IMPROVISED SECURITY PROTOCOL USING NEAR FIELD COMMUNICATION IN SMART CARDS

Mythily V.K[1], Jesvin Veancy B[2]

[1]*Student, ME. Embedded System Technologies, Easwari Engineering College, Ramapuram, Anna University, Chennai, (India)*

[2]*Assistance professor, ECE, Easwari Engineering College, Ramapuram, Anna University, Chennai, (India)*

ABSTRACT

The combination of NFC with smart devices has various mobile terminals equipped in widening the range of NFC in recent years especially, replacing credit cards in electronic payment. Thus security issues need to be addressed for NFC electronic payment. The standards of NFC security which is currently being applied require the use of user's public key at a fixed value in the process. Fake profile can be created by attackers or third parties server by collecting the associated messages based on public key of user's, through the created profile users privacy can be exposed and their privacy can be compromised. The conditional privacy prevention method are implemented in this paper based on multiple pseudonyms is used to solve these problems. Additionally, PDU (Protocol Data Unit) for conditional privacy method is defined. Users can communicate to the device that they will transfer the data according to the protocol by sending PDU through NFC terminals. The self updatable method in this paper is expected to succeed in minimizing the update cost and computation time by taking advantage of the physical characteristics of NFC and the processor.

Index Terms: NFC Security, Pseudonym, Conditional Privacy Protocol

I. INTRODUCTION

Near-field communication (NFC) is a form of short-range wireless communication where the antenna used is much smaller than the wavelength of the carrier signal, preventing a standing wave from developing within the antenna. In the near-field communication there is no standard definition of length, for practical purposes one can assume it is roughly one quarter of a wavelength the antenna cannot produce electromagnetic (radio waves). Thus NFC communicates either by modulated electric field or by modulated magnetic field, and not by electromagnetic wave (radio waves). For example, a small loop antenna that is also known as a magnetic loop produces a magnetic field, which later can be gathered by another small loop antenna, if it is close to it. Magnetic NFC has a useful property of being able to penetrate conductors that would reflect the radio waves.

Many mobile phones now use electric-field NFC which is operating at its standard frequency of 13.56 MHz, has close similarity to its wavelength of 22.11 m transaction because the very short range of NFC makes it difficult to gain access to private communication (eavesdrop). To efficiently generate the data's over greater distances, this sends out radio waves of particular type of wavelength covering in practice say a meter or more. If the antenna is just a few centimetres long, it will only set up the 'near-field' with respect to its length depth and width around itself roughly the same as the dimensions of the antenna. Very little energy will diverge away, it is absolutely necessary a stationary electromagnetic field pulsating at 13.56 MHz's. If another similarly small

antenna comes into contact, it will bring an electric potential into the field, altering the frequency by modifying the signal in the field. Signals can be transmitted to passive antenna when one modifies data only in active region of the antenna. An analysis is conducted on the security threats that can occur in the current NFC environment, and the security requirements necessary for NFC are deduced.

II. BACKGROUND

In this section, the current NFC standards have been introduced, and the pseudonyms are also introduced as conditional privacy preserving method, requires both standards of NFC and pseudonyms. The NFC standards, defines a variety of standards ranging from the basic interface protocols that has to be tested along with the security methods. This also introduces the basic interface, which is done between NFCIP and NFC-SEC (the security method).

2.1. NFCIP: Near Field Communication Interface and Protocol

In NFC, the main object of basic communication is divided into an initiator and a target. An initiator is used as it generates RF field (Radio Frequency field) and ignites NFCIP-1. A target that receives signals from initiator responds to it that the signal is through the RF field this target communication is usually called passive communication mode where, the target communicates using RF field and using self generated method RF field is referred to as active communication mode. Communication mode is determined according to applications it runs for when transaction starts. Once the transaction is initiated, the communication mode is set and cannot be altered until the target becomes disabled or removed completely from the device. The main purpose of using NFCIP-1 is SDD (Single Device Detection) and RFCA (Radio Field Collision Avoidance). The SDD is an algorithm that is used in RF field for initiator to find a specific target among multiple targets. Collision problem might occur in existing RFID system.

