Performance Analysis of Mobile Payment Protocols over the Bluetooth Wireless Network

Rafael Martínez-Peláez[1], Francisco Rico-Novella[1], Cristina Satizábal[2] and Jhon J. Padilla[1, 3]

[1]Technical University of Catalonia, Telematics Engineering Department, {rafaelm, f.rico}@entel.upc.edu
[2]Pamplona University, Engineering and Architecture Department, isabel.satizabal@unipamplona.edu.co
[1, 3]Pontificia Bolivariana University, Electronic Engineering Department, jpadilla@upbbga.edu.co

Abstract

In the last years, mobile commerce have appeared thanks to the growth in the use of mobile devices, multiple wireless technology for personal communication and program language such as Java. A parallel step has been the design of new mobile payment protocols that provide strong security because the financial data is transmitted over wireless networks. In this sense, cryptographic operations are used to provide security services such as authentication, confidentiality, integrity and non-repudiation. Although the use of cryptographic operations enhance the network security, its use requires a priori high execution time of the CPU, battery consumption and storage capacity of the mobile device. On the other hand, the process to create and transmit each packet requires additional resources. For these reasons, the correct use of cryptographic operations is a key element in the development of mobile payment protocols. In this paper, we present a performance analysis of different mobile payment protocols. The performance analysis includes the computational cost required by each entity to perform all the cryptographic operations and the transmission time required to transmit each message. Our results show that the time taken to complete each protocol is acceptable.

Key words: Bluetooth technology, cryptography, computational cost, transmission time, Virtual POS, Real POS, KSL

1 Introduction

Mobile payment is defined as the process of exchanging financial values between two parties using a mobile device to pay for products or services [16]. With this new payment option, customers can pay for products and services anywhere and anytime with the comfort offered by their mobile devices. It is designed to operate with wireless technologies such as Bluetooth, Infrared or 802.11x

Mobile payment protocols have been examined in different papers. Research has been focused on studying the state of the art [3], [22]. In [7], Heijden has examined the successful factors of mobile payment systems. Also, in [4] they have to compose a security framework for ad hoc mobile payment. The performance of cryptographic operations on mobile devices have examined in [1], [20].

In previous work [17], we evaluated the computational cost required by customers and merchants to complete mutual authentication process with WTLS protocol using a hierarchical PKI infrastructure in a peer to peer (p2p) mobile payment scenario and compared it with an alternative mechanism, called TRUTHC [18]. Moreover, we evaluated the performance of mutual authentication process required by SET protocol in [14].

In this paper, we present a performance analysis assessment of four mobile payment protocols with different characteristics. The performance includes the computational cost carried out by each entity to perform cryptographic operations and the transmission time for each message stream. Specifically, we analysed virtual POS, real POS [11], KSL [9] and E-cash model [13], [12] protocols. The scenario is a network that modelled a piconet in Bluetooth with two nodes. The two nodes can for example be a mobile phone and PDA. We use RSA algorithm, DES algorithm and SHA-1 hash function to compute cryptographic operations for each mobile payment protocol. We considered the runtime of cryptographic operations described in [6], [20] and the transmission time of Bluetooth technology described in [2], [8].

The rest of the paper is organized as follows. In Section 2, we describe mobile payment and Bluetooth technology. In Section 3, we present the parameters that are common for all the analysis we have performed. In Section 4, we analyze virtual POS and real POS protocols. Section 5 presents the analysis of KSL protocol. E-cash model is described in section 6. Section 7 concludes the paper.

2 Background

2.1 Mobile Payment

Mobile payment provides a new option to pay for goods and services at anytime and anywhere using mobile devices such as mobile phones, laptops or PDAs. Mobile payment is defined as the process of exchanging financial values between two parties using mobile devices in return for goods or services. Below, we explain some on the basic concepts in this subject.

2.1.1 Types of Mobile Payment

Mobile payment systems inherited types of payment from electronic payment systems such as credit card schemes. Mobile payment systems can be classified according to the basis of payment [3], [22]:

Bank account: Customers must have a credit or debit card associated with a specific bank account. Customers disclose the information printed on the card such as card number, CVV2, expiration date, and name to merchant. Then, the merchant forward the information to Trusted Third Party (TTP). Finally, the TTP transfer the total amount of payment from customer's bank account to merchant's bank account.

Electronic cash: Customers must establish a business agreement with a TTP, called payment gateway. The main function of the payment gateway is convert real money to their electronic equivalent. Then, the electronic cash must be store in a secure device like smart cards or SIM to avoid frauds. The electronic cash have monetary value supported by financial institutions.

Phone bill: Customer should have a business agreement with a cell phone service provider. The business agreement consists of two parts: 1) cell phone service provider gives credit to customers for making calls and paying for goods or services; 2) customers pay the bill every month.

