Performance Analysis of SAP-NFC Protocol

Mustafa Al-Fayoumi[1], Shadi Nashwan[2]

[1]King Hussein School of Computing Sciences, Princess Sumaya University for Technology (PSUT), Jordan
[2]College of Computer and Information Sciences, Aljouf University, Saudi Arabia

***Abstract*:** Near field communication (NFC) is a wireless communication technology. It is one of the most recent technologies that offers great and varied promise in the area of application development and service delivery via mobile phone, such as payment, ticketing, voting, access control function, navigation, and many others. NFC technology enables the mobile equipment to act as identification and a virtual credit card for customers, but one of the most challenging problems introduced by NFC mobile payment protocol is security. Therefore, a secure and efficient authentication mechanism is particularly crucial for NFC mobile payment systems. The operations cost of authentication sessions is considered as a strict indicator to evaluate the authentication protocols side by side with the security requirement achievements in NFC technology. The secure authentication protocol for NFC mobile payment systems (SAP-NFC) is one of the recent authentication protocols that have been proposed to achieve high levels of security, which includes fully mutual authentication, anonymity, and untraceability. Moreover, the SAP-NFC protocol can prevent current security attacks. In this paper, we analyze the performance of the SAP-NFC protocol compared with other recent NFC mobile payment protocols in all system entities. The performance analysis finds that the SAP-NFC protocol not only supports strong security features, but also offers a low cost in terms of the amount of computations. Therefore, the performance analysis proves that SAP-NFC protocol is secure and reasonable for practical implementation.

***Keywords*:** Symmetric authentication protocol, near field communication (NFC), point of sale (POS), trusted third party (TTP).

1. Introduction

NFC is an attractive technology that is now widely used in mobile payment applications [4, 7, 9, 10, and 11].

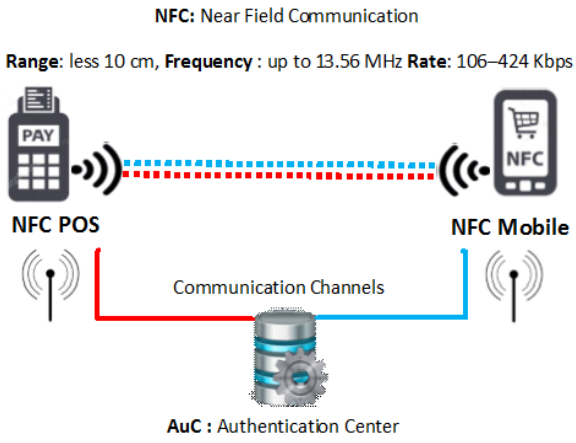


Figure 1. NFC mobile payment application parties

Figure 1 illustrates the main parties to the NFC mobile payment application, as follows: (1) the credit card that is identified through the NFC mobile to deliver the payment service to the customer; (2) the point of sale (POS) that is integrated with the NFC technology; and (3) the authentication center (AuC) that serves as the trusted third party (TTP), which includes the security parameters of NFC mobiles and NFC POSs in the payment system.

In general, payment is performed through the following operations [6, 13, 16, 22, 23, 24]: (1) the customer tabs the NFC mobile in the range of the NFC POS to send the payment request message; (2) the NFC POS resends the payment request message to the AuC; (3) the AuC checks the security information of both POS NFC and NFC mobile devices; (4) the AuC transmits the response payment message to the NFC POS; (5) the latter authenticates the NFC mobile; (6) the NFC POS sends the response payment message to the NFC mobile; and (7) on receiving the response payment message, the NFC mobile verifies the NFC POS and completes the payment operation.

Numerous authentication protocols have been proposed to overcome the security drawbacks in NFC mobile payment applications [25, 26, 27, 28, 29]. The secure authentication protocol for the NFC mobile payment applications (SAP-NFC) is a recent symmetric authentication protocol that has been found to achieve a high level of security [1].

