The Journal of Supercomputing (2022) 78:10893–10905
https://doi.org/10.1007/s11227-021-04252-y

URAP: a new ultra-lightweight RFID authentication protocol in passive RFID system

Ming Gao[1] · YuBin Lu[1]

Accepted: 16 December 2021 / Published online: 1 February 2022

Abstract
RFID (Radio Frequency Identification) is a crucial application technology in the Internet of Things (IoT) technology. The IoT terminal device needs to be authenticated before accessing the IoT network in order to avoid security holes. Due to the limited resources of the tag side in passive RFID systems, ultra-lightweight RFID authentication protocols are often used in such systems. Based on the characteristics of the ultra-lightweight authentication protocol, we propose a safe and efficient mutual authentication protocol which uses only bitwise operation including XOR and circular left-rotation operation. Cryptanalysis shows that the proposed protocol can prevent many known attacks and has better security performance than some existing ultra-lightweight protocols. In addition, performance evaluation shows that the proposed protocol performs better than the existing ultra-lightweight protocols in terms of computational cost, storage requirement and communication cost.

Keywords IoT · RFID tags · Ultra-lightweight · Mutual authentication

1 Introduction

RFID is a technology that uses radio frequency signals for automatic identification in an open environment. Because RFID tags have the advantages of low manufacturing cost and small size, they are widely used in practice. RFID tags are roughly divided into two categories: passive RFID tags and active RFID tags. The active RFID tag is equipped with a battery, and its service life is affected by the battery. It needs to be replaced regularly, and cannot work normally at high or low temperatures. The

✉ Ming Gao
mgao@mail.xidian.edu.cn

YuBin Lu
luyubinll@163.com

[1] Department of Communication Engineering, Xidian University, 2 South Taibai Road,
Xi'an 710071, Shaanxi, China

passive RFID tags have no batteries. The working principle is: the reader transmits a certain frequency radio frequency signal through the transmitting antenna; when the tag enters the working area of the transmitting antenna, an induced current is generated; and the energy is obtained through the current for transmitting the signal from the RFID. Compared with active RFID tags, passive tags have the advantages of maintenance-free, lower cost, longer service life, and can work normally at high temperatures. Therefore, the passive RFID system can be applied in a much wider scope.

The wireless communication method in the RFID system makes the RFID system face many security threats [1–3], such as channel eavesdropping, tag or reader forgery, tag tracking, replaying information, information tampering, and desynchronization attacks. In the RFID system, the security of information is ensured by verifying the legality of the identity of the tag and the reader. Passive RFID tags have limited computing and storage capabilities and cannot support conventional cryptographic functions such as symmetric encryption; therefore they usually use lightweight RFID authentication protocols or ultra-lightweight authentication protocols. The lightweight protocols require a random number generator and simple functions such as Cyclic Redundancy Code (CRC) checksum but not hash function. The ultra-lightweight protocols only involve simple bitwise operations (e.g., XOR, AND, OR, etc.) on tags.

Early popular RFID ultra-lightweight security protocols include MMAP (Minimalist Mutual Authentication Protocol) [4], LMAP (Lightweight Mutual Authentication Protocol) [5] and EMAP (Efficient Mutual Authentication Protocol) [6]. The common point of these three protocols is that they no longer use traditional algorithms such as hash functions and block ciphers, but use bitwise operations which offers an adequate security level for certain applications and can be implemented even in the most limited low-cost RFID tags. Since then, a large number of ultra-lightweight protocols for RFID have been proposed to improve the security of the protocol, such as SASI [7] which can provides strong authentication and strong integrity of the transmissions, RAPP [8] which proposed an ultra-lightweight authentication protocol with permutation operation, etc. For these protocols, many scholars have analyzed their security. For example, Li et al. analyzed the security of the protocol [4–6] and proposed corresponding attacks [9, 10]. Qurat et al. give the desynchronization attack and full disclosure attack on SASI and RAPP [11]. In 2017, Tewari and Gupta proposed a new ultra-lightweight authentication protocol [12], which is denoted by TGAP (Tewari and Gupta Authentication Protocol) in this paper. TGAP mainly utilizes two bit-operations, XOR and rotate operation. Compared with other protocols, TGAP further reduces the computational cost of tags and thus gains widespread attention. Many researchers have studied and analyzed TGAP. Wang et al. gave a full disclosure attack on the protocol and modified it to prevent this attack [13]. But Jing et al. pointed out that the modified protocol of Wang and TGAP are susceptible to full disclosure, man-in-the-middle, and desynchronization attacks [14]. Madiha et al. devised another desynchronization attack after analyzing TGAP [15], and Huang et al. designed a full disclosure attack on TGAP [16]. Therefore, the TGAP still have some significant security issues.

