ICEB 2007 Proceedings

International Conference on Electronic Business (ICEB)

Winter 12-2-2007

Peer to Peer Mobile Coupons: Adding Incentives without Sacrificing Security

Sue-Chen Hsueh

Jun-Ming Chen

Proceedings of The Seventh International Conference on Electronic Business, Taipei, Taiwan, December 2-6, 2007, pp. 204-210.

PEER TO PEER MOBILE COUPONS: ADDING INCENTIVES WITHOUT SACRIFICING SECURITY

Sue-Chen Hsueh, Chaoyang University of Technology, Taiwan, schsueh@cyut.edu.tw
Jun-Ming Chen, Chaoyang University of Technology, Taiwan, s9514604@cyut.edu.tw

ABSTRACT

Mobile commerce is flourishing today due to the advance of the mobile technology. Many conventional marketing activities are moving their ways to the mobile environment. Efficient marketing instruments such as the paper coupons and the electronic coupons are also evolving into the mobile coupons. In comparison with conventional coupons, mobile coupons are personalized and suitable for peer to peer delivery. Coupons are commonly issued by the merchants, used by the interested customers, and discarded by the uninterested receivers. Raising the redemption rate of the coupon will increase the sales of the promoted items. The raise can be accomplished by forwarding coupons from uninterested receivers to potentially interested customers. The ease-of-use exchange mechanism in mobile devices pushes the delivery in the peer to peer environment. Moreover, the characteristic of personalization inspires trust into mobile coupons. Thus, adding the incentives of coupon forwarding, such as a reward bonus, may activate the movement of stationary coupons and eventually increase the redemption rate of mobile coupons. Nevertheless, the incentives adding may bring the threats of alterations and forgery; if the adding mechanism is improperly made. Additionally, complicated security means are hindered by the limitations of storage space, computation power, and communication bandwidth of mobile devices. Therefore, we propose a scheme that uses digital signatures for verifying the incentive-added coupons and design a hash chain to detect possible forgery. The proposed scheme may increase the use of peer to peer mobile coupons without sacrificing the security.

Keywords: Electronic commerce, mobile coupon, peer to peer, security.

INTRODUCTION

Coupons have long been used as a powerful instrument in marketing and are presented in different forms in the information age. Electronic coupons (E-coupons) are commonplace now to be downloaded, printed, and used as traditional paper coupons. A modern substitute of the paper coupon, or e-coupon, is the appearance of the mobile coupon, which can be transmitted and used on-the-go. The potential of mobile coupons for sales promotion is promising due to the convenience of coupon issuing and redemption.

In general, e-coupons are published in the Web for free downloading and printing before redemption in a physical store. The merchant constructs a coupon downloading Web-page and saves the dispatching of coupons. Nevertheless, the additional costs of searching and printing for the consumers are introduced, not to mention the willingness to surfing the Web for coupons. The alternative of emailing e-coupons is easy for both the issuer and the receiver but the probability of being treated as spam mails and discarded could be high. Moreover, the need-to-printout e-coupons is hard to remember and less portable in use. Although e-coupons are popularly used as an advertising tool with the prevalence of Email and Web, its usage is still limited.

Mobile coupons are electronically issued from a merchant to the mobile devices of targeted customers. Mobile devices are generally considered as personal devices for the portability and availability today. Hence, mobile coupons are just right at hand while using without having to be printed out in advance. In addition, mobile coupons are suitable for peer to peer delivery since the ad hoc communication capability is built-in for most mobile devices. The ease-of-exchange mechanism may push the delivery of mobile coupons a step further in the peer to peer environment. Furthermore, recommendations of the coupon-promoted products from friends through their mobile devices represent certain trust so that the potential of coupon redemption is increased. The movement of the stationary coupons can be activated and the redemption rate of the coupons is raised eventually. Thus, the effect of word-to-mouth marketing can be achieved via mobile message sending. The value and the practice of the mobile coupon can be increased within the community of the mobile coupon receiver, provided that certain incentives are rewarded to the coupon forwarder.

A bonus point model was proposed in [7] that adding the incentives to the e-coupons in the mobile environment. When the providers send out e-coupons, which are passed from user to user, they may receive bonus points if the coupon is redeemed. A general model and an optimal strategy for users to determining the claiming bonus points were presented in the paper. However, the protection mechanism and the integrity of the incentive-added coupon were not addressed. Now that the coupon bears potential bonus, an alternation or forgery of the forwarding history, and even the coupon itself, is greatly possible. Extending mobile coupons with assured security that can protect the value of the coupon and reward bonuses to the actual forwarders is desirable as a result.

