Security in Near Field Communication for m-payment service

Tasnuva Ali[1], M. Abdul Awal[2]
[1]ETE Department, Daffodil International University, Dhaka, Bangladesh
[2]EECS Department, North South University, Dhaka, Bangladesh

Abstract— *Near Field Communication technology is a short range wireless communication interface that allows for the assimilation of a mobile in existing contactless applications infrastructure. Therefore, these m-payment applications are being expanded for both online and in-store purchases that offer both security as well as ease of use for the customers. In this paper, we present a NFC gateway protocol for network driven services and a secure authentication process for m- payment system with existing wireless communication network.*

Keywords — *NFC, POS, Gateway Protocol.*

I. INTRODUCTION

Near field communication is a new short-range wireless connectivity technology that provides a simple two-way interactions between electronic devices. Therefore, consumers can perform contactless transactions and access digital contents to connect NFC enabled devices with a single touch. This independent system is a combination of RFID and contactless card technologies with the purpose of creating independent communication such as secure mobile payment and data store functions [1]. Hence, this procedure can be classified into four groups such as touch-and-go, touch-and-confirm, touch-and-connect and touch-and-explore.

The standard of NFC allows peer to peer communication between NFC-enabled devices like NFC phone and NFC point of sale (POS), called wireless near field communication technology that allows variety of business opportunities like m-payment system, public transport ticketing system, peer to peer data transfer system etc [3]. The point of sales (POS) terminal has dual interface such as RF interface to the host computer and wire interface to the mobile phone implementing the bar code or tag or more complex functionality of a NFC device. Due to the new NFC based m-payment solution, crowded check-out counters can be avoided improving customer satisfaction and eliminating the need for staying in line to wait until others finish their own transactions [4]. This physical connection between two devices is established through bringing these devices close to each other that should not be more than twenty centimetres distance.

In this paper, a new gateway protocol with its authentication process related to security has been proposed in detail between client applications and NFC gateway using the accessible wireless network.

II. GATEWAY PROTOCOL

NFC gateway protocol is a special type of protocol that has been designed to communicate between cellular phone and NFC point of sale gateway. As per client requirement, the NFC based mobile phone sends a specific service request to the server for set-up the connection between phone and wireless network. After getting the acknowledgement from the server and the confirmation of the mobile number, bar code or RFID tag from the client, the NFC gateway performs the final transactions using the available wireless mobile network.

TABLE I
NFC GATEWAY RESPONSE PROTOCOL

0-15 bits	16-23 bits	24-31 bits	32-47 bits	48-63 bits
Payload or start Flag	Major version	Minor version	Message type or flag	Length of message bit

In this paper, the proposed header field is divided into five groups such as 16 bits start bit or payload field, 8 bits major version, 8 bits minor version, 16 bits message type or flag while 16 bits length field represents the client's message size. The maximum size of the sender identity information and NFC tag ID is 32 bits and 64 bits respectively.

Figure 1 shows the NFC transport layer gateway key negotiation for set up a secure communication channel between customer mobile and NFC enabled POS. Firstly, the transport layer starts a new session as to receive the client's NFC tag identification number and mobile identification number with a new private key. As per security, the client can disconnect the connection after getting these new public key pair from the server.

TABLE III
NFC GATEWAY REQUEST PROTOCOL

0-15 bits	16-23 bits	24-31 bits	32-47 bits	48-63 bits
Payload or start Flag	Major version	Minor version	Message type or flag	Length of message bit
Sender ID number				
NFC Bar Code or Tag ID				

