EAI Endorsed Transactions
on on Industrial Networks and Intelligent Systems Research Article ICST.ORG

A Trusted Mobile Payment Scheme Based on Body Area Networks

Huawei Zhao[1], Jiankun Hu[2*]

[1]Department of Internet Finance, Qilu University of Technology, Sangyuan Road 58, Licheng District, Jinan, China
[2]School of Engineering and Information Technology, UNSW@ADFA, Northcott Drive, Canberra 2600, Australia

Abstract

With the development of intelligent mobile phones and the improvement of wireless communication infrastructure, mobile payment is gradually accepted by the public. However, since intelligent mobile phones are not trusted devices, mobile payment faces serious security problems. To address the problems, this paper designs a trusted mobile payment scheme based on body area networks. The scheme builds a bridge between a body area network deployed on the human body and an intelligent mobile phone by the fuzzy vault technology and the human interference, and imports the security from a body area network to the mobile payment to establish a trusted mobile payment system. Because the scheme uses PPG signals with high-entropies to produce authentication data, its security is superior to traditional mobile payment schemes; at the same time the scheme uses trusted body area networks to design mobile payment systems and does not use external trusted devices, which is convenient to the users.

Keywords: body area networks, trusted mobile payment, security, biosensor nodes, fuzzy vault, PPG.
Received on 29 December 2014, accepted on 02 February 2015, published on 25 February 2015

doi: 10.4108/inis.2.2.e5

1. Introduction

Mobile payment is about purchasing goods online using intelligent mobile phones, and it is the core of mobile E-Business. At present, mobile payment is in a prosperous development and the emergence of it mainly owes to two reasons: the rapid technologies development of intelligent mobile phones and the improvement of wireless communication infrastructure. These two technology advancements enable people browse, select and purchase goods online by intelligent mobile phones at anytime and anyplace, which means that shopping could be beyond all limits of space and time. Now the public gradually accept the burgeoning mobile payment trend , for instance, 24% of the total turnover comes from mobile E-Business in 2014 Tmall 1111 carnival, while the ratio is 8% in 2013 Tmall 1111carnival [1].

Though mobile payment brings a convenient life to the public, it also brings the hidden security threats to the users. It is because that the carriers of mobile payment, intelligent mobile phones, are not trusted devices, and what is more, most users lack of general knowledge of information security, which causes mobile payment face serious threats of information security. And these threats could mainly be divided into two categories.

- Malicious APPs.

Most mobile intelligent phones have not installed the trusted roots, which makes them are not trusted devices. And in such an environment a user usually cannot identify the validation of the APPs he installs because his intelligent mobile phone cannot verify these APPs. And then if an APP is malicious, it will open a backdoor in the intelligent mobile phone, and send the use's private information, such as SMS, transactions authentication codes and the users' input to the adversary secretly. For instance, two famous malicious APPs emerge in 2014 Tmall 1111 carnival. One is "1111 SMS thief". The malicious APP disguises as a frequently-used APP and entices users to install it in intelligent mobile phones. Once the malicious APP is installed in intelligent mobile phones, it will intercept users' critical transaction messages such as SMS and authentication codes, and send these messages to the adversary. The other is "thief cat". The malicious APP disguises as the "Tmall management service" and induces users to run it in intelligent mobile phones. Once it runs, it will close the safeguard APP in intelligent mobile phones, collect various private data and send these data to the adversary. After completing these operations, it deletes itself from intelligent mobile phones in order to hide its attack.

Many malicious APPs could be detected by safeguard APPs, and most users depend on these APPs to protect their intelligent mobile phones. However, safeguard APPs belong to software and the "soft protection" is not a trusted solution. For instance, just as mentioned above, the "thief cat" can close safeguard APPs. In addition, according to the investigation of Alibaba's mobile security center, 97% tested APPs have security flaws, and what is more ironic, 21% of these unsecure APPs are safeguard APPs that account for a largest proportion.

- SIM card replication.

SIM card replication is a serious security problem ignored by most users. When users go to a maintenance point to repair their intelligent mobile phones, they generally don't unplug SIM cards, and then the SIM cards will face the risk of being replicated. According to the existing technologies, most kinds of SIM card are not trusted devices, and can be replicated. And once a SIM card is illegally replicated, the adversary can easily get the user's SMS and eavesdrop on his/ her mobile phone conversation, which bring serious threats to mobile payment.

