Journal of Computers Vol. 30 No. 1, 2019, pp. 52-63
doi:10.3966/199115992019023001006

An Improved Secure Data Transmission Protocol Based on D2D for Mobile Health System

Ya-Nan Zhang[1], Hai-Bing Mu[1*]

[1] School of Electronic and Information Engineering, Beijing Jiaotong University,
Haidian District, Beijing, P. R. China
15120186@bjtu.edu.cn, hbmu@bjtu.edu.cn

Received 9 January 2018; Revised 22 January 2018; Accepted 22 January 2018

Abstract. Mobile-Health (M-Health) system is a growing field that enables physicians to monitor remote patients' health status and facilitates the sharing of medical records among medical service providers. Most existing schemes mainly focus on security and privacy. However, these schemes may not work well in M-Health scenarios. For instance, the system may consume lots of time for an intended user equipment (UE) to verify a large number of signatures sequentially. To reduce the computational overhead of intended UE, we propose a batch verification scheme using distributed computing in the improved secure data transmission protocol based on D2D (SDTP). In this paper, when the NM is not available, this case still guarantees normal communication process by applying back-up solution. In addition, if a signature is disputed, the malicious user can be traced by NM or by Shamir's (t,n) secret share scheme from the disputed signature. Besides, we give a specific D2D communication establishment process. Performance analysis and evaluation further prove to be effective for proposed scheme with regard to its privacy, security, availability, computation complexity, and communication cost.

Keywords: availability, D2D communication, ID-based signcryption, Mobile-Health, privacy, security

1 Introduction

The M-Health system is a recent technology innovation, which can make physicians remotely monitor their patients' health and give advice with no need for physical meeting with their patients. In a typical scenario of M-Health system that is shown in Fig. 1, if we send mass data to the healthcare center via cellular networks, the burden of the cellular network will be heavy. Fortunately, spectrum reuse in Device-to-Device (D2D) communications in 5G can improve the data transmission capacity, which works on a licensed band and resulting in a better user experience.

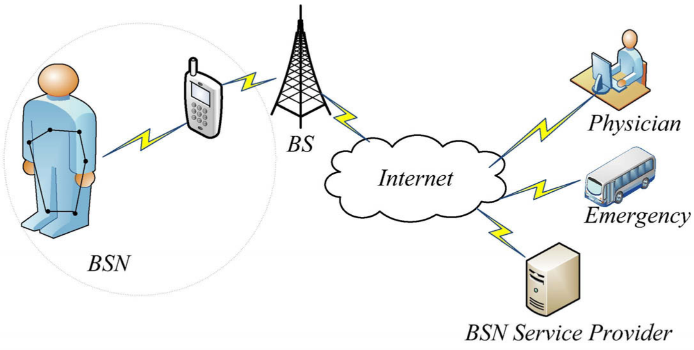

Fig. 1. A typical M-Health system

[*] Corresponding Author

Even though we solve security challenges in D2D communication and open nature of wireless communications [1], such as modification and so on, NM or other client doesn’t reveal the real identity of a malicious user, which leads to the malicious user to occupy available medical resources and patients having real medical need not be treated in time to aggravate life threaten. Besides, Time is crucial when dealing with acute diseases, such as heart disease and stroke. However, before a physician receives multiple personal health information (PHI) at the same time, it needs to get early verification and deals with messages to make rapid diagnosis [2]. When NM suffers some unpredictable situation, such as earthquake, to make it unavailable, it can’t finish the PHI transmission and message verification, even it is impossible to track the controversial recipient. Therefore, how to ensure PHI fast authentication and normal transmission among the patient and his physician is also crucial to system stability and availability.

In this paper, our goal is to tackle the aforementioned security, availability and efficiency problem of the existing schemes. In particular, we will propose an improved secure data transmission protocol based on D2D for Mobile-Health Systems for this purpose. In this proposed scheme, NM plays an important role, which is adopted to trace disputed entity real identity. We also design a back-up mechanism to achieve data normal transmission and reveal the disputed user by shamir’s (t,n) secret share scheme [3] for scene where NM is unavailable. Besides, intended destination can authenticate multiple messages with the help of a verification function at the same time. This way, distributed computing can be used to shed the time-consuming computing loads. Specifically, the design requirements of the proposed SDTP can be summarized as follows.

(1) The scheme should be designed to meet the general security requirements of M-Health system, such as message integrity and authentication, traceability, etc.

(2) The scheme has the property that enables the communication process to continue even in the event that NM gets unavailable in M-Health.

(3) The scheme should be designed to have better performance on computational efficiency and communication overhead.

The remainder of this paper is organized as follows. An overview on the related work is conducted in Section 2. System model and security requirements of the proposed protocol are presented in Section 3. In Section 4, ID-based signcryption scheme is formed and the proposed protocol is described and discussed in detail, followed by security analysis and performance evaluation in Section 5. Finally, Section 6 concludes this paper.

