Improvements to NFC Mobile Transaction and Authentication Protocol

Muhammad Qasim Saeed
Information Security Group (ISG)
Royal Holloway University of London, Egham, UK
muhammad.saeed.2010@live.rhul.ac.uk

***Abstract*—A protocol for NFC mobile authentication and transaction is recently proposed by W. Chen *et al.* This protocol is used for micropayments, where the Mobile Network Operator (MNO) pays for its customers. The main advantage of this protocol is its compatibility with the existing GSM network. This paper suggests some improvements in this protocol from security point of view. As this protocol is used for monetary transactions, it should be as secure as possible. This paper presents an improved version of the existing protocol with a detailed analysis at the end. The user interaction with the system is improved making it more user friendly. An additional layer of security has been added by introducing PIN authentication by the user. Mutual authentication is improved by adding freshness by the mobile device in order to resist replay attack. We also add digital signatures with the transaction messages for data integrity and non-repudiation.**

***Index Terms*—Near Field Communication; Security; mobile transaction; GSM authentication.**

I. Introduction

This paper takes a close look at the authentication and transaction protocol proposed by W. Chen *et al.* [1]. This protocol is used for payment through mobile device using existing GSM infrastructure. The protocol first authenticates the mobile device to the Mobile Network Operator (MNO), and after successful authentication, monetary transaction is being performed by the MNO. The mobile device is equipped with the Near Field Communication (NFC) technology. The overall scenario is a user who purchases some goods from a shop and pays through his mobile device. The three major entities in this protocol are the user with mobile device, registered shop with NFC POS terminal and the MNO.

Since this protocol involves monetary transaction, it must be secure against known attacks to maximum possible extent. This paper proposes an improved version of this protocol making it more secure. We revise the interaction of user with the system resulting in more user-friendly mechanism. We add PIN authentication, which did not exist in the original protocol. The authentications phase is also improved by adding freshness from the mobile device. This prevents replay attack in the authentication phase. We add digital signature with the transaction messages to provide data integrity and non-repudiation. We add a key generation phase to generate encryption and MAC keys. Therefore, in our version, we use separate keys for encryption and MAC calculation.

This paper is organized as follows. The first part introduces the NFC technology and its application in the field of m-commerce. After this, the GSM authentication process is explained followed by the Chen's authentication and transaction protocol. It is followed by its improved version with the detailed analysis.

II. Near Field Communication

Near Field Communication (NFC) is a short-range wireless technology compatible with contactless smart cards (ISO/IEC 14443) and radio-frequency identification (RFID). NFC communicates on the 13.56 MHz frequency band at a distance of less than 4 cm. It uses magnetic field induction for communication and powering the chip [2].

This technology is now available on the cell phones. Considerings the exponential growth in the mobile technology, the use of NFC technology is also on the sharp rise. A wide variety of applications is possible using the technology because of the different operation modes supporting both communication from device to device (peer-to-peer mode), communication between a device and a passive tag (read/write mode) and an emulation mode where the mobile device can act like a contactless smart card [3]. Since this technology has a very short range of operation, it is considered to be hard to eavesdrop. This makes NFC suitable for monetary transaction.

III. Mobile Commerce

Mobile Commerce, also known as M-Commerce, is the ability to conduct commerce using a mobile device, such as a mobile phone, a Personal Digital Assistant (PDA), a smartphone, or other emerging mobile equipment such as dashtop mobile devices. This usually, but not at all times, involve the Mobile Network Operator (MNO). The use of m-commerce has seen rapid growth in the recent years, with several different services like Short Message Service (SMS), Wireless Application Protocol (WAP), Unstructured Supplementary Service Data (USSD) and K-Java on GSM network and NFC.

The concept of m-commerce is not matured yet in terms of new technology and modes. Zhang has compared the differences between online payment services and mobile payments. He concluded that the main problem of the m-commerce is the insufficient choice of payment methods [4].

Alpár et al [5] introduced Tap2 technology where the users need only their NFC-enabled mobile devices and credentials implemented on their smart cards. They proposed the use of

NFC technology in the on-line banking solution based on EMV Chip Authentication Program (EMV-CAP).

