A MOBILE TELEPHONE BASED, SECURE MICRO-PAYMENT TECHNOLOGY USING THE EXISTING ICT INFRASTRUCTURE

Hasan AMCA: Electrical and Electronic Engineering Department, hasan.amca@emu.edu.tr
Raygan KANSOY: Information Technology Department, raygan.kansoy@emu.edu.tr
Eastern Mediterranean University, North Cyprus,

ABSTRACT

The need to use mobile telephones and PDA's as electronic-payment devices became stronger as the global mobile penetration rate reached 17 percent. However, due to the technological limitations and security considerations, the well established jargon of electronic-payment could not be employed in mobile-payment (m-payment), specifically for payment of very low amounts (e.g. micro-payment). Therefore, new technologies are needed for enabling m-payment.

In this paper, we investigate the shortcomings of the available card-based micro-payment schemes and propose a new scheme that is suitable to apply to multiple-vendors for m-payment. The proposed scheme uses a Variable Transaction Number (VTN) used per purchase, in the form of an on-screen barcode, readable by the CCD barcode scanners. The proposed method satisfies requirements of micro-payment systems in terms of financial, technological, computational and managerial costs.

1. INTRODUCTION

Using credit cards such as Visa, Master-Card, Card Plus and American Express as a secure and easy way of payment has been well established worldwide. However, due to the fraudulent use, loss or damage problems, yearly, there is a significant financial loss [1]. Hence, alternative, more secure and versatile payment methods are needed. As the global mobile equipment penetration such as mobile phones and PDA's reached almost 17 percent [2], businesses are searching for ways of using mobile equipment for electronic payments. This technique, commonly called the mobile-payment or m-payment can be carried out by using any one of the available technologies such as SMS, IrDa, Bluetooth, RFID [3] and the like. Each of the available payment methods, sometimes referred to as E-Charge-My-Phone methods [4], address the needs of consumers in different applications and provide clear and acceptable benefits. In addition, all of these methods integrate the purchasing expenses and mobile phone bill.

E-Charge-My-Phone Using SMS method is a premium SMS service that allows users to anonymously and securely pay for the products and services they purchased via their mobile phone by sending a text message to a premium number. The customers are then charged on their mobile phone invoice. The SMS method is designed to work in batch processing mode and therefore might take a long time to confirm the credit approval by the bank and complete the transaction [5].

In Switzerland, Swisscom Mobile introduced a mobile payment scheme based on Unstructured Supplementary Service Data (USSD) to purchase beverages in wending machines [16]. The customer had only to dial the USSD number and select the desired beverage. This service is used because it is considered simpler and faster than the use of SMS.

IrDa specifications are well defined and make it extremely secure for m-payment. The "express payment" reduces the transaction time significantly. However, it also reduces the security of IrFM by giving the privilege to devices to bill the consumer without authentication. Therefore, the "express payment" application is potentially vulnerable to financial fraud. However, the most important drawback for the application of IrDA is the necessity of providing an IrDA device at every merchant's counter [2,6].

Bluetooth technology has also been found useless for its set-up time required in addition to the non-selective nature. A Bluetooth device will search for all devices within a short range. This might mean a large number of Bluetooth devices in a shopping mall [7]. The usage of RFID in m-payment could be comparable to Bluetooth and therefore is delay and complexity limited [8,9].

The method we proposed in this article uses a credit provider generated secure transaction number, unique for each transaction. This number is transformed into a barcode by the mobile terminal (MT) that can easily be read by the merchant's barcode reader. Hence, overcoming the shortcomings mentioned above in terms of latency, security and usability. The on-screen generated barcode could also be used as tickets for such places as cinema and theatre.

This method of payment could be made available in societies where Mobile Telephone usage is more widespread than the Credit Card. Most of the underdeveloped and developing countries have higher rate of mobile telephone penetration than Credit Card. Hence, m-payment in such countries can help improve on-line payment technologies as a whole by using MTs instead of CCs.