The SAP-NFC protocol supports fully mutual authentication between all authentication parties using a set of hash parameters within the validation messages. At the same time, the SAP-NFC protocol can achieve the key backward and key forward secrecy (KFS/KBS) feature based on a set of the key derivation functions (KDF). Moreover, to conceal the identities of the authentication parties, the SAP-NFC protocol renews the identities and the secret keys of the NFC devices in each successful authentication session. Consequently, this protocol can defeat existing attacks on NFC mobile payment applications [4, 9, 13].

NFC technology is used to establish the connection between the NFC mobile and the NFC POS [29]. Unfortunately, this connection has the following limitations: (1) the range between NFC devices is not more than 10 cm; (2) the frequency is around 13.56 MHz; (3) the transfer rate is within the range 106–424 Kbps. Therefore, the cost of authentication operations is considered as a strict indicator to evaluate the authentication protocols side by side with the security requirement achievements of the authentication protocols of NFC mobile payment applications [1, 30].

This paper analyzes the performance of the SAP-NFC protocol compared with two other recent symmetric authentication protocols for NFC mobile payment applications [2, 3]. The performance analysis is conducted in terms of the cost of authentication operations and the number of computations in NFC devices. This paper is organized as follows: section 2 introduces related works; the SAP-NFC protocol is overviewed in section 3; the security analysis of

the proposed protocol is discussed in section 4; and finally, section 5 presents the conclusions.

2. Related Work

In recent years, many authentication protocols for NFC mobile payment applications have been proposed [5, 8, 12, 14, 15, 17, 18, 20, 21]. The majority of these protocols are based on asymmetric methods. Owing to performance considerations, NFC technology is considered as a restricted and poor resources environment, and the authors believe that symmetric methods are more suitable for such an environment than asymmetric methods.

Therefore, to compare the SAP-NFC protocol with other authentication protocols in terms of the number the amount of computations, this section presents a summary of the recent authentication protocols for NFC mobile payment applications.

Ceipidor et al. [31] introduce a mutual authentication protocol between NFC Phone device and NFC POS based on asymmetric method. This protocol includes three different authentication entities: (1) the POS, which is a sale station that is supported NFC (POS); (2) the NFC Mobile (N); and (3) the Authentication Server (AS). This protocol includes the following operations: (1) exchanges five authentication messages; (2) executes two asymmetric encryption functions; (3) executes two asymmetric decryption functions; and (4) executes five hash functions. The protocol achieves the confidentiality and mutual authentication security features. However, this protocol is not satisfied the following security features: (1) message integrity; (2) the session keys are not dynamic parameters; (3) cannot prevent the brute-force attacks; and (4). the session keys are sent through as clear text.

Lee et al. [32] introduce an authentication protocol for NFC contactless. This authentication protocol includes three authentication entities: (1) the Mobile (U1), which is used as an authenticator; (2) the Mobile (U2), which is used as a medium to support authentication; and (3) Authentication Center (AUC). The protocol adapts both of the symmetric and asymmetric cryptography techniques as well as hash functions. The protocol includes two main sub protocols: The Registration protocol which is executed between the authentication server and mobiles; and Authentication protocol which is executed between the Mobile (U1) and Authentication Center (AuC) through Mobile (U2). This protocol includes the following operations: (1) exchanges six authentication messages; (2) executes one asymmetric encryption functions; (3) executes one asymmetric decryption functions; (4) executes four symmetric encryption functions; (5) executes four symmetric decryption functions; and (6) executes three hash functions. Lee et al. [7] claim that, the protocol can be prevented different types of attacks such as the man-in-the-middle replay attacks. However, this protocol lacks a set of necessary security features and limitations: (1) the protocol still lacks mutual authentication; and (2) the AuC deploys public key encrypted message without verify the recipient of the message.

Thammarat et al. [2] introduce a symmetric authentication protocol for NFC mobile payment applications called a secure lightweight protocol. This protocol includes two main sub protocols: "NFCAuthv1," which is executed between the authentication server and the NFC mobile; and "NFCAuthv2," which is executed between the authentication server, NFC mobile and NFC POS. The proposed protocol includes the following operations: (1) the encryption/decryption functions are performed six times; (2) the message authentication code (MAC) functions are executed more than nine times; (3) the challenge and response messages are exchanged between the authentication parties eight times. However, this protocol contains a set of limitations: (1) the authentication is not achieved between all authentication parties; (2) the KFS and KBS are not achieved; (3) the anonymity feature is not satisfied for the NFC mobile and NFC POS; (4) the NFC mobile is susceptible to tracking attack; and (5) the desynchronization attack is not defeated.

