IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received Date December 1, 2016; accepted December 19, 2016, date of publication December 29, 2016, date of current version January 23, 2017.

Digital Object Identifier 10.1109/ACCESS.2016.2645904

A Secure System For Pervasive Social Network-Based Healthcare

JIE ZHANG[1,2], NIAN XUE[1,2], AND XIN HUANG[1]

[1]Department of Computer Science and Software Engineering, Xi'an Jiaotong-Liverpool University, Suzhou 215123, China
[2]School of Electrical Engineering and Electronics and Computer Science, University of Liverpool, Liverpool L69 3BX, U.K.

Corresponding author: X. Huang (Xin.Huang@xjtlu.edu.cn)

This work was supported by the XJTLU research development fund projects under Grant RDF140243 and Grant RDF150246, in part by the by the Suzhou Science and Technology Development Plan under Grant SYG201516, and in part by the Jiangsu Province National Science Foundation under Grant BK20150376.

ABSTRACT Modern technologies of mobile computing and wireless sensing prompt the concept of pervasive social network (PSN)-based healthcare. To realize the concept, the core problem is how a PSN node can securely share health data with other nodes in the network. In this paper, we propose a secure system for PSN-based healthcare. Two protocols are designed for the system. The first one is an improved version of the IEEE 802.15.6 display authenticated association. It establishes secure links with unbalanced computational requirements for mobile devices and resource-limited sensor nodes. The second protocol uses blockchain technique to share health data among PSN nodes. We realize a protocol suite to study protocol runtime and other factors. In addition, human body channels are proposed for PSN nodes in some use cases. The proposed system illustrates a potential method of using blockchain for PSN-based applications.

INDEX TERMS IEEE 802.15.6, blockchain, e-health, healthcare, human body channels.

I. INTRODUCTION

The rapid development of mobile computing, wireless sensing and communicating technique prompts a new concept of pervasive social network (PSN)-based healthcare [1]. PSN-based healthcare enables users to share data collected by medical sensors. Sharing health data benefits people in many aspects, including personal applications such as remote medical care and public health services like disease monitor and control.

To realize PSN-based healthcare, one essential research question is how to securely share health data among the PSN nodes. This is because health data directly relate to people's life and health; therefore, it is important to protect these data from being modified or stolen. In addition, the network of PSN-based healthcare consists of a large number of mobile nodes; therefore, a mechanism for these nodes easily sharing health data is required.

However, the sensor nodes are less powerful compared with the mobile devices [2]. Advanced cryptographic protocols are acceptable for mobile devices, but may overburden the computationally limited sensor nodes.

Second, there is still no mature scheme that specifies how to use blockchain to share health data in PSN, although blockchain is considered a driven force of future PSN-based healthcare applications. In addition, it is infeasible to store heath data on the blockchain since this will cause heavy load on the PSN nodes.

Bearing these challenges in mind, a PSN-based healthcare system that mainly relies on two security protocols is designed. In our design, the network is divided into two areas, wireless body area network (WBAN) area and PSN area. The WBAN area aims to establish secure links for sensor nodes and mobile devices through *Protocol I authenticated association*, and the PSN area aims to use the blockchain technique to realize health data sharing through *Protocol II adding data to the blockchain*.

Protocol I establishes secure links for sensor nodes and mobile devices in the WBAN area. This protocol is based on IEEE 802.15.6 display authenticated association protocol [3].

Protocol II provides a blockchain-based method for PSN nodes to share heath data in the PSN area. This protocol adds addresses of sensors (generated through Protocol I) and mobile devices to a healthcare blockchain [4], [5]. Through the addresses stored in the blockchain, a PSN node can visit other nodes in the network and access the health data.

The main contributions of this paper are summarized as follows:

- Protocol I, an improved IEEE 802.15.6 display authenticated association protocol, is designed. Using this protocol, nodes are able to agree on a master key as well as their addresses. The protocol is better than that in the standard because it can significantly reduce the computational burden on the resource-limited sensor node.
- Protocol II demonstrates how users can share their health data to other PSN nodes using blockchain techniques. Recently, blockchain is considered as a driven force of future PSN-based healthcare applications; however, how blockchain can be used is still an open question. This protocol gives us an insight into this question.
- A protocol suite is realized for performance evaluation. Protocol running time and some other factors are studied using this suite.
- Human body channels are proposed to cope with some of the major usability problems when display-based out-of-band (OOB) channels are used. Security features of human body channels are discussed with the help of the use case.

II. RELATED WORK

In this section, we review some existing work of PSN-based healthcare and authenticated association protocols for medical sensors.

A. PSN-BASED HEALTHCARE

Current research of PSN-based healthcare mainly focuses on networks, security and privacy, and applications. Authors in [6] and [7] study the network stack of PSN-based e-Health applications. In [8]–[10], body area networks for pervasive healthcare are studied. The security and privacy issues are studied in [11]–[14]. PSN-based healthcare applications are researched in [15]. None of the above papers proposes a feasible scheme for PSN nodes to securely share health data.

B. AUTHENTICATED ASSOCIATION FOR MEDICAL SENSORS

Some authenticated association protocols for medical sensors are proposed in [16]–[18]. Authors in [16] propose a Heart-to-Heart protocol. In [17], the authors use the technique of digital signature and propose a scheme named IMDGuard. Researchers in [18] present a proximity-based access control scheme. All of these schemes have drawbacks. Protocol in [16] does not establish a symmetric key. The IMDGuard scheme in [17] may overburden the medical sensors since digital signature brings heavy computational load. Protocol in [18] may fail due to time-delay caused by poor network condition. In addition, all of these protocols require balanced computation on the sensor and the coordinator.

In addition to the above protocols, the international standard IEEE 802.15.6 [3] also provides several authenticated association protocols for sensors and coordinator in WBANs, including public key hidden association (Std PKH) protocol, password authenticated association (Std PW) protocol, and display authenticated association (Std Dis) protocol. Some of them are vulnerable to attacks. This has been discussed in [19]–[21]. The authors in [19] and [21] also propose improved versions of the Std PW protocol to eliminate attacks.

III. NOTATION AND PRELIMINARIES

In this section we provide notation and preliminaries that are used in our work.

A. NOTATION

We use the following notation to describe security protocols and cryptographic algorithms in this paper:

- S and C are principals. S denotes the computationally limited sensor node, and C denotes the coordinator such as a smart phone installed specific applications.
- M_i denotes the message in the ith communication within a protocol run.
- N_S and N_C are nonce generated by S and C respectively (a nonce is an unpredictable bit string, usually used to achieve freshness).
- R_S and S_C are random integers selected by S and C respectively.
- E is an elliptic curve over finite fields and G is the base point of E.
- $\times$ is the operation of scalar multiplication. In this paper, the two inputs for this operation are an integer and an element of E, and the output is an element of E.
- $\|$ represents the concatenation of bit strings
- SK_S and SK_C are elliptic curve cryptography (ECC) private keys of S and C respectively. The private keys are random integers.
- PK_S and PK_C are ECC public keys of S and C respectively. The public keys are elements of elliptic curve E computed through $PK_S = SK_S \times G$ and $PK_S = SK_S \times G$.
- $Hash = \mathrm{H}(M)$ denotes computing and outputting the hash result $Hash$ for message M through a hash function $H()$.
- $MAC = \mathrm{HMAC}_L(K, M)$ represents outputting the L-bit message authentication code (MAC) MAC for message M through the algorithm of hash-based message authentication code (HMAC) under key K.
- W specifies a witness committed by a 128-bit MAC.
- D specifies a digest that is a 16-bit MAC.
- $Sig = \mathrm{SIG}(SK, M)$ denotes outputting the digital signature Sig for M through the signature algorithm under private key SK.
- $Temp$ denotes a temporary secret computed during a protocol run.
- MK denotes the master key between the communicating parties.
- $address_S$ and $address_C$ represents the address of S and C according to some standard naming systems such as Internet Protocol (IP), Extensible Resource Identifier (XRI) and so on.