2 Related Work

The advancement of M-health system have made patient monitoring more feasible. Research about healthcare system have been done and brought about the security requirements in application. The paper [4] presents the key challenges in order to develop secure patient-centric monitoring system of M-Health applications. The survey only provides framework or research direction instead of specific security solutions. Liu et al. [5-6] proposed two certificateless remote authentication protocols for WBANs to retain the good aspects of ID-PKC and traditional PKI simultaneously, which solves the key escrow problem by the full private key of the user generated by a semi-trusted KGC and the user himself. A lightweight certificateless anonymous remote protocol [7] has been put forward to secure the extra-body communication, but the issue about how to revoke a illegitimate user from the system has not been addressed in [5-7]. Besides, there are various designs of revocation approaches for the ID-PKC [8-10] and CL-PKC [11-12], adding the revocation functionality on the certificateless remote anonymous authentication turns out to be difficult. Moreover, in view of the huge numbers of users in the large scale WBAN system, the work of KGC on user revocation will become a bottleneck once the overhead on user revocation increased linearly in the number of users. The paper [13] proposes a remote authentication protocol featured with nonreputation, client anonymity, key escrow resistance, and revocability for extra-body communication in the WBANs. However, key management [14] and D2D communication [15] are not mentioned. The paper [16] focuses on authentication strategies with progressive privacy requirements in different interactions among participating entities in M-Health systems while neglecting security during data transmission processes. The paper [17] designs a D2D-assist data transmission protocol for M-Health system, but case that NM is unavailable and batch verification are not considered. These are the facts, greatly inspired us to propose a SDTP based ID-signcryption using BSN, in which we will clearly demonstrate that how easily to achieve all security requirements and efficiency.

3 Models and Goals

3.1 System Model

In this paper, we design an M-Health model composed of four entities, considering entity structure in [17-18]: Network manager (NM), WBAN clients, medical service providers, and gateway (GW) as shown in Fig. 2.

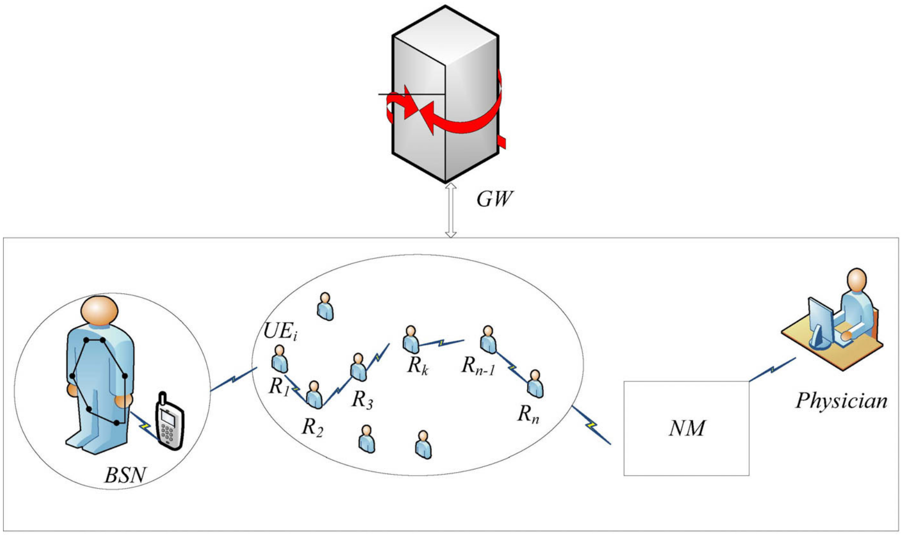

Fig. 2. Model of the M-Health system

NM. The NM is trusted by all entities in the system. It is in charge of distributing the secret keys to all entities, and it has the ability to trace the real identity of a source clients whenever any uncertainty occurs. NM also acts as key generation center (KGC).

WBAN clients. The WBAN client is a medical user equipped with BAN and a mobile terminal device, denoted by UE_i. Clients have two roles, one is source client and the other one is relay. The former is to send PHI and the latter is used to establish a routing to relay message to intended destination. The Relay-Set is denote by $R=(R_1,R_2,...,R_n)$.

Medical service providers. Medical service providers can be acted by the physician and hospital, providing medical services to the clients. They also need to register to the NM after they are selected as the target destination to communicate with client. In our model, we assume that the physician takes the role of medical service providers, denoted by UE_j.

GW. GW serves as the gate from the local subsystem to the core network. In addition to routing Internet Protocol packets from/to the Internet, the GW is able to detect the potential D2D user with the proximity service control function (PSCF). The PSCF earmarks the message flows and looks for pairs of D2D enabled device.

3.2 Security Requirement

In order to provide secure communication for the M-Health systems, we developed an anonymous authentication scheme based on our ID-based signcryption scheme. The proposed authentication scheme achieves the following security requirements [16]:

Message integrity and confidentiality. PHI from a UE_i is authenticated to confirm that it isn't indeed modified, forged and obtained by a malicious adversary.

Mutual authentication. The WBAN client and the physician can authenticate each other to guarantee that the data comes from the claimed source and arrives at the intended destination.

Anonymity and unlinkability. A pseudo identity of source client is employed as a mask, and only NM, UE_{j} know real identity. Besides, the transmissions of any two sessions should not be linked to the same source WBAN clients.

Forward and backward security. If the full private key of the entity in the current session is exposed, the transmission process protected by the time stamp remains secure.

Contextual privacy. When relay knows the source of the data, he doesn't find out the intended destination. Similarly, if relay knows the destination of the data, he doesn't find out where data comes from.

Traceability. NM and other client have the capability to retrieve the real identity of UE_i from a transmitted message when signature is in dispute or when the content of a message is bogus.