Tung and Juang [3] introduce another symmetric authentication protocol for NFC mobile payment applications. The proposed protocol contains two stages: (1) the registration stage that is executed between NFC devices and the authentication server; (2) the authentication stage that is executed between the NFC mobile, NFC POS, and the authentication sever. The proposed protocol executes the following operations between the authentication parties: (1) the hash function is executed nine times; (2) the challenge and response messages are exchanged between the authentication parties seven times. However, this protocol has some security drawbacks such as: (1) authentication is not achieved between all authentication parties; (2) KFS and KBS secrecy are not achieved; (3) the anonymity aspect is not achieved for the NFC mobile; (4) the NFC mobile is susceptible to tracking attack.

3. Overview of SAP-NFC Protocol

In the SAP-NFC protocol [1], the authentication session is accomplished through the registration phase and authentication phase with the following assumptions: (1) the registration process between the NFC devices and AuC is performed through secure communication lines, while the communication lines during the authentication process are susceptible to different type of attacks; (2) both in the registration phase and in the authentication phase, the AuC verifies the NFC devices by a set of identities and authentication parameters; and (3) the NFC mobile must be within the range of NFC POS to execute the payment transaction.

The design requirements of the SAP-NFC protocol can be summarized as follows: (1) all the authentication parties can generate random numbers; (2) the AuC and the NFC devices can renew their secret keys for each authentication session; (3) both the old secret keys of previous authentication session and the new secret keys of the current authentication session of the NFC devices will be saved in the AuC database; (4) the mutual authentication must be conducted between all authentication parties; (5) the new session keys are derived by the KDF functions; (6) the identities of the authentication parties are concealed by a set of hash functions.

3.1 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
F1, F2	Flag values

3.2 Registration Phase

In this phase, the NFC devices must be registered in the AuC database, as illustrated in Figure 2. The registration phase is accomplished according to the following steps, for either the NFC mobile or the NFC POS: (1) both the identity (IDNj) and the random number (Rj) are sent to AuC from the NFC devices through the registration request message; (2) the AuC executes the KDF to generate the secret key (Kj) based on the parameters in the request messages; (3) the confirmation message is sent back to the NFC device from AuC; (4) the NFC device executes the KDF function to derive the secret key (Kj).