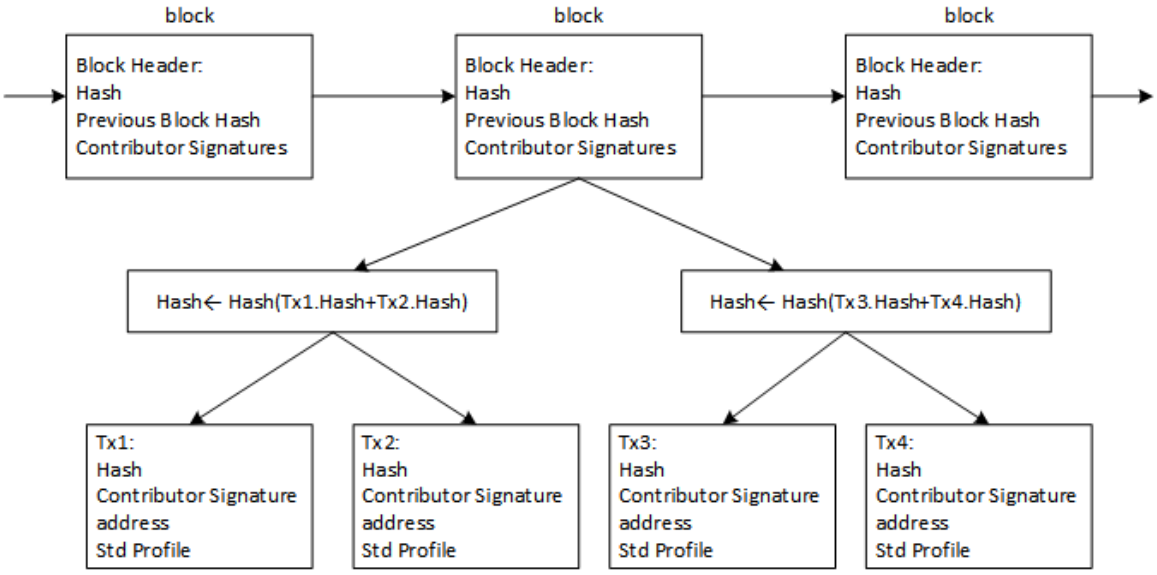


FIGURE 1. Healthcare blockchain. Each block is a Merkle Tree-based structure [24]. Healthcare transactions (e.g. Tx1, Tx2...) are recorded in the leaf nodes. Each transaction contains the address of a PSN node and a digital signature of that node.

- *Std Profile* represents the profile of a standard naming system.

B. HEALTHCARE BLOCKCHAIN

Recently, researchers start to focus on using the blockchain technique to manage health data and medical records [22], [23]. Blockchain is considered as an effective technique for future PSN-based healthcare applications.

In this paper, we propose a method of applying healthcare blockchain in PSN-based healthcare. In our design, we store the healthcare blockchain in some powerful nodes of the PSN-based healthcare system. As shown in Fig. 1, the healthcare blockchain stores and shares network consensus that specifies the addresses, contributors of health data. Authorized PSN nodes can access health data of other nodes through the addresses.

C. IEEE 802.15.6 DISPLAY AUTHENTICATED ASSOCIATION PROTOCOL

In the above mentioned system, nodes authentication and key establishment is the first step. To realize this process, we design an authenticated association protocol. The protocol is based on IEEE 802.15.6 display authenticated association protocol. Here we briefly review the IEEE protocol as follows.

1. S selects a private key SK_S and computes the public key $PK_S = SK_S \times G$. Then S generates a nonce N_S and computes a witness $W_S = \text{CMAC}_{128}(N_S, S\|PK_S)$. S sends the following message M_1 to C.

$$M_1 =< S, PK_S, W_S >$$

2. C selects a private key SK_C and computes the public key $PK_C = SK_C \times G$. Then C generates a nonce N_C and sends S with the following message M_2.

$$M_2 =< C, PK_C, N_C >$$

3. C computes the temporary secret $Temp = SK_C \times PK_S$. Then C computes and sends a MAC $MAC_1 = \text{CMAC}_{64}(Temp, S\|C\|W_S\|N_C)$ to S.

$$M_3 =< MAC_1 >$$

4. S computes $Temp = SK_S \times PK_C$ and verifies MAC_1. If the verification succeeds, S will send C with N_S.

$$M_4 =< N_S >$$

5. S and C compute and compare the following digest D shown on their displays.

$$D = \text{CMAC}_{16}(N_S\|N_C, S\|PK_S\|C\|PK_C)$$

If the two digests equal, S and C go to the next step.

6. S and C compute the master key $MK = \text{CMAC}_{128}(Temp, N_S\|N_C)$

IV. PSN-BASED HEALTHCARE SYSTEM

In this section, we provide an overview of our system. Security goals and challenges are also listed.

A. SYSTEM DESIGN

The PSN-based healthcare system is a system consists of a large number of mobile devices and medical sensors. In this system, PSN nodes can securely share health data in the network. It is divided into two areas, i.e. WBAN area and PSN area as shown in Fig. 2.

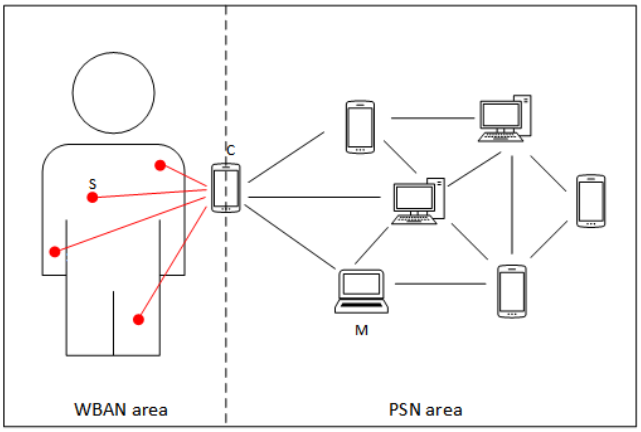


FIGURE 2. Architecture of the PSN-based healthcare system. WBAN area: medical sensors and a coordinator; PSN area: mobile devices.

1) WBAN AREA

medical sensors and a coordinator. Two types of channels are accessible between the medical sensors and coordinator.

