An Improved Authentication Protocol for Mobile Agent Device in RFID Environment

Chia-Hui Wei

Department of Computer Science, National Tsing Hua University
101, Section 2, Kuang Fu Road, Hsinchu 300, Taiwan, R.O.C.
E-mail: chwei@cs.nthu.edu.tw

Min-Shiang Hwang*

Department of Computer Science and Information Engineering,
Asia University, 500, Lioufeng Rd., Wufeng, Taichung 41354,
Taiwan, R.O.C.
Email: mshwang@asia.edu.tw
*Corresponding author

Augustin Yeh-Hao Chin

Department of Computer Science, National Tsing Hua University
101, Section 2, Kuang Fu Road, Hsinchu 300, Taiwan, R.O.C.
E-mail: yhchin@cs.nthu.edu.tw

Abstract: In the past researches, most of the authentication protocols were designed in an effort to solve the RFID security and privacy problem regarding the encrypted communication between the database and readers, and readers and tags. Based on the proposal of mobile agent device for RFID privacy protection (MARP), some security problems have been exposed. Later on, protecting the privacy with a mobile agent device in RFID environment (eMARP) has shown improvement on MARP. The mobile agent device provides more powerful computation than the tag, in addition to the privacy protection along with the forgery detection. However, we found out that the authentication protocol of eMARP could not resist location tracking. Therefore, we will discuss and demonstrate that the eMARP-based RFID system doesn't have ability to achieve location tracking in this paper. We have improved the authentication protocol of eMARP-based RFID system and also have eliminated its vulnerability.

Keywords: Authentication, RFID, Security, Mobile Agent, Mobile Communication

Biographical notes: Chia-Hui Wei received the M.S. degree in Information Management from Chaoyang University of Technology, Taiwan. Currently, she received the Ph.D. degree in Computer Science from National Tsing Hua University, Taiwan. Her current research interests include RFID security, information security, and mobile communications.

Min-Shiang Hwang received the B.S. in Electronic Engineering from the National Taipei Institute of Technology, Taipei, Taiwan, Republic

Copyright © 2009 Inderscience Enterprises Ltd.

of China, in 1980; the M.S. in Industrial Engineering from the National Tsing Hua University, Taiwan, in 1988; and a Ph.D. in Computer and Information Science from the National Chiao Tung University, Taiwan, in 1995. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He was the chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He was a professor and chairman of the Department of Management Information Systems, National Chung Hsing University (NCHU), during 2005-2009. He was an outstanding professor of the department of Management Information Systems, NCHU, during 2007-2011. He obtained the 1997, 1998, 1999, 2000, and 2001 Outstanding Research Award of National Science Council of the Republic of China. He is currently a Chair Professor of the department of Computer Science & Information Engineering, Asia University. His current research interests include Information Security, electronic commerce, and mobile computing. Dr. Hwang has published over 170+ articles on the above research fields in international journals.

Augustin Yeh-hao Chin reveived the the Ph.D. degree from University Texas at Austin. Currently, he is a professor with the Department of Computer Science from the National Tsing Hua University, Hsinchu County, Taiwan. His current research interests include database systems, algorithm design, system programming, and software engineering.

1 Introduction

A RFID system consists of three components: a tag, a reader, and a database. The tag transfers data through radio wave to the reader, and then the reader transfers data to the backend database by wired network. The backend database can authenticate whether the tag is legal or not. The procedure is finished when the backend server have successfully verified the tag [19]. Due to its convenience and efficiency, RFID system is being widely used in various applications, providing users with automated procedures to identify goods and to engage in registration processes without much human intervention. Examples are supply chain management, e-passports, door security control, luggage tracking, and automatic road tolls [2, 4, 6]. Although RFID system has many advantages [9, 10, 15], it still faces several challenges. The privacy and security are the major concerns because the tag is used in an open environment. Tags are vulnerable to eavesdrop, spoofing attack, and tag forgery, which will cause unauthorized readers to access tags so that privacy might be invaded [5, 7, 17]. Therefore, some research [9, 13, 16, 17] suggested that to design a good RFID system we need to achieve certain requirements for security and privacy. This RFID system is required to resist tag forgery, spoofing attack, and eavesdropping for security purposes in order to protect users from location tracking and secure individual data for privacy.

