Security Protocol for RFID System Conforming to EPC-C1G2 Standard

Feng Xiao
Information Security Center, Beijing University of Posts and Telecommunications Beijing, China
Email: xfstone1985@yahoo.com.cn

Yajian Zhou
Information Security Center, Beijing University of Posts and Telecommunications Beijing, China
Email: zhouyajian@126.com

Jingxian Zhou
Information Security Center, Beijing University of Posts and Telecommunications Beijing, China
Email: jingxian629@163.com

Hongliang Zhu
Information Security Center, Beijing University of Posts and Telecommunications Beijing, China
Email: zhuhongliang-82@163.com

Xinxin Niu
Information Security Center, Beijing University of Posts and Telecommunications Beijing, China
Email: xxniu@bupt.edu.cn

***Abstract*—Last few years, many security schemes are designed for RFID system since the release of the EPC Class 1 Generation 2 standard. In 2010, Yeh et al. proposed a new RFID authentication protocol conforming to EPC Class 1 Generation 2 standard. Yoon pointed that their protocol still had two serious security problems such as DATA integrity problem and forward secrecy problem. Then he proposed an improved protocol which claimed to eliminate the weakness in 2011. This paper shows that Yoon' s protocol had no resistance to replay attack and did not resolve the problem of data forge and tag's location privacy. An improved protocol is also proposed to protect RFID system from all major attacks. By comparing to other authentication protocols with respect of security and performance, the results shows that the proposed protocol is feasible for RFID tags which are low cost and resource-constrained devices.**

***Index Terms*—RFID system, EPC-C1G2 standard, Security protocol, privacy**

I. INTRODUCTION

As a mature information sensing technology, Radio frequency identification (RFID) has played an important role in the Internet of Things and pervasive computing environment. The RFID system consists of three elements: RFID tags, readers and back-end database server. The reader first exchanges information with a tag via radio transmission and requests to access the data about this tag, and after some certification process are executed among the three parties, the reader can retrieve the corresponding record from the database of the backend server[1].

While a lot of new standards of RFID are designed by some organizations and enterprises, EPC-C1G2(the Electronic Product Code Class-1 Generation-2 specification) which is adopted by EPCGlobal in 2004[2] is widely used in many fields such as logistics industry and retail business[3]. EPC-C1G2 is a new generation standard for passive tags which have limited computation and memory capacity due to their cost constraint on implementation[4]. However, the EPC-C1G2 does not take much account on the security and privacy issue about RFID system. So how to design a security protocol conforming to EPC-C1G2 for RFID system has been the focus of the research domain, which is also our concern in this paper.

The remaining sections of the paper are organized as follows: the related work is reviewed in Section 2. We briefly review Yoon's protocol in section3 and suggest the security problems on Yoon's protocol in Section 4. The new proposed protocol is presented in Section 5, and in Section 6 we analyze the proposed protocol with respect of security and the performance. Finally, conclusions are given in Section 7.

II. RELATED WORK

Motivated by the release of EPC-C1G2 specification[5], some researchers have recently proposed a lot of schemes[6-11] trying to solve the practical

Corresponding author: Feng Xiao

doi:10.4304/jcp.8.3.605-612

problems due to the fact that the EPC-C1G2 only provides a low security level. In this section, we will summarize some related proposals in this field.

In 2007 Chien et al.[12] proposed a mutual authentication protocol conforming to EPC-C1G2 standard, the security of their scheme heavily relied on the abuse of the cyclic redundancy code (CRC). However, Peris-Lopez et al.[13]showed that the protocol cannot resist to tag impersonation, desynchronization attacking and location tracking. So the Chien et al.'s protocol not only is vulnerable to such attacks, but also does not provide tag privacy.

Chen and Deng[14] proposed an EPC-friendly mutual authentication scheme by using a pseudo-random number generator (PRNG) and CRC which is conformed to the EPC-C1G2 standard. Their protocol tried to apply CRC as cryptographic hash function for message authentication. However, CRC functions are linear and should not be used for any cryptographic purpose—only for detection of random errors in the channel[15]. So attacker is able to impersonate a tag or a reader, to trace a tag, and even to launch a DoS attack. These security vulnerabilities are all due to the misuse of the CRC function.