4 The Proposed Protocol

4.1 Our Proposed ID-based Signcryption Scheme

The proposed ID-based signcryption scheme is composed by the following steps:

Set up (k). Let F_n be the finite field over a prime order *n*. Let $(a,b) \in F_n$ be the parameters of elliptic curve E over F_n . KGC chooses four one-way hash functions: $H_1 : (0,1)^* \to Z_q$, $H_2 : (0,1)^* \to Z_q$, $H_3 : (0,1)^* \to Z_q$, $H_4 : (0,1)^* \to Z_q$. KGC selects $s \in Z_q$ as the system master private key, and computes its corresponding public key $P_{pub} = sP$ and publishes $\left(P, P_{pub}, q, H_1, H_2, H_3, H_4\right)$ as the system public parameters. Notice that the system public parameters are preloaded into the all entity.

Extract. When a user registers on KGC, this user first sends his identity ID_i to KGC via a secure channel. Upon receiving ID_i from the user, KGC selects $K_i \in Z_q$ and computes $K_i = k_i P$, $S_{ID_i} = k_i + sH_1\left(ID_i, K_i\right)$. After that, KGC sends $\left(K_i, S_{ID_i}\right)$ back to the user via a secure channel.

Signcryption. Define an index function *f(ID)* as follows: *f(ID)* = 0 if $ID = \phi$; otherwise *f (ID)* = 1; Computes $f\left(ID_i\right)$, $f\left(ID_j\right)$; Randomly selects $r_i \in Z_q$, and computes $R_i = r_i P$, $B_i = H_4(m_i, R_i, P_{pub})$, $\sigma = (K_i, R_i, V_i)$, $V_i = f(ID_i)[H_2(K_i, R_i, ID_i, B_i) r_i + S_{ID_i}]$; Computes $U_i = f(ID_i) r_i [K_j + H_1(ID_i, K_j) P_{pub}]$, $m_i^* = H_3(U_i) \oplus m_i$, and sends $\{B_i, m_i^*, \sigma\}$ to UE_j . We denote this algorithm as $\varphi(UE_i, UE_j, m)$.

Verification. Computes $V_i P = f(ID_i)[H_2(K_i, R_i, ID_i, B_i) R_i + K_i + H_1(ID_i, K_i) P_{pub}$; Computes $U_i^* = R_i S_{ID_j}$, $m_i = m_i^* \oplus H_3(U_i^*)$, $B_i^* = H_4(m_i, R_i, P_{pub})$, and checks $B_i^* = B_i$. If the equation holds, the message is accepted.

Correctness of the $U_i^* = R_i S_{ID_j}$ is listed as follows:

$$\begin{aligned} U_i^* &= R_i S_{ID_j} \\ &= R_i (K_j + sH_1(ID_j, K_j)) \\ &= r_i (K_j + H_1(ID_j, K_j) P_{pub}) \\ &= UE_i \end{aligned}$$

4.2 Our Proposed Protocol

The proposed authentication protocol consists of five parts: system setup, user discovery phase, data transmission and communication phase, batch verification phase and trace disputed source client. To protect the stability of the system, we apply a back-up solution to prevent unpredictable things from happening. For clarity of presentation, the notations used throughout this paper are listed in Table 1. Details of each step are described as follows.

Table 1. Notations

Notation	Description
UE_i, UE_{j}	Source client and intended destination
S, P_{pub}	The system master private key and public key
H_1, H_2, H_3, H_4	One-way hash function
RID_i, PID_i	The real identity and pseudonym of UE_i
t_1, t_2, t_3	timestamp
ΔT	A period of time
$T^{'}$	Back-up solution

System setup.

System parameter generation: See set up (k) in the third section.

WBAN clients Register: When UE_i registers to the NM with real identity RID_i by secure channel, NM generates a new pseudonym PID_i by computing $PID_i = RID_i \oplus H_3(sP_{pub})$ and public/private key (K_i, S_{ID_i}) by selecting an integer $k_i \in Z_q$, and computing $K_i = k_i P$, $S_{ID_i} = k_i + H_1(PID_i, K_i) \times s$. Finally, the NM sends the public/private key (K_i, S_{ID_i}) pair to the UE_i through a secure channel.

Physicians Register: UE_j generates public/private key (K_j, S_{ID_i}) in the same way as UE_i.

User discovery phase.

Service Request: UE_i randomly selects an integer $a \in Z_q$, and sends request message along with a, its pseudonym PID_i and the timestamp t_1, namely $(a \| PID_i \| t_1 \| H_4(a \| PID_i \| t_1))$ to the *NM.*

Authentication: Upon receiving the request message, the *NM* first computes hashed value of the message $H_4^*(a \| PID_i \| t_1)$, and verifies $H_4(a \| PID_i \| t_1) = H_4^*(a \| PID_i \| t_1)$. Then, it tries to check whether RID_i is generated. If the RID_i isn't generated by NM, the message is ignored. Otherwise, the NM will forward request message with RID_i to the GW for detecting and finding out the intended physician.

Intended User Detection: The PSCF performs the proximity service detection and searches the potential D2D pairs for the requesting UE_i. Supposing NM chooses UE_j as the intended physician, and then inform UE_i that the intended physician is UE_i, and selects timestamp t_2 as the time they will communication.