The article is organized as follows: In section 1, an introduction is made into the m-payment technologies. In section 2, a preview of online payment processing is presented. In section 3, the Variable Transaction Number Barcode (VTNB) method is described with reference to the infrastructure and security issues. Conclusions are provided in the last section.

2. PREVIEW OF ONLINE PAYMENT PROCESSING

An Online Payment Processing (OPP) solution is broadly defined as electronically paying for the purchase of goods or services without using hard cash. An OPP solution should be secure, reliable and easy to use so that the common fraud-related risks such as product theft, identity theft and cash theft will be avoided. OPP consists of 2 steps: Authorization and settlement.

Authorization verifies that the card is active and the customer has sufficient credit to make the transaction. This is shown in Figure 1. Settlement is the process of charging the customer's payment account and transferring money from the customer's account to the merchant's account through a transaction broker such as PayPal [14]. This is depicted in Figure 2 below.

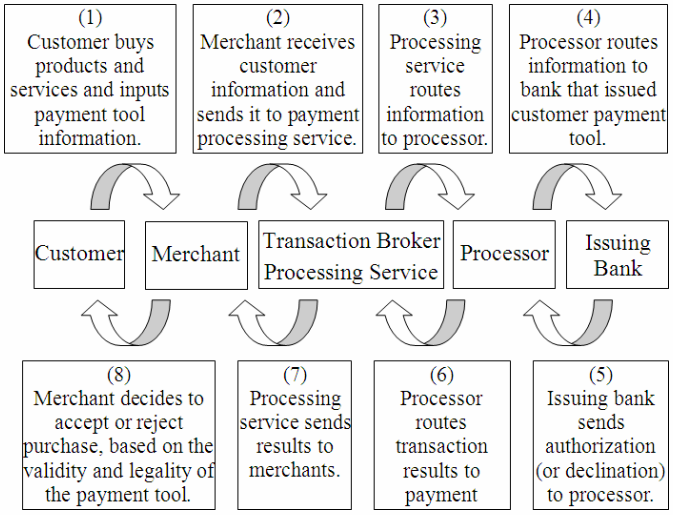

(1) Customer buys products and services and inputs payment tool information.
(2) Merchant receives customer information and sends it to payment processing service.
(3) Processing service routes information to processor.
(4) Processor routes information to bank that issued customer payment tool.
Customer
Merchant
Transaction Broker Processing Service
Processor
Issuing Bank
(8) Merchant decides to accept or reject purchase, based on the validity and legality of the payment tool.
(7) Processing service sends results to merchants.
(6) Processor routes transaction results to payment
(5) Issuing bank sends authorization (or declination) to processor.

Figure 1: Payment Processing Authorization cycle.

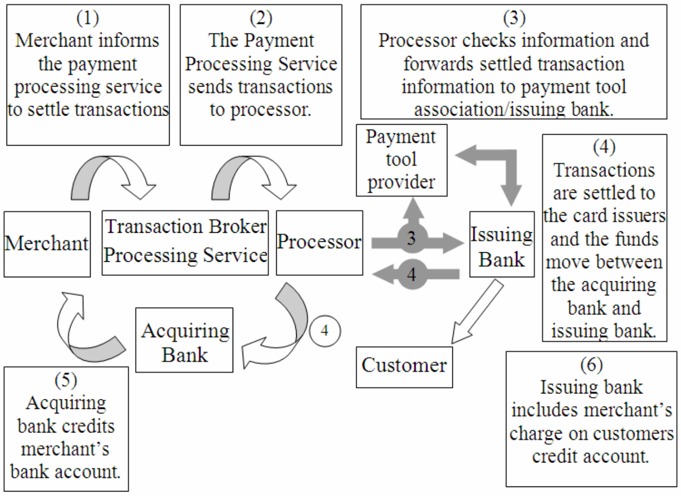

(1) Merchant informs the payment processing service to settle transactions
(2) The Payment Processing Service sends transactions to processor.
(3) Processor checks information and forwards settled transaction information to payment tool association/issuing bank.
Payment tool provider
(4) Transactions are settled to the card issuers and the funds move between the acquiring bank and issuing bank.
Merchant
Transaction Broker Processing Service
Processor
3
4
Issuing Bank
Acquiring Bank
4
Customer
(5) Acquiring bank credits merchant's bank account.
(6) Issuing bank includes merchant's charge on customers credit account.