Therefore, we propose a scheme that adds incentives to the peer to peer mobile coupons without sacrificing the security. The contents of the coupon, including the incentive and forwarding history, need to be protected. Most systems use asymmetric key cryptosystem to fulfill the security requirements. However, the storage capacity and computing power of most available mobile devices are too limited to perform asymmetric key cryptosystem. Thus, we use the digital signatures for the integrity verification of the mobile coupons. A hash chain is designed to detect any possible forgery of the incentive-added coupon. The proposed scheme may increase the redemption and promotion effect of the peer to peer mobile coupons, with the security assured incentives.

RELATED WORK

Peer to Peer Environment

Forwarding electronic coupons without proper identifications usually are considered as spam [11]. Random spreading of coupons thus will not occur in the P2P environment since the parties in the environment is trusted in general. In comparison with broadcasting electronic coupons in traditional client/server models, mobile users may find the peers more easily, so that forwarding mobile coupons can be conducted effectively in the P2P environment, especially with the trusted interactions. Furthermore, the P2P mobile coupon has an intrinsic property of interpersonal interactions so that the receiver will have more confidence on using the received coupon. A coupon received from the forwarding of known persons generally will not be ignored by the receivers. The promotion thus will be more likely successful in such a forwarding of coupons. The redemption rate will be increased since the forwarding is intentionally made by the forwarder, who knows more about the potential receivers. However, a mobile user who participates in the P2P environment has to provide his/her resources, e.g. the storage space of the mobile devices, the bandwidth of communications, and the required computations [7]. To activate the volume usage of this operation, lightweight computations are preferred. In the proposed scheme, each mobile user needs to pay the transmission cost only once. Fair bonuses are rewarded to those who have participated in the forwarding of the mobile coupon in the P2P environment.

The Incentive Mechanism

The e-coupon may promote the sales not much without proper targeting of the potential customers. Not every receiver of the e-coupon is a consumer. Without incentives, the receiver generally discards the e-coupon so that the promotion effect is limited. If we can provide incentives to the forwarder of the coupon, the receiver who has no intention to use the coupon might transfer the coupon to who will potentially use the coupon. That is, to encourage the forwarding of the previously stationary coupons, incentives have to be added to the coupon forwarders. Therefore, the incentive mechanism can promote the redemption rates of the e-coupons and reduce the possibility of the stationary e-coupons.

Kangasharju and Heinemann proposed an incentives mechanism for e-coupon system [7]. In the mechanism, the incentives will be offered to the forwarder, e.g. frequent flyer miles are rewarded after the e-coupon is redeemed. The mechanism emphasizes on the distributions of the incentives. The total amount of incentives is set in the initial phase. Each forwarder can take at least one bonus point. No forwarding is allowed if the bonus point is just one point. In the proposed scheme, the incentive can be offered is depend on the agreement between the provider and the merchant, and set up in the initial phase.

Shojima and Ikkai, and Komoda proposed an incentive mechanism for P2P e-coupon system. In that mechanism, each e-coupon can record the information about the forwarder becomes distribution history information [11]; according to the distribution history can easily computes the incentive can be obtained for each forwarder. The distribution history is the basis information for the incentive mechanism, hence must be protected [12]. Shojima et al. adopt the asymmetric key encryption and computation the hash value, and embed the hash value into the image as digital water mark to protect the basis information.

The Electronic Coupon

The electronic coupon is an efficient instrument for advertisement and marketing when developing electronic commerce [6]. Advertising is considered an effective manner to promote the commercial affairs; however, promotion means stimulate the amount of purchase is a familiar and efficient manner of advertising. Any consumer can have a discount or additional gift when he/she use the e-coupon to purchase the advertisement merchandise. According to the viewpoint, the e-coupon is an instrument of marketing to stimulate the amount of purchase and attach the advertisement value.

Currently, the actual exercise of the e-coupon needs the consumer prints it, and redeems in the realistic store [1], or directly redeems in the virtual store on the internet [2]. Nevertheless, the amount of the redeemed e-coupon will influence the profit of the merchant; the appropriate amount of the redeemed e-coupon can make the maximum profit to the store. Contrarily, the excessive amount of the redeemed e-coupon might reduce the profit or even make a loss. Due to the electronic information can easily make a duplicate; but in order to make the maximum profit must control the amount of the published e-coupon, hence, in this kind of research prevent double-redemption is the preferential considering and then control the amount of the redeemed e-coupon smaller than the published amount. Nevertheless, since the e-coupon is an implement to help with complete the transaction of the merchandise or service; hence prevent the included contents information be altered is the main purpose. Currently, majority of this kind of research utilize the asymmetric key cryptosystem to protect the contents of the e-coupon from the alteration; or through the third party to do encryption and verification; by way of the mechanism also can detect the double-redemption.