- Wireless radio channels: Attackers in these channels can eavesdrop, block and modify messages.
- OOB channels: The OOB channels [25] are established with user's cooperation. These channels can be modeled as non-spoofing-blocking (NSB) channels [26] where attackers find it is difficult to spoof or block messages. For example, in IEEE 802.15.6, displays are used to compare a 5-digit number. This is a display-based NSB channel.

2) PSN AREA

mobile devices such as smart phones, tablets, personal computers and so on. The blockchain technique is used in this area to share network consensus. The network consensus specifies the addresses, contributors and affiliations of health data. The mobile devices can be categorized into two types.

- User nodes: The coordinator of WBAN area works as a user node in the PSN area. It generates and broadcasts healthcare transactions. The healthcare transactions contain addresses of the coordinator and medical sensors.
- Miner nodes: The miner nodes are more powerful than user nodes. They are responsible for healthcare transaction verification and new block generation.

B. SYSTEM PROCEDURE

Phase I Initialization: This phase initializes the secure links between the medical sensor S and the coordinator C. A master key is generated for S and C, and an address is assigned to S.

Phase II Adding Data to The Blockchain: In this phase, the coordinator broadcasts transactions in PSN area. The transaction contains addresses of C and S. Then the transaction will be verified by miner nodes and recorded in a new block.

C. SECURITY GOALS

The security goals of our system are specified as follows.

Phase I:

- Authentication of communicating parties and messages.
- Confidentiality of secret keys.
- Forward secrecy of master key.

Phase II:

- Authentication. The transaction added in the new block is the original one generated by the coordinator.
- Integrity. The transaction added in the new block has not been modified during transmission.

D. CHALLENGES

First, sensors are computationally limited devices. Besides, many sensors touch the skin of users and some even are implanted in the body. Temperature rising caused by executing heavy-load computations may hurt users.

Second, there is no mature scheme that specifies how to use the blockchain for PSN nodes to share health data. In addition, it is infeasible to store health data in the blockchain since it may bring heavy storage load to PSN nodes.

V. CORE PROTOCOLS

In the proposed system, two protocols are essential. They are introduced below.

A. PROTOCOL I: AUTHENTICATED ASSOCIATION

1) PROTOCOL DESCRIPTION

Protocol I realizes the initialization phase of our system. This protocol uses NSB channels to transmit short MAC messages. The protocol is described as follows.

1. S generates a random number R_S and computes U_S.

$$U_S = R_S + SK_S$$

Then S generates a nonce N_S and computes a commitment W_S.

$$W_S = \mathrm{HMAC}_{128}(N_S, S \| PK_S \| U_S)$$

S sends message M_1 including its identity S, the public key PK_S, U_S and the witness W_S over wireless radio channels.

$$M_1 =< S, PK_S, U_S, W_S >$$

2. After receiving M_1, C selects a random number R_C and computes U_C:

$$U_C = R_C + SK_C$$

C then computes T_C:

$$T_C = U_C \times G = (R_C + SK_C) \times G$$

C generates a nonce N_C and assigns an address $address_S$ for S. Then C sends message M_2 to S over wireless radio channels.

$$M_2 =< C, PK_C, N_C, T_C, address_C, address_S >$$

3. S sends out message M_3 including N_S over wireless radio channels.

$$M_3 =< N_S >$$

C verifies the commitment W_S. If the verification succeeds, it goes to step 4; otherwise, it sends a failure message to S via NSB channels.

4. S and C compute and compare the following D via NSB channels:

$$D = \text{HMAC}_{16}(N_S \oplus N_C, S\|PK_S\|U_S\|C\|PK_C \|T_C\|address_C\|address_S)$$

If the verification fails, both sides will stop running the protocol; otherwise, S and C will compute the temporary secret $Temp$ and the master key MK as follows.

$$Temp = G \times R_S \times R_C$$
$$MK = \text{HMAC}_{128}(Temp, N_S\|N_C)$$

The algorithms for S and C to compute $Temp$ are described in Algorithm 1 and 2.

Algorithm 1 S Calculates $Temp = G \times R_S \times R_C$

Input: The elliptic curve E
Input: The received data T_C, PK_C
Input: The secret random value R_S
$mid1 \leftarrow \text{ECCNegative}(PK_C, E)$
$mid2 \leftarrow \text{ECCAdd}(T_C, mid1, E)$
$Temp \leftarrow \text{ECCScalarMultiplication}(mid2, R_S, E)$

Algorithm 2 C Calculates $Temp = G \times R_S \times R_C$

Input: The elliptic curve E and the base point G
Input: The received data U_S, PK_S
Input: The secret random value R_C
$mid1 \leftarrow \text{ECCNegative}(PK_C, E)$
$mid2 \leftarrow \text{ECCScalarMultiplication}(G, U_S, E)$
$mid3 \leftarrow \text{ECCAdd}(mid2, mid1, E)$
$Temp \leftarrow \text{ECCScalarMultiplication}(mid3, R_C, E)$

2) ADVANTAGES

This protocol overcomes the first challenge in Section IV-D through **reducing computational load on the sensor**. That is, *the coordinator carries out the scalar multiplication using U_C on behalf of the sensor*. The sensor involves only one scalar multiplication.

B. PROTOCOL II: ADDING DATA TO THE BLOCKCHAIN

1) PROTOCOL DESCRIPTION

Protocol II realizes the second phases of our system. As shown in Fig. 3, in this protocol, the coordinator C works as a user node of PSN area and broadcasts a transaction to the neighbor nodes. The protocol is described as follows.

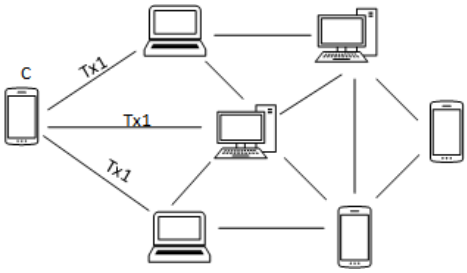


FIGURE 3. *C* broadcasts Tx_1 in the PSN area. Smart phones forward Tx_1 to their neighbors. Laptops and personal computers verify Tx_1.

1. C broadcasts a transaction Tx_1 to the neighbor nodes. As shown in Fig. 4, the transaction includes the addresses of C and S, the profile of the standard naming system, the digital signature and a hash.

$$Tx_1 = < Hash, Sig_T, address_C, address_S, Std\ Profile >$$

where

$$Sig_T = \text{SIG}(SK_C, address_C\|address_S \|Std\ Profile)$$

and

$$Hash = \text{H}(Sig_T\|address_C\|address_S\|Std\ Profile)$$

2. After receiving Tx_1, the miner node verifies Sig_T. If the verification succeeds, the miner node will reply C with a success message.

2) ADVANTAGES

This protocol illustrates a method of using the blockchain technique for PSN nodes to share health data and overcomes the second challenge in Section IV-D. **The data involved in the blockchain are addresses rather than health data.** It is feasible for PSN nodes to store a healthcare blockchain of addresses.

VI. SECURITY ANALYSIS

We prove the security of our protocols through the following theorems. Each theorem corresponds to one security goal in Section IV-C.