Previous researches [1, 3, 14, 18, 21] have proposed various cryptographic operations in security mechanisms and attack models. Since the processing units and memory are limited, the tag can only perform simple arithmetic operations [8, 12]. Kim et al. [11] proposed a mobile agent device for RFID privacy protection (MARP), which possesses a more powerful computation than the tag. This protocol is based on mobile agent device, which has powerful CPU and battery system that can replace the tag. The mobile agent device guarantees higher level security than any other protection protocol. Later, Yeo et al. [20] proposed eMARP-based RFID system and then improved the security flaws of MARP. However, we pointed out and proved that eMARP-based RFID system cannot resist location tracking as they claim. In this paper, we will review eMARP-based RFID system and explain how an attacker performs location tracking against the tag in eMARP-based RFID system. We eventually improved authentication protocol for eMARP- based RFID system.

The rest of this paper is organized as follows. We briefly review eeMARP-based RFID system in Section 2 and present analysis of the attack in Section 3. In Section 4, we will demonstrate our security enhancement of authentication protocol for eMARP-based RFID system. Conclusions are presented in Section 5. In Table 1, we have listed the notations that are used throughout the paper.

Table 1 Notations and indexing terms.

Uid_t	The unique identifier of Tag t
Key_t	The secret value of Tag t
PIN_t	The mode change key of tag t
$\|\|$	Concatenation operator
$\oplus$	Exclusive-or operator
$h(\cdot)$	One way hash function
PIN_t^i	The tag t is executed the ith-time

2 Review eMARP-based RFID system

In this session, we will briefly introduce eMARP-based RFID system [20]. The eMARP-based RFID system includes six entities: the reader, the tag, the backend server, the public-key center, the mobile agent device, and a store database. The mobile agent device has high performance capability, large memory, and strong calculation capability. Two phases of authentication protocol are implemented in the mobile agent device based RFID system, namely the tag registration phase and the agent working phase as shown in Figure 1. In tag registration phase, all data of the tag are registered in mobile agent device by a store database. In the agent working phase, the mobile agent device performs the authentication with the tag and the backend server.

The steps of tag registration phase are described in Figure 2. The channel established between the store database and mobile agent device is considered secure, while the channel established between the mobile agent device and the tag is insecure. The store database and the tag are pre-stored with the value (Uid_t, PIN_t) and (Uid_t, PIN_t, Key_t) in their memory, PIN_t is one of the secret values

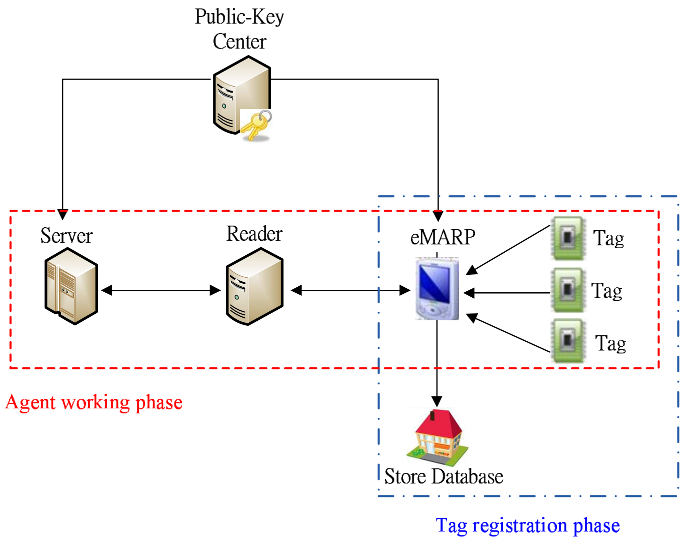


Figure 1 eMARP-based RFID system.

of Tag t.

