Hindawi
Mobile Information Systems
Volume 2017, Article ID 2349149, 7 pages
https://doi.org/10.1155/2017/2349149

Research Article

ULMAP: Ultralightweight NFC Mutual Authentication Protocol with Pseudonyms in the Tag for IoT in 5G

Kai Fan,[1] Panfei Song,[1] and Yintang Yang[2]

[1] *State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, China*
[2] *Key Laboratory of Ministry of Education for Wide Band-Gap Semiconductor Materials and Devices, Xidian University, Xi'an, China*

Correspondence should be addressed to Kai Fan; kfan@mail.xidian.edu.cn

Received 24 January 2017; Revised 3 March 2017; Accepted 20 March 2017; Published 27 April 2017

Academic Editor: Jing Zhao

As one of the core techniques in 5G, the Internet of Things (IoT) is increasingly attracting people's attention. Meanwhile, as an important part of IoT, the Near Field Communication (NFC) is widely used on mobile devices and makes it possible to take advantage of NFC system to complete mobile payment and merchandise information reading. But with the development of NFC, its problems are increasingly exposed, especially the security and privacy of authentication. Many NFC authentication protocols have been proposed for that, some of them only improve the function and performance without considering the security and privacy, and most of the protocols are heavyweight. In order to overcome these problems, this paper proposes an ultralightweight mutual authentication protocol, named ULMAP. ULMAP only uses Bit and XOR operations to complete the mutual authentication and prevent the denial of service (DoS) attack. In addition, it uses subkey and subindex number into its key update process to achieve the forward security. The most important thing is that the computation and storage overhead of ULMAP are few. Compared with some traditional schemes, our scheme is lightweight, economical, practical, and easy to protect against synchronization attack.

1. Introduction

IoT [1] is a large network that consists of various information sensing devices and the Internet. As a new technology, the NFC [2, 3] is one of the core technologies of IoT and is listed as one of the most promising technologies.

NFC is a short-range, high-frequency, noncontact automatic identification wireless communication technology using the 13.56 MHz frequency band at a distance of less than 10 cm. It is a development and breakthrough of the RFID [4–6] technology. NFC now has been widely used in electronic ticket, product security, and other fields. But the security issues, especially the authentication problem between the reader and the tag, have become an important factor restricting its development. The problem of authentication is to confirm the validity of the tag and the reader. Since NFC communication is completely exposed to the wireless environment, it faces a lot of malicious attacks such as clone attack [7, 8], man-in-the-middle attack, and packet losses attack. Once the authentication protocol is under the above attack, the authentication will be failed. Meanwhile, because the NFC system is limited by many factors, such as computing power, storage space, and power supply, it is a challenging task to design a secure and efficient NFC authentication protocol.

So far, although a lot of security authentication schemes for NFC are presented, researchers at home and abroad do not put forward a universal applicability scheme. For example, Yun-Seok et al. [3] proposed a scheme that uses the asymmetric encryption and hash function to try to eliminate the security and privacy thread. Although the solution can solve the problem of mutual authentication and prevent replay attack and the man-in-the-middle attack, it lacks some necessary security attributes, such as the message authentication. In 2013, Eun et al. [9] presented a new conditional privacy preserving security protocol to protect the user's privacy. In 2015, Kannadhasan et al. [10] proposed the similar approach as presented in CPPNFC. In the same year, He et al. [11] proposed a pseudonym-based NFC protocol, but it cannot solve the forward security. In order to better promote the NFC technology, a scheme is needed to be proposed to solve the security and privacy thread.

Therefore, in this paper, we propose an ultralightweight mutual authentication protocol (ULMAP). Compared with the old NFC scheme, this protocol not only solves the security and privacy problem but also reduces the computation and storage cost.

Our Contributions. In this paper, we propose an ultralightweight mutual authentication protocol (ULMAP) for NFC using less memory storage and computational power for low-cost NFC tags. Our scheme has the following features:

(1) Ultralightweight: the scheme is designed only with simple shift and XOR operations, not hash or other encryption operations.

(2) Secure and efficient: the scheme we proposed could meet requirements of forward security, mutual authentication, synchronization, and non-denial of service by subkey and pseudonym.

Paper Organization. The remainder of the paper is organized as follows: In Section 2, we will present the detailed protocol of our new NFC mutual authentication protocol (ULMAP). In Section 3, the security proof with BAN logic of the proposed protocol will be provided. Section 4 provides the security and performance analysis of our protocol. Finally, our conclusion is shown in Section 5.

2. NFC Authentication Protocol for Mobile Device

In this section, we will propose ULMAP and basic ideas are as follows: the scheme only with a simple shift and XOR operations, greatly reducing the cost of operations. And it uses the concept of pseudonym, thus improving the system of security. And the scheme uses the concept of subkeys, preventing the man-in-the-middle attack as compared to the related existing authentication protocols.