However, the mobile coupon is applied to the mobile devices. On the mobile devices operate the asymmetric key cryptosystem is a heavy load; or by the method of through the third party will increase the cost of transmission medium for the mobile user. Chang and Wu, and Lin proposed a secure e-coupon system for mobile users [4]. Though the design construct with the hash function just needs the simple computation, but in the forward phase needs the third party to do the verification and redesign the coupon for the new receiver to complete the forwarding action; this mechanism not match the main spirit of the P2P: the sharing between the peer to peer. Shojima et al. proposed mechanism, though apply to the P2P mobile environment; but operate the RSA public key cryptosystem needs compute the large amount of factorizations on the mobile devices; however, the computation of the mobile devices is very weak; hence, the efficacy of the actual operation needs to examine. Therefore, the proposed scheme modifies the concept of the hash chain from the electronic payment system [9][10], and adopts the skill of digital signature to protect the mobile coupon to attain the excellent efficacy.

THE PROPOSED INCENTIVE ADDED MOBILE COUPON SCHEME

The proposed scheme enables the mobile coupon to be used in the P2P environment and to have incentives added, with the consideration of the limitations of the mobile devices. The components of the mobile coupon are shown in Figure 1. The *Coupon* represents a delivered coupon in the transmission. The *C* represents the identity of the mobile coupon and having the details about the coupon. The *SN* is the serial number, such as M00009183, on the mobile coupon. The amount of published mobile coupons can be controlled by the *SN*. The ID_R represents a merchant, such as CYUT 3C, who can accept the mobile coupon. The P_{ID} is the content about the merchandise, such as CYUT 22" LCD (FP 222 W). The *Discount* records the discount such as 20% off. Finally, the *EXD* is the expiration of the mobile coupon, such as 2007/12/31. Table 1 presents the notations used in this paper. A mobile coupon is described as *Coupon C*{ *SN*, ID_R,P_{ID}, *Discount*, *EXD* }.

The Framework of The Mobile Coupon System

Figure 2 depicts the proposed scheme utilizing digital signatures and hash chains. The mobile coupon provides with an incentive added in P2P environment. In the framework, the merchant (*M*) and the mobile coupon provider (*P*) define the settings and the parameters of the mobile coupon initially. Then, the mobile coupon provider establishes the database to record the status of the mobile coupon and delivers the mobile coupon to the target mobile users (MU_i). The mobile user may either redeem the mobile coupon or forward it to another mobile user. If the mobile user redeems the mobile coupon from the merchant, the merchant will use the database to verify the validity of the mobile coupon. If the mobile user wants to forward the mobile coupon to another mobile user, the mobile user will add his/her digital signature, compute the corresponding *R* value, and combine both with the mobile coupon. In this way, the receiver can verify the coupon upon receiving. The mobile user can use the hash function to compute the R_{i+1} from the R_i, but cannot use the reverse engineering to compute the R_{i-1}. With regard to the protection of the mobile coupon, the mobile coupon provider (*P*) uses another hash function H' to compute the H'(R_0) from the R_0, and the value will be a proof of the verification. The detection of alteration and the query of incentives can be efficiently performed. The participated mobile users are assumed to have registered and own the key pair in the proposed scheme.

