Anonymity-Aware Face-to-Face Mobile Payment

Koichi Kamijo, Toru Aihara, and Masana Murase

IBM Research - Tokyo,
1623-14, Shimotsuruma, Yamato-shi, Kanagawa-ken, 242-8502, Japan
{kamijoh,aihara,mmasana}@jp.ibm.com

Abstract. On-line payments are increasingly popular in paying bills for Internet shopping, and payment-capable mobile phones support making purchases anytime and anywhere, without cash. However, mobile payments are rarely used for making face-to-face payments, with concerns about anonymity, security, and usability. This paper proposes a face-to-face mobile payment protocol that addresses these concerns. To address anonymity and security concerns, the proposed protocol uses unique information for the payment transaction, such as the location and the time, and introduces two procedures for optimizing the matching time slots and exchanging random numbers when needed, to secure the transactions without exposing the seller's or the buyer's personal identification. To address usability concerns, the proposed protocol optimizes the parameters for the two introduced procedures to match the seller-buyer pairs, depending on the number of the people involved in the mobile payments, the delays caused by human operations with the mobile phones, mobile communication, and so on. Experimental results prove that the proposed protocol is practical, solving the addressed concerns.

Keywords: Mobile payment, mobile phone, anonymity, security, usability.

1 Introduction

Mobile phones are changing the way we shop every day. While on-line payments are increasingly popular for paying bills for Internet shopping and public services by paying with a credit card, a bank account, or a prepaid on-line account, mobile phones are also enhancing our experiences by allowing us to pay anytime and anywhere, without carrying cash [1,2]. For example, Safaricom M-PESA [3,4,5,6,7] and similar services [8,9,10,11,12] are useful for sending payments within a country where the financial infrastructure is still immature and expensive. Such mobile payments are leading to new financial infrastructures, especially in African countries, where Automatic Teller Machines (ATMs) are scarce and people have difficulty in withdrawing money from banks. The service of M-PESA is based on Short Message Service (SMS), which supports a widely used application "Twitter", and most mobile phones have SMS capabilities, without regard to the brand or system software.

P. Sénac, M. Ott, and A. Seneviratne (Eds.): MobiQuitous 2010, LNICST 73, pp. 198–209, 2012.

However, mobile payments have yet to make major inroads, especially for micropayments in face-to-face transactions. The Global System for Mobile communications Association (GSMA) [13] is promoting a pay-by-mobile [14] initiative to address this situation. The main inhibiting factors seem anonymity, security, and usability. Especially, anonymity is rarely addressed mainly due to identification of the sellers and the buyers are usually assumed with currently existing mobile payment technologies.

Cash payments are inherently anonymous. On the other hand, mobile payments may lack anonymity, being backed by information technology, and are often traced based on the security requirements. In fact, people, not only the buyers but the sellers, sometimes do not wish to disclose their identities, i.e. their names or telephone numbers, in some cases, e.g. at flea market, in charity bazaars, in street stalls in Asian countries or even though they are performing legal economic activities.

In this paper, we propose a face-to-face mobile payment (F2FMP) protocol with full anonymity, in which the anonymity of both the sellers and the buyers is guaranteed. We also briefly discuss anonymity levels and symmetry, relaxing the anonymity of either a seller or a buyer or the both. We mainly focus on the anonymity concerns, since anonymity is the problem not addressed in existing technologies, and security and usability can be solved accordingly once a proposal addressed to anonymity is finalized. We choose SMS for our protocol communicating between the payment server and the users (the sellers and the buyers), because it is widely available as already discussed and its communication cost is reasonable.

The remainder of this paper is organized as follows. Section 2 identifies the technical problems of current mobile payments, i.e. anonymity, security, and usability. Section 3 discusses the related protocol and Section 4 proposes a F2FMP protocol. Section 5 reports our experimental results and Section 6 evaluates our F2FMP protocol addressing the three problems identified in Section 2. Section 7 finally concludes our discussion.