2.1. Initialization. The explanations of symbols are shown in Abbreviation.

MixBits(X, Y) [12] is defined as follows:

```
$Z = \mathrm{MixBits}(X, Y)$
⋮
$Z = X;$
for $(i = 0; i < 32; i++)$
{
    $Z = (Z \gg 1) + Z + Z + Y;$
}
```

In this scheme, the message $(\mathrm{IDS}, \mathrm{ID}, K_1, K_2)$ is stored in each tag. Meanwhile, $(\mathrm{ID}, (\mathrm{IDS}_{\mathrm{old}}, K_{\mathrm{old}}^1, K_{\mathrm{old}}^2), (\mathrm{IDS}_{\mathrm{new}}, K_{\mathrm{new}}^1, K_{\mathrm{new}}^2))$ is stored in the server corresponding to each tag.

2.2. The Authentication Process. The authentication process of ULMAP is shown in Figure 1. The protocol involves three entities: tag, reader, and database. The channel between the reader and the database is assumed to be secure, but that between the reader and the tag faces all the possible potential attacks [13–15]. Each tag has a unique static identification (ID) and preshares a pseudonym (IDS) and two keys K_1, K_2 with the database.

Each database actually has two entries of $(\mathrm{ID}, (\mathrm{IDS}_{\mathrm{old}}, K_{\mathrm{old}}^1, K_{\mathrm{old}}^2), (\mathrm{IDS}_{\mathrm{new}}, K_{\mathrm{new}}^1, K_{\mathrm{new}}^2))$: one is for the old values and the other is for the potential next values. The reader first sends "Query" and T_R message to the tag. The tag will respond with its IDS after it verifies that the timestamp T_R is larger than T_t. Then, the reader will use the tag's response IDS to find a matched entry in the database and goes to the mutual authentication stage if a matched entry is found no matter what $\mathrm{IDS} = \mathrm{IDS}_{\mathrm{old}}$ or $\mathrm{IDS} = \mathrm{IDS}_{\mathrm{new}}$. In the mutual authentication phase, the reader and the tag authenticate each other, and they, respectively, update their local pseudonym and the keys after successful authentication, which are shown in Figure 1.

There are four stages in the scheme that we proposed, such as initialization, tag identification, mutual authentication, and index-pseudonym and key updating. Then, we will in detail introduce the four stages as follows.

Initialization. The database selects a pseudorandom generator PRNG [16] $g : \{0,1\}^k \rightarrow \{0,1\}^{2k}$ to generate pseudorandom number. The database generates the key $K = K_1 \mid K_2$, which is initialized to $K_1 = \mathrm{Rot}(\mathrm{Rot}(n_{i,2} + \mathrm{ID} + n_{i,3}, n_{i,2}) + \mathrm{ID}, n_{i,1}) + n_{i,3}$ and $K_2 = \mathrm{Rot}(\mathrm{Rot}(n_{i,1} + \mathrm{ID} + n_{i,3}, n_{i,1}) + \mathrm{ID}, n_{i,2}) \oplus n_{i,3}$, and places it in a valid tag and the legitimate reader. $n_{i,j}$ is the jth random number of the ith tag in the initialization phase, $j = 1, 2, 3$. The database, reader, and tag will store the IDS and $K = K_1 \mid K_2$ corresponding to the tag.

Tag Identification. The reader generates the random timestamp T_R and the random number n_2 and sends authentication queries n_2, Query, and T_R to the tag. Then, the tag judges whether $T_R > T_t$; if T_R is not larger than T_t, the authentication is failed. Otherwise, the mutual authentication phase will begin.

Mutual Authentication. After identification phase, the tag will generate a random number n_2, calculate A, B, and C as shown in Figure 1, and send IDS, A, B, and C to the reader. Using the IDS, the reader tries to find an identical entry in the database. If this search succeeds, the reader can get the nonce from submessages A and B. Then, the reader will compute n_3' and $\overline{K_1^*}/\overline{K_2^*}$ and build a local version of submessage C' as shown in Figure 1. It will be compared with the received value. If it is verified, the tag is authenticated. Finally, the reader sends message $D = (\overline{K} \oplus \mathrm{ID}) \oplus ((K_2 + K_1) \cup \overline{K_2^*})$ to the tag. When the message D is received by the tag, it will be compared with a computed local version $D' = (\overline{K}_1 \oplus \mathrm{ID}) \oplus ((K_2 + K_1) \cup \overline{K}_2)$. If comparison is successful, the reader is authenticated. Otherwise, the authentication protocol is failed.