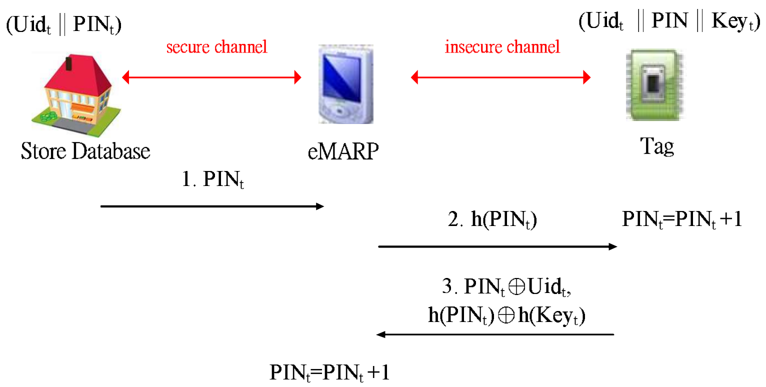


Figure 2 Tag registration phase of eMARP-based RFID system.

Tag Registration Phase:

Step 1. The store database sends PIN_t to mobile agent device via secure channel.

Step 2. After the mobile agent device receives the message, it computes the hashed value $h(PIN_t)$ and then sends it to the tag.

Step 3. After the tag successfully confirms the $h(PIN_t)$, the tag updates $PIN_t = PIN_t + 1$; otherwise the tag omits it. The tag computes $PIN_t \oplus Uid_t$ and $h(PIN_t) \oplus h(Key_t)$ by its pre-stored values Uid_t, PIN_t, and Key_t, and then sends it to the mobile agent device. The mobile agent device updates and stores Uid_t, new PIN_t, and $h(Key_t)$.

3 Weakness of eMARP Based RFID System

In normal operation, eMARP-based RFID system is executed with two rounds of the tag registration phase in Figure 3. In Figure 3, the upper part is the first round of the tag registration phase and the lower part is the second round, the same tag was executed in those two rounds. The values are indicated as PIN_t^i, and Uid_t^i, where i is the ith time.

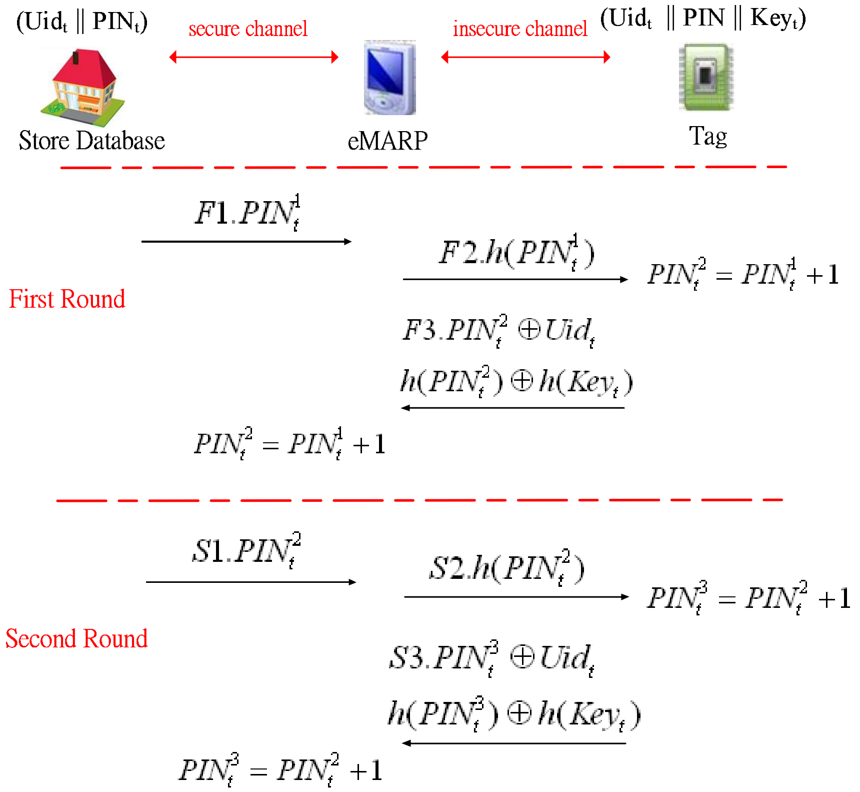


Figure 3 Two rounds of eMARP-based RFID system in normal operation.

