Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 846739, 14 pages
http://dx.doi.org/10.1155/2015/846739

Research Article

Making It Trustable: Acoustic-Based Signcryption Mutual Authentication for Multiwearable Devices

Shuhua Zhu,[1,2] Xiaojie Li,[3] Chunsheng Zhu,[4] Lei Shu,[5] and Wei Sun[6,7]

[1]*School of Information Science and Technology, Sun Yat-sen University, Guangzhou, Guangdong Province 510006, China*
[2]*School of Information Science and Technology, Jinan University, Guangzhou, Guangdong Province 510632, China*
[3]*International School, Jinan University, Guangzhou, Guangdong Province 510632, China*
[4]*Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC, Canada V6T 1Z4*
[5]*Guangdong Provincial Key Laboratory of Petrochemical Equipment Fault Diagnosis, Guangdong University of Petrochemical Technology, Maoming, Guangdong Province 525000, China*
[6]*School of Software, Sun Yat-sen University, Key Laboratory of Information Technology, Ministry of Education, Guangzhou, Guangdong Province 510006, China*
[7]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100864, China*

Correspondence should be addressed to Wei Sun; sunwei@mail.sysu.edu.cn

Received 12 August 2014; Accepted 29 August 2014

Academic Editor: Xiaoling Wu

We address the problem of authentication and secure communication between wearable devices. As people rely heavily on such mobile and wearable devices, the need for seamless and secure communication across these spectra of devices becomes increasingly important. In order to provide secure communication, mutually trusted authentication becomes the first line of protection to guard our personal information. We propose an acoustic-based signcryption mutual authentication (ASMA), which is a key-agreement protocol by employing timestamp and owning functions of multiple-times identity authentication, password change, and devices addition and alteration. Through series of experiments verifying the reliability and accuracy, the protocol shows that it can ensure secure data transmission and data sharing for multiwearable devices.

1. Introduction

With the popularization of Wi-Fi and Internet connection, multiwearable devices and other intelligent terminals are wildly used in our daily life as a part of the Internet of Things (IoT) [1]. Glasses and wrist watches are no longer simply what they used to be. They are now more intelligent and are able to track your eyeball, identify your voice, and even record your heart rate and breathing rate. These devices become someone who knows you best.

As digital device usage becomes more widespread in various domains [2], such as education, management information systems, and healthcare [3, 4], Internet security is becoming an increasingly important issue. Any unreliable connections can cause the leaking of important personal information stored in digital devices. But what can be done to handle this problem? The answer is authentication.

What is authentication? Authentication is the process of determining whether someone or something is. In fact, who or what it is declared to be. In traditional authentication, the identity usually belongs to a person, but, in digital authentication, it belongs to a device, which is the main difference between the traditional and the digital ones. In private and public computer networks (including the Internet), it is hard for our machines to tell whether the physical identity corresponds to the digital one. For this reason, a stringent authentication process is needed. The purpose is to provide secure communication between the desired devices. It also helps to break the barriers that a mobile could only communicate with the wearable devices of the same company.

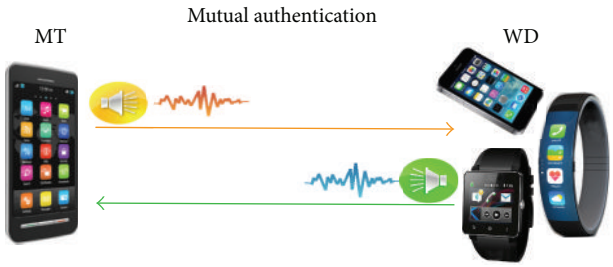


Figure 1: Acoustic-based mutual signcryption authentication for multiwearable devices.

This paper aims to propose an acoustic-based signcryption mutual authentication (ASMA) scheme for wearable devices and movable terminals. Figure 1 shows the authentication scheme. It is about a key agreement protocol by employing timestamp and signcryption which owns functions of multiple-times identity authentication, password change, and devices addition and alteration. The scheme belongs to noncontact biometrics authentication which is different from 2D barcodes-based [5] and some other visual-channel-based [6] authentication. Meanwhile, as a wireless communication technology with short range and low power consumption, it is also different from Bluetooth or NFC (near-field communication) [7] technology which requires users to spend extra cost on inbuilt NFC chip or external NFC tags. With the support of cell phone, earphone, and other cheap wearable devices, the protocol can effectively resist the MITM (man-in-the-middle) attack [8], replay attack [9], and nonsynchronous attack [10].

Apart from the ASMA scheme for wearable devices and movable devices, an agreed-upon shared key is generated which can be applied in the mass data transferring like long strings, text files, and video streams. With the help of shared key, we can achieve data delivering via Bluetooth address and data sharing among the wearable devices and moveable devices in a secure condition.

The main contributions of this paper are summarized as follows.

(i) This paper proposes an ASMA scheme, supporting authentication and secure communication between multiple wearable devices. In this scheme, an agreed-upon key agreement protocol is created by signcryption, employing timestamp for mutual authentication and data transmission.

(ii) This paper further presents the architecture, design, and security analysis of ASMA. It shows that ASMA will automatically complete certification in less than 10 seconds, significantly reduce cost, and increase efficiency.

(iii) The proposal is also achieved and verified in practice and a positive feedback is received. People could make the mutual authentication and transmit data about their health, bodily functions, text messages, schedules, and videos between their multiwearable devices.

The rest of this paper is organized as follows. The related works are given in Section 2. System design and problem statement are given in Section 3. The authentication protocol is described in Section 4. Security analysis is performed in Section 5. The implementation is demonstrated in Section 6. Finally, the conclusions are presented in Section 7.

2. Related Works

How to authenticate devices' identities is a long time issue. Two main problems should be solved to make two mutually distrusted devices establish key agreement to achieve identity authentication and provide secure communication.

(i) What kind of contact channel can transmit authentication information?

(ii) Which method or protocol can ensure the security of contact channel?

2.1. Contact Channel. To solve the first problem, Stajano and Anderson introduced a "resurrecting duckling" model [11]. They use secret data exchanged over a contact channel (usually a physical contact) to bootstrap a particular authentication and key exchange protocol. Such an exchange directly captures the user's intention that the user wants to communicate with that device. To some extent, QR (quick response) code, which is widely used currently, is based on this model. QR code is a readable bar code which uses black and white rectangular patterns to signify binary data. They can be preconfigured and printed on labels that are attached to devices, or they can be generated on demand and shown on a screen. A device with Internet access and cameras can complete the whole authentication steps. However, its disadvantage is that a user must visually identify the desired device. And it also brings problems when users read the wrong QR code or in the areas without network signal.

Compared with QR code, NFC [12] and the Bluetooth have some advantages. NFC has characteristics of high reliability and its authentication method is very simple, which is evolved from RFID (radio-frequency identification) [13]. NFC is suitable to exchange important data such as financial information and personal information, while the Bluetooth is more suitable for a longer distance data communication. Hence NFC and the Bluetooth can complement each other. However, these two techniques have a disadvantage: they are dependent on inbuilt chips.

As mentioned above, we adopt acoustic wave contact channel to make identity authentication, which can avoid both component redundancy and dependence on Internet access.

