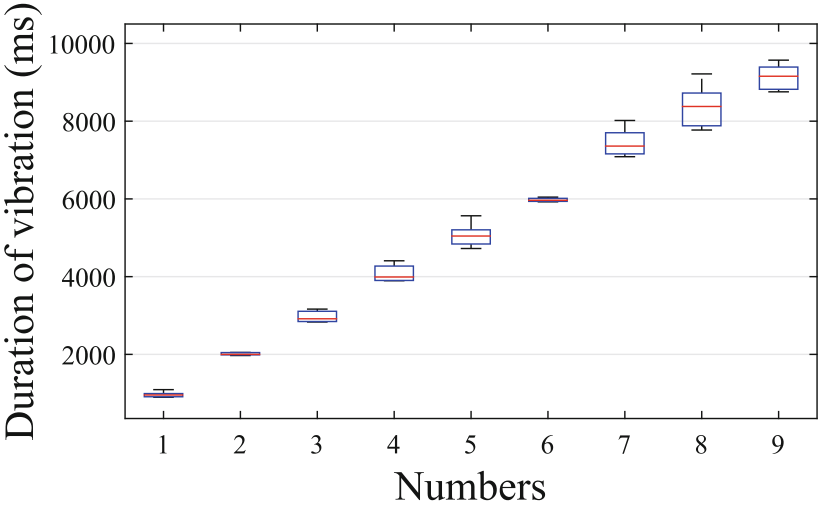

Fig. 2. The duration of vibration with SVM = 0.210

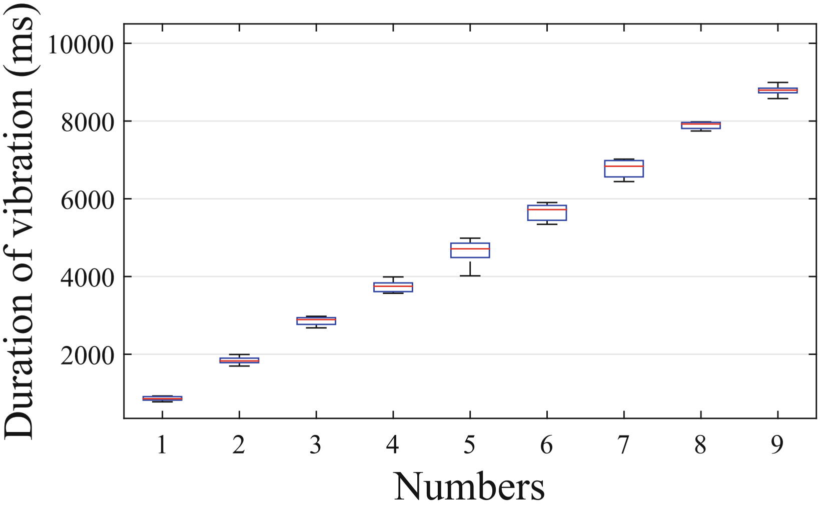

Fig. 3. The duration of vibration with SVM = 0.215

The Influence of Password Length for Vibration Detection Accuracy. As we all know, the key length determines the security of the key. In vibration-based key transfer systems, will the key recognition rate decrease with the increase of the key length? We test three sets of keys that go up to 2, 3 and 4, respectively. The experimental data are shown in Figs. 4, 5 and 6. It is found from the experiment that the average deviation of identifying vibration cipher