2.1.2 Mobile Payment Security

Mobile payment protocols must offer robust security because the financial data are sending over wireless networks. In this sense, customers and merchants require mutual authentication, payment authorization, confidentiality, integrity and non-repudiation [7], [19]. We describe the security factors as follows:

- Authentication: Mobile payment systems must offer the option to authenticate each entity (mutual authentication).
- Authorization: Mobile payment systems should request confirmation of the payment.
- Confidential: Mobile payment systems must avoid eavesdroppers have access to the messages.
- Integrity: Mobile payment systems must guarantee that the messages have not been modified.
- Non-repudiation: Mobile payment systems should avoid refuting payments.

2.2 Bluetooth Technology

Bluetooth is mainly oriented to establish a communication between closely devices instead of data transfer cables. Bluetooth is a wireless technology to interconnect mobile devices with each other or with other devices via point-to-many or point-to-point communications. This technology transfers voice, data, and video in real time. The transmission area is omni directional and its transfer rate is 1Mbps. The maximum distance between the data origin (source) and receiver is around 10m. Bluetooth technology transmits and receives on frequency band 2.45 GHz. Bluetooth technology is a key element in mobile commerce because it enables mobile devices to pay for goods or services [2], [5].

2.2.1 Baseband Layer

Bluetooth technology uses two link types to establish a connection among devices: synchronous connection oriented (SCO) and asynchronous connection less (ACL) links. SCO link establishes a point-to-point connection and is a symmetric dedicated link between two devices. On the other hand, ACL link establishes a point-to-multipoint connection and is an asynchronous link between all the devices. The first link type is a circuit switched connection between the master and slave, while the ACL link is a packet switched connection between the master and all the slaves. SCO link provides guaranteed delay and bandwidth to transmit average quality voice and music by the use of link management protocol (LMP). LMP performs link configuration such as quality of service (QoS) [5].

ACL links are appropriate for non-real time transmission data. This means that, applications requiring different QoS parameters cannot be supplied. There are two different ACL link packets: 1) DMx, which the payload is encoded, and 2) DHx which the payload is unprotected. The value of x stands for the number of slots that is required to transmit the packet. DMx types are DM1, DM3 and DM5, which includes forward error correction (FEC), cyclic redundancy check (CRC) code and automatic repeat request (ARQ). The payload header is one or two bytes long, depending on packet type and its specification such as logical channel, user payload length and flow control [2]. Table 1 summarizes the ACL packet characteristics [2]:

Table 1 Characteristics of ACL packets

					Asymmetric max rate (Kbps)	
Type	User Payload (bytes)	FEC	CRC	Symmetric max rate (Kbps)	Forward	Reverse
DM1	0-17	2/3	YES	108.8	108.8	108.8
DM3	0-121	2/3	Yes	258.1	387.2	54.4
DM5	0-224	2/3	Yes	286.7	477.8	36.3
DH1	0-27	no	Yes	172.8	172.8	172.8
DH3	0-183	no	Yes	390.4	585.6	86.4
DH5	0-339	no	Yes	433.9	723.2	185.6

2.2.2 Physical Layer

Bluetooth technology operates on the radio frequencies of 2.4 GHz band. The band is divided into 79 MHz wide channels that are spaced of 1 MHz. This layer utilizes a frequency hopping spread spectrum (FHSS) as technique of transmission. FHSS can reduce the impact of jamming and interference caused by other systems. The transmission channel changes 1600 times per second. Bluetooth technology uses a slotted time division duplex (TDD) scheme for duplex transmission, where transmission frequency for each slot is 625μs. Each slot corresponds to a different

packet. The master uses the even numbered time slots to transmit, while the slaves use the odd numbered time slots [5]. The frame structure is shown in figure 1.

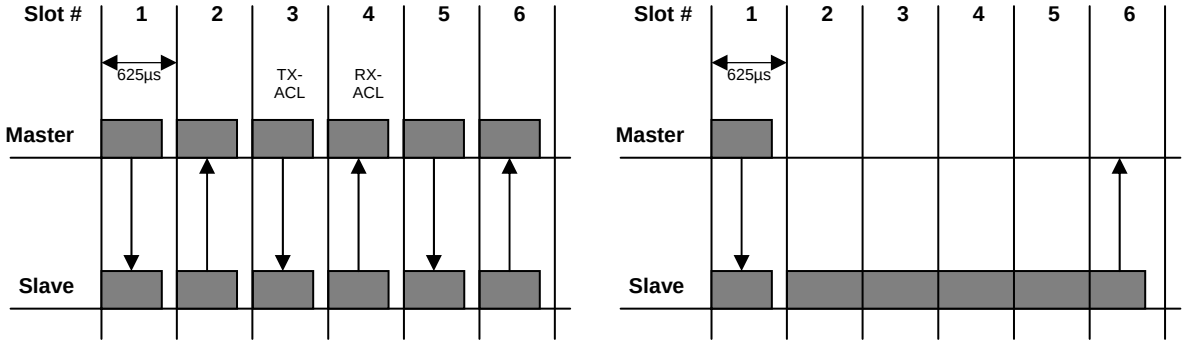

Figure 1: Transmissions of single-slot and multi-slots packet

3 Methodology

We begin by describing in detail the parameters used to evaluate the efficiency of the mobile payment protocols.