2 Technical Problems with Mobile Payments

In this section, we investigate three important technical problems for the F2FMP, anonymity, security, and usability, and use these problems as criteria to evaluate the quality of the mobile payment technology:

Anonymity: Mobile payment is usually lack of anonymity. Cash payment is always anonymous, but an SMS-based mobile payment is inherently designed to disclose the identities of the seller and the buyer each other to confirm the transaction on the server. Once identity information becomes generally available due to careless management or malicious attacks, it may be misused for spamming or phishing. Therefore, the sellers or the buyers do not wish to disclose their identities.

Security: Mobile payment always carries security concerns, not only from its technology, but also from user experience. Cash can be counterfeited, is easily stolen, and is very hard to recover. On the other hand, mobile money cannot be stolen since its value is electrically exchanged. Even if the mobile phone is stolen, we already have several measures to disable the payments function, e.g. to prompt a password or remotely disable the function via Mobile Network Operator (MNO). Nevertheless, people still do not fully trust electronic forms of money, because of the security concerns. Security of the SMS-based mobile payments is widely addressed on communication channel, payment device, and the payment server, but we accept these concerns as givens, as discussed in Section 6. Other possible concerns are the mis-typing of the information to the mobile phone which will cause incorrect payment or mismatching of the seller-buyer pairs, and the falsification of the agreed price.

Usability: Mobile payment must be as simple as possible, since payments are basic and everyday actions. In some cases, cash is easy to pay. However, it often involves calculating and handling the changes, which bothers us. Or it sometimes takes time to find appropriate coins from the wallet. Although the SMS-based mobile payment released us from such burden of the changes, it typically requires a series of key inputs such as the seller's phone number, which is not ideal for the F2FMP in comparison to cash [15].

In addition, cost, availability, and portability are also important concerns. However, since they depend on the strategy of the MNOs, pervasiveness, and the performance of the mobile phones, not on the performance of the payment protocols, we do not evaluate them in this paper.

3 Related Protocol

In this Section, we discuss a typical SMS-based mobile payment protocol, M-PESA. This protocol is not intended for a F2FMP, but is the closest existing payment protocol that can be compared with our proposal, since it uses SMS and completes a transaction using only a pair of mobile phones.

A typical SMS-based payment, M-PESA, transfers a value from a buyer's (B) account to a seller's (S) account using following four steps (Fig. 1):

(I) The B and the S agree on a price (p) for the purchase.

(II) The B sends an SMS message containing the p and the S's identification, such as a phone number, to the payment server (V), which typically knows the telephone numbers of the senders of the messages.

(III) The V confirms that the payment transaction is requested by the B. This involves checking the identities of both the B and the S, and testing some other parameters.

(IV) The V sends a confirmation message, which includes the p and the identities of the two parties, to both the B and the S.

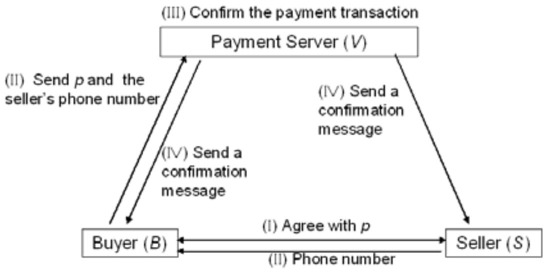

(III) Confirm the payment transaction
Payment Server (V)
(II) Send p and the seller's phone number
(IV) Send a confirmation message
(IV) Send a confirmation message
(I) Agree with p
Buyer (B)
Seller (S)
(II) Phone number

Fig. 1. Payment steps of M-PESA

4 Anonymous Face-to-Face Mobile Payment

In this Section, we propose a new protocol, an SMS-based anonymous F2FMP protocol, in which neither the seller nor the buyer needs to disclose their identities (Fig. 2). The main difference from the related protocol is that we use information uniquely associated with a transaction, such as the location and the time, and if necessary, the secrets only the pair of the seller and the buyer know, generated by our random number procedure, or the RN procedure hereafter, guarantee the anonymity and security. Also, our time shift procedure, or the TS procedure hereafter, improves the probability of correct pair-matching. Here are the steps:

(1) The B and the S agree on a price (p) for the purchase.
(2) The B and the S send messages containing the p to the V, respectively.
(3) The V collects all the messages from the sellers and the buyers received in the same time slot T_d, where d is a sequence number of each time slot as shown in Fig. 3 (a). The V first counts $N_s(d, c, p)$ and $N_b(d, c, p)$, the numbers of the messages which include only the price (p) received in the time slot T_d from the Cell ID c, from the sellers and the buyers, respectively. For pair matching, we introduce the TS procedure, which uses two buckets of time slots, D_1 and D_2, each shifted by $T/2$, as shown in Fig. 3, where T is the length of each time slot. We use these shifted time slots to avoid failing to find the pairs near the border of each time slot.

    If there is only one seller-buyer pair with the same price, the same location, and the same time, or $N_s(d, c, p) = N_b(d, c, p) = 1$, the V determines that the seller and the buyer are paired, so processing goes to Step (8). If not, then the Ss and the Bs go through the RN procedure, as described in Steps (4) to (7). For example, in Fig. 3 (a), S_j and B_j corresponds to the seller and the buyer and they are pair if j's are identical. In this case, $N_s(d, c, p) = N_b(d, c, p) = 1$ is satisfied for the pair of S_2 and B_2 at T_2.
(4) If $N_s(d, c, p) = N_b(d, c, p) = 1$ is not satisfied but $N_s(d, c, p) + N_b(d, c, p) > 0$ in Step (3), the V assigns one unique random number to each of the seller and the buyer that already existed in T_{d-1}. Then the V sends the assigned random number to each of the seller and the buyer. For example, in Fig. 3 (a), S_1, S_3, and B_1 are in T_1 and all of them already existed in T_0. Therefore,

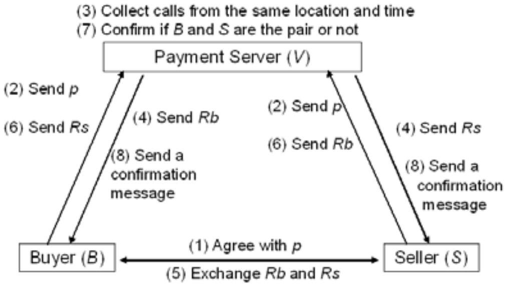
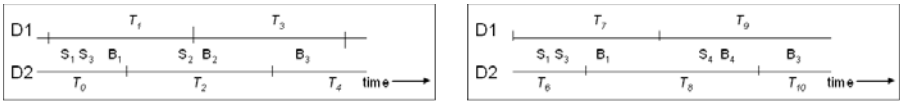

(3) Collect calls from the same location and time
(7) Confirm if B and S are the pair or not
Payment Server (V)
(2) Send p
(6) Send Rs
(4) Send Rb
(8) Send a confirmation message
(2) Send p
(6) Send Rb
(4) Send Rs
(8) Send a confirmation message
Buyer (B)
(1) Agree with p
(5) Exchange Rb and Rs
Seller (S)

Fig. 2. Payment steps of the anonymous face-to-face mobile payment



(a) At Step (4).

(b) At Step (7).

Fig. 3. Pair matching with the time shift procedure

random numbers are assigned to all of the three at T_1. As well, for B_3, a random number is assigned at T_4. S_2 and B_2 are already excluded in Step (3). None of the generated random number overlaps at least during $2T$, to avoid same random number being assigned to different buyer or seller.

Now random numbers R_b and R_s are assigned to the B and the S, respectively. The reason why the V needs different random numbers for both the B and the S, not only one random number for the S or the B, is discussed in the "Security" part in Section 6.

(5) The B and the S receive R_b and R_s, respectively, and exchange them.

(6) The exchanged random numbers are sent back to the V. This means the S and the B send R_b and R_s to the V, respectively.

