IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 15, 2019, accepted February 8, 2019, date of current version March 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2900727

Sec-D2D: A Secure and Lightweight D2D Communication System With Multiple Sensors

MINGSHENG CAO[1], (Member, IEEE), LUHAN WANG[1], HUA XU[2], (Member, IEEE), DAJIANG CHEN[1], (Member, IEEE), CHUNWEI LOU[3], (Member, IEEE), NING ZHANG[4], (Member, IEEE), YIXIN ZHU[5], AND ZHIGUANG QIN[1], (Member, IEEE)

[1]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[2]School of Physics and Electronic Engineering, Yancheng Teachers University, Yancheng 224007, China
[3]Institute of Innovation and Entrepreneurship, University of Electronic Science and Technology of China, Chengdu 611731, China
[4]Department of Computing Science, Texas A&M University at Corpus Christi, Corpus Christi, TX 78412, USA
[5]School of Computer Science and Engineering, Xinjiang University of Finance and Economics, Ürümqi 830012, China

Corresponding author: Zhiguang Qin (qinzg@uestc.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61872059, Grant 61502085, Grant 61771417 and Grant 61751110, and in part by the China Postdoctoral Science Foundation under Grant 2015M570775.

ABSTRACT Device-to-Device (D2D) communication is a promising method for the emerging Internet of Things. Secure information exchange plays a key role in the application of D2D communication. Considering that the wireless devices are powered by batteries, in this paper, a lightweight secure D2D system is designed by using multiple sensors on mobile devices. Specifically, by leveraging an acceleration sensor equipped in two wireless devices, a lightweight and efficient key distribution scheme for secure D2D communication is proposed. Based on the distributed secure key, an efficient near-field authentication is developed with a speaker and a microphone to determine whether these two devices are physically close; and a secure information exchange scheme with high efficiency, which includes message encryption/decryption and message authentication, is presented over the audio channel and the RF channel. The Extensive experiments are provided to demonstrate that our system can achieve a secure information exchange between two wireless devices with low energy consumption and computing resources.

INDEX TERMS Secure D2D communication, sensors, key distribution, near field authentication, Internet of Things.

I. INTRODUCTION

As one of the promising technologies for wireless networks, Device-to-Device (D2D) communication [2], which allows direct communication between two mobile devices without the assistance of the base station and other network infrastructures, has been widely used in Internet-of-Things (IoT) to improve the network throughput, reduce energy consumption and overcome the shortage of spectrum. IEEE 802.11, 802.15 standards provide many protocols for D2D communication, such as, Wi-Fi, LTE, and Bluetooth. However, due to the security issues of IEEE standards protocols [3], [4] and the built-in vulnerability of wireless mechanism, D2D communication faces several serious security issues, e.g., information tampering, node impersonation, message replay, and message eavesdropping.

Security is very important in many application scenarios of D2D communication, such as near-field payment, personal medical information (PMI) transferred in Wireless Body Area Network (WBAN), vehicle information in Internet of Vehicles (IoV), and smart home(as shown in Fig. 1). It is necessary to find a way to achieve secure D2D communication when the transmitted information includes personal private or sensitive data. Usually, encryption schemes (e.g., Data Encryption Standard (DES), and Advanced Encryption Standard (AES)) are used to resist message eavesdropping attack, while message authentication methods are used to resist the attack of information tampering, node impersonation and message replay, [5], [6]. However, a secure key is required to be pre-shared between legitimate users when encryption schemes and message authentication protocols are used for secure communication. It is crucial in secure D2D communication to generate and distribute a secure key. Traditionally, trusted-third-party-based method (e.g.,

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

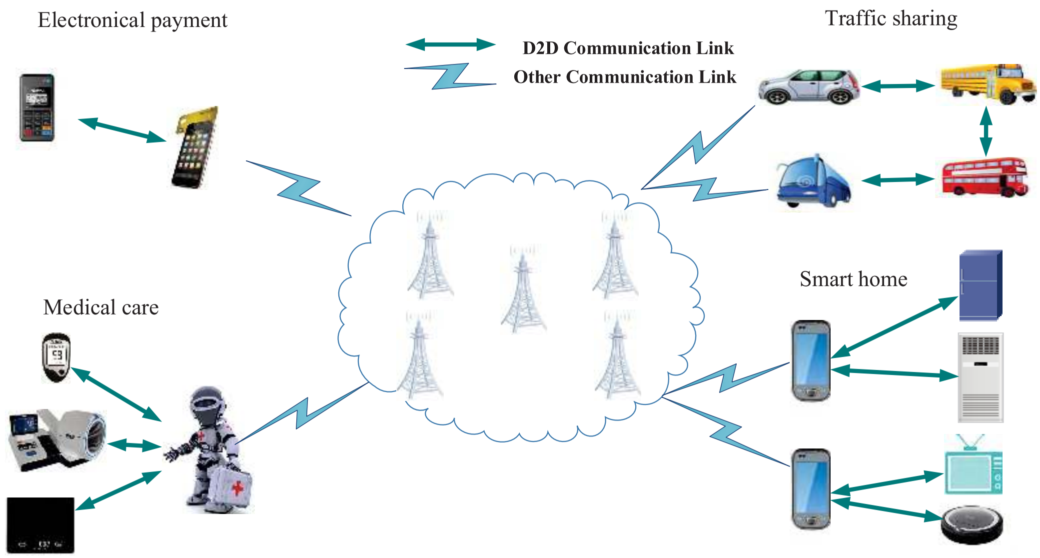


FIGURE 1. D2D communication scenarios.

Kerberos protocol [7], [8]) and public-key-based method (e.g., Diffie-Hellman protocol [9]) are used to distribute a secure key. However, when these schemes meet D2D communication, they face several problems as follows. (1) It is difficult to generate and distribute a key with the help of the third party due to the mobility of wireless devices in D2D communication scenarios; and (2) public-key-based key distribution methods require high computing ability and energy consumption, while wireless devices have limited computing capability and energy as most of them are powered by batteries. Hence, a secure D2D communication system with a lightweight and efficient key distribution method is the keystone for the wide application of D2D communication.

In this paper, a lightweight and efficient secure D2D communication system is proposed, which includes a key distribution scheme, a near field authentication scheme and a secure data transmission scheme. Acceleration sensor is equipped in many wireless devices, for instance, smart watches, smart phones, and smart bracelets. Considering the increasing commercialization of the acceleration sensor in many existing wireless devices, a lightweight and efficient key distribution scheme for secure D2D communication is proposed by using the acceleration sensor. Moreover, considering that most existing wireless devices equipped with the microphones and speakers, we present a lightweight near field authentication protocol by leveraging acoustic hardware (i.e., Speaker and Microphone). Furthermore, we propose a lightweight secure data transmission scheme, which includes message encryption/decryption and message authentication, to further improve the efficiency of the communication system.

In the proposed secure D2D communication system, two wireless devices Dev_A and Dev_B equipped with an acceleration sensor and the acoustic hardware Speaker/Microphone, plan to transmit some secure data to each other. First of all, they need to pre-share a symmetrical secure key for transmitting and authenticating the message. A key distribution scheme is proposed as follows. Holding two devices in one hand and randomly shaking over a period of time, the accelerometer's 3-dimensional data is measured as random resource for key generation. Since the trajectories of movement of these two phones are similar and random. The measurements of these two devices should have a certain similarity and sufficient randomness. Hence, a symmetrical secure key can be generated from the randomness and the similarity. The key distribution scheme includes four steps: random source measurement; measurement preprocessing; bit quantification; and information reconciliation and privacy amplification.