Figure 2: Payment Processing Settlement cycle.

3. THE VARIABLE TRANSACTION NUMBER BARCODE (VTNB) METHOD

One of the major disadvantages of credit cards such as Visa, Master-Card and American Express, is the repetitive use of the fixed credit cards and the fixed verification numbers in all transactions. Because such numbers are easy to remember, it is relatively easy for some attackers to steal them. Some common ways are [13]:

- *Shoulder surfing*: An attacker watches a customer from a nearby location as the customer punches in his credit card number or listens in on the conversation if the customer gives his credit card number over the telephone to a hotel or car rental company.

- *Dumpster diving*: An attacker goes through a customer's garbage cans or a communal dumpster or trash bin to obtain copies of credit card statements or other records that bear the customer's identifying information.

- *Packet intercepting*: An attacker sniffs e-commerce packets during on-line credit card payment. In some cases, the attacker does not need to break down the possibly encrypted on-line payment packets (e.g., over Secure Socket Layer), but fools the customer into thinking that he/she is visiting an intended site but actually the attacker's spoofing site.

- *Database stealing*: To encourage easier purchasing, many merchants (who provide services to customers) choose to store credit card numbers in online databases. Recent news reported that attackers broke into merchants' sites and stole databases of millions of credit card numbers [2].

However, due to the fraudulent use, loss or damage problems, yearly, there is a significant financial loss [2]. Not only does the credit card fraud cause money loss, but also significant worry among customers.

A successful method for m-payment should depend on different factors such as: systematic simplicity and feasibility, short transaction delay, ease of use by the target customers, reliability, and interoperability between different vendors, security and technical feasibility of the transactions. The VTNB method will use the existing infrastructure and satisfy all of the above criteria.

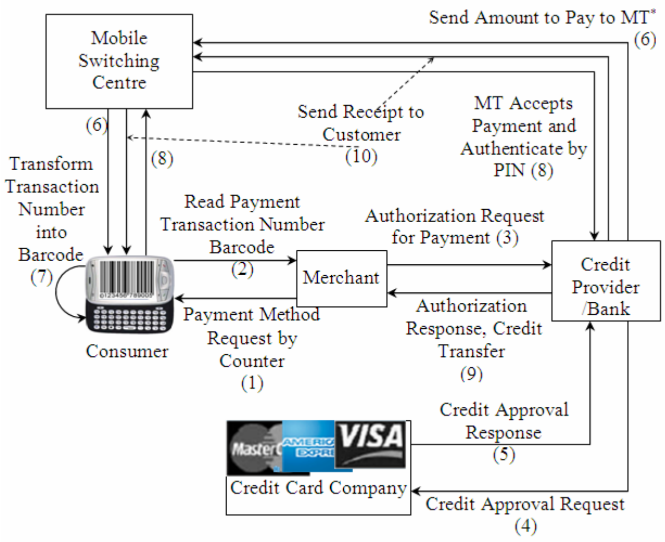
3.1. Systematic Simplicity and Feasibility

The systematic simplicity and feasibility refers to the additional hardware and software required to build the VTNB over the existing payment system. The VTNB system should also be fast, traversing minimum number of proprietary networks. This way, payment of small amounts is possible since network usage is limited and the overhead is low. This can be better understood with reference to Figure 3 below.