Issue back-up solution: In order to avoid the situation that a new system master private key cannot be issued due to unavailability of NM when UE_i knows that UE_j was chosen as the intended destination (e.g., in M-Health based on MANET), the NM can issue one or more back-up solutions, described $T^{'} = (s^{'}, P_{pub}^{'}, PID_i^{'}, K_i^{'}, S_{ID_i}^{'}, PID_j^{'}, K_j^{'}, S_{ID_j}^{'}, t_2^{'})$, where $s^{'}$ is a new system master private key different from *s*; $P_{pub}^{'}$ is its corresponding public key; $(PID_i^{'}, K_i^{'}, S_{ID_i}^{'})$ is a pseudo, private key different from (PID_i, K_i, S_{ID_i}) of UE_i; $(PID_j^{'}, K_j^{'}, S_{ID_j}^{'})$ is a pseudo, private key different from (PID_i, K_i, S_{ID_i}) of UE_j; $t_2^{'}$ is an extension of t_2 for a period of time.

Data transmission and communication phase.

Send Data formulation: This step is performed by UE_i. Suppose that UE_i will send PHI. Then UE_i runs algorithm $\varphi(UE_i, UE_j, m)$ on *m* as follows: Computes $f\left(PID_i\right)$, $f\left(PID_j\right)$; Randomly selects $r_i \in Z_q$, and computes $R_i = r_i P,\ B_i = H_4(m_i, R_i, P_{pub})$; Computes $V_i = f(PID_i)[H_2(K_i, R_i, PID_i, B_i)r_i + S_{ID_i}],\ \sigma = (K_i, R_i, V_i)$; Computes $U_i = f(PID_i)r_i[K_j + H_1(PID_i, K_j)P_{pub}],\ \ m_i^* = H_3(U_i) \oplus m_i$. So, the signcryption of UE_i for UE_j on *m* is presented as $SC = \{B_i, m^*, \sigma\}$.

Moreover, UE_i performs encryption on his identity ID_i. The encryption algorithm $\varphi(\phi, UE_j, UE_i)$ is performed as follows: UE_i randomly picks $r_i \in Z_q$ and computes $R_i = r_i P$, $B_i = H_4(PID_i, R_i, P_{pub})$;

Computes $U_i = r_i[K_j + H_1(PID_i, K_j)P_{pub}]$, $PID_i^* = H_3(U_i) \oplus PID_i$; The encryption of UE_j on ID_i is $E_{UE_j}^{UE_i} = (B_i, PID_i^*, R_i)$, which only be decrypted with its private key.

After, $M = \left(SC \,||\, E_{UE_j}^{UE_i}\right)$ is signed by UE_i, signature Algorithm $\varphi(UE_i, \phi, M)$ as follows: UE_i randomly chooses $r_i \in Z_q$, and computes $R_i = r_i P$, $B_i = H_4(M, R_i, P_{pub})$; Computes $V_i = [H_2(K_i, R_i, PID_i, B_i)r_i + S_{ID_i}]$. The signature of UE_i on *M* is $S_{UE_i} = (K_i, R_i, V_i, B_i)$. UE_i sends the data *M*, his signature, and his identity in the $data = \left(M, PID_i, S_{UE_i}\right)$ to predetermined R_1.

Data transmission: After receiving the data from UE_i by all relays, *NM* verifies the signature S_{UE_i} as follows:

Computes $V_i P$, $H_2(K_i, R_i, PID_i, B_i)R_i + K_i + H_1(PID_i, K_i)P_{pub}$. If both are equal, *NM* accepts the data. Then *NM* sends $SC \,||\, E_{UE_j}^{UE_i}$ to UE_j.

Data receiving: After receiving the data from the NM, UE_j computes $|t_3 - t_2| > \Delta T$. If inequality holds, communication interrupts; otherwise UE_j decrypts $E_{UE_j}^{UE_i}$, where t_3 is the timestamp now, ΔT is the predefined time scale. UE_j decrypts $E_{UE_j}^{UE_i}$ as follows: Computes $U_i^* = R_i S_{ID_j}$, $PID_i = PID_i^* \oplus H_3(U_i^*)$, $B_i^* = H_4(PID_i, R_i, P_{pub})$, if $B_i^* = B_i$ holds, UE_j verifies signcryption as follows: Computes $f(ID_i)$, $f(ID_j)$, checks $V_i P = f(ID_i)[H_2(K_i, R_i, ID_i, B_i)R_i + K_i + H_1(ID_i, K_i)P_{pub}]$; Compute $U_i^* = R_i S_{ID_j}$, $m = m^* \oplus H_3(U_i^* \,||\, t_2)$, $B_i^* = H_4(m_i, R_i, P_{pub})$, checks $B_i^* = B_i$.

Issue Backup communication: When *NM* is unavailable, we can achieve data transmission by selecting registered clients as relay. In Send Data formulation stage, we compute $\varphi(UE_i, UE_j, m)$, $\varphi(\phi, UE_j, UE_i)$, and then forward $data = (PID_i, SC, E_{UE_j}^{UE_i})$ to relay. In destination, we decrypt $E_{UE_j}^{UE_i}$ and verify SC.

