Secure Authentication Protocol for NFC Mobile Payment Systems

Shadi Nashwan

Aljouf University, Computer Science and Information Department, SAKAK 42421, Saudi Arabia

Summary
Near Field Communication (NFC) is an attractive technology which is used in several countries for contactless payment operations via mobiles. This technology is suffered from increasing the security weaknesses. In the NFC mobile payment systems, the payment operations are vulnerable to various attacks. Therefore, the authentication protocol in the NFC technology has the highest priority to develop such systems. This paper proposes a new secure authentication protocol to provide strong security features for the NFC mobile payment systems, called (SAP-NFC) protocol. Compared with the recent NFC mobile payment authentication protocols, the security analysis has illustrated that the proposed SAP-NFC protocol can achieve highest level of security by supporting the fully mutual authentication, the key forward/backward secrecy, anonymity and untraceability features. In addition to, the SAP-NFC protocol is secure against replay attack, impersonate attack, tracking attack and desynchronization attack.

Key words:
NFC, PSP, POS, TTP, RFID.

1. Introduction

Mobile payment systems are becoming a key tool for payment serving providers (PSPs) [4]. In growing countries, the mobile payment systems have been used as a means of expanding the marketing services to their local communities, which is estimated to be more than half of the world population [2], [3]. The investment on mobile payment systems can grow up to 22.2% during the next year across the world, that will increase the revenue share of mobile money up to 9% in 2018 [4].

The NFC technology is one of the most attractive technology that is used in a wide range of mobile payment systems to deliver the payment services for customers via their mobiles [2]. In these systems, the NFC mobile is served as identification device or as a credit card [9], [10].

The NFC technology is a wireless communication technology that has been developed from Radio Frequency Identification (RFID) technology [12], [15], and [16]. The NFC technology has the following attributes [17], [19], and [26]: (1) the distance between communication NFC devices (i.e., the NFC mobile and NFC Point of Sale (POS)) must be less than 10 cm; (2) the frequency band is 13.56 MHz; (3) the speed range from 106 Kbps up to 424 Kbps.

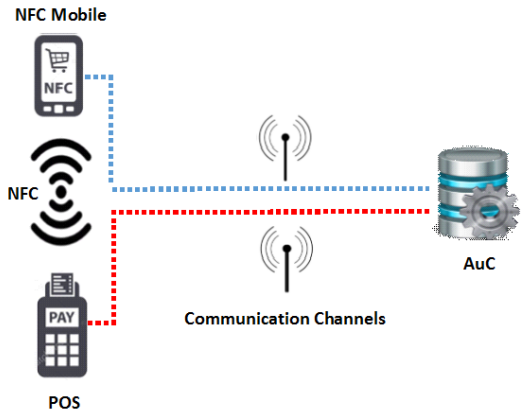

Fig. 1. The NFC mobile payment entities.

Fig.1 shows the main entities of the NFC mobile payment systems that can be summarized as the following: (1) the Authentication Center (AuC) that contains the security information of all NFC mobiles and NFC POSs in the system; (2) the mobile that is integrated with the NFC technology; (3) the POS that also must be integrated with the NFC technology.

In order to establish a secure communication due to no credibility between the NFC devices, both of the NFC mobile and NFC POS have to register in the AuC as trusted third party (TTP) using secure communication channels [18], [25], and [27]. In general, to execute the payment transactions, the NFC mobile payment system executes the following steps [22], [23], and [24]: (1) the NFC mobile user puts his/her phone near the NFC POS to send the transaction request message; (2) the NFC POS forwards the received request message to the AuC; (3) the AuC verifies the NFC devices and sends the transaction response message back to the NFC POS; (4) upon receiving the transaction response message, the NFC POS authenticates NFC mobile, then NFC POS forwards the response message to the NFC mobile; (6) the latter

Manuscript received August 5, 2017
Manuscript revised August 20, 2017

authenticates the NFC POS and executes the payment transaction with the NFC POS.