3.2. VTNB Protocol Layered Architecture

The choice of the protocol suite is a critical issue in designing fast and reliable data transmission. Hence, our survey among the available protocol suits revealed that either TCP/IP Protocol Suite or the OSI 7-Layered Architecture should be chosen in order to describe the layered protocol suit of VTNB. The OSI 7-Layered Architecture is chosen for the following reasons:

In TCP/IP Protocol Suite, the services offered by the IP layer (equivalent to the OSI network layer) are unreliable. It does not provide a mechanism for flow control and does not guarantee delivery nor notify the end host system about packet loss due to errors or network congestion. These responsibilities are assigned to the next higher layer (TCP). If the underlying network or inter-network service is unreliable, such as the case of IP, then a reliable connection-oriented transport protocol becomes quite complex [10]. The basic cause of this complexity is the need to deal with the relatively large and variable delays experienced between end systems.


Mobile Switching Centre
Send Amount to Pay to MT*
(6)
(6)
(8)
Send Receipt to Customer
(10)
MT Accepts Payment and Authenticate by PIN (8)
Transform Transaction Number into Barcode
(7)
Read Payment Transaction Number Barcode
(2)
Authorization Request for Payment (3)
Merchant
Credit Provider /Bank
Consumer
Payment Method Request by Counter
(1)
Authorization Response, Credit Transfer
(9)
Credit Approval Response
(5)
Credit Card Company
Credit Approval Request
(4)

* VTN for the next transaction is also transmitted along with the amount to pay. This will save time without creating security problems.

Figure 3: The VTNB system components and operation

These large, variable delays complicate the flow control and error control techniques. Also, the transport layer in TCP/IP does not always guarantee reliable delivery of packets as the transport layer in the OSI model does. TCP/IP offers an option called User Datagram Protocol (UDP), which also does not guarantee reliable packet delivery. Since the VTNB system is very sensitive to delays and security problems, the TCP/IP Protocol Suite does not guarantee fast and reliable data transmission.

The OSI transport layer protocol (TP4) and the Internet Transport Protocol (TCP) have many similarities but also some remarkable differences. One difference between TP4 and TCP to be mentioned is that, TP4 uses nine different TPDU (Transport Protocol Data Unit) types whereas TCP knows only one. This makes TCP simpler but every TCP header has to have all possible fields and therefore the TCP header is at least 20 bytes long whereas the TP4 header takes at least 5 bytes [15]. The header overhead in TCP/IP is very large for small packets. Another difference is the way both protocols react in case of a call collision. TP4 opens two bidirectional connections between the TSAPs, whereas TCP opens just one connection [15].

Furthermore, TCP does not perform well over links with high bit-error rates, such as wireless links. Since TCP was designed for wired networks, where bit-errors are uncommon and where packet drops nearly always are due to congestion, TCP always interprets packet drops as a sign of congestion and reduces its sending rate in response to a dropped packet, even though the network is not congested. This leads to low performance over wireless links where packets frequently are dropped because of bit-errors. TP4 uses a different flow control mechanism for its messages, which provides means for quality of service measurement. Being more general, The OSI model with its increased numbers of layers provides for more flexibility rather than the TCP/IP model. The protocols in the OSI model are better hidden than in the TCP/IP model and can be replaced relatively easily as the technology changes.

Each layer of VTNB protocol stack, shown in Figure 4, is described in the following section [10,11]:

Layer 1: VTNB Physical Layer (PHY): Defines a combination of wireless GPRS link (MT-BTS) and wired WAN (BTS-MSC-WAN……WAN-MSC-BTS). Maximum transmission rate equals to GPRS rate which can be up to 115 kbps, depending on the network availability, channel coding scheme and terminal capability.

Layer 2: VTNB Data Link Protocol (DLP): Channel sharing support mechanisms such as simultaneous channel sharing by multiple applications, are defined in this layer. Provides reliable data transfer by the means of flow control, error detection, error correction, and the control of data frame retransmission.