Index-Pseudonym and Key Updating. After successfully completing the mutual authentication phase between the tag and

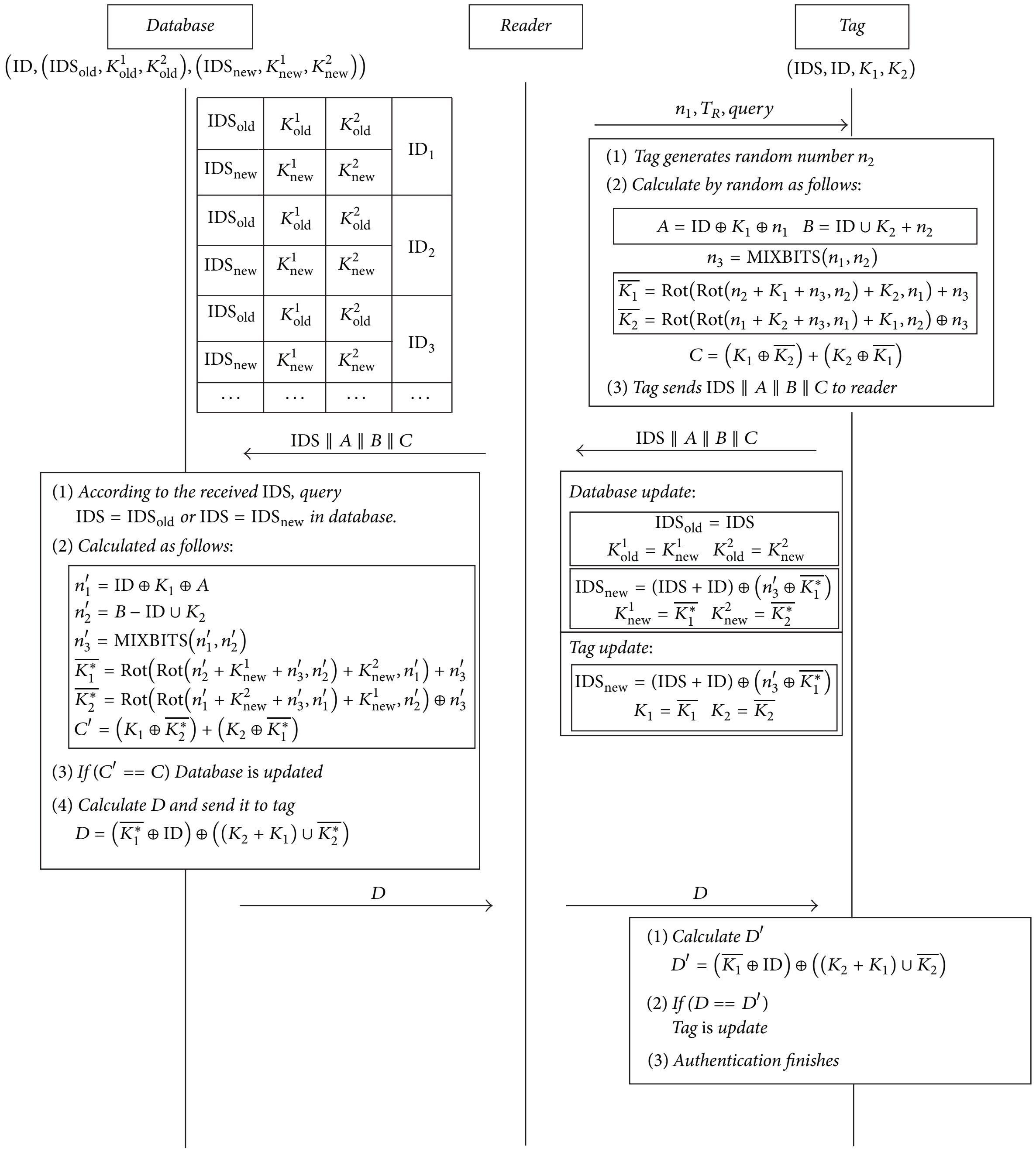

Database
Reader
Tag
$(\mathrm{ID}, (\mathrm{IDS_{old}}, K^1_{old}, K^2_{old}), (\mathrm{IDS_{new}}, K^1_{new}, K^2_{new}))$
$(\mathrm{IDS}, \mathrm{ID}, K_1, K_2)$
$\mathrm{IDS_{old}}$ K^1_{old} K^2_{old} ID_1
$\mathrm{IDS_{new}}$ K^1_{new} K^2_{new}
$\mathrm{IDS_{old}}$ K^1_{old} K^2_{old} ID_2
$\mathrm{IDS_{new}}$ K^1_{new} K^2_{new}
$\mathrm{IDS_{old}}$ K^1_{old} K^2_{old} ID_3
$\mathrm{IDS_{new}}$ K^1_{new} K^2_{new}
$\cdots$ $\cdots$ $\cdots$ $\cdots$
$n_1, T_R, query$
(1) Tag generates random number n_2
(2) Calculate by random as follows:
$A = \mathrm{ID} \oplus K_1 \oplus n_1 \quad B = \mathrm{ID} \cup K_2 + n_2$
$n_3 = \mathrm{MIXBITS}(n_1, n_2)$
$\overline{K_1} = \mathrm{Rot}(\mathrm{Rot}(n_2 + K_1 + n_3, n_2) + K_2, n_1) + n_3$
$\overline{K_2} = \mathrm{Rot}(\mathrm{Rot}(n_1 + K_2 + n_3, n_1) + K_1, n_2) \oplus n_3$
$C = (K_1 \oplus \overline{K_2}) + (K_2 \oplus \overline{K_1})$
(3) Tag sends IDS $\|$ A $\|$ B $\|$ C to reader
IDS $\|$ A $\|$ B $\|$ C
IDS $\|$ A $\|$ B $\|$ C
(1) According to the received IDS, query
IDS = $\mathrm{IDS_{old}}$ or IDS = $\mathrm{IDS_{new}}$ in database.
(2) Calculated as follows:
$n'_1 = \mathrm{ID} \oplus K_1 \oplus A$
$n'_2 = B - \mathrm{ID} \cup K_2$
$n'_3 = \mathrm{MIXBITS}(n'_1, n'_2)$
$\overline{K^*_1} = \mathrm{Rot}(\mathrm{Rot}(n'_2 + K^1_{new} + n'_3, n'_2) + K^2_{new}, n'_1) + n'_3$
$\overline{K^*_2} = \mathrm{Rot}(\mathrm{Rot}(n'_1 + K^2_{new} + n'_3, n'_1) + K^1_{new}, n'_2) \oplus n'_3$
$C' = (K_1 \oplus \overline{K^*_2}) + (K_2 \oplus \overline{K^*_1})$
(3) If (C' == C) Database is updated
(4) Calculate D and send it to tag
$D = (\overline{K^*_1} \oplus \mathrm{ID}) \oplus ((K_2 + K_1) \cup \overline{K^*_2})$
Database update:
$\mathrm{IDS_{old}} = \mathrm{IDS}$
$K^1_{old} = K^1_{new} \quad K^2_{old} = K^2_{new}$
$\mathrm{IDS_{new}} = (\mathrm{IDS} + \mathrm{ID}) \oplus (n'_3 \oplus \overline{K^*_1})$
$K^1_{new} = \overline{K^*_1} \quad K^2_{new} = \overline{K^*_2}$
Tag update:
$\mathrm{IDS_{new}} = (\mathrm{IDS} + \mathrm{ID}) \oplus (n'_3 \oplus \overline{K^*_1})$
$K_1 = \overline{K_1} \quad K_2 = \overline{K_2}$
D
D
(1) Calculate D'
$D' = (\overline{K_1} \oplus \mathrm{ID}) \oplus ((K_2 + K_1) \cup \overline{K_2})$
(2) If (D == D')
Tag is update
(3) Authentication finishes

Figure 1: Authentication process of ULMAP.

the reader, they locally update IDS and key as indicated in Figure 1.

3. Security Proof with BAN Logic

The security assurance of the proposed protocol is the secure mutual authentication, which means the following security aims should be achieved.

Security Aim 1. The database needs to make sure the received message IDS $\|$ A $\|$ B $\|$ C is exactly the one sent by the tag. This means that we need to achieve Database|≡ Tag|~ (IDS, A, B, C) and Database|≡ Tag|≡ (IDS, A, B, C).

Security Aim 2. The tag needs to make sure the received message D is exactly the one sent by the database, which means the following formulas need to be achieved: Tag|≡ Database|~ D and Tag|≡ Database|≡ D.

3.1. Security Assumption. According to the given protocol and the assumption that the server and the reader are connected securely, the following conditions can be achieved:

AS1: $\text{Database}|\equiv \text{Database} \overset{n_{i,j}}{\rightleftarrows} \text{Tag}_i$.

AS2: $\text{Tag}_i|\equiv \text{Database} \overset{n_{i,j}}{\rightleftarrows} \text{Tag}_i$.

AS3: $\text{Reader} \Longrightarrow (n_1)$.

AS4: $\text{Reader}|\equiv \#(n_1)$.

AS5: $\text{Database}|\equiv \#(n_1)$.

AS6: $\text{Tag}_i \Longrightarrow (n_2)$.

AS7: $\text{Tag}_i|\equiv \#(n_2)$.