According to the characteristics of the low-cost passive RFID system, we propose a safe and efficient ultra-lightweight RFID mutual authentication protocol. The protocol uses only bitwise operations and is superior to existing ultra-lightweight protocols in terms of computational cost and communication overhead. Moreover, the protocol can effectively prevent typical attacks, such as replay attacks, desynchronization attacks and man-in-the-middle attacks, etc., so it has good security performance.

The remainder of the paper is organized as follows: Sect. 2 introduces an ultra-lightweight RFID authentication protocol (URAP), which is followed by the security analysis in Sect. 3. Sect. 4 use GNY logical protocol proof methods to verify the URAP protocol. Sect. 5 further analyzes the performance of the proposed protocol from the aspects of computational cost, storage requirement and communication cost. Finally, Sect. 6 states our conclusions.

2 URAP: a new ultra-lightweight RFID authentication protocol

In this section, we will introduce the newly proposed ultra-lightweight authentication protocol. RFID systems consist of back-end servers, readers, and various tags. Usually, an assumption was made that the channel between reader and a backend server is secure, whereas the channel between the reader and the tag is insecure. In URAP, the backend server and each tag have a static identification (ID).Each tag preshares a pseudonym (IDS) and a key K with the backend server. After a successful authentication, K and IDS will be updated. In addition, the backend server will also store the old values of IDS and K used in the previous round of agreements IDS_{old}, K_{old}. The reader can get the values of IDS, IDS_{old}, K and K_{old} from the back-end server. The typical length value of IDS and K is 96 bits. Table 1 lists notations that are used in URAP:

The steps of our proposed protocol are given below: Step 1. The reader uses a PRNG to generate a random number R1 and sends R1|| ″Query″ to the tag to initiate a protocol session.

Table 1 Notations and description

Symbol	Description
wt(Y)	Hamming weight of Y
Rot(A,B)	Circular left-rotation operation A shifted in wt(B)
$\oplus$	Exclusive OR operation
IDS_{new}	Tag's new pseudonym
IDS_{old}	Tag's old pseudonym
K_{new}	New secret key
K_{old}	Old secret key
PRNG	pseudo-random number generator

Step 2, Upon receiving the reader's query, the tag will use R1, K and IDS to compute the messages A, B and transmit messages A||B to the reader.

$$A = \text{Rot}[IDS \oplus R1,K] \oplus K$$
$$B = \text{Rot}[R1,K] \oplus \text{Rot}[IDS,K] \oplus K$$

Step 3: After receiving A||B, the reader uses the IDS_{new}, IDS_{old}, K_{new}, K_{old} to compute the verification messages A_{new}, A_{old}:

$$A_{new} = \text{Rot}[IDS_{new} \oplus K_{new}, R1] \oplus K_{new}$$
$$A_{old} = \text{Rot}[IDS_{old} \oplus K_{old}, R1] \oplus K_{old}$$

Two cases arise while matching the values sent by the tag:

Case I:

A sent by the tag matches the corresponding A_{new} stored in the database. Here we set

$$IDS = IDS_{new};$$
$$K = K_{new};$$

Case II:

A_{old}=A, which means that, in the last session, the updating process was not successful at the tag side. Here we set

$$IDS = IDS_{old}$$
$$K = K_{old}$$

After this check, the reader uses the 3-tuple R1, K, IDS to compute the message B',

$$B' = \text{Rot}[R1,K] \oplus \text{Rot}[IDS,K] \oplus K;$$

If $B = B'$, the verification is successful; otherwise the verification fails.

Step 4, The reader uses a PRNG to generate a random number R2 and uses the R2, IDS, K, B to computer the messages C, D. The values C||D are then sent to the device tag.

$$C = R2 \oplus K \oplus IDS$$
$$D = \text{Rot}[IDS \oplus R2,B \oplus K] \oplus K$$

Step 5. On receiving the messages C||D, the device tag obtains R2 by XOR values C, K, IDS.

$$R2 = C \oplus K \oplus IDS$$

Then, using these values R2, IDS, K, B, it calculates D'.

$$D' = \text{Rot}\ [IDS \oplus R2', B \oplus K] \oplus K$$

If the received D and D' are equal, the verification is successful; otherwise the verification fails.