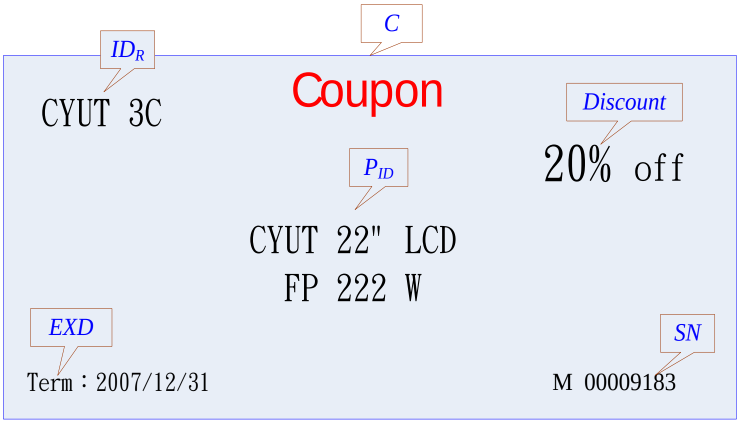

FIGURE 1: Illustration of a Coupon

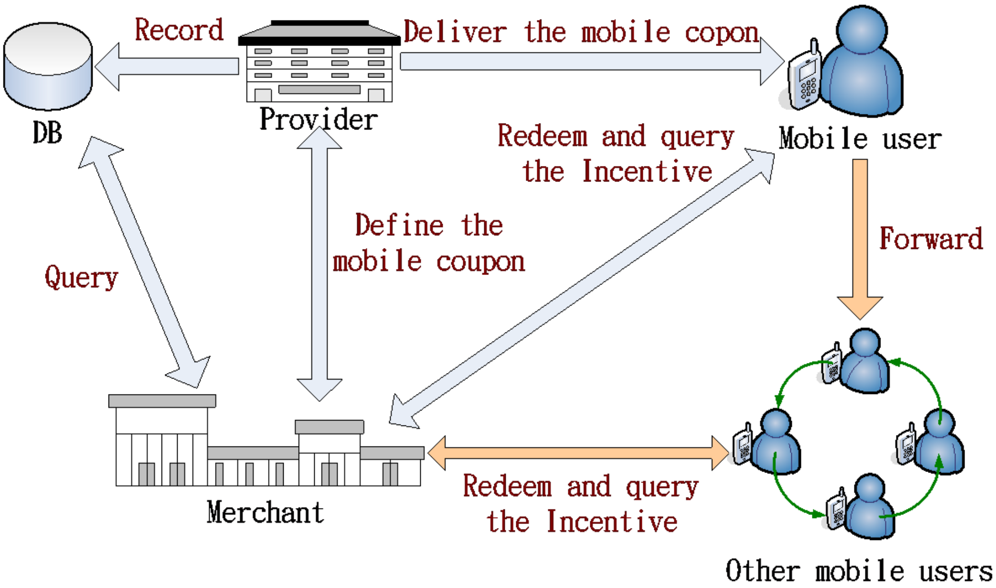

FIGURE 2: The Framework of the Incentive Added Mobile Coupon in P2P Environment

TABLE 1: Notations Used in this Paper

Notation	Representational content	Notation	Representational content
C	Coupon	S_i	The signature of *i* ※ i=*MU1~MUn, P, R*
P	Provider of the mobile coupon	PK_i	The public key of *i* ※ i=*MU1~MUn, P, R*
M	Merchant	SK_i	The private key of *i* ※ $i=MU_1 \sim MU_n$, *P, R*
MU	Mobile user	H( )	One way hash function
IDi	The identity of *i* ※ $i=MU_1 \sim MU_n$, *P, R*	H'( )	Another one way hash function
R_0	Random number	S	The process of signing
$R_1 \sim R_n$	Seed chain	| |	Connection

Issuing Phase Of The Mobile Coupon

The *P* generates a coupon and a random number R_0. Using another one way hash function, the value of H'(R_0) is computed and combined with *C*, then were signed using the digital signature S_P, by the SK_P on the mobile coupon. The random number R_0 also computes the value of R_1 through the one way hash function. Finally, they are combined into a mobile coupon to be delivered to the mobile user. The process is shown in Figure 3.

Forwarding Phase Of The Coupon

When MU_1 obtains the mobile coupon from *P*, he/she might redeem it or forward it to another mobile user to gain some incentives eventually. Assume that the MU_1 wants to forward the mobile coupon to his/her friend who might redeem the coupon, he/she may forward the mobile coupon to MU_2 via MMS (Multimedia Messaging Service) bluetooth, or infrared ray; as presented in Figure 4. The MU_1 computes his/her digital signature S_1, and computes the R_2 using the one way hash function from R_1, and embeds them into a mobile coupon to be delivered to MU_2.

When the MU_2 receives the mobile coupon from MU_1, he/she will use the attached PK_P to verify the digital signature S_P, and uses the attached PK_1 to verify the S_1. Finally, he/she compares the R_2 to the output computed from R_1 by the one way hash function. The mobile coupon is secure and valid if the result is equal. MU_2 may forward the coupon and obtain certain reward bonus if he/she has no desire to redeem. The procedures of signing the digital signature and generating the R_3, for the third receiver and beyond, are similarly performed.

