International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 4 – MARCH 2017.

Secure Device for Offline Micro payment

Bazeem Ismaeil Khan [#1] and Shaikh Zubair Ahmed [*2]

[#] PG Student (ME-CSE), Everest Educational Society's College of Engineering and Technology, Aurangabad, India

[*] PG Student (ME-CSE), Everest Educational Society's College of Engineering and Technology, Aurangabad, India

***Abstract*— The paper introduces a novel offline payment system in mobile commerce using the case study of micro-payments. The present paper is an extension version of our prior study addressing on implication of secure micropayment system deploying process oriented structural design in mobile network. The previous system has broad utilization of SPKI and hash chaining to furnish reliable and secure offline transaction in mobile commerce. However, the current work has attempted to provide much more light weight secure offline payment system in micro-payments. The empirical operation is carried out on three types of transaction process considering maximum scenario of real time offline cases. Therefore, the current idea introduces two new parameters i.e. mobile agent and mobile token that can ensure better security and comparatively less network overhead.**

Index Terms*— Micropayment System, Mobile Agent, Hash Function, Wireless Adhoc Network

I. INTRODUCTION

With the development of e-commerce, electronic payment protocols have gained tremendous popularity in the modern world. Credit/debit cards and online payments are in widespread use. A payment scheme usually consists of three parties involved: the user, the merchant, and the bank [1]. In order to assure the security of payment, cryptography techniques have been used to achieve authentication, privacy, and other requirements. Of course, some cryptography techniques are not lightweight such as public key digital signature and verifiable random number that is introduced in [2]; these techniques are usually used to transfer large sums of money, which are defined as micropayment.

Recently, the computer and network have developed so rapidly that complicated public crypto algorithm can be efficiently executed in the fixed network platform. Nowadays, mobile internet service providers are developing lots of innovative services to make people's daily life more convenient and interesting with the popularity of Smartphone and other hand-held computer, as a result, the number of online commercial transactions involving small amount of money grow fast, especially that the tiny value intangible goods (non-physical assets such as data and information) are booming. These tiny value payments are defined as micropayment [3].

Applications of micropayments include paying for each web page visited, for music or video as it is streamed to the user, data traffic, and so on. Micropayment could be implemented by electronic checks over the internet, the computation burden of digital signature is negligible for the development of CPU, but the cost of bank's processing is really an obstacle for micropayment. For example, processing a credit card transaction costs about 25 cents, whereas a micropayment value may be only 1 cent, which makes the traditional transaction protocol unsuitable for tiny value transaction. As for mobile network, the computation time and processing cost are all obstacles for micropayment [4].

The limited memory, computing power, and battery capacity restrict the mobile terminal to execute complicated calculation. Moreover, the overhead of communication is also influencing the availability of micropayment scheme since more rounds of data exchange makes the scheme is not economic. Recently, some micropayment schemes have been proposed to satisfy the enhanced feature for different requirements. Pay word is proposed by Rivest and Shamir [5], but it has a main problem: a merchant cannot aggregate micropayments of different users.

A non-selected micropayment will be discarded,whereas a selected one will cause the user to debit an amount of money equal to 1/s. On the average, user pays what he or she should during the long-term process. Rivest's lottery overcomes the disadvantage of Payword; however, it suffers from other two problems: (1) interaction (the user and merchant must interact to select micropayments) and (2) user risk (the user may pay more than he or she should).

MR1 scheme solves the first problem, but does not address the second one. MR2 solves both problems, but it is possible for the user and the merchant to collude to cheat Bank. MR3 shifts the deterministic role from the merchant to the bank, avoiding the collusion between the user and the merchant. At the same time, the small risk of excessive payment is also shifted to the bank, which is accustomed to risk management. In addition, there is a main attraction: rather than trying too hard to prevent cheating, the bank simply punishes or eliminates cheating parties before they can create any substantial damage. Although MR2 and MR3 achieve a series of requirements of micropayment, there are perhaps some difficulties for implementing them in mobile network. The algorithm should be lightweight, which is a basic requirement for mobile e-commerce protocol. Each transaction is signed by the user and sent to the merchant; the merchant or bank decides which transaction is payable in MR2 and MR3.