3.2. Security Analysis. According to the proposed protocol (ULMAP) $K_1 = \text{Rot}(\text{Rot}(n_{i,2} + \text{ID} + n_{i,3}, n_{i,2}) + \text{ID}, n_{i,1}) + n_{i,3}$ and $K_2 = \text{Rot}(\text{Rot}(n_{i,1} + \text{ID} + n_{i,3}, n_{i,1}) + \text{ID}, n_{i,2}) \oplus n_{i,3}$, together with the assumptions AS1 and AS2, we can deduce $\text{Tag}_i| \equiv \text{Database} \overset{K_{i,j}}{\rightleftarrows} \text{Tag}_i$ and $\text{Database}| \equiv \text{Database} \overset{K_{i,j}}{\rightleftarrows} \text{Tag}_i$, because, in this scheme, the database will receive the message (IDS, A, B, C) forwarded from the reader, where $C = (K_1 \oplus \overline{K_2}) + (K_2 \oplus \overline{K_1})$. As we have achieved $K_{i,j}$ as secret between the database and the tag, we can take $K_{i,j}$ as the secret key to protect messages. So we can simply write the received message of database as $(\text{IDS}, A, B, C)_{K_{i,j}}$, and we have $\text{Database} \triangleleft (\text{IDS}, A, B, C)_{K_{i,j}}$. For the reason of "message-meaning rule" of BAN $(P|\equiv Q \overset{Y}{\parallel} P, P \triangleleft \langle X\rangle_Y)/(P|\equiv (Q|\sim X))$, we can deduce $\text{Database}|\equiv \text{Tag}_i|\sim (\text{IDS}, A, B, C)$.

From the assumption $\text{AS5}: \text{Server}|\equiv \#(n_1)$ and the BAN rule of $(P|\equiv \#(X))/(P|\equiv \#(X, Y))$, we know $\text{Database}|\equiv \#(\text{IDS}, A, B, C)$. Because we have achieved $\text{Database}|\equiv \text{Tag}_i|\sim \#(\text{IDS}, A, B, C)$, together with the "nonce-verification" rule $(P|\equiv (\#(X)), P|\equiv (Q|\sim X))/(P|\equiv (Q|\equiv X))$, we will achieve $\text{Database}|\equiv \text{Tag}_i|\equiv (\text{IDS}, A, B, C)$, and the first security aim of the given protocol is achieved.

For the same reason, we can also deduce $\text{Tag}_i|\equiv \text{Database}|\sim D$ and $\text{Tag}_i|\equiv \text{Database}|\equiv D$, and the second security aim is also achieved, and the security of mutual authentication of the proposed protocol has been proved.

4. Evaluation

In this section, we will analyze the proposed protocol (ULMAP) from the security and performance point of view.

4.1. Security Analysis. It is obvious, from the protocol specification, that not only can the tag and the reader successfully authenticate each other, but also ULMAP is able to resist the common NFC attacks effectively. In particular, it makes the scheme have the anti-DoS attack capability through using the timestamp. We now analyze our proposed scheme from the point of view of security as follows.

4.1.1. Mutual Authentication. The tag and the reader can authenticate each other by messages C and D, because only the genuine tag has the subkeys K_1 and K_2 which generate the consistent message C with random numbers n_1, n_2. Similarly, only the genuine reader keeps the ID that is used to generate the response message D. In this way, the reader and the tag can achieve mutual authentication.

4.1.2. Tag Anonymity. The tag uses the pseudonym in the whole authentication process. The pseudonym of each tag will be updated after every successful authentication by the random numbers n_1, n_2. So the pseudonym from the same tag looks different at each session authentication and the attackers cannot get the real identity of the tag. Moreover, even if the attackers intercept authentication pseudonym IDS, they cannot analyze the practical information from it.

4.1.3. Resistance to Tracking. The data stored in the database and the tag will be updated after the successful authentication process. So the message and the response message are different at each session authentication, making it almost impossible for the attackers to track the tag. In addition, the tag uses the pseudonym which improves the difficulty of tracking.

4.1.4. Data Confidentiality [17]. The calculation of each value of A, B, C, and D involves at least two secret values, including the subkey and random number. So, it is very hard to get the tag ID except for the tag itself that has K_1, K_2 and n_1, n_2.

4.1.5. Forward Security. After each successful session, the key and IDS value will be updated in the tag and the database. So even if the attacker achieves some session information, he cannot use it to trace back to previous communications. In addition, ULMAP makes the subkey and random number involved in the entire update process, which makes the entire update process have stronger stochastic properties. So ULMAP is forward security.

4.1.6. Nonreplaying. Because the value of IDS will be updated after the successful authentication process, the response message $\text{IDS} \parallel A \parallel B \parallel C$ from the same tag is different in each session authentication process. Moreover, the timestamp T_R is constantly changing over time. Therefore, the attacker cannot priorly disguise information to achieve legality certification.

4.1.7. Non-Denial of Service (Non-DoS) [18]. When the reader starts a new session, the tag will judge whether $T_R > T_t$. If not, the authentication is failed. Otherwise, the authentication process will continue. Compared with all most schemes responding to the query, ULMAP can reduce the number of denial of service attacks to some extent and prevent unauthorized readers from continuing to send queries which consume lots of resources of the tag. Therefore, this scheme can resist denial of service attacks in some cases.

The comparison between LMAP [19], SASI [20], and ULMAP in security is shown in Table 1. "√" means satisfaction, "×" means to dissatisfy, and "#" means satisfaction to a certain extend.

It is very obvious, in Table 1, that neither of SASI and LMAP can resist desynchronization and DoS attacks. However, in addition to the forward security, data confidentiality,

Table 1: The security and functionality comparison.