2.2. Protocol. The second problem is mainly solved by encryption systems and digital-signature techniques.

In encryption systems, public-key cryptography (PKC) is a significant technique to ensure the security of network and information. Traditional PKC requires certification authority (CA) to issue certificate to bind users' identity and public key, which brings about problem with certificate management.

However, it is solved by Shamir's public-key scheme based on identity [14], which was introduced in 1984. This scheme set users' identity such as name, student number, and ID number as the public key. However, it needs an authentic private-key generation center (KGC), which brings about problem with private-key escrow. To solve the problems of certificate management and private-key escrow, Al-Riyami, and so forth, first put forward certificateless public-key cryptography scheme [15], which can make users' public key authenticated without certificate and only make a part of users' private key known to KGC.

As to digital-signature techniques, Diffie and Hellman initially proposed the digital-signature method [16] in 1976. Then other scholars have developed the well-known methods such as RSA, ElGamal, and DSS. To meet the demand, more digital signatures are developed, such as group signatures, ring signatures, proxy signatures, threshold signatures, and signcryption [17–20].

In practical application, users often need to implement signature and encryption at the same time. To achieve this purpose, firstly we sign the information and then encrypt the signature. In 1998, Zheng and Imai [21] introduced a new password scheme, signcryption, which combines digital-signature and public-key encryption into one process. It led to a new signcryption scheme based on identity which has been further developed by the later scholars [22–26]. Barbosa and Farshim [27] first initially proposed the signcryption concept based on certificateless public-key cryptography. In recent years, some improved certificateless digital signcryption schemes have been put forward.

Along with the development of signcryption theory, signcryption is extensively adopted to achieve security efficiently in areas such as e-payment, ad hoc network, ATM network, and VoIP network. As a result, key-agreement protocol on the basis of signcryption technology was instantly introduced. Based on the point of Kim and Youm onwards, we have achieved the key-agreement protocol [28] on the basis of timestamp and signcryption technologies to guarantee the trusted authentication and security between devices.

Apart from that, our scheme requires wearable devices and mobile devices to authenticate at the beginning and end of data transmission, respectively, to ensure its security. When false identity is detected, the system will destroy the data ciphertext immediately. Additionally, the scheme also provides the mechanisms for password change and multiple devices addition as well as their alteration, which increases convenience.

3. System Design and Problem Statement

In this paper, we consider the problem of authentication between mutually distrusted devices. We assume that there is a many-to-many relationship among US (user), MT (mobile terminal), and WD (wearable device), and their pairings are random. That is, one MT or WD can be paired with several mutually trusted MTs or WDs at the same time. Many MTs and WDs can be found around US when we use them, which could lead to their mutual distrust and cause confusion. In this environment, the identity and trust authentication as well as data transmission between MT and WD can be realized via the key agreement.

Usually, an authentication process has three entities: MT, WD (it can also be replaced by other devices such as sensors and actuators), and US (with the ownership of MT and WD). We also assume that both MT and WD, equipped with Bluetooth, acoustic wave transmitter, and absorber, can process encryption/decryption algorithms.

The first subproblem of this paper is to choose a contact channel, which should be costless and convenient.

The second subproblem of this paper is to find a protocol to adapt to the channel we choose, which will complete the authentication part and generate an agreed-upon shared key for the following data transmission.

Based on these two problems, we propose a new acoustic-based authentication, which consists of three parts: authentication protocol, data transmission, and additional function.

4. Proposed Protocol

We have started the research project to create an innovative ASMA system according to the two key problems. This section provides detail of system functions, design, and architectures.

Our system consists of three parts: authentication protocol, data transmission, and additional function. In the protocol, we will use acoustic channel to obtain session key, which is of great importance in the following data transmission. The additional function contains device addition, device alteration, and change of password. For a better understanding, Figure 2 displays an overview of this scheme.

The authentication protocol is presented in Figure 2.

4.1. Definitions. Here are the definitions of symbols used in our protocol shown in definitions of symbols used in our protocol section.

4.2. Authentication Protocol

Step 1. Setup

(i) Enc is a deterministic encryption algorithm, which takes data m of any length and a shared key K of some predetermined length as input and outputs an encryption $C = Enc_K(m)$ of that data.

(ii) Dec is a deterministic decryption algorithm, which takes a ciphertext C of any length and a shared key K of some predetermined length as input and outputs either data $m = Dec_K(C)$ or the error symbol $\perp$.

(iii) US sets the 8-bit initial password PW_{mt} and PW_{wd} in MT and WD.

(iv) Compute: MT and WD generate key $K_{mt} \leftarrow (PW_{mt}, ID_{mt})$, $K_{wd} \leftarrow (PW_{wd}, ID_{wd})$.

(v) If MT and WD are pairing for the first time, the device must be initialized at first. After the mutual authentication, US, MT, and WD are mutually trusted

Figure 2: Mutual authentication infrastructure.

devices. MT and WD can transmit data under the successful connection and authentication. Once the connection is interrupted or abnormal, go to Step 3.

Step 2. Communication Preparation

Because the factory settings of CB in MT and WD are the same, MT encrypts the CB in ID_{mt} and ID_{wd} and receives SB_{mt} and WD encrypts the CB in ID_{wd} and ID_{mt} and receives SB_{wd}. This step ensures that the only SB_{mt} and SB_{wd} can mutually identify and communicate.

(i) MT and WD compute $Enc_{k_{mt}}(ID_{mt})$ and $Enc_{k_{wd}}(ID_{wd})$ and generate SW_{mt} and SW_{wd}, which are stored in the memory and used for device pairing and authentication. During the process of communication, they do not need to be computed again, thus saving the time for reaching address.

(ii) When MT makes a request to WD for connection and authentication, WD sent SW_{wd} to MT. After encrypting $Dec_{k_{mt}}(SW_{wd})$, MT receives identity ID_{wd}. If abnormal, return $\perp$. Otherwise, MT computes $SB_{mt} \leftarrow Enc_{k_{mt}}(ID_{mt}, ID_{wd}, CB)$ and generates SB_{mt}. MT and WD communicate by SB_{mt}. If acoustic waves sent by MT and WD are not coordinating with SB_{mt}, the session terminates.

(iii) MT sent SW_{mt} to WD. After decrypting $Dec_{k_{wd}}(SW_{mt})$, WD receives identity ID_{mt}. If abnormal, return $\perp$. Otherwise, compute $SB_{wd} \leftarrow Enc_{k_{wd}}(ID_{wd}, ID_{mt}, CB)$ and generate SB_{wd}. WD and MT communicate by SB_{wd}. If acoustic waves transmitted by WD and MT are not coordinating with of SB_{wd}, the session terminates.

(iv) For multiple pairs of trust devices, different pairs generate different SB, which is the foundation of mutual authentication communication.

(v) When US wants to use MT or WD, TS_{mt} or TS_{wd} begins timing, and US must input the correct password of MT and WD. Otherwise, if US inputs wrong password more than many times (US can set) in valid time, output "password error," delete SW_{wd} and SB_{wd}, and end the current session.

(vi) For a better understanding, the workflow of encoding and decoding is shown in Figure 3.