The communication channels between the NFC devices in NFC mobile payment systems are susceptible to numerous attacks such as; replay attack, impersonate attack, tracking attack and desynchronize attack [1], [8], and [11] . In this situation, the authentication service is considered an essential component to develop secure mobile payment protocol. In order to achieve high level of security, there have been many research works on authentication protocols for NFC mobile payment systems [5], [6], [14] [20], and [21]. This paper proposes a secure authentication protocol for NFC mobile payment systems to defeat the security threats during the transactions of payment, called SAP-NFC protocol. The proposed protocol can overcome the existing attacks; such as replay attack, impersonate attack, tracking attack and desynchronize attack. Furthermore, the SAP-protocol can achieve a set of attractive security features such as fully mutual authentication feature, the key forward/backward secrecy feature, anonymity feature and untraceability features.

This paper is organized as follows: Section 2 introduces the related works. The SAP-NFC protocol is introduced in section 3 .The security analysis of the proposed protocols are discussed in section 4. Finally, this paper will be concluded in section 5.

2. Related Work

Recently, a lot of research works on the authentication protocol for NFC mobile payment systems have been conducted. It is reasonable to suggest that majority solutions to defeat security drawbacks of the NFC mobile payment systems in the reported investigation are based on asymmetric techniques [12], [13], [15], [20], and [21]. Due to the limited resources of NFC devices and the amount of data that can be transferred by NFC technology, the author believes that symmetric techniques are more efficient to solve these problems. Therefore, this section introduces the summary about the recent protocols that are based on the symmetric technique to solve such issue.

In 2015, Thammarat et al. [7] introduce a secure lightweight protocol for NFC communications with mutual authentication based on limited-use of session key. The proposed protocol contains two main sub-parts: (1) the NFCAuthv1 is performed between the NFC device and authentication server; (2) the NFCAuthv2 is performed between the NFC device, POS, and authentication server. Moreover, the introduced protocol contains a set of authentication operations that can be summarized as the following: (1) executes the encryption/decryption operations base on symmetric techniques six times; (2) performs the hash function nine times; (3) exchanges eight authentication messages between the authentication entities. However, the proposed protocol includes a set of drawbacks: (1) the mutual authentication is satisfied partially; (2) the key forward/backward secrecy is not satisfied; (3) cannot achieve the NFC mobile anonymity aspect; (4) connote defeat the tracking attack; (5) cannot defeat the desynchronization attack; (6) is not efficient in term of the amounts of data that are transmitted among the NFC devices.

In 2017, Tung and Juang [28] design a secure and efficient mutual authentication scheme for NFC mobile Devices. The proposed scheme includes two phase: (1) the registration phase that is performed between NFC mobile and the authentication server; (2) the authentication phase that is performed between the NFC1, POS and authentication sever. In this protocol, the authentication entities perform a set of authentication operations: (1) execute the hash function nine times; (2) exchange seven authentication messages; (3) However, the proposed protocol is lacked for some security aspects, which are important for NFC mobile authentication protocols: (1) the mutual authentication is satisfied partially; (2) the key forward/backward secrecy is not satisfied; (3) cannot achieve the NFC mobile anonymity and untraceability aspects; (4) cannot prevent the tracking attack; (5) the amounts of data that are transmitted among the NFC devices relatively is not efficient.

3. Proposed Work (SAP-NFC protocol)

This section demonstrates the assumptions, design requirements and the notation of the SAP-NFC protocol, respectively. In addition to, the SAP-NFC protocol description during the registration phase and authentication phase is discussed, respectively.

3.1 Assumptions

The SAP-NFC protocol is performed based on a set of assumptions: (1) the structure of SAP-NFC protocol consists of two NFC devices and AuC as TTP to perform the registration and Identification processes during the authentication session; (2) the NFC devices can register in the AuC using secure communication channels during the registration phase; (3) the communication channels between the authentication entities during the authentication phase are susceptible to various attacks; (4) the AuC can verify the identities of an NFC device by a set of the authentication messages; (5) the authentication

parameters that are stored in the authentication entities can be accessed and updated using a secure access control method; (6) the NFC mobile cannot perform any payment operations outside the range of NFC POS; (7) each NFC device has its own session key.

3.2 Design Requirements

In order to resist the existing attacks: (1) the NFC devices can produce pseudo random numbers; (2) both of the AuC and NFC devices can update their secret key; (3) the AuC can save the new and old secret keys of the NFC devices in database; (4) the mutual authentication must be achieved between all authentication entities; (4) the hash function is used to conceal the NFC devices identities; (5) the Key derivation function (KDF) is used by the authentication entities to derive a new session secret key.