(7) The V receives the messages with the random numbers. For each matching condition with the same time slot number d, the same Cell ID c, and the same price p, or (d, c, p) hereafter, the V first verifies the responses from the sellers and the buyers, respectively. If a same random number is included in two or more messages from the different buyers, the V excludes all of such buyers from the matching pairs. V also runs the same procedure for the sellers. The reason why the V excludes these is discussed in the "Security" part in Section 6.

After those are excluded, the V looks for a pair of response messages, $M_{bx} = (d, c, p, R_y)$ from the buyer B_x and $M_{sy} = (d, c, p, R_x)$ from the seller S_y, which satisfies $A(R_x) = B_x$ and $A(R_y) = S_y$, where $A(R)$ is the seller or the buyer that V assigns the random number R at Step (4). The V accepts such pairs as a real pair and continues with Step (8). For those sellers and buyers whose partner is not found, including those excluded earlier in this

Step, the V goes back to Step (4), by assigning new random numbers. At pair matching of this step, we also use two time slots as Step (4). Therefore, every seller or buyer has chances of pair-matching at two overlapping time slots. Fig. 3 (b) is an example of the time chart for a given (d, c, p). The B_2-S_2 pair matched at Step (3), and skips the RN procedure of Steps (4) to (7). In this case, B_1 and S_1 do not match at T_6 but match at T_7, and the V accepts them as a pair. As well, the B_4-S_4 pair matches at T_8, so the V accepts them as a pair. This pair also matches at T_9, but is already matched at T_8. B_3 and S_3 does not match in any time slot. Therefore, the transaction is unsuccessful and they must send the transaction request to the V again.

If the number of retries is greater than N_r, where N_r is maximum number of retries for some users, then the V terminates the transaction for such users. In such cases, the V should investigate the reasons, such as a malicious user among the sellers and the buyers involved in the matching attempts, and if malicious users are identified, then the V will exclude such users for the F2FMP from the next time.

(8) Now that a pair has been recognized, the V sends a confirmation message to each member of the pair. The confirmation message includes the values of d, c, p, and a unique random number that is exclusively common between the seller-buyer pair, so that the pairs can confirm that they are correctly matched.

The protocol above does not include the steps to match pairs in adjacent Cells. If the paired S and B are located at the border of a Cell ID, either or both of the seller and the buyer may fail to belong to the same Cell ID. However, the area covered by each Cell is normally duplicated to avoid the existence of the non-covered areas, so, even for such a case, they should belong to one or more same Cell IDs. If the V finds the same pairs with the same d and p at different Cell IDs, they should accept them only in one Cell ID.

5 Experimental Results

To evaluate the feasibility of the F2FMP, some concerns, e.g. some attacks for security, can be evaluated by an armchair theory as discussed in Section 6. However, it is not good enough for complete evaluation. In a sense, feasibility of the F2FMP should be evaluated both by the experimental results and the armchair theory.

In this Section, we report the results of two experiments which evaluate the anonymity, security, and usability, that cannot be evaluated just by an armchair theory: Experiment (a) evaluates of the probability of the pair-matching failure for anonymity and security, and Experiment (b) evaluates of the probability of skipping the RN procedure for usability.

We select Experiments (a) and (b) because the pair matching is the fundamental concern for our proposal, and because skipping the RN procedure most contributes to improve the usability, respectively.

Other concerns, such as some attacks for security, will be evaluated by discussion in Section 6.

For both of the two experiments, we simulate the case that both the Cell ID (c) and the agreed price (p) are the same for all the users. This can be possible in several cases, e.g. in the bargain sale with a same price, discount food shop at lunch time, in street stalls, especially in Asian countries, and so on. The following [1] to [4] show our assumptions:

[1] The occurrence of the payment transactions within a given time slot at a given location follows a Poisson distribution as

$$P(N = k) = e^{-\lambda}\lambda^k/k!, \tag{1}$$

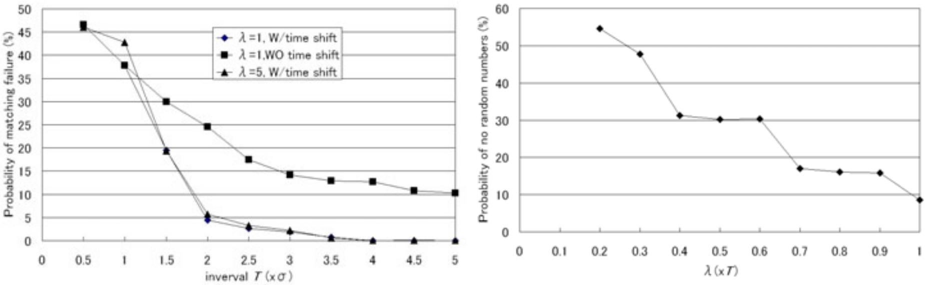
where $P(N = k)$ is the probability that the mobile payment transactions take place k times in a given unit time slot, e.g. one minute, and λ is a parameter of the expected number of transactions during the given time slot.
[2] The probability density function of the delay time t from a pair agreed on the price till V receives the random numbers from the B or the S, i.e. from Steps (1) to (3) follows normal distribution as

$$f(t - \mathit{\Delta} t) = \frac{2}{\sqrt{2\pi}\sigma}\exp(-\frac{(t-\mathit{\Delta} t)^2}{2\sigma^2}), t \geq \mathit{\Delta} t, \tag{2}$$

where $\mathit{\Delta} t$ is a minimum time delay, and σ is a parameter for the time delay.
[3] The delay from a seller-buyer pair exchange the random numbers till the random numbers arrive to the V, i.e. from Steps (5) to (7), follows Eq. (2) as well since both cases involves a single-way transaction from a seller or a buyer to the server.
[4] No congestion of SMS takes place.

We simulate both Experiments (a) and (b) by generating the mobile payment transactions with the probability in Eq. (1) with the delays in Eq. (2), each for the time period of $1000T$. Fig. 4 (a) shows the result of Experiment (a). In this experiment, we change T (x-axis) as the multiple of σ with $\lambda = 1$ and $\lambda = 5$, and calculate the probability that the pairs are not successfully matched (y-axis). We do not count the case of RN procedure being skipped. We also compare the results with and without the TS procedure (W/time shift and WO time shift in Fig. 4 (a)). We regard the mobile payment is successful if both the S and the B of a pair stay within a same time slot of T_d for some d without retries. Unsuccessful pair matching takes place when the difference of the delays of the seller and the buyer between Step (5) to (7) causes their messages arrive in different time slot. From this result, we find that the probability of matching failure is zero when $T \geq 4\sigma$ regardless of the value of λ. We also find that the TS procedure is effective, since we observe approximately 15% of matching failure without the TS procedure while 0% with the TS procedure at $\lambda = 1$.

Fig. 4 (b) shows the result of Experiment (b). In this experiment, we evaluate the probability to skip RN procedure (y-axis) by changing the value of λ as multiple of T (x-axis). To calculate the probability above, we count the number



(a)Prob. of matching failure

(b)Prob. of skipping the RN procedure

Fig. 4. Experimental results

of the seller-buyer pairs which satisfy $N_s(d, c, p) = N_b(d, c, p) = 1$ with some d. $N_s(d, c, p) = N_b(d, c, p) = 1$ is not satisfied when the occurrences of the mobile payment transactions are frequent enough, or, even if transactions are not frequent, when the difference of the delays of the seller and the buyer between Step (1) to (3) is so large that the messages with the price do not arrive to the V in the same time slot. From this result, we find that when the occurrences of the mobile payment transactions are rare, e.g. $\lambda = 0.2T$, more than 50% of the pair matching can be done without RN procedure, but we need RN procedure with the probability of more than 90% when $\lambda \geq T$. Therefore, we can increase the probability of completing the payment transactions skipping the RN procedure by optimizing T according to the value of λ.