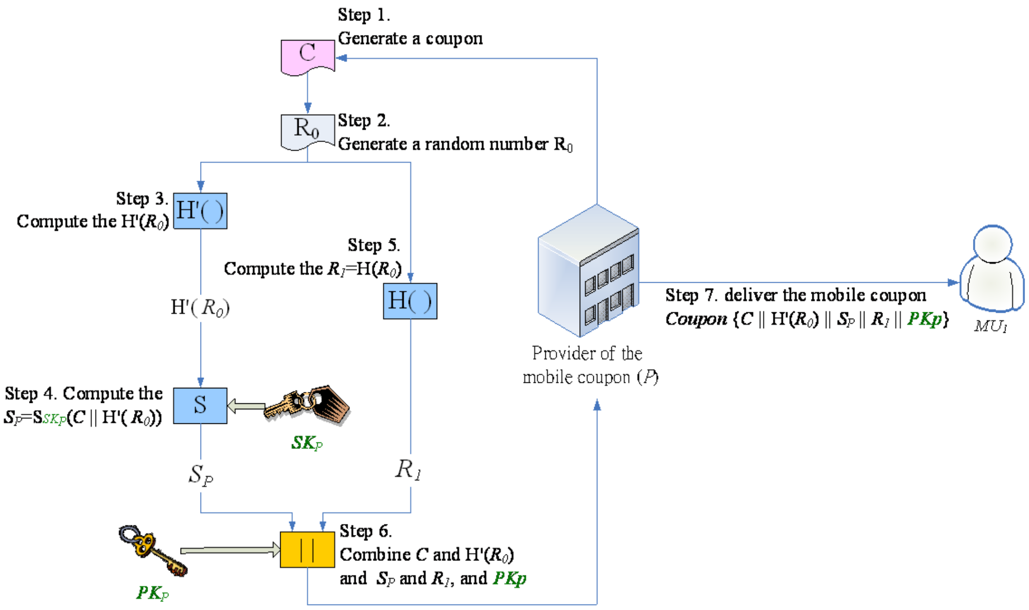

FIGURE 3: The Mobile Coupon Issuing Phase

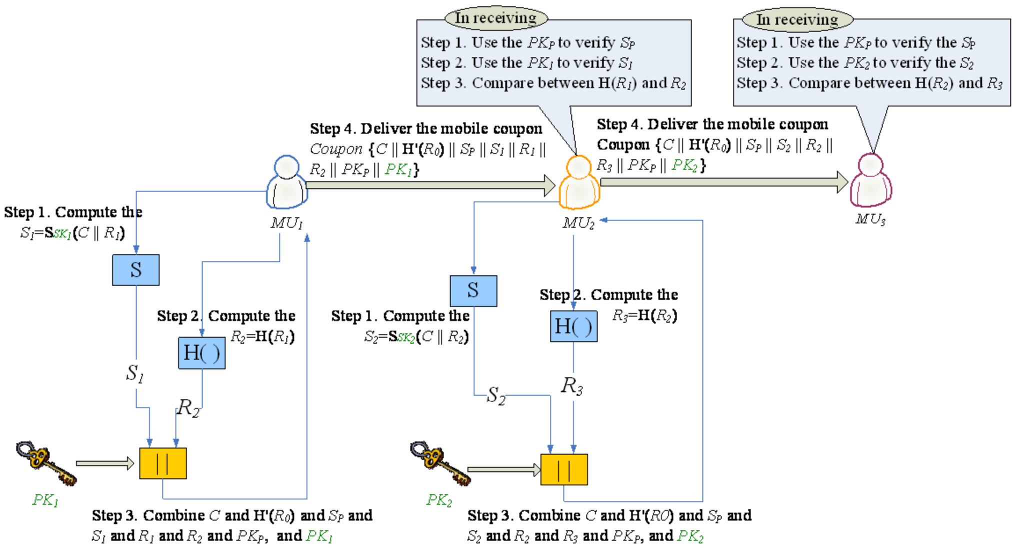
In receiving
Step 1. Use the PK_P to verify S_P
Step 2. Use the PK_1 to verify S_1
Step 3. Compare between H(R_1) and R_2
In receiving
Step 1. Use the PK_P to verify the S_P
Step 2. Use the PK_2 to verify the S_2
Step 3. Compare between H(R_2) and R_3
Step 4. Deliver the mobile coupon
Coupon {C ‖ H'(R_0) ‖ S_P ‖ S_1 ‖ R_1 ‖ R_2 ‖ PK_P ‖ PK_1}
Step 4. Deliver the mobile coupon
Coupon {C ‖ H'(R_0) ‖ S_P ‖ S_2 ‖ R_2 ‖ R_3 ‖ PK_P ‖ PK_2}
MU_1
MU_2
MU_3
Step 1. Compute the
S_1=S$_{SK_1}$(C ‖ R_1)
S
Step 2. Compute the
R_2=H(R_1)
H( )
S_1
R_2
||
PK_1
Step 3. Combine C and H'(R_0) and S_P and S_1 and R_1 and R_2 and PK_P, and PK_1
S
Step 1. Compute the
S_2=S$_{SK_2}$(C ‖ R_2)
Step 2. Compute the
R_3=H(R_2)
H( )
S_2
R_3
||
PK_2
Step 3. Combine C and H'($R0$) and S_P and S_2 and R_2 and R_3 and PK_P, and PK_2