3.3 Notation

Table 1: SAP-NFC Protocol notation.

Notation	Description
IDNj	NFC device with identity j
Kj	initial secret key of NFC device j
KPnew	New secret key of the NFC POS that is stored in AuC
KPold	Old secret key of the NFC POS that is stored in AuC
KMnew	New secret key of the mobile that is stored in AuC
KMold	Old secret key of the mobile that is stored in AuC
KM	Secret key of NFC mobile
KP	Secret key of NFC POS
IDP	Identity of NFC POS
IDM	Identity of NFC mobile
Rj	Random number that is generated by NFC device j
HIDP	Hash value that is generated by the NFC POS
R1,R3	Random numbers that are generated by NFC POS
HIDM	Hash value that is generated by the NFC mobile
R2	Random number that is generated by the NFC mobile
M1	Hash value that is generated by the NFC mobile
XM7	Expected Hash value that is generated by the mobile
M2	Validation message that is generated by NFC mobile
M3	Hash value that is generated by the NFC POS
XM5	Expected Hash value that is generated by the POS
M4,M7	Validation message that is generated by NFC POS
M5,M6	Hash values that are generated by the AuC
XM1,XM3	Expected Hash values that are generated by the AuC
E( )	Encryption function
D( )	Decryption function
IDMX	Encryption value of NFC mobile identity
IDPX	Encryption value of NFC mobile identity
KDF	Derivation function
H	Hash function
X ⊕ Y	X value is Xored with the Y value
X← Y	X value is updated to the Y value
j	Authentication session number
F1,F2	Flag values

3.4 Registration Phase

In the registration phase, each NFC device must sign itself into the AuC as shown fig. 2. The communication channels are secured between the NFC devices and AuC during the registration phase. The detail of the registration phase is summarized as follows: (1) the NFC device sends the registration request message which contains the NFC device identity (IDNj) and the random number (Rj) that is generated by the NFC device; (2) upon receiving the registration request message, the AuC generates the initial secret key (Kj) of the NFC device using the KDF; (3) the AuC sends the confirmation message to the NFC device; (4) when the confirmation message is received, the NFC device performs the KDF function to derive the Kj.