A. SECURITY PROOFS FOR PROTOCOL I

Theorem 1: Suppose adversaries can intercept and modify messages transmitted in wireless radio channels, and cannot block or spoof messages in NSB channels, such adversaries are unable to impersonate the sensor or the coordinator without being detected in Protocol I.

Proof: Assume A_S is an attacker who attempts to impersonate the sensor and establish a session key with the coordinator. A_S attacks Protocol I as follows:

1. A_S generates a random number R_A and a nonce N_A and sends C with M_{1A}

$$M_{1A} =< S, PK_S, U_A, W_A >$$

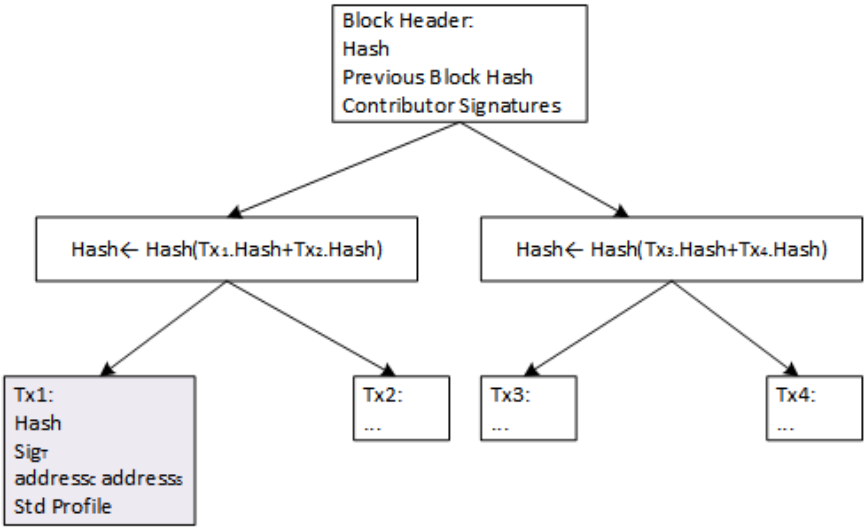


FIGURE 4. A block with a transaction Tx_1. After a verification process, the block will be added to the blockchain.

where

$$U_A = R_A + SK_A$$

and

$$W_A = \text{HMAC}_{128}(N_A, S \| PK_S \| U_A).$$

2. After receiving M_{1A}, C replies A_S with M_2 as follows

$$M_2 =< C, PK_C, N_C, T_C >$$

3. A_S sends C with $M_{3A} =< N_A >$. C verifies W_A and goes to step 4.

In step 4, A_S needs to compare a 16-bit D with C through NSB channels. The comparison fails. As specified in Protocol I, C stops running the protocol.

Similarly, A_C who impersonates the coordinator is unable to establish the master key with the sensor through Protocol I. This attack will be detected in step 4. □

According to Theorem 1, at the end of a completed run of Protocol I, both the sensor and the coordinator can confirm the received messages are from the legal source and the sent messages are received by the legal communicating parties. This means Protocol I achieves the first security goal of Phase I, i.e. authentication of communicating parties and messages.

Theorem 2: Suppose adversaries can intercept and modify messages transmitted in wireless radio channels, and cannot block or spoof messages in NSB channels, such adversaries are unable to acquire information about secret keys in Protocol I.

Proof: Secret keys in Protocol I include the new generated master key MK and the private keys SK_S and SK_C. Assume A is an adversary who can eavesdrop all the messages transmitted between S and C through wireless channels. A records the following values in the current run of Protocol I

$$\{S, C, PK_S, PK_C, N_S, N_C, U_S, T_C\}.$$

Based on the above knowledge, A attempts to derive $MK = \text{HMAC}_{128}(G \times R_S \times R_C, N_S \| N_C)$.

However, without R_S and R_C, A is unable to compute $G \times R_S \times R_C$. The value of $G \times R_S \times R_C$ can be acquired from the following three ways:

- Input R_S and R_C and calculate $G \times R_S \times R_C$.
- Input U_S, PK_S and R_C and calculate $(G \times U_S - PK_S) \times R_C$
- Input T_C, PK_C and R_S and calculate $(T_C - PK_C) \times R_S$

All of the above three methods require A to input either R_C or R_S.

Therefore, the only way for A to acquire K is guessing. The probability for A to guess the correct K is $\frac{1}{2^{128}}$ which is negligible during the life cycle of key.

Besides, A also attempts to derive the private keys SK_S and SK_C. Since SK_S is encrypted using R_S and PK_C is encrypted using R_C during transmission, and R_S and R_C are random secret values, A is unable to decrypt the private keys.

From the above analysis we can see that the adversary is unable to acquire information about the secret keys. □

According to Theorem 2, Protocol I provides confidentiality of secret keys which is the second security goal of Phase I.

Theorem 3: Suppose adversaries can intercept and modify messages transmitted in wireless radio channels, and cannot block or spoof messages in NSB channels. Adversaries who compromise the long-term secret values are unable to compromise keys established in previous runs of Protocol I.

Proof: The long-term secret values in Protocol I are private keys SK_S and SK_C. Assume A compromises these values.

A can also get the public values S, C, PK_S, PK_C, N_S, N_C, U_S and T_C.

In order to compute the master key $MK = \text{HMAC}_{128}(G \times R_S \times R_C, N_S \| N_C)$, A has N_S and N_C and only needs to derive $G \times R_S \times R_C$ from the acquired knowledge.

As in Theorem 2, to acquire $G \times R_S \times R_C$, A should have either R_S or R_C. However, R_C and R_S are random values generated in each run of the protocols. Therefore, A is unable to compute the value of $G \times R_S \times R_C$. Thus, A cannot derive MK. □

According to Theorem 3, Protocol I provides forward secrecy of master key, which corresponds to the last security goal of Phase I.

B. SECURITY PROOFS FOR PROTOCOL II

Theorem 4: Suppose the miner nodes in the PSN area have the public key of the coordinator, it is difficult for adversaries to impersonate the coordinator in Protocol II.

Proof: In order to generate a transaction Tx on behalf of C, the adversary A needs to compute a digital signature:

$$Sig_T = \text{SIG}(SK_C, addresses||Std\ Profile)$$

The miner nodes will check the validity of the transaction by verifying the signature. The private key of C is only held by C. Therefore, the adversary is unable to generate a legal transaction on behalf of C. □

According to Theorem 4, Protocol II achieves authentication of communicating parties and messages, which is the first security goal of Phase II.

Theorem 5: Suppose the miner nodes in the PSN area have the public key of the coordinator, it is difficult for adversaries to modify transaction generated by the coordinator in Protocol II without being detected.

Proof: As in Theorem 4, the transaction of the coordinator involves $address_C$, $address_S$, *Std Profile*, a signature Sig_T and a hash *Hash*.

If any of $address_C$, $address_S$ and *Std Profile* is modified, the verification of the signature will fail.

If *Hash* is modified, the miner nodes can identify and recover *Hash* by inputting $address_C$, $address_S$, *Std Profile*, Sig_T and executing the hash algorithm.

Overall, any change in the transaction will be detected by miner nodes. □

According to Theorem 5, Protocol II provides integrity, which corresponds to the second security goal of Phase II.