The collision is a state in which refers to, two or more initiators or targets transmitting data at the same time, and it is not possible to distinguish which data is original.

The RFCA detects other RF fields the occurrence of collision is resolved by NFC standard using algorithm known as RFCA and prevents data from getting collided using carrier frequency. RFCA begins by assuring the presence of other RF fields. The SDD finds specific target within the range and RFCA does not permit other fields, thus helps the NFC protected from MITM (Man-In-The-Middle) attacks.

2.2 NFC-SEC: NFCIP Security Services and Protocol

NFC-SEC defines SSE (Shared Secret service) and SCH (Secure Channel service) for NFCIP. A secret key for secure communication between NFC devices and the smart card are generated in this process by SSE, where key agreement and key confirmation is acknowledged. SCH service provides the communication between NFC devices with confidentiality and quality of integrity using a key that are generated through SSE service. For SCH between NFC terminals in SSE, NFC-SEC defines the procedure of key agreement using ECSDVP-DH (Elliptic Curve Secret Value Derivation Primitive, Diffie-Hellman version). To reaches that are made from above methodologies, NFC terminal must have at least one public key and private key based on multiplication defined algebra (Elliptic curve). SCH makes three keys to arrange in order of rank by using the key generated through SSE and provides strict privacy and integrity to the messages using generated keys. The three keys

created in SCH and are used to provide the confidentiality and integrity of the message. The key agreement and confirmation protocols are implemented as shown in the table.

TABLE NOTATION

Notation	Description
||	Concatenation symbol
NX	Nonce of userX
IDX	Random ID of userX for the activation of transport protocols
QX, QX', QX?	Compressed elliptic curve public key of userX
QX, Q'X, Q?X	Elliptic curve public key of user X dX Elliptic curve private key of userX
G	Elliptic curve base point KDF Key derivation function
MacTagX	Key verification tag received fromX
MK	Shared secret key
z	Unsigned integer
rX	Random integer generated by userX
PN	Pseudonym set
Enc(k, m)	Encrypt m with k
Sig(k, m)	Signature on m with k

III. PROPOSED SYSTEM

The conditional privacy protocol method has widened the study in the light of pseudonyms. The paper proposes various techniques that are tailored to the NFC environment. Since this method can reuse NFCIP and NFC-SEC, the NFC standards are more efficient and production is possible to implement in chip design sector.

3.1MuPM: Multiple Pseudonym Based Method

If request for pseudonyms is given by the user A, TSM generates multiple pseudonyms and transmit it to the user. Then, the TSM stores the transmitted pseudonyms and their ID. A pseudonym composed of public key, private key (that is encrypted with long-term public key of user A), ID of the TSM, and signature of the TSM in order to maintain a record for future references

Based on the generated data TSM creates pseudonym sets and delivers it to user. The

used pseudonym is managed through cancellation list. This method has its advantage of simple protocol and easy access of service to the users. It requires a storage space to maintain the pseudonyms, revocation list, and communication costs for issuance of pseudonyms.

3.2 uPM: Self-Updateable Pseudonym Based Method

Considering the NFC features in the design process, the protocol can be configured without the need to communication channel. This communication with TSM can be used, only to maintain the records of the message constructor. This method does not specify the owner of the public key, but it helps to identify whether the public key is periodically generated or not. Therefore, it can identify the message being generated by using the public key received from TSM. When the protocol is disconnected from process of one-to-one short range communication, users have an impression of the existence and they can discontinue or restart the communication all over again. In this paper, users can request services through protected conditional privacy PDU where the data are protected from third-party.

3.3 Algorithm

The proposed protocol method consisting two users A and B. User B can obtain Q'A and Q″A by decompressing QA' and QA″.

Q'A and Q″A are the points on the encrypted public key.

Q'A=rA QA = rA d AG

Q"A=rA d A QS + QA = rA d A d S G + d AG

According to the algorithm, user B cannot find that Q'A is QA which is the message given by the same person, even if user B knows QA the message cant not be extracted. Likewise, in Q″A, user B cannot find rAdAQS

because user B does not know rAdA value. Thus, user B cannot extract rAdAQS from Q″A, and cannot recognize that the message was instructed by the user A. In contrast, the TSM can recognize who created this message by following decryption method.