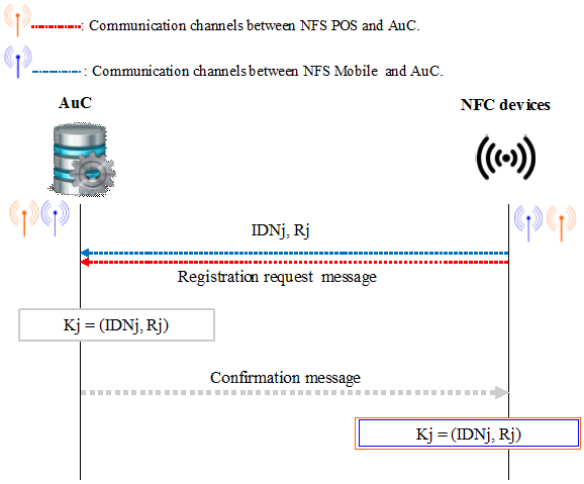

Fig. 2. The registration phase in SAP-NFC protocol

3.5 Authentication Phase

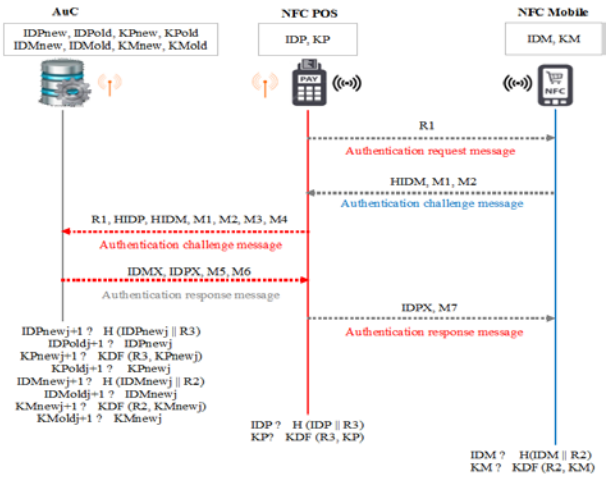

Fig. 3. The authentication phase in SAP-NFC protocol

Initially, the authentication entities have the following data: (1) each NFC mobile includes the mobile identity (IDM) and secret key (KM); (2) each NFC POS includes the POS identity (IDP) and its secret key (KR); (3) the AuC contains the secret data of all NFC devises in the system such as the IDM and IDP. To manage the updating process of the secret keys for all NFC devices in each authentication session (j), the AuC also contains the old and new secret keys of NFC devices such (KPold, KPnew, KMold, KMnew).

Fig. 3 illustrates the steps of the authentication phase in the SAP-NFC protocol. In order to start the payment transaction, the NFC POS sends the authentication request message for NFC mobile. This message contains the random number (R1) that has been generated by the NFC POS.

Upon receiving the authentication request message from the NFC POS, the NFC mobile performs the following steps to identify itself to the AuC: (1) generates the random number (R2); (2) calculates the hash value (HIDM) as HIDM = H (IDM || R1); (3) computes the hash value (M1) as M1 = H (KM || R1 || R2); (4) computes the validation message (M2) as M2 = IDM ⊕ R2; (5) sends the authentication challenge message back to the NFC POS which contains HIDM, M1 and M2.

When the authentication challenge message is received, the NFC POS performs the following steps to identify itself to the AuC: (1) generates the random number (R3); (2) calculates the hash value (HIDP) as HIDP = H (IDP || R1); (3) computes the hash value (M3) as M3 = H (KP || R1 || R3); (4) computes the validation message (M4) as M4 = IDP ⊕ R3; (5) forwards the authentication challenge message back to the AuC which contains R1, HIDM, HIDP, M1, M2, M3 and M4.

Upon receiving the authentication challenge message from the NFC POS, the AuC computes the following steps to verify NFC mobile: (1) for all the stored IDMs either in the IDMnew or IDMold lists, the AuC computes H (IDMnew/IDMold || R1) until it finds a match value with the received value of HIDM, if the IDM in the IDMnew list then the flag value (F1) sets 1 and the KMnew is retrieved, else if the IDM in the IDMold list then F1 sets 0 and KMold is retrieved. In case there is no match value, the AuC terminates the session; (2) extracts the R2 as R2 = IDM ⊕ M2; (3) computes expected hash value XM1 as XM1 = (KMnew/KMnew || R1 || R2), in case the computed XM1 value is not equal to M1 value that has been received, the AuC terminates the session, else the NFC mobile is verified.

In the same context, the AuC computes the following steps to verify the NFC POS: (4) for all the stored IDPs either in the IDPnew or IDPold lists, the AuC computes H (IDPnew/IDPold || R1) until it finds a match value with the received value of HIDP, if the IDP in the IDPnew list then the flag value (F2) sets 1 and the KPnew is retrieved, else if the IDP in the IDPold list then F2 sets 0 and KPold is retrieved. In case there is no match value, the AuC terminates the session; (5) extracts the R3 as R3 = IDP ⊕ M4; (6) computes expected hash value XM3 as XM3 = (KPnew/KPnew || R1 || R3), in case the computed XM3 value is not equal to M3 value that has been received, the AuC terminates the session, else the NFC POS is verified.

Through steps 3 and 6, both of the NFC mobile and NFC POS are authenticated by the AuC. In order to prepare the authentication response message, the AuC performs the following steps: (7) computes the hash value (M5) as M5 = H (R1 || R3 || IDM); (8) encrypts the IDM as IDMX E(IDM)KPold/KPnew; (9) computes the hash value (M6) as M6 = H (R1 || R2 || IDP); (10) encrypts the IDP as IDPX = E(IDP)KMold/KMnew; (11) sends the authentication response message which includes M5, M6, IDPX and IDMX back to the NFC POS; (12) if F1 = 1, the AuC updates the NFC mobile identity and their secret key as IDMnewj+1←H (IDMnewj || R2), IDMoldj+1← IDMnewj and KMnewj+1←KDF (KMj, R2), KMoldj+1 ← KMj, respectively; (13) if F2 = 1, the AuC updates the NFC POS identity and the secret key as IDPnewj+1←H (IDPj || R3), IDPoldj+1←IDPj and KPnewj+1←KDF (KPj,R3), KPoldj+1←KPj, respectively.