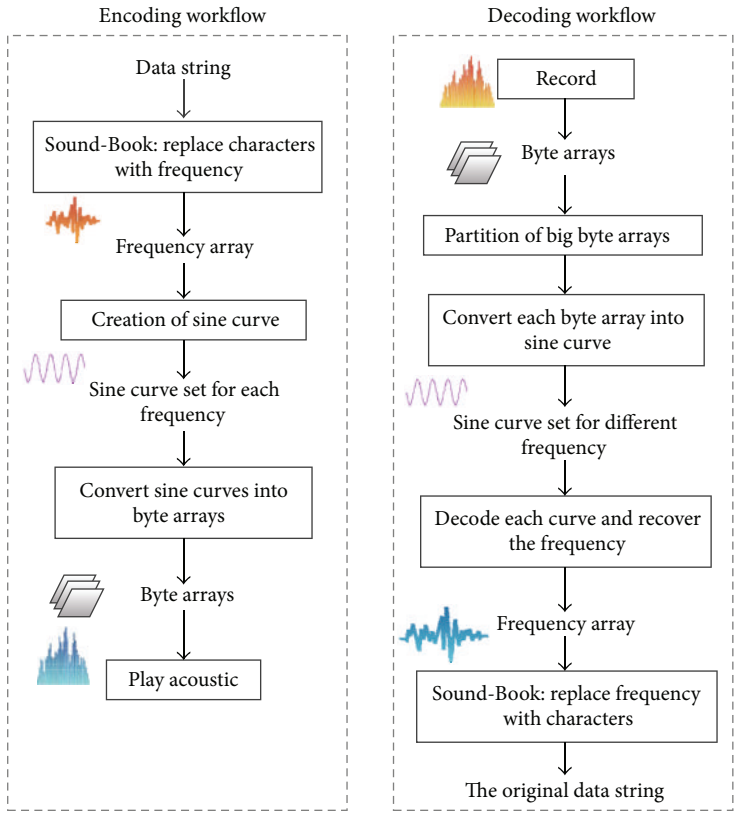


FIGURE 3: Encoding and decoding for acoustic waves.

Step 3. Mutual Authentication

MT and WD are mutually trusted devices which own timestamp-based key-agreement protocol that can generate the shared key K_{mtwd} to transmit messages.

(1) The scheme of MT is as follows.

(i) Choose a 32-bit element k randomly, $k \in R[1, \ldots, q-1]$.

(ii) Compute

$$(k_1, k_2) \leftarrow hash_1(pk_{wd}^k),$$
$$c \leftarrow hash_2(ID_{mt}, ID_{wd}, k_1) \times g^k,$$
$$r \leftarrow hash_3(k_2, c), s \leftarrow k/(r + sk_{mt}),$$
$$t \leftarrow Enc_{pk_{wd}}(ID_{mt}, ID_{wd}, TS_{mt}).$$

(iii) MT transmits the data (c, r, s, t) to WD by acoustic waves.

(2) WD verifies the identity of MT and computes the shared key K_{mtwd}.

(i) If $(c, r, s, t) \notin SB_{wd}$, WD returns $\perp$ and sends "reject" acoustic wave to MT.

(ii) Otherwise, compute $ID'_{mt}, TS_{mt} \leftarrow Dec_{sk_{wd}}(t)$; if $ID'_{mt} \neq ID_{mt}$, WD returns $\perp$ and sends "reject" acoustic wave to MT.

(iii) Otherwise, compute $(k_1, k_2) \leftarrow hash_1((pk_{mt}) \times g^r)^{s \times sk_{wd}} \bmod p$; if $r \neq hash_3(k_2, c)$, WD returns $\perp$ and sends "reject" acoustic wave to MT.

(iv) Otherwise, randomly choose a 32-bit element $k', k' \in R[1, \ldots, q-1]$.

(v) Get a timestamp TS_{wd}.

(vi) Compute

$$\mu \leftarrow g^{k'},$$
$$\sigma \leftarrow (c/hash_2(ID_{mt}, ID_{wd}, k_1))^{k'},$$
$$\delta \leftarrow hash_3(k_1, \sigma), K_{mtwd} \leftarrow hash_4(\sigma),$$
$$\varphi \leftarrow Enc_{k_1}(K_{mtwd}, TS_{wd}),$$
$$\tau \leftarrow Enc_{k_{wd}}(ID_{wd}, ID_{mt}).$$

(vii) WD returns data $(\mu, \delta, \varphi, \tau)$ to MT by acoustic waves.

(3) MT verifies the identity of WD and computes the shared key K_{mtwd}.

(i) If $(\mu, \delta, \varphi, \tau) \notin SB_{mt}$, MT returns $\perp$ and sends "reject" acoustic wave to WD.

(ii) Otherwise, compute $ID'_{wd} \leftarrow Dec_{sk_{mt}}(\tau)$; if $ID'_{wd} \neq ID_{wd}$, MT returns $\perp$ and sends "reject" acoustic wave to WD.

(iii) Otherwise, compute $\sigma \leftarrow \mu^k$; if $\delta \neq hash_3(k_1, \sigma)$, MT returns $\perp$ and sends "reject" acoustic wave to WD.

(iv) Otherwise, compute $TS_{wd} \leftarrow Dec_{k_1}(\varphi)$; if TS_{wd} is not valid time, MT returns $\perp$ and sends "reject" acoustic wave to WD.

(v) Otherwise, compute $K_{mtwd} \leftarrow hash_4(\sigma)$, and accept K_{mtwd} as shared key.

(4) MT and WD are successfully verified. They become mutually trusted devices and transmit data by agreed-upon shared session key K_{mtwd}.

4.3. Data Transmission. MT and WD are mutually trusted devices. MT transmits data m, which should be signcrypted by keys with a sign, to WD via the Bluetooth. After receiving the data, MT and WD will hold a mutual authentication again. Upon successful authentication, data will be decrypted to ensure that it is sent to the trusted receiver. Otherwise, the data will be self-destructed and a "reject" acoustic wave will be sent to the receiver. Then the session will be ended and the linkage between them will be interrupted.

(1) MT gets the Bluetooth address of WD.

(i) WD computes $\gamma \leftarrow Enc_{K_{mtwd}}(Add_{wd})$. Send γ to MT via acoustic wave to open the Bluetooth to receive data.

(ii) After reviving γ, MT computes $Add_{wd} \leftarrow Dec_{K_{mtwd}}(\gamma)$ and opens its Bluetooth. Then establish connection with WD's Bluetooth to send data.

(2) MT signcrypts and transmits the data.

(i) If TS_{mt} is not in the valid time, a "reject" acoustic wave will be sent to MT and the session will be ended. Otherwise, MT signcrypts Add_{wd} and TS_{mt} via shared key to produce signcrypted ciphertext: $C_1 \leftarrow Enc_{K_{mtwd}}(Add_{wd}, TS_{mt})$.

(ii) Signcrypt the data via shared key to produce signcrypted ciphertext: $C_2 \leftarrow Enc_{K_{mtwd}}(m)$.

(iii) Send C_1 and C_2 to WD via the Bluetooth.

(3) WD unsigncrypts the data.