6 Discussion

In this section, we evaluate the proposed protocol based on the criteria discussed in Section 2, by comparing them with the related protocol:

Anonymity: For M-PESA, the sellers must disclose their phone numbers. In the proposed protocol, neither the seller nor the buyer needs to disclose the phone number, and the results from Experiment (a) prove that the pairs can be matched correctly without disclosing phone numbers by optimizing T.

At other times, people may be willing to disclose their identities to some extent. For example, the sellers may wish to disclose their shop name only, but not their phone numbers, to avoid some nuisance phone calls. Another case is that the sellers may wish to disclose their identities, perhaps by giving out receipts or business cards. The other case is that the buyers may wish to disclose some identities, such as in their favorite restaurants, shopping malls, or movie theaters, where they may have customer loyalty cards today and receive benefits as frequent customers. They will allow the sellers to analyze their purchase histories under certain conditions [16,17,18]. Therefore, we believe both the sellers and the buyers should be able to negotiate and control the level of anonymity depending on the payment situation. In that sense, there are typically three levels of anonymity appropriate to the payment types and amounts:

Case (1): Full exposure (e.g. M-PESA discussed in Section 3): The key information is disclosed, including the telephone number, name, and address.

Case (2): Partial anonymity: No information is disclosed but some ID other than the telephone numbers, e.g. shop names or nicknames.

Case (3): Full anonymity (e.g. our proposal discussed in Section 4): No information is disclosed.

We now describe the example of Case (2) since Case (2) is not discussed so far. An example is that in the F2FMP, the buyers do not get the sellers' phone number, but they get the possible list of the shops located near the buyers, which may be displayed on their mobile phones' display, then select the shop names to which they pay money from the list. One way to achieve Case (2) is to modify Step (4) and later of the proposed protocol to send such lists from the V to the B and the B sends back the seller's shop name to the V. In this case, Step (1) may be skipped.

If we support all of the three cases above, both the sellers and the buyers can select the anonymity level depending on their preference.

Many users may want to remain anonymous even from the payment server, the same way that cash payments can not even be traced by banks. Regarding this issue, we accept the anonymity, as well as security, of the payment server is given, as discussed in the next paragraph.

Security: First, we discuss the security of the communication channel and so on, then the comparison results between the related protocol and our proposal. We accept the security of the communication channel, the device hardware, and the servers are given. Regarding channel security, we can apply "Onion Routing" [19] that encrypts the messages including the IP headers. Regarding device security and server security, we can validate the software stack running on both servers and client devices by using the Trusted Platform Module (TPM)'s attestation feature, before the secure communication is established [20,21]. We can also apply Homomorphic Encryption [22] for server security.

For M-PESA, only the buyers input the agreed price. Therefore, if they falsify or mis-type the price, it would take time for the sellers to notice the injustice or the mistake, or they may not notice. In our protocol, since both the sellers and the buyers have to input the agreed prices, the matching will fail in such injustices or mistakes.

Regarding the risk of payments between a mismatched pair, we experimentally demonstrated how to minimize this risk without sacrificing the usability by studying the number of the payments and the communication delays. The nice property of the proposed protocol is that even if a matching fails, users can retry the F2FMP.

Other than the risk above, we studied the following two major possible attacks that could be directed against the sellers or the buyers.

The first attack by a seller would be to seek double payments from a buyer by claiming that the money had not yet been paid to the seller. For example, a malicious seller S prepares two mobile phones, M_1 and M_2. The S initiates the F2FMP as discussed in Section 4 using M_1, but at Step (8), the S could tell the buyer B that the payment has not been completed, by switching the phones to show the display of M_2. This attack would be possible when the server V generates only one random number, e.g. to the B, and the process requires only the S to return the random number sent to the B. However, in the proposed protocol, since each of the S and the B receives different random number and exchange them, V detects the injustice by the process of Step (7).