The NFC technology over mobile devices has given a new direction to m-commerce. W. Chen *et al.* proposed an authentication and transaction protocol that utilizes the existing GSM network [1]. In this protocol, the user buys some services and the payment to the shop is made through the MNO of the user. It is mostly suitable for such customers that do not have their bank account; yet they need to be pay bills, receive money from abroad, transfer it between each other, and access microcredit. Orange, a French based telecom company, has launched a project 'Orange Money' in Africa where only 3 to 7 percent of most countries' population have bank accounts. The project is very successful and has tripled its customer base in the past one year [6].

IV. GSM Authentication

When a Mobile Station (MS) signs into the network, the Mobile Network Operator (MNO) first authenticates the MS. Authentication verifies the identity and validity of the SIM card and ensures that the subscriber has authorized access to the network. The Authentication Centre (AuC) of the MNO is a responsible to authenticate each SIM card that attempts to connect to the GSM core network through Mobile Switching Centre (MSC). The AuC stores two encryption algorithms A3 and A8, as well as a list of all subscribers identity along with corresponding secret key K_i. This key is also stored in the SIM. The AuC first generates a random number known as R. This R is used to generate two numbers, signed response S and K_c as shown in Figure 1, where $S = E_{K_i}(R)$ using A3 algorithm and $K_c = E_{K_i}(R)$ using A8 algorithm [7].

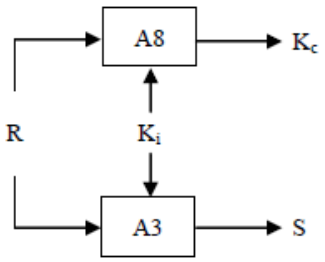

Fig. 1. Generation of K_c and *S* from *R*

The triplet (R, S, K_c) is known as *Authentication triplet* generated by AuC. AuC sends this triplet to MSC. On receiving a triplet from AuC, MSC sends R (first part of the triplet) to the MS. SIM computes the response S from R, as K_i is already stored in the SIM. MS transmits S to MSC. If this S matches the S in the triplet (which it should in case of a valid SIM), then the mobile is authenticated. K_c is used for communication encryption between the mobile station and the MNO.

V. Chen's Protocol

This protocol is used for monetary transaction through MNO. Three basic entities involved are the MNO, shop POS terminal registered with the corresponding MNO and the user who has an NFC enabled mobile device operating with the same MNO. The user buys some items from the shop and pays through his mobile device. He places his mobile device on the shop POS terminal and mutual authentication occurs between the mobile device and the MNO. The MNO billing centre makes the payment against the specific user after successful authentication. This protocol is subdivided into three parts; Price checking, Triple Authentication and Transaction execution as shown in Figure 2. The summary of the protocol is described below, whereas the detail is available at [1].

TABLE I
Abbreviations

AuC	Authentication Center (subsystem of MNO)
IMSI	Internet Mobile Subscriber Identity
K_i	SIM specific key. Stored at a secure location in SIM and at AuC
K_c	$E_{K_i}(R)$ using A8 algorithm
K_{c_1}	H(K_c). Used for MAC calculation
K_{c_2}	H(K_{c_1}). Encryption key
K_p	Shared key between PG and shop POS terminal
LAI	Local Area Identifier
MNO	Mobile Network Operator
NFC	Near Field Communication
PI	Payment Information
POS	Point of Sale. Part of shop
R	*RAND,* Random Number (128 bits)
R_s	Random number generated by SIM (128 bits)
TC	Transaction counter
TRM	Transaction Request Message
TI	Transaction Information
TMSI	Temporary Mobile Subscriber Identity
TP	Total Price
TRM	Transaction Request Message
TS_U	User's Time Stamp
$TS_{Transaction}$	Transaction Time Stamp

A. Triple authentication

Mutual authentication between the Mobile device and the MNO is performed from step 5 to 13. Payment Gateway (PG), a part of MNO, receives authentication triplet (R, S, K_c) from MSC. PG initializes a challenge response mutual authentication protocol by sending $R, MAC_{K_c}(R)$ to the mobile device through the shop POS terminal in step 10. Once user SIM receives $R, MAC_{K_c}(R)$, it first computes K_c from R by using K_i (already stored in the SIM), as mentioned in Section IV. SIM generates MAC on the received R and compares with the received MAC. Correct matching verifies the correctness of R and authentication of shop PG and the MNO. In step 13, the SIM transmits response of the challenge as $E_{S_1}(R)$, where $S_1 = H(S)$.