We assume that the customer's terminal is a mobile phone Nokia 6600 [20] and the other entities use a PDA. The PDA platform is a Compaq iPAQ H3630 with a 206MHz StrongARM processor and 32MB in RAM [6]. For the analysis of the investigated protocols, we employed RSA algorithm, DES algorithm and SHA-1 hash function. When the mobile payment protocols required a communication link among the entities, we used Bluetooth technology. The network modelled is a piconet in Bluetooth with two nodes where the master is the merchant and the slave is the customer.

3.1 Scenario

A mobile device with Bluetooth may operate in either master or slave mode. In the scenario defined in this paper, the merchant operates in master mode while the customers operate in slave mode, which is the simplest configuration of a Bluetooth network. The other piconet can be built between the merchant and bank. In order to simplify the analysis, we considered the communication between one slave and master as show in figure 2.

Under this scenario, we considered the following cases:

1. The customer performs all the mobile payment protocol using a mobile phone Nokia 6600 and merchant uses a PDA.
2. The client and merchant perform all the operations of each mobile payment protocol using a PDA.

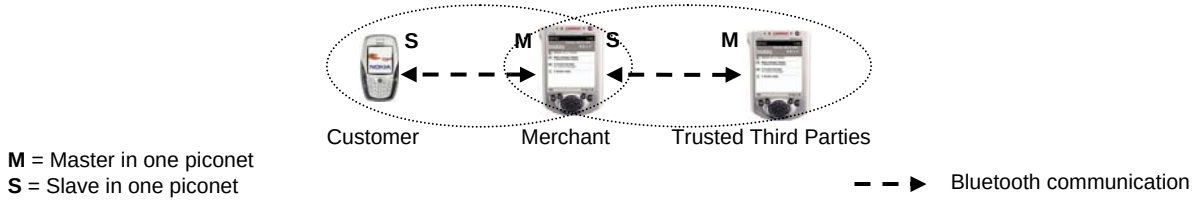

Figure 2: Scenario of study

3.2 Data Packet Characterization

A realistic characterization of the traffic is quite difficult due to the lack of an exact knowledge of the packets' length transmitted during the operation of each mobile payment protocol. For that reason, we modelled the length of each packet transmitted between the customer and merchant in a piconet scenario. We decided to use DH5 packets in the analysis.

The total size of the packet is fixed in the payload of each ACL packets with a length of 339 bytes and each ACL packet fits into 5 slots. A packet that arrives at the Bluetooth layer consists of three parts: 1) an IP header with 20

bytes; 2) a TCP header with 32 bytes; 3) a data with variable length. In addition, L2CAP adds 4 bytes as channel identification and packet length [8]. The format of ACL packet is shown in figure 3.

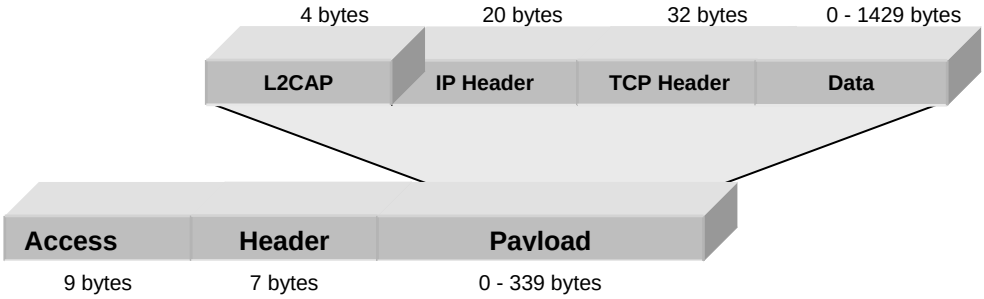

Figure 3: ACL packet structure

3.3 Computational Cost

We use equation (1) to compute the computational cost (*COST*) of the cryptographic operations carried out by the customer, merchant and trusted third parties in the different mobile payment protocols. The definition of the computational cost expresses the performance of the mobile devices to complete the mobile payment protocols. We define the number of public key operations encryption/decryption with OP_{ENC} and OP_{DEC}, the number of signature creation/verification with OP_{SIG} and OP_{VER}, the number of symmetric key operations encryption/decryption with OP_{SYM}, and the number of hash function with OP_{HASH}. The execution time of each operation is defined with T_X where *x* denotes the operation.