The second attack would involve stealing the random number from the buyer by some methods, impersonating the seller, and then trying to steal the buyer's payment. For example, when a legitimate seller-buyer pair S_1 and B_1 exchange their random numbers, and a hacker S_2 tries to impersonate S_1 to get the money from B_1 stealing the random number of B_1, and sends the random number to the server V. However, in this case, the V will not match the pair since the V will have received two messages with the same random number R_b from different sellers. The V will block such pairs and ask for a retry, as described in Step (7). If many of these retries occur, the V can contact the sellers that are frequently sending messages with duplicated R_b values and the V will exclude such malicious sellers from the next time.

Usability: For M-PESA, each buyer must input at least the agreed price and the seller's telephone number. In contrast, although each seller and buyer must input the agreed price for the proposed protocol, the buyer need not input any telephone number, which is usually around ten digits. Instead, the buyer may have to input random numbers.

However, in the experiment, we found that, by choosing the appropriate T depending on λ, we could minimize the necessity of inputting random numbers. Even if we have to input random numbers, the digits can be small. Random numbers are generated only for pairs whose Cell ID, time slot, and the agreed price are all the same. Also, for a random number, we can use alphabets of large and small capitals, and numeric numbers, which is 62 in all. Therefore, we need to input only $\log_{62}(2N-1)+1$ digits for N pairs, and even if $N = 100,000$, we need only three digits. In actual cases, such large number of pairs would be very rare. We may want random numbers sparse enough to avoid a random number assigned to another person which causes mismatching. In this case, we will need to add only one or two additional digits which will make the distribution of the random numbers 62 or 3844 times sparser. Therefore, it is expected that the digits of the random numbers we have to input would be at most between two to five.

Taking these discussions into consideration, we can improve not only anonymity, but security and usability compared with M-PESA.

So far, we discussed the protocol for the F2FMP that uses SMS. However, there are several alternative methods to improve the usability while guaranteeing the anonymity and security, if the mobile phones have more functionality. For

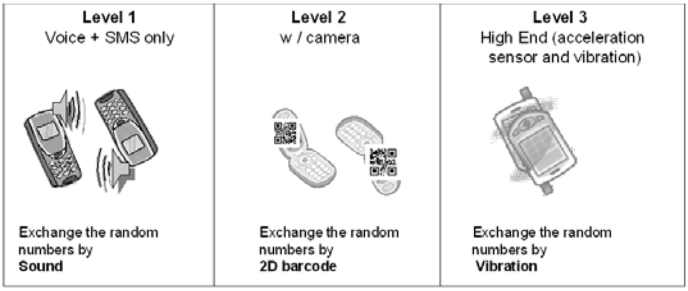

Level 1
Voice + SMS only
Exchange the random numbers by Sound
Level 2
w / camera
Exchange the random numbers by 2D barcode
Level 3
High End (acceleration sensor and vibration)
Exchange the random numbers by Vibration

Fig. 5. Methods to exchange the random numbers with high end mobile phones

example, we can convert random numbers to sounds, barcodes, or vibrations, and exchange them, by capturing them with the mobile phones of the pair as shown in Fig. 5. To use barcodes or vibrations, the mobile phones of both users need to have cameras or acceleration sensors, as appropriate.

Instead of using random numbers, we can use the background noise, music, or image, to identify the pair. If the V can confirm that a pair of mobile phones are located close to each other, then the V can use that information, instead of or in addition to the Cell IDs, and match the pair for the transaction without using random numbers.

We may not have to input even p by taking photos of the price tag, if such an application is installed to the mobile phones.

7 Conclusion

In this paper, we introduced a F2FMP protocol in which the anonymity of both the buyers and the sellers is guaranteed. The technical contributions of the proposed protocol are the use of unique information, such as the same location and the time, and our TS and RN procedures for optimization. The random numbers used in our RN procedure and the time shift used in our TS procedure guarantee the anonymity and security of both the seller and the buyer. As well, the optimization to skip the RN procedure when possible improves the usability. We evaluated the proposed protocol from two points of view, pair matching failure and skipping the RN procedure, and showed that the proposed protocol is practical and offers advantages over the existing protocol. We also discussed methods for the F2FMP considering the capabilities of the mobile phones, showing that mobile phones with more features can improve the usability of the F2FMP. We believe that the proposed F2FMP protocol is attractive for both the sellers and the buyers for the protected anonymity, as well as easy and safe payment without carrying cash. We also believe our F2FMP protocol will further contribute to promote a cashless world, and a more effective digital economy.