In 2009 Yeh et al.[16] also proposed a RFID mutual authentication protocol conforming to EPC-C1G2 standard which allows us free from the assumption of the channel's security. The information transmitted between reader and back-end database may also eavesdropped and intercepted by the attacker in actual environment, so the protocol applied a one-way hash function to guarantee the communication security between reader and back-end database. Nevertheless, Yoon[17]pointed out that Yeh et al.'s protocol still had two serious security problems such as DATA integrity problem and forward secrecy problem.

The most recent proposal is Yoon's protocol which claimed that it was free from weakness mentioned above. The protocol revised the forward secrecy problem and increased a message authentication code to check the integrity of the data transmitted between database and reader based on the Yeh et al.'s protocol. However, the improved protocol cannot resist the replay attack and did not solve the DATA integrity problem.

III. REVIEW OF YOON'S PROTOCOL

In this section we briefly review Yoon's protocol[17]. Notations used in this paper are defined as follows:

EPC_s: The 96 bits of EPC code are divided into six 16-bit blocks, and then the six blocks are XORed to get EPCs.

$DATA$: The corresponding record for the tag kept in the database.

K_i: The authentication key stored in the tag for the database to authenticate the tag at the (i + 1)th authentication phase.

P_i: The access key stored in the tag for the tag to authenticate the database at the (i + 1)th authentication phase.

K_{old}: The old authentication key stored in the database.

K_{new}: The new authentication key stored in the database.

P_{old}: The old access key stored in the database.

P_{new}: The new access key stored in the database.

C_i: The database index stored in the tag to find the corresponding record of the tag in the database.

C_{old}: The old database index stored in the database.

C_{new}: The new database index stored in the database.

t: The timestamp which is created by reader.

T: The system time of the reader and database.

Δt: The maximum time difference between t and T.

X: The value kept as either new or old to show which key in the record of the database is found matched with the one of the tag.

$A \to B$: A forwards a message to B.

N_Y: The random number generated by device Y.

$A \oplus B$: Message A is XORed with message B.

RID: The reader identification number.

$H(\cdot)$: Hash function.

The information kept within respective devices:

Tag: (K_i, P_i, C_i, EPC_s)

Reader: RID

Database: $(K_{old}, P_{old}, C_{old}, K_{new}, P_{new}, C_{new}, RID, EPC_s, DATA)$

Yoon's protocol consists of two phases: the initialization phase, and the (i + 1)th authentication phase.

A. Initialization Phase

In this phase, some initial information such as K_0, P_0 and C_0 of tag and database are randomly generated by the manufacturer, and sets the values for the record in the tag $(K_i = K_0, P_i = P_0, C_i = C_0)$ and the corresponding record in the database $(K_{old} = K_{new} = K_0, P_{old} = P_{new} = P_0, C_{old} = C_{new} = 0)$.

B. The Detailed Steps of Yoon's Protocol

The communication messages exchanged are presented as follows:

Step 1. Reader $\to$ Tag: The reader generates random number N_R as a challenge and forwards it to the tag.

Step 2. Tag $\to$ Reader: After receiving N_R, the tag generates random number N_T, then computes $M_1 = PRNG(EPC_s \oplus N_R \oplus N_T) \oplus K_i$, $D = N_T \oplus K_i$, $E = N_T \oplus PRNG(C_i \oplus K_i)$, then forwards (M_1, D, C_1, E) back to the reader.

Step 3. Reader $\to$ Database: The reader computes $V = H(RID \oplus N_R)$, then forwards (M_1, D, C_1, E, N_R, V) to the database.

Step 4. Database $\rightarrow$ Reader: After receiving (M_1, D, C_i, E, N_R, V), the database performs the following operations:

(a) Retrieves each stored RID sequentially to compute $H(RID \oplus N_R)$ with N_R, and compares the product with the received V to identify the correct matching record and authenticate the reader.