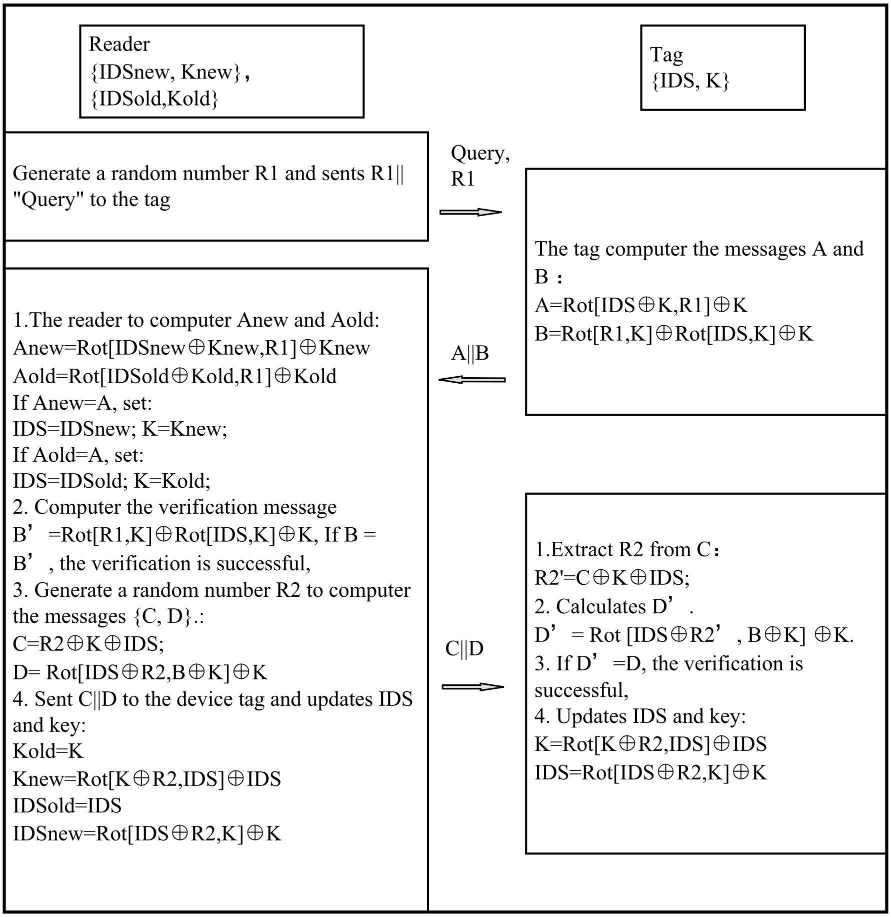
Step 6, After the completion of this process, the tag will update IDS and key value as

$$\mathrm{K} = \mathrm{Rot}[\mathrm{K} \oplus \mathrm{R2}', \mathrm{IDS}] \oplus \mathrm{IDS}$$
$$\mathrm{IDS} = \mathrm{Rot}[\mathrm{IDS} \oplus \mathrm{R2}', \mathrm{K}] \oplus \mathrm{K}$$

The reader will update values IDS_{new}, IDS_{old}, K_{new} , K_{old} as

$$\mathrm{K}_{old} = \mathrm{K}$$
$$\mathrm{K}_{new} = \mathrm{Rot}[\mathrm{K} \oplus \mathrm{R2},\mathrm{IDS}] \oplus \mathrm{IDS}$$
$$\mathrm{IDS}_{old} = \mathrm{IDS}$$
$$\mathrm{IDS}_{new} = \mathrm{Rot}[\mathrm{IDS} \oplus \mathrm{R2},\mathrm{K}] \oplus \mathrm{K}$$

Figure 1 depicts the flow diagram of our protocol.