B. Transaction Execution

After a successful mutual authentication, a transaction message is generated by the customer in step 19. The message is verified by the shop POS terminal and relayed to the MNO.

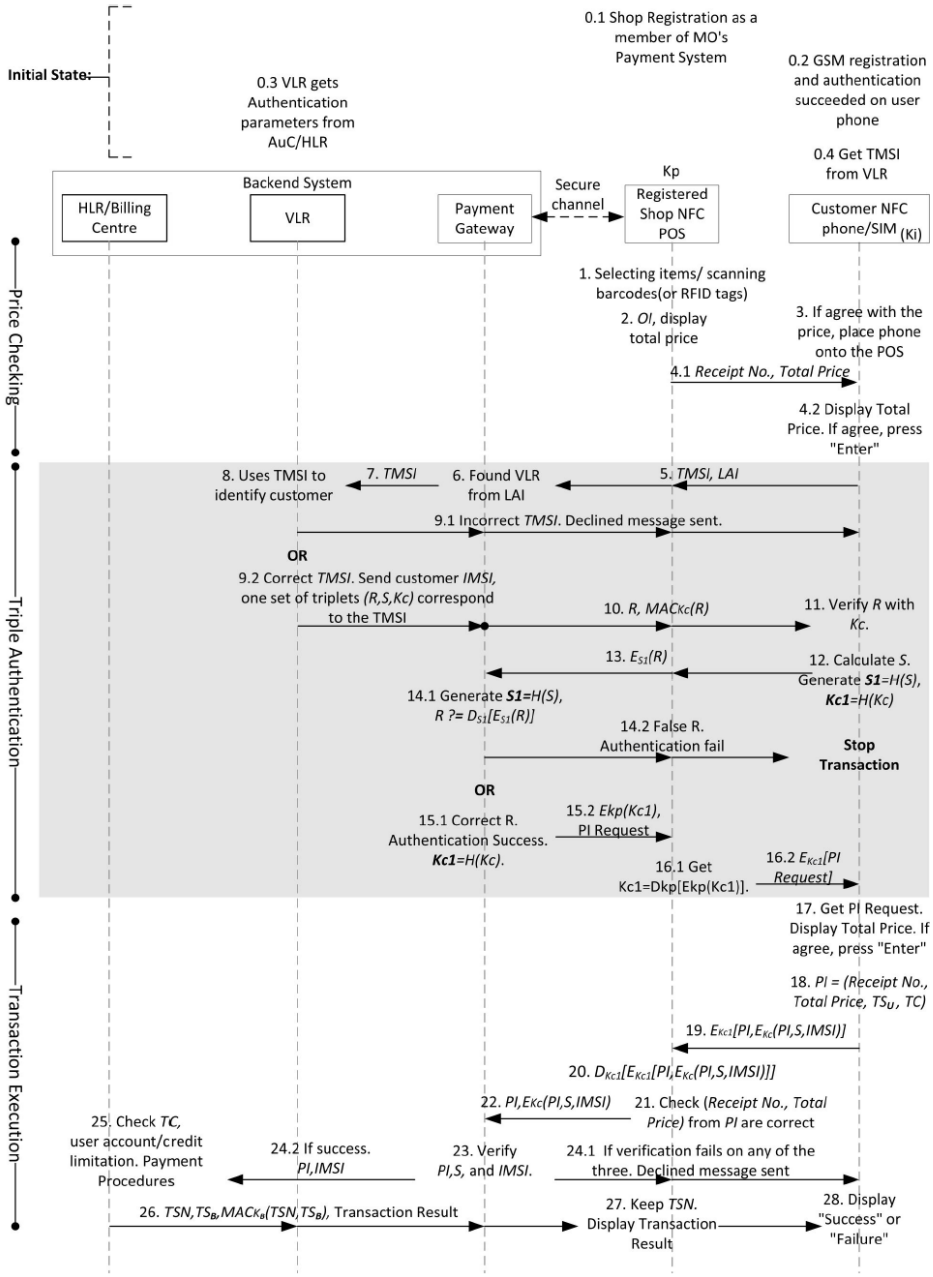

Fig. 2. GSM Authentication and Transaction (Chen's Protocol [1], fig. 1)

The MNO after transaction execution, sends a confirmation message to the customer in step 28.

VI. Our Improved Protocol

In this section we present an improved version of the Chen's protocol. The main improvement is in authentication phase and in transaction phase. We assume that the communication is secure between various subsystems of the MNO. The shop POS terminal, registered with one or more MNO, shares an MNO specific secret key K_p with the corresponding MNO. This key is issued once a shop is registered with the MNO. The bank detail of the shopkeeper is also registered with the MNO for monetary transactions. The communication between the shop POS terminal and the mobile device is wireless using NFC technology. The mobile device has a valid SIM.

The proposed protocol executes in three different phases; *Authentication*, *Keys generation* and *Transaction*. The protocol initiates when the customer places his cell phone for the payment after agreeing to the total price displayed on the shop POS terminal. The details of these phases are described as follows:

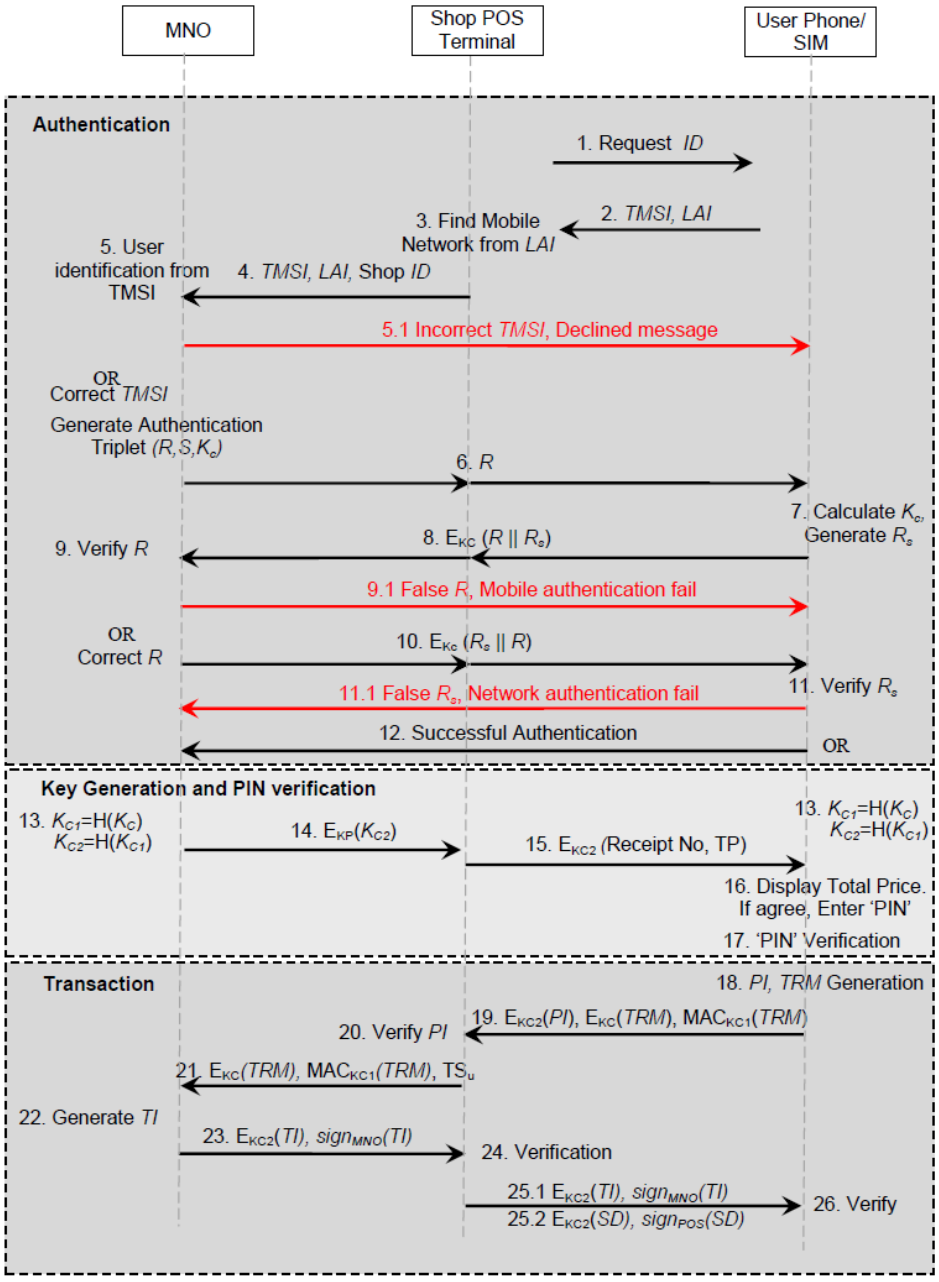

Fig. 3. Improved version of Authentication and Transaction Protocol

A. Phase 1: Authentication

Step 1. As soon as the user places his mobile device, NFC link between the mobile device and the shop POS terminal is established. The shop POS terminal sends an *ID Request* message to the mobile device.

Step2-3. The mobile device sends *TMSI, LAI* as its ID. On receipt of the information from the mobile device, the shop POS terminal determines the user's mobile network. The network code is available in *LAI* in the form of Mobile Country Code (*MCC*) and Mobile Network Code (*MNC*). An *MNC* is used in combination with *MCC* (also known as a *'MCC/MNC tuple'*) to uniquely identify a mobile phone operator/carrier [8].

Step 4-5. The shop POS terminal sends *TMSI, LAI, Shop ID* to respective MNO for customer authentication and shop identification.

Step 5.1. In case of incorrect *TMSI*, a declined message is sent.

Step 6. In case of correct identification, the MNO generates one set of authentication triplet (R, S, K_c) and sends R to mobile device through shop POS terminal.

Step 7-8. SIM computes K_c from R as explained in Section IV. SIM generates a random number R_s and concatenates with R, encrypts with key K_c and sends it to the MNO through

shop POS terminal.