(b) Then the database will examine the value of C_i in the tag to decide which of the following two procedures is proceeded. $C_i = 0$ stands for the first access, then the database will iteratively picks up an entry $(K_{old}, P_{old}, C_{old}, K_{new}, P_{new}, C_{new}, RID, EPC_s, DATA)$ and compute the values $I_{old} = M_1 \oplus K_{old}$ and $I_{new} = M_1 \oplus K_{new}$, and check whether I_{old} or I_{new} matches $PRNG(EPC_s \oplus N_R \oplus D \oplus K_{old})$ or $PRNG(EPC_s \oplus N_R \oplus D \oplus K_{new})$ computed by the database itself. Once the matching record is found, value of X is set as old or new according to which authentication key K_{new} or K_{old} in the record is found matched with the one in the tag. When $C_i \neq 0$, C_i is set as an index to find the corresponding record in the database. If the record is found by matching up by its field C_{old}, X is marked as old; otherwise database marks X as new if the record's field C_{new} matches up. Then databse will verify M_1, which is received from the reader, to see whether it is equal to $PRNG(EPC_s \oplus N_R \oplus D \oplus K_X) \oplus K_X$.

(c) The database Retrieves K_X from the matching record and checks whether E matches $N_T \oplus PRNG(C_X \oplus K_i)$. If the two values do not match, then the protocol aborts.

(d) The database computes $(M_2, Info, MAC)$ as follows:

$$M_2 = PRNG(EPC_s \oplus N_T) \oplus P_X$$
$$Info = (DATA \oplus RID)$$
$$MAC = H(DATA \oplus N_R)$$

Finally forwards them to the reader.

(e) If X = new, then the database will update the record by replacing K_{old} with K_{new} and P_{old} with P_{new}. New values for K_{new} and P_{new} will be reset as $PRNG(K_{new})$ and $PRNG(P_{new})$ respectively. If X = old, then just C_{new} is renewed as $PRNG(N_T \oplus N_R)$.

Step 5. Reader $\rightarrow$ Tag: The reader retrieves RID kept inside, XORs it with the received $Info$ to obtain $DATA$, and then verifies MAC, received from the database, to see if it is equal to $H(DATA \oplus N_R)$ computed by the reader itself. If the two values do not match, then the protocol aborts. Otherwise, forwards M_2 to the tag.

Step 6. The tag retrieves P_i kept inside to compute XOR with the received M_2. If the product matches $PRNG(EPC_s \oplus N_T)$ computed by the tag itself, then the authentication to the database is completed and the content kept inside is renewed as $K_{i+1} \leftarrow PRNG(K_i)$, $P_{i+1} \leftarrow PRNG(P_i)$, and $C_{i+1} \leftarrow PRNG(N_T \oplus N_R)$ for next access.

Fig. 1 illustrates the detailed steps of Yoon's protocol.