We know digital signature algorithm is more complicated than hash function and symmetric cryptographic algorithm, which may affect the performance of the mobile device. Second, each transaction signed with user's private key may reveal user's identification such that the user's privacy is disclosed. Third, the micropayment scheme should be economic; that is, the rounds of challenge–response should be reduced to a minimum level. In this paper, we propose an improved lightweight micropayment scheme based on hash chain and Lagrange interpolation formula to achieve privacy, fairness, security, efficiency, and low cost of use [6].

The remainder of this paper is organized as in the following sections. Section 2will describe the related works on data micropayment schemes. Section 3 will present the proposedmicropayment scheme method. In Section 4, we will analyzethe results ofproposed method and compare it with standard data micropayment methods. Finally, a brief conclusion will be given in Section 5.

II. RELATED WORK

Zhi-Yuan Hu et al. has designed an innovative and practical authentication system, Anonymous Micropayments Authentication (AMA), is designed for micropayments in mobile data network. But his work has a relative drawback for common problems of authentication mechanism based on symmetric key cryptography [7].

Xiaoling Dai et al. has researched on micropayment protocols in offline with multiple vendors. They introduced several micro-payment schemes based on one-way hash chain and review some literatures on supporting multiple payment. The author has also proposed a new micropayment scheme, which achieves the following three goals: micro-payment multiple transactions, service providers, and anonymity [8].

Aboud et al. has proposed a trust model from user point of view and combined it with MR2 micropayment scheme and called the new scheme TMR2. This trust model is supported by micropayment provider and assures the users that they will not be charged for in case the product is not satisfactory or it is corrupt [9].

Min-Shiange.t. al. has studied various probabilistic micropayment Scheme shows that the scheme by Rivest may reduce the administrative cost of the bank, however it brings extensive computational overhead to the merchant [10].

Lih-ChyauWuu has proposed a secure and efficient off-line micro payment scheme which uses coin chain technique to make coin that the verification of coin can be done quickly by hash computation. This scheme also ensures that coins could only be used by their owner, and protects the privacy of the consumer [11].

VivekKatiyare.t. al. has discussed about role of Elliptical Curve Cryptography and presents a survey on the current use of ECC in the pervasive computing environment. Husna Osman and Hamish Taylor has discussed three key design considerations in implementing a fully distributed reputation system for ad hoc m-commerce trading systems, namely relevant reputation information, its storage and reliability [12].

FouziaMousumi and Subrun Jamil has described cost effective push pull services officering SMS based mobile banking concept has been illustrated for 24 hours banking convenience which helps customers stay on top of any recent changes made in their current or deposit account or loan through SMS [13].

Arogundade e.t. al. propose an open network system which can adapt to users changing needs as well as allowing effective and secured transaction via any customers' bank account. They proposed a novel approach by utilizing cancelable biometric features for securely storing the fingerprint template by generating Secured Feature Matrix and keys for cryptographic techniques applied for data Encryption or Decryption [14].

Mohammad Al-Fayoumi discuss an important epayment protocol namely pay-word scheme and examine its advantages and limitations, which encourages the authors to improve the scheme that keeps all characteristics intact without compromise of the security robustness [15].

Kaylash Chaudhary e.t. al. have carried out an assessment of micro-payment against a non-micro-payment credit systems for file sharing applications. Charles K. Ayo and Wilfred IsiomaUkpere proposed a unified (single) smart card-based ATM card with biometricbased cash dispenser for all banking transactions Wang proposes a novel payment system with smart mobile devices, wherein customers are not limited to purchase e-cash with the fixed face-value Currently, researchers focus on the e-payment system such that electronic cash electronic check electronic traveler's check and so on. Moreover, many researchers proposed the e-cash payment protocol using plenty of computational resources such that exponential operation. It causes the big burden for the system [16].