Q"A- d S QA= (rA d A (d S G)) + QA - d S (rA (d AG)) = QA

Two users can obtain the common values by using the exchanged messages of Q'A and Q'B. To obtain the same value, multiply private key are used and the random values are obtained. The random value is the constant number used in generating Q″A and Q″B. The following Equation expresses the process in which the two users get the same value.

P=rAdAQ'B=rAdA(rBdBG)=rAdArBdBG=rBdB(rAdAG)=rBdBQA

SIZE OF THE FIELDS	
Field Size	
[illegible]	16bits
[illegible]	96bits
MacTagx	96bits
MK	128bits
[illegible]	192bits
[illegible]	200bits
[illegible]	352bits
[illegible]	384bits
[illegible]	448bits

Additional storage to maintain the pseudonyms are required which comprises of public key, private key (encrypted with long-term key of user), ID of TSM, and signature of the message. TSM should generate multiple pseudonyms and send to use in order to preserve the privacy of user's.

Encrypted message size is given in above table. Two users can get a shared secret value say z by taking x coordinate value at point P. When compared with the existing protocols based on the process, Q'A and Q'B can replace by QA and QB using existing public key. In other words, the anonymity of users can be guaranteed by replacing the public key alone. Finally pseudonyms consists of the following form,

Table II Coding of the Conditional Privacy PDU

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU	ONE	ONE	MI	NAD	DID	PNI	PNI

- Bit 7: Reserved for future use. The initiator will set it to Zero.
- Bit 6 to Bit 5: Will be set ONE.
- Bit 4: If bit is set to ONE then it indicates multiple information chaining activated.
- Bit 3: If bit is set to ONE then it indicates node address is available.
- Bit 2: If bit is set to ONE then it indicates Device ID is available.
- Bit 1 and Bit 0: Packet number information.

Coding of the PFB (Control information for transaction) bit 7 to 5

Bit7	Bit6	Bit5	PFB
0	0	0	Information PDU
0	0	1	Protected PDU
0	1	0	Acknowledge PDU
0	1	1	Conditional privacy PDU
1	0	0	Supervisory PDU
Other setting are reserved for future use			

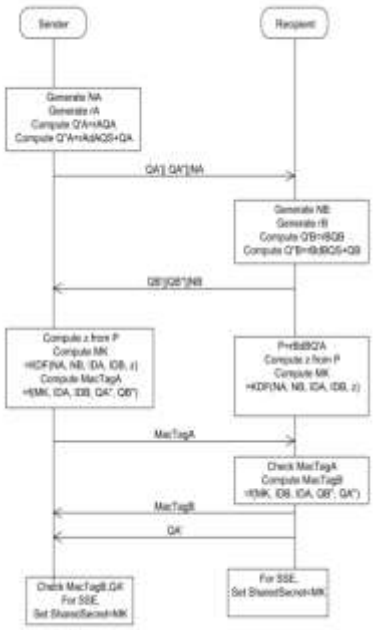

Figure 3.1 Flow of Algorithm

PN=Public key + Encrypted Private Key+ ID of TSM + Signature.

If they are attackers, they cannot decrypt the information's of sender.

IV. SYSTEM IMPLEMENTATION

First the connections are established by using the algorithmic steps. Then the interface between the hardware and the microcontroller are made after which the transmitter node sends the encrypted message to the recipient. Here in the Figure 4.1 the message gets displayed in the LCD

The smart phone which consists of NFC module is used to encrypt the message to establish the connection. After receiving the data, the recipient decrypts the message and sends it back to the transmitter. This process happens for every single transition that takes place in the system in order to find out if the user is authenticated or not. If the sender receives the data which matches with the predefined data, which ensures that the user is authenticated and thus the connection is established otherwise automatically the connection will get discarded and no further transaction take place between the transmitter and the receiver assuming that the user is hacker.

When the connection is successfully established, the data packets will be forwarded to the recipient. If the hacker is pretending to actual the recipient, the sender can identify the hacker and terminate the connection with the hacker protection the privacy of the user and the system.