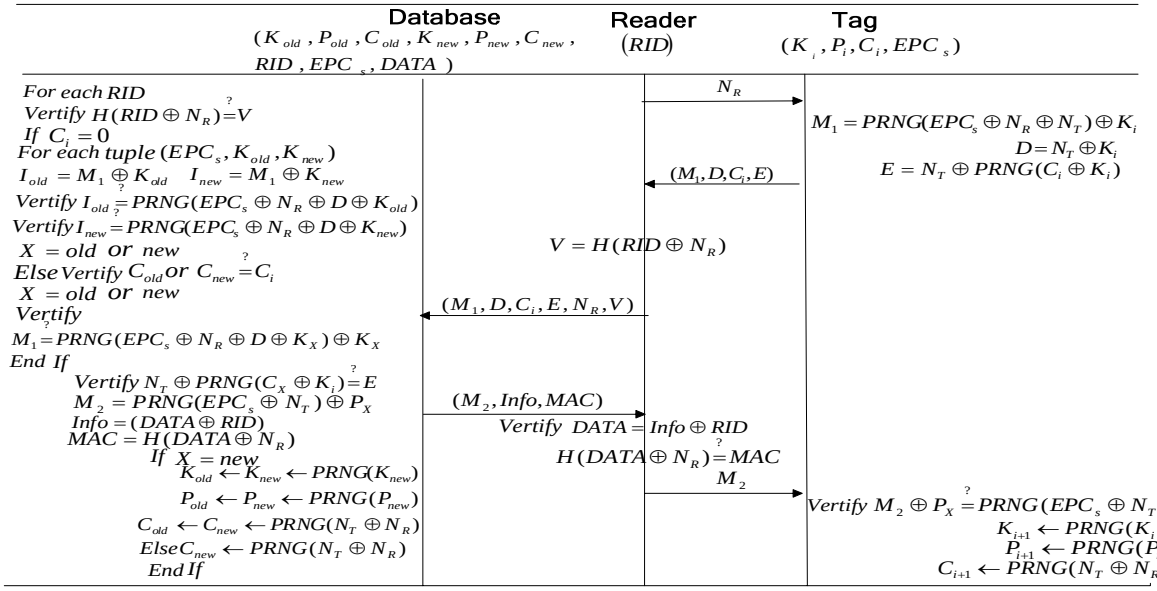

Figure 1. The detailed steps of Yoon's protocol.

IV. WEAKNESSES OF YOON'S PROTOCOL

Yoon analyzed Yeh et al.'s protocol and pointed out that their scheme had two serious weaknesses: data integrity problem and forward secrecy problem. Then Yoon proposed a revised protocol and claimed that the new protocol resolved the security problems. This section shows that Yoon's protocol still has the following two security problems.

A. Replay Attack and Privacy Problem

In Yoon's security analysis, he claimed that the improved protocol can resist replay attack and had no privacy problem. However, we will show that the revised protocol is also vulnerable to replay attack and the tag may be traced down by the adversary. An adversary A can perform operations as follows:

(1) After finishing a successful authentication procedure among the three parties, the adversary A can collect and record the authentication message including (M_1, D, C_i, E, N_R, V) by eavesdropping the communication channel.

(2) The adversary A pretends to play as a reader and resends the message (M_1, D, C_i, E, N_R, V) which is collected previously to the database. After receiving the message, the database will identify the reader and verify whether the authentication message is match to the record. This authentication procedure must be passed because the message (M_1, D, C_i, E, N_R, V) is legitimate.

(3) When the database completes the authentication of reader and tag, the message $(M_2, Info, MAC)$ is computed and sends to the reader. The message is identical to last one and it is no doubt that the tag will accomplish the validation to reader.

It is obvious that neither of tag and database has a mechanism which can detect the replay message. So the improved protocol has no resistance to the replay attack described above. On the other hand, the value $Info = (DATA \oplus RID)$ which is transmitted in step 4 is still at every round of authentication. So the adversary A can track the tag by discerning the value of $Info$. It means that Yoon's protocol cannot provide the tag's location privacy either.

B. DATA Integrity Problem

In Yeh et al.'s protocol, they assumed that the channel between reader and database was not secure. So the DATA between the database and reader can be spoofed or modified by an adversary A. Yeh et al.'s protocol applied $Info = (DATA \oplus RID)$ to protect the information because the RID is unknown to adversary A. However Yoon presented that the adversary can intercepted the information $(M_2, Info)$ between database and reader in step 4, and computer a forged value $Info^* = Info \oplus I$ and send $(M_2, Info^*)$ to the reader, the reader would still believed the wrong result $DATA^* = Info^* \oplus RID$ and accepted a false $DATA^*$ of the tag. In order to resolve this problem, Yoon increased a message authentication code by using a one-way hash function $MAC = H(DATA \oplus N_R)$ to guarantee the integrity of DATA. Unfortunately, the improper design of MAC leads to the improved protocol still has the integrity of DATA problem. An adversary A can perform operations as follows:

(1) When reader forwards (M_1, D, C_i, E, N_R, V) to database in step 3, an adversary A can obtain $V = H(RID \oplus N_R)$ by eavesdropping the

communication channel. When the database sends $(M_2, Info)$ to the reader in Step 4, A intercepts them.

(2) A computes the forged values of $Info^* = 0$ and $MAC^* = V = H(RID \oplus N_R)$, then sends the forged $(M_2, Info^*, MAC^*)$ to the reader.