Chang and Lai proposed a flexible date attachment scheme on e-cash and Juang proposed the Dcash. Curanintroduced some possible additional security measures which could be implemented to strengthen the overall security architecture of Bluetooth enabled devices for ecommerce applications against man-in-the middle attack and denial-of-service attacks [17].

Wanget al.proposed a novel payment system with smart mobile devices, wherein customers are not limited to purchase e-cash with the fixed face-value. The amount of every transaction is deducted directly from the customer's account, eliminating the inconvenience of fixed face-value of the e-cash, and reducing online computation cost of a bank. Using a technique of trapdoor hash function to mitigate the computational cost, our system can be used with the mobile devices effectively [18].

Natarajan introduced a system and method of extensible authentication protocols (EAPs) based on ECC and SKE with a permutation technique evolved. The permutation in our EAPs is a process of cubing a random number w.r.to a prime. These EAPs are compatible with 3G and 4G networks and no certificates exchanged during the communication [19].

Panjwani has analyzed two token-based authentication schemes, designed for authenticating users in banking systems implemented over mobile networks. The first scheme is currently deployed in India by a mobile banking service provider named Eko with a reach of over 50,000 customers.

The second scheme was proposed recently (in joint effort with Eko) to fix weaknesses in the first one, and is now being considered for deployment. Both systems rely on PINs and printed codebooks (which are unique per user) for authentication [20].

Chaix explores the economic models associated to different mobile-payment systems. Obviously it can be seen that majority of the work is carried on wired network with much less consideration of wireless network. The issues related to dynamic topologies of wireless adhoc network are not discussed in detailed in any of the researches described above. Although there are some effective research being done in the area of payment system, but there is a huge research gap in this area with respect to wireless mobile adhoc network [21].

III. PROPOSED WORK

The proposed protocol now termed as Secure Payment in Mobile Commerce deploys the authority that has to be signed by mobile agent and m-token key authorized by merchant. The authority file that is signed is utilized by merchant in order to confirm the transaction parameters and authorized m-token that needs to be used in order to resist any malicious activity from any customer. The similar phenomenon can also be used to determine any issues with merchants too. The proposed method contains the following modules namely, broker agreement, cost and endorsement delivery, initiating payments, new route consideration, transferring tokens, and broker approval. The proposed methodology can be explained in brief steps as following:

A. Broker Agreement

A broker supplies it's registered and authorized user will a secure and tamper-proof token with public key pair along with highly encrypted user identity. Any micropayment schemes like credit card can be used for designing the application. The user then sends a signature message consisting of hash value and payment information which is encrypted with public key of broker. The broker generates (agreement) secret endorsement data which consists of a random number, an anchor value, length of hash chain, user-identity, and expiry of chain. These set of information is secured by private keys of broker. Therefore the broker agreement can only be deciphered by user's token. However, the security of tokens (smart cards) are not reliable as it can be deciphered, so the broker private information is appended with expiry date in order to restrict an unauthorized user in the range of mobile network to have an access on the confidential information transacted between user and broker.

B. Cost and Endorsement Delivery

A sender node P sends the cost request message encrypted with digital signature using their private keys to query the route of recipient node Q. All intermediate nodes attach certificates so that the origin node will be able to validate the digital certificates on the cost details. The data for cost reply message is returned to P. After estimating the cost involvement in routing, the encrypted broker endorsement is sent to all relay nodes in the network. These endorsements are private data, so each user encrypt with their public key, which can be received from cost reply message. This scheme pays the intermediate routers for forwarding the packets.

C. Initiating Payment

This step is about initiating payments in the system by the user. P transmits message in his network and appends a hash token from sub-chains. The payment scheme in independent of increased used of hash values for multiple payments by the user ensuring much less network overhead. In case the intermediate relay nodes have captivated the hash values, they will not be able to decipher them without broker agreement and its respective signature.