$$COST = (OP_{ENC} * T_{ENC}) + (OP_{DEC} * T_{DEC}) + (OP_{SIG} * T_{SIG}) + (OP_{VER} * T_{VER}) + (OP_{SYM} * T_{SYM}) + (OP_{HASH} * T_{HASH}) \quad (1)$$

The analysis was performed using two RSA keys with equivalent security [10]. The PDA uses a RSA key of 2,048 bits size, with small public exponent (65,537). The execution time of encryption and verification operations with RSA algorithm is 0.0039s/operation while the decryption and signature operations require 1.274s/operation. On the other hand, the mobile phone Nokia 6600 uses a RSA key of 1,937 bits size. The implementation of RSA-1937 bits is based on the IAIK JCE micro edition, which uses the Chinese Remainder Theorem and Montgomery multiplication. In this case, the execution time of encryption and verification operations with RSA algorithm is 0.00157s/operations, and the decryption and signature operations require 7.125s/operation. Moreover, we consider the execution time of encryption and decryption operations with DES algorithm is 0.00102s/operation and the execution time of SHA-1 is 0.0004s/operation with a payload of 160 bits. Finally, we consider the size of the certificate is 700 bytes according with the WAP Forum. [21].

3.4 Transmission time

We assume an ideal channel without packet lost and we consider a multi-slot packet transmission.

In order to initialize a new communication, the master device uses the inquiry procedure (Inq_p) and page scheme (Pag_s) to discover and establish a new communication with slave devices. The average time for the inquiry phase is 0.71s and 0.64s for the page phase [5].

Let us introduce some notation adopted in this paper. For the total size of the packet *L*, we denote with *U* the payload of each ACL packets (type DH5). We will refer to the number of ACL packets with N_{DH5}, so that, we have:

$$N_{DH5} = L/U \quad (2)$$

Now we can determine the delay (*D*) caused by the segmentation on TCP layer (TCP_D), IP layer (IP_D), L2CAP layer ($L2CAP_D$) and Baseband layer ($Base_D$), where its values are 1µs, 1µs, 1ms and 1ms, respectively [8].

$$D = TCP_D + IP_D + L2CAP_D + Base_D \quad (3)$$

Furthermore, we indicate with S_T the total number of slots used to transmit the ACL packets, we have:

$$S_T = \left(\frac{N_{DH5} * DH5}{1} + \frac{N_{DH5} * DH5}{5} \right) - 1 \quad (4)$$

After we obtained the S_T, we know the total number of slots used to transmit the ACL packet and the slots empty.

The whole transmission time (T_T) to transmit each message is given by equation 5, where T_{SLOT} is the transmission frequency (625μs).

$$T_T = (ST * T_{SLOT}) + D \quad (5)$$

4 Virtual and Real Point of Sale (POS)

Hassinen et al. proposed two mobile payment protocol using the PKI provided by the Finnish Population Register Centre (PRC) to provide public key services such as authentication, encryption and signature creation/verification [11]. The private keys can be store in SIM cards for mobile phones by means the Finnish Electronic Identification (FINEID). The structure of the PKI is hierarchical with one CA, so that, all the participants trust in the same root CA.

4.1 Virtual POS

In this protocol, the merchant is a service provider that accepts mobile payments. The communication between the customer and merchant is established using Bluetooth. The payment scheme is as follows:

1. Merchant discovers and associates customer's mobile phone.
2. Customer (C) initiates the protocol requesting the product options to Merchant (M).
3. M sends a list with the service options.
4. C responses with his product selected from the service list signed with his private key K_C^{-1} and his private key K_C^{-1} encrypted with merchant's public key K_M.
5. M decrypts the message using his private key K_M^{-1} and verifies the signature. Then, he encrypts the payment request using K_B and sends it to Bank (B).
6. B receives the message and decrypts it using his private key K_B^{-1}. B transfers the total amount of Money (AM) from C's account to M's account. B sends to M the payment confirmation message signed with his private key K_B^{-1}.
7. M verifies the signature and checks the status of the payment. M forwards the message to C and the product is delivered.

Table 2 summarizes the cryptographic operations performed by the customer and merchant.

Table 2 Cryptographic operations carry out by customer and merchant in Virtual POS protocol

Cryptographic operation	Customer	Merchant	Bank
Encryption	1	1	0
Decryption	0	1	1
Signature creation	2	1	1
Signature verification	1	2	2
Symmetric encryption/decryption	0	0	0
Hash function	5	5	6

We can use the number of cryptographic operations carried out by each entity to determine the *COST* of virtual POS protocol using equation (1).

$$CustomerCOST = (1 * T_{ENC}) + (2 * T_{SIG}) + (1 * T_{VER}) + (5 * T_{HASH})$$

$$MerchantCOST = (1 * T_{ENC}) + (1 * T_{DEC}) + (1 * T_{SIG}) + (2 * T_{VER}) + (5 * T_{HASH})$$

The *COST* required by the customer, merchant and bank to perform the cryptographic operations in the first case is 14.566s, 2.667s and 2.628s respectively. In the second case, the customer requires 2.628s while the merchant and bank do not have modifications.