(3) When receiving the forged $(M_2, Info^*, MAC^*)$, the reader will retrieve RID kept inside, XORs it with the received $Info^*$ to obtain $DATA^*$, and forward M_2 to the tag.

We can see that the XORed results which are $DATA^* = Info^* \oplus RID = 0 \oplus RID = RID$ and $H(DATA^* \oplus N_R) = H(RID \oplus N_R) = MAC^* = H(RID \oplus N_R)$. So the message authentication code does not work in this case. So the reader will believe that the forged $DATA^*$ sent by the database. In this attack, the tag cannot detect this forgery attack because A also did not change M_2 for the tag. As a result, Yoon's protocol still has DATA integrity problem.

V. PROPOSED PROTOCOL

We will propose an improvement of the Yoon's protocol which can resolve the problems presented in last section. The information kept within respective devices is same as Yoon's protocol. In addition, the initialization phase is identical as in the Yoon's protocol. We increase a timestamp t in order to resist to the replay attack. Fig. 2 illustrates the detailed steps of protocol. The messages exchanged are presented as follows:

Step 1. Reader $\rightarrow$ Tag: This step is the same as Yoon's protocol.

Step 2. Tag $\rightarrow$ Reader: This step is the same as Yoon's protocol.

Step 3. Reader $\rightarrow$ Database: The reader computes $V = H(RID \oplus N_R \oplus t)$, and then forwards $(M_1, D, C_i, E, N_R, V, t)$ to the database.

Step 4. Database $\rightarrow$ Reader: After receiving $(M_1, D, C_i, E, N_R, V, t)$, the database performs the following operations:

(a)The database checks the timestamp t in order to exclude the possibility of replay message. If $T - t > \Delta t$, which means the difference between t and system time T is beyond the maximum extent Δt , then the message will be discarded by database and the authentication operation will stop. Otherwise database retrieves each RID sequentially to compute $V = H(RID \oplus N_R \oplus t)$ with N_R and t , and compares the product with the received V to identify the correct matching record and authenticate the reader.

(b) The database examines the value of C_i in the tag to decide which of the following two procedures is proceeded. $C_i = 0$ stands for the first access. Then the database will iteratively pick up an entry $(K_{old}, P_{old}, C_{old}, K_{new}, P_{new}, C_{new}, RID, EPC_s, DATA)$ and computes the values $I_{old} = M_1 \oplus K_{old}$ and $I_{new} = M_1 \oplus K_{new}$, and check whether I_{old} or I_{new} matches $PRNG(EPC_s \oplus N_R \oplus D \oplus K_{old})$ or $PRNG(EPC_s \oplus N_R \oplus D \oplus K_{new})$ computed by the database itself. Once the matching record is found, the value of X is set as old or new according to which authentication key K_{new} or K_{old} in the record is found matched with the one in the tag. When $C_i \neq 0$, C_i is set as an index to find the corresponding record in the database. If the record is found by matching up by its field C_{old} , then database marks X as old; otherwise marks X as new if the record's field C_{new} matches up. Then the database will verify M_1 , which is received from the reader, to see whether it is equal to $PRNG(EPC_s \oplus N_R \oplus D \oplus K_X) \oplus K_X$.

(c) The database retrieves K_X from the matching record and checks whether E matches $N_T \oplus PRNG(C_X \oplus K_i)$ computed by the database itself. If the two values do not match, then the protocol aborts.

(d) The database computes $(M_2, Info, MAC)$ as follows:

$$M_2 = PRNG(EPC_s \oplus N_T) \oplus P_X$$
$$Info = (DATA \oplus RID \oplus t)$$
$$MAC = H(DATA \oplus t)$$

Finally forwards them to the reader.

(e) If X = new, then the database will update the record by replacing K_{old} with K_{new} and P_{old} with P_{new} . K_{new} and P_{new} will be reset as $PRNG(K_{new})$ and $PRNG(P_{new})$ respectively. If X = old, then just C_{new} is renewed as $PRNG(N_T \oplus N_R)$.