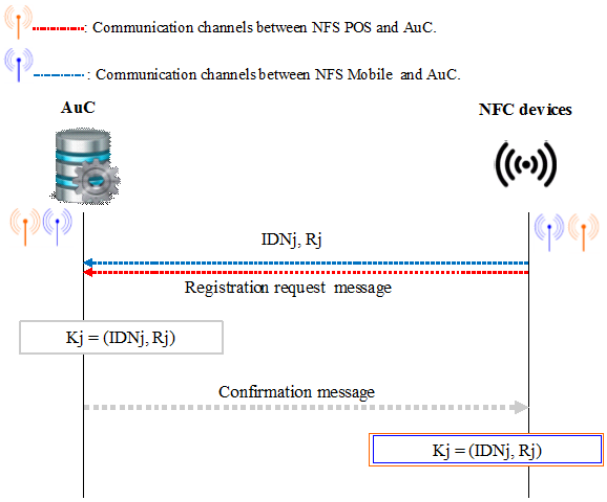


Figure 2. The registration phase in SAP-NFC protocol

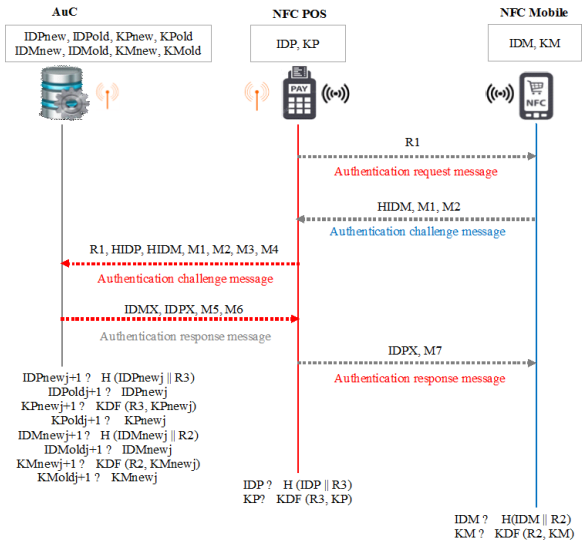


Figure 3. The authentication phase in SAP-NFC protocol

3.3 Authentication Phase

In order to execute the payment transaction successfully, mutual authentication must be achieved within the authentication phase between all the authentication parties. Initially, the NFC mobile contains the secret key (KM) with the mobile identity (IDM), while the NFC POS contains the secret key (KR) and POS identity (IDP). The AuC includes the current secret keys, the old secret keys, the old identities and the new identities of all NFC devices (KPold, KPnew, KMold, and KMnew). Figure 3 shows the authentication phase processes of the SAP-NFC protocol.

In the initial step in the authentication phase, the NFC POS generates the random number (R1), and the NFC mobile then receives the authentication request message from NFC POS that includes R1. The value of R1 is used by the NFC mobile

to compute the following authentication parameters to prepare the authentication challenge message: (1) generates the random number (R2); (2) executes the H (IDM || R1) function to compute the hash value (HIDM); (3) performs the H (KM || R1 || R2) function to compute the hash value (M1); (4) calculates the validation message (M2) as M2 = IDM ⊕ R2. After that, the NFC mobile transmits the authentication challenge message to the NFC POS that includes M1, M2, and HIDM.

In order to identify itself to the AuC, the NFC POS executes the following functions on the values of M1, M2, and HIDM that have been received through the authentication challenge message from the NFC mobile: (1) generates the random number (R3); (2) executes the H (IDP || R1) function to compute the hash value (HIDP); (3) performs the H (KP || R1 || R3) function to compute the hash value (M3); (4) calculates the validation message (M4) as M4 = IDP ⊕ R3. After that, the NFC POS sends the authentication challenge message to the AuC that includes M1, M2, M3, and M4 with HIDM, HIDP, and R1.

The AuC executes the following functions on the values of the authentication parameters to authenticate the NFC mobile: (1) using all values of IDMnew or IDMold, the AuC performs the H (IDMnew/IDMold || R1) function to compute the hash value (HIDM) that is equal to the hash value (HIDM) that has been received from the NFC POS; if HIDM is satisfied based on the IDMnew, the corresponding KMnew is retrieved and the flag value F1=1, else if IMD = IDMold, KMold is retrieved and F1=0, else the authentication session is terminated by the AuC; (2) computes R2 value where R2 = IDM ⊕ M2; (3) executes the XM1 = H (KMnew/KMnew || R1 || R2) function to compute the expected hash value XM1; if XM1 = M1 then the NFC mobile is verified, else the AuC terminates the session.

In the same manner, the AuC executes the following functions to authenticate the NFC POS: (4) using all values of IDPnew or IDPold, the AuC performs the H (IDPnew/IDPold || R1) function to compute the hash value (HIDP) that is equal to the hash value (HIDP) received from NFC POS; if HIDP is satisfied based on the IDPnew, the corresponding KPnew is retrieved and the flag value F2=1, else if the IDP = IDPold then KPold is retrieved and F2=0, else the authentication session is terminated by the AuC; (5) computes R3 value where R3 = IDP ⊕ M4; (6) executes the XM3 = (KMnew/KMnew || R1 || R3) function to compute expected hash value XM3; if XM3 = M3, the NFC POS is verified, else the AuC terminates the session.