Generate a random number R1 and sents R1|| "Query" to the tag

The tag computer the messages A and B：
$A=Rot[IDS \oplus K,R1] \oplus K$
$B=Rot[R1,K] \oplus Rot[IDS,K] \oplus K$

1.The reader to computer Anew and Aold:
$Anew=Rot[IDSnew \oplus Knew,R1] \oplus Knew$
$Aold=Rot[IDSold \oplus Kold,R1] \oplus Kold$
If Anew=A, set:
IDS=IDSnew; K=Knew;
If Aold=A, set:
IDS=IDSold; K=Kold;
2. Computer the verification message
$B' =Rot[R1,K] \oplus Rot[IDS,K] \oplus K$, If B = B’ , the verification is successful,
3. Generate a random number R2 to computer the messages {C, D}.:
$C=R2 \oplus K \oplus IDS$;
$D= Rot[IDS \oplus R2,B \oplus K] \oplus K$
4. Sent C||D to the device tag and updates IDS and key:
Kold=K
$Knew=Rot[K \oplus R2,IDS] \oplus IDS$
IDSold=IDS
$IDSnew=Rot[IDS \oplus R2,K] \oplus K$

1.Extract R2 from C：
$R2'=C \oplus K \oplus IDS$;
2. Calculates D’ .
$D' = Rot [IDS \oplus R2' , B \oplus K] \oplus K$.
3. If D’ =D, the verification is successful,
4. Updates IDS and key:
$K=Rot[K \oplus R2,IDS] \oplus IDS$
$IDS=Rot[IDS \oplus R2,K] \oplus K$

Fig. 1 Flow diagram of URAP protocol

3 Security analysis of URAP

We analyze the security of URAP in two main aspects: the functionality of the protocol and the resistance to the attacks. The functionality of the protocol includes the data confidentiality, data integrity, mutual authentication, forward security, and tag anonymity. The attacks considered here are replay attack, desynchronization attack, and man-in-the-middle attack.

3.1 Data confidentiality

The channel between the reader and the tag is insecure, and the transmitted messages are easily eavesdropped. In this protocol, the messages A||B and C||D are masked by bit operation with random number and K, and the adversary cannot obtain the secrets of the tag and reader through the values of A||B and C||D.

3.2 Data integrity

The messages A and C which are used to ensure the mutual authentication also ensure the data integrity. Suppose that the adversary modifies the values of A and C; then the value of B and D will be invalid and the protocol will terminate. It is difficult for the adversary to modify these values such that the values of B and D are correctly calculated. Thus, our protocol ensures the data integrity.

3.3 Mutual authentication

We have designed the protocol with both tag-to-reader authentication (message A||B), and reader-to-tag authentication (message C||D).

3.4 Forward security

After completing the mutual authentication, the reader and tag will update K and IDS. In addition, both K and IDS updates use random numbers for bit operations, and the adversary cannot reveal the past communications by eavesdropping on channel messages.

3.5 Tag anonymity

In this protocol, the IDS and K of each tag are updated per successful authentication, and the update operation involves random numbers. Therefore, the message from the same tag appears to be random in different sessions, and the attacker cannot identify and track the tag.

3.6 Resistance to replay attack

The adversary could store all the messages interchanged between the reader and the tag. Then, it can try to impersonate a reader, resending the message (Query||R1). For K and IDS have updated with random numbers, the messages A, B calculated by R1, K, IDS cannot obtain the legal authentication of the reader. The calculation of A||B and C||D uses random numbers, K and IDS, and these messages (numbers, K and IDS) are different from the previous session. Replaying A||B and C||D will also not complete authentication.

3.7 Resistance to de-synchronization attack

In URAP, if the last messages (C||D) are intercepted, the reader will not update its secrets while the tag updates them. In order to prevent the secret de-synchronization, the reader keeps two entries of its local data (K_{new} and K_{old}, IDS_{new} and IDS_{old}); the reader and the tag can still authenticate each other for such a situation, using the old values.

3.8 Resistance to man-in-the-middle attack

The protocol is secure against the man-in-the-middle attack. The adversary is not successful in getting key and pseudonym value. If the values of A||B and C||D intercepted and changed will cause the authentication unsuccessful. When the adversary performs a man-in-the-middle attack by modifying A||B and C||D, if the value of the K, IDS or R2 is not known, the authentication cannot be passed and the man-in-the-middle attack will fail.

3.9 Resistance to disclosure attack

A||B and C||D are both masked messages after the bit operation. The adversary cannot intercept the messages to obtain K and IDS, and the K and IDS will be updated after each authentication. Therefore the protocol can resist full disclosure attacks.