Step 5. Reader $\rightarrow$ Tag: The reader retrieves RID and t kept inside, XORs them with the received $Info$ to obtain $DATA$, and then verifies MAC , received from the database, to see if it is equal to $H(DATA \oplus t)$ computed by the reader itself. If the two values do not match, then the protocol aborts. Otherwise, forwards M_2 to the tag.

Step 6. This step is the same as Yoon's protocol.

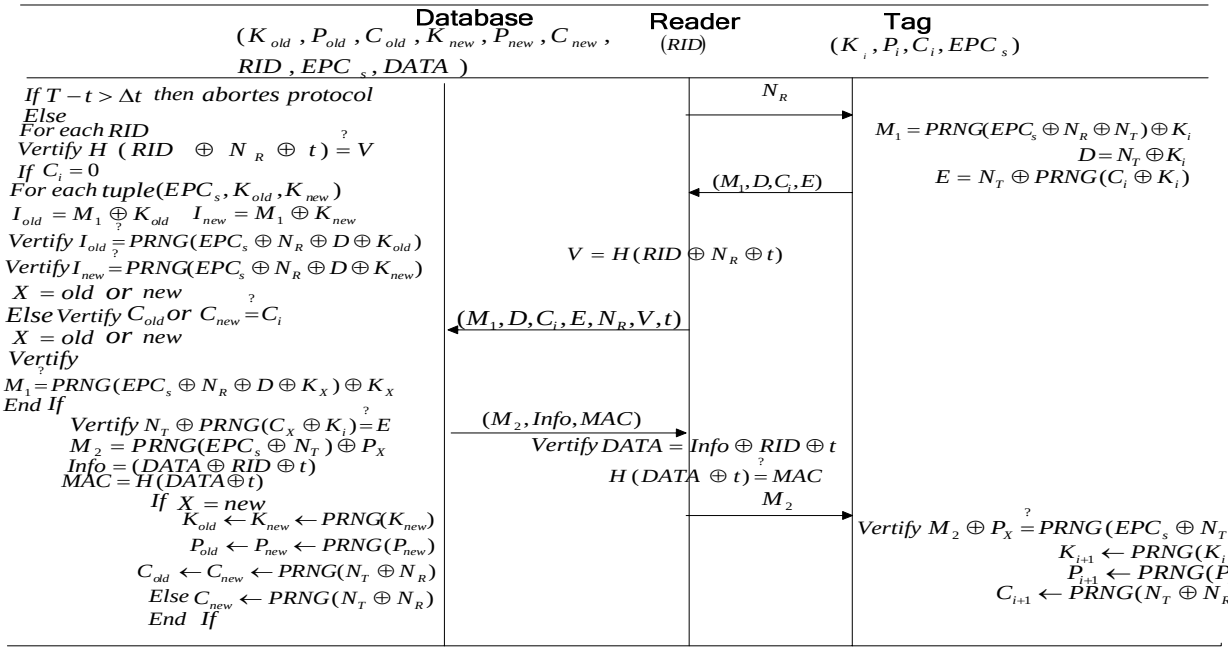

Figure 2. the detailed steps of proposed protocol.

VI. SECURITY AND PERFORMANCE ANALYSIS

In this section we will discuss our proposed protocol with respect of security and performance. As previous shown, Yoon's protocol is vulnerable to replay attack and still has the privacy and data integrity problem. So in our design, we will show how our improved protocol eliminates the two weaknesses while preserving the security and performance level of original protocol.

Theorem 1. The improved protocol withstands the replay attack and privacy problem.

Proof. Suppose adversary A collects and records the authentication message including $(M_1, D, C_i, E, N_R, V, t)$ by eavesdropping the communication channel after a successful authentication. Then A resends the message $(M_1, D, C_i, E, N_R, V, t)$ to the database attempting to finish the authentication operation. However, the database will check the timestamp first and see whether the difference between t and system time T is beyond the maximum extent Δt. This mechanism can get rid of the possibility of replay attack. On the other hand, the $Info = (DATA \oplus RID \oplus t)$ which is transmitted in step 4 is also protected by the timestamp t. The adversary cannot trace down the tag anymore because the value of $Info$ will not same at every round of protocol. Therefore, it is obvious that our protocol can withstand the replay attack and privacy problem.