D. New Route Consideration

This step is performed as wireless adhoc network quite often changes their topology dynamically. In case of new route, the system needs not to contact the any TTP. Overhead is reduced by observing the new nodes in the route and using only them for the distributing the secure endorsement. The following algorithm explains the route consideration policy.

```
   Input : grid, number_of_column

   temp A (number_of_column) % 4
   noc Å number_of_column
    **if** (temp = 0)
   two_col Å noc
   two_col_zigzag(grid,two_col)
      **else if**(temp = 1)
   two_col Å noc-3
   two_col_zigzag(grid,two_col)
   three_col_path(grid)
      **else if(**temp = 2)
   two_col Å noc-2
   two_col_zigzag(grid,two_col)
   straight_up(grid,noc-1)
   straight_down(grid,noc)
   **else if**(temp = 3)
   two_col Å noc-1
   two_col_zigzag(grid,two_col)
   straight_down(grid,noc)
      **end**
horizontal_path(grid)
```

E. Transferring Tokens

Here the intermediate relay node transmits the greater hash values in one chain that has spent it by the node. The user token then transmit the hash value to the consecutive broker with their endorsement digitally signed. The message and its highly encrypted contents are validated by the broker as well as issue an acknowledgement. 6. Broker Approval: The proposed system does support multiple brokers for reliable communication which allows any user to get associated with any broker available in the network. The user in the first network receives payment chain from the broker in that network, it assist the same user for validating the digital certificates generated by the nodes in new network when the network topology changes. The assumption to this step is that the user, broker and all the entities involved should first get them registered and then perform the task.

IV. EXPERIMENTAL ANALYSIS

To give a performance evaluation of the proposed micropayment scheme, we present simulation results of proposed method and compared it with PayWord and PPayWord schemes a computational and communicational costs. Computational cost is considered as the overall needed CPU cycles at broker and communicational cost is overall the transmitted payment messages volume. Results are showed in two typical fixed lengths of chains, 10 and 20 and a chain is considered as partially used and is not transferable if its spent length is less than the configured chain length.

A. Computational Cost of Broker

Figure 1 shows the comparison of broker load for proposed work in comparison with PPaWord and PayWord. As it seems, when most of the payments are made with transferred chains, load of the broker is divided by two, approximately. For both of the chain length configurations, results confirm the latter claim since the load of the broker in PPayWord is reduced about40 %. We use semi-online term to point the load of a broker in case of transferring chain between peers due to the fact that this transference is online but offline against payments and do not affect their performance. This figure shows that most of the broker workload is semi-online and there is a few job of broker in case of online checking payment accuracy and offline balancing accounts. We can adjust offline load and semi-online load of broker according to the system requirements. To this end, an upper bound for transferring every chain must be applied by adding a new column to broker's database. The value of this column is incremented one unit per chain transference and when it reaches to the considered upper bound, the chain cannot further be transferred.

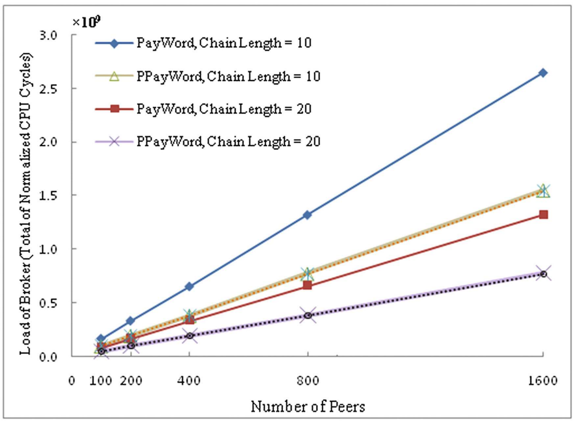

Figure 1. Computational cost

B. Communicational Cost

Figure 2 shows that in PPayWord communication cost increases based on the length of the chains because lesser chain length means we need more commitment messages. Onthe other hand, unlike PayWord scheme wherein most of the messages are sent toPPayWord: A Secure and Fast P2P Micropayment Scheme for Video Streaming 89broker at the end of day, in PPayWord this cost is distributed over time and does notmake the broker as a bottleneck of the payment system. Higher stability of peers' linksin the overlay structure results higher length of transferred chains which can reduce communication costs by decreasing needed commitment messages.