In order to investigate the transmission time to exchange all the messages between the customer and merchant, we estimated the length of each packet and the transmission parameters. Table 3 describes the length of each packet exchanged between the customer and merchant during the protocol. We believe are realistic values for this mobile payment protocol. N_{DH5} provides criteria to identity the number of ACL packets required to transmit the packet length. So we used equation (2), where the length of each packet is described in table 3 and the *U* is 339 bytes. The ACL packets for each message are described in table 3. Equation (3) defines the number of slots required to transmit the ACL packets of DH5 type. The definition of the slots expresses the time to transmit the entire ACL packet

considering the empty slots. Equation (4) and (5) are used to determine a realistic transmission time considering the delay generated by the segmentation process in each layer.

The transmission time required for exchanging the messages between the customer and merchant is 1.414s and between the merchant and bank is 1.388s; these times include the inquiry and page phases. Table 3 summarizes the time for each message exchanged among the entities.

Table 3 Transmission parameters considered in Virtual POS protocol

Message	Data (*bytes*)	Packet length (*bytes*)	ACL packets N_{DH5}	Slots S_T	T_T (*s*)	Ing_p (*s*)	Pag_s (*s*)
1	-	-	-	-		0.71	0.64
2	500	556	2	11	0.0088	-	-
3	1200	1256	4	23	0.0163	-	-
4	2320	2376	8	47	0.0333	-	-
5	2480	2536	8	47	0.0333	-	-
6	160	216	1	5	0.0051	-	-
7	160	216	1	5	0.0051	-	-

The whole time including *COST* and T_T is 22.663s in the first case and 10.725s in the second one. Although the observed time is significant, it does not prohibit the use of virtual POS protocol on mobile devices since the worst time is 22.663s.

4.2 Real Point of Sale (POS) protocol

In this protocol, the merchant accepts mobile payments. The communication between the customer and merchant is established using Bluetooth. The communication between the merchant and bank is established using another communication system. The process of the protocol is described as follows:

1. Merchant discovers and associates customer's mobile phone.
2. Customer (C) initiates the protocol requesting the product options to Merchant (M)
3. M sends to C his certificate ($Cert_M$), random nonce (N_M) and product list.
4. C responses with his product selection (S) and random nonce (N_C) encrypted with merchant's public key K_M, his certificate ($Cert_C$) concatenated with the signature of S, N_M and N_C. The signature is created with its private key K_C^{-1}.
5. M verifies the signature and decrypts the message using his private key K_M^{-1}. M sends the payment request message signed with his private key K_M^{-1} to C.
6. C verifies the signature. C creates and sends to Bank (B) the payment order message (PO) and its signature.
7. B verifies the signature and processes the payment. Then, B sends to C the response message signed with its private key K_B^{-1}.
8. C verifies the signature. C adds the bank's id (ID_B) in the messages and sends it to M.
9. M verifies the response message.

Table 4 summarizes the cryptographic operations carried out by the customer and merchant.

Table 4 Cryptographic operations perform in Real POS protocol

Cryptographic operation	Customer	Merchant	Bank
Encryption	2	0	0
Decryption	0	1	1
Signature creation	3	2	1
Signature verification	3	2	2
Symmetric encryption/decryption	0	0	0
Hash function	6	4	3

According with table 4, we can determine the COST required by each entity using equation (1). The *COST* required by a customer in the first case is 22.162s and 4.019s in the second one. On the other hand, the merchant and bank require 3.901s and 2.627s in both cases. The whole COST to perform all the cryptographic operations by the customer, merchant and bank in the first case is 28.691s and 10.548s in the second one. We must note at this point that the best performance depends on the capability of the CPU and the crypto library used to program the cryptographic operations.

For our test, we used the packet length described in table 5. Table 5 summarizes the number of ACL packets, number of slots required to transmit each ACL packet and T_T. The total time expended by the customer and

merchant to exchange all the messages in both cases is 1.438s. On the other hand, the customer and bank required 1.401s to exchange two messages.

Table 5 Transmission parameters considered in Real POS protocol

Message	Data (*bytes*)	Packet length (*bytes*)	ACL packets N_{DH5}	Slots S_T	T_T (*s*)	Ing_p (*s*)	Pag_s (*s*)
1	-	-	-	-		0.71	0.64
2	500	556	2	11	0.0088	-	-
3	7920	7976	24	143	0.0933	-	-
4	6684	6740	20	119	0.0763	-	-
5	1320	1376	5	29	0.0201	-	-
6	3480	3536	11	65	0.0466	-	-
7	160	216	1	5	0.0051	-	-
8	660	716	2	11	0.0088	-	-

The whole time (*COST* + T_T) required between the customer and merchant is 12.902s in the first case and 6.815s in the second. On the other hand, the whole time carried out by the customer and bank is 18.750s in the first case and 6.694s in the second one. We considered the *COST* and T_T where the customer and merchant exchanged messages and carried out some cryptographic operation, such as steps 2, 3, 4, 5, 8 and 9. In addition, we considered the discover and association phases that are necessary to establish a new communication. The observed overhead caused by the transmission time is less significant in comparison with the high time required to establish a new communication in a Bluetooth network.