Theorem 2. The improved protocol resolve the data integrity problem.

Proof. Yoon's protocol increased a message authentication code to check the integrity of the data. However, the improper design of $MAC = H(DATA \oplus N_R)$ still leads to the data integrity problem as we showed in section 4. So we revised the value of $V = H(RID \oplus N_R \oplus t)$ in step 3 and $MAC = H(DATA \oplus t)$ in step 4. Suppose adversary A intercepts all the communication message value $(M_1, D, C_i, E, N_R, V, t)$ of previous session, however, it makes no sense to forge the value of V and MAC for adversary. It is true because both the V and MAC are protected by timestamp t. As a result, the improved protocol can resolve the data integrity problem.

Theorem 3. The improved protocol provides same performance like Yoon's protocol.

Proof. The main difference between our protocol and Yoon's is that the we use timestamp to computer the value of V, $Info$ and MAC .The other steps of protocol are the same as Yoon's protocol. Therefore, the improved protocol still provides same performance like Yoon's protocol.

As shown in the Table 1, we compare our proposed protocol with the protocols introduced previously with respect of security and performance. It is clear that our proposed protocol is not only resistance to all kinds of attacks, but also provides good performance.

TABLE I.
SECURITY AND PERFORMANCE PROPERTIES OF PROTOCOLS

	Chien and chen's protocol	Yeh et al.'s protocol	Yoon's protocol	Proposed protocol
Replay attack	Secure	Insecure	Insecure	Secure
Impersonation attack	Secure	Secure	Secure	Secure
DoS attack	Insecure	Secure	Secure	Secure
DATA forgery attack	Insecure	Insecure	Insecure	Secure
Privacy	No provide	No provide	No provide	Provide
Forward secrecy	No provide	No provide	Provide	Provide
Database loading time	Slow	Fast	Fast	Fast

VIII. CONCLUSIONS

The release of EPC-C1G2 standard signals a milestone for the RFID technology. Many schemes are proposed in order to enhance the security of EPC system. However, neither of them is proven to be completely safe. This paper demonstrates that Yoon's protocol still has DATA integrity problem and cannot resist to the replay attack unlike their claims and we present an improved protocol which avoids the security deficiencies of Yoon's protocol. A comparison of the security and performance is also made with other schemes, the result shows that the proposed protocol offers a better security level and is feasible for the EPC-C1G2 compliant systems.

ACKNOWLEDGMENT

The authors are grateful to the editor and anonymous reviewers for their valuable suggestions which improved the paper. This work was supported by the National Natural Science Foundation of China (No. 6097 2077, 61121061), the Fundamental Research Funds for the Central Universities (No.BUPT2012RC0216), and the National Science and technology key project (No. 2010ZX03003-003-01).

REFERENCES

[1] X.B Zhang, L.L Cheng, Q.M Zhu, "Improvement of Filtering Algorithm for RFID Middleware Using KDB-tree Query Index", Journal of Software, vol.6, No.12, pp2521-2527, 2011.

[2] P. Peris-Lopez, J. C. H. Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard", Computer Standards and Interfaces, vol.31, No.2, pp372–380, 2009.

[3] M.B Li, H. Li, "Research on RFID Integration Middleware for Enterprise Information System", Journal of Software, vol.6, No.2, pp167-174, 2011.

[4] S.S Yu, Y. Peng, J. Yang, J.J Zhang, "The design and realization of a Lightweight RFID Mechanism Integrating Security and Anti-collision", Journal of Software, vol.6, No.7, pp1235-1240, 2011.

[5] K. Bai, S.X Li, T. Liu, J. Tian, "A Novel Method for Modeling RFID Data", Journal of Software, vol.7, No.4, pp835-843, 2012.

[6] S.Cai, Y.Li, T.Li and R.Deng, "Attacks and improvements to an RFID mutual authentication protocol",2nd ACM Conference on Wireless Network Security (WiSec'09), pp51-58 ,2009

[7] CC.Tan, B.Sheng and Q.Li, "Secure and serverless RFID authentication and search protocols", IEEE Transtracitons on Wireless Communications, vol.7, No.4, pp1400-1407, 2008.