Table 2 shows the comparison of security between URAP and other ultra-lightweight protocols. (”no” indicates that it cannot prevent attacks, ”yes” indicates that it can prevent attacks.)

4 GNY logical Proof

In this section, we use GNY [17] logical protocol proof methods to verify the URAP protocol. Before the proof, we introduce the GNY logic symbols and rules used in this paper.

Table 2 Comparison of the security between protocols

	MMAP	LMAP	EMAP	SASI	RAPP	TGAP	URAP
Tag anonymity	No	No	No	No	No	No	Yes
replay attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes
de-synchronization attack	No	No	No	No	No	No	Yes
man-in-the-middle attacks	No	No	No	No	No	No	Yes
disclosure attack	No	No	No	No	No	No	Yes

P and Q are entities. X and Y are formulas. Shared secrets and encryption keys, are denoted as S and K respectively. The following are also formulae:

(X, Y) : conjunction of two formulae.

X_{K} and X_{K}^{-1} : encryption and decryption.

$P \lhd X$: P received a message containing X.

$P \ni X$(P possesses X): P possesses, or is capable of possessing, formula X.

$P| \sim X$: P once conveyed formula X.

$P| \equiv \#(X)$: P believes, or is entitled to believe, that formula X is fresh.

$P| \equiv \phi(X)$: P believes, or is entitled to believe, that formula X is recognizable.

$P| \equiv P\overset{S}{\longleftrightarrow}Q$: P believes, or is entitled to believe, that S is a suitable secret for P and Q.

$P| \equiv C$: P believes, or P would be entitled to believe, that statement C holds.

The GNY logic proof formulas are as follows:

Freshness Rules

F1: $\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y),P|\equiv\#(F(X))}$

F2: $\frac{P|\equiv\#(X),P\ni K}{P|\equiv\#(\{X\}_K),P|\equiv\#(\{X\}_K{}^{-1})}$

Recognizability Rules

R1: $\frac{P|\equiv\phi(X)}{P|\equiv\phi(X,Y),P|\equiv\phi(F(X))}$

Message Interpretation Rules

I1: $\frac{P\lhd*\{X\}_K,P\ni K,P|\equiv P\overset{K}{\longleftrightarrow}Q,P|\equiv\phi(X),P|\equiv\#(X,K)}{P|\equiv Q|\sim X,P|\equiv Q|\sim\{X\}_K,P|\equiv Q\ni K}$

In order to prove the security of the ultra-lightweight RFID authentication protocol, we use GNY logic to prove as follows:

4.1 Protocol description

The message transmitted between entities in the protocol is described. (T represents the tag and R represents the reader)

(1). R-T: $R1$

(2). T-R: $\{IDS, R1\}_K$

(3). R-T: $\{IDS, R2\}_K$

4.2 Protocol idealization

Rewrite the message in the protocol to a formula that conforms to the GNY logic syntax.

(1). $T \triangleleft * R1$
(2). $R \triangleleft * \{IDS, R1\}_K$
(3). $T \triangleleft * \{IDS, R2\}_K$

4.3 Initial assumptions

Based on the scenario in which the protocol is located and the capabilities of each entity, the following rationalization assumptions are derived:

(1) $R| \equiv \Phi(R1)$
(2) $R| \equiv \#(R1)$
(3) $R \ni K$
(4) $R| \equiv R \overset{K}{\longleftrightarrow} T$
(5) $T| \equiv \Phi(IDS)$
(6) $T| \equiv \#(IDS)$
(7) $T \ni K$
(8) $T| \equiv R \overset{K}{\longleftrightarrow} T$

4.4 Proving goals

According to the functions of the protocol, the security goals that the protocol should meet are as follows: (1). $R| \equiv T| \sim \#(IDS, R1)$
(2). $T| \equiv R| \sim \#(IDS, R2)$

4.5 Proof process

From GNY logic recognizability Rules R1, Initial Assumptions (1),we can get:

$$R| \equiv \Phi(IDS, R1) \tag{1}$$

From GNY logic freshness Rules F1, Initial Assumptions(2),we can get:

$$R| \equiv \#(IDS, R1) \tag{2}$$

From GNY logic freshness Rules F2, formula (2) and Initial Assumptions (3), we can get:

$$R| \equiv \#(\{IDS, R1\}_K) \tag{3}$$

From GNY logic message Interpretation Rules I1, Protocol Idealization (2), Initial Assumptions (3), Initial Assumptions (4), formula(1) and formula(3), we can get:

$$R| \equiv T| \sim (IDS, R1) \tag{4}$$

From the definition of freshness, formula (2) and formula (4), we can get: $R| \equiv T| \sim \#(IDS, R1)$. Proving Goals (1) is proved.