Step 9-10. The MNO checks the validity of the SIM (or mobile device). It receives $E_{K_c}(R\|R_s)$ from the mobile device and decrypts the message by K_c, the key it already has in authentication triplet. The MNO compares R in the authentication triplet with the R in the response. In case they do not match, a 'Stop' message is sent to the mobile device and the protocol execution is stopped. If both R are same, then the mobile is authenticated for a valid SIM. In this case, the MNO swaps R and R_s, encrypts with K_c and sends it to mobile device.

Step 11-12. This step authenticates the MNO to the mobile device. The mobile device receives the response $E_{K_c}(R_s\|R)$ and decrypts it with the key K_c already computed in Step 7. The mobile device compares both R and R_s. If both are same, then the MNO is authenticated and a *'successful authentication'* message is sent to the MNO.

B. Phase 2: Keys Generation and PIN Verification

Step 13-14. K_p is a shared secret between the MNO and the shop POS terminal. K_c is the shared secret between the MNO and the customer's mobile device (computed in step 7). There is no shared secret between the POS terminal and the mobile device till this stage. MNO and mobile device compute one-way hash function of K_c to generate K_{c_1}, the key that will be used for MAC calculation. The MNO computes K_{c_2} from K_{c_1} using one-way hash function and sends it to shop POS terminal by encrypting it with K_p. Mobile device also computes K_{c_2} as it already has K_{c_1}. K_{c_2} is the encryption key between MNO, shop POS terminal and the customer's mobile device.