When the NFC POS receives the authentication response message, the NFC POS performs the following steps: (1) decrypts IDMX as IDM = D (IDMX) KP; (2) computes the expected hash value (XM5) as XM5 = H (R1 || R3 || IDM) to verify the AuC and NFC mobile. In case both values, i.e., XM5 and M5 values are not equal then the NFC POS terminates the authentication session else; (3) computes the validation message (M7) as M7 = M6 ⊕ IDP; (4) forwards the authentication response message which contains the M7 value and IDPX to the NFC mobile; (5) updates both of the NFC POS identity and the secret key as IDP←H (IDP || R3) and KP←KDF (KP, R3), respectively.

Upon receiving the authentication response message, the NFC Mobile performs the following steps: (1) decrypts IDPX as IDP = D (IDPX) KM; (2) computes the expected hash value (XM7) as XM7 = (H (R1 || R2 || IDP) ⊕ IDP) to authenticate both of the NFC POS and AuC. In case both values, i.e., XM7 and M7 are not equal then the NFC terminates the authentication session else; (3) updates both of NFC mobile identity and the secret key as IDM←H (IDM || R2) and KM←KDF (KM, R2), respectively.

4. Security Analysis

In this section, the security analysis is conducted to demonstrate that the SAP-NFC protocol can support attractive security features with high security level during

the mobile payment transactions. Moreover, this section illustrates how the SAP-NFC protocol can resist the existing attacks. The security achievements of the SAP-NFC protocol have been compared with the security achievements of the recent NFC mobile payment authentication protocols in [7], [28].

4.1 Mutual authentication

The SAP-NFC protocol supposes that all the communication channels between the authentication entities are susceptible to attack during the authentication phase. Therefore, the SAP-NFC protocol deploys a set of hash values and validation messages to achieve the mutual authentication between all authentication entities. In order to authenticate the NFC mobile, the AuC checks whether the IDM in the NFC mobile identity Lists (i.e., IDMold and IDMnew Lists) or not. After that, the AuC verifies whether XM1 value is equal to the M1 value or not. Subsequently, if the IDM is not in the IDM lists or XM1 is not the same as M1, the NFC mobile will be considered is not legitimate then the AuC terminates the authentication session.

The same process is performed by the AuC to authenticate the NFC POS, the AuC checks whether the IDP in the NFC POS identity Lists (i.e., IDPold and IDPnew Lists) or not. After that, the AuC verifies whether XM3 value is equal to the M3 value or not. Subsequently, if the IDP is not in the IDP lists or XM3 is not the same as M3, the NFC POS will be considered is not legitimate then the AuC terminates the authentication session.

The NFC POS verifies whether the XM5 value is equal to the M5 value or not. If XM5 is not the same as M5, the AuC will be considered is not legitimate TTP then, the NFC POS terminates the authentication session. In the same manner, the NFC mobile verifies whether the M7 value is equal to the M7 value or not. If XM7 is not the same as M7, the AuC will be considered is not legitimate TTP, then the NFC mobile terminates the authentication session. Whereas both of NFC devices authenticates each other indirectly through the IDPX and IDMX. Therefore, the SAP-NFC protocol can support fully mutual authenticate feature between all authentication entities.

4.2 Key backward/forward secrecy (KFS/KBS)

An attacker cannot deduce the session keys during the authentication phase in the SAP-NFC protocol due to using a set of one time functions. The KM is protected by the hash function with the R2 that is generated by the NFC mobile and is not transmitted as plain message between the authentication entities. In the same manner, the KP is not sent as plain text between authentication entities, it is protected by the hash function with the R3 that is generated by the NFC POS. In addition to, the KM and KP are updated after each successful authentication session by the AuC and NFC devices using the KDF function. Therefore, if the validation messages and hash values are compromised by the attacker, the latter cannot guess the session keys. In other words, deducing the session keys is difficult problem computationally.