5 KSL protocol

S. Kungpisdan et al proposed a mobile payment protocol, called KSL [9]. This protocol reduces the number of public key operations carried out by the customer in SET protocol [15]. The customer must establish a business relation with a merchant to obtain a symmetric key. The symmetric key is used to encrypt messages exchanged with the merchant. In this case, each merchant must to store *n* symmetric keys. Because of the storage capacity is out of the scope of this paper, we do not analyze it. The payment procedure is defined as follows:

1. Merchant discovers and associates customer's mobile phone.
2. Customer (C) sends to Merchant (M) the requesting message of the transaction date.
3. M responses with the transaction date (TID) and his id (ID_M) encrypted with the symmetric key X_i.
4. C sends to M the order information encrypted with the symmetric key X_i.
5. M decrypts and verifies the message. M creates and sends to Payment Gateway (PG) the order information and payment information encrypted with the payment gateway's public key K_{PG}, and transaction date signed with merchant's private key K_M^{-1}.
6. PG verifies the signature and decrypts the order information. PG forwards to issuer (I) the information unencrypted.
7. PG sends to acquirer (A) the price and ID_M.
8. I and A accepts or rejects the payment transaction. I sends to PG the response message encrypted with symmetric key Y_i and the response YES/NO unencrypted.
9. PG encrypts the response YES/NO with merchant's public key K_M and signs it with his private key K_{PG}^{-1}. PG sends to M the original response messages and his response.
10. M verifies the signature and decrypts de message. Then, M encrypts the original response message and sends it to C.
11. C verifies the response.

Table 6 summarizes the cryptographic operations carried out by the customer and merchant.

Table 6 Cryptographic operations perform by the customer, merchant and payment gateway

Cryptographic operation	Customer	Merchant	Payment Gateway
Encryption	0	1	1
Decryption	0	1	1
Signature creation	0	1	1
Signature verification	0	1	1
Symmetric encryption/decryption	3	4	0
Hash function	3	3	0

According with table 6, we can determine the *COST* required by the customer, merchant and payment gateway to perform the cryptographic operations indicated in the protocol using equation (1). The customer needs to carry out three symmetric key operations and three hashing operations. Therefore a successful completion of these cryptographic operations requires 0.004s. On the other hand, the merchant requires 2.631s to perform four public

key operations, four symmetric key operations and three hashing operations, and the bank requires 2.626s. It is obvious that the *COST* required by the customer is less expensive than the merchant. Although the merchant requires more processing power to compute the cryptographic operations than the customer, its *COST* is suitable.

This protocol requires several messages exchanged among different entities. We defined the transmission parameters for all the messages in Table 7. We used equations (2) and (3) to determine the number of ACL packets and number of slots required to transmit the payload. Then, we used equations (4) and (5) to determine the full time to transmit each slot.

Table 7 Transmission parameters considered in KSL protocol

Message	Data (*bytes*)	Payload (*bytes*)	ACL packets N_{DH5}	Slots S_T	T_T (*s*)	Ing_p (*s*)	Pag_s (*s*)
1	-	-	-	-		0.71	0.64
2	2500	2556	8	47	0.0333	-	-
3	1000	1056	4	23	0.0163	-	-
4	4044	4100	13	77	0.0541	-	-
5	4320	4376	13	77	0.0541	-	-
6	4320	4376	13	77	0.0541	-	-
7	1000	1056	4	23	0.0163	-	-
8	660	716	3	17	0.0126	-	-
9	1320	1376	5	29	0.0201	-	-
10	600	656	2	11	0.0088	-	-

The successful exchange of message between the customer and merchant requires 1.462s, between the merchant and the payment gateway is 1.424s and between the payment gateway and bank is 1.433s. Each communication includes discover and association phases previous to initialize any transmission. The calculated time needed for the completion of the protocol is 9.581s. We have taken into account the transmission time needed between the payment gateway and bank, and the time required by both entities to perform the cryptographic operations.