Step 15-17. The shop POS terminal sends the Total Price *(TP)* and the Receipt Number encrypted with K_{c_2}. The user's mobile device decrypts the information and displays to the user. If he agrees, he enters the PIN. The PIN is an additional layer of security and adds trust between the user and the shopkeeper. A PIN binds a user with his mobile device, so the shopkeeper is to believe that the user is the legitimate owner of the mobile device. Moreover, the user feels more secure as no one else can use his mobile device for transaction without his consent.

PIN is stored in a secure location in the SIM. The SIM compares both PINs and if both are same, the user is authenticated as the legitimate user of the mobile device. Otherwise, the protocol is stopped.

C. Phase 3: Transaction

Step 18. The customer's cell phone generates two messages, *PI* and *TRM*, such that;

PI= Receipt No, Total Price, Time Stamp (TS_U)
TRM=PI, R_s, Transaction Counter

Step 19. TS_U represents the exact time and date the transaction has been committed by the user. *TC* is a counter that is incremented after each transaction and is used to prevent replay attack. *PI* is encrypted with K_{c_2} so that it can be verified by the shop POS terminal. The user encrypts the *TRM* with K_c so that it cannot be modified by the shop terminal. The user computes MAC with K_{c_1} over the *TRM* using Encrypt-then-MAC approach for integrity protection.

Step 20-21. The POS terminal can decrypt only the *PI* encrypted with by K_{c_2} to check its correctness. The POS terminal does not need to verify the MAC (and it cannot do so), as it already knows the main contents of *PI*. The Shop POS terminal also verifies the TS_U to be in a defined time window. If *PI* is correct, the POS terminal relays the encrypted *TRM* with corresponding MAC along with the TS_U to the MNO.

Step 22. On receipt of the message, the MNO checks the integrity of the message by verifying the MAC with K_{c_1}. If the MAC is invalid, the transaction execution is stopped. In case of a valid MAC, the MNO decrypts the message. The MNO compares the R_s in the *TRM* with the R_s received earlier in the authentication phase. A correct match confirms that the user is the same who was earlier authenticated. It also verifies the *TC* and TS_U. In case of successful verification, the MNO communicates with the concerned subsections for monetary transaction. The concerned subsections of the MNO checks the credit limitations of the user, and if satisfied, execute the transaction.

Once the transaction is executed, the MNO generates *Transaction Information (TI)* message as:

TI = Transaction Serial Number, Amount, $TS_{Transaction}$

Step 23-25. The MNO encrypts *TI* with K_{c_2}, digitally signs the message and sends it to the shop POS terminal. The POS terminal verifies the signature. A valid signature indicates correct *TI*. The POS also verifies the *TI* for the amount mentioned in the *TI*. In case of successful verification, the POS terminal appends the message it received from the MNO with the *Shopping Details (SD)* and corresponding digital signature.

Step 26. The user verifies both signatures. It verifies the contents of *TI* and *SD*.

VII. Protocol Analysis

In this section, we analyze our proposed model from multiple security aspects. This analysis encompasses the authentication and security of the messages among customer, shop POS terminal and the MNO. The analysis also includes multiple attack scenarios, such as a customer is dishonest and has intentions to pay less, or the shopkeeper is dishonest and has plans to receive more money.

A. Mutual Authentication

A mutual authentication between a customer and MNO occurs whenever the customer agrees to pay some amount. Since this authentication is performed through shop POS terminal, we analyzed our protocol from an angle that if the POS terminal has some malicious intentions. In this case, there can be following two scenarios:

1) **POS terminal impersonation as a customer.** We assume that the shop POS terminal is dishonest and keeps a record of all messages against a legitimate

customer (we call it as 'target customer'). The aim of the shopkeeper is to transfer money from the target customer without his consent. The shop POS terminal impersonates as target customer to the MNO by replaying message 4. In case the *TMSI* and *LAI* are valid at that time (the chances are higher if the message is replayed just after the legitimate transaction of the target customer), the MNO will send a random number R to the terminal. R is 128 bit random number generated by the MNO so the chances for its repetition are almost negligible. The shopkeeper cannot compute a valid response in step 8 for a different R, as Shop lacks K_i to compute K_c. Therefore, a shop cannot successfully impersonate as a customer by replaying old messages.