From above analyses, it can be seen that the own security problems of mobile intelligent phone and users' unsecure usage habits cause the mobile payment not as secure as we expected. And the core problem is that our mobile intelligent phones including their SIM cards are not trusted devices. So how to design a trusted mobile payment scheme on the basis of the untrusted intelligent phones is very important to the further development of E-Business, and it is exactly the problem we want to address in this paper.

Recently, a new kind of wireless network, named as body Area networks (BANs) [2], achieves a rapid development. BANs are composed of tens of small biosensor nodes. These biosensor nodes are deployed on or into the human body to collect physiological signals continuously, and send these signals to the remote medical center in real time to further analyses and processing. While due to limitation of operation resources, biosensor nodes have not enough energy to send signals to remote medical center by themselves. And they must complete the transmission with the help of a PDA (Personal Digital Assistant). Since intelligent phones are usually put nearby the human body, they are the most suitable candidates for PDA.

Since the signals collected and sent by the BANs concern private privacy, serious medical negligence can happen once the security problems emerge, such as modification and leak of physiological signals. So information security is very important to BANs and it is a hot research area at present. The core of BANs' security is key management schemes, and so far many key management schemes have been developed to build a trusted BAN system that can realize the authentication of biosensor nodes and secrecy transmission between biosensor nodes. And the relationship between BANs and intelligent mobile phone inspire us to use trusted BANs to design a trusted mobile payment.

In this paper, we consider BANs and intelligent mobile phones as a whole communication system, and our intension is to use a key management technology of BANs, named as fuzzy vault, to design a trusted mobile payment scheme. Our contributions include: (i) The scheme does not need extra trusted devices, and it realizes trusted mobile payment only with the help of a BAN which is already deployed on the human body; (ii) In the scheme users do not need to input any password when they purchase goods online using intelligent mobile phones; (iii) The security root of the payment scheme is the cryptographic keys pre-deployed in the biosensor nodes, and malicious APPs in intelligent mobile phones cannot threaten the security of mobile payment.

The rest of this paper is organized as follows. In section II, existing researches of trusted mobile payment and the introduction of fuzzy vault technology are present. In section III, we provide a concrete trusted mobile payment scheme using fuzzy vault technology. In section IV, we give security analyses for the mobile payment scheme. Finally, we give a conclusion in section V.

2. Related work

In this section, we first present current researches of trusted payment of mobile intelligent phones in the literature, and then we introduce the fuzzy vault technology that is the mainstream method in designing key management scheme for BANs.

2.1 The trusted mobile payment

Currently, more and more people realize that the trusted mobile payment plays an important role in fund security, which motivates the interests of researchers.

Some researches explored the security issues of mobile payment. For example, the research in [3] presents a detailed classification about vulnerabilities, threats, risks and protection solutions in mobile payment systems and analyses the future challenges; the research in [4] also investigates the security threats and attacks in mobile payment, and gives an indeepth discussion about security problems from three areas including network security, transmission security and mobile device security.

And some researches are developed to design trusted mobile payment schemes. At present, these researches could be divided into three categories.

The first category is using external trusted devices to secure mobile payment schemes. In this category, the external trusted devices generally are pre-deployed keys in the initialization and can communicate with intelligent mobile phones by audio interface or wireless interface and so on. For the sake of security, the pre-deployed keys cannot be read from outside of the trusted devices. When a mobile payment happens, the external trusted devices produce cryptographic transaction proofs using pre-

deployed keys, and send these proofs to intelligent mobile phones to secure mobile payment. For instance, research [5] proposed to use electronic security keys to secure mobile payment. In the research, a trusted device connects to an intelligent mobile phone by an adaptable interface, and is pre-deployed a security key and some security policies. In fact, the key is a trust root of the mobile payment. In a mobile payment an intelligent mobile phone will send essential transaction messages to the device, and the device will use its security key to produce a trusted proof for these messages to secure the payment. Similar researches appear in [6]. The advantage of the schemes falling into this category is that the security key is pre-deployed and protected by a trusted device and out of the intelligent mobile phone, and thus the malicious environment of intelligent mobile phones cannot compromise the key to launch an attack to mobile payment. While the disadvantage is that the external trusted devices are lacking of portability and are inconvenient to users.