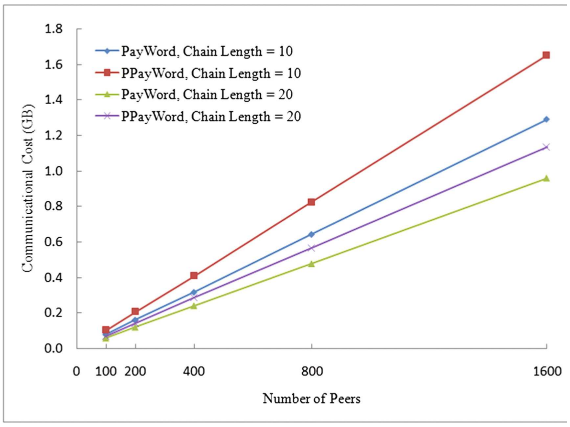

Figure 2.Computational cost

The secure channel information in the proposed scheme are not specific to customer or merchant thereby permitting secure offline transaction for payments evaluated for large number of merchants over the network. One of the noteworthy advantages of the proposed scheme is that OSPM transfer the authenticated network channel issues from Mobile-agent and allocates it among the entire merchant. Hence this schema balances the network and processing overhead from merchant over the network. Another advantage is that it assures safe exchange of legitimate m-token for credit to the merchant as well as it also permits the merchants to concentrate on content scheduling and Mobile-agent to furnish operation related to management of amount in their registered financial institution.

The transaction between mobile user and vendor has dual benefits. Primarily, the transfer of the secure message from M1 to M2 does not include any mobile agent and it diminishes the network overhead of the mobile agent. Secondarily, the consecutive secure message posses the m-token of the authorization for which it resists the customer C from any sorts of malicious activities while in offline even when C swaps to another merchant M2. Exactly, this scheme thereby renders a novel, costeffective, and secure network with better business role in ecommerce.

V. CONCLUSION

The current work is focused on designing an offline payment system in mobile commerce specifically taking micro-payment as case study. Majority of the work done in prior research work is concentrated on online safety along with service provider too. But, in this work, it can be seen that SP also requires generating secure supportive hash value for every secure channel data that is sent via smart-phone of the customer C. Then SP forwards the legitimate secure channel information and subsequent supportive hash vale to the merchant in every transactions offline. The m-token in system schema considered in customer and merchant dependent. This phenomenon restricts the portability of the secure channel information to a greater extent. The current work therefore has introduced a real time offline payment system from a Mobile-agent and service providers and termed the scheme. The proposed scheme restricts the customers for performing a malicious activity even in offline mode using m-token. Therefore, the proposed system is found to satisfy all the critical security requirements in micro-payment system. The proposed schema is also cost-effective as it does not posses any operation with public key for any types of purchases being made.

REFERENCES

[1] Zygmunt J. Haas, Jing Deng, Ben Liang, Panagiotis Papadimitratos, S. Sajama,"Wireless ad hoc Networks", John Wiley & Sons, Inc, 2003

[2] Yuntsai Chou, Chiwei Lee and Jianru Chung, "Understanding m-commerce payment systems through the analytic hierarchy process", Journal of Business Research, Volume 57, Issue 12, December 2004, Pages 1423-1430

[3] Neal Leavitt, "Payment Applications Make E-Commerce Mobile", IEEE Computer Society, 2010