In eMARP-based RFID system [20], the security analysis indicated that the proposed protocol was unable to resist a location tracking. The attacker is capable of recognizing and tracing from a particular message to the target tag. The eMARP-based RFID system claims that the value PIN_t is refreshed after the registration phase, so the adversary cannot guess PIN_t or the hashed $h(PIN_t)$. On the other hand, the eMARP-based RFID system also claims that the tag is designed to keep secured data Key_t, this value is protected by hash function $h(Key_t)$, and it is only used for the authentication between the tag and the mobile agent device. Therefore, tracking the tag becomes infeasible. However, the attacker can pretend as the third party, and eavesdrop between the mobile agent device and the tag to obtain the useful information. We will demonstrate that the eMARP-based RFID system is vulnerable to eavesdropping attack and location tracking during tag registration phase in Figure 4.

In Figure 4 4, we used the eMARP-based RFID system to execute the two rounds described in Figure 3 3 with the third party acting as the attacker to demonstrate the tracking process of the tag. The three steps for the attacker scenario are shown in Figure 4.

A1. The attacker uses the previously eavesdropped from Step 3 of the first round $F3 : h(PIN_t^2) \oplus h(Key_t)$ and Step 2 of the second round $S2 : h(PIN_t^2)$ to compute $h(PIN_t^2) \oplus h(Key_t) \oplus h(PIN_t^2)$, and then obtains $h(Key_t)$. The result is described step by step as follows.

$$F3 : h(PIN_t^2) \oplus h(Key_t) \tag{1}$$

$$S2 : h(PIN_t^2) \tag{2}$$

$$(1) \oplus (2) \longrightarrow h(PIN_t^2) \oplus h(Key_t) \oplus h(PIN_t^2) = h(Key_t) \tag{3}$$

A2. The attacker uses Equation (1): $h(PIN_t^2) \oplus h(Key_t)$ and Equation (3): $h(Key_t)$ to compute $h(PIN_t^2) \oplus h(Key_t) \oplus h(Key_t)$, and then acquires $h(PIN_t^2)$. The result is described step by step as follows.

$$(1) \oplus (3) \longrightarrow h(PIN_t^2) \oplus h(Key_t) \oplus h(Key_t) = h(PIN_t^2) \tag{4}$$

A3. The attacker uses Step 3 of the second round $S3 : h(PIN_t^3) \oplus h(Key_t)$ and the value $h(Key_t)$ obtained from Equation (3) to compute $h(PIN_t^3) \oplus h(Key_t) \oplus h(Key_t)$, and then the attacker can get $h(PIN_t^3)$. This step is repeated in different round, so the attacker can identify $h(PIN_t^i + 1) \oplus h(Key_t) \oplus h(Key_t)$ in the ith round due to the value $h(Key_t)$ at the same tag. As a result, the attacker can track the tag.

$$S3 : h(PIN_t^3) \oplus h(Key_t) \tag{5}$$

$$(5) \oplus (3) \longrightarrow h(PIN_t^3) \oplus h(Key_t) \oplus h(Key_t) = h(PIN_t^3) \tag{6}$$

$$h(PIN_t^i + 1) \oplus h(Key_t) \oplus h(Key_t) = h(PIN_t^i + 1) \tag{7}$$

As staged above, the attacker can certainly got hold of all of the value $h(Key_t)$, $h(PIN_t^2)$, and $h(PIN_t^i)$ from Equations (3), (6), and (7) between the mobile agent device and the tag. The attacker can collect successive value of $h(PIN_t^i)$ and identify $h(PIN_t^i)$ by Step 2 of next round and secret value $h(Key_t)$ of the tag, and then track the tag. Because the value $h(Key_t)$ is a static value and it is not changed, the attacker can compute $h(PIN_t^i + 1)$ and track the tag. For example, the attacker could collect message $h(PIN_t^i) \oplus h(Key_t)$ and compute its value $h(PIN_t^i)$ by $h(Key_t)$ from various locations. Yet the tag could be successfully tracked if the attacker have obtained the same value of $h(Key_t)$, which would give the attacker the ability to discover the location of the user of the tag. The problem exists not only with the tracking of the tag, but also serious encroachment of individual privacy.