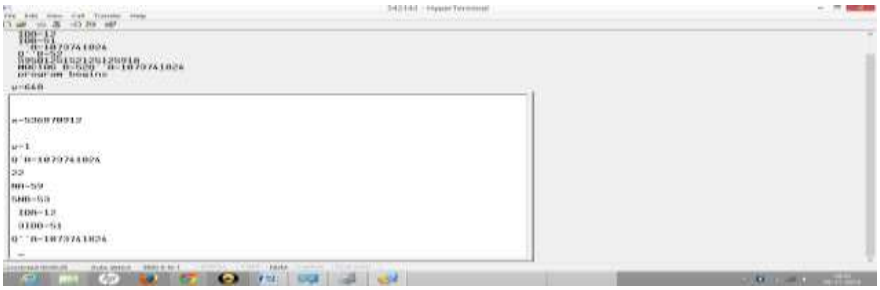

Figure 4.1 Inputs are Given Manually

In the above Figure 4.1 the inputs are fed to the system for processing. Here the inputs are given manually and for the system to compute using the improved conditional privacy preserving algorithm.

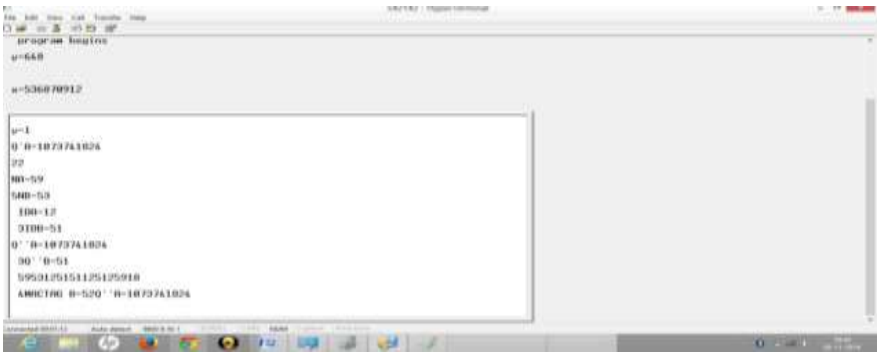

Figure 4.2 Generating MAC tag

For the corresponding input Q"B is computed and a Mac tag is generated which is shown in the above Figure 4.2

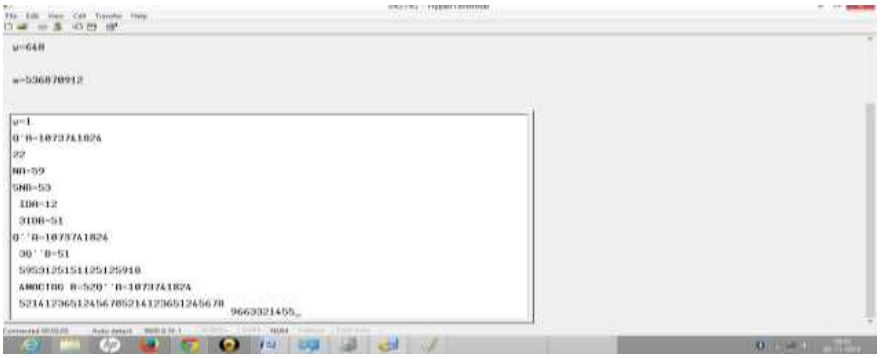

Figure 4.3 The Standardized 16-Digit Number Gets Displayed

In each step the data packets gets transmitted and the corresponding operations are performed. In above Figure 4.3 the sequence of data gets standardized producing a 16-digit string of number.

V. RESULT AND DISCUSSION

The system protects the data from unauthorized users such that the privacy is maintained and nobody breaks into computers. The Figure 5.1 bellow shows the detection of hacker that tries to acquire the data.