The AuC executes the following functions to compute the authentication parameters of the authentication response message: (7) executes the H (R1 || R3 || IDP) function to compute the hash value (M5); (8) executes the E (IDM) KPold/KPnew function to compute IDMX; (9) executes the H (R1 || R2 || IDP) function to compute the hash value (M6); (10) executes the E (IDP) KMold/KMnew function to compute IDPX; (11) transmits the authentication parameters (M5, M6, IDPX, and IDMX) through the authentication response message to the NFC POS; (12) if F1 = 1, the AuC executes the following functions to update the identity and secret key of the NFC mobile: (a) IDMnewj+1←H (IDMnewj || R2); (b) IDMoldj+1← IDMnewj and KMnewj+1←KDF (KMj, R2); and (c) KMoldj+1 ← KMj; (13) if F2 = 1, the AuC executes the following functions to update the identity and secret key of the NFC POS: (a) IDPnewj+1←H (IDPj || R3); (b) IDPoldj+1←IDPj and KPnewj+1←KDF (KPj, R3); and (c) KPoldj+1←KPj, respectively.

On receiving the authentication parameters from the AuC (M5, M6, IDPX, and IDMX), the NFC POS performs the following functions: (1) executes the D (IDMX) KP function to compute the IDM value; (2) executes the H (R1 || R3 || IDM) function to compute the expected hash value (XM5) and to verify the AuC and NFC mobile according the following cases: (a) if XM5 is not equal to M5, the authentication session is terminated by the NFC POS; (b) if XM5 = M5, the NFC POS executes M7 = M6 ⊕ IDP to compute validation message (M7); (3) sends the M7 and IDPX through the authentication response message to the NFC mobile; (4) executes the IDP←H (IDP || R3) and KP←KDF (KP, R3) functions to renew the identity and the secret key of NFC POS, respectively.

Upon the M7 and IDPX, the NFC mobile executes the following functions: (1) executes the D (IDPX) KM function to compute IDP; (2) executes the H (R1 || R2 || IDP) ⊕ IDP function to verify the AuC and NFC POS according to the following cases: (a) if XM7 does not equal M7, the authentication session is terminated by the NFC mobile; (b) if XM7 equals M7, the NFC mobile executes the IDM←H (IDM || R2) and KM←KDF (KM, R2) functions to renew the identity and the secret key of the NFC mobile, respectively.

4. Performance Analysis

The performance analysis evaluates the impact of security features that have been accomplished in the SAP-NFC through the authentication phase.

The performance analysis in terms of authentication cost functions is conducted by comparing the SAP-NFC protocol with the two recent symmetric authentication protocols for NFC mobile payment applications that are described in section 2 [2, 3].

Table 2. Functions notation and cost

Notation	Description	Cost
G	Random number generation function	2 units
P	Encryption/decryption function	4 units
T	Timestamps functions	2 units
C	Concatenation function	1 unit
X	XOR operations	1 unit
H	Hash function	2 units
I	Condition function	1 unit
K	Key derivation function	2 units
M	MAC function	4 unit

Table 2 shows the basic functions of the authentication protocols and the number of units consumed by each operation. The predictable execution time of basic functions excluding the inner operation can be assumed for the various levels as follows [30]: (1) the encryption, decryption, and MAC functions consume 4 units; (2) random number

generation, key derivation, timestamps, and hash functions consume 2 units; (3) concatenation, exclusive, and verification functions consume 1 unit.

In order to conduct the performance analysis, the function vector (VF) of the symmetric authentication protocol is described as VF = [G, P, T, C, X, H, I, K, M], and the element weight of the VF is represented by how many times these functions are performed in the protocol multiplied by the cost in units for each authentication session. In this context, the element weight of each function is increased in the AuC according to the number of NFC mobiles and NFC POSs in the system; especially when the AuC retrieves the secret keys according to the identities of NFC devices from its database, the authentication parameters have the same size in all protocols. In contrast to the AuC, the NFC devices are considered poor resource platforms. Consequently, the cost of authentication operations is considered a strict indicator to evaluate the performance of the NFC mobile or NFC POS. Therefore, the costs of authentication operations are calculated for the NFC devices in this section.