From GNY logic recognizability Rules R1, Initial Assumptions(5), we can get:

$$T| \equiv \Phi(IDS, R2) \tag{5}$$

From GNY logic freshness Rules F1, Initial Assumptions(6), we can get:

$$T| \equiv \#(IDS, R2) \tag{6}$$

From GNY logic freshness Rules F2, formula (6) and Initial Assumptions (7), we can get:

$$T| \equiv \#(\{IDS, R2\}_K) \tag{7}$$

From GNY logic message Interpretation Rules I1, Protocol Idealization (3), Initial Assumptions (7), Initial Assumptions (8), formula(5) and formula(7), we can get:

$$T| \equiv R| \sim (IDS, R2) \tag{8}$$

From the definition of freshness, formula (6) and formula (8), we can get:$T| \equiv R| \sim \#(IDS, R2)$. Proving Goals (2) is proved.

To conclude, our reasoning leads us to the conclusions that our protocol meets its security goals.

5 Performance evaluation of URAP

In order to show that the URAP can be safely implemented in low-cost tags, performance evaluation of the protocol is required. In this section, we analyze the performance of URAP in terms of computational cost, storage requirement and communication cost.

5.1 Computational cost

Low-cost passive RFID tags are very limited devices, in terms of computational resources. Regarding the computational cost, the tag involves only simple bit-wise

Table 3 Comparison of the operation types between protocols

	MMAP	LMAP	EMAP	SASI	RAPP	TGAP	URAP
Types of computation operations	AND,⊕, OR,+	+,⊕, OR	⊕,AND, OR	Rot,⊕, OR,+	⊕,Rot, Per	⊕,Rot	⊕,Rot

Table 4 Comparison of the storage cost between protocols

	MMAP	LMAP	EMAP	SASI	RAPP	TGAP	URAP
Types of computation operations	6L	6L	6L	4L	6L	6L	3L

Table 5 Comparison of the communication cost between protocols

	MMAP	LMAP	EMAP	SASI	RAPP	TGAP	URAP
rounds of communications	4	4	4	4	5	4	3
Number of bits sent by tag	3L	2L	3L	2L	2L	3L	2L
Number of bits sent by reader	4L	4L	4L	4L	5L	4L	4L
The total number of bits required	7L	6L	7L	6L	7L	7L	6L

operations: XOR and right rotate. These operations are very low-cost and can be effectively implemented on low-cost passive RFID tags. Table 3 compares the types of Types of computation operations between URAP and other ultra-lightweight protocols. (″+″ denotes the addition mod 2L, ″Per″ denotes a new bit operation [10].)

5.2 Storage requirement

We assume that the length of each message stored by the tag is L. In MMAP [4], LMAP [5], EMAP [6] , each tag has 4 keys (K1||K2||K3||K4) of length L, which is used for mutual authentication between the reader and the tag. In addition, the tag must store ID and IDS; hence it needs 6L of memory; in the SASI [7], it needs to store ID, IDS and two keys (K1, K2) for each tag, which adds up to a total of 4L; the tags in RAPP [8] store 5 messages: ID, IDS and three keys (K1, K2, and K3), the length to be stored is 5L; in the TGAP, each tag needs to store 5 values: ID, K_{new}, K_{old}, IDS_{new} and IDS_{old}. The total storage requirement is 5L bits. In the URAP, the tag only needs to store ID, IDS and K, which further reduces the tag compared to other protocols the cost of. Table 4 is a comparison of the tag storage cost between URAP and other ultra-lightweight protocols.

5.3 Communication cost

Regarding the communication cost, the ultra-lightweight protocol proposed in this paper only transmits Query||R1||A||B||C||D during the authentication process, which has very low communication overhead. Table 5 shows the comparison of the communication cost between URAP and other ultra-lightweight protocols.

From the analysis of the above three aspects, the URAP has lower cost and is more suitable for promotion and implementation in passive RFID systems.