Layer 3: VTNB Network Layer (NL): responsible for establishing, maintaining and terminating connections (between the end-points) needed for the VTNB application.

Layer 4: VTNB Transport Protocol (TP): This defines the transport layer for the stack; i.e., the flow control for end-to-end data transmission fidelity on a per-VTNB-connection basis.

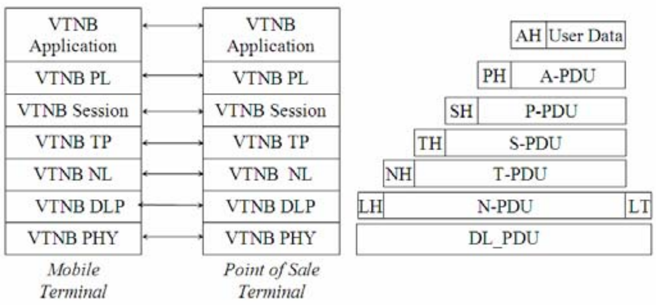
Layer 5: VTNB Session Layer (SL): Defines a session for each VTNB operation to transmit data objects between applications. Establishes, manages and terminates connections between cooperating applications during VTNB operation.

Layer 6: VTNB Presentation Layer (PL): PL relieves the VTNB application layer of concern regarding syntactical differences in data representation within the end-user systems. Encoding and Decoding of VTNB application data are also the responsibility of PL.

Layer 7: Application Layer for the VTNB: The application program is responsible for receiving the VTN through the GPRS line and transforming it into a barcode.

Steps (1) through (9) in Figure 3 are defined in the VTNB Application Layer Protocol. Accepting the payment amount and presenting the barcode for the merchant's barcode reader to initiate payment process is followed by verification of the VTN by the local bank. The software at the barcode reader's terminals should be updated so that the POS terminal is removed from the system. The on-line connection to the bank is provided by the computing terminal instead of the POS device. The protocol stack described above is displayed in Figure 4 below. It is obvious that there is a one-to-one correspondence with this diagram and Figure 2 in [3].

The interaction between the card and the POS terminal is replaced by the MT and the Barcode Reader (BCR). After the barcode is read, the transaction amount is transmitted to the MT screen, waiting for accept/reject payment response. Once the user accepts (by entering the PIN code on the MT) to pay the amount on the screen, the payment process is completed.



(A,P,S,T,L,N)H: (Application, Physical, Session, Transport, Network, Link) Header
PDU: Protocol Data Unit, LH: Link Header, LT: Link Trailer

Figure 4: The 7 layer VTNB Protocol Stack for connection management between the Mobile Terminal and Point of Sale terminal.

The VTNB payment system is suitable for other applications such as petrol stations, vending machines, buses, car parks, ATM's, cinema entrance, classroom attendance check etc.

3.3. Transaction Delay

Transaction delay is one of the most important factors for acceptability of an m-payment system. Detailed investigation studies have shown that such a delay should be less than 1 second [12]. The transaction delay in VTNB system is expected to be longer than that of the IrDA and similar to the conventional Credit Card (CC). The delay is due to the provision of the VTN by the credit company. The VTN is randomly drawn from a set with a negotiation between the CC network and the mobile terminal (MT), preferably as a function of the International Mobile Equipment Identity (IMEI) number of the MT. The provision of the VTN is a major issue in the proposed method of payment and more research is to be made to eliminate delay in generating VTN without compromising security. The delays involved are presented in Figure 5. Parameters effecting delay are; set-up time, connection time, data transfer time, processing time, security verification time and disconnection time. The following section clarifies the delay mechanism.