The second category is using security algorithms or security protocols to build trusted mobile payment schemes. The work in [7] proposes to improve the security of mobile payment based on SET protocol. In the scheme an improved SET protocol available to mobile payment is designed to address the conflicting decision analysis problem between the customers and merchants. Also the protocol can provide security services such as transaction atomicity and goods atomicity. The work in [8] proposes a mobile payment model where the E-Business center (mobile businessman) is considered as a trusted part, and uses the mechanism of symmetric keys to design a key management scheme and a mobile payment scheme to secure mobile payment. The work in [9] proposes a flexible online payment model, and in the model it combines “pre-trusted” hierarchical certification model and “public-service-domain” to address the problems of dynamic change of payment system and cross-platform service. And then the research further design a mobile payment protocol based on the proposed model. The common feature of the schemes falling into the category is using cryptographic algorithms or protocols to secure mobile payment. However, since intelligent mobile phones are not untrusted devices, the security of these schemes are uncertain in the further with the development of attack technologies.

The third category is using biometrics to secure mobile payment. The representative of the category is the research in [10]. In this work, fingerprints and finger vein are collected and processed to help the bank authenticate users and mobile payment. Because fingerprints and finger vein keep unchanged over time, if they are compromised, they are lost forever. To address the problem, the research uses a cryptography modal to derive keys from biometrics, and uses a time-synchronized one-time password (TOTP) encryption modal to protect the derived keys. The advantage of the research is that it can realize seamless integration with the existing password-payment system, and has higher security than traditional mobile payment. Similar research appears in [11], and it proposes a secure mobile payment framework based on biometrics using (WPKI) wireless public key infrastructure and UICC (universal integrated circuit card) in intelligent mobile phones. In order to realize the trusted mobile payment, the research designs a MBA (mobile biometrics application) to control the access of secret information in the UICC, and MBA can permit the user uses the secret information in UICC to execute mobile payment only if a user is pass the fingerprint authentication. The two researches give good guides about how to use biometrics to protect mobile payment, however, both of them have a security problem, that is the two schemes use fingerprint or finger vein to design trusted mobile payment and these physiological features can be easily collected from the surface of the human body. Once these features can be counterfeited, it will bring serious attacks to mobile payment.

2.2 Fuzzy Vault

The fuzzy vault is a popular technology used to key management scheme of BANs. In the technology, a structure called *vault* is used to hide a secret value *M* by a set *A*, and if another set *B* is similar enough to *A*, it can unhide *S*. Using fuzzy vault, research in [12] proposed a *PKA* protocol to use photoplethysmogram (PPG) signals from the human body to negotiate a common key between two biosensor nodes. The *PKA* protocol consists of 5 steps [12]:

(i) Generating PPG vector. Assume that both of the sender *A* and the sender *B* are adjacent biosensor nodes, and o when they want to build a common key, both of them measure PPG signals under a loose time mechanism. And then, the two parts use a fast Fourier transform (FFT) to encode their PPG signals into two vectors $F_s =< f_s^1, f_s^2, \dots, f_s^a >$ and $F_r =< f_r^1, f_r^2, \dots, f_r^a >$ respectively.

(ii) Producing polynomial. *A* produces a polynomial *p* with a^{th} order and random coefficients where a^{th} is public and the random coefficients are encoded into a a common key. For instance, if c_a, $c_{a-1}, \dots$, c_1 ,c_0 are the coefficients, the common key will be $K=c_a || c_{a-1} || \dots || c_1 || c_0$.

(iii) Creating vault. The sender *A* first uses f_s^i as the input to compute a set $D = \{f_s^i, p(f_s^i)\}, 1 \le i \le N$, and then constructs a chaff points set $J=\{j_i, d_i\}, 1 \leqslant i \leqslant N$, where *N* is a value previously defined by *A*; j_i and d_i are random values, $d_i \neq p(j_i)$. Next, *A* mixes the values in *D* and *J* to produce a vault $R=D \cup J$.

(iv) Transferring vault. A computes the authentication code of *R* using a keyed hash function with *K*, and sends *R* and its authentication code to *B*.