6 E-cash Model: A Script Anonym

We proposed a payment protocol based on a new e-cash [13], [12]. This protocol is suitable for electronic and mobile payments. After the customer and merchant finalized the authentication protocol, they generate a shared key. The payment scheme is as follows:

1. Merchant discovers and associates customer's mobile phone.
2. Customer (C) initializes the protocol sending the product list request message to merchant (M).
3. M responds sending the product list.
4. C sends to M his/her product selection encrypted with a symmetric key established in previous phase using SSL protocol
5. M responds with AEPO (agreement of electronic payment order). The AEPO is encrypted with a symmetric key.
6. C decrypts the AEPO and verifies the total amount. If the total amount is correct, he computes the electronic cash using hash chain and sends it is encrypted using his private key to M, in the other case, the transaction is finalized.
7. M decrypts the electronic cash. He computes the hash value of AEPO and sends to payment gateway (PG), the AEPO, H(AEPO), the certificate of customer c ($Cert_C$) and electronic cash.
8. PG verifies the hash value of the AEPO and decrypts the electronic cash. Finally, he computes the hash chain. If the hash chain is correct he deposits the payment in merchant's account and responds with the accept message, in the other case, the responds with the reject message. The messages are encrypted with a symmetric key.
9. M verifies the responds message and forwards it encrypted with the symmetric key to C.
10. C verifies the responds message.

Table 8 summarizes the cryptographic operations carried out by the customer, merchant and payment gateway.

Table 8 Cryptographic operations perform by customer and merchant and payment gateway

Cryptographic operation	Customer	Merchant	Payment Gateway
Encryption	1	0	0
Decryption	0	2	2
Signature creation	0	0	0
Signature verification	0	0	0
Symmetric encryption/decryption	4	6	2
Hash function	0	1	1

In this case, the customer and merchant establish a secure channel using SSL protocol to communicate with it does not share a secret key. The entire protocol has two phases. In the first phase, the customer and merchant exchange certificates to authenticate each other and generate a shared key. The second phase is the payment protocol where all the exchange of message between the customer and merchant are encrypted using the shared key. The successful completion of the cryptographic operations requires 5.266s in the first case and 5.148s in the second. This means that, the customer requires 0.161s, the merchant requires 2.554s and the payment gateway requires 2.55s.

Table 9 describes the transmission parameters used for our test.

Table 9 Transmission parameters considered in E-cash model protocol

Message	Data (*bytes*)	Payload (*bytes*)	ACL packets N_{DH5}	Slots S_T	T_T (*s*)	Ing_P (*s*)	Pag_P (*s*)
1	-		-	-		0.71	0.64
2	500	556	2	11	0.0078	-	-
3	1000	1056	4	23	0.0153	-	-
4	112	168	1	5	0.0041	-	-
5	2000	2056	7	41	0.0276	-	-
6	2064	2120	7	41	0.0276	-	-
7	2924	2980	9	53	0.0351	-	-
8	660	716	3	17	0.0116	-	-
9	660	716	3	17	0.0166	-	-

The transmission time between the customer and merchant requires 1.444s and between the merchant and payment gateway is 1.396s. The whole time to exchange all the messages is 2.841s. The complete time to perform the protocol is 8.106s in the first case and 7.988s in the second.

7 Conclusions

We have presented a performance analysis of four mobile payment protocols considering its computational cost and transmission time. The results obtained in the analysis carried out in this paper demonstrate the feasibility of using mobile payment protocols with strong security on mobile devices. In addition, we have presented the benefit of Bluetooth wireless technology related with the transmission time and its feasibility to operate in a personal area network for mobile payment transactions. We believe that the results obtained in this study are realistic although we did not consider the runtime performance in the authentication process of each protocol.

We have observed that the discover and association phases increase the transmission time among the entities. However, the relatively low transmission time of each message decreases the whole transmission time making a Bluetooth a good wireless technology in scenarios where the transmission area is short.

It is obvious that the merchant requires computing less cryptographic operations and creating fewer messages than the customer because of the limited battery consumption. Unfortunately, the four mobile payment protocols analyzed in this paper require high runtime of the CPU from the merchant's point of view.

The difference between the first case and second one in each mobile payment is the capacity of the CPU. Mobile devices with more powerful processor and more memory can reduce the execution time of each mobile payment protocol.

Although the results presented in this paper are acceptable, our future work involve the performance analysis of mobile payment protocols using elliptic curve cryptography (ECC) instead of RSA. We want to compare the benefits of the two cryptographic schemes with each other; for that reason, we need to validate its performance.

Acknowledgement

This work has been supported in part by the Spanish public funded projects ARES (CONSOLIDERINGENIO-2010 CSD2007-00004) and ITACA (TSI2006-13409-C02-02), and graduate scholarship from CONACYT (Mexico).

Reference

[1] P. Argyroudis, R. Verma, H. Tewari, and D. O'Mahony, Performance Analysis of Cryptographic Protocols on Handheld Devices, in Proceedings of the Third IEEE International Symposium on Network Computing and Applications (NCA'04), Massachusetts, USA, 2004, pp. 169-174.