The main goal of this paper is to design a secure near field D2D communication system. Due to the fact that most of the wireless devices in D2D communication are powered by small batteries with limited energy, energy saving should be taken into account seriously in the system design of the D2D communication. To reduce unnecessary information interaction and extend the life cycle of the devices, a near field authentication before data transmission is required to identify if these two devices are physically close. Considering that speakers and microphones are low prices and can be easily found in the most of mobile devices, in this paper, a near field authentication scheme is proposed with speaker and microphone. This proposed scheme can be used for determining if these two devices are physically close or not according to the time consumption of the audio transmission between these two devices. Moreover, a lightweight secure data transmission scheme with the high efficient message encryption/decryption algorithm and message authentication algorithm is presented over two wireless channels, i.e., audio channel and RF channel (WiFi or Bluetooth). An application software of the proposed secure D2D communication system is designed for android system. Extensive experiments are conducted to evaluate the performance of the proposed D2D communication scheme by using the application on mobile phones. It shows that our system can provide secure communication with high security, high efficiency and low energy consumption.

The proposed system can be used for exchanging private and sensitive data in wireless body area networks (WBAN). Actually, the doctor and the patient can share information with each other securely with the proposed system, in which, both of them wear a smart device with the required sensors, such as smart watch and smart phone. The main contributions of this paper is summarized as follows.

(1) A new system model for secure D2D communication is designed by using multiple sensors, in which, a lightweight key distribution scheme is proposed with the measurements of acceleration sensor by holding two wireless devices together and shaking them randomly; a near field authentication is presented with speaker and microphone to identify if these two devices are physically close; and message encryption and authentication scheme is developed over audio channel and RF channel (e.g., WiFi or Bluetooth).

(2) An application software is developed on android system to realize the proposed secure D2D communication system. Moreover, extensive experiments based on the application software are conducted. The results demonstrate that the proposed system can achieve secure D2D communication with low computing resources and energy consumption.

This paper is organized as follows. We review the state-of-the-art related work in Section II. Section III introduces the architecture designed in this paper. Section IV presents our key distribution scheme. In Section V, the near field authentication and secure data transmission schemes are proposed. Section VI provides performance evaluation of the proposed system. Section VII gives the conclusion.

II. RELATED WORK

Key distribution has been proposed in many active research works based on dynamic biometric features [12], [13] and radio channel features [14]–[16]. In [12] and [13], the key generation schemes were proposed by using Electrocardiograph (ECG). Due to the reciprocity, space uniqueness and time variability of wireless channel, a secure key can be obtained by measuring the channel gains [17]. Generally, several channel parameters, (e.g., Received Strength Signal (RSS) and Channel State Information (CSI) [15], [17]) can be collected as the random source to extract a secure key. However, the methods above require to measure physical quantities or dynamic biometric features which cannot be available in a general D2D communication device [21].

Recently, the acceleration sensor was leveraged in device identification and key distribution. In [18] and [19], the measurements of acceleration sensor were used to detect if two wireless devices have been experienced a similar movement trajectory or movement patterns. A gesture-based identification scheme by using accelerometers was proposed in [20]. More recently, a device identification protocol with acceleration information was presented in [11]. Key distribution with acceleration sensor was studied in [22], [24], and [25]. Specifically, pairwise nearest neighbor quantization was used in [22], while hash functions and heuristic search trees was leveraged in [23]. A symmetric key distribution protocol by capturing users walking characteristics with accelerometers was proposed in [24]. In [25], accelerometer and vibration motor were used to secure information transmission. The related works also include [26] and [27].

Traditionally, sound is used for communication which takes acoustic waves as carrier waves via the air or other mediums. Recently, sound for authentication has attracted a lot of researches. Voice recognition was proposed for device authentication in [28]. But these schemes were vulnerable to replay attack. Zhang *et al.* [29] proposed a practical liveness detection scheme by using sound recognition. Audio hardware (i.e., Microphone and Speaker) fingerprints can be leveraged for device authentication [21], [30]. Specifically, Chen *et al.* [21] found that each audio hardware, speaker and microphone, has unique characteristics for device identification.

In this paper, a secure D2D communication system is proposed, in which, a lightweight key generation and distribution protocol is designed by leveraging acceleration information. The system also includes an audio based near field authentication scheme, which uses the sound transmission time to measure the distance between source devices and target devices. Many D2D communication scenarios can leverage the proposed communication system for secure information transmission, for example, Near Field payment and name card transmission.

III. THE SYSTEM ARCHITECTURE

In this section, an architecture of the secure D2D transmission system is first proposed, and then, the key distribution scheme, near field authentication scheme, and secure information transmission scheme are introduced, respectively.

A. SYSTEM ARCHITECTURE

It is assumed that there two devices Dev_A and Dev_B, which are equipped with the acoustic hardware Speaker/Microphone as well as an acceleration sensor, plan to exchange some private information with each other (without the assistance of network infrastructures) in the presence of an opponent Eve. To achieve the goal, a secret key generation and exchange between Dev_A and Dev_B is required before secure information transmission. Considering each device powered by battery, a lightweight key extraction scheme is proposed to generate common random bits as secret key by using accelerators. In order to further save energy consumption, Dev_A and Dev_B need to make sure they are physically close before secure transmission to avoid unnecessary information interaction.

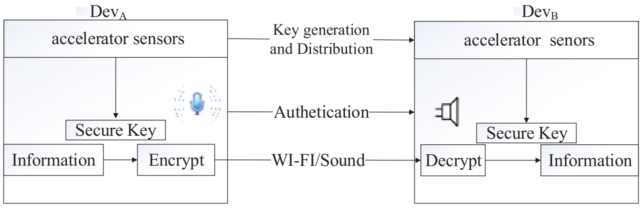


FIGURE 2. Architecture of our secure D2D communication system.

Hence, a near field authentication is necessary when a session request is initiated by Dev_A or Dev_B. To this end, a near field authentication scheme is proposed by using acoustic hardware Speaker/Microphone. Following that, a secure information transmission scheme is proposed over two channels (audio channel and FR channel) which can achieve in both confidentiality, integrity, and authentication with a high efficiency encryption/decryption algorithm. Fig. 2 shows the architecture of our system.

B. KEY GENERATION AND DISTRIBUTION

Accelerators are used to produce keys as the two devices share the same movement. It includes four steps: random source generation, measurements preprocessing, bit quantification and information reconciliation and privacy amplification. (1) Random Source Generation Step: the acceleration measurements will be recorded as the random source by shaking Dev_A and Dev_B randomly; (2) Measurements Preprocessing Step: the extreme points of the measurements will be extracted for bit quantification; (3) Bit Quantification Step: the vector of extreme points will be converted into random bit string; (4) Information Reconciliation and Privacy Amplification Step: information reconciliation is used to make Dev_A and Dev_B agree upon the same bit string though information exchange between them, while privacy amplification is to improve the key's entropy as the information exchange during information reconciliation could make the entropy of bit string loss.

C. NEAR FIELD AUTHENTICATION AND SECURE TRANSMISSION

Speakers and microphones are the common hardware equipped on a lot of wireless devices, e.g., mobile phones, smart watches and many IoT devices, while speakers can be used for sound propagation and microphones can be used to receive the sounds. The distance between source devices and target devices can be measured by using the spread of sound, as $distance = v \cdot t$, where v is the speed of sound, and t is the transmitted time. Based on the traditional sound-based distance measuring method, a lightweight near field authentication scheme is proposed to verify if these two devices are physically close. Moreover, a high efficiency and secure information transmission scheme over two channels is proposed, in which, an audio channel is used to distribute the session key and provide the integrity and authentication of the message, and a FR channel (e.g., WiFi and Bluetooth) is used to transmit the encrypted information.