(v) Unhiding vault. Once receiving the vault including *R* and its authentication code, *B* chooses the points from *R* to build a set *Q* according to F_r. That is, the *x* ordinates of points in *Q* is the elements in F_r. And

then ,*B* tries to rebuild the polynomial *p* using the set *Q* by Lagrangian Interpolation. If *B* builds a polynomial *p'*, it will use the coefficients of *p'* to generate a key *K*' as mentioned in step (i). Finally, *B* uses *K'* to check the validity of *R*'s authentication code, and the soundness of the authentication code means that *A* and *B* share the common key *K* (or *K'*).

The fuzzy vault technology only needs a loose time synchronization mechanism between biosensor nodes to negotiate common keys [13], and it does not require the order of collected physiological signals. These features makes fuzzy vault be very suitable to key negotiation in BANs and many related researches are developed based on fuzzy vault, such as [14,15].

3. A trusted mobile payment scheme based on body sensor networks

With the help of fuzzy vault, a BAN can realize security connections among biosensor nodes, and it means that once a user wears a BAN, a trusted communication system is deployed on the human body. Since the operation of mobile payment is near to the human body, in this section we intend to build a bridge between a BAN and a mobile payment system and introduce the security of BAN to the mobile payment system. Our final goal is to establish a trusted mobile payment system based on a trusted BAN using fuzzy vault technology. The structure of our scheme can be shown by figure 1.

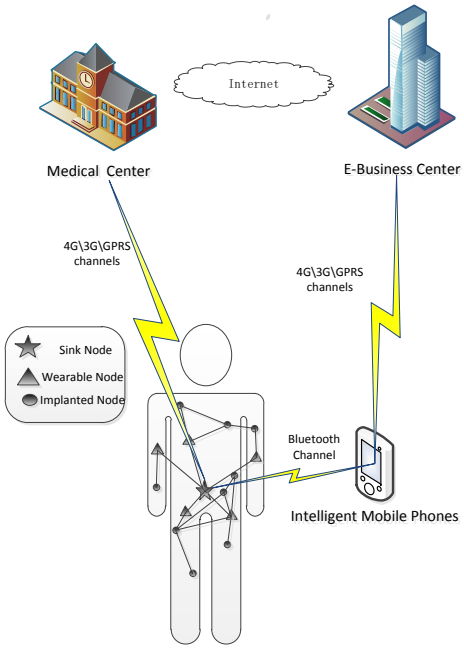

Figure 1. The structure of a BAN

3.1 The design of body sensor network

In our scheme, a BAN has two kinds of nodes: tens of biosensor nodes and a sink node.

Biosensor nodes can be divided into two categories: wearable nodes that are deployed on the human body and implanted nodes that are deployed into the human body. Biosensor nodes of the two categories are all integrated with IEEE 802.15.6 modules and biosensor modules. The former module is used to communicate with other biosensor nodes and the sink node; and the latter module can be used to install some kinds of physiological sensors to collect physiological signals such as temperature, blood pressure, blood sugar, PPG, blood oxygen and so on. In addition, a biosensor node has a storage unit and a calculation unit. The storage unit is used to storage the operation system and few collected data, and the calculation unit is used to simple computation. It would be specially mentioned that since PPG is a high-entropy signal and could be collected from almost any point of the human body, a biosensor modular in an implanted biosensor node generally installs a PPG sensor to negotiate common keys with other biosensor nodes in most key management schemes of BANs. And in our scheme we will use two implanted biosensor nodes to collect PPG signals to realize trusted mobile payment.

The sink node is deployed on the human body, and compared to biosensor nodes it has more operation resources such as energy, computation ability, storage and so on. The sink node is designed with three communication modules. The first one is IEEE 802.15.6, and it is used to communicate with biosensor nodes to receive physiological signals from them and send operation commands to them; the second one is the short distance communication module: Bluetooth, and it is used to communicate with an intelligent mobile phone in mobile payment for the distance between the sink node and the phone is always within one meter long; the third one is SIM module, and it is used to communicate with the remote medical center by 4G\3G\GPRS channels. In addition in order to improve the security of mobile payment, the sink node is installed a small LED screen with two little buttons: *confirm* and *cancel*, and the screen is used to show the transaction amount of a mobile payment. The design of the screen can be descripted by the figure 2.