[2] R. Bruno, M. Conti, and E. Gregori, Bluetooth: Architecture, Protocols and Scheduling Algorithms, Cluster Computing, vol. 5, pp. 117-131, 2002.

[3] Y. B. Choi, R. L. Crowgey, J. M. Price, and J. S. VanPelt, The state-of-the-art of mobile payment architecture and emerging issues, International Journal of Electronic Finance, vol. 1, pp. 94-103, 2006.

[4] M. L. Das, A. Saxena, and V. P. Gulati, A security framework for mobile-to-mobile payment network, in Proceedings of the IEEE International Conference on Personal Wireless Communications, (ICPWC'05), 2005, pp. 420- 423.

[5] E. Ferro and F. Potorti, Bluetooth and Wi-Fi wireless protocols: a survey and a comparison, IEEE Wireless Communications, vol. 12, pp. 12-26, 2005.

[6] V. Gupta, S. Gupta, S. Chang, and D. Stebila, Performance Analysis of Elliptic Curve Cryptography for SSL, in Proceedings of the 3rd ACM Workshop on Wireless Security, Georgia, USA, 2002, pp. 87-94.

[7] H. v. d. Heijden, Factors affecting the successful introduction of mobile payment system, in Proceedings of the 15th Bled Electronic Commerce Conference eReality: Constructing the eEconomy, Slovenia, 2002, pp. 430-443.

[8] N. Johansson, M. Kihl, and U. Körner, TCP/IP Over the Bluetooth Wireless Ad-hoc Network, in Proceedings of the the IFIP-TC6 / European Commission International Conference on Broadband Communications, High Performance Networking, and Performance of Communication Networks, 2000, pp. 799-810.

[9] S. Kungpisdan, B. Srinivasan, and P. D. Le, Lightweight Mobile Credit-Card Payment Protocol, in Proceedings of the 4th International Conference on Cryptology in India, Progress in Cryptology, INDOCRYPT, New Delhi, India, 2003, pp. 295-308.

[10] A. K. Lenstra and E. R. Verheul, Selecting Cryptographic Key Sizes, in Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptography (PKC'00), Victoria, Australia, 2000, pp. 446-465.

[11] M. Hassinen, K. Hyppönen, and K. Haataja, An Open, PKI-Based Mobile Payment System, in Proceedings of the International Conference on Emerging Trends in Information and Communication Security, (ETRICS '06), 2006, pp. 86-100.

[12] R. Martínez Peláez and F. J. Rico Novella, Application of Electronic Currency on the Online Payment System like PayPal, in Proceedings of the 6th IFIP Conference on e-Commerce, e-Business and e-Government, (I3E'06), 2006, pp. 44-56.

[13] R. Martínez-Peláez and F. J. Rico-Novella, NEW ELECTRONIC CASH MODEL: A SCRIPT ANONYM, in Proceedings of the IADIS International Conference on e-commerce, (e-commerce'06), 2006, pp. 392-396.

[14] R. Martínez-Peláez, C. Satizabal, F. Rico-Novella, and J. Forné, Efficient Certificate Path Validation and Its Application in Mobile Payment Protocols, in Proceedings of the 3rd International Conference on Availability, Reliability and Security, (ARES'08), 2008, pp. 701-708.

[15] Mastercard and VISA, "SET Secure Electronic Transaction Specification," 1997.

[16] S. Nambiar, C. T. Lu, and L. R. Lian, Analysis of Payment Transaction Security in Mobile Commerce, in Proceedings of the IEEE International Conference on Information Reuse and Integration (IRI'04), Nevada, USA, 2004, pp. 475-480.

[17] C. Satizabal, R. Martínez-Peláez, J. Forné, and F. Rico-Novella, Reducing the Computational Cost of Certification Path Validation in Mobile Payment, in Proceedings of the 4th European PKI Workshop, (EuroPKI'07), Mallorca, Spain, 2007, pp. 280-296.

[18] C. Satizabal, R. Paez, and J. Forne, WAP PKI and certification path validation, International Journal of Internet Protocol Technology, vol. 2, pp. 88-95, 2007.

[19] T. H. Shon and P. Swatman, Identifying effectiveness criteria for Internet payment systems, Internet Research, vol. 8, pp. 202-218, 1998.

[20] S. Tillich and J. Grobschädl, A Survey of Public-Key Cryptography on J2ME-Enabled Mobile Devices, in Proceedings of the 19th International Symposium on Computer an Information Sciences (ISCIS'04), Antalya, Turkey, 2004, pp. 935-944.

[21] WAPForum, "WAP Certificate and CRL Profiles, Specification WAP-211-WAPCert-20010522-a," 2001.

[22] K. Wrona, M. Schuba, and G. Zavagli, Mobile Payments - State of the Art and Open Problems, in Proceedings of the 2nd International Workshop on Electronic Commerce, (WELCOM'01), 2001, pp. 88-100.