Scheme	Mutual authentication and forward security	Confidentiality and anonymity	Resistance to tracking	Nonreplaying	Resistance to desynchronization attack	Non-DoS
LMAP	×	×	×	×	×	×
SASI	√	√	√	√	×	×
ULMAP	√	√	√	√	√	#

Table 2: The storage overhead comparison.

Scheme	Database	Reader	Tag
LMAP	$6ml$	0	$6L$
SASI	$4ml$	0	$7L$
ULMAP	$7ml$	0	$5L$

Table 3: The cost of communication comparison.

Scheme	The number of interactions	Total cost of communication
LMAP	4	$5L$
SASI	4	$5L$
ULMAP	3	$7L$

Table 4: Computation cost comparison.

Scheme	LMAP	SASI	ULMAP
Cost	$\oplus, +, \wedge, \vee$	$\oplus, +, \wedge, \vee$, Rot	$\oplus, +, \wedge, \vee$ Rot^2, MixBits

nonreplaying, and so forth, the proposed protocol ULMAP can prevent synchronicity attacks effectively and prevent DoS attacks to some extent. In summary, ULMAP improves the security.

4.1.8. Synchronization. In a normal session, if the tracker heads off the last message that the database sends to the tag, the database cannot be successfully verified. Once this case happens, the tag cannot be updated, but the database has been updated successfully. So the tag and the database will lose the synchronization. However, in the ULMAP protocol, the IDS, K_1, K_2, used in the last session is stored in $(\text{ID}, (\text{IDS}_{\text{old}}, K^1_{\text{old}}, K^2_{\text{old}}), (\text{IDS}_{\text{new}}, K^1_{\text{new}}, K^2_{\text{new}}))$ in the database, so that this tag is still able to finish the authentication and get the synchronization again successfully.

4.2. Performance and Complexity Analysis. We will compare ULMAP with SASI and LMAP in performance and complexity. In order to compare easily, assume there are m tags in the system and the length of data is L.

4.2.1. The Cost of Storage. To achieve the authentication, in SASI protocol, the tag stores the message $(\text{ID}, (\text{IDS}_{\text{new}}, K_{1\text{new}}, K_{2\text{new}})(\text{IDS}_{\text{old}}, K_{1\text{old}}, K_{2\text{old}}))$ and $(\text{ID}, \text{IDS}, K_1, K_2)$ is stored in the database, so the cost of storage in the tag and database is $7L$ and $4mL$, respectively. As it is shown in Table 2, in LMAP, the tag storage space needs $6L$ and the corresponding database storage space requires $6mL$. But in our protocol, the cost of storage space in the tag is $5L$ and the cost of storage space in the database is $7mL$.

Usually, the database has more resources than the tag, so the resource of tag is more valuable. Comparing with other protocols, the ULMAP needs smaller storage space in the tag that will greatly reduce the cost of the tag and increase a little cost of storage space in the database. Therefore, the proposed protocol can greatly reduce input cost. The specific storage overhead is shown in Table 2.

4.2.2. The Cost of Communication. The cost of communication consists of the number of interactions and the length of the communication data. From Table 3, we can know that the interaction times of both SASI and LMAP are 4. Although the transmitted data is increased a little, our protocol is just transmitted three times between the reader and the tag, which are four times in other protocols. Therefore, ULMAP has a relatively low communication overhead.

Comparing with other protocols, the ULMAP uses the timestamp for the first time. This will make the ULMAP resist the attack of DoS to a certain extent. Moreover, the subkey and random numbers are used widely in the database and the tag in the authentication update phase. This can make the whole protocol have stronger random feature which will greatly improve the ability of resisting desynchronization and the forward security of ULMAP.

4.2.3. The Cost of Computation Time. In order to better compare the computation performance of different protocols in Table 4, + represents AND operation, $\oplus$ represents the XOR operation, Rot is the displacement $\text{Rot}(x, y)$ operation, Rot^2 is two displacement $\text{Rot}(x, y)$ operations, and T represents the pseudorandom number or timestamp.

From Table 4, it is shown that the tag in ULMAP needs one random number generation. In addition, ULMAP also needs more computation operation (like Rot, MixBits) in the tag compared with SASI and Gossamer. Although this will increase the cost of computation, the computations also become more secure and effective with it.

By comparing our protocol with other schemes, it shows that our proposed protocol not only can provide mutual authentication function but also has the advantage of higher level of security and performance.

5. Conclusions

This paper proposes a new NFC mutual authentication protocol, named ULMAP. ULMAP can achieve not only mutual authentication but also complete anonymity. Moreover, the proposed scheme possesses higher security and performance. Because the database stores the new and old session private key and IDS, when the new session private key of the tag fails to update, the corresponding old private key and IDS can also be used. So the proposed protocol can effectively resist the desynchronization attack.