[4] Rafael Martínez-Peláez, Francisco Rico-Novella, Cristina Satizábal and Jhon J. Padilla, "Performance Analysis of Mobile Payment Protocols over the Bluetooth Wireless Network", Whitepaper, 2008

[5] HeikoKnospe, Scarlet Schwiderski-Grosche, "Future mobile networks: ad-hoc access based on online payment with smartcards", IEEE, 2002

[6] Peter Tarasewich, Robert C. Nickerson, Merrill Warkentin, "Wireless/Mobile E-commerce: technologies, applications, and issues", Seventh Americas Conference on Information Systems, 2001

[7] Zhi-Yuan Hu, Yao-Wei Liu, Xiao Hu, Jian-Hua Li, Anonymous Micropayments Authentication (AMA) in Mobile Data Network, INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies Iss: 7 March 2004,

[8] Min-Shiang Hwang, Pei-Chen Sung, A Study of Micropayment Based on One-Way Hash Chain, International Journal of Network Security, Vol.2, No.2, PP.81–90, Mar. 2006

[9] Al-Fayoumi, M., Aboud, S., Al-Fayoumi, M., "Practical E-Payment Scheme", International Journal of Computer Science Issues, vol. 7, no. 7, May. 2010

[10] Xiaoling Dai, OluwatomiAyoade, and John Grundy, Offline Micro-payment Protocol for Multiple Vendors in Mobile Commerce, Proceeding PDCAT '06 Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, IEEE Computer Society Washington, 2006 R. Hauser, M. Steiner, and M. Waidner, "Micro-payments based on iKP", in Proc. of the 14th Worldwide Congress on Computer and Communications Security Protection, Paris, 1996, pp.67-82, http://www.zurich.ibm.com

[11] Lih-Chyau Wuu, Kuang-Yi Chen, Chih-Ming Lin, OffLine Micro Payment Scheme with Dual Signature, Journal of Computers, Vol.19, No.1, April 2008

[12] VivekKatiyar, Kamlesh Dutta, Syona Gupta, A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment, International Journal of Computer Applications (0975 – 8887) Volume 11– No.10, December 2010

[13] FouziaMousumi, Subrun Jamil, Push Pull Services Offering SMS Based m-Banking System in Context of Bangladesh, International Arab Journal of e-Technology, Vol. 1, No. 3, January 2010

[14] Arogundade O.T, Ikotun A. Motunrayo, OlaniyiAdemola, Developing a Usage-centered e-Payment Model using Open Network System, International Journal of Computer Applications (0975 – 8887) Volume 12– No.6, December 2010

[15] Mohammad Al-Fayoumi, SattarAboud and Mustafa AlFayoumi, Practical E-Payment Scheme, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 7, May 2010

[16] Kaylash Chaudhary, Xiaoling Dai and John Grundy, Experiences in Developing a Micro-payment System for Peer-to-Peer Networks, International Journal of Information Technology and Web Engineering, vol. 5, no. 1, 2010

[17] C. C. Chang and Y. P. Lai, "A flexible Date-attachment Scheme on E-cash", Computers & Security, Vol. 22, No. 2, pp.160-166, 2003.

[18] Jian-Sen Wang, Fuw-Yi Yang, and Incheon Paik, "A Novel E-cash Payment Protocol Using Trapdoor Hash Function on Smart Mobile Devices", IJCSNS International Journal of Computer Science and Network Security, Vol.11 No.6, June 2011

[19] Natarajan Vijayarangan, "A system and design of Extensible Authentication Protocols based on ECC and SKE mechanisms for mobile and wireless communications", Advances in E-Activities, Information Security and Privacy, 2011

[20] Saurabh Panjwani, Prasad Naldurg, RaghavBhaskar, "Analysis of Two Token-Based Authentication Schemes for Mobile Banking", Technical Report of Microsoft Research, 2010

[21] Laetitia Chaix and Dominique Torre, "Different models for mobile payments, research paper, 2010