IV. KEY DISTRIBUTION SCHEME

It is assumed that Dev_A and Dev_B are equipped with an acceleration sensor, and they want to share a symmetrical key for secure communication. In the proposed key distribution scheme, the 3-dimensional accelerator measurements are leveraged as random source. Specifically, this scheme includes the following steps. (1) Random Source Generation Step: holding Dev_A and Dev_B in one hand, and shaking them several seconds to record the measurements of their accelerometers. (2) Measurements Preprocessing Step: a data synchronization method is designed to overcome the problem that time asynchrony during sampling process, and extreme points extraction algorithm is proposed to avoid low entropy of the generated key. (3)Bit Quantification Step: due to the fact that symmetric key used in many cryptographical protocols is a random bit string, a bit quantification algorithm [31] is presented to convert the extreme points into bit string. (4) Information Reconciliation and Privacy Amplification Step: an information reconciliation algorithm is proposed with error-correcting code and index matching algorithm; and a privacy amplification algorithm by using a lightweight hash function is presented to improve the key's entropy.

A. RANDOM SOURCE GENERATION

Let x, y and z be the 3-dimensions values measured by acceleration sensor. In our scheme, the magnitude v of vector (x, y, z) is used as random source to extract the secure key, i.e., $v = \sqrt{x^2 + y^2 + z^2}$.

Assume that there is a wireless channel (e.g., WiFi or Bluetooth) between Dev_A and Dev_B. In this step, Dev_A informs Dev_B to measure and record the accelerometer data with the wireless channel. After receiving Dev_A's information, Dev_B sends an acknowledgement to Dev_A over the wireless channel between them. Then Dev_A and Dev_B start to record the measurements with a fixed sampling frequency f. We use D_A and D_B to denote the measurements recorded by Dev_A and Dev_B, respectively.

$$D_A = \{N_1^A, N_2^A, \ldots\}, \tag{1}$$
$$D_B = \{N_1^B, N_2^B, \ldots\}, \tag{2}$$

where

$$N_i^{\mathcal{J}} = \{i, v_i^{\mathcal{J}}\}, \quad i \in \mathcal{I},\ \mathcal{J} \in \{A, B\}, \tag{3}$$

$v_i^{\mathcal{J}}$ is the magnitude of 3-dimensions vector of accelerometer of device $Dev_{\mathcal{J}}$ at time slot t_i, and $\mathcal{I}$ is the index set of the measurements. Taking the sampling frequency $f = 100Hz$, Fig. 3 plots the random source (i.e., D_A and D_B) from Dev_A and Dev_B, where the measuring time is 10 seconds. The result shows that the similarity of the random source between Alice and Bob is high.

B. MEASUREMENTS PREPROCESSING

Because of hardware defect of two wireless devices Dev_A and Dev_B and the time delay caused by the operation of software, time asynchrony between these two devices would happen

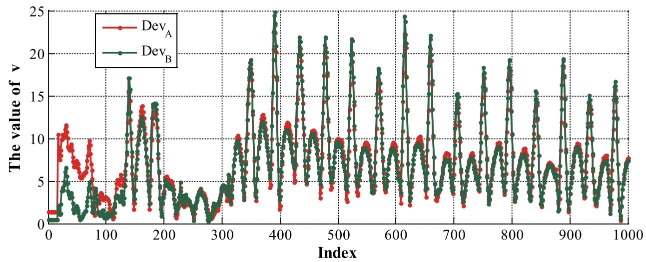


FIGURE 3. Random source at Dev_A and Dev_B.

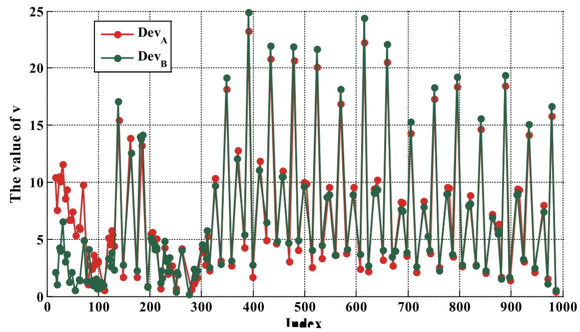


FIGURE 4. Data set at Dev_A and Dev_B after extracting extreme points.

during the random resource collection phase. Note that, time asynchrony would result in a high bit string mismatch rate between Dev_A and Dev_B after bit quantification, which would decrease the probability of success of key distribution. In the proposed scheme, we reselect the first extreme point as the starting point in order to solve the problem of time asynchrony. From Fig. 3, it can be find that the reselected start point at Dev_A is at the original index number 20. Moveover, as shown in Fig. 3, the adjacent measurements of the random source are similar. If all the data in random source D_A and D_B are used in bit quantification step, a long list of 0s and 1s in the bit string would occur frequently, which would decrease the entropy of the generated key. In this scheme, the extreme points (i.e., local minimum and maximum points) are used for bit quantification, in which, local minimum (resp. maximum) point means that it is smaller (resp. bigger) than the backward and forward data.

As shown in Fig. 4, it plots the data set of Dev_A or Dev_B after synchronizing the measurement sequence between them and extracting extreme points. However, the chattering phenomenon of extreme points still exists. If the extreme points are used for bit quantification directly, the bit mismatch rate will be high. In this scheme, a lightweight filtering algorithm is designed to overcome the problem of chattering phenomenon. The main idea of the proposed filtering algorithm is that, if the difference between the maximum and minimum value of w consecutive extreme points is smaller than a threshold δ, then these extreme points will be discarded, where w is the sliding windows.

The Extreme Points Extracting and Filtering Algorithm (EPEFA) is shown in Alg. 1. Note that the time cost of EPEF algorithm is lower than that of data-mining-based algorithm. Hence, this algorithm is lightweight and easy to implement on mobile platform. After the measurements preprocessing step, the data set at Dev_A and Dev_B is denoted by P_A and P_B, respectively, where

Algorithm 1 EPEFA

Input: the random source D at Dev_A or Dev_B; the sliding window, w; and the threshold, δ.
Output: Sequence P; Index set I_P

$P = \emptyset$; $I_P = \emptyset$; $T = \emptyset$; $I = \emptyset$
for $i \in \{1, 2, \cdots, Length(D)\}$ **do**
  if $D(i) > D(i+1)$ and $D(i) > D(i-1)$ **then**
    $T = T \cup \{D(i)\}, I = I \cup \{i\}$
  end if
  if $D(i) < D(i+1)$ and $D(i) < D(i-1)$ **then**
    $T = T \cup \{D(i)\}, I = I \cup \{i\}$
  end if
end for
for $i \in \{1, \cdots, Length(T) - w\}$ **do**
  if $|D(i) - D(i+1)| \geq \delta$ **then**
    $P = P \cup \{D(i), D(i+1)\}$
    $I_P = I_P \cup \{index(D(i)), index(D(i+1))\}$
  else $|D(i) - D(i+1)| < \delta$
    Denote $A = T[i : i+w]$
    Find $v_{min} = \min(A)$, $v_{max} = \max(A)$
    if $v_{max} - v_{min} > \delta$ **then**
      if $index(v_{max}) \notin I_P$ **then**
        $P = P \cup \{v_{max}\}, I_P = I_P \cup index(v_{max})$
      end if
      if $index(v_{min}) \notin I_P$ **then**
        $P = P \cup \{v_{min}\}, I_P = I_P \cup index(v_{min})$
      end if
    end if
  end if
end for
Return P and I_P

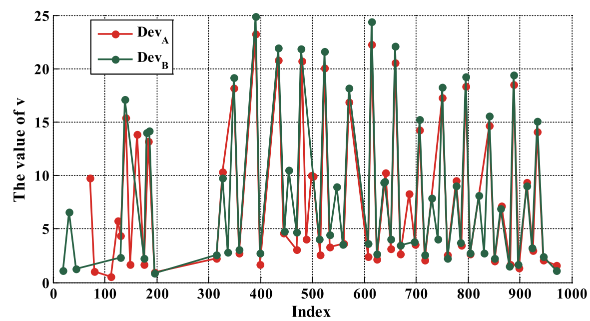


FIGURE 5. Data set at Dev_A and Dev_B after preprocessing.

$$P_A = \{N^A_{i_1}, \ldots, N^A_{i_s}, \ldots\}, \tag{4}$$
$$P_B = \{N^B_{j_1}, \ldots, N^B_{j_s}, \ldots\}, \tag{5}$$

i_s and j_s are the index number. Taking $w = 5$ and $\delta = 10$, Fig. 5 plots P_A and P_B after measurements preprocessing.