Abbreviations

IDS:	The pseudonym of tag identity
IDS_{old}:	The index number used last time
IDS_{new}:	The index number successfully used this time
ID:	The unique static identification of tag
K:	The shared key of the tag and database, which is divided into two parts
T_R:	The random timestamp generated by the reader
T_t:	The last time timestamp
K_{old}:	The key of the tag successfully used in the last round session
K_{new}:	The key of the tag used in this session
n_1, n_2:	The random number generated by the tag and the reader
$\text{Rot}(x, y)$:	The operation of rotation $x \ll W(y)$, where $W(y)$ denotes Hamming weight of y.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work has been financially supported by the National Natural Science Foundation of China (nos. 61303216, 61272457, U1401251, and 61373172), the National High Technology Research and Development Program of China (863 Program) (no. 2012AA013102), the Open Research Project of the State Key Laboratory of Industrial Control Technology, Zhejiang University, China (no. ICT170312), and National 111 Program of China (nos. B16037 and B08038).

References

[1] H. Ning and B. Wang, *RFID Major Projects and the State Internet of Things*, Mechanical Industry Press, Beijing, China, 2008.

[2] V. Odelu, A. K. Das, and A. Goswami, "SEAP: secure and efficient authentication protocol for NFC applications using pseudonyms," *IEEE Transactions on Consumer Electronics*, vol. 62, no. 1, pp. 30–38, 2016.

[3] L. Yun-Seok, K. Eun, and J. Min-Soo, "A NFC based authentication method for defense of the man in the middle attack," in *Proceedings of the 3rd International Conference on Computer Science and Information Technology*, Bali, Indonesia, January 2013.

[4] K. Fan, J. Li, H. Li, X. Liang, X. Shen, and Y. Yang, "RSEL: revocable secure efficient lightweight RFID authentication scheme," *Concurrency Computation Practice and Experience*, vol. 26, no. 5, pp. 1084–1096, 2014.

[5] E. Haselsteiner, "Security in near field communication (NFC)," in *Proceedings of the Workshop on RFID Security*, Malaga, Hungary, 2006.

[6] K. Fan, Y. Gong, C. Liang, H. Li, and Y. Yang, "Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G," *Security and Communication Networks*, vol. 9, pp. 3095–3104, 2016.

[7] M. Dong, K. Ota, L. T. Yang, A. Liu, and M. Guo, "LSCD: a low-storage clone detection protocol for cyber-physical systems," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 5, pp. 712–723, 2016.

[8] L. Zhang, L. Wei, D. Huang, K. Zhang, M. Dong, and K. Ota, "MEDAPs: secure multi-entities delegated authentication protocols for mobile cloud computing," *Security and Communication Networks*, vol. 9, no. 16, pp. 3777–3789, 2016.

[9] J. C. Paillès, C. Gaber, V. Alimi, and M. Pasquet, "Payment and privacy: a key for the development of NFC mobile," in *Proceedings of the International Symposium on Collaborative Technologies and Systems (CTS '10)*, pp. 378–385, May 2010.

[10] M. Hassinen, K. Hyppönen, and E. Trichina, "Utilizing national public-key infrastructure in mobile payment systems," *Electronic Commerce Research and Applications*, vol. 7, no. 2, pp. 214–231, 2008.

[11] Z. Kabir, *User centric design of an NFC mobile wallet framework [M.S. thesis]*, The Royal Institute of Technology (KTH), Stockholm, Sweden, 2011.

[12] E. G. Ahmed, E. Shaaban, and M. Hashem, "Lightweight mutual authentication protocol for low cost RFID tags," *International journal of Network Security & Its Applications*, vol. 2, no. 2, pp. 27–37, 2010.

[13] A. Juels, "Strengthening EPC tags against cloning," in *Proceedings of the ACM Workshop on Wireless Security (WiSe '05)*, pp. 67–75, Cologne, Germany, September 2005.

[14] C. Mulliner, "Vulnerability analysis and attacks on NFC-enabled mobile phones," in *Proceedings of the 4th International Conference on Availability, Reliability and Security*, pp. 695–700, IEEE, Fukuoka, Japan, March 2009.

[15] L. Francis, G. P. Hancke, K. Mayes et al., "Practical NFC peer-to-peer relay attack using mobile phones," in *Proceedings of the 6th International Workshop on Radio Frequency Identification: Security and Privacy Issues (RFID-SEC '10)*, pp. 35–49, Istanbul, Turkey, 2010.

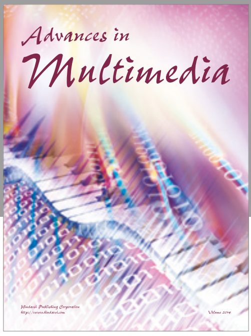
[16] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "LAMED—a PRNG for EPC class-1 generation-2 RFID specification," *Computer Standards and Interfaces*, vol. 31, no. 1, pp. 88–97, 2009.