2) **POS terminal impersonation as MNO.** In this scenario, we assume that the shop is dishonest and communicates with a target customer without establishing a communication link with the MNO. Again, we assume that the shop keeps a record of legitimate messages of the target customer. The shop sends message 1 (*Request ID*) to the target customer and gets its response in message 2. Since shop does not communicate with MNO in this scenario, it does not send message 4 to MNO. However, the shop replays the recorded R in message 6 to the target customer. The target customer believes that he has been correctly identified by the MNO and the R is actually generated the MNO. So the user computes a response and sends it in message 8 to the shop. Message 8 contains R_s encrypted with the K_c. The R_s is a random number generated by the SIM and is different in each transaction. So, message 8 will be different than the one already recorded with the shop. Since message 8 is different, the shop can neither replay message 10, as it will be different for this transaction, nor it can compute a valid message 10. This scenario is, again, not successful.

B. Encryption and MAC Keys

Separate keys are used for encryption and MAC calculation making the protocol more secure. *Encrypt-then-MAC* is an approach where the ciphertext is generated by encrypting the plaintext and then appending a MAC of the encrypted plaintext. This approach is cryptographically more secure than other approaches [9]. Apart from cryptographic advantage, the MAC can be verified without performing decryption. So if the MAC is invalid for a message, the message is discarded without decryption. This results in computational efficiency.

C. User Interaction

The user interaction with the system is reduced to single interaction making it a user-friendly protocol. The user feels more secure as the transaction is protected by PIN verification. There are chances that a user withdraws his mobile device from NFC terminal as a psychological move to enter PIN. This will break NFC link, but as the PIN is stored in the SIM, it does not require NFC link for verification. Once the user PIN has been verified by the SIM, the user places his mobile device back on the NFC terminal and the protocol resume from the same point. There are chances that a dishonest user withdraws his mobile device in order to enter the PIN, and then places back another mobile device for transaction. To counter this threat, R_s is transmitted by the mobile device in *Transaction Request Message* (message 19). R_s is generated by the SIM and is encrypted with K_c (message 7,8), so it cannot be eavesdropped in the authentication phase. This ensures that the mobile device does not change.

D. Disclosure of Relevant Information

The protocol is designed considering disclosure of information on need to know basis. For example, *TC* is a counter that increments after each successful transaction. The record of the *TC* is kept by both, the user and the MNO. Shop POS terminal does not need to know the TC. In our proposed protocol, the TC is not exposed to POS terminal as it is a part of *TRM*.

Similarly, the MNO does not need to know the shopping details of the customer. Therefore, only the total amount is transmitted to the MNO for transaction.

E. Transaction Security

The transaction phase of the protocol requires maximum security. The *TRM* message is initiated by the customer rather than the shop terminal in order to satisfy the customer. The integrity of the *TRM* message is protected by the MAC so any alteration in this message is not possible. The message 19 is designed in such a way that the first half of the message containing encrypted *PI* is for shop POS terminal. POS terminal can decrypt and check the authenticity of the payment information. The remaining half of the message, containing encrypted *TRM* and corresponding MAC can neither be decrypted nor altered by the shop POS terminal. The POS terminal relays the remaining half to the MNO along with the Time Stamp. Hence, the transaction information generated by the customer is relayed to the MNO without any alteration.