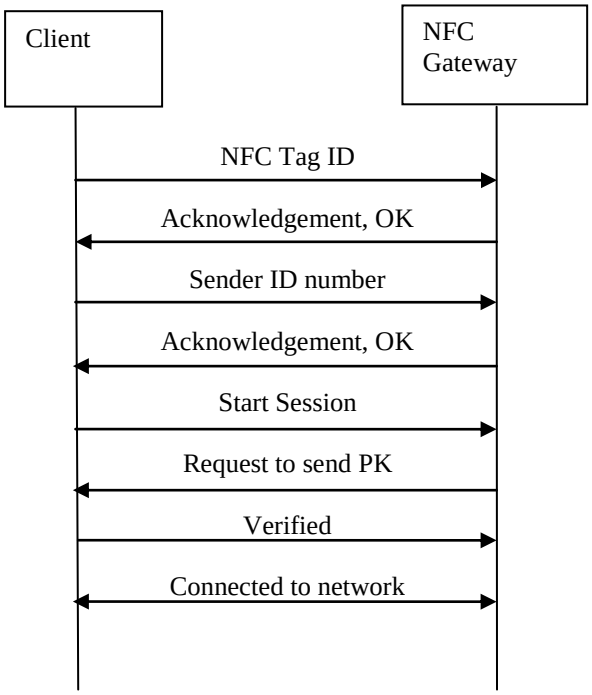

Fig. 1 NFC gateway key negotiation

III. NFC M-PAYMENT SYSTEM BASED ON WIRELESS NETWORK

Any products with built-in NFC tag will dramatically simplify the way of consumer devices interactions with one another, helping people through different applications like high speed data and secure mobile payment systems [5].

Figure 2 shows that, the NFC mobile based m-payment system using existing cellular network. As soon as the phone touches the RFID tag, an

application is started which connects a server and retrieves the authentication data [6].The first four steps involves the item bar code scanning, displaying the price of the item and the confirmation at both the point of scale or reader and the mobile phone.

Step 1-2: Firstly, the reader or POS scans the bar code or RFID tags from each selected product and calculates the total price (TP), Order information (OI) and the order time. The total price must be displayed on the mobile phone and customer then starts the m-payment application using payment service.

Step 3-4: The customer checks the TP which is displayed on mobile phone and if he agrees with the price, he may place the mobile onto the POS. Then the customer is ready to pay his bill using his personal identification number (PIN). Inputting the PIN, the customer verifies the ownership of the phone and also confirms that the TP is received. The customer also gets the acknowledgement from the POS to go onto the next step.

Step 5-8: To pay the bill using existing cellular network, the MS requests to the BTS for the allocation of a dedicated signaling channel. After allocation of a signaling channel, the channel setup request included the TMSI and last LAI is forwarded to the VLR. Hence, the VLR requests the AC via HLR for triples (RAND, SRES, K_c).

The VLR initiates authentication, cipher start, IMEI check and TMSI reallocation. If all these procedures have been successful, then the MS sends the set up information. Therefore, the MSC requests the VLR to check the subscriber data whether the requested service number can be handled. If the VLR indicates that the channel should be allocated, the MSC commands the BSC to assign a channel to the MS (mobile phone).

Step 9-11: After completion of authentication process, the payment gateway (PG) sends payment information to the billing centre. The billing centre checks the user's account or credit limitation with the TMSI. If the customer's credit check is valid, then the POS gets the transaction number (TSN) from VLR. Thus, it must be ensured that the transaction number would not be modified by anyone and can only be scan by the customer phone [7].

Finally, the paper receipt should contain at least order information, TSN and displaying the transaction result on the phone which assures the correctness of the transactions to the customer.