[8] S. Han, V. Potgar and E. Chang, "Mutual authentication protocol for RFID tags based on synchronized secret information with monitor", Proceedings of ICCSA, Lecture Notes in Computer Science, vol.4707, pp227-238,2007.

[9] S.Y. Kang and I.Y. Lee, "A Study on low-cost RFID system management with mutual authentication scheme in ubiquitous", Proceedings of APNOMS, Lecture Notes in Computer Science,vol.4773,pp. 492– 502, 2007.

[10] C. Qingling, Z. Yiju, W. Yonghua, "A minimalist mutual authentication protocol for RFID system and BAN logic analysis", ISECS International Colloquium on Computing, Communication, Control, and Management.pp.449-453,2008.

[11] H.T Zhang and P Miao, "An Improved RFID Localization Algorithm Based on Layer By Layer Exclusion", Journal of Computers, vol .6, No 12, pp.2734-2739, 2011.

[12] H. Y. Chien and C. H. Chen , "Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards", Computer Standards and Interfaces, vol.29,No.2,pp. 254-259,2007.

[13] P. Peris-Lopez, T. Li, T.L. Lim, J.C. Hernandez-Castro, and J.M. Estevez-Tapiador, "Practical attacks on a mutual authentication scheme under the EPCClass-1Generation-2standard", Computer Communications,vol.32, No7,pp.1185-1193,2008.

[14] C. L. Chen and Y.Y. Deng, "Conformation of EPC class 1 generation 2 standards RFID system with mutual authentication and privacy protection", Engineering Applications of Artificial Intelligence, vol.22, No.8, pp.1284–1291,2009.

[15] P. Peris-Lopez, J. C. Hernandez-Castro, J. E. Tapiador, and J. C. A. van der Lubbe, "Cryptanalysis of an EPC class-1generation-2 standard compliant authentication protocol". Engineering Applications of Artificial Intelligence, vol.24,No.6, pp. 1061-1069, 2011.

[16] T. C. Yeh, Y. J Wang, T. C. Kuo and S. S. Wang," Securing RFID systems conforming to EPC Class 1 Generation 2 standard", Expert Systems with Applications, vol.37,No 12, pp. 7678 – 7683 ,2011.

[17] E.-J. Yoon. "Improvement of the securing RFID systems conforming to EPC class 1 generation 2 standard". Expert Systems with Applications, vol.39, No1, pp. 1589 – 1594,2012.

Feng Xiao was born in Hubei province, China in 1985.He received Software Engineering M.S. degree in school of Software Engineering from Beijing University of Posts and Telecommunications in 2009. He is currently a PH.D candidate in school of computer science, Beijing University of Posts and Telecommunications. His research interests include security protocol and privacy protection for the Internet of Things.

Yajian Zhou was born Shanxi province, China in 1971. He received his Ph.D. degree in communications engineering from Xidian University at Xi'an, China in 2003. His main research interests include mobile communications, security of wireless networks, security of databases, cryptography theory and its application.

He is currently an associate professor of school of Computer Science and Technology of Beijing University of Posts and Telecommunications.

Jingxian Zhou was born in Henan province, China in 1982. He received his M.S. degree in Department of Math from Zhengzhou University in 2010. He is currently a PH.D candidate in school of computer science, Beijing University of Posts and Telecommunications. His research interests are security authentication protocol in RFID air interface and wireless sensor networks, and architecture for the Internet of Things.

Hongliang Zhu was born in Henan province, China in 1982. He received his Ph.D. degree in Signal and Information Processing from Beijing University of Posts and Telecommunications, in 2010. His research interests are information security, traffic flow monitoring and identification.

He is current a lecturer of school of Computer Science and Technology of Beijing University of Posts and Telecommunications.

Xinxin Niu was born in Zhejiang province, China in 1963.She received her Ph.D. degree in Signal and Information Processing from The Chinese University of Hong Kong. Her main research interests include information security, information hiding and digital watermarking, digital content and its security.

She is currently a professor and Ph.D. supervisor of school of computer science and of Beijing University of Posts and Telecommunication.