4.3 Anonymity and Untraceability

The SAP-NFC protocol protects the IDM and IDP within the challenge and response messages either by the hash or encryption functions. Moreover, NFC devices identities are updated after each successful authentication session using the hash function with fresh random numbers that are generated during the authentication phase. Thus, the SAP-NFC protocol can support anonymity and untraceability features, only a legitimate AuC that has information related to the NFC devices can determine the identity and the location of the NFC devices during the payment transactions.

4.4 Resistance to attacks

Assume that the adversary can eavesdrop and obtain the authentication messages that are exchanged between the NFC payment system entities. In the same time, assume the adversary can reuse and retransmit these messages to impersonate the authentication entities.

In contrast, the SAP-NFC protocol provides many security features that can be summarized as the following: (1) all authentication parameters are protected by hash functions; (2) an adversary cannot obtain the session keys or any authentication parameters that are transmitted between the authentication entities; (3) both of IDM and IDP are updated after each successful authentication session by the AuC and the NFC devices; (4) the NFC devices identities (i.e., IDP and IDM) are concealed during the authentication phase; (5) the secret session keys (i.e., KP and KM) are renewed after each successful authentication; (6) if the authentication session is not successful, the existing identities and session keys of the NFC devices will be used for next authentication session with fresh authentication parameters such as the R1,R2 and R3;(7) fully mutual authentication must be achieved between all authentication entities; (8) the session keys cannot be deduced by the adversary. Therefore, the SAP-NFC protocol can defeat the following attacks:

4.4.1 Replay attack

In the SAP-NFC protocol, just a legitimate AuC that has information related to the NFC devices can authenticate both of the NFC mobile and NFC POS. The IDM and IDP

are protected during transmission via the hash function, the IDM and IDP are updated after each successful authentication session by the AuC and the NFC devices, the secret session keys also are renewed after each successful authentication by the AuC and the NFC devices. Therefore, only an authorized authentication entities can decrypt the NFC mobile's or NFC POS's reply. If the adversary tries to reuse the authentication messages that have been eavesdropped from the previous authentication sessions, the authentication entities in the SAP-NFC protocol can avoid the reusing of the same random numbers for next authentication sessions. Therefore, the SAP-NFC can defeat replay attack.

4.4.2 Tracking attack

The SAP-NFC protocol achieves the Location privacy feature. In the proposed protocol, the authentication entities update their authentication parameters after each successful authentication session, so the exchanged messages values are updating continuously. This means, the authentication entities responses are anonymous. Suppose the authentication session is not successful, the adversary will not be able to track the mobile location where the IDMX, IDPX, M1, M2, M3, M4, M5, M6 and M7 are not fixed due to the freshly random numbers that are generated by the NFC devices. Thus, the SAP-NFC can defeat the tracking of the mobile holder location.

4.4.3 Desynchronization attack

The SAP-NFC protocol can defeat the desynchronization attack between the authentication entities. In despite of an adversary can block the messages between the authentication entities, the AuC can use the IDPold and IDMold to identify NFC POS and NFC mobile, respectively. Assume that the AuC is failed to authenticate the NFC mobile or the NFC POS. Subsequently, the NFC devices will not receive IDMX, IDPX, M5, M6 and M7. In this case, the NFC devices will not update their identities and their secret session keys. Then the NFC mobile and NFC POS will still match the AuC values of (IDMold, KMold) and (IDPold, KPold), respectively.

4.4.4 Impersonate attack

The SAP-NFC protocol can defeat the impersonate attacks. In particular, the adversary cannot impersonate any of the authentication entities. In order to impersonate the NFC mobile entity, the adversary must be able to compute a valid response (i.e., HIDM, M1 and M2) to NFC POS request. However, the adversary cannot compute such responses without knowledge of IDM, KM and R2. In the same manner, the adversary cannot impersonate the NFC POS, adversary must be able to compute a valid challenge messages (i.e., R1, HIDP, M3 and M4) to the AuC, and also must be able to compute a valid response messages (i.e., R1, IDPX and M7) to NFC mobile. However, the adversary cannot compute such challenge and response messages without knowledge of IDP, KP and R3. Due to the adversary cannot compute the response (i.e., M5, M6, IDPX and IDMX) without knowledge of IDM, IDP, KM, KP, R2 and R3, the adversary also cannot impersonate the AuC. Moreover, the current value of HIDM, HIDP, M1, M2, M3, M4, M5, M6, m7, IDPX and IDMX are updating continuously in each authentication session.