Batch verification phase. Upon receiving *n* distinct messages, UE_j can choose batch verification on signature of the signcryption for reducing the computation time. Suppose that n messsages are $MES = \{MES_1, MES_2, \cdots, MES_n\}$, $MES_i = \{B_i, m_i^*, \sigma\}$ $(i = 1, 2, \cdots, n\}$.

$$(\sum_{i=1}^{n} V_i)P = (\sum_{i=1}^{n} H_2(K_i, R_i, ID_i, B_i)R_i) + \sum_{i=1}^{n} K_i + (\sum_{i=1}^{n} H_1(ID_i, K_i))P_{pub} \tag{1}$$

If the equation holds, the UE_j continues to decrypt *m* by performing *n* calculation. Notice that the receiving health-related signatures are generated by *n* distinct users. In order to overcome the attack proposed by Liu et al. [19], we can replace this equation with the following equation by adding the well-known small exponents test [19-21], where $a_i = {}_R\{0,1\}^l$ are randomly chosen for *i=1,...,n*. Usually *l =80* is enough for normal M-Health systems.

$$(\sum_{i=1}^{n} a_i \cdot V_i)P = (\sum_{i=1}^{n} a_i H_2(K_i, R_i, ID_i, B_i)R_i) + \sum_{i=1}^{n} a_i \cdot K_i + (\sum_{i=1}^{n} a_i H_1(ID_i, K_i))P_{pub} \tag{2}$$

When *NM* is unavailable, we also verify signature by this way together. Supposing that *n* messsages are $MES' = \{MES_1', MES_2', \cdots, MES_n'\}$, $MES_i' = \{B_i', m_i^{*'}, \sigma'\}, (i = 1, 2, \cdots, n\}$.

$$\begin{aligned}(\sum_{i=1}^{n} a_i \cdot V_i + a_i \cdot V_i^*)P = (\sum_{i=1}^{n} a_i H_2(K_i, R_i, ID_i, B_i)R_i + a_i H_2(K_i', R_i', ID_i', B_i')R_i' + \sum_{i=1}^{n}(a_i \cdot K_i + a_i \cdot K_i') \\ +(\sum_{i=1}^{n}(a_i H_1(ID_i, K_i) + a_i H_1(ID_i', K_i'))P_{pub}\end{aligned} \tag{3}$$

Trace disputed source client. If equation is not held, the client is considered malicious. So we put forward Binary search method to find the specific user. The algorithm is shown in Table 2.

Table 2. The algorithm to malicious client

```
Alg1(MES)
begin
if BatchVerify (MES) then
        return True
        else if Num (BR)= =1 then
            return PIDi ∈ BR as an invalid request;
else
        set $MES_F = \left(MES_1,...,MES_{\lceil n/2\rceil-1}\right)$
        set $MES_L = \left(MES_{\lceil n/2\rceil+1},...,MES_n\right)$
        $Alg1(MES_F)$
        $Alg1(MES_L)$
    end if
end
```

Then *TA* can traces the disputed client by computing $RID_j = PID_i \oplus H_3(sP_{pub})$, prevents it from registering and participates in the communication processes later and eliminates its pseudonym and timestamp t_2 in UE_i and UE_j.

When *NM* is unavailable, we can recover system master private key s by Shamir's (t,n) secret share scheme and then trace real identity. In system Setup stage, *NM* preselects $x_r = \left(x_1, x_2, ..., x_n\right)$ from F_n to denote each Shareholders $C_r = \left(C_1, C_2, ..., C_n\right)$, $r = \left(1,2,...,n\right)$, where Client C_r has been registered for *NM.* x_r and C_r are open. Select a Lagrange interpolation polynomial $f\left(\mathrm{x}\right) = \sum_{i=1}^{t-1} a_i x^i + s^{'} \bmod n$, where $a_i \in F_n$, $i \in (1,2,...,t-1)$ and s is the secret. Then each shareholder receives a $f\left(x_r\right)$, where $r = \left(1,2,...,n\right)$; With knowledge of at least *t* data points, we can reconstruct the exact polynomial using Lagrange interpolation in F_n and thus reconstruct the secret *s'*, namely $s^{'} = \sum_{i=1}^{t} f\left(x_i \prod_{v=1,v\neq l}^{t} -x_l / x_1 - x_l \bmod n\right)$. *s'* is the system master private key. Then, we compute the real identity by $RID_i = PID_i^{'} \oplus H_3\left(s^{'} P_{pub}^{'}\right)$, reveal it and eliminate it. Finally, we destroy timestamp t_2 in UE_i and UE_j.

5 Performance Evaluation

5.1 Security Analysis

In this section, we show that the proposed scheme can achieve the following security requirements.

Message integrity and confidentiality. Confidentiality of the PHI is guaranteed by $\varphi\left(PID_i, PID_j, m\right)$ and time stamp t_2. Without gaining UE_j the private key, the eavesdroppers cannot decrypt the cipher text. Meanwhile, PHI confidentiality is ensured.

Mutual authentication. Only $UE_j^{'}s$ private key can decrypt the ciphertext $E_{UE_j}^{UE_i}$ and $UE_i^{'}s$ public key can be verify the S_{UE_i}. The WBAN client and the physician can authenticate each other.

Anonymity and unlinkability. In the Service Request phase, the pseudonym of all entity is generated and used in the communication process. So it is clear that anonymity requirement is set to achieve unlinkability. r_1 is different when UE_i sends request every time. So, the scheme can achieve unlinkability by r_1.