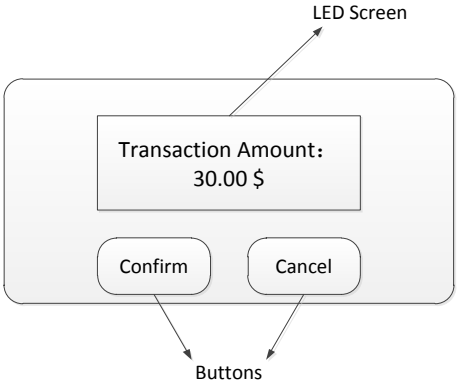

Figure 2. The design of the LED screen

3.2 Initialization

Our trusted mobile payment system includes three parts, the user, the remote medical center M_c and the E-Business center F_c. When a user wants to use a BAN for medical usages, he first applies to M_c for it. After authenticating the user by necessary procedures, M_c deploys a BAN on the user's body. And before the deployment M_c will first install a secret symmetric key K_m and the user's identity card number *IDN* into the sink node and two specified implanted biosensor nodes *A* and *B*, and all of them will serve for the trusted mobile payment. At the same time, M_c recodes the following messages into Table 1.

Table 1. The table in M_c

Identity Card Number	Identity of Node *A*	Identity of Node *B*	Information of Secret Key
IDN	ID_A	ID_B	K_m

When the user wants to possess a trusted mobile payment system, he first applies to the E-Business center F_c using his *IDN*. Next, F_c asks $M_c$for the key information of the user according to his *IDN*. Once M_c receives the request of F_c, it seeks its Table 1 by the *IDN* to find the corresponding key K_m. And then, M_c computes a hash value: $K_f = Hash(K_m||IDN||R_m)$, where *Hash*() is a hash function such as MD5, R_m is a random value produced by M_c and || denotes concatenation operation. And then, M_c sends K_f to F_c by a security manner. Since the communication between F_c and M_c belongs to Internet communication system and there are many mature methods such as VPN and SSL to protect the communication, in this section we don't give a deep discussion about it.

When F_c receives K_f in a security manner, it will maintain a table shown by Table 2.

Table 2. The table in F_c

Identity Card Number	Identity of Node *A*	Identity of Node *B*	Information of Secret Key
IDN	ID_A	ID_B	K_f

In order to establish security connection between the BAN and the mobile payment system, $M_c$generates and sends $R_m||Hash(K_m||R_m)$ to the sink node in the user's BAN by SIM card with 4G/3G/2G channels. And then, the sink node will check the validation of $R_m||Hash(K_m||R_m)$ using K_m. If $R_m||Hash(K_m||R_m)$ is fresh and valid, the sink node will produce $K_f = Hash(K_m||IDN||R_m)$ and deliver $R_m||Hash(K_m||R_m)$ to *A* and *B*. When *A* and *B* receive the message, both of them also use K_m to verify the validation of the message respectively. If $R_m||Hash(K_m||R_m)$ is fresh and valid, both *A* and *B* produce $K_f = Hash(K_m||IDN||R_m)$. Here, we assume that the three nodes could judge the freshness of R_m by storing old R_ms. Because R_m is only used in the initialization phrase, the three nodes don't need to store man old R_ms.

Thus in the following we use the security key K_f to build a bridge to introduce the security from the BAN to the mobile payment system.

Before serving for trusted mobile payment, both of *A* and *B* equally divide the binary form of $K_f$into v+1 parts, and if the length of the binary form of K_f is not equally divided into v+1 parts, we should padding K_f at the end of it. Assume that $(K_f)_2$denotes the binary form of K_f, and the i^{th} part of $(K_f)_2$ is $c_i(0 \le i \le v)$, we can define : $(K_f)_2 = c_v||c_{v-1}||\ldots||c_0$. And then, *A* and *B* produce the same polynomial with v^{th} order respectively: $p(x) = (c_v)_{10}x^v + (c_{v-1})_{10}x^{v-1} + \cdots + (c_0)_{10}$, where $(c_i)_{10}$ denotes the decimal form of c_i.

The initialization process can be shown in Figure 3.