4.5 Security Achievements

Table 2 shows that the SE-H protocol achieves the highest level of security among the other authentication protocols in [7], [28]. The notation (=), (T) and (ǂ) denote that the security feature is fully satisfied, partially satisfied and is not satisfied, respectively.

Table 2. Statues of Security Achievements of the authentication protocol

Security features	[7]	[28]	SAP-NFC
Mutual Authentication.	T	T	=
Anonymity and untraceability.	ǂ	ǂ	=
Key backward/forward secrecy.	ǂ	ǂ	=
Renew the session key periodically.	ǂ	ǂ	=
Secure against replay attack.	T	T	=
Secure against desynchronization attack.	ǂ	=	=
Secure against Impersonate attack.	T	T	=
Secure against tracking attack.	ǂ	ǂ	=

5. Conclusions

This paper proposes a new secure authentication protocol to provide strong security features for the NFC mobile payment systems, called (SAP-NFC) protocol. Comparing with the recent mobile payment protocols that are based on symmetric cryptography, the SAP-NFC protocol can achieve highest level of security by supporting the fully mutual authentication, the KFS/KBS, anonymity and untraceability features. The fully mutual authentication between all authentication entities is achieved based on a set of hash values and validation messages, the KFS/KBS are satisfied by using the KDF functions to derive the new secret keys of the NFC devices. The identities of the authentication entities are completely concealed using the hash function whereas the identities and the secret keys of the NFC devices are renewed in each successful authentication session. The security analysis demonstrates that the SAP-NFC protocol can defeat the existing attacks

such as replay attack, impersonate attack, tracking attack and desynchronization attack.

References

[1] A. Alshehri, S. Schneider, "Addressing NFC Mobile Relay Attacks: NFC User Key Confirmation Protocols", International Journal of RFID Security and Cryptography, Vol. 3, No. 2, pp. 137-147, 2014.

[2] A. Allyson, V. Lakshmi, A. Packialatha, "Mobile Devices using NFC in Payment Applications", International Journal Of Innovative Research in Technology & Science, Vol. 3, No. 1, pp, 32-36, 2015.

[3] A. Chaia, A. Dalal, T. Goland, M. Gonzalez, J, Morduch, R. Schiff, "Half the World is Unbanked", Financial Access Initiative Framing Note, 2009. www.financialaccess.org.

[4] A. Khan, M. Gandhi, A. Jain, N. Kacholia, "Emerging Markets Driving the Payments Transformation", PWC network, 2016. www.pwc.com/emergingmarketspayments.

[5] A. Matos, D. Romao, P. Trezentos, "Secure Hotspot Authentication through a Near Field Communication Side-Channel", in Proc. IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Spain, pp. 807 – 814, 2012.

[6] B. Seo, S. Lee, H. Kim, "Authenticated Key Agreement Based On NFC for Mobile Payment", International Journal of Computer and Communication Engineering, Vol. 5, No. 1, pp. 71-78, 2016.

[7] C. Thammarat, R. Chokngamwong, and C. Techapanupreeda, "A secure lightweight protocol for NFC communications with mutual authentication based on limited-use of session keys", Proceedings of the IEEE International Conference on Information Networking, Siem reap, Cambodia, pp. 133-138, 2015.

[8] F. Ota, M. Roland, M. Holzl, R. Mayrhofer, A. Manacero, "Protecting Touch: Authenticated App-To-Server Channels for Mobile Devices Using NFC Tags", Information, Vol. 8, No. 3, pp. 1-18, 2017.

[9] J. Ahn, S. Lee, H. Kim, "NFC based privacy preserving user authentication scheme in mobile office", International journal of computer and communication engineering, Vol. 5, No. 1, pp. 61-70, 2016

[10] J. Lee, "A system functions set-up through Near Field Communication of a smartphone", International journal of computer, electrical, automation, control and information engineering, Vol. 10, No. 5, pp. 841-838, 2016.

[11] J. Ling, Y. Wang, W. Chen, "An improved privacy protection security protocol based on NFC", International journal of network security, Vol. 19, No. 1, pp.39-46, 2017.