Contextual privacy. If $p\left(\mathrm{x}\right) < \theta$ for any communication process, we say our scheme has guaranteed the users contextual privacy request, where x denotes event that all relays collude to link the UE_i or UE_j and denotes the highest privacy leaking probability that the system can accept. Due to trusted NM, all relays don't know intended destination, so contextual privacy is secure. If relay knows the destination, the probability tracing the source client is $p(x) = 1/2^{n+1} - 1$. Get *n=20*, $p(x) = 4.8 \times 10^{-7} \approx 0 < \theta$. In the practical transmission process, n may be far greater than 20 [22]. So the contextual privacy is ensured.

Traceability. NM has the capability to know the real identity of UE_i from a transmitted message by computing $RID_i = PID_i \oplus H_3(sP_{pub})$ when the targeted vehicle disputes its signature associated with the corresponding message. When NM is unavailable, at least *t* clients can recover system master private key by Shamir's (t,n) secret share scheme, and then reveal the real identity.

Table 3 compares the security properties of our SDTP protocol with Hu [13], He-I [24], He-II [24], and Zhang [17] for WBANs. The table demonstrates that only our proposed protocol has the property of Traceability as well as the other properties.

Table 3. Comparison of the security properties with other authentication protocols

Properties	Hu [13]	He-I [23]	He-II [25]	Zhang [17]	SDTP
Data confidentiality	√	√	√	√	√
Data integrity	√	√	√	√	√
Mutual authentication	√	√	√	√	√
Anonymous	√	√	√	√	√
Unlinkability	×	√	√	√	√
Contextual privacy	×	×	×	√	√
Traceability		×	×	×	√

5.2 Computational Overhead

In order to evaluate computation overhead of the proposed scheme, experiments were conducted to compare computation time among our scheme and RSCRA [13], APAAA [23], LRSDDT [16]. Let T_P be the time for performing a pairing operation, T_M be the time for performing a scalar multiplication operation, T_E be the time for performing a exponentiation multiplication operation. On an Intel PXA270 processor at 624 MHz installed on the Linux personal digital assistant, Crypto library MIRACL is used to measure time consumption of these three cryptographic operations, so the running time are T_E = 53.85ms, T_M = 30.67ms, T_P = 96.20ms. In our proposed SDTP protocol, the UE_i needs to conduct signcryption on the message about health, encryption on the identity, and signature on M. All these operations take up 6 T_M computational overhead. In Table 4, we compare the computational overhead at the client and the AP, respectively. As estimated in [13], the running time of the AP, which runs on a PIV-3GHz processor featured with Windows XP OS and 512M bytes memory, are $T_E^{'}$=11.2ms, $T_M^{'}$=6.38ms, $T_P^{'}$=20.01ms, respectively. $T_M^{'}, T_P^{'}, T_E^{'}$.

Table 4. Comparison of computation overhead

Scheme	Sender	AP	AP(n messages)
RSCRA	$11\,T_E + T_P$ =688.55ms	$8\,T_P^{'}$ +$3\,T_E^{'}$ =193.60ms	($8\,T_P^{'}$ +$3\,T_E^{'}$)n=193.68n
APAAA	$3\,T_M$ =92.01ms	$T_M^{'}$ =6.38ms	$n\,T_M^{'}$ =6.38n
LRSDDT	$9\,T_M$ =276.03ms	$6\,T_M^{'}$ =38.28ms	$6n\,T_M^{'}$ 38.28n
SDTP	$6\,T_M$ =184.02ms	$4\,T_M^{'}$ =25.52ms	(2n+2) $T_M^{'}$ =12.76(n+1)

From Fig. 3 and Fig. 4, we can see that the our proposed SDTP scheme has a slightly expensive computational cost than the protocols of APAAA. This happens because our scheme implements encryption operations on the identity and twice signature operations on the data to achieve contextual privacy, which are absent in the protocols of He-I [23]. Notably, compared with RSCRA, LRSDDT, our scheme has lower computation. When compared with latest research results LRDDT, Hence, the computation time for sender is reduced by 2.97/4.5=33% in our scheme. In order to simultaneously verify n distinct signatures signed by *n* distinct signers, our scheme also developed a batch verification process. The batch verification process only needs *2n+2* scalar multiplication operations, reducing *(2n-2)* T_M compared to traditional computation *4n* computation time for intended destination is reduced by *2n-2/4n=0.5-0.5/n* in our scheme. From Fig. 5, it is advantageous to verify multiple signatures simultaneously.