When receiving ciphertext (C_1, C_2), WD will run the following steps to unsigncrypt the ciphertext.

(i) Compute $Add_{mt}, Add'_{wd}, TS_{mt} \leftarrow Dec_{K_{mtwd}}(C_1)$.

(ii) If there is a mismatch between Add'_{wd} and Add_{wd}, C_2 will be self-destructing and will then transmit a "reject" acoustic wave to MT to end the session.

(iii) Otherwise, if TS_{mt} does not belong to the valid time, a "reject" acoustic wave will be sent to MT to end the session.

(iv) Otherwise, compute $m \leftarrow Dec_{K_{mtwd}}(C_2)$.

(v) Display the computing results in terms of the data type (characters, string, picture, video, etc.) of m.

(vi) Return m to MT via the Bluetooth and finish the session.

(vii) If more data should be transmitted, perform the data transmission part again.

(viii) Perform until data transmission completes.

(4) Complete data transmission.

4.4. Devices Addition or Alteration. Both MT and WD are supported by multi-USs as people tend to possess more than one of them in modern society. In other words, one MT or WD might simultaneously match with other trusted MTs or WDs. For instance, when MT_1 and WD_1 are available, in case of the occurrence of bugs in MT_1 or WD_1 or the requirement of MT_2 or WD_2 addition (similar procedures), to add MT_2, it operates as follows.

(i) Initialization: US should store an eight-digit initial password PW_{mt_2} on MT_2.

(ii) Key generation: MT_2 then generates its own key $K_{mt_2} \leftarrow (PW_{mt_2}, ID_{mt_2})$.

(iii) Generation of acoustic wave database: perform Step 2 to produce SW_{mt_2} and SB_{mt_2}.

(iv) Device mutual authentication: perform Step 3 to authenticate that MT_2 and MT_1 (or WD_1) are mutually trusted devices and then produce shared key $K_{mt_2mt_1}$ (or $K_{mt_2wd_1}$) to transmit data, and so forth.

(v) Data transmission test: perform the data transmission part. Transmit test data between MT_2 and MT_1 (or WD_1) via the shared key $K_{mt_2mt_1}$ (or $K_{mt_2wd_1}$) to ensure the mutual trust between devices.

(vi) Complete the MT_2 addition.

4.5. Change Password

(1) Change the password of MT.

US changes the password of MT as follows.

(i) TS_{mt} starts timing as soon as US starts to change password in MT. If US cannot complete the operation to change the password in valid time, output "Password rejects change."

(ii) Otherwise, if US inputs wrong initial password more than many times (US can set) in valid time, output "Password rejects change," delete SW_{mt} and SB_{mt}, and end the current session.

(iii) Otherwise, change the password successfully and the new password is $PW_{mt.new}$.

(iv) MT regenerates its key $K_{mt.new} \leftarrow (PW_{mt.new}, ID_{mt})$, and then use it in the later authentication, operation, and data transmission.

(v) MT regenerates its SW_{mt} and SB_{mt} as a base for communication.

(vi) Device mutual authentication: perform Step 3: the device authentication of MT and WD. Then generate the shared key K_{mtwd} on the basis of timestamp.

(vii) Data transmission test: perform the data transmission part. Transmit test data between MT and WD via the shared key K_{mtwd} to ensure the mutual trust between devices.

(viii) MT password is successfully changed.

(2) Change the password of WD.

US needs to change the password of WD in the procedure as follows.

(i) TS_{wd} starts timing as soon as US starts to change password in WD. If US cannot complete the operation to change the password in valid time, output "Password rejects change."

(ii) Otherwise, if US inputs wrong initial password three times in valid time, output "Password rejects change" and end the current session and delete SW_{wd} and SB_{wd}.

(iii) Otherwise, perform Step 3; if MT and WD are not successfully mutually authenticated, output "Password rejects change."

(iv) Otherwise, change the password successfully and the new password is $PW_{wd.new}$.

(v) WD regenerates its key $K_{wd.new} \leftarrow (PW_{wd.new}, ID_{wd})$, and then use it in the later authentication, operation, and data transmission.

(vi) WD regenerates its SW_{wd} and SB_{wd} as a base for communication.

(vii) Device mutual authentication: perform Step 3: the device authentication of MT and WD. Then generate the shared key K_{mtwd} on the basis of timestamp.

(viii) Data transmission test: perform the data transmission part. Transmit test data between WD and MT via the shared key K_{mtwd} to ensure the mutual trust between devices.

(ix) WD's password is successfully changed.

5. Security Analysis

The security of our system is mainly to ensure the authentication and communication between our devices. It contains the integrity, confidentiality, and effectiveness of data we transmit through acoustic waves. Besides, it also needs to prevent the acoustic channel from recording, replaying, and interfering so as to avoid illegal access to data. So, in this section, we will analyze the security of our scheme. Firstly, the security mechanism in mutual authentication and key-agreement protocol will be introduced. Secondly, we will verify that our scheme is immune to the replay attack. At last, we also demonstrate the resistance to man-in-the-middle attack, which is mostly concerned by consumers. Through these arguments, it is easy to conclude that this scheme has a good security.

5.1. Mutual Authentication. In this system, the relationship between US and MT, WD is pairwise and mutually trusted. In this way, a mutual authentication can be implemented among devices. In the process of mutual authentication between MT and WD, the acoustic waves they use are those with sole device identifier and key encryption. (Taking MT as an example, $SB_{mt} \leftarrow Enc_{k_{mt}}(ID_{mt}, ID_{wd})$, $K_{mt} \leftarrow (PW_{mt}, ID_{mt})$.) Only the MT and WD can identify each other, which is regarded as the basis to enable communication and thereby strengthen the data confidentiality.

During the mutual authentication and data transmission, the system firstly judges whether the transmitting acoustic waves between the two devices belong to SB or not; if not, the system would terminate the session immediately, and then ensure each other's identity to make sure it is trusted.

5.2. Key-Agreement Protocol. MT and WD have established a timestamp-based key-agreement protocol. After the authentication, the shared key K_{mtwd} which is used for data transmission is generated. Based on the mutual authentication between MT and WD, the data confidentiality can be fulfilled by the agreed-upon key K_{mtwd} encrypting the data m and generating $C_2 \leftarrow Enc_{K_{mtwd}}(m)$. When data transmission is finished, the key would employ the Bluetooth address for MT and WD identity authentication and then decrypt the receiving data after the confirmation of identity authentication to make sure the data is from the trusted senders. This proves that the data transmission is secure and valid, the communication between MT and WD is secure, and the transmitted data is confidential, secure, and valid.

5.3. Replay Attack Resistance. (1) Suppose that an attacker attempts to replay the acoustic wave used in the process of the device authentication and data transmission; this would cause interferences such as multiple acoustic sources, unidentified acoustic source, and inappropriate wavelength. Once the interferences are detected, exceptions would occur in the system and the current session $\perp$ would be terminated immediately. So the attacker in this scheme would fail to get the relevant information by replaying any acoustic wave.