FIGURE 4: The Mobile Coupon Forwarding Phase

Redemption Phase Of The Coupon

Figure 5 shows the redemption phase. The mobile coupon is forwarded to a redeemer MU_n, who stops forwarding and proceeds to the redemption phase. If MU_n decides to redeem the mobile coupon upon receiving of the mobile coupon, MU_n will present the mobile coupon to the merchant. The merchant will verify the embedded digital signature, and the value of R_n in the mobile coupon. The merchant also verifies by computing the output through the one way hash function from R_0 and comparing the result with the R_n. The mobile coupon is not altered and the information integrity is preserved during the forwarding phase if both values are equal. That is, the mobile coupon is valid for redemption.

After verifying the mobile coupon, the merchant examines whether the mobile coupon is redeemed. If the mobile coupon has not been redeemed yet, the merchant will provide the recorded discounts or services on the mobile coupon for the redeemer, and record the redemption status of the mobile coupon. Otherwise, a double-redemption message is sent to MU_n.

Querying Phase Of The Coupon

The MU_i has forwarded the mobile coupon, then he/she might want to know the amount of reward bonuses. The MU_i delivers the forwarded mobile coupon to the merchant to query whether the mobile coupon was redeemed and the amount of the bonuses. Figure 6 details the procedures. The merchant receives the query and examines the redemption status of the coupon. If the mobile coupon was redeemed, the incentive (bonus) is computed according to the record in the database and returned to the mobile user. The user will receive no bonus if the mobile coupon is not been redeemed yet.

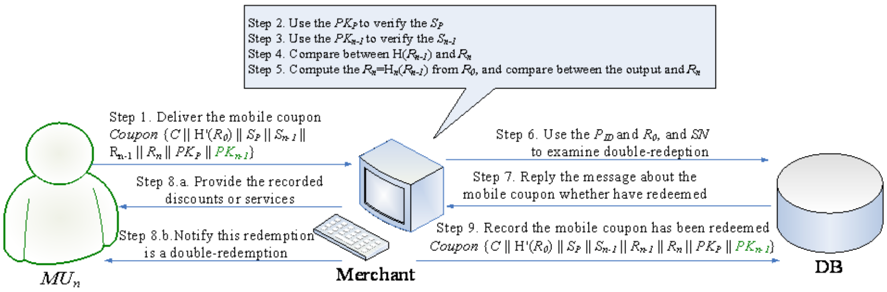
Step 2. Use the PK_P to verify the S_P
Step 3. Use the PK_{n-1} to verify the S_{n-1}
Step 4. Compare between H(R_{n-1}) and R_n
Step 5. Compute the R_n=H$_n$(R_{n-1}) from R_0, and compare between the output and R_n
Step 1. Deliver the mobile coupon
Coupon {C ‖ H'(R_0) ‖ S_P ‖ S_{n-1} ‖ R$_{n-1}$ ‖ R_n ‖ PK_P ‖ PK_{n-1}}
Step 8.a. Provide the recorded discounts or services
Step 8.b.Notify this redemption is a double-redemption
Step 6. Use the P_{ID} and R_0, and SN to examine double-redeption
Step 7. Reply the message about the mobile coupon whether have redeemed
Step 9. Record the mobile coupon has been redeemed
Coupon {C ‖ H'(R_0) ‖ S_P ‖ S_{n-1} ‖ R_{n-1} ‖ R_n ‖ PK_P ‖ PK_{n-1}}
MU_n
Merchant
DB

FIGURE 5: The Mobile Coupon Redemption Phase

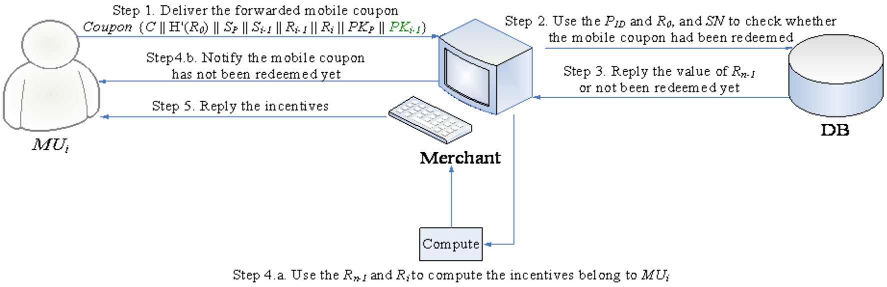
Step 1. Deliver the forwarded mobile coupon
Coupon {C ‖ H'(R_0) ‖ S_P ‖ S_{i-1} ‖ R_{i-1} ‖ R_i ‖ PK_P ‖ PK_{i-1}}
Step4.b. Notify the mobile coupon has not been redeemed yet
Step 5. Reply the incentives
Step 2. Use the P_{ID} and R_0, and SN to check whether the mobile coupon had been redeemed
Step 3. Reply the value of R_{n-1} or not been redeemed yet
MU_i
Merchant
DB
Compute
Step 4.a. Use the R_{n-1} and R_i to compute the incentives belong to MU_i