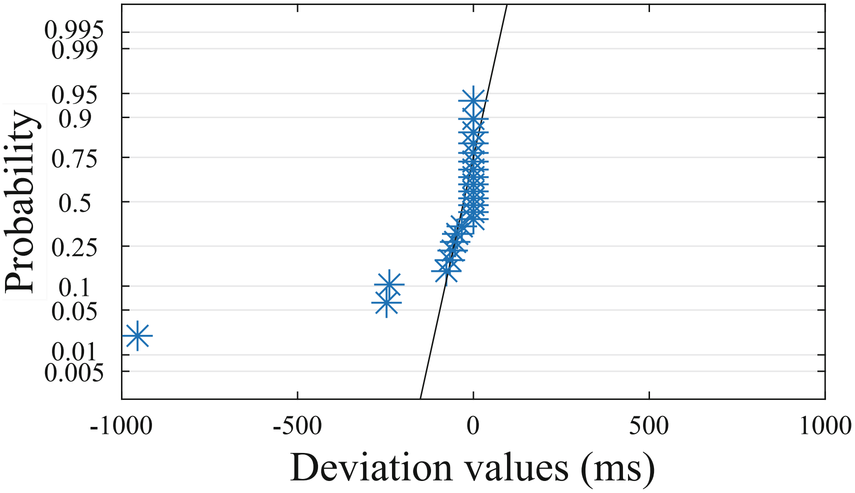

Fig. 4. 2bit Probability plot for Normal distribution

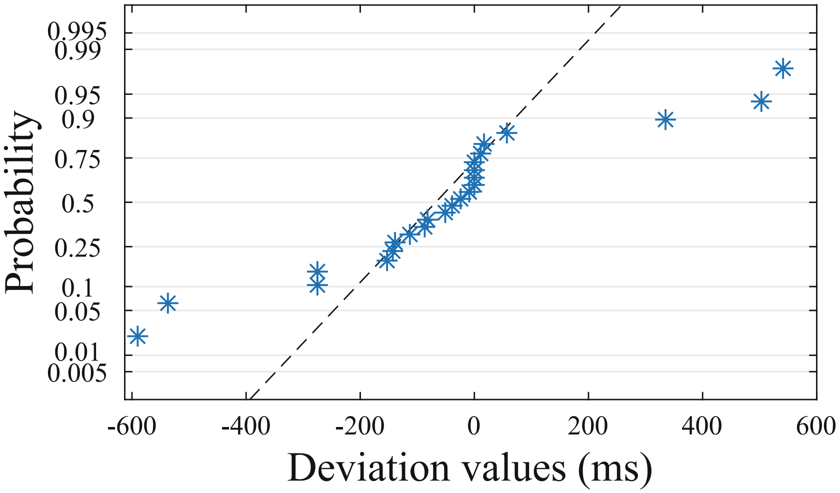

Fig. 5. 3bit Probability plot for Normal distribution

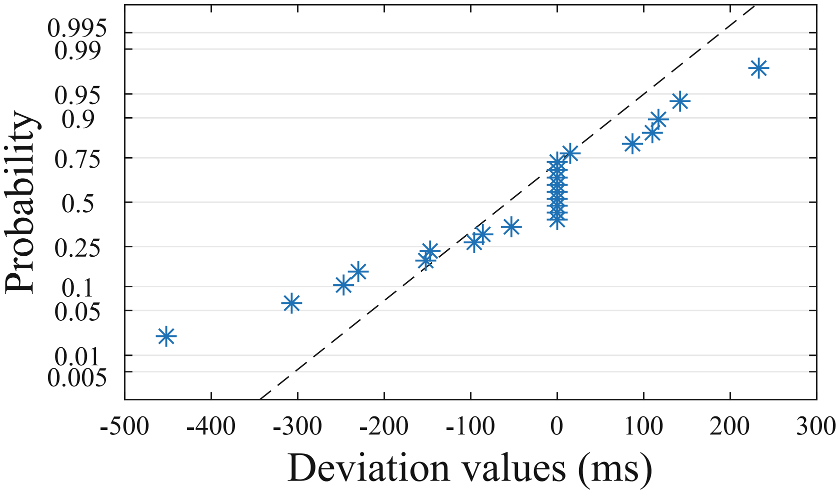

Fig. 6. 4bit Probability plot for Normal distribution

data is 71.7 ms when the key length is 2(Fig. 4), When the key length is 3(Fig. 5), the average identification deviation of the vibration key is 71.06. When the key length is 4(Fig. 6), the average deviation of the vibration key is 62.65. Experimental results show that the recognition rate of the key transferred by physical vibration does not increase with the increase of the key length. This is mainly due to the fact that the physical transmission is not susceptible to outside interference. In the experiment, we also found that in the two-length code, the maximum deviation of 95 data in the vibration key is 250, in the key with length 3, the maximum deviation is 450, and in the key with length 4, the maximum deviation is 350. Therefore, we limit the decoding bias to 450 during the decoding process, which will guarantee a key identification rate of no less than 95%.