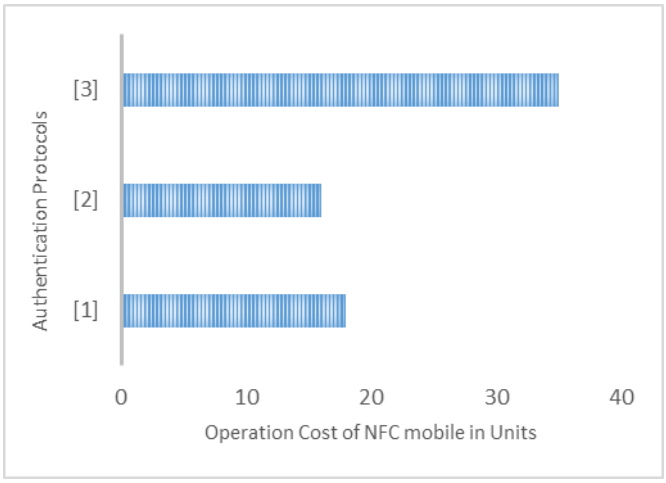
Table 3. Vectors of operations of NFC devices.

Protocols	VF (NFC Mobile)	VF (NFC POS)
[1]	[1, 1, 0, 5, 2, 3, 1, 0, 0]	[2, 1, 0, 5, 2, 3, 1, 0, 0]
[2]	[1, 0, 0, 5, 0, 0, 1, 0, 2]	[1, 0, 0, 6, 0, 0, 1, 0, 2]
[3]	[1, 2, 1, 0, 0, 0, 3, 2, 4]	[1, 1, 0, 0, 0, 0, 2, 1, 4]

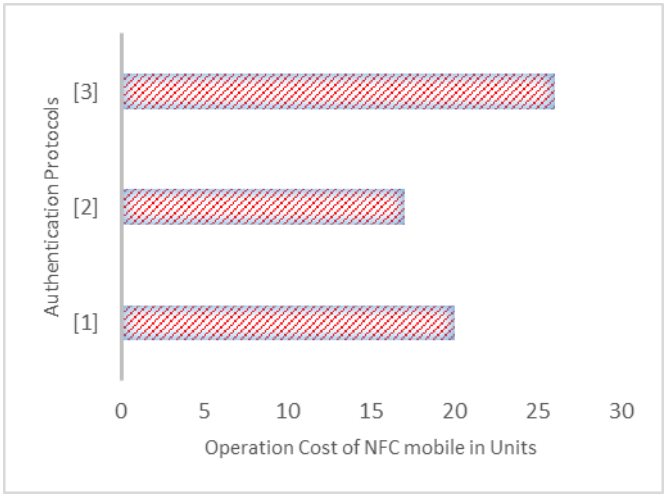
Table 4. Vector cost (VC) of NFC devices.

Protocols	VC (NFC Mobile)	VC (NFC POS)
[1]	[2, 4, 0, 5, 2, 4, 1, 0, 0]	[4, 4, 0, 5, 2, 4, 1, 0, 0]
[2]	[2, 0, 0, 5, 0, 0, 1, 0, 8]	[2, 0, 0, 6, 0, 0, 1, 0, 8]
[3]	[2, 8, 2, 0, 0, 0, 3, 4, 16]	[2, 4, 0, 0, 0, 0, 2, 2, 16]

For each authentication protocol, Table 3 shows that the maximum number of functions that are executed in each successful authentication session through the VFs of NFC devices. Table 4 illustrates the vector costs (VCs) of the NFC devices where the elements of each VC are equal to the operation cost multiplied by the element weight of the VF, as in Table 3.



(a) The VT of the NFC Mobile



(b) The VT of the NFC POS

Figure 4. The total vector cost of NFC devices

Consequently, the total vector cost (VT) is equal to the total element weight of VC for each NFC device. In particular, the VT (NFC mobile) and VT (NFC POS) represent the VT of the NFC mobile and VT of the NFC POS, respectively.

The comparisons in terms of VT among mobile payment protocols are shown in Figure 4 (a) and (b). According to the value of VT, the SAP-NFC protocol in both the NFC mobile and the NFC POS has medium values compared with other protocols.