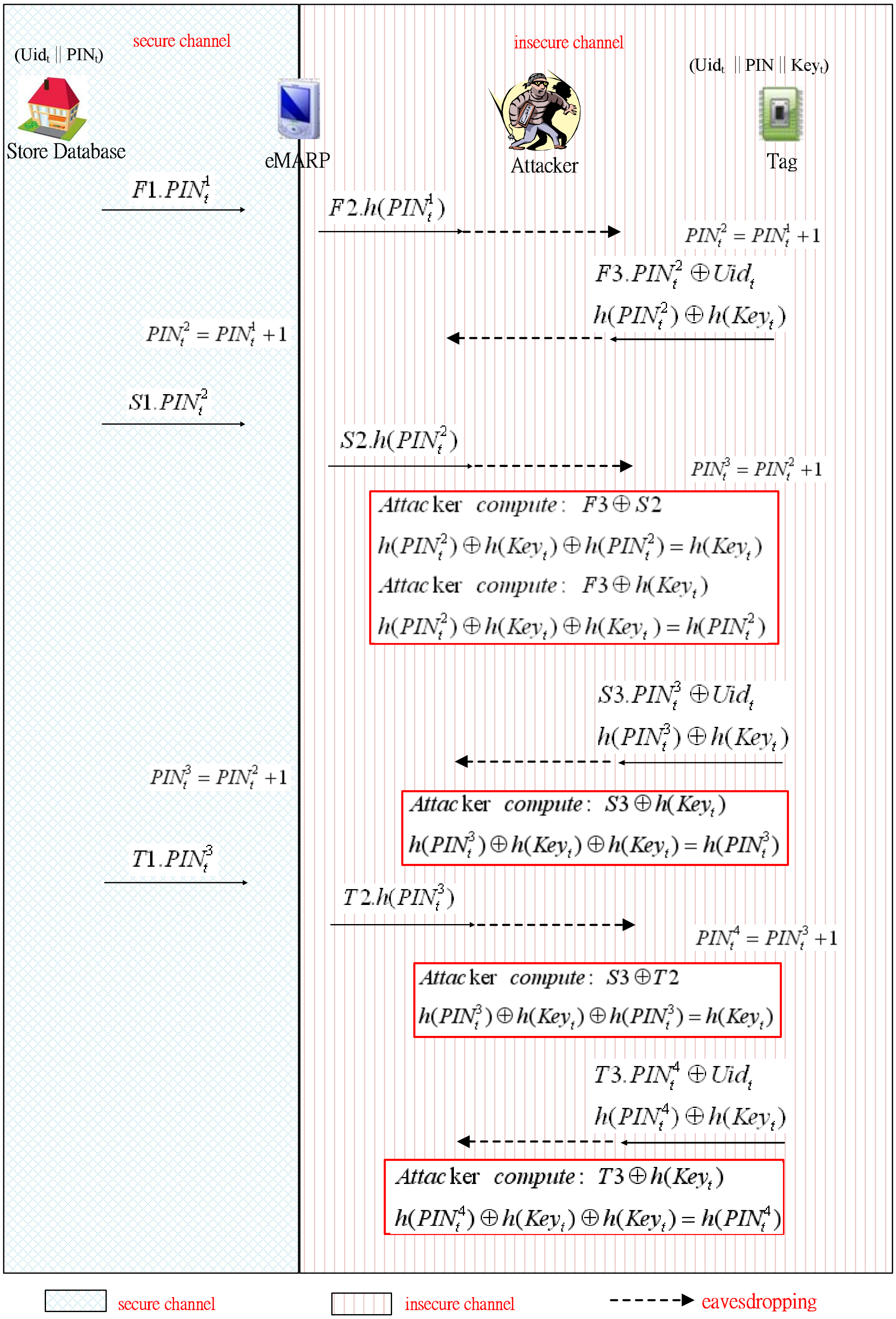
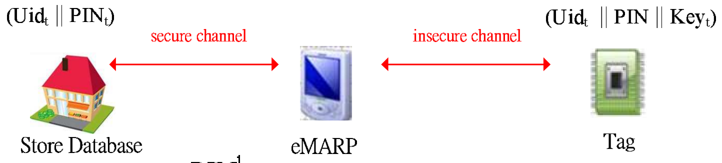


Figure 4 Weakness of the tag registration phase of eMARP-based RFID system.