FIGURE 6: Query the Incentive Phase

ANALYSIS ON ASPECTS OF SECURITY AND PERFORMANCE

In the mobile P2P environment, the incentive mechanism can be realized through the proposed scheme. The merchants may reach more potential consumers for advertising, discover new consumers, and enhance the loyalty of the registered consumers. The mobile coupon receiver who uses the coupon may enjoy the discount. The coupon forwarder may receive reward bonuses. Therefore, the proposed scheme can make the win-win situation for both the merchants and the mobile users. The proposed scheme may avoid potential threats and satisfy the security requirements, as discussed below.

Considering the confidentiality aspect, the receiver knows only the identity of the forwarder, without the knowledge of the upstream users of the forwarder, in the proposed scheme. The forwarder and the receiver have to establish a connection channel during transmission in the P2P environment. Hence, the forwarder is excluded in the requirement of confidentiality. If the receiver forwards the mobile coupon to another mobile user, the new receiver cannot know the identity of the original forwarder. Thus, the confidentiality of the original forwarder is secured.

Considering the authentication aspect, the transmitted mobile coupon has the digital signature and the public key of the forwarder. The receiver can utilize the public key of the forwarder to verify the digital signature, and confirm that the mobile coupon was actually delivered from the forwarder.

Considering the integrity of the coupon, in the issuing phase, the provider has signed on the content to generate a digital signature S_P in the mobile coupon. The S_P can be generated only by the private key of the provider (SK_P), and only the provider knows the SK_P. A malicious mobile user cannot forge a mobile coupon or alter the information recorded in the mobile coupon since the malicious user does not know SK_P. Besides, if a mobile user receives an altered mobile coupon, the receiver may detect the alteration by using the public key of the provider (PK_P) to verify S_P and the content of coupon C. The integrity of the mobile coupon is assured.

Considering the verifiability of the coupon, each coupon has a digital signature S_P and the corresponding public key PK_P. Hence, a receiver may use the PK_P to verify the mobile coupon. Furthermore, the merchant may perform the hash function to compute the R_i from R_0, and verify R_1 through R_i.

Considering the non-repudiation aspect, the provider can not deny they had published the mobile coupon because each mobile coupon is associated with the digital signature S_P. The transmitted mobile coupon has the digital signature of the forwarder, so the forwarder cannot deny the forwarding.

Considering the double-redemption aspect, the merchant examines whether the coupon is redeemed by using SN, PID, and R_0. Thus, a redeemed mobile coupon was recorded in the database so that double-redemption is avoided.

Considering the forgery of the mobile coupon, a mobile coupon is appended with the digital signature of the provider in the issuing phase and becomes an incentive added mobile coupon. A malicious mobile user cannot forge a mobile coupon since the SK_P is unknown. Furthermore, the mobile coupon has R_i, which is computed from R_0 using the one way hash function. The forge will fail to generate a valid R_0 that can pass the verification in the redemption phase.

Finally, the performance of the scheme is described here. Common mobile devices have several inherent limitations on operating complicated security mechanisms. A list of the operations in each phase is shown in Table 2. It confirms that the scheme is efficient.

The size of a mobile coupon in the proposed scheme is 2048 bytes, including *SN* (128 bytes), ID_R (128 bytes), P_{ID} (1280 bytes), *Discount* (384 bytes), and *EXD* (128 bytes). The size of the public key and that of the digital signature are both 512 bits. The size of the one way hash function value is 160 bits. Hence, the maximum size of the mobile coupon is merely 2364 bytes.

The digital signature in the scheme is computed from the private key encrypted output of the one way hash function. Hence, it can be efficiently obtained than that generated by using the public key to encrypt the 2048-byte coupon. Besides, in the forwarding phase, the maximum size of the mobile coupon is fixed at 2364 bytes. Therefore, the proposed scheme is efficient and suitable for the mobile devices.