(2) Suppose that an attacker attempts to intercept the transmitting ciphertext C_2 and replay it; the attacker would fail. There exist four reasons: firstly, this scheme is timestamp-bound; secondly, the transmit data is ciphertext encrypted in different ways; thirdly, before decryption, the data needs Add_{wd} matching; and, fourthly, it is impossible for the attacker to get the one-time agreed-upon shared key K_{mtwd} in valid time. Also, once the attack is detected, the system would self-destruct the ciphertext C_2 and terminate the current session $\perp$ immediately. So the attackers in this scheme would fail to get the transmit data.

(3) In each connection between MT and WD, the system would choose random 32-bit element k for which the attacker would be unable to guess, get, change, forge, or break the confidentiality criterion without being detected by MT and WD. So the attackers in our scheme would fail the replay and nonsynchronous attack.

Table 1: Experiment environment.

	Telephone 1 (MT)	Wearable devices 2 (MT_2 as WD)	Telephone 3 (MT_3)	Telephone 4 (MT_4)
Type	HTC One	Samsung Galaxy S4	Nubia Z5S	Huawei C8650
OS	Android 4.2	Android 4.3	Android 4.2	Android 2.3.3
Microphone and loudspeaker	Yes	Yes	Yes	Yes
Bluetooth	4.0	4.0	4.0	2.1
Memory	2 GB	2 GB	2 GB	256 MB

5.4. Man-in-the-Middle Attack Resistance. (1) Suppose that the attacker gains SW_{mt} or SW_{wd} and is involved in the arithmetic when the basic communication is built between MT and WD. However, exceptions would occur because ID_{mt} and ID_{wd} cannot be obtained after decryption, so the system would end the current session $\perp$ immediately.

(2) Suppose that, in the process of the mutual authentication between MT and WD, attackers record the data (c, r, s, t) transmitted by MT to WD through the acoustic wave into (c', r', s', t') and then deliver it to WD to be authenticated. If there are interferences such as multiple acoustic sources, unidentified acoustic sources, or inappropriate wavelength when WD is accepting (c', r', s', t'), the system will immediately terminate the current session $\perp$ due to exceptions. Otherwise the system would compute $ID'_{mt} \leftarrow Dec(t')$, where $ID'_{mt} \neq ID_{mt}$, which also leads to exceptions that make the system end the current session $\perp$ at once.

Suppose that the attackers record data $(\mu, \delta, \varphi, \tau)$, transmitted by WD to MT through acoustic waves, into $(\mu', \delta', \varphi', \tau')$ and then deliver it to MT to be authenticated. If there are interferences such as multiple acoustic sources, unidentified acoustic sources, or inappropriate wavelength when MT is accepting $(\mu', \delta', \varphi', \tau')$, the system will immediately end the current session $\perp$ due to exceptions. Otherwise the system would compute $ID'_{wd} \leftarrow Dec(\tau')$, where $ID'_{wd} \neq ID_{wd}$, which also leads to exceptions that make the system kill the current session $\perp$ at once.

(3) Suppose that, in the data transmission between MT and WD, attackers get γ, which is transmitted by WD to MT. However, the Bluetooth device address cannot be obtained because γ is encrypted. Thus the attack cannot be implemented. Therefore, this scheme is secure and reliable because it can resist the man-in-the-middle attack.

6. Implementation

6.1. Experiment Environment. Openness is the characteristic of Android system, which is the mainstream OS for intelligent mobile. So we choose it as the main experiment OS. To test the stability, we use various devices with different versions of Android. Other details of our experiment environment are shown in Table 1.

6.2. Experimental Process. We develop an app to implement our scheme, which is called "VoiceBluetooth." It has 6 modules: "Bluetooth open," "Bluetooth close," "Enable search," "Traditional search," "VoiceBluetooth Client," and "VoiceBluetooth Server."

(i) "Bluetooth open" and "Bluetooth close" are for data transmission and data sharing between multiwearable devices after mutual authentication.

(ii) "Enable search" allows multiple devices to search for a connection and connect.

(iii) "Traditional search" is for Bluetooth search, authentication, and connection.

(iv) "VoiceBluetooth Server" and "VoiceBluetooth Client" are flexible for devices to select as a role to connect to one another, enabling sharing of data between any two devices.

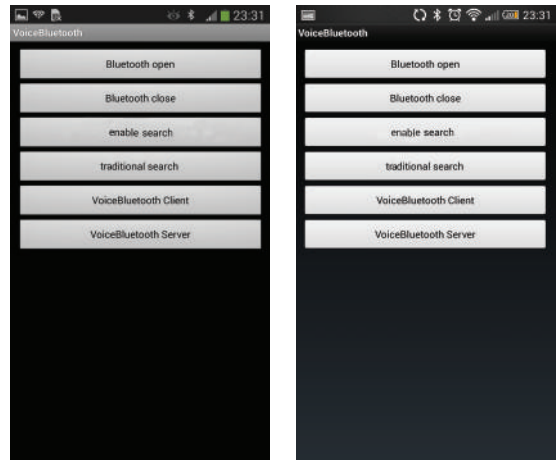
The app should be running on both MT and WD. One is acting as a server; the other is a client.

In the authentication process, MT will use the app to emit authentication acoustic wave, while WD will receive it. Data can only be transmitted when the devices are authenticated as trusted devices by each other. Mutual authentication and data sharing process workflow are shown in Figures 4, 5, 6, 7, 8, 9, and 10.

In the experiment, by changing the conditions from a relative quiet environment to a noisier one, we repeatedly tested the device authentication and data transmission, probing into MT and WD's encryption towards *CB* and other situations like device authentication, data transmission, password updating, adding and changing MT_3, and recording relevant experimental data.

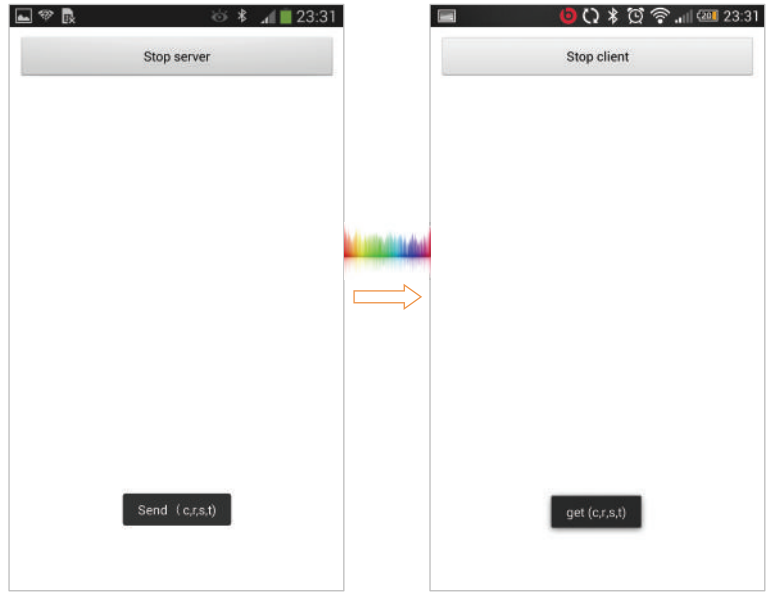
6.3. Experimental Data and Conclusion. In a not absolutely quiet environment where the experiment is conducted, mobile phones and wearable device can identify each other in a distance less than 20 cm well, while, in a distance beyond 20 cm, the recognition rate is slightly lower. This distance rightly matches the secure distance of a person who has multiple mobile phones and wearable devices. Within the distance, people can make the mutual authentication and data sharing possible between their devices. For example, people can transmit data about their health and bodily functions saved in the wearable devices to mobile phones and then to computers or the Internet. Likewise, data such as text messages, schedules, and videos can also be transmitted to the wearable devices, which is convenient for reminding and reading.