4 New eMARP Based RFID System

In previous section, we have proved that the eMARP-based RFID system cannot achieve un-traceability. This weakness is caused by that the message exposes the useful information in the Equations (3), (4), and (6) in Figure 4. Thus, the attacker can construct the database by recording all of the authentication transcripts from the tag. Furthermore, the attacker would be able to compare the recording with the previous recordings, and then retrieves the same tag from different transaction records. In order to mend the authentication protocol of the eMARP-based RFID system, we have modified the authentication protocol to prevent an attacker from tracking the tag. We improved the authentication protocol of eMARP-based RFID system as shown in Figure 5.



I1. PIN_t^1 (Store Database → eMARP)

I2. $h(PIN_t^1)$ (eMARP → Tag)

$$PIN_t^2 = PIN_t^1 + 1$$
$$PIN_t^3 = PIN_t^2 + 1$$
$$M1 = h(PIN_t^2) \oplus h(Key_t),$$
$$M2 = h(PIN_t^3) \oplus Uid_t$$
$$M3 = h(PIN_t^1 \oplus h(Key_t) \oplus Uid_t)$$
$$update\ PIN_t^4 = PIN_t^3 + 1$$

I3. M1, M2, M3 (Tag → eMARP)

$$update\ PIN_t^2 = PIN_t^1 + 1$$
$$update\ PIN_t^3 = PIN_t^2 + 1$$
$$compute\ h(Key_t) \leftarrow M1 \oplus h(PIN_t^2)$$
$$compute\ Uid_t \leftarrow M2 \oplus h(PIN_t^3)$$
$$M3 \overset{?}{=} h(PIN_t^1 \oplus h(Key_t) \oplus Uid_t)$$
$$update\ PIN_t^4 = PIN_t^3 + 1$$

Figure 5 New eMARP-based RFID system.

I1. The store database sends PIN_t^1 to mobile agent device via secure channel.

I2. The mobile agent device received PIN_t^1 and computes $h(PIN_t^1)$ by the hash function and then sends it to the tag.

I3. The tag checks whether the received value $h(PIN_t^1)$ is matched or not with its value. If the value $h(PIN_t^1)$ is matched, the tag goes on to the next step; otherwise, the tag omits it. The tag computes PIN_t^2 and PIN_t^3 as follows:

$$PIN_t^2 = PIN_t^1 + 1$$
$$PIN_t^3 = PIN_t^2 + 1.$$

Next the tag computes $M1$, $M2$, and $M3$ by PIN_t^2, PIN_t^3, and PIN_t^1, respectively, as follows:

$$M1 = h(PIN_t^2) \oplus h(Key_t)$$
$$M2 = h(PIN_t^3) \oplus Uid_t$$
$$M3 = h(PIN_t^1 \oplus h(Key_t) \oplus Uid_t).$$

The tag updates and stores its value $PIN_t^4 = PIN_t^3 + 1$ for next identity of the tag, and then sends $M1$, $M2$, and $M3$ to the mobile agent device.

I4. After the mobile agent device receives the message, the device uses its PIN_t^1 to compute $PIN_t^2 = PIN_t^1 + 1$, $PIN_t^3 = PIN_t^2 + 1$ as follows:

$$PIN_t^2 = PIN_t^1 + 1$$
$$PIN_t^3 = PIN_t^2 + 1.$$

Then the device obtains $h(Key_t)$ and Uid_t by PIN_t^2 and PIN_t^3, respectively, as follows:

$$h(PIN_t^2) \oplus M1 = h(Key_t)$$
$$h(PIN_t^3) \oplus M2 = Uid_t.$$

After the mobile agent device obtains $h(Key_t)$ and Uid_t, the device checks along with verification of $M3$ whether it is equal to the received value or not as follows:

$$M3 \stackrel{?}{=} h(PIN_t^1 \oplus h(Key_t) \oplus Uid_t).$$

The tag is genuine if the verification is successful; otherwise, the message $I3(M1, M2, M3)$ fails. Afterwards, the mobile agent device updates $PIN_t^4 = PIN_t^3 + 1$ in its database. And the PIN_t^4 is used in next round to verify the tag.