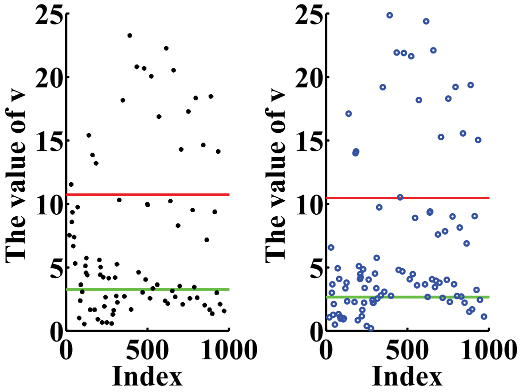


FIGURE 6. Bit Quantification: (a) bit string at Dev_A; (b) bit string at Dev_B.

C. BIT QUANTIFICATION

It is necessary to convert the extreme points P_A and P_B into bit strings, as the secure key is a bit string in general cryptographic protocols. For our system to be lightweight, the single-value quantification [31] algorithm is used in our key distribution scheme. Let PV be the n-dimensional vector, and μ and σ be the mean and the standard deviation of the vector. Denoted two quantization thresholds by q^- and q^+as follows:

$$q^- = \mu - \alpha * \sigma \tag{6}$$
$$q^+ = \mu + \alpha * \sigma \tag{7}$$

in which, α is a system parameter. Specifically, if $P(i) < q^-$, then $P(i)$ is mapped to 0; if $P(i) > q^+$, then $P(i)$ is mapped to 1; otherwise, $P(i)$ is discarded. The bit quantification algorithm is performed by Dev_A and Dev_B independently and locally. After bit quantification, the bit strings at Dev_A and Dev_B are denoted by Q_A and Q_B, respectively, i.e.,

$$Q_A = \{(s_1, a_1), ...(s_t, a_t)...\} \tag{8}$$
$$Q_B = \{(s'_1, b_1), ...(s'_t, b_t)...\} \tag{9}$$

where s_t and s'_t are the index number. Taking the system parameter $\alpha = 0.6$, Fig. 6 illustrates the bit quantization process.

D. INFORMATION RECONCILIATION AND PRIVACY ENLARGEMENT

After bit quantification, it cannot guarantee that the bit strings at Dev_A and Dev_B are exactly the same. An information reconciliation method is proposed to obtain the same bit string between Dev_A and Dev_B. This method includes two steps: index matching and error correction. In the index matching step, Dev_A transmits his valid index set $S_A = \{s_1, s_2, \cdots, s_t, \cdots\}$ to Dev_B And then, Dev_B find his own valid index set by using a lightweight index matching algorithm (as shown in Alg. 2). When Dev_B obtains V_A and V_B with Alg. 2, he transmits V_A to Dev_A. The bit string corresponding to V_A and V_B at Dev_A and Dev_B is denoted by KQ_A and KQ_B, respectively.

Algorithm 2 Indexes Matching Algorithm

Input: Dev_A's index set $Index_A$; Dev_B's index set $Index_B$; and the threshold δ'.
Output: Valid index V_A and V_B

$V_A = \emptyset$; $V_B = \emptyset$
Dev_A transmits S_A to Dev_B
for $i \in Index_A$ **do**
  for $k \in Index_B$ **do**
    $D_k = |k - i|$
  end for
  find $D_m = \min(D)$
  if $D_m < \delta'$ **then**
    $V_A = V_A \cup \{i\}$; $V_B = V_B \cup \{k\}$
  end if
end for
return V_A and V_B

In our system, BCH codes are used for data correction. For example, the code length of BCH (15,5) is 15, the message length is 5, the minimum Hamming distance is 7, and the maximum error correction number is 3. Accordingly, the error correction rate of BCH (15, 5) is less than 20%. Since the decoding algorithm of BCH code can be based on table query. It is applicable in D2D communication platform. The details of error correction are shown as follows: let $BCH[N, k, 2t + 1]$ be the error correcting code used in error correction.

1) Dev_A first generates the random permutation matrix T, and transmits T to Dev_B over a public but insecure wireless channel. Then, Dev_A and Dev_B compute $\mathsf{K_A} = \mathsf{KQ}_A \cdot \mathsf{T}$ and $\mathsf{K_B} = \mathsf{KQ}_B \cdot \mathsf{T}$, respectively.
2) Dev_A and Dev_B divide $\mathsf{K_A}$ and $\mathsf{K_B}$ into several blocks, respectively, where each block has N bits. If the last block is less than N bits, then we set the vacancy positions as 0.
3) For each block K^i_A, Dev_A first picks a codeword C from the codebook $\mathcal{C}$ uniform at random. And then, he computes $\mathsf{K}^i_\mathsf{A} \oplus \mathsf{C}$ and transmits it to Dev_B over the public channel.
4) After receiving $\mathsf{K}^i_\mathsf{A} \oplus \mathsf{C}$, Dev_B computes $\mathsf{C}' = \mathsf{K}^i_\mathsf{A} \oplus \mathsf{C} \oplus \mathsf{K}^i_\mathsf{B}$. Then, he decodes C' to codeword C by BCH decoding algorithm. Finally, Dev_B computes $\mathsf{K}^i_\mathsf{B} \oplus \mathsf{C} \oplus \mathsf{C}'$ to generate K^i_A.
5) Repeat the above 3)-4) steps until all bits are exchanged.

After information reconciliation, Dev_A and Dev_B can obtain the same bit string K_A.

Finally, a hash function is used for privacy amplification, in order to further improve the entropy of the generated key. After privacy amplification, the secure key denoted by $Key_A = Key_B = Hash(K_A)$. In our system, we realize the hash function $Hash(\cdot)$ with $MD5$. When Dev_A and Dev_B obtain the symmetric key, they can use it for transmitting information securely, authenticating message, *etc.*

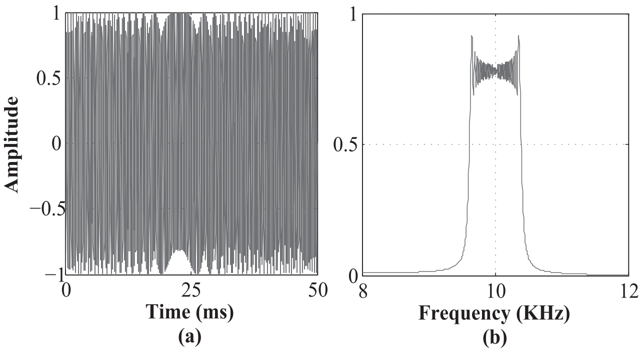


FIGURE 7. Chirp signals over time and frequency domain.