C. FORMAL VERIFICATION

In addition to theoretical proofs, we use formal verification to verify the authenticity of Protocol I. Firstly we re-write Protocol I as follows.

1. $S \longrightarrow C : S, msg_{SC}, W_S$
2. $C \longrightarrow S : C, msg_{CS}, N_C$
3. $S \longrightarrow C : N_S$
4. $C \Longrightarrow S : \text{HMAC}_{16}(N_S \oplus N_C, S \| msg_{SC} \| C \| msg_{CS})$
5. $S \Longrightarrow C : Yes/No$

Here, $\Longrightarrow$ is modeled as NSB channels, and $\longrightarrow$ is modeled using Dolev-Yao model [27]. Authenticity of the protocol is formally verified using Casper/FDR [28]. The objective of verification is that both

$$msg_{SC} = \{PK_S, U_S\}$$

and

$$msg_{CS} = \{PK_C, T_C, address_C, address_S\}$$

have not been maliciously modified. This can guarantee the authenticity of the protocol. If the authenticity can be guaranteed, it is easy to see that the secrecy of MK can be guaranteed based on the security analysis in the last subsection.

The verification results are shown in Fig. 5. No attacks were found.

```
User(id,ns) = Send(id,ns) [] Resp(id,ns)

Send(id,ns) = (ns!=<>) &
                [] a:diff(agents,{id}), n:nonces, m:sessmess @

                comm.id.a.Sq.<mess(id,a),hash(head(ns))> ->
                (
                comm.a.id.Sq.<m,n> ->
                comm.id.a.head(ns) ->
                commE.id.a.digest(xor(head(ns),n),mess(id,a)) ->
     User(id,tail(ns)))


Resp(id,ns) = (ns != <>) &
              ([] a:diff(agents,{id}) @
                  ([] m:sessmess, n:nonces @
                  comm.a.id.Sq.<m,hash(n)> ->
                  comm.id.a.Sq.<mess(id,a),head(ns)> ->
                  comm.a.id.n ->
                  commE.a.id?w:message4 ->
                  testeq.w.digest(xor(n,head(ns)),m) ->
                  if ok(id,a,m) then
                  User(id,tail(ns)) else ERROR))
```

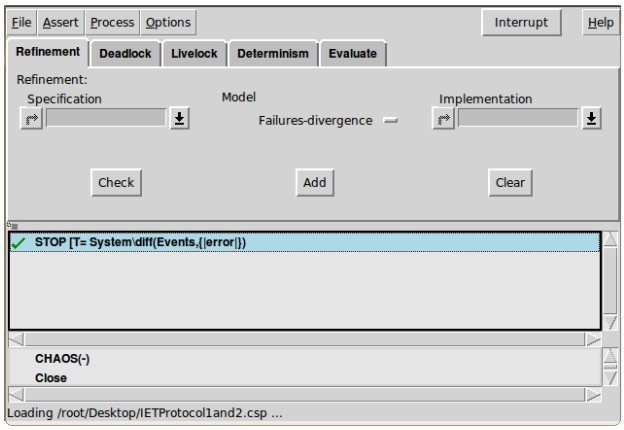


FIGURE 5. Authenticity of Protocol I. No attacks were found.

We have not formally verified the other two security goals of Protocol I and Protocol II, because the analysis is quite straightforward.

VII. PROTOCOL SUITE AND PERFORMANCE EVALUATION

In this section, we realize a protocol suite to evaluate the performance of the proposed system. A set of experiments are carried out. In addition, we compare the overall burden with related works.

A. PROTOCOL SUITE

The protocol suite realizes the core protocols. HMAC is realized using Secure Hash Algorithm (SHA) 512. Elliptic

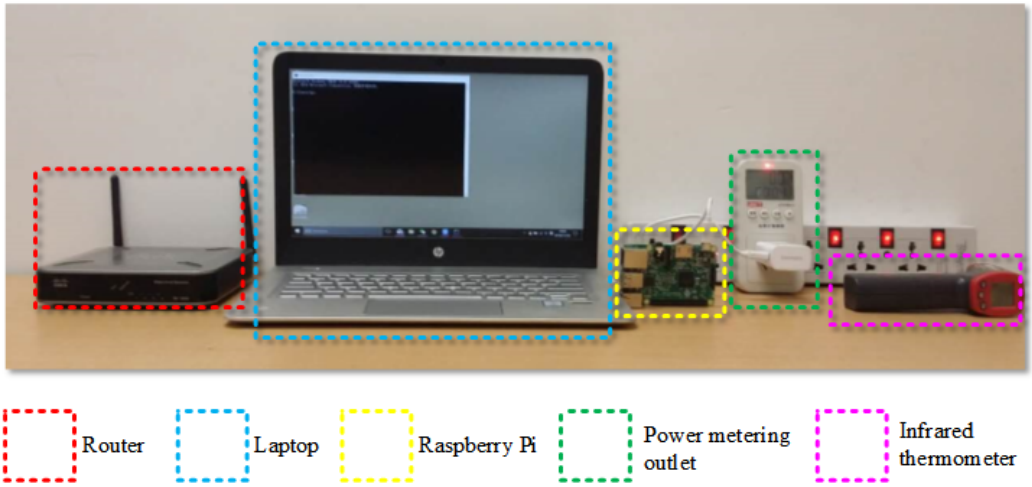


FIGURE 6. Experiment environment.

TABLE 1. Details about the experimental devices.

Protocols	Experiments	Details
Sensor	Raspberry Pi	CPU: 1.2GMHz ARM v8, Memory: 1G
Coordinator	Laptop	CPU: 2.60GHz(i5-3230M), Memory: 8G, Hard Disk: 500G
\	power metering outlet	Type: UNI-T UT230A-II, Function: metering power
\	infrared thermometer	Type: UNI-T UT300A, Function: metering temperature

Curve Digital Signature Algorithm (ECDSA) is used to realize digital signature. The elliptic curves are Federal Information Processing Standards (FIPS) approved standard curves, i.e. Curve P-192, P-256, P-384 and P-521. The NSB channel is established using displays. That is the experimenter compares the digits shown on two displays.

B. EXPERIMENTS

To test the performance of the proposed system, we do a set of experiments using the protocol suite. The sensor is deployed on a Raspberry Pi and the coordinator is realized on a laptop. Obviously, the laptop is more powerful than the Raspberry Pi. Experiment environment is shown in Fig. 6. More details are listed in Table 1.

1) EXPERIMENT I

If Protocol I has unbalanced computational requirements?

We run Phase I of the protocol suite with each curve for ten times. The average runtime are shown in Table 2 and Fig. 7. We can see that the computational load on Raspberry Pi is lower than that on the laptop.

TABLE 2. Average runtime (in second) of protocol/algorithm for different curves.