[12] M. Badra, R. Badra," A lightweight security protocol for NFC-based mobile payments", Proceedings of the 7th international conference on ambient systems, networks and technologies Madrid, Spain, Procedia Computer Science 83, pp. 705 – 711, 2016.

[13] M. Rahman, H. Elmiligi, "Classification and analysis of security attacks in near field communication", International Journal of Business & Cyber Security Vol. 1, No. 2, pp. 1-14, 2017.

[14] N. El Madhoun, F. Guenane, G. Pujolle, "An online security protocol for NFC payment: formally analyzed by the scyther tool", Proceedings of the IEEE Second international conference on mobile and secure services (MobiSecServ), FL, USA, pp. 1-7, 2016..

[15] N. El Madhoun, G. Pujolle, "Security enhancements in EMV protocol for NFC mobile payment", Proceedings of the IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, pp. 1889 – 1895, 2016.

[16] N. El Madhoun, F. Guenane, G. Pujolle," A cloud-based secure authentication protocol for contactless NFC payment". Proceedings of the IEEE 4th international conference on cloud networking, Niagara Falls, Canada, pp.328-330, 2015.

[17] N. Shrangare, S. Joshi, "Secure protocol implementation using near field communication", International research journal of engineering and technology, Vol. 2, No. 3, pp. 589-593, 2015.

[18] N. Singh, A. Maity, R. N, "Conditional privacy preserving security protocol for NFC applications", International journal of innovations in engineering research and technology, Vol. 5, No. 2, pp. 1-11, 2015.

[19] O. Jensen, M. Gouda, L. Qiu, "A secure credit card protocol over NFC", Proceedings of the 17th International Conference on Distributed Computing and Networking, Singapore, Singapore, No. 32, 2016. ACM digital library.

[20] P. Pourghomi, M. Saeed, G. Ghinea, "A secure cloud-based NFC mobile payment protocol", International journal of advanced computer science and applications, Vol. 5, No. 10, pp. 24-31, 2014.

[21] R Sivaranjani, R. Sujitha, D. Sindhu, T. Tharani, "Secure and efficient authentication protocol using pseudonym", Journal of chemical and pharmaceutical sciences, special issue 5: 2017.

[22] S. Nashwan, B. Alshammari, "Mutual chain authentication protocol for span transactions in Saudi Arabian banking", International journal of computer and communication engineering, Vol. 3, No. 5, pp. 326-333, 2014.

[23] S. Sung, E. Kong, C. Youn," Mobile payment based on transaction certificate using cloud self-proxy server", ETRI Journal, Vol. 39, No. 1, pp. 135-144, 2017.

[24] S. Yang, K. Yang, "Design and application of NFC-based identity and access management in cloud services", International journal of computer, electrical, automation, control and information engineering, Vol. 11, No. 4, pp. 408-416, 2017.

[25] S. Zaidi, M. Shah, M. Kamran, Q. Javaid, S. Zhang, "A survey on security for smartphone device", International journal of advanced computer science and applications, Vol. 7, No. 4, pp. 206-219, 2016.

[26] V. Coskun, B. Ozdenizci, K Ok, "A Survey on Near Field Communication (NFC) Technology", Wireless personal communications, Vol. 71, No. 3, pp. 2259-2294, 2013.

[27] Y. Ma, "NFC communications-based mutual authentication scheme for the internet of things", International journal of network security, Vol. 19, No. 4, pp.631-638, 2017.

[28] Y. Tung, W. Juang, "Secure and efficient mutual authentication scheme for NFC mobile devices", Journal of electronic science and technology, VOL. 15, NO. 3, pp, 1-6, 2017.

Shadi Nashwan received his B.Sc. degree in Computer Science from Alazhar University, Palestine, in 2001, and the M.Sc. degree in Computer Science from university of Jordan, Jordan, in 2003, and the Ph.D. degree in Computer Science from Anglia Ruskin University, UK, in 2009. Dr. Nashwan currently is assistant professor in Computer science and information department, Aljouf University, Saudi Arabia. His research focuses on authentication protocol of mobile network, mobility management, and wireless network security. He has published several papers in the area of authentication protocol, recovery techniques and mobility management.