IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 6, Ver. V (Nov – Dec. 2015), PP 98-101
www.iosrjournals.org

Protocol Payment in M-commerce Transaction

K. Maazouz[1], H. Benlahmer[2], N. Achtaich[3]
[1](*Analysis, Modeling and Simulation Laboratory, University Hassan II, Morocco.)*
[2](*Laboratory of Information Technology and Modeling, University Hassan II, Morocco.)*
[3](*Analysis, Modeling and Simulation Laboratory, University Hassan II, Morocco.)*

Abstract: *With the rapid proliferation of Internet-enabled mobile handsets, empirical research has been undertaken in large number. The rapid growth of mobile commerce is being driven by number of factors , increasing mobile user base, rapid adoption of online commerce and technological advances. Regarding the development of mobile technology, it seems essential to have a payment protocol which provides the required security features along with an acceptable efficiency in mobile environment. This article introduces a payment protocol based on secure wireless payment using the m-check system. The proposed mobile payment protocol not only minimizes the computational operations and communication passes between the engaging parties, but also achieves a completely privacy protection for the payer.*

Keywords: *mobile commerce; m-payment ; M-check ; security; privacy*

I. Introduction

The emergence of M-commerce create the need to develop a new ways of purchasing on mobile devices. The payment trough mobile devices make arise different security and efficiency drawbacks due to mobile environment limitations as low Bandwith, the connection cost, computational and storage capabilities. Different electronic payment protocols are proposed in the literature among which SET[2], iKP protocols[], KSL[9], but they are not suitable for mobile environment. Some protocols are developed to satisfy the efficiently in mobile environment as SWPP[4] which is designed to overcome the WPP[3] limitation. The protocol SSMCP[1] was designed for mobile lightweight client and concern the problem of fair commitment. In this article we introduce a secure protocol for payment. One integral tool utilized within this protocol is the use of m-check. The m-check system or mobile check system is a mobile payment system[6] based on the use of mobile version of e-cheque provided by the bank who is the first responsible of the payment management . The proposed protocol based on the use of the m-check system for payment which guarantee a high level of security and prevent a replay attack. The rest of this paper is organized as follows. Some existing mobile payment protocols are briefly explained in section II. Section III details our new protocol for mobile payment. Finally, the conclusion will be made in part 6.

II. Payment Protocols

SSL and SET are considered as two standard for electronic payments protocols. But they cannot be directly adopted in wireless area due to their heavy computational operations and communication passes[2].

The protocol proposed by MSET[5] which based on SET, it's a wireless protocol proposed by replacing time consuming public key encryption and decryption algorithms, but it falls short on convenience.

The WPP[3] is an efficient wireless protocol which address convenience, based on fewer messages comparing to MSET, but it present some shortcoming and security drawbacks.

SWPP[4] address the security problem of WPP, it's based on the WTLS, and the WAP infrastructure[7], it considered as a protocol with many advantages over SSL and SET protocols, and it appropriate for being developed into some secure protocols. But it leaves out user's anonymity and privacy.

ASWPP[10] is an anonymous payment protocol based on secure wireless payment protocol (SWPP). Contrary to SWPP, this protocol manages to provide anonymity and privacy of the customer. it uses a blindly signed pseudo digital certificate and anonymous bank account in order to protect the customer's identity.

The SSMCP [1] protocol is a secure protocol developed to reduce the amout of communication, and use the e-cheque[8] as an integral tool of payment . that's way it has been selected as the basic idea of our protocol in this article. Therefore the SSMCP protocol is a secure protocol used for m-commerce transaction and it's developed to reduce the amount of communication to comply with wireless bandwidth limitation. the protocol is based on the concept that the way the merchant receive the e-cheque from the customer. And it's reside on the creation of a public URL from the bank and specific to each individual customer.

III. Our Proposed Protocol

This protocol is based on the message flow of SSMCP protocol[]. The protocol uses different data flow from SWPP in order to make sure the protocol convenient. As illustrated in Fig1 the customer start a WTLS class 3 connection with the merchant and start by selecting the random number which is used to prevent the bank from accessing the order information, and sends the merchant a purchase request. After receiving the customer's request the merchant compute the amount h(OI,R), and create the transaction identity which contain the ID and date of transaction signs them all as well as the price and his information MI, and then sends them to the customer, who signed the m-check filled with the received information (MI, amount, and date) and conceal it with the nonce N, sends it to the merchant with the transaction information. The merchant verify the m-check and deposit it to his bank and wait for response to deliver the order to the customer.

Table1: Notification

Symbol	Description
{C,M,CB,MB}	Are used to denote respectively Customer, Merchant, Client's Bank, and Merchant's Bank
$Cert_C$	Certificate of X
ID_X	Identity of X
TID	Identity of the transaction that include time and date of the transaction
TID_{REQ}	The request of TID
MI_{req}	The request of the merchant information
OI	order information. OI = {TID, h(OD, Price), where OD and Price are order descriptions and its amount.
R	A random number used by the customer to keep the order information
$Sign_{privX}$	From the bank
H()	Signature of X by the his private key
mcheck	Hash function
Nonce	The mobile check
	Random number used to conceal the m-check

Purchase request: The payment is initiated from the customer who send his identity ID_C , the order information with the random number R , and ask the merchant to send him the merchant's information MI and the transaction ID .