V. NEAR FIELD AUTHENTICATION AND SECURE INFORMATION TRANSMISSION

A. NEAR FIELD AUTHENTICATION

From [32], sound could be used to measure the distance between two devices. In our system, the transmitted time of audio signal is used to determine if those two devices are physically close. Note that, sound wave is a kind of mechanical wave, which has the common properties of mechanical wave, e.g., channel noise, multi-path effect and doppler effect. Liner Frequency Modulation (LFM) was used for sound signal producing. LFM is also named chirp signal, in which, the frequency increases ('up-chirp') or decreases ('down-chirp') linearly over time. Chirp signal is a good solution to overcome channel noise, multi-path effect and doppler effect, which can be easily detected in noisy environment. Moreover, the frequency spectrum of chirp signal is suitable with the speaker and microphone characteristics of mobile phones. Hence, in this work, chirp signal is leveraged as the source of audio signals. The chirp signals can be expressed as follows:

$$f(t) = A \cdot \sin(w_0 t + \frac{\pi F}{T} t^2) \tag{10}$$

where A is the amplitude, w_0 is the central angular frequency, and F is the change rate of angular frequency. Fig. 7 shows the typical chirp signal over time and frequency domain, respectively.

As shown in Fig. 8, the details of the proposed authentication scheme are as follows. Suppose that Dev_A wants to launch a near field authentication with Dev_B, they perform the following steps.

(1) Dev_A sends its request, which includes Dev_A's identification information ID_A and a request information, with an audio data transmission scheme to Dev_B.

(2) After receiving Dev_A's request, Dev_B first generates a chirp signal $f(t)$ and transmits it by air with its speaker, where $t \in (0, T_0]$. Then Dev_A and Dev_B receive and recognize the chirp signal with their microphone, and record the signal arrival time T_{A1} and T_{B1}, respectively.

(3) After receiving and recognizing the chirp signal from Dev_B, Dev_A sends a response chirp signal. Then Dev_A and Dev_B receive and recognize the chirp signal, and record the signal arrival time T_{A2} and T_{B2}, respectively.

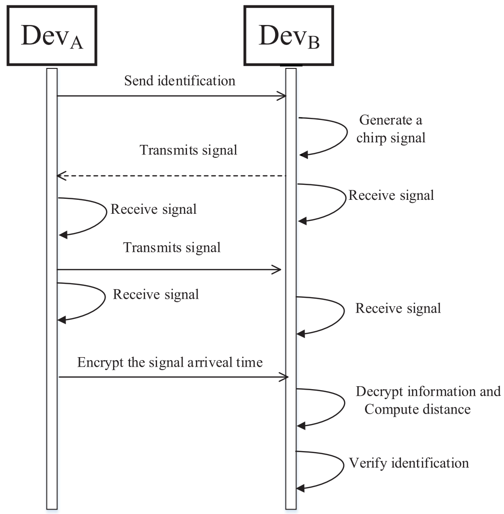


FIGURE 8. The process of authentication scheme.

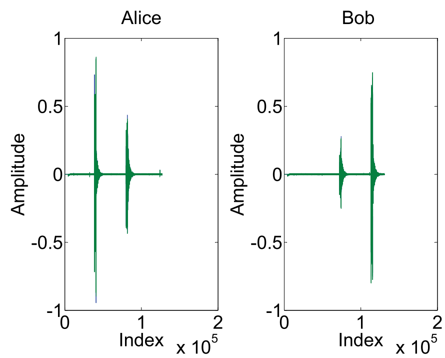


FIGURE 9. The voice recorded by Dev_A and Dev_B.

(4) Dev_A encrypts the arrival times T_{A1}, T_{A2} and the hash value $h_A = Hash(T_{A1}, T_{A2})$ with secret key K to $C_A = E_K(T_{A1}, T_{A2}, h_A)$, and then sends the ciphertext C_A with an the audio data transmission scheme to Dev_B, where $E(\cdot)$ is the encryption algorithm.

(5) Suppose that the received information at Dev_B is C'_A. Dev_B first decodes C'_A with secret key K to T'_{A1}, T'_{A2} and h'_A. Then, Dev_B verifies if $h'_A = h(T'_{A1}, T'_{A2})$:
- If so, it computes $\Delta T = \Delta T'_A - \Delta T_B$, where $\Delta T'_A = T'_{A2} - T'_{A1}$ and $\Delta T_B = T_{B2} - T_{B1}$. Then, Dev_B authenticates if these two devices is physically close by comparing ΔT and a threshold Ω: if $\Delta T < \Omega$, the authentication is successful; otherwise, it fails.
- If not, the authentication fails.

(6) If the authentication is successful, Dev_B sends $C_B = E_K(T'_{A1}, T'_{A2}, T_{B1}, T_{B2}, h_B)$ as a response with an audio data transmission scheme to Dev_A, where $h_B = Hash((T'_{A1}, T'_{A2}, T_{B1}, T_{B2})$. Then, Dev_A can authenticate Dev_B like Step (5).

Fig. 9 plots the recorded chirp signals at Dev_A and Dev_B. Note that, the distance between Dev_A and Dev_B can be

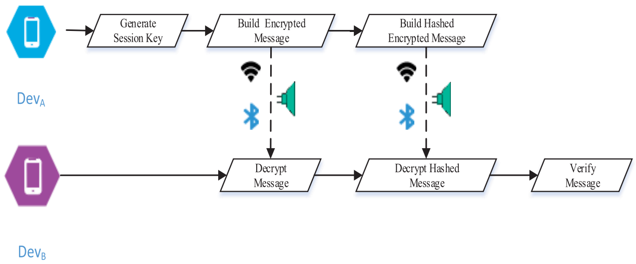


FIGURE 10. The proposed transmission scheme.

expressed by

$$Distance_{AB} = 0.5 \cdot v \cdot [(T_{A1} - T_{B1}) + (T_{B2} - T_{A2})] = 0.5v(\Delta T_A - \Delta T_B) = 0.5v\Delta T \quad (11)$$

where $v = 340m/s$ (i.e., the propagation speed of sound wave in the air). Therefore, the value ΔT can be used to determine if the distance between these two devices is small or not.

In our system, the audio data transmission scheme is realized by dual-tone multifrequency (DTMF) [34], the frequencies of chirp signal are between 8000-12000HZ, the sampling frequency is 44100HZ, and the time lasts 50ms (i.e., $T_0 = 50ms$).

B. SECURE INFORMATION TRANSMISSION

Up to now, Dev_A and Dev_B have the same key K. If Dev_A passes the near field authentication, then it can transmit the secure information to Dev_B. In the proposed transmission scheme, it is assumed that there are two channels, i.e., audio channel and RF channel (WiFi or Bluetooth), between Dev_A and Dev_B. As shown in Fig. 10, the proposed secure information transmission scheme.

(1) Encryption: Dev_A first generates a randomness R as a session key. And then, it sends $C_1 = E_R(M)$ over RF channel (i.e., WiFi, Bluetooth, etc.) and $C_2 = E_K(R, T, Hash(E_R(M))$ over audio channel to Dev_B, where T is the timestamp.

(2) Decryption: After receiving C_1' and C_2', Dev_B decrypts C_2' to R', T' and $Hash'$ with secret key K. If $Hash(C_1', R', T') = Hash'$, Dev_B decrypts C_1' to M' with R'; if not, it rejects the message.

Note that, Confidentiality, *Integrity*, and *Authentication* (i.e., CIA) are the fundamental requirements for secure information transmission. Confidentiality ensures that an unauthorized entity cannot obtain the information, integrity protects the completeness and accuracy of information during transmission, while authentication is used to assure that the source of information is the legitimate transmitter [33].

In the proposed system, we combine confidentiality, integrity, and authentication together. It can provide the confidentiality as (1) the encryption/decryption algorithm is used to protect the message, and (2) only Dev_B can obtain the session key R from C_2 with K (besides Dev_A). It can provide the integrity and authentication due to the fact that the secure key K is used to encrypt hash value $Hash(E_R(M), R, T)$. Actually, if an adversary wants to launch an impersonation attack, he must choose and send C_1' and C_2' (in which, $C_1' \neq C_1$) to Dev_B, such that $(R', T', Hash') = D_K(C_2')$, and $Hash' = Hash(C_1', R', T')$, where $D(\cdot)$ is the decryption algorithm. However, the probability of the event described above is very low. To improve the efficiency of the proposed scheme, in our system, we realize the encryption/decryption algorithm with AES (i.e., Advanced Encryption Standard).