In order to let people have a better acoustic experience and know that their devices are communicating with each other, the range of frequency of acoustic wave used in our experiment is mainly from 588 Hz to 4419 Hz. They are called coloring ring back tone (CRBT) [29].



(a) (b)

Figure 4: The first step of experimental process. (a) First MT screen; (b) first WD screen.



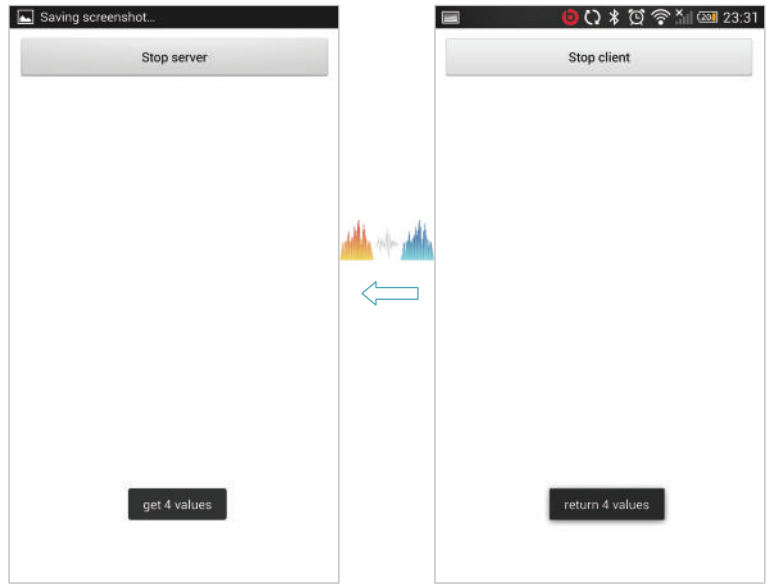
(a) (b)

Figure 5: The second step of experimental process. (a) MT computes (c, r, s, t) and sends their acoustic waves to WD; (b) WD gets (c, r, s, t).

Table 2: Performance of computations.

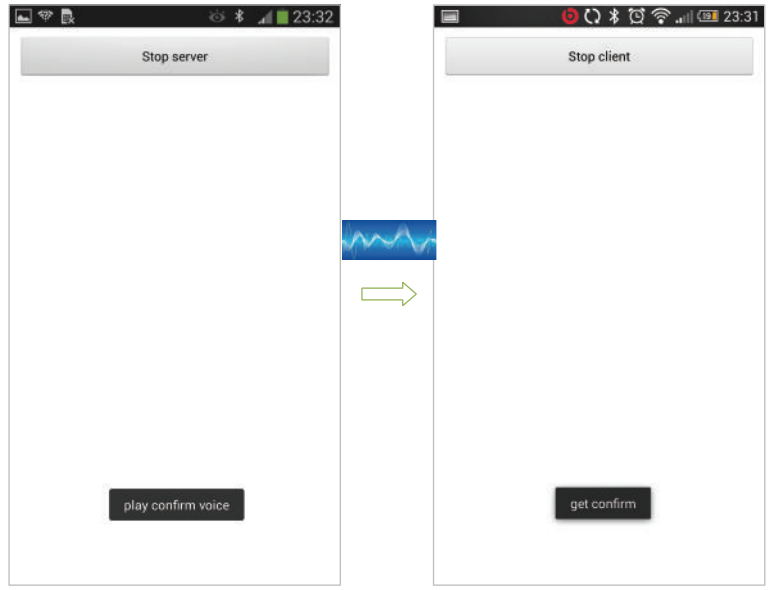
	Exp	Hash	Enc	Dec	Multi	Div	Nonce	Timestamp	Times of TAW[1]	Determine	Times of TDVB[2]
Communication preparation											
MT			2	1					2		
WD			2	1					1		
Mutual authentication											
MT	2	5	1	2	1	1	1		1 (+3 opt)	4	
WD	4	5	2	1			1	1	1 (+1 opt)	3	
Data transmission											
MT			2	1				1	(+1 opt)		2
WD				3					1 (+2 opt)	4	

[1]Times of transmit acoustic waves.
[2]Times of transmit data via Bluetooth.



(a) (b)

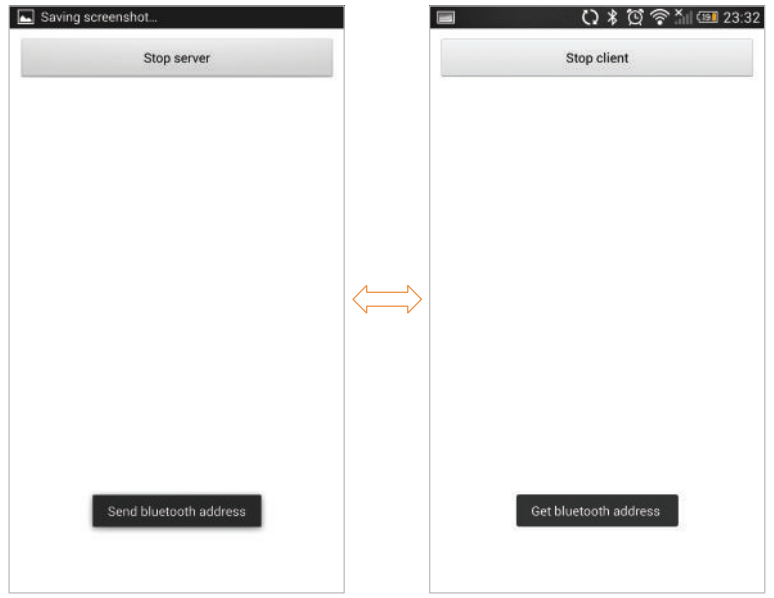
FIGURE 6: The third step of experimental process. (a) MT gets $(\mu, \delta, \varphi, \tau)$; (b) WD verifies the identity of MT, computes $(\mu, \delta, \varphi, \tau)$, and returns them to MT by acoustic waves.