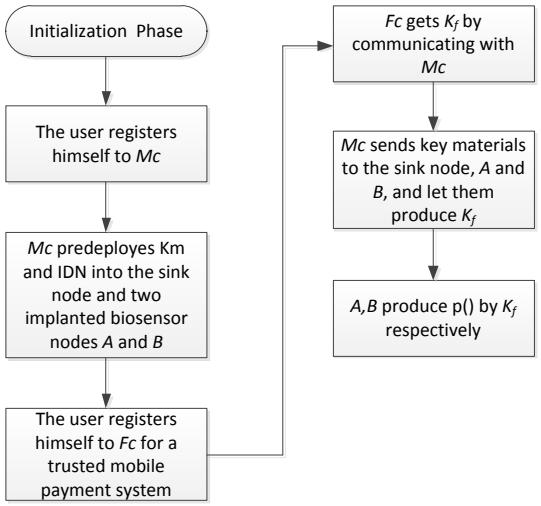

Figure 3. The process of initialization

3.3 Authentication phase

If a user wants to purchase a good by his intelligent mobile phone, he first opens a specified APP in the intelligent mobile phone and chooses goods. When he presses the "payment" button to pay for the chosen good, the authentication flow can be descripted as follows.

(i) The APP opens the Bluetooth module in the intelligent mobile phone to search the sink node nearby to build a connection. After both of them connect with each other, the APP sends the transaction amount *M* to the sink node, and then the sink node displays *M* on its LED screen. If the displayed *M* is just the transaction amount the user wants to pay for, the user will press the "confirm"

button on the LED screen to continue the payment process. Under this condition, we design the security protocol, *P1*, to let the sink node ask *A* and *B* to submit the authentication data.

P1:

1. $Sinknode \rightarrow A(B): R_S$,
2. $A(B) \rightarrow Sinknode: R_{A(B)}, Hash(K_m, A(B)||Sinknode||R_{A(B)}||(R_S + 1))$
3. $Sinknode \rightarrow A(B): Hash(K_m, Sinknode||A(B)||(R_{A(B)} + 1))$

Here, R_S and $R_{A(B)}$ are random values, $Hash(K_m,*)$means a keyed hash function. Otherwise, the user will press the "cancel" button on the LED screen, and in the condition the sink node won't execute *P1*, and the APP will cancel the transaction after a period of time it does not receive any available data.

(ii) Once *A* and *B* receives the message of step 3 in *P1*, and find the message is valid, both of them will collect their PPG signals respectively: $F_A = f_A^1, f_A^2, \ldots, f_A^N$ *and* $F_B = f_B^1, f_B^2, \ldots, f_B^N$.

(iii) Next, *A* computes$P_A = \{f_A^i, p(f_A^i)\}$, where $f_A^i \in F_A$, $1 \le i \le N$. At the same time, *A* generates a random point set $C_A = \{cf_A^j, d_j\}$, where $cf_A^j \notin F_A$, $d_j \notin p(cf_A^j)$, and $1 \le j \le U$. And then, *A* mixes P_A and C_A to get a point set $R_A = mix(P_A, C_A)$, where $mix()$ is a randomly mixing function. Similarly, *B* generatesR_B.

(iv) *A* generates authentication data: $V_A = ID_A, IDN, N_A, M, E(K_f, R_A), MAC(K_f, ID_A||IDN||N_A||M||R_A)$, where $E(K_f, R_A)$ denotes encrypting R_A by K_f in a symmetric encryption manner and N_A is the nonce of *A*. Similarly, *B* generates $V_B = ID_B, IDN, N_B, M, E(K_f, R_B), \mathrm{MAC}(K_f, ID_B||IDN||N_B||M||R_B)$. Finally, *A* and *B* send V_A and V_B to the sink node, and then the sink node deliver V_A and V_B to the E-Business with the help of the APP's forwarding.

(v) If F_c receives V_A and V_B, it first checks whether the two *IDN*s from V_A and V_B respectively are equal. If the two *IDN*s are the same, F_c will seek a row in Table 2 where the field of Identity Card Number is *IDN*. And if the row named as *W* exists, F_c will further check whether there are ID_A and ID_B in *W*. Neither ID_A nor ID_B means a fault. If both of the ID_A and ID_B exist, F_c will execute the operation in step vi. Here, we assume F_c can check the freshness of $N_A$and N_B by storing old $N_A s$ and $N_B s$.