[17] L. Gu, L. Wang, K. Ota, M. Dong, Z. Cao, and Y. Yang, "New public key cryptosystems based on non-Abelian factorization problems," *Security and Communication Networks*, vol. 6, no. 7, pp. 912–922, 2013.

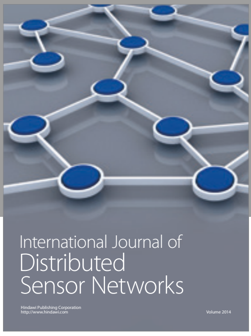
[18] F. Fahrianto, M. F. Lubis, and A. Fiade, "Denial-of-service attack possibilities on NFC technology," in *Proceedings of the 4th International Conference on Cyber and IT Service Management*, pp. 1–5, IEEE, April 2016.

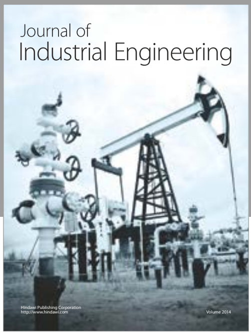
[19] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. E. Tapiador et al., “LMAP: a real lightweight mutual authentication protocol for low-cost RFID tags,” in *Proceedings of the Workshop on RFID Security*, Graz, Austria, July 2006.

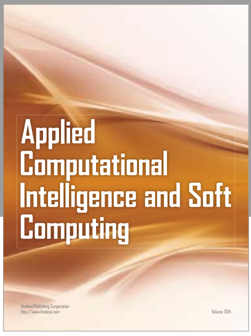
[20] H.-Y. Chien, “SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity,” *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 4, pp. 337–340, 2007.

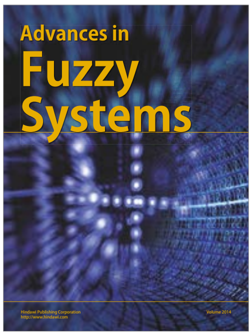

Advances in
Multimedia

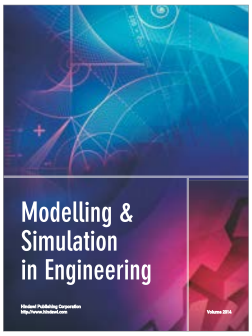
The Scientific
World Journal

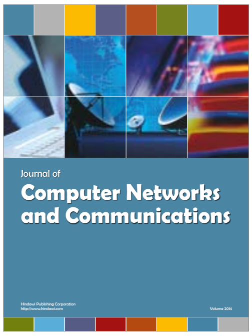

International Journal of
Distributed
Sensor Networks


Journal of
Industrial Engineering

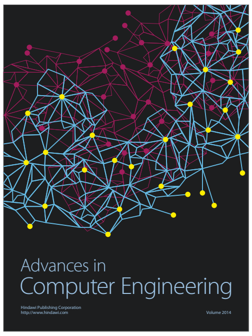

Applied
Computational
Intelligence and Soft
Computing


Advances in
Fuzzy
Systems

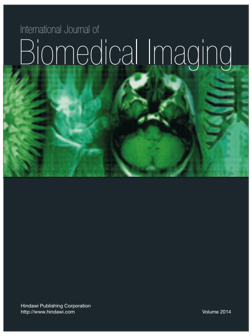

Modelling &
Simulation
in Engineering

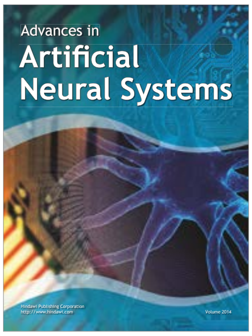

Journal of
Computer Networks
and Communications

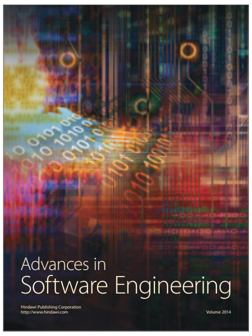
Advances in
Artificial
Intelligence


Advances in
Computer Engineering

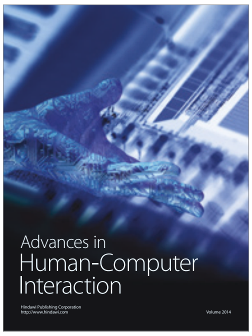
International Journal of
Computer Games
Technology

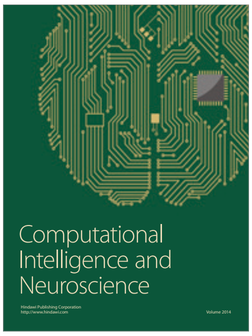

International Journal of
Biomedical Imaging


Advances in
Artificial
Neural Systems


Advances in
Software Engineering

Journal of
Robotics


Advances in
Human-Computer
Interaction


Computational
Intelligence and
Neuroscience

International Journal of
Reconfigurable
Computing

Journal of
Electrical and Computer
Engineering