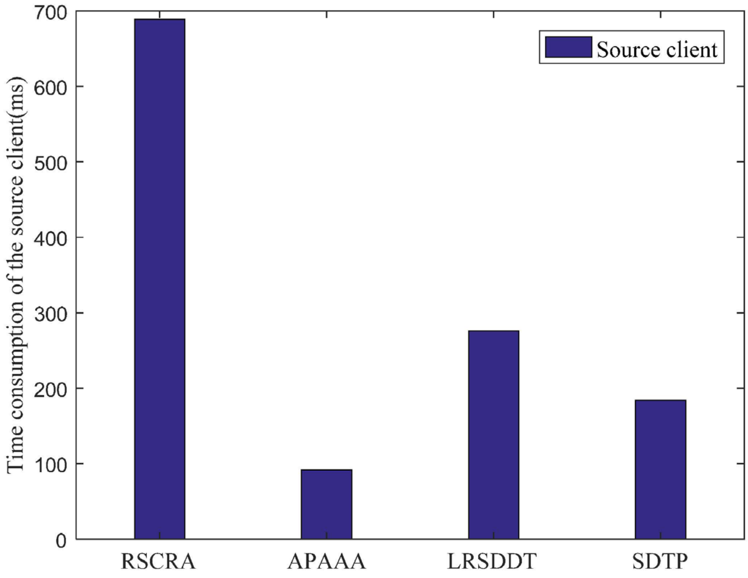

Fig. 3. Time consumption of the source client

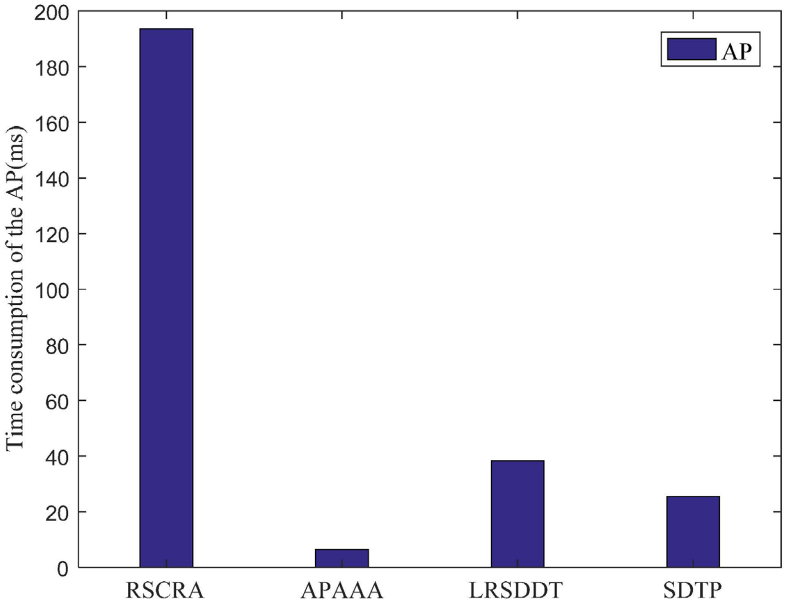

Fig. 4. Time consumption of the AP

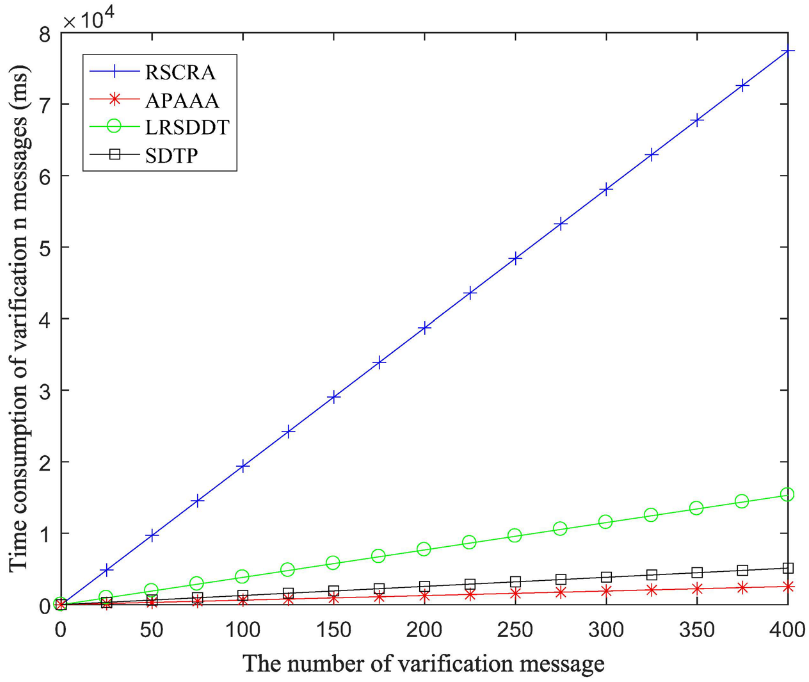

Fig. 5. Time to verification n messages

5.3 Communication Overhead

Transmission message format is listed in Table 5. In SDTP, the communication overhead between the UE and eNB for service request is 44+4=48B, where the first term represents the overhead caused by the requesting message from the UE_i, and the second term represents the communication overhead is 4B in D2D candidate detection process. The message sent by UE_i is (M, ID_i, S_{UE_i}), $M = SC \| E_{UE_j}^{UE_i}$, so the communication overhead is *20*+*L*+*L*+2+20=42+2L. Suppose that the number of the candidate detected by GW is 1. Communication overhead comparisons among SeCD [25], SeDS [17], SDTP are listed in Table 6.

Table 5. Transmission message format

RID_i	PID_i	Encryption	Timestamp	Signature
2Bytes	2Bytes	20Bytes	2Bytes	20Bytes

Table 6. Comparison of communication overhead

Overhead	SeCD	SeDS	SDTP
Communication	480	208	102

5.4 Availability

The proposed scheme takes advantage of the NM to provide a reliable communication mechanism by applying the NM to undertake most computation tasks to release the computation burden of the client and intended destination. Even though the TA is not available, the client and physician can still continue communications for some time using the back-up solution. In addition, the back-up solution can generate different key pairs. So, it is possible to sign different messages with these private keys. Thus, availability is ensured.