VI. PERFORMANCE EVALUATION

In this section, extensive experiments are conducted to verify the efficiency and security of the proposed system. In the experiments, we select several mobile phones, i.e., HUAWEI MATE8, as wireless devices in D2D communication. HUAWEI MATE8 is equipped with a 3D digital accelerometer with sampling frequency 0-400kHz. Moreover, in information reconciliation step of our key distribution, we choose $BCH(15, 5)$ as the error correcting code.

A. PARAMETER SELECTION

First of all, we consider the effect of the four system parameters (i.e., the sampling frequency, the difference of magnitude δ, the window size w, and the coefficient of quantization α) on the bit agreement rate (i.e., the ratio of the number of match bits to the number of whole bits) in the proposed key distribution scheme. For enlarging the difference of sample data, 10 participants (6 males and 4 females) take part in our experiments, and each participant shakes two devices for ten seconds. Fig. 11 plots the bit agreement rate under different parameters before error correction. The results show that, No matter how the system parameters are chosen, the key agreement rate is larger than 90%. Note that, BCH(15,5) can correct all of the bit errors if the error rate is less than 20%. It means that BCH(15,5) can meet the requirement to correct each bit error for any value of these four system parameters. Hence, in the following part of this section, we take the sampling frequency as 100Hz, $\delta = 1$, $w = 5$, and $\alpha = 0.6$.

Secondly, the effect of the parameter on successful authentication rate in the proposed near field authentication scheme is studied. In our system, it is assumed that the valid distance between Dev_A and Dev_B is 50 cm, i.e., the authentication should be successful with a high probability when the distance between them is less than 50 cm, and the authentication should be failure with a high probability when the distance between them is larger than 50 cm. We measure the performance of the authentication scheme with false positive error (FP error) rate and false negative error (FN error) rate. In our experiment, different distances(i.e., 20cm, 50cm, 80cm, 100cm, 150cm, and 200cm) are chosen to test the performance of the proposed near field authentication scheme. For convenience, the number of sampling points can be used to represent the threshold (i.e., Ω in Section V-A). Actually, $\Omega = NS/FS$, where NS is the number of sampling points and FS is the sampling frequency of acoustic wave in the proposed authentication scheme ($FS = 44.1$KHz in our system). For instance, $\Omega = NS/FS = 80/44100s = 80/44100 \times$

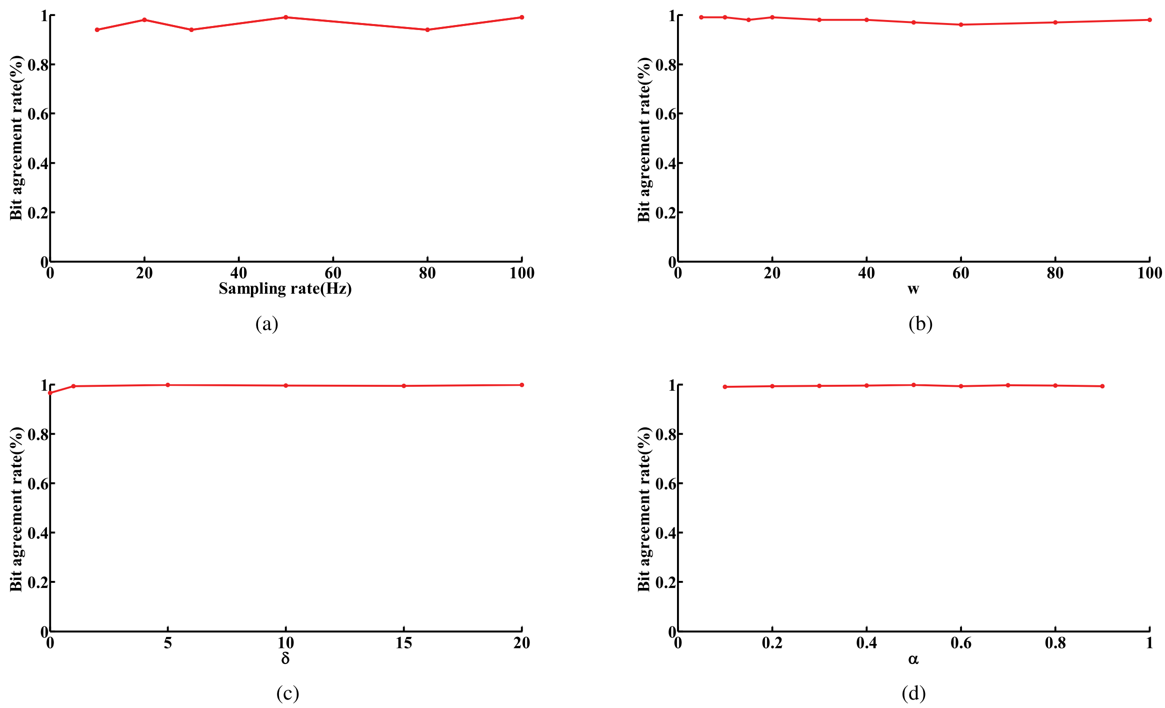


FIGURE 11. Impact of different parameters on the performance of the proposed scheme. (a) Impact of sampling frequency on agreement rate. (b) Impact of w on agreement rate. (c) Impact of δ on agreement rate. (d) Impact of α on agreement rate.

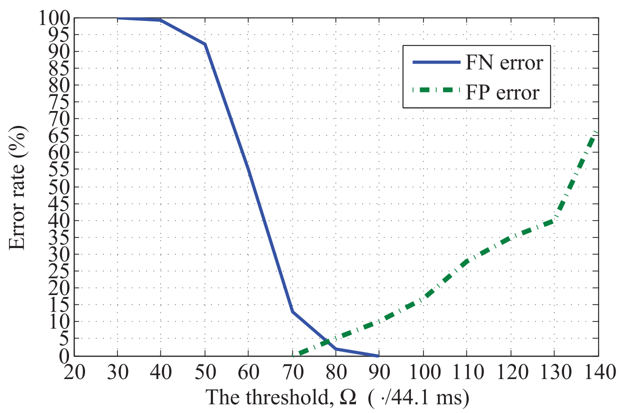


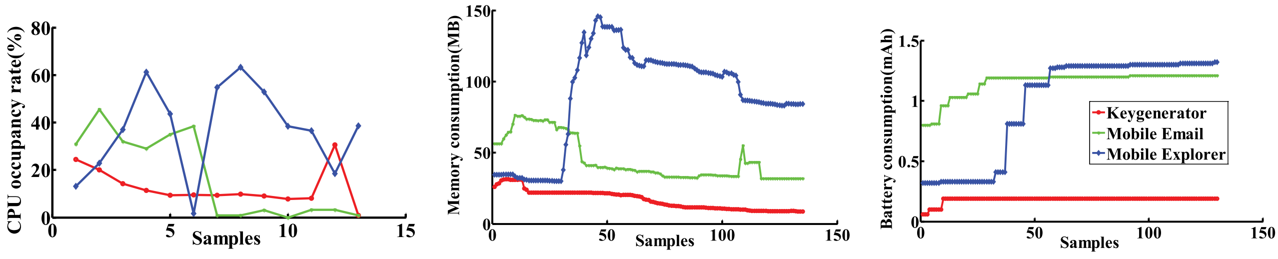
FIGURE 12. The FN and FP error rate under different value of Ω.