Curve	Protocol I on S	Protocol I on C	ECDSA on C
P-192	0.057188	0.054845	0.003457
P-256	0.087148	0.094569	0.003384
P-384	0.157747	0.218153	0.003398
P-521	0.264521	0.431773	0.003385

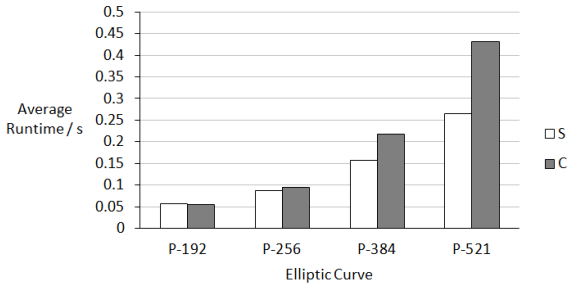


FIGURE 7. Average runtime of Protocol I on FIPS recommended elliptic curves. Protocol I requires unbalanced computational load on S and C. In curve P-521, the runtime on the Raspberry Pi is nearly half of that on the laptop.

Additionally, to observe the reduced runtime on S more clearly, we use the following formula to quantitatively express the reduced runtime:

$$RT_S = \frac{T_S - T_C}{T_S}$$

where RT_S denotes the reducing rate of runtime on S; T_S and T_C denote the average runtime on S and C respectively. The results are shown in Fig. 8.

In most cases, the runtime of S is shorter than that of C. *Given the laptop is much powerful than the Raspberry Pi, Protocol I significantly reduces burden on S.*

The sizes of compiled file are 5.36 K and 5.89 K on the Raspberry Pi and the laptop respectively. *It requires less space on S.*

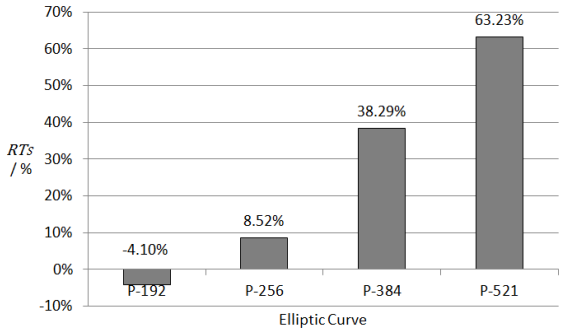


FIGURE 8. Reduced runtime of Protocol I on S. It is expressed by $RT_S = (T_S - T_C)/T_S$.

2) EXPERIMENT II

If the additional burden caused by Protocol II is acceptable for a PSN nodes?

We test the time for the PSN node (i.e. laptop used in Experiment I) to generate a digital signature for Tx_1 (10 times). We also use the four curves. The average runtime is shown in Table 1 and Fig. 9.

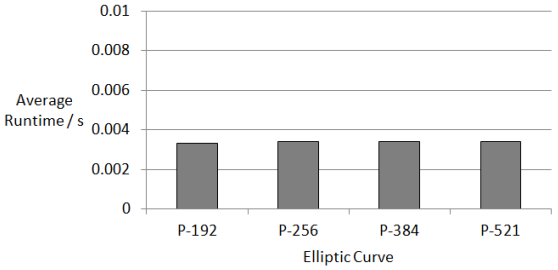


FIGURE 9. Average runtime of ECDSA on FIPS recommended elliptic curves. The time used to run ECDSA is around 0.003 seconds.

According to Fig. 9, the average runtime is around 0.003 seconds for all of the four curves.

3) EXPERIMENT III

If Protocol I reduces lifetime of a sensor? If running Protocol I burns users skin?

We meter the power and temperature on the Raspberry Pi. Before running Protocol I, the power is 16 W and the temperature is 33 °C. The increasing rates are computed and illustrated in Fig. 10.

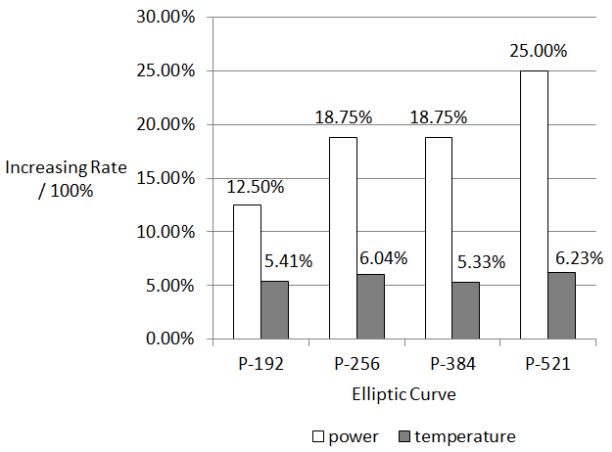


FIGURE 10. Increasing rates of power and temperature of running Protocol I on Raspberry Pi.

The results show that power and temperature increased by executing the protocol are not high. According to Fig. 10, increasing rate of the power is no more than 25%, and that of the temperature is no more than 6.23%. Given the runtime is very short (less than 0.3 seconds), it will not reduce lifetime of sensor. It will also not burn users' skin.

C. COMPARISON

We evaluate the overall burden of the protocols from two aspects: communication cost and computation cost on each side (S, C and the miner node M). To estimate communication cost, we count the number of messages transmitted between communicating parties. For the computation cost, we count the number of scalar multiplication, CMAC algorithm, hash function, signature generation, and signature verification (since other operations such as addition and subtraction require minor computation cost).

Denote a piece of message by $\mathcal{M}$, the operation of scalar multiplication by $\mathcal{S}$, the algorithm of hash function by $\mathcal{H}$, the algorithm of signature generation and verification by $\mathcal{SI}$ and $\mathcal{VE}$ respectively, and the algorithm of CMAC by $\mathcal{C}$, the cost of a completed run of Protocol I and II is listed in Table 3.

TABLE 3. Evaluation of burden.

Protocol	Computing Cost On S	Computing Cost On C	Computing Cost On M	Communicating Cost
Protocol I	$3\mathcal{C}+\mathcal{S}$	$3\mathcal{C}+3\mathcal{S}$	\	$5\mathcal{M}$
Protocol II	\	$\mathcal{H}+\mathcal{SI}$	$\mathcal{H}+\mathcal{VE}$	$2\mathcal{M}$

TABLE 4. Comparison with related work.

Protocol	Computing Cost On S	Computing Cost On C	Communicating Cost	Additional Requirements
Protocol I	$3\mathcal{C}+\mathcal{S}$	$3\mathcal{C}+3\mathcal{S}$	$5\mathcal{M}$	NSB channels between S and C
Std PKH	$3\mathcal{C}+2\mathcal{S}$	$3\mathcal{C}+2\mathcal{S}$	$4\mathcal{M}$	public keys being pre-shared
Std PW	$3\mathcal{C}+2\mathcal{S}$	$2\mathcal{S}+3\mathcal{C}$	$4\mathcal{M}$	password being pre-shared
Std Dis	$5\mathcal{C}+2\mathcal{S}$	$5\mathcal{C}+2\mathcal{S}$	$5\mathcal{M}$	display-based NSB channels between S and C

Besides, we also compare the performance of Protocol I with protocols in the IEEE 802.15.6. The results are shown in Table 4.

As we can see from Table 4, Protocol I is the most suitable authenticated association protocol for healthcare applications. It requires *the least number of scalar multiplication on S*.