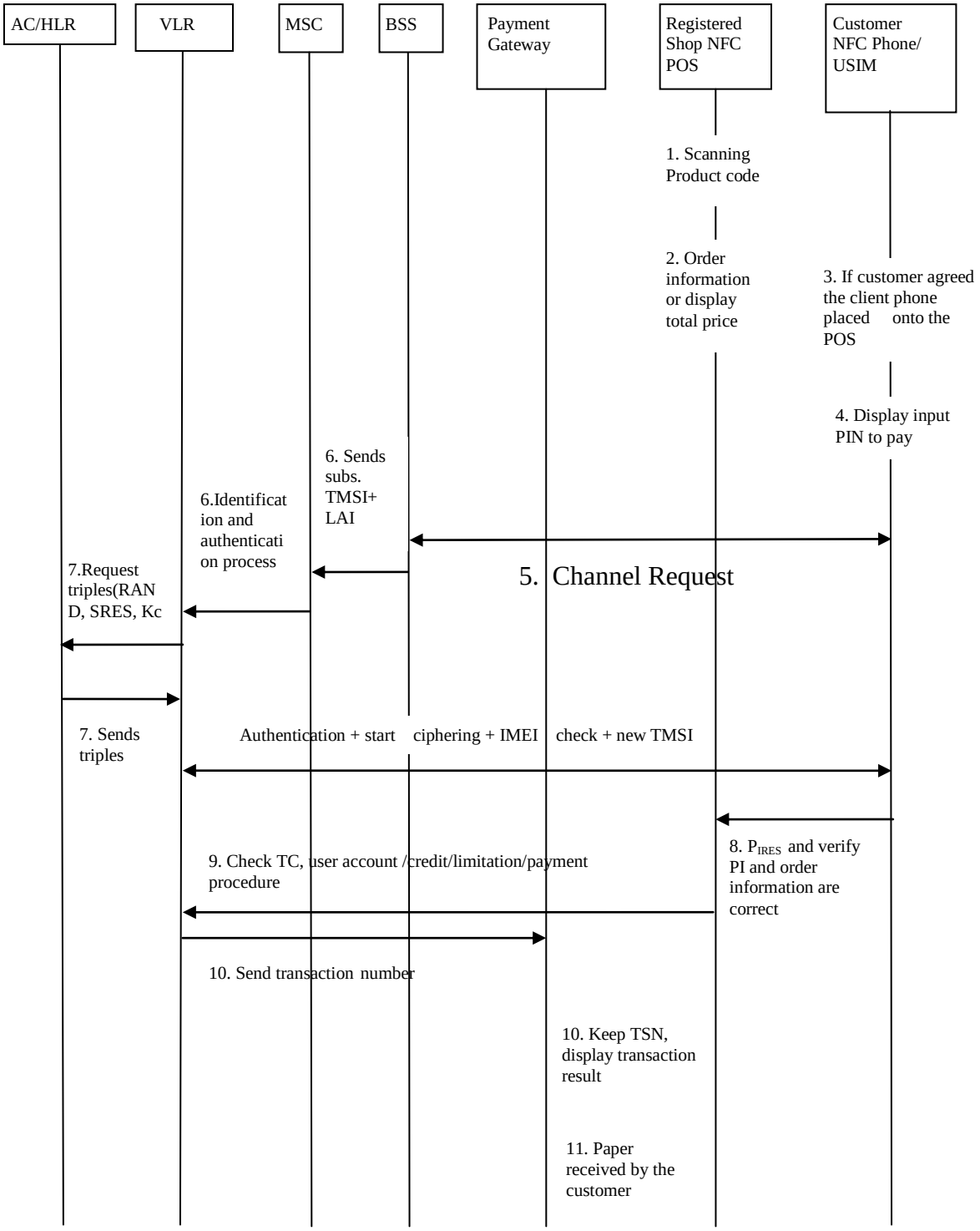

Fig. 2 NFC m-payment system using existing wireless network

IV. SECURE CHANNEL FOR NFC

Today, m-payment system suffers from their lack of usability. As the client cannot check their balance anytime and they cannot easily transfer their money without having to connect to a central server or POS. Therefore, the current technology is not sufficient to provide a secured system for the customer. Hence, the service provider and network operator can be managed their application remotely to determine the security required to access the handset and control the person to person distribution of the application through the NFC interface or GPRS. In this paper, a

secure online payment phone has been discussed to improve user acceptance of m-payment systems. This NFC enabled phones contain a Secure Element (SE) which is connected to the NFC module so that SE can be accessed in the passive NFC card emulation mode. The SE gets new software from a Specific Service Manager for authentication process and can be fully trusted to handle valuable digital vouchers to ensure the security of the customer.

V. CONCLUSION

NFC is going to be one of the major technologies in m-payment system. In this paper, a new gateway service and wireless mobile based authentication process has been discussed with different functions for generating new cipher and integrity keys to achieve a secured NFC m-payment system. Moreover, the software of a SE in which only a Trusted Services Manager can upload and maintain the access for the phone which provides more secure mobile communication.

REFERENCES

[1] M. Csapodi, A. Nagy, "New applications for NFC devices", 16th IST Mobile and Wireless Communication, IEEE 2007.

[2] J. Ylinen, M. Koskela, L. Iso-Anttila and P. Loula," Near field communication network services", Third National Conference of Digital Society, IEEE 2009.

[3] B. Benyo, A. Vilmos, K. Kovacs and L. Kutor, "The Design of NFC based applications", 11th International Conference on Intelligent Engineering Systems, IEEE, 2007, pp: 277-280.

[4] B. Benyo, A. Vilmos, K, Kovacs and L. Kutor, "NFC applications and business model of the ecosystem", 16th IST Mobile and Wireless Communication, IEEE 2007.

[5] H. Aziza,"NFC technology in mobile phone next-generation services", Second International Workshop on Near Field Communication (NFC), IEEE 2010.

[6] M. Massoth and T. Bingel, "Performance of different mobile payment service concepts compared with a NFC-based solution", Fourth International Conference on Internet and Web Applications and Services, IEEE 2009.

[7] W. D. Chen, G. P. Hancka, K. E. Mayes, " Using 3G network components NFC mobile transactions and authentication", International Conference on Progress in Informatics Computing (PIC), IEEE 2010.