(vi) F_c uses K_f from *W* to decrypt R_A and R_B from $E(K_f, R_A)$ and (K_f, R_B) respectively. Next, F_c will construct a set $Q = \{(b,c)|(b,c) \in R_A, b \in F_B\}$ from R_A and R_B. And when *Q* includes *v*+1 points, F_c will try to rebuild the polynomial *p*(). Here we denote the polynomial generated by F_c as *p'*(). F_c uses the coefficients of *p'*() to generate K_f', and then compares K_f' with K_f. If K_f' is equal to K_f, F_c further checks the validation of the *MAC* values of V_A and V_B, and if both of the two *MAC* values are valid, the authentication is successful, and F_c will transfer the fund from the user's account to the merchant.

(vii) Finally, because PPG signals belong to the feature signals of the human bodies and different persons have different PPG signals [16], F_c can store the set *Q* as the proof of the user's transaction.

4. Analysis of security

The core idea of our trusted mobile payment scheme is introducing the physiological signals into the mobile payment, and making use of the security of BANs to realize a trusted mobile payment. In the following, we give a security analysis to our schemes.

- The security protocol *P1*

In *P1*, only if the user presses the "confirm" button of the sink node, the sink node could execute the authentication process by asking biosensor nodes *A* and *B* to submit authentication data. If the adversary pretends to be the sink node to send a "R_S" to *A* and *B*, when *A* and *B* feedback the message in step 2, the sink node will find the attack as the user has not pressed the "confirm" button. Besides, though the adversary can eavesdrop on the message in step 2, he cannot fake the message in step 3 for he does not knowK_m. And what is more, the freshness of $R_{A(B)}$ and the operation of $R_{A(B)} + 1$ can resist the replay attack launched by the adversary.

Thus, we can say that only the user check the transaction amount displayed in the LED screen and press the "*confirm*" button, the sink node can ask *A* and *B* submit the authentication data.

- The security of keys

Because the BAN is deployed on the human body and is under the surveillance of the user all the time, the adversary hardly has a chance to compromise the nodes in it. Thus, we believe that the adversary cannot obtain K_m and K_f from biosensor nodes *A* and *B*. In addition, as long as we believe M_c and F_c are honest, we could believe the adversary cannot obtain K_m directly from M_c or obtain K_f directly from F_c. What is more, due to $K_f = Hash(K_m||IDN||R_m)$, F_c does not know K_m from K_f, it means that K_m could be used in other security applications in BANs.

- The security of PPG

In our scheme the information of PPG signals are delivered from the BAN to the untrusted intelligent mobile phone and next are delivered to F_c. Because the information is very important to our trusted mobile payment, in the following we give an analysis about the security of PPG signals.

Since the information of PPG is included in the messages R_A and R_B which are encrypted by K_f, the adversary hardly obtain the information of PPG signals directly from R_A and R_B. Besides, generally the length of f_A^i and f_B^i are 13 bits, and N=10, and then the length of F_A and F_B is 130bits, it means that the adversary cannot guess the right PPG signals by brute attack.

- The security of communication system

In our scheme the transmitted messages include N_A and N_B, and they can be used to resist the replay attack, that is when the adversary eavesdrop on V_A and V_B, he cannot replay these messages to F_C to launch a relay attack.

It can be seen that our scheme does not protect the communication between the intelligent mobile phone and the sink node. It is because we design an artificial confirmation mechanism, and if the transactions amount delivered from the intelligent mobile phone to the sink node is modified by the adversary, the user will find the modification and he will cancel the payment.

5. Conclusion

In this paper, we deign a trusted mobile payment scheme based on BANs. The scheme uses the fuzzy vault technology and the human interference to build a bridge between the BAN and the mobile payment, and introduces the security from the trusted BAN to the mobile payment. Below are the advantages of our scheme: i) Different to the researches in [10, 11], our scheme uses PPG with high-entropies to authenticate the user, which increases the difficulties of the adversary attacking the mobile payment by faking valid physiological signals such as fingerprint and finger vein. ii) Our scheme does not need any password, which makes the user not need to remember the complex password as traditional schemes do. iii) Though malicious APPs are installed into the intelligent mobile phone, they cannot get any useful authentication data, and cannot influence the security of mobile payment. iv)Our scheme does not need any trusted external device, and only makes use of the BAN already deployed on the human body, which is convenient to the users.