$10^3 ms = 1.8ms$ when $NS = 80$. Fig. 12 plots the FP and FN error rate of the proposed near field authentication against the threshold Ω. The result shows that the FN error rate is less than 2% and the FP error rate is less than 5%, when $NS = 80$ (i.e., $\Omega = 1.8ms$). where the FN error rate is less than 2% and the FP error rate is less than 5%. Accordingly, $\Omega = 1.8ms$ in our system.

B. KEY RANDOMNESS

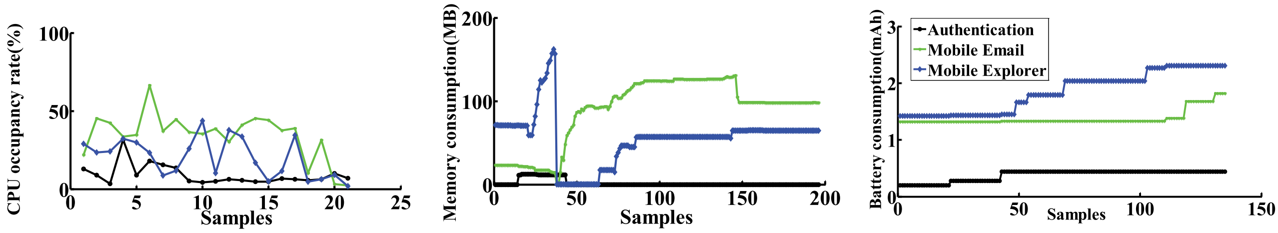
Our system includes key distribution scheme, near field authentication scheme, and secure information transmission scheme. The security of the key generated in the key distribution scheme is the key point of the whole system as the secret key is used in the last two schemes to provide the confidentiality, integrity, and authentication of the (part of) information transmitted between two devices. Our key distribution scheme can be regarded as two phase: (1) the random bit string generation phase, i.e., the first three steps of our scheme; and (2) key agreement phase, i.e., the last steps of our scheme. In the proposed key distribution scheme, there only two information transmitted over the public but insecure channel: one part of Dev_A's index and random codeword used for error correction. Even if the adversary Eve can obtain the above information by eavesdropping the public channel. However, Eve cannot uncover the bit string K_A, which obtained by Dev_A and Dev_B after bit quantification, as (1) he does not know the value with regarding to index set transmitted over public channel and (2) the codeword transmitted over public channel is chosen by Dev_A uniform at random from codebook. Moreover, it can further reduce the entropy loss of the secure key Key_A during public discussion by using privacy amplification.

Since the randomness of a cryptographic key is crucial for the security of a communication system. It is necessary to study the randomness of the generated key in our system. In our experiment, a randomness test of the generated key with NIST, a commonly used statistical testing standards, is conducted Several randomness index (i.e, Frequency,Block Frequency, Cumulative Sums, *etc.*) are used in our test. The p-values of the generated key with our key distribution scheme are given in Table 1, in which, The tested data passes the randomness test if the p-value is more than 0.01. The result shows that the generated key with the proposed scheme pass all the tests.



(a) (b) (c)

FIGURE 13. Performance testing on the proposed key generation scheme. (a) CPU consumption. (b) Memory consumption. (c) Battery consumption.



(a) CPU consumption (b) Memory consumption (c) Battery consumption

FIGURE 14. Performance testing on the proposed near field authentication scheme. (a) CPU consumption. (b) Memory consumption. (c) Battery consumption.

TABLE 1. P-values of NIST statistical test.

Test suite	P-value
Frequency	0.17
Block Frequency	0.72
Cumulative Sums	0.3
Longest Run	0.04
FFT	0.90
Nonoverlapping Template	0.4
Approximate Entropy	0.1
Linear Complexity	0.98

C. ENERGY CONSUMPTION

Due to the fact that most of mobile devices in D2D communication are powered by batteries, and have limited energy, it is necessary to conduct an experiment to evaluate the consumed resources, such as, CPU, memory and battery, of the proposed system. Another two applications, mobile explorer and mobile email, are chosen for comparison. A test tools, named iTest 4.5.0, is used to test resource consumption. Fig. 13 plots the resource consumption of our key generation scheme compared with that of mobile explorer and mobile email. Fig. 14 plots the resource consumption of the proposed near field authentication scheme compared with that of mobile explorer and mobile email. The results show that both the consumption the proposed key generation and near field authentication are less than that of mobile explorer and mobile email. Hence, the proposed schemes in our system have a high efficiency and can be performed well on wireless devices in D2D communication.

VII. CONCLUSION

In this paper, an efficient and lightweight information exchanging system for secure D2D communication has been proposed by using multiple sensors, such as, speaker, microphone and acceleration sensors. This system includes a key distribution scheme by using the acceleration sensor, a near field authentication scheme by leveraging the microphone and speaker, and a message encryption and authentication scheme with two wireless channels. Moreover, an application based on android system and developed by JAVA has been designed to realize the proposed system. Extensive experiments have also been provided by using mobile phones to demonstrate that our system can achieve secure D2D communication with low computing resources and energy consumption. The proposed system can be used for secure communication for many D2D communication scenarios, such as, electronic business card exchange, near-field payment and medical information exchange between doctors and patients.

ACKNOWLEDGMENT

This paper was presented in part at the IEEE MOWNET 2018 [1].

REFERENCES

[1] M. Cao, D. Chen, Z. Yuan, Z. Qin, and C. Lou, "A lightweight key distribution scheme for secure D2D communication," in *Proc. IEEE MOWNET*, Tangier, Morocco, Jun. 2018, pp. 117–124.

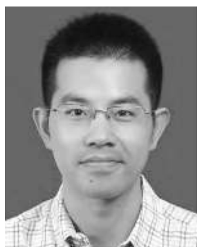
[2] L. Lei, Z. Zhong, C. Lin, and X. Shen, "Operator controlled device-to-device communications in LTE-advanced networks," *IEEE Wireless Commun.*, vol. 19, no. 3, pp. 96–104, Jun. 2012.

[3] C. Castelluccia and P. Mutaf, "Shake them up!: A movement-based pairing protocol for CPU-constrained devices," in *Proc. ACM MobiSys*, New York, NY, USA, Jun. 2005, pp. 51–64.