5. Conclusions

This paper analyzes the performance of the secure authentication protocol for the NFC mobile payment (SAP-NFC) protocol. Compared with recent mobile payment protocols that use the symmetric cryptography method, the SAP-NFC protocol can achieve the highest level of security features, such as fully mutual authentication between authentication parties, forward/backward secrecy, anonymity, and untraceability. Moreover, the SAP-NFC protocol renews the identities of the authentication parties in all successful authentication sessions. Consequently, the SAP-NFC protocol can defeat existing attacks such as the replay attack, impersonation attack, tracking attack, and desynchronization attack. Moreover, the performance analysis in terms of operation costs of the authentication protocol illustrates that the SAP-NFC protocol satisfies the highest level of security with low cost in terms of the number of computations, both in the NFC mobile and the NFC POS, compared with other recent mobile payment protocols.

References

[1] S. Nashwan, "Secure Authentication Protocol for NFC Mobile Payment Systems," International Journal of Computer Science and Network Security, Vol. 17, No. 8, pp. 256-262, 2017.

[2] 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.

[3] Y. Tung and 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.

[4] M. Al-Zewairi, S. Hamdan, and M. Al-Fayoumi, "Enhanced Multi-Key Model for Risk Adaptive Hybrid RFID Access Control System," International Arab Conference on Information Technology (ACIT 2017), Yasmine Hammamet, Tunisia, 22-24 December, 2017.

[5] A. Alshehri and 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.

[6] A. Allyson, V. Lakshmi, and 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.

[7] A. Matos, D. Romao, and P. Trezentos, "Secure hotspot authentication through a near field communication side-channel," Proceedings of the IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, pp. 807-814, 2012.

[8] B. Seo, S. Lee, and 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.

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

[10] J. Ahn, S. Lee, and 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.

[11] 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.

[12] J. Ling, Y. Wang, and W. Chen, "An improved privacy protection security protocol based on NFC," International Journal of Network Security, Vol. 19, No. 1, pp. 39-46, 2017.

[13] M. Rahman and 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] M. Badra and 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.

[15] N. Shrangare and S. Joshi, "Secure protocol implementation using near field communication," International Research Journal of Engineering and Technology, Vol. 2, No. 3, pp. 589-593, 2015.

[16] N. El Madhoun, F. Guenane, and G. Pujolle, "An online security protocol for NFC payment: formally analyzed by the scyther tool," Proceedings of the IEEE 2nd International Conference on Mobile and Secure Services (MobiSecServ), FL, USA, pp. 1-7, 2016.

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

[18] N. El Madhoun, F. Guenane, and 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.

[19] N. Singh, A. Maity, and 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.

[20] O. Jensen, M. Gouda, and 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.

[21] P. Pourghomi, M. Saeed, and 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.

[22] R. Sivaranjani, R. Sujitha, D. Sindhu, and T. Tharani, "Secure and efficient authentication protocol using pseudonym," Journal of Chemical and Pharmaceutical Sciences, Special Issue 5, 2017.

[23] S. Nashwan and B. Alshammari, "Formal analysis of MCAP protocol against replay attack," British Journal of Mathematics & Computer Science, Vol. 22, No. 1, pp. 1-14, 2017.

[24] S. Nashwan and 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.

[25] S. Nashwan, "SAK-AKA: A secure anonymity key of authentication and key agreement protocol for LTE network," International Arab Journal of Information Technology, Vol. 14, No. 5, 2017.

[26] S. Yang and 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.

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

[28] S. Zaidi, M. Shah, M. Kamran, Q. Javaid, and 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.

[29] 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.

[30] S. Nashwan, "SE-H: Secure and Efficient Hash Protocol for RFID System," International Journal of Communication Networks and Information Security, Vol. 9, No. 3, pp. 358-365, 2017.

[31] U. Ceipidor, C. Medaglia, S. Sposato, and A. Moroni, "KerNeeS: A protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions," Proceedings of the 9th International ISC Conference on Information Security and Cryptology, pp. 115-120, 2012.

[32] Y. Lee, E. Kim and M. Jung, "A NFC based authentication method for defense of the Man in the Middle attack," Proceedings of 3rd International Conference on Computer Science and Information Technology, pp. 10-14, 2013.