References

[1] DFDaily (2014) http://epaper.dfdaily.com/dfzb/html/2013-11/13/content_835090.htm.

[2] Zhao, H.W., Qin, J., Hu, J.K. (2013)Energy Efficient Key Management Scheme for Body Sensor Networks. *IEEE transactions on Parallel and Distributed Systems* 24(11):2202-2210.

[3] Lsaac, J.T., Zeadally, S. (2014) Secure Mobile Payment Systems. *Mobile Commerce* May/June 2014:36-43.

[4] Lelia, E., Zeinab, B.F., Arasteh, M.A. (2012) A Survey on Mobile Systems Security. *Research Journal of Applied Science, Engineering and Technology* 4(20):4043-4050.

[5] Pan,T.G., Zheng, L.N. (2007)Mobile Payment System Enhanced by Electronic Security Key. *WSEAS Transactions on Systems* 6(3): 455-460.

[6] Xu,Y., Yao, R.Y., Liu, X.Y. (2009) A payment model of mobile phone based on third-party security. 2009 International Conference on Management of e-Commerce and e-Government, Nanchang, China, September 16, 2009(IEEE Computer Society: Piscataway), 400-403.

[7] Li, X.M., Liang, B., Wang, J.P. (2012) Analysis and improvement of mobile payment security based on SET protocol. *2011 International Conference on Applied Mechanics, Materials and Manufacturing*, Shenzhen, China, Nov. 18, 2011 (Trans Tech Publications: Clausthal-Zellerfeld), 615-618.

[8] Shuai, F., You, J., Li, Z.S. (2010) Research on Symmetric key-Based Mobile Payment Protocol Security. *Proceedings 2010 IEEE International Conference on Information Theory and Information Security*, Beijing, Dec. 17,2010 (IEEE Computer Society: Piscataway), 340-344.

[9] Wang, H.X., Yang, D.L., Wang, J.J., Ma, H. (2012) Online Mobile Payment Model and Protocol with Flexibility and Security. *ICIC Express Letters* 3(5):1139-1146.

[10] Yang, W.C., Hu, J.K., Yang, J.C., Wang, S., Shu,L. (2013) Biometrics for Securing Mobile Payments: Benefits, Challenges and Solution. 6th International Congress on Image and Signal Processing, Hangzhou, China, Dec.16,2013 (IEEE Computer Society: Piscataway), 1699-1704.

[11] Ahamad, S.S., Sastry,V.N., Nair, M. (2013) A Biometric Based Secure Mobile Payment Framework. 4th IEEE International Conference on Computer and Communication Technology, ICCCT 2013, Allahabad,Setp.23, 2013 (IEEE Computer Society: Piscataway),239-246.

[12] Venkatasubramanian, K.K., Banerjee, A. and Gupta, S. K. S. (2008) Plethysmogram-based Secure Inter-Sensor Communication in Body Area Networks. *In Proc. IEEE Military Communications Conference*, Washington, Nov.17, 2008 (Institute of Electrical and Electronics Engineers Inc.: Piscataway), pp.1-7.

[13] Venkatasubramanian, K.K., Gupta, S. K. S. (2010) Physiological Vaule-Based Efficient Usable Security Solutions for Body Sensor Networks. *ACM Transactions on Sensor Networks* 6(4): pp.1-36.

[14] Cao, C.Z., He, C.G., Bao, S.D., Li, Y.(2011) Improvement of Fuzzy Vault Scheme for Securing Key Distribution in Body Sensor Network. *33rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Boston, Aug.30,2011 (Institute of Electrical and Electronics Engineers Inc.: Piscataway), pp.3563-3567.

[15] Miao, F., Bao, S.D., LI, Y. (2010) A Modified Fuzzy Vault Scheme for Biometrics-Based Body Sensor Networks Security. *IEEE Global Telecommunications Conference*, Miami, Dec.6,2010 (Institute of Electrical and Electronics Engineers Inc.: New York), pp.1-5.

[16] Poon, C. C. Y., Zhang, Y. T., Bao, S. D. (2006) A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine* 44(4): pp. 73-81.