References

1. Hammond, A., Kramer, W.J., Tran, J., Katz, R., Walker, C.: The Next 4 Billion: Market Size and Business Strategy at the Base of the Pyramid. World Resource Institute (2007)
2. United Nations Conference on Trade and Development, Information economy report 2007-2008 Science and technology for development: the new paradigm of ICT (2008)
3. Morawczynski, O., Miscione, G.: Examining Trust in Mobile Banking Transactions in Kenya: The Case of M-PESA. In: IFIP WG 9.4-University of Pretoria Joint Workshop, Pretoria, South Africa (2008)
4. Vaughan, P.: Providing the Unbanked with Access to Financial Services: The Case of M-PESA in Kenya, Presentation given during the Mobile Banking & Financial Services Africa Conference, Johannesburg, South Africa (2008)
5. Hughes, N., Lonie, S.: M-PESA: Mobile Money for the 'Unbanked': Turning Cellphones into 24-Hour Tellers in Kenya. MIT Press Journal, Innovations: Technology, Governance, Globalization 2(1-2), 63–81 (2007)
6. Mas, I., Morawczynski, O.: Designing Mobile Money Services Lessons from M-PESA. MIT Press Journal, Innovations: Technology, Governance, Globalization 4(2), 77–91 (2009)
7. Safaricom M-PESA, `http://www.safaricom.co.ke/index.php?id=745`
8. Voda M-Pesa, `http://www.vodacom.co.tz/docs/docredir.asp?docid=3518`
9. Zain Kenya Me2U,
   `http://www.ke.zain.com/en/phone-services/me2u/index.html`
10. Starcomms DashMe, `http://www.starcomms.com/v_dashme.php`
11. MTN MobileMoney Account, `http://www.mtnbanking.co.za/`
12. eTranzact, `http://www.etranzact.com/Web/index.htm`
13. GSMA, `http://www.gsmworld.com/`
14. Pay-Buy-Mobile Business Opportunity Analysis – Public White Paper Version 1.0, GSMA Association (2007)
15. Medhi, I., Gautama, S.N.N., Toyama, K.: A comparison of mobile money-transfer UIs for non-literate and semi-literate users. In: Proc. of ACM Conference on Computer Human Interaction (CHI), Boston, USA, pp. 1741–1750 (2009)
16. Karnouskos, S., Hondroudaki, A., Vilmos, A., Csik, B.: Security, Trust and Privacy in the SEcure MObile Payment Service. In: 3rd International Conference on Mobile Business, New York City, USA (2004)
17. Linck, K., Pousttchi, K., Wiedemann, D.G.: Security Issues in Mobile Payment from the Customer Viewpoint. In: Ljungberg, J. (Hrsg.) Proc. of the 14th European Conference on Information Systems, Gteborg, Sweden, pp. 1–11 (2006)
18. Lu, C.T., Liang, L.R.: Analysis of payment transaction security in mobile commerce. In: Proc. of the IEEE International Conference on Information Reuse and Integration, pp. 475–480 (2004)
19. Anderson, R.: Hiding Routing Information. In: Anderson, R. (ed.) IH 1996. LNCS, vol. 1174, pp. 137–150. Springer, Heidelberg (1996)
20. Trusted Computing Group, Trusted Platform Module,
    `http://www.trustedcomputinggroup.org/developers/trusted_platform_module`
21. Trusted Computing Group, Mobile Phone Work Group Mobile Trusted Module Specification, Version 1.0,
    `http://www.trustedcomputinggroup.org/resources/`
    `mobile_phone_work_group_mobile_trusted_module_specification_version_10`
22. Homomorphic Encryption, `http://ja.wikipedia.org/wiki/`