(a) (b)

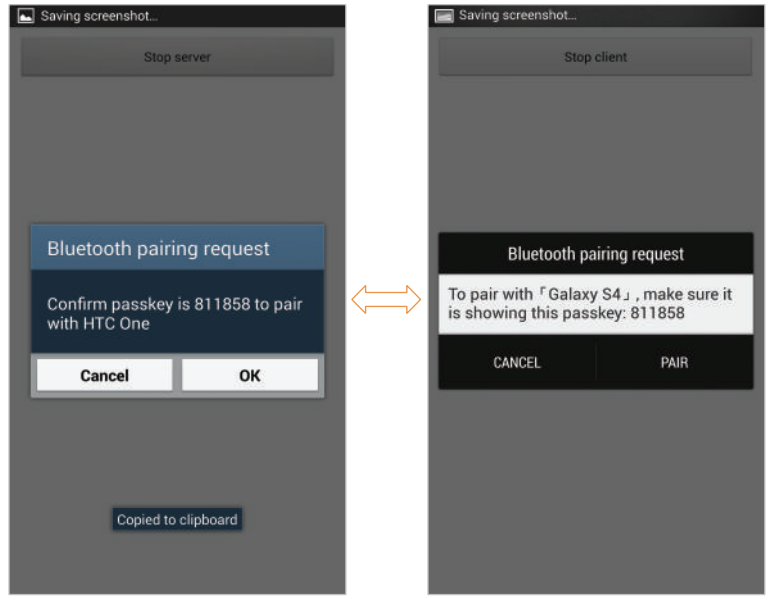
FIGURE 7: The fourth step of experimental process. (a) MT verifies the identity of WD, computes K_{mtwd}, and accepts it as shared key; (b) MT and WD are now mutually authenticated.

According to the recognition rate in our experiment, using acoustic waves of too high or too low frequency is temporally not recommended. The highest frequency of the acoustic waves used in this experiment is 15 KHZ, which is beyond the identification of experimenters' hearing. However, that still can be authenticated by experimental devices, though the authentication rate is slightly reduced. If the frequency is increased to 20 KHz or more, we can realize the ultrasonic wave transmission. Ultrasonic propagation is not affected by environmental noise interference; it is more stable, directionally stronger, and easier to concentrate, and it can shorten the time for certification. Because the human ear cannot hear ultrasonic, it is more concealed and could spread farther, so the authentication will be better and achieve the desired distance. Based on this, a conclusion can be made that if ultrasonic wave transmission is used, the hardware of devices



(a) (b)

Figure 8: The fifth step of experimental process. (a) Transmit the Bluetooth address, (b) WD gets the Bluetooth address of MT.



(a) (b)

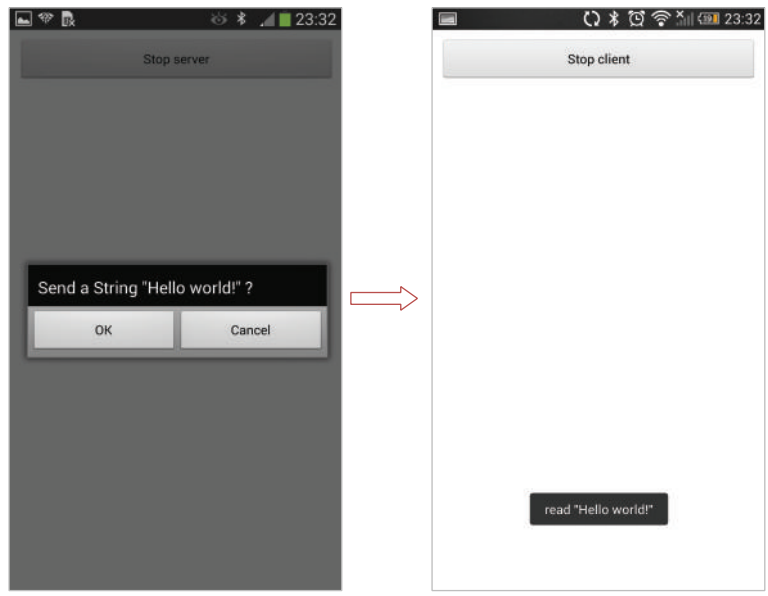
Figure 9: The sixth step of experimental process. (a) Bluetooth pairing; (b) Bluetooth pairing.

such as loudspeakers and microphones should be equally matched.

In the experiment, the increase of volume can lower the influence of noise from external environment within a certain range and improve the authentication rate.

The range of per unit play time of the frequency corresponding to each acoustic wave is from 30 ms to 150 ms. When the play time is 100 ms, the time used in transmitting an IMEI code with 15 bits via acoustic wave is less than two seconds, and a mutual authentication time is about 10 seconds, processed automatically, so the recognition rate is high. When the play time is at the shortest 30 ms, the recognition rate is a little bit lower. But if the distance between experimental devices is cut short, it can still remain a good recognition rate.

After experimental devices are mutually authenticated through acoustic waves, data transmission, password updating, and adding and changing MT_3 can be done successfully by using Bluetooth, which all can be proved in this scheme.



(a) (b)

Figure 10: The seventh step of experimental process. (a) MT signcrypts and transmits the data; (b) WD unsigncrypts the data and completes data transmission.

In the experiment, after MT and WD are mutually authenticated, MT_4 tries to record and play the acoustic waves when MT and WD are reconnecting. However, the attack cannot be implemented because the system would interrupt the connection automatically when recognizing interferences which result from the asynchronization with the acoustic waves played between the trusted devices. Therefore only mutually trusted devices can be interconnected.

This scheme makes it possible that mutually trusted authentication can be realized via acoustic waves and that data can be transmitted through Bluetooth among multiple wearable devices. The scheme can also protect private data, making sure they can be shared.

6.4. Characteristic Analysis. We would like to attain the following characteristic analysis in Table 2. It is obvious in Table 2 above that the time complexity of our algorithm in the process belongs to $O(1)$, that is, constant level. And this is satisfactory, which means that the time for preparation and authentication is fixed.

7. Conclusions

In this paper, we presented new schemes for mutual authentication between multiwearable devices based on acoustic channel. We have designed an authentication protocol to ensure that the acoustic wave authentication is secure and efficient. In the process of the authentication, by adopting multiple-times identity authentication, agreed-upon shared key, and on-the-fly password change, we have realized the secure data transmission and sharing among mutually trusted devices and effectively precluded the unauthorized third-parties or third-party devices from stealing the data. In addition, the protocol brings convenience for the users in the case that they have multi-MTs, multi-WDs, and multi-laptops. In addition, the protocol brings convenience for the users because it can enable the automatic data synchronization and sharing among their multiple devices.

Compared with other transmission technologies like NFC and Bluetooth, acoustic wave transmission can reach more people due to lower hardware requirements and implementation costs because only the hardware included in each mobile phone or wearable device such as microphone and loudspeaker is needed to fulfill the mutually trusted identification authentication and data transmission. So we can see how acoustic wave technology is widely used in the market and its tremendous development potential.

In the future, we would endeavor to make some further optimizations and improvements such as making per unit play time of the frequency shorter and recognition rate more accurate, improving the security and confidentiality of the scheme by reducing the hardware requirements, and employing ultrasonic wave to transmit data.