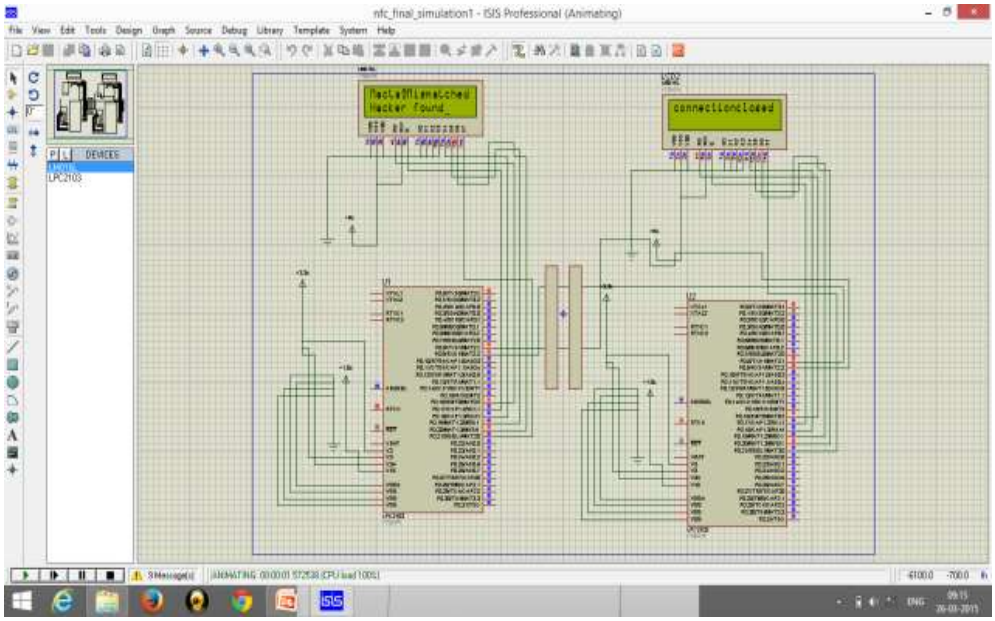

Figure 5.1 Detection of Hacker

This method uniquely identifies each teams by taking the advantage of physical characteristics of the hardware components. The NFC takes 424Kbps bit rate with less than 0.1s set up time.

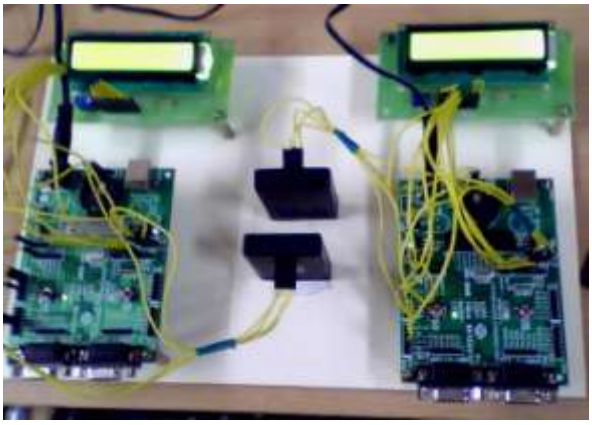

Figure 5.2 Hardware Interfacing

VI. CONCLUSION AND FUTURE WORK

NCF can identify each other through the NFCID but they cannot figure out the definite identity. In creating updatable public key, additional time is required. This additional time does not have an impact on the transfer time since pre-computation is done. Points are calculated in advance and the doubling operation takes more time to run the task.

The proposed method takes less time for computation, because it performs 288 doubling operations for calculation. Accordingly, conditional privacy method does not provided any additional transfer time since it is self-updatable. In future, the proposed algorithm can be extended by using various other processors and the entire system can be implemented with less duration.

REFERENCE

[1] A.Chandrasekar, V.R. Rajasekar, and V. Vaasudevan, "Improved authentication and key agreement protocol using elliptic curve cryptography," International Journal of Computer Science and Security (IJCSS), Vol. 3, Issue 4, pp. 325-333, Oct. 2009.

[2] D.Huang, S. Misra, M. Verma, and G.Xue, "PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs," IEEE Transactions on Intelligent Transportation Systems, Vol. 12, No. 3, pp. 736-746, Sept. 2011.

[3] D.Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping," Proceedings of the 2010 IEEE Vehicular Networking Conference (VNC 2010), pp. 174-181, Dec. 2010.

[4] E.Haselsteiner and K. Breitfuß, "Security in Near field Communication (NFC) – Strengths and Weaknesses –," RFIDSec 2006, Jul. 2006.