The transmission delay in VTNB includes, connection time and data transfer time. These include (connection from MT to the BTS, BTS to MSC, MSC to Bank (WAN), Bank to CC Company)×2. The components contributing to the time delay are shown in Figure 5. The VTN is obtained and stored in the MT during the initial registration to the VTNB service. In the next payment to make, VTN is transmitted along with the "Send Amount to Pay" signal (step 6 in Figure 3) through the GPRS line prior to payment time. There is always one extra transaction number stored in the MT. When the VTNB Application in Figure 3 is executed, the VTN is translated into a barcode and displayed on the screen. MT is now ready for payment. So, during a payment process, the following steps take place:

(1): The merchants counter asks for the payment method.

(2): The customer shows the barcode on the screen and the barcode is scanned by the barcode reader.

(3): The merchant asks the bank for authorization for payment.

(4): Credit approval request is sent from the bank to the credit provider.

(5): Credit approval sent to the bank.

(6): Send amount to pay to the MT. The VTN for the next transaction is also transmitted along with the amount to pay. This will save time without creating security problems. In case the VTN is lost or unusable, an algorithm should be developed for generating the VTN through the GPRS channel.

(7): Transform Variable Transaction Number into barcode.

(8): MT accepts payment and authenticates by PIN.

(9): Authorization response and credit transfer sent to the merchant. The receipt sent to the customer.

The timing diagram should be drawn in accordance with the above operational steps, as shown in Figure 5.

The timing diagram for the VTNB m-payment system is very similar to that of the CC payment system. The only difference is the usage of MT instead of CC. The magnetic stripe or micro chip in the CC is replaced by the VTNB in the MT, which could also be related to the International Mobile Equipment Identity (IMEI) number and the Personal Identification Number (PIN) code in the Subscriber Identification Module (SIM). The PIN code for the CC is replaced by the PIN code of the MT. The PIN code for the CC is replaced by the PIN code of the MT. The overall delay mechanism therefore, does not have any extra delay component other than those in the CC.

3.4. Ease of Use by the Target Customer

The usage of the VTNB technology is as simple as sliding a good in front of the barcode reader. Therefore, it is a candidate to be used by everyone and spread all around the world quickly. On top of all of the advantages introduced by the credit card system, such as simplicity, security and portability; this technology has the added advantage of using mobile telephones.

A set of global foundational m-payment standards need to be agreed upon in order for content providers to reach a critical mass of paying customers who, in turn, will then have a plentiful supply of applications and services to choose from. This will enable widespread availability of m-payment and the target customer range will also increase.

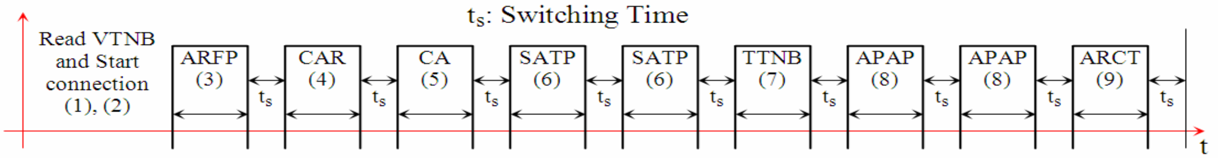


Figure 5: Timing diagram for the VTNB m-payment system

3.5. Security

VTN is made random in order to avoid photocopying and reproducing without the MT holders consent. VTN should be accompanied by the PIN number of the MT user. The process of entering PIN number to the POS machine is now replaced by entering the PIN number on your mobile, in privacy and comfort of your palm. User portability is provided by the SIM card.

Other security issues: The loss or theft of consumers' wallets with their physical credit cards will not be noticeable until the next time they carry out a purchase. This can occur anytime from immediately to several days later. However, the awareness of a loss or theft of one's MT can be felt more immediately.

Keeping and protecting the paper receipts for future reference is also a security issue in m-payment method. Paper receipts can be lost and cause consumer inconvenience and dissatisfaction in CC payment systems. However, the storage nature of the MT helps to protect receipts and work them out easily in the electronic form.

3.6. Transferability

VTN is transferable to third parties, such as a friend or relative. The VTN generated by a MT could be transmitted by Bluetooth, IrDA or MMS devices with an accompanying temporary PIN number, which is also transmitted along with the VTN. The credit provider should be informed about the transfer of the VTN so that the Barcode and the PIN number matching will be arranged.