Customer $\longrightarrow$ *Merchant :{* ID_C *,*TID_{req} *,* MI_{req} *, OI, R}*$sign_{privC}$ *,*$Cert_C$

Request confirmation: The merchant receive the customer's request , create the unique transaction identity and send it along with his MI, the price, h(OI, R) , signed with his private key in addition of his certificate.

Merchant $\longrightarrow$ *Customer: {TID,* ID_M *,MI, price, h(OI, R),* ID_C*}*$sign_{PrivM}$ *,* $Cert_M$

M-check upload: Upon receiving the answer the customer create and filled the m-check with the information extracted from the message, and signs it with his private key along with TID, the price, and the his bank ID. After signing it, the customer uploads the mcheck to the merchant .

Customer $\longrightarrow$ *Merchant: { TID,* ID_{CB} *, MI, price, h(OI, R),* ID_C *, mCheck}*$sign_{PrivC}$

After, the merchant receive the M-check, and verifies the signature, the m-check's information, and the received data. The merchant can cash the m-check at any time before the time of expiration. The merchant then send the m-check to his bank for endorsement.

Merchant $\longrightarrow$ *MBank : { TID,* ID_{CB} *, price, MI, h(OI, R),*ID_C *, mCheck}*$sign_{PrivC}$ *, { TID,*ID_{CB}*,* ID_M *, price, h(OI, R),* ID_C *, mCheck}*$sign_{PrivM}$ *,* $Cert_C$

Transaction verification: The merchant's bank receives the message, verifies the signatures, and mCheck informations and compare it with the one sent by the merchant to make sure that they are similar and they are not modified. So it compare the price with amount signed in the m-check, compare also the expiry date of the purchase with the date in the m-check. If there isn't problem the bank will sends the customer's bank a payment request and start the clearness process between them.

MBank $\longrightarrow$ *CBank: Notification of payment*

The customer's bank verifies the customer's account and withdraw the price off the customer's account and sends the merchant's bank a response to deposit the money to the merchant's account and sends the signed confirmation to the merchant.

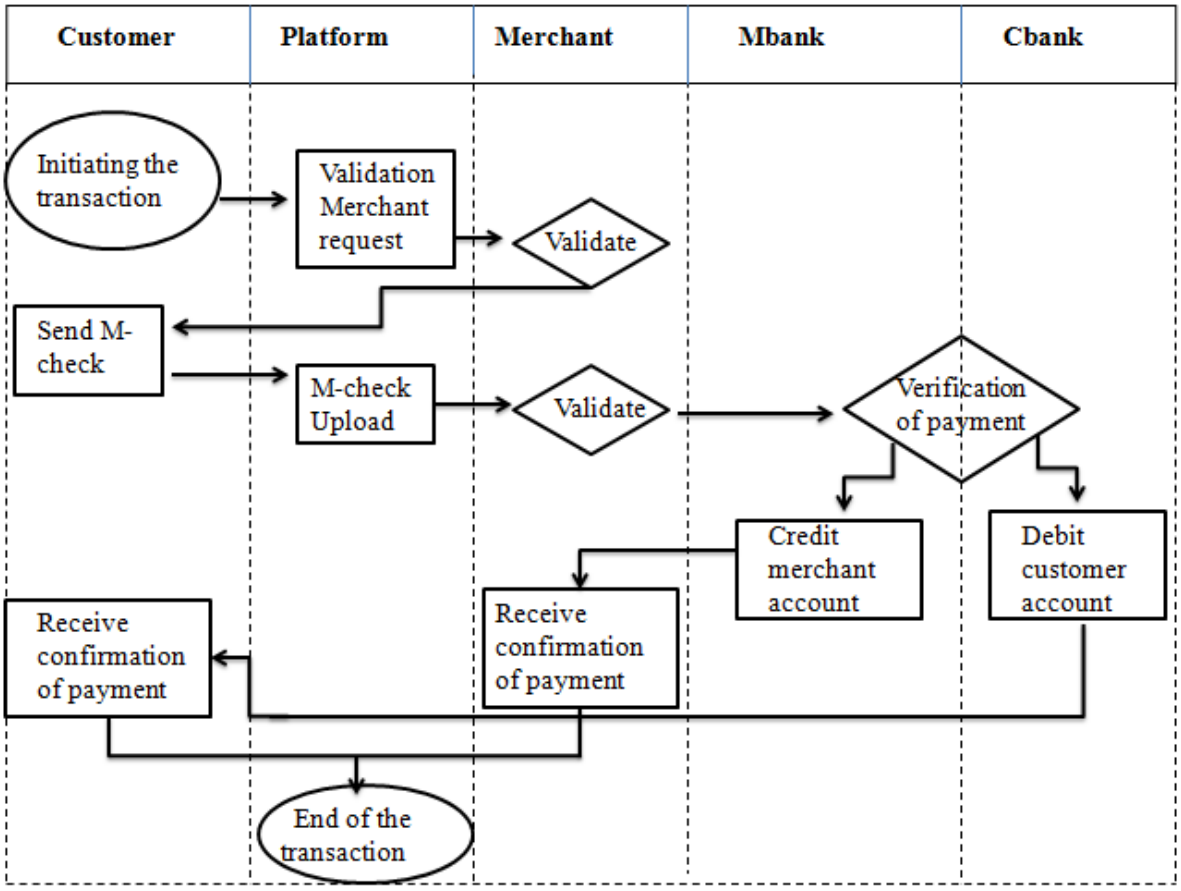
MBank $\longrightarrow$ *Merchant: confirmation of payment:{TID,* ID_M *,* ID_C*, price, h(OI,R)}*$sign_{PrivMB}$