In this phase, there can be a scenario where a dishonest customer has an intention of paying less than the actual amount. The customer designs a malicious *TRM* message (TRM') consisting of PI' (an illegitimate payment information, $PI' < PI$). The dishonest customer then forms message 19 as:

PI=Receipt Number, Total Price, Time Stamp TS_U
TRM'=PI', R_s, *Transaction Counter (TC)*

It may be noted that the *PI* is legitimate whereas, the TRM' consists of amended PI (PI'). The dishonest customer forms message 19 as:

Message 19 = $E_{K_{c2}}$ (PI), E_{K_c} (TRM'), $MAC_{K_{c1}}$ (TRM')

The first half of the message, consisting of encrypted *PI*, is legitimate and shop can verify it; whereas, the malicious part cannot be decrypted by the shop. So the shop cannot determine that the remaining part contains amended price information. The shop forms message 21 as *PI* is verified. The MNO executes the transaction with amended price and forms message 23 and digitally signs it. Message 23 contains

the information about the amount deducted from the customer. Once this message is received by the shop terminal, the shop detects that the deducted amount is not the same as required. Hence, a dishonest customer with the intentions to pay fewer amounts does not succeed in our proposed design.

F. New set of Keys for every transaction

The keys are generated from random number R (generated by the MNO). The R acts as a seed for all keys. As R is fresh for every transaction, therefore the keys are also new in each transaction.

G. Non-repudiation of Transaction Messages

The transaction result messages (message 23, message 25) are digitally signed. In case of any dispute about the payment, the MNO is to honour message 23 as it contains the MNO's digital signature. The shopping detail is also digitally signed by the shop POS terminal so the shop has to honour the prices mentioned in this message. Therefore the customer is completely secured about the transaction.

H. Securing long term secret

K_p is the long term secret between MNO and shop POS terminal. In our protocol, K_p is used with the least exposure (only once). The security policy of the MNO can define the update of this key after a defined interval.

VIII. Conclusion

In this paper we have proposed a transaction protocol that provides a secure and trusted communication channel to the communication parties. Our protocol is an improved version of already proposed Chen's protocol. The improved version provides freshness in the authentication part by introducing randomness by the mobile device. The original protocol lacks this randomness and hence is prone to replay attack in the authentication phase. The user interaction with the system is also reduced to a single interaction. We have added another security layer by introducing PIN authentication. This binds a user with his mobile device making the system more secure and user friendly. Digital signatures are also added in the transaction messages to provide data integrity and non-repudiation. Hence, our improved version provide a better security features than the original protocol.

References

[1] W. Chen, G. Hancke, K. Mayes, Y. Lien, and J.-H. Chiu, "NFC Mobile Transactions and Authentication Based on GSM Network," in *International Workshop on Near Field Communication*. Los Alamitos, CA, USA: IEEE Computer Society, 2010, pp. 83–89.

[2] C. Mulliner, "Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones," in *Proceedings of the The Forth International Conference on Availability, Reliability and Security, ARES, March 16-19, Fukuoka, Japan*. IEEE Computer Society, 2009, pp. 695–700.

[3] M. Q. Saeed and C. D. Walter, "A Record Composition/Decomposition Attack on the NDEF Signature Record Type Definition," *The* 6^{th} *International Conference for Internet Technology and Secured Transactions (ICITST-2011)*, 2011.

[4] Q. Zhang, "Mobile payment in mobile e-commerce," in *7th World Congress on Intelligent Control and Automation, WCICA 2008*. IEEE, 2008, pp. 6650 – 6654.

[5] G. Alpár, L. Batina, and R. Verdult, "Using NFC Phones for Proving Credentials," in *Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance - 16th International GI/ITG Conference, MMB & DFT 2012, Kaiserslautern, Germany, March 19-21, 2012.*, ser. Lecture Notes in Computer Science, vol. 7201. Springer, 2012, pp. 317–330.

[6] Macharia Kamau, "Orange Money triples its customer numbers in Africa," 2011. [Online]. Available: http://in2eastafrica.net/orange-money-triples-its-customer-numbers-in-africa/

[7] Wikipedia, "Subscriber Identity Module." [Online]. Available: http://en.wikipedia.org/wiki/Subscriber_identity_module

[8] ——, "Mobile Network Code." [Online]. Available: http://en.wikipedia.org/wiki/Mobile_Network_Code

[9] M. Bellare and C. Namprempre, "Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm," in *International Conference on Advances in Cryptology ASIACRYPT*, 2000, pp. 531–545.