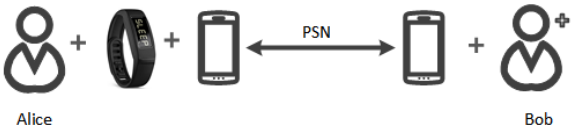


FIGURE 11. The demo system for the use case. Alice presses a button on the wearable blood pressure monitor and launches an application in her phone, and Bob launches a corresponding application in his smart phone to access the latest data of Alice's blood pressure.

VIII. USE CASE

In this section, we illustrate our system through a use case.

A. A DEMO SYSTEM

The demo system (shown in Fig. 11) illustrates how a PSN node shares health data with another PSN node. Assume Alice is a patient with hypertension. Bob is an expert of this disease. In order to use the PSN-based healthcare system, Alice wears a wearable blood pressure monitor on her wrist. Besides, both Alice and Bob carry a smart phone. Using the proposed system, Bob gets Alice's blood pressure through the following steps.

1) USER INITIALIZATION

Alice only needs to press a button on the blood pressure monitor to initialize secure links with her smart phone. According to the experiment, this process takes less than 0.3 seconds.

2) ADDING DATA TO THE HEALTHCARE BLOCKCHAIN

This process is executed by the smart phone automatically. Alice's smart phone generates and broadcasts a healthcare transaction Tx_1 to its neighbor PSN nodes. Tx_1 will be received by a miner node eventually.

3) NEW BLOCKCHAIN GENERATION

The whole process is executed automatically. According to Fig. 12, there are four steps for Tx_1 being added to the blockchain

- After a time interval $[T_i, T_j]$, the miner node M stops receiving new transactions.
- M generates a new block B (shown in Fig. 13) that contains Tx_1 and other transactions received during $[T_i, T_j]$. Then it sends the block to Alice's smart phone.
- Alice's smart phone generates a signature for B and sends back the block with the signature to M.
- M checks the signature. If the verification succeeds, M will add the block to the local chain and broadcast the new chain to its neighbor nodes.

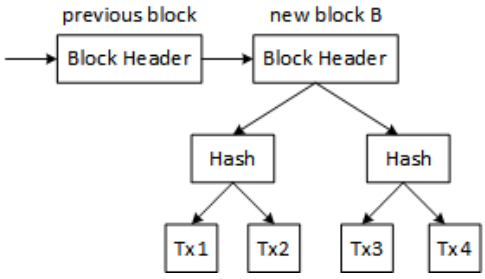


FIGURE 13. The new blockchain. New block *B* is added to the blockchain. Tx_1 is recorded in the new blockchain.

After the above process, the nodes P, Q, C and M hold the new blockchain and PSN nodes can use the blockchain to share health data.

4) ACCESSING HEALTHCARE DATA

In this stage, Bob uses his smart phone to require data of Alice's blood pressure monitor. The data will help Bob to learn about the latest health condition of Alice. Then Bob can make accurate plan of treatment remotely.

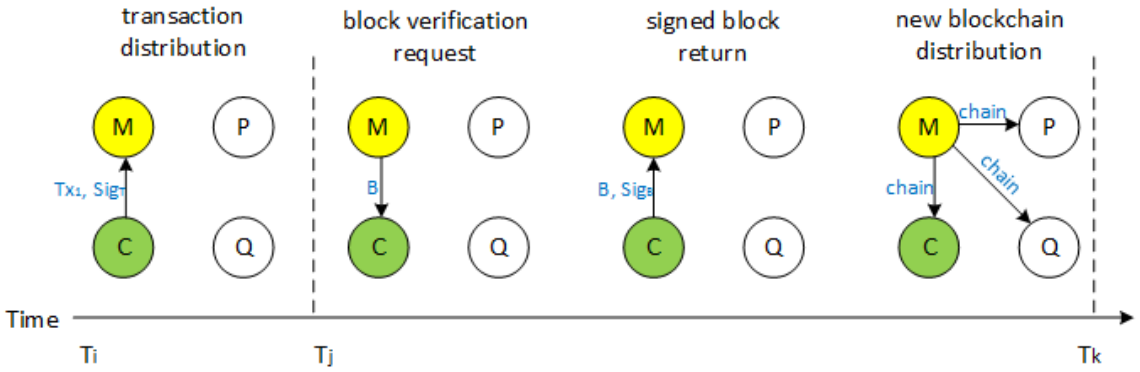


FIGURE 12. Generation of new blockchain that contains Tx_1. In $[T_i, T_j]$, M receives new transactions. From T_j to T_k, M stops receiving new transactions. In this time interval, new blockchain is distributed in PSN area. Tx_1 is recorded by the new blockchain.

B. ADVANTAGES

A secure link is established between Alice's blood pressure monitor and smart phone. It reduces computational burden on the blood pressure monitor.

It also illustrates a method of using blockchain in PSN-based healthcare application. This method does not bring heavy storage load to PSN nodes.

In addition, it avoids data leakage caused by illegal behavior of an untrustworthy third party, since data are stored in Alice's smart phone and blood pressure monitor.

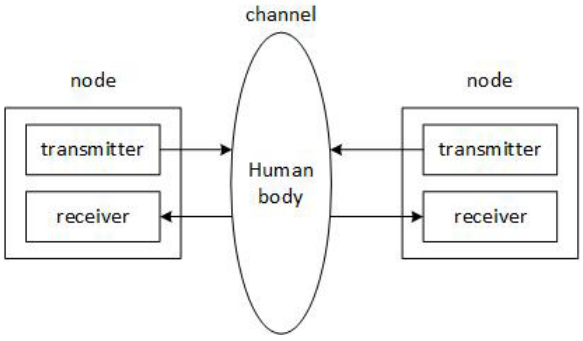


FIGURE 14. A simplified communication model with HBCs. Each node is associated with a transmitter and a receiver. The transmitter is used to send signals through human tissue. The receiver receives signals from human tissue.

FIGURE 15. The HBCs between implanted medical sensor and coordinator (i.e. the smart phone in hand). The user's body is modelled as an NSB channel.

C. HUMAN BODY CHANNELS

Human body channels (HBCs) use human body as transmission medium [29]–[31]. A typical HBC is modelled in Fig. 14. According to Fig. 14, each communicating participant is associated with a transmitter and a receiver. The transmitter sends signals through human tissue. The receiver receives signals from human tissue.

HBCs can be used in PSN-based healthcare applications when display-based OOB channels are infeasible. In the above use case, the medical sensor is a wearable device with a display and buttons. However, in some other scenarios, users may have medical sensors implanted inside the body. In this case, NSB channels cannot be established based on displays and buttons. We introduce HBCs as NSB channels for this situation. The HBC between implanted sensor and mobile devices is shown in Fig. 15.

HBCs can be modelled as NSB channels. Attackers find it difficult to spoof or block messages [29]–[31]. Users can easily find and prevent attacks in HBCs. If an attacker intends to block or spoof messages, the attacker is required to attach malicious signal sources to user skin. In most practical situations a user could easily perceive and stop such an attack.

IX. CONCLUSION

In this paper, we illustrate how to apply blockchain technique in PSN-based healthcare. The proposed method initializes secure links for PSN nodes. Healthcare blockchain is used for the nodes to share health data with others.