6 Conclusion

In this paper, we propose an ultra-lightweight RFID mutual authentication protocol for low-cost passive RFID systems. Based on the security problems of the existing protocols, we modified the calculation method of the information to eliminating the security defects of these protocols and can effectively resist tracking attacks, replay attacks, and synchronization attacks, man-in-the-middle attacks, disclosure attacks, etc. In addition, we redesigned the content of the message which makes the proposed protocol can further reduce the computational cost, storage requirements and communication costs compared with the existing protocols.

At last, in the protocol, we assume that the channel between reader and a backend server is secure which is true in traditional backend server systems. However, with the rapid development of the Internet of Things in recent years, the amount of data that RFID systems need to process is increasing therefore, cloud servers based on cloud storage and cloud computing are more suitable than traditional servers. Since the channel between the cloud server and the reader is generally insecure, we will further study how to apply the proposed protocol to this scenario.

References

1. Kfir Z, Wool A (2005) Picking virtual pockets using relay attacks on contact—less Smartcard Systems. In: Proceedings of the 1st Int'l Conference on Security and Privacy for Emerging Areas in Comm. Networks (Securecomm 05), IEEE CS Press, 2005, pp 47–58
2. Rotter P (2008) A Framework for Assessing RFID System Security and Privacy Risks. IEEE Pervasive Comput 7(2):70–77
3. Avoine G, Carpent X, Hernandez-Castro J (2016) Pitfalls in Ultralightweight Authentication Protocol Designs. IEEE Trans Mobile Comput 15(9):2317–2332
4. Peris-Lopez P, Hernandez-Castro JC, Estévez-Tapiador JM et al (2006) M^{2}AP: a minimalist mutual-authentication protocol for low-cost RFID tags. In: International Conference on Ubiquitous Intelligence and Computing, pp 912–923
5. Peris-Lopez P, Hernandez-Castro JC, Estévez-Tapiador JM et al (2006) LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags. In: Proceedings of 2nd Workshop on RFID Security, pp 12–14
6. Peris-Lopez P, Hernandez-Castro JC, Estevez-Tapiador JM et al (2006) EMAP: an efficient mutual-authentication protocol for low-cost RFID tags. In: OTM Confederated International Conferences" On the Move to Meaningful Internet Systems", pp 352–361
7. Chien H-Y (2007) SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. IEEE Trans. Dependab. Secure Comput. 4(4):337–340
8. Tian Y, Chen G, Li J (2012) A new ultralightweight RFID authentication protocol with permutation. IEEE Commun. Lett. 16(5):702–705
9. Li T, Deng R (2007) Vulnerability analysis of EMAP-an efficient RFID mutual authentication protocol. In: The Second International Conference on Availability, Reliability and Security (ARES'07), pp. 238–245
10. Li T, Wang G (2007) Security analysis of two ultra-lightweight RFID authentication protocols. In: IFIP International Information Security Conference, pp 109–120
11. Ul Ain Q, Mahmood Y (2014) Cryptanalysis of Mutual Ultralightweight Authentication Protocols: SASI & RAPP, In: International Conference on Open Source Systems and Technologies
12. Tewari A, Gupta BB (2017) Cryptanalysis of a novel ultralightweight mutual authentication protocol for IoT devices using RFID tags. J. Supercomput. 73:1085–1102

13. Wang K-H, Chen C-M, Fang W, Wu T-Y (2018) On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags. J Supercomput 74:65–70
14. Khor Jing Huey, Sidorov Michail (2018) Weakness of Ultra-Lightweight Mutual Authentication Protocol for IoT Devices Using RFID Tags. In: 8th International Conference on Information Science and Technology, June 30–6, pp 91–97
15. Madiha Khalid, Umar Mujahid, Muhammad Najam-ul-Islam (2018) Cryptanalysis of ultralightweight mutual authentication protocol for radio frequency identification enabled Internet of Things networks. Int J Distrib Sensor Netw 14(8):1–9
16. Huang Shao-Cheng, Tsai Chia-Wei, Hwang Tzonelih (2018) Comment on Cryptanalysis of A Novel Ultralightweight Mutual Authentication Protocol for IoT Devices Using RFID Tags. In: DSIT ’18: Proceedings of the 2018 International Conference on Data Science and Information Technology, pp 23–27
17. Gong L, Needham RM, Yahalom R (1990) Reasoning about Belief in Cryptographic Protocols. In: IEEE Symposium on Security and Privacy, pp 234–248