Definitions of Symbols Used in Our Protocol

p: A large prime
q: A large prime factor of $p - 1$
g: An integer with order q modulo p chosen randomly from $[1, \ldots, p - 1]$
(sk_{mt}, sk_{wd}): MT's and WD's private key, chosen uniformly at random from $[1, \ldots, q - 1]$

(pk_{mt}, pk_{wd}):	MT's and WD's public key, $pk_{mt} = g^{sk_{mt}} \bmod p$, $pk_{wd} = g^{sk_{wd}} \bmod p$
$hash_1, hash_2, hash_3, hash_4$:	A one-way hash function
Add_{mt}, Add_{wd}:	The Bluetooth device address of MT and WD
ID_{mt}, ID_{wd}:	The device identification of MT and WD (default 15 bits)
PW_{mt}, PW_{wd}:	The initial password of US stored in MT and WD
$PW_{mt.new}, PW_{wd.new}$:	The new password of MT and WD
CB:	The factory settings acoustic waves database of MT and WD; all the devices are the same (Code-Book)
SB_{mt}, SB_{wd}:	The encrypted and mutually trusted acoustic waves database of MT and WD with a predetermined length based on the factory setting (Sound-Book)
SW_{mt}, SW_{wd}:	The acoustic waves computed by the mutually trusted Bluetooth device address and the device identification of MT and WD
K_{mt}, K_{wd}:	The key of MT and WD (default 32 bits)
TS_{mt}, TS_{wd}:	The timestamp of MT and WD
m:	Data will be transferred between MT and WD.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors wish to thank the anonymous reviewers for their insightful and invaluable suggestions and comments. This work was in part supported by 973 Program (Grant no. 2011CB302400), Natural Science Foundation of Guangdong Province, China (Grant no. S2013010013728), Educational Commission of Guangdong Province, China, Project no. 2013KJCX0131, and Guangdong University of Petrochemical Technology's Internal Project no. 2012RC0106. Wei Sun is the corresponding author.

References

[1] P. Castillejo, J.-F. Martínez, L. López, and G. Rubio, "An internet of things approach for managing smart services provided by wearable devices," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 190813, 9 pages, 2013.

[2] S. Abolfazli, Z. Sanaei, A. Gani, F. Xia, and L. T. Yang, "Rich mobile applications: genesis, taxonomy, and open issues," *Journal of Network and Computer Applications*, vol. 40, no. 1, pp. 345–362, 2014.

[3] M. A. Chowdhury, W. McIver Jr., and J. Light, "Data association in remote health monitoring systems," *IEEE Communications Magazine*, vol. 50, no. 6, pp. 144–149, 2012.

[4] P. Castillejo, J.-F. Martinez, J. Rodriguez-Molina, and A. Cuerva, "Integration of wearable devices in a wireless sensor network for an E-health application," *IEEE Wireless Communications*, vol. 20, no. 4, pp. 38–49, 2013.

[5] J. Gao, V. Kulkarni, H. Ranavat, L. Chang, and H. Mei, "A 2D barcode-based mobile payment system," in *Proceedings of the 3rd International Conference on Multimedia and Ubiquitous Engineering (MUE '09)*, pp. 320–329, IEEE, June 2009.

[6] J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing-is-believing: using camera phones for human-verifiable authentication," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 110–124, IEEE, May 2005.

[7] L. Li, X. Zhao, and G. Xue, "Near field authentication for smart devices," in *Proceedings of the 32nd IEEE Conference on Computer Communications (INFOCOM '13)*, pp. 375–379, April 2013.

[8] K. M. J. Haataja and K. Hyppönen, "Man-in-the-middle attacks on bluetooth: a comparative analysis, a novel attack, and countermeasures," in *Proceedings of the 3rd International Symposium on Communications, Control, and Signal Processing (ISCCSP '08)*, pp. 1096–1102, IEEE, March 2008.

[9] R. Pries, W. Yu, X. Fu, and W. Zhao, "A new replay attack against anonymous communication networks," in *Proceedings of the IEEE International Conference on Communications (ICC '08)*, pp. 1578–1582, Beijing, China, May 2008.

[10] G. Yong, H. Lei, X. Kun, L. Shu-ru, and Q. De-pei, "An improved authentication protocol with dynamic update in rfid system," in *Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '08)*, IEEE, October 2008.

[11] F. Stajano and R. Anderson, "The resurrecting duckling: security issues for ad-hoc wireless networks," in *Proceedings of the 7th Security Protocols Workshop*, Lecture Notes in Computer Science, pp. 172–194, April 1999.

[12] A. Matos, D. Romão, and P. Trezentos, "Secure hotspot authentication through a near field communication side-channel," in *Proceedings of the IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '12)*, pp. 807–814, IEEE, October 2012.

[13] Q. Z. Sheng, S. Zeadally, A. Mitrokotsa, and Z. Maamar, "RFID technology, systems, and applications," *Journal of Network and Computer Applications*, vol. 34, no. 3, pp. 797–798, 2011.

[14] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, pp. 47–53, Springer, Berlin, Germany, 1985.

[15] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology-ASIACRYPT*, vol. 2894 of *Lecture Notes in Computer Science*, pp. 452–473, Springer, 2003.

[16] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[17] L. Chen, "Ring group signatures," in *Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in*

Computing and Communications (TrustCom '12), pp. 409–418, IEEE, June 2012.

[18] J. Ren and L. Harn, "An efficient threshold anonymous authentication scheme for privacy-preserving communications," *IEEE Transactions on Wireless Communications*, vol. 12, no. 3, pp. 1018–1025, 2013.

[19] Q. Jing, Y. Zhang, X. Liu, and A. Fu, "An efficient handover authentication scheme with location privacy preserving for EAP-based wireless networks," in *Proceedings of the IEEE International Conference on Communications (ICC '12)*, pp. 857–862, Ottawa, Canada, June 2012.

[20] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) ≪ cost(signature) + cost(encryption)," in *Advances in Cryptology—CRYPTO '97. Proceedings 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, 1997*, vol. 1294 of *Lecture Notes in Computer Science*, pp. 165–179, 1997.

[21] Y. Zheng and H. Imai, "How to construct efficient signcryption schemes on elliptic curves," *Information Processing Letters*, vol. 68, no. 5, pp. 227–233, 1998.

[22] B. Libert and J.-J. Quisquater, "A new identity based signcryption schemes from pairings," *Cryptology ePrint Archive*, vol. 2003, p. 23, 2003.

[23] H. Wang, Y. Zhang, and B. Qin, "Analysis and improvements of two identity based anonymous signcryption schemes for multiple receivers," in *Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom '12)*, pp. 1057–1062, IEEE, June 2012.

[24] P. S. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Proceedings of the 11th International Conference on Theory and Application of Cryptology and Information Security (ASIACRYPT '05)*, pp. 515–532, Springer, 2005.

[25] J. K. Liu, J. Baek, J. Zhou, Y. Yang, and J. W. Wong, "Efficient online/offline identity-based signature for wireless sensor network," *International Journal of Information Security*, vol. 9, no. 4, pp. 287–296, 2010.

[26] F. Li, M. K. Khan, K. Alghathbar, and T. Takagi, "Identity-based online/offline signcryption for low power devices," *Journal of Network and Computer Applications*, vol. 35, no. 1, pp. 340–347, 2012.

[27] M. Barbosa and P. Farshim, "Certificateless signcryption," in *Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS '08)*, pp. 369–372, ACM, March 2008.

[28] "Chinese association for cryptologic research," China Development Report, 2012.

[29] H. Fukai and Y. Mitsukura, "Design support system for coloring illustrations by using the colors preferred by a user as determined from the hue patterns of illustrations prepared by that user," *IEEJ Transactions on Industry Applications*, vol. 131, no. 5, pp. 685–691, 2011.