6 Conclusion

In this study, an improved secure data transmission protocol based on D2D is proposed for improving the security, availability and efficient of the M-Health. For tracking the signature controversial client, we design strategy to reveal its real identity by NM. To avoid NM unavailable case, our proposed Shamir's (t,n) secret share schemes can recover system master private key to trace the disputed entity. Moreover, we have introduced a back-up solution to keep normal communication and. To reducing intended destination computation overhead at the same time, we implement batch verification scheme. Analysis shows that our proposed authentication scheme is more advantageous than the existing schemes in terms of security, availability, computational and communication overhead. The future development of this work is to devise more efficient signcryption algorithm to further reducing the computation time.

Acknowledgements

This work was supported by National Natural Science Foundation of China (Grant No. 61201159).

References

[1] M. Wang, Y. Zheng, A survey on security in D2D communications, Mobile Networks & Applications 22(2)(2017) 195-208.

[2] X. Lin, R. Lu, X. Shen, Y. Nemoto, N. Kato, Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems, IEEE Journal on Selected Areas in Communications 27(4)(2009) 365-378.

[3] Z. Wang, M. Karpovsky, L. Bu, Design of reliable and secure devices realizing Shamir's secret sharing, IEEE Transactions on Computers 65(8)(2016) 2443-2455.

[4] A. Sawand, S. Djahel, Z. Zhang, F. Nait-Abdesselam, Toward energy-efficient and trustworthy eHealth monitoring system, China Communications 12(1)(2015) 46-65.

[5] J. Liu, Z. Zhang, R. Sun, K.-S. Kwak, An efficient certificateless remote anonymous authentication scheme for wireless body area networks, in: Proc. IEEE International Conference on Communications, 2012.

[6] J. Liu, Z. Zhang, X. Chen, K.-S. Kwark, Certificateless remote anonymous authentication schemes for wireless body area networks, IEEE Transactions on Parallel & Distributed Systems 25(2)(2013) 332-342.

[7] H. Xiong, Cost-effective scalable and anonymous certificateless remote authentication protocol, IEEE Transactions on Information Forensics & Security 9(12)(2014) 2327-2339.

[8] J.-H. Seo, K. Emura, Revocable identity-based encryption revisited: security model and construction, in: Proc. Public Key Cryptography, 2013.

[9] J.-H. Seo, K. Emura, Revocable identity-based cryptosystem revisited: security models and constructions, IEEE Transactions on Information Forensics & Security 9(7)(2014) 1193-1205.

[10] J. Li, X. Chen, C. Jia, W. Lou, Identity-based encryption with outsourced revocation in cloud computing, IEEE Transactions on Computers 64(2)(2015) 425-437.

[11] T.-T. Tsai, Y.-M. Tseng, Revocable certificateless public key encryption, IEEE Systems Journal 9(3)(2015) 824-833.

[12] T.-T. Tsai, Y.-M. Tseng, S.-S. Huang, Efficient revocable certificateless public key encryption with a delegated revocation authority, Security & Communication Networks 8(18)(2016) 3713-3725.

[13] H. Xiong, Z. Qin, Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks, IEEE Transactions on Information Forensics & Security 10(7)(2015) 1442-1455.

[14] M. Li, S. Yu, J.D. Guttman, W. Lou, K. Ren, Secure ad hoc trust initialization and key management in wireless body area

networks, Acm Transactions on Sensor Networks 9(2)(2013) 1-35.

[15] L. Guo, C. Zhang, J. Sun, Y. Fang, a privacy-Preserving attribute-based authentication system for mobile health networks, IEEE Transactions on Mobile Computing 13(9)(2014) 1927-1941.

[16] A. Zhang, L. Wang, X. Ye, X. Lin, Light-weight and robust security-aware D2D-Assist data transmission protocol for mobile-health systems, IEEE Transactions on Information Forensics & Security 12(3)(2017) 662-675.

[17] A. Zhang, J. Chen, R.Q. Hu, Y. Qian, SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks, IEEE Transactions on Vehicular Technology 65(4)(2016) 2659-2672.

[18] R. Lu, X. Lin, X. Shen, SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency, IEEE Transactions on Parallel & Distributed Systems 24(3)(2013) 614-624.

[19] J.K. Liu, T.-H. Yuen, M.-H. Au, W. Susilo, Improvements on an authentication scheme for vehicular sensor networks, Expert Systems with Applications 41(5)(2014) 2559-2564.

[20] J.-H. Cheon, D.-H. Lee, Use of sparse and/or complex exponents in batch verification of exponentiations, IEEE Computer Society 55(12)(2006) 1536-1542.

[21] C. Jan, H. Susan, P. M. Ø, Batch verification of short signatures, in: Proc. International Conference on the Theory and Applications of Cryptographic Techniques, 2007.

[22] N.-U. Amin, Secure MANET Communication Based on Hybrid Cryptosystem: Ad-hoc Networks Security, LAP LAMBERT Academic, 2013.

[23] D. He, S. Zeadally, Authentication protocol for an ambient assisted living system, IEEE Communications Magazine 53(1)(2015) 71-77.

[24] D. He, S. Zeadally, N. Kumar, J.-H. Lee, Anonymous authentication for wireless body area networks with provable security, IEEE Systems Journal 11(4)(2016) 2590-2061.

[25] Y. Hao, J. Tang, Y. Cheng, Secure cooperative data downloading in vehicular ad hoc networks, IEEE Journal on Selected Areas in Communications 31(9)(2013) 523-537.