To initialize the secure links, an improved version of IEEE 802.15.6 display authenticated association protocol is designed. The protocol is better since it requires unbalanced computational load. In addition, HBCs are proposed to establish NSB channels for special situations.

The proposed method can be extended to other PSN-based applications, including environment monitor and transport. It will improve quality of people's life.

In our future work, a large-scale PSN-based healthcare system will be built. More experiments will be carried out to test the performance.

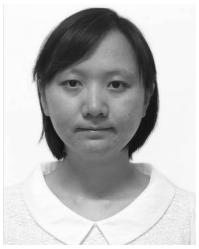
ACKNOWLEDGEMENTS

The authors appreciate the help of Kai Zheng to assist the experiments in this paper.

REFERENCES

[1] U. Varshney, "Pervasive healthcare and wireless health monitoring," *Mobile Netw. Appl.*, vol. 12, no. 2, pp. 113–127, 2007.
[2] G. Horn, K. M. Martin, and C. J. Mitchell, "Authentication protocols for mobile network environment value-added services," *IEEE Trans. Veh. Technol.*, vol. 51, no. 2, pp. 383–392, Feb. 2002.
[3] *IEEE Standard for Local and Metropolitan Area Networks—Part 15.6: Wireless Body Area Networks*, IEEE Standard 802.15.6-2012, 2012. [Online]. Available: http://standards.ieee.org/about/get/802/802.15.html
[4] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, no. 10, p. 218, 2016.
[5] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[6] M. A. Rahman, A. El Daddik, and W. Gueaieb, "Building dynamic social network from sensory data feed," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 5, pp. 1327–1341, Sep. 2009.
[7] M. A. Rahman, M. F. Alhamid, W. Gueaieb, and A. El Saddik, "An ambient intelligent body sensor network for E-health applications," in *Proc. IEEE Int. Workshop Med. Meas. Appl.*, Washington, DC, USA, May 2009, pp. 22–25.
[8] B. Yuvaradni, D. Dhanahsri, G. Sonali, T. Gauri, and M. S. Thite, "Health monitoring services using wireless body area network," *Imperial J. Interdiscipl. Res.*, vol. 2, no. 5, 2016. [Online]. Available: http://imperialjournals.com/index.php/IJIR/article/view/722

[9] M. M. Hassan, K. Lin, X. Yue, and J. Wan, "A multimedia healthcare data sharing approach through cloud-based body area network," *Future Gen. Comput. Syst.*, vol. 66, pp. 48–58, Jan. 2016.
[10] K. Lin and T. Xu, "A novel human body area network for brain diseases analysis," *J. Med. Syst.*, vol. 40, no. 10, p. 211, 2016.
[11] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Inf. Syst.*, vol. 48, pp. 132–150, Mar. 2015.
[12] N. A. Pulur, D. K. Altop, and A. Levi, "A role and activity based access control for secure healthcare systems," in *Proc. Inf. Sci. Syst.*, 2016, pp. 93–103.
[13] A. Sajid and H. Abbas, "Data privacy in cloud-assisted healthcare systems: State of the art and future challenges," *J. Med. Syst.*, vol. 40, no. 6, pp. 1–16, 2016.
[14] X. Su *et al.*, "Privacy as a service: Protecting the individual in healthcare data processing," *Computer*, vol. 49, no. 11, pp. 49–59, 2016.
[15] M. W. Häckell, R. Rolfes, M. B. Kane, and J. P. Lynch, "Three-tier modular structural health monitoring framework using environmental and operational condition clustering for data normalization: Validation on an operational wind turbine system," *Proc. IEEE*, vol. 104, no. 8, pp. 1632–1646, Apr. 2016.
[16] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): Authentication for implanted medical devices," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 1099–1112.
[17] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1862–1870.
[18] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, 2009, pp. 410–419.
[19] X. Huang, D. Liu, and J. Zhang, "An improved IEEE 802.15.6 password authenticated association protocol," in *Proc. 4th IEEE/CIC Int. Conf. Commun. China (ICCC)*, Shenzhen, China, Nov. 2015, pp. 2–4.
[20] M. Toorani, "Security analysis of the IEEE 802.15.6 standard," *Int. J. Commun. Syst.*, vol. 16, no. 17, pp. 2471–2489, 2016.
[21] J. Zhang, X. Huang, P. Craig, A. Marshall, and D. Liu, "An improved protocol for the password authenticated association of IEEE 802.15.6 standard that alleviates computational burden on the node," *Symmetry*, vol. 8, no. 11, pp. 1–14, 2016.
[22] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman. (2016). *A Case Study for Blockchain in Healthcare: 'MedRec' Prototype for Electronic Health Records and Medical Research Data*. [Online]. Available: https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf
[23] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles. (2016). *A Blockchain-Based Approach to Health Information Exchange Networks*. [Online]. Available: https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf
[24] R. C. Merkle, "A certified digital signature," in *Proc. Conf. Theory Appl. Cryptol.*, New York, NY, USA, 1989, pp. 218–223.
[25] R. Kainda, I. Flechais, and A. W. Roscoe, "Usability and security of out-of-band channels in secure device pairing protocols," in *Proc. 5th Symp. Usable Privacy Secur.*, 2009, Art. no. 11.
[26] S. Creese, M. Goldsmith, R. Harrison, B. Roscoe, P. Whittaker, and I. Zakiuddin, "Exploiting empirical engagement in authentication protocol design," *Secur. Pervasive Comput.*, 2005, pp. 119–133.
[27] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Feb. 1983.
[28] G. Lowe, "Casper: A compiler for the analysis of security protocols," *J. Comput. Secur.*, vol. 6, nos. 1–2, pp. 53–84, 1998.
[29] X. Huang, "Multi-channel security protocols in personal networks," Ph.D. dissertation, Dept. Comput. Sci., Univ. Oxford, Oxford, U.K., 2014.
[30] M. S. Wegmueller *et al.*, "An attempt to model the human body as a communication channel," *IEEE Trans. Biom. Eng.*, vol. 54, no. 10, pp. 1851–1857, Oct. 2007.
[31] M. S. Wegmueller, "Intra-body communication for biomedical sensor networks," Ph.D. dissertation, ETH Zurich, Zürich, Switzerland, 2007.



JIE ZHANG received the M.S. degree from Nanjing Normal University in 2013. She is currently pursuing the Ph.D. degree with Xi'an Jiaotong-Liverpool University. Her current research interests include public key cryptography, information security, and Internet of Things.

NIAN XUE received the B.E. degree from Xi'an Jiaotong University in 2004. He is currently pursuing the master's degree with Xi'an Jiaotong-Liverpool University. His current research interests include usable security protocols, software defined network, and Internet of Things.

XIN HUANG received the B.E. degree from Xi'an Jiaotong University in 2004, the M.S. degree from the Royal Institute of Technology in 2008, the Licentiate degree from Mid Sweden University in 2011, and the Ph.D. degree from the University of Oxford in 2015. He is currently a Lecturer with Xi'an Jiaotong-Liverpool University. His current research interests include usable security protocols, software defined network, and Internet of Things.