[4] X. Lan, J. Xu, Z. Zhang, and W. T. Zhu, "Investigating the multi-ciphersuite and backwards-compatibility security of the upcoming TLS 1.3," *IEEE Trans. Depend. Sec. Comput.*, to be published. doi: 10.1109/TDSC.2017.2685382.
[5] D. Chen *et al.*, "An LDPC code based physical layer message authentication scheme with prefect security," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 748–761, Apr. 2018.
[6] D. Chen *et al.*, "Channel precoding based message authentication in wireless networks: Challenges and solutions," *IEEE Netw.*, vol. 33, no. 1, pp. 99–105, Jan. 2019.
[7] G. J. Steiner *et al.*, "*Kerberos*: An authentication service for open network systems," in *Proc. Usenix Winter*, Mar. 1988, pp. 191–202.
[8] C. Neuman *et al.*, "The Kerberos network authentication service (V5)," document RFC-4120, 2005.
[9] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.
[10] Y. Hidir *et al.*, "ShakeMe: Key generation from shared motion," in *Proc. IEEE PICom*, Liverpool, U.K., Oct. 2015, pp. 2130–2133.
[11] B. Liu and C. Chen, "A novel authentication scheme based on acceleration data in WBAN," in *Proc. IEEE/ACM CHASE*, Philadelphia, PA, USA, Jul. 2017, pp. 120–126.
[12] N. Jammali and L. C. Fourati, "PFKA: A physiological feature based key agreement for wireless body area network," in *Proc. IEEE WINCOM*, Marrakech, Morocco, Oct. 2015, pp. 1–8.
[13] E. Zaghouani *et al.*, "ELPA: A new key agreement scheme based on linear prediction of ECG features for WBAN," in *Proc. IEEE Eusipco*, Nice, France, Aug. 2015, pp. 81–85.
[14] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: Body area network authentication exploiting channel characteristics," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1803–1816, Sep. 2013.
[15] W. Xi, J. Han, and K. Zhao, "Instant and robust authentication and key agreement among mobile devices," in *Proc. ACM CCS*, Vienna, Austria, May 2016, pp. 616–627.
[16] L. Shi, J. Yuan, S. Yu, and M. Li, "MASK-BAN: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks," *IEEE Internet Things J.*, vol. 2, no. 1, pp. 52–62, Feb. 2015.
[17] D. Chen, Z. Qin, and X. Mao, "SmokeGrenade: An efficient key generation protocol with artificial interference," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1731–1745, Aug. 2013.
[18] L. Holmquist *et al.*, "Smart-its friends: A technique for users to easily establish connections between smart artefacts," in *Proc. ACM UbiComp*, Atlanta, Georgia, Sep. 2001
[19] R. Mayrhofer and H. Gellersen, "Shake well before use: Authentication based on accelerometer data," in *Proc. IEEE PerCom*, Toronto, ON, Canada, May 2007, pp. 144–161.
[20] M. Chong, G. Marsden, and H. Gellersen, "GesturePIN: Using discrete gestures for associating mobile devices," in *Proc. ACM HCI*, Lisbon, Portugal, Sep. 2010, pp. 261–264.
[21] D. Chen *et al.*, "S2M: A lightweight acoustic fingerprints based wireless device authentication protocol," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 88–100, Feb. 2017.
[22] D. Bichler *et al.*, "Key generation based on acceleration data of shaking processes," in *Proc. ACM UbiComp*, Innsbruck, Austria, Sep. 2007, pp. 304–317.
[23] B. Groza and R. Mayrhofer, "SAPHE: Simple accelerometer based wireless pairing with heuristic trees," in *Proc. ACM MoMM*, Bali, Indonesia, Dec. 2012, pp. 161–168.
[24] 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. ACM/IEEE IPSN*, Vienna, Austria, vol. 3, Apr. 2016, pp. 1–12.
[25] N. Roy and R. Choudhury, "Ripple II: Faster communication through physical vibration," in *Proc. ACM/IEEE NSDI*, Santa Clara, CA, USA, Mar. 2016, pp. 671–684.
[26] R. Mayrhofer and H. Gellersen, "Shake well before use: Intuitive and secure pairing of mobile devices," *IEEE Trans. Mobile Comput.*, vol. 8, no. 6, pp. 792–806, Jun. 2009.
[27] A. Studer, T. Passaro, and L. Bauer, "Don't bump, shake on it: The exploitation of a popular accelerometer-based smart phone exchange and its secure replacement," in *Proc. IEEE ACSAC*, Orlando, FL, USA, Aug. 2011, pp. 333–342.
[28] D.-S. Kim and K.-S. Hong, "Multimodal biometric authentication using teeth image and voice in mobile environment," *IEEE Trans. Consum. Electron.*, vol. 54, no. 4, pp. 1790–1797, Nov. 2008.
[29] L. Zhang *et al.*, "VoiceLive: A phoneme localization based liveness detection for voice authentication on smartphones," in *Proc. ACM CCS*, Vienna, Austria, Oct. 2016, pp. 1080–1091.
[30] P. Xie, J. Feng, Z. Cao, and J. Wang, "GeneWave: Fast authentication and key agreement on commodity mobile devices," *IEEE/ACM Trans. Netw.*, vol. 26, no. 4, pp. 1688–1700, Aug. 2018.
[31] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. ACM CCS*, Alexandria, VA, USA, Oct. 2007, pp. 401–410.
[32] C. Peng, G. Shen, and Y. Zhang, "BeepBeep: A high-accuracy acoustic-based system for ranging and localization using COTS devices," *ACM Trans. Embedded Comput. Syst.*, vol. 11, no. 4, pp. 42–49, Mar. 2012.
[33] D. Chen, N. Zhang, N. Cheng, K. Zhang, Z. Qin, and X. S. Shen, "Physical layer based message authentication with secure channel codes," *IEEE Trans. Depend. Sec. Comput.*, to be published. doi: 10.1109/TDSC.2018.2846258.
[34] T. L. Szabo, "Time domain wave equations for lossy media obeying a frequency power law," *J. Acoust. Soc. Amer.*, vol. 96, no. 1, pp. 491–500, Mar. 1994.

MINGSHENG CAO received the B.Sc. and M.Sc. degrees from the University of Electronic Science and Technology of China, Chengdu, China, in 2008 and 2011, respectively, where he is currently pursuing the Ph.D. degree with the College of Software Engineering. His research interests include network security and pervasive computing.

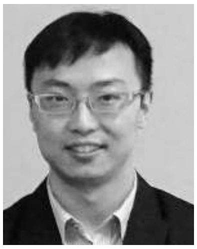
LUHAN WANG is currently pursuing the master's degree with the School of Information and Software Engineering, University of Electronic Science and Technology of China. Her research interests include security and privacy in wireless communication networks (e.g., 5G, the IoT, and vehicular networks) and data mining.



HUA XU received the M.S. degree from Soochow University, China, in 2003, and the Ph.D. degree from the Nanjing University of Posts and Telecommunications, China, in 2007. He was a Visiting Scholar with the BCWS Centre, Carleton University, Canada, from 2010 to 2011. He is currently a Professor with the School of Physics and Electronic Engineering, Yancheng Teachers University, China. His research interests include LDPC codes design, compressed sensing, and magnetic induction communication.

DAJIANG CHEN (M'15) received the B.Sc. degree from Neijiang Normal University, in 2005, the M.Sc. degree from Sichuan University, in 2009, and the Ph.D. degree in information and communication engineering from the University of Electronic Science and Technology of China, in 2014, where he is currently an Assistant Professor with the School of Information and Software Engineering. He was a Postdoctoral Fellow with the University of Waterloo, Waterloo, ON, Canada, from 2015 to 2017. His current research interests include information theory, secure channel coding, and their applications in wireless network security, wireless communications, and other related areas. He serves/served as a Technical Program Committee Member of the IEEE GLOBECOM, the IEEE VTC, the IEEE WPMC, and the IEEE WF-5G.

CHUNWEI LOU received the Ph.D. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2012, where he is currently an Associate Researcher and also the Executive Dean of the Institute of Innovation and Entrepreneurship. His research interests include wireless network security, big data, data mining, and multi-objective decision making.



NING ZHANG (M'15) received the B.Sc. degree from Beijing Jiaotong University, Beijing, China, in 2007, the M.Sc. degree from the Beijing University of Posts and Telecommunications, Beijing, in 2010, and the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada, in 2015. He was a Postdoctoral Fellow with the University of Waterloo and the University of Toronto. He is currently an Assistant Professor with Texas A&M University at Corpus Christi, TX, USA. His current research interests include physical-layer security, dynamic spectrum access, 5G, and vehicular networks.

YIXIN ZHU received the Ph.D. degree from the School of Information and Software Engineering, University of Electronic Science and Technology of China, in 2015. He is currently an Associate Professor with the Xinjiang University of Finance and Economics. His current research interests include information security, applied cryptography, and complex network propagation dynamics.

ZHIGUANG QIN (S'95–A'96–M'14) was the Dean of the School of Software, University of Electronic Science and Technology of China (UESTC). He is currently the Director of the Key Laboratory of New Computer Application Technology and the Director of the UESTC-IBM Technology Center. His research interests include wireless sensor networks, mobile social networks, information security, information management, intelligent traffic, electronic commerce, and distribution and middleware. He served as the General Co-Chair for WASA 2011 and Bigcom 2017.