4. CONCLUSION

The future m-payment services are expected to be simple, fast, easy to use, reliable, interoperable between different vendors, secure, and technically feasible. For such services to be successful, service provisioning by banks, operators and terminal manufacturers have to be independent from each other. Banks manage the authentication in their banking and payment services. Easy-to-use and fast-to-use services that offer value for money are the key success factors to wide-scale customer acceptance in mobile financial service area.

Due to the security gap in Credit Card usage, mobile telephones are better candidates as authentication and payment devices. The Variable Transaction Number Barcode system of m-payment is introduced as an alternative method of payment. This method is shown to be more efficient, faster and more secure than all of the other electronic payment systems

For prepaid mobile customers, the new m-payment solution will not require topping up their phone via scratch cards, credit cards, or ATM. VTNB solution delivers a high level of security as it requires a PIN for authentication of the user's identity. In addition, by providing payment direct from the user's bank account, m-payment means the spending power of users is not limited to the amount of credit available on their phone account.

5. REFERENCES

[1] Eliminating Some Credit Card Risk for E-Business, http://ecommerce.Internet.com/solutions/ec101/article/0,1467,6321_569741,00.html.

[2] Internet Usage Statistics – The Big Picture, http://www.internetworldstats.com/

[3] Pi Huang And A.C. Boucouvalas, Future Personal "E-Payment: Irfm", IEEE Wireless Communications, pp. 60-66, Feb. 2006.

[4] S. Schwiderski-Grosche and H. Knospe, "Secure Mobile Commerce", *Electronics & Communication Engineering Journal*, October 2002, pp. 228-238.

[5] S. F. Mjpllsnes and C. Rong, "On-line e-wallet system with decentralized credential keepers," *Mobile Network Applications,* vol. *8 ,* pp. 87--99,2003.

[6] IrDA, Infrared Financial Messaging Point and Pay Profile (IrFM), ver. 1.0, Dec. 2003.

[7] Bluetooth Core Specification, ver. 1.2+EDR, Bluetooth SIG, Nov. 2003.

[8] Weiping Z.H.U, Dong WANG and Huanye SHENG, "Mobile RFID Technology for Improving M-Commerce". Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE'05), March 2005, Shanghai, China.

[9] Raj BRIDGELALL, "Enabling Mobile Commerce Through Pervasive Communications with Ubiquitous RF Tags", Wireless Communications and Networking, WCNC 2003, Volume 3, Page(s):2041 – 2046, 16-20 March 2003.

[10] William Stallings, "Data and Computer Communications, Seventh Edition", Prentice-Hall, 2004.

[11] C.D. KNUTSON and J.M. BROWN, "IrDA Principles and Protocols:" The IrDA Library, Vol.1, MCL Press, 2004.

[12] H.R. DAMON, R.J. BROWN, and L. FAULKNER, White Paper, "Creating an End-To-End Digital Payment System," *IrDA Press*, Oct. 1999.

[13] Yingjiu Li and Xinwen Zhang, "A Security-Enhanced One-Time Payment Scheme for Credit Card", Proceedings of the 14th International Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications, RIDE-WS-ECEG'2004, Boston, USA , March 28-29, 2004.

[14] PayPal "Online Payment Processing", https://www.paypal.com/cgi-bin/webscr?cmd=_wp-pro-overview-outside.

[15] Sami IREN, Paul D. AMER and Phillip T. CONRAD, "The Transport Layer: Tutorial and Survey", *ACM Computing Surveys*, Vol. 31, No. 4, December 1999.

[16] Jan ONDRUS and Yves PIGNEUR, "Towards a Holistic Analysis of Mobile Payments: A Multiple Perspectives Approach", *Electronic Commerce Research and Applications,* 5 (2006) 246-257.