TABLE 2：Statistics of the Operations in Each Phase

Phase	Processor	Action	Times
Issue	P	Hash function	2
		Sign	1
Forward	MU_n	Hash function	1
		Sign	1
Receive	MU_{n+1}	Verifying	2
		Hash function	1
Redeem	M	Verifying	2
		Hash function	2

CONCLUSIONS

Conventional coupons are shifting towards mobile coupons. Utilizing the mobility and exchangeability of mobile devices, trusted societies may circulate mobile coupons widely. The trust between the sender and the receiver strengthens the recommendation so that the mobile coupon could move toward potential customers. The receiver will probably use the coupon or forward it to who is possibly interested. Adding the incentive to the mobile coupon will eventually increase the redemption rate of the mobile coupon and improve the sales. The uninterested coupon receiver will be more willingly to forward the coupon, which might be discarded without incentives, in our proposed scheme.

The proposed scheme is characterized in the security integration of the incentive-added coupons in the peer to peer environment. The content is secured by the employment of digital signatures. The threats of alternations and forgery are resolved by the integrity of the signature accompanied with the coupon. Furthermore, the scheme provides the necessary security protection without complicated security mechanisms so that it can be effectively adopted in the common mobile devices, which are short of strong computation power and large storage space. Both the verification and the claim of reward bonuses can be efficiently performed with the coupon-forwarding chain, protected by a hash chain technique. The distribution history of the coupon is well protected from potential forgery.

In addition, the merchant may easily control the total amount of the mobile coupons and the upper bound of the reward bonus. In comparison with the paper coupons and those e-coupons requesting print-out before use, the cost of publishing and distribution is reduced. The mobile coupons can actually reach the potential customers either by direct sending or trusted forwarding in the scheme. Merchants, the consumers, and the coupon forwarders will all benefit from the peer to peer mobile coupons in the proposed scheme.

REFERENCES

[1] Anand, R., Kumar, M., and Jhingran, A. (1999) “Distributing e-coupons on the internet”, *Proceedings of 9th Conference on Internet Society (INET ’99)*.

[2] Blundo, C., Cimato, S., and Bonis, A.D. (2002) “A lightweight protocol for the generation and distribution of secure e-coupons”, *Proceedings of the 11th International Conference on World Wide Web*, pp. 542-552.

[3] Chen, Y., Susilo, Y., and Mu Y. (2006) “Identity-based anonymous designated ring signatures”, *Proceedings of the 2006 international conference on Communications and mobile computing*, pp. 189-194.

[4] Chin-Chen Chang, Chia-Chi Wu, and Iuon-Chang Lin. (2006) “A secure e-coupon system for mobile users”, *International Journal of Computer Science and Network Security*, Vol. 6, No. 1, pp. 273-279.

[5] Horne, B., Pinkas, B., and Sander, T. (2001) “Escrow services and incentives in peer-to-peer networks”, *Proceedings of the 3rd ACM Conference on Electronic Commerce*, pp. 85-94. http://www.isoc.org/inet99/proceedings/1d/1d_1.htm

[6] Jakobsson, M., Mackenzie, P.D., and Stern, J.P. (1999) “Secure and lightweight advertising on the web”, *International Journal of Computer and Telecommunications Networking*, Vol. 31, No. 11, pp. 1101-1109.

[7] Kangasharju, J. and Heinemann, A. (2006) “Incentives for electronic coupon systems”, *Proceedings of the 1st international workshop on Decentralized resource sharing in mobile computing and networking*, pp. 60-62.

[8] Kumar, M., Rangachari, A., Jhingran, A., and Mohan, R. (1998) “Sales promotions on the internet”, *Proceedings of the 3rd conference on USENIX Workshop on Electronic Commerce*, Vol. 3, pp.14-23.

[9] Patil, V. and Shyamasundar, R.K. (2004) “An efficient, secure and delegable micro-payment system”, *Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service*, pp. 394-404.

[10] Rivest, R.L. and Shamir, A. (1996) “PayWord and MicroMint:Two simple micropayment schemes”, *Proceedings of the International Workshop on Security Protocols*, pp. 69-87.

[11] Shojima, T., Ikkai, Y., and Komoda, N. (2004) “An incentive attached peer to peer electronic coupon system”, *Studies in Informatics and Control*, Vol. 13, No. 4, pp. 233-242.

[12] Shojima, T., Ikkai Y., and Komoda, N. (2004) “A method for mediator identification using queued history of encrypted user information in an incentive attached peer to peer electronic coupon system*”, *Proceedings of the 2004 IEEE International Conference on System, Man and Cybernetics*, Vol. 1, pp. 1086-1091.