the customer's bank signed the receipt and send it to the customer, and stores TID and the mcheck identity in the database to resolve any possible dispute.

CBank $\longrightarrow$ *Customer: {TID,* ID_M *,* ID_C *,price, h(OI, R)}*$sign_{PrivCB}$

The bank of merchant compare if the amount of h(OI,R) signed by the merchant and h(OI,R) signed by the customer are identical and verify the validity of the m-check by comparing the price with the amount signed in the m-check, the expiry date of the purchase with the date in the m-check, and the merchant and customer's information to make sure the merchant didn't manipulate the m-check and the customer and merchant agree about items. In the next stage the merchant's bank contacts the customer's bank to start the process of regulation of the payment between them trough a virtual private network. If the transaction is done successfully, the merchant 's bank will send a signed receipt to the merchant to start deliver the items ordered to the customer because the signature make him sure that his account is credited with the amount. The customer's bank in turn send a signed receipt to the customer to reassure him that the transaction is done successfully and the merchant is obliged to deliver his orders.

Fig1: Messages flow corresponding to the protocol



The security of our protocol is based on the use of the m-check for payment and the advantages of the m-check system are apparent. The protocol provides privacy because the customer and the merchant don't have to communicate their banking information, and each participant have limited access to the information. So why the customer don't have to hide his identity by creating an anonymous identity. All public keys issued are certified by a certification authority, which assure authentication. WTLS provides confidentiality and integrity of the sent data.

IV. Conclusion

This paper is to suggest a more private mobile payment protocol by involving the m-check system. The improvements help this protocol provides a higher performance, in addition to covering some security drawbacks of some protocols such as un anonymity of the customer. The future work will concentrate on improving the verification of the protocol proposed and to introduce a simulation of the protocol to prove to be able to meet the requirements both theoretically and practically.

References:

[1]. E, Haddad and B, King; A Simple Secure M-Commerce Protocol SSMCP*; IJCSNS International Journal of Computer Science and Network Security; 2007

[2]. Isaac,J.T.,&Camara,J.S.(2007).Anonymous payment in a client centric model for digital ecosystem. In Digital Eco Systems and Technologies Conference (DEST ’07)(pp.422–427).

[3]. Hall, J., Killbank, S., Barbeau, M., & Kranakis, E. (2001). WPP: A secure payment protocol for supporting credit and debit card transactions over wireless networks. In Proceedings of ICT 2001 international conference on telecommunications (pp.4–7).

[4]. Wang,H.,&Kranakis,E.(2003).Securewirelesspaymentprotocol.InProceedingsoftheinternational conference on wireless networks, LasVegas,NV.

[5]. Shedid, S. M., El-Hennawy, M & Kouta, M.(2010). Modified SET protocol for mobile payment: An empirical analysis. IJCSNS International Journal of Computer Science and Network Security, 10(7), 289–295.

[6]. K.Maazouz; H.Benlahmer; N.Achtaich, Generic Architecture for Mobile Check System, International journal of computer technology and applications, vol4, issue6, 897-901pp,2013.

[7]. Misra,S.K.,&Wickamasinghe,N.(2004).Securityofamobiletransaction:Atrustmodel.Electronic Commerce Research, 4(4),359–372.

[8]. Beadle H., Gonzalez R., Safavi-Naini R., Bakhtiari S.“A Review of Internet Payments Schemes”, In Proceedings of the Australian Telecommunication Networks and Applications Conference (ATNAC’96), Melbourne, Australia, December 1996, pp.486-94

[9]. P. D. L. Kungpisdan and S. Bala, “A secure account-based mobile payment protocol,” in Proc. International Conference on Information Technology: Coding and Computing, pp. 35-39, 2004

[10]. S.Layeghian Javan and A Ghaemi Bafghi, An Anonymous mobile Payment Protocol based on SWPP, Springer; 2014