5 Conclusion

In this work, we have proposed PVKE, which use a wearable device to generate a vibration password and thus simplify device matching. There are three main contributions: designing the vibration based key transfer method; study the coding mechanism of key transfer via physical vibration without adding additional equipment; completing the vibration key generation method and wireless sensor key generation method. Experiments showed the secure decryption and unlock mechanism without additional device is implemented.

References

1. Haartsen, J.: The bluetooth radio system. IEEE Pers. Commun. **7**(1), 28–36 (2000)
2. Suda, H., Lehmer, M.J.: Remote keyless entry system: U.S. Patent 6,718,240[P] (2004)
3. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and privacy aspects of low-cost radio frequency identification systems. In: Hutter, D., Müller, G., Stephan, W., Ullmann, M. (eds.) Security in Pervasive Computing. LNCS, vol. 2802, pp. 201–212. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-39881-3_18
4. Komine, T., Nakagawa, M.: Fundamental analysis for visible-light communication system using LED lights. IEEE Trans. Consum. Electron. **50**(1), 100–107 (2004)
5. Microchip Technology Inc.: Passive keyless entry (PKE) reference design users manual[Z] (2006)
6. Want, R.: An introduction to RFID technology. IEEE Pervasive Comput. **5**(1), 25–33 (2006)
7. Baronti, P., Pillai, P., Chook, V.W., Chessa, S., Gotta, A., Hu, Y.F.: Wireless sensor networks: a survey on the state of the art and the 802.15.4 and ZigBee standards. Comput. Commun. **30**(7), 1655–1695 (2007)
8. Curran, K., Millar, A., Garvey, C.M.: Near field communication. Int. J. Electr. Comput. Eng. (IJECE) **2**, 371–382 (2012)
9. Wifi (wireless fidelity). http://www.wi-fi.org
10. Nguyen, N., Sigg, S., An, H., Ji, Y.: Using ambient audio in secure mobile phone communication. In: IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 431–434 (2012)
11. Sigg, S.: Adhocpairing: Spontaneous audio based secure device pairing for android mobile devices (2012)
12. Schürmann, D., Sigg, S.: Secure communication based on ambient audio. IEEE Trans. Mob. Comput. **12**(2), 358–370 (2013)
13. Nandakumar, R., Chintalapudi, K.K., Padmanabhan, V., Venkatesan, R.: Dhwani: secure peer-to-peer acoustic NFC. ACM SIGCOMM Comput. Commun. Rev. **43**(4), 63–74 (2013)

14. Miettinen, M., Asokan, N., Nguyen, T.D., Sadeghi, A.R., Sobhani, M.: Context-based zero-interaction pairing and key evolution for advanced personal devices. In: ACM Sigsac Conference on Computer and Communications Security, pp. 880–891 (2014)
15. Zhang, L., et al.: Montage: combine frames with movement continuity for realtime multi-user tracking. IEEE Trans. Mob. Comput. **16**(4), 1019–1031 (2017)
16. Yang, L., Li, Y., Lin, Q., Jia, H., Li, X., Liu, Y.: Tagbeat: sensing mechanical vibration period With COTS RFID systems. IEEE/ACM Trans. Netw. **25**(6), 3823–3835 (2017)
17. Guo, Z., Gao, X., Ma, Q., Zhao, J.: SDP: towards secure device pairing via handshake detection, Tsinghua Science and Technology (2018). https://doi.org/10.26599/TST.2018.9010085