5 Security and Performance Analysis

The detailed steps of an improved authentication protocol are described in Section **??**. In this session, we will analyze our proposed protocol in different types of security threats. For each threat, we first give a brief description, then we analyze the security of our improved protocol, and then we compare our improved authentication with the eMARP-based RFID system.

1. Eavesdropping: The attacker can surreptitiously listens to all the communications between the reader and the tag since the communications are established through radio wave, which makes it easy to be sniffed or eavesdropped. In our protocol, the attacker is able to observe all interactions between the mobile agent device and the tag. In other words, the messages including $h(PIN_t^1)$, M1, M2, and M3 are being eavesdropped. However, the new PIN_t^i is updated in each session and not repeatedly used in previous round. Therefore, the attacker cannot obtain useful message to track or fake a tag from a different query and a response each time. Even if the attacker is querying the same tag repeatedly, the attacker gets nothing from eavesdropping.

2. Spoofing attack: The adversary can pretend that he is a normal mobile agent device and gathers just enough information from the tag to spoof other mobile agent device. In our improved protocol, the secret value PIN_t, Key_t of the tag is protected by one-way hash, and PIN_t is updated during each session. Even though the attacker could gather all of the $h(PIN_t)$ value of Step 1, the attacker still cannot compute or infer the next hash value $h(PIN_t + 1)$. Thus, the attacker cannot perform spoofing to other eMARP.

3. Tag tracking: The attacker would be able to track a fixed serial number of the tag from different locations or transaction records if the tag always sends a fixed serial number to somewhere nearby the reader. In our protocol, the tag responds message $h(PIN_t^1)$, Equations (8), (8), and (8) to the mobile agent device. The attacker could link Equations (8), (8) and previous Equations (8) and (8) to obtain $h(PIN_t^2) \oplus h(PIN_t^5)$ and $h(PIN_t^3) \oplus h(PIN_t^6)$ to infer related information for every query. But the answer should be incorrect since the $h(PIN_t^4)$ is generated by the tag, so the attacker would not be able to link correctly with the next $h(PIN_t)$ value. In addition, the hash function is well-constructed, and it makes deriving the original value Uid_t from the message impossible. As a result, the attacker cannot track the tag.

4. Tag cloning: The attacker obtains a response from the tag, and then places the response on a fake tag. The attacker then attempts to deceive the reader that his/her counterfeits are legitimate. Under our protocol, although the attacker knows $h(PIN_t^1)$, it can not clone Equations (8), (8), and (8) because the hash function $h(.)$ is well-constructed and appropriately deployed. The key points are the $h(PIN_t^1)$, $h(PIN_t^2)$, and $h(PIN_t^3)$, which are continuously changing values in each session. In addition, the attacker would encounter difficulties while trying to identify the disclosed message such as Equations (8), (8), and (8), which are protected by secret value Uid_t,

successive value PIN_t^i, and hash function. Therefore, the attacker would not be able to clone the tag from the previous communication messages.

5. Privacy: The attacker can get partial privacy data but inferring personal information from the data is not possible. The scenario is constructed as follows: The tag is attached to a product in a store. We assumed that the attacker can obtain a list of targeted tags PIN_t, but he/she cannot identify which tag on his/her list, so we can protect the privacy of the tag. In our protocol, when the attacker queries the tag, the tag responses Equations (8), (8), and (8) for authentication. The attacker cannot identify whether the tag is in his/her list or not. Since the attacker could not identify the successive value PIN_t^i, thus the privacy data of the tag is protected.

The performance is evaluated in our proposed protocol in terms of security, computational cost, and storage requirement. First, we compared security with MARP and eMARP based RFID system in Section **??**. Next, we analyzed the attack model in eMARP based RFID system, which is vulnerable to tag tracking in the critical the Step 3 of tag registration phase. After the same tag was used to execute both rounds, the attacker got $h(Key_t)$ and $h(PIN_t^i)$ then he/she can track the tag and discloses the privacy information easily. In Section **??**, we designed a modified version to improve eMARP based RFID system and compared security list with the original. The results are shown in Table 2. It's obvious that our proposed protocol is more secure than eMARP based RFID system. Because PIN_t^i is combined with the message at Step 3 and updated in each round, such that the attacker cannot guess or compute Key_t, and $h(PIN_t^i + 1)$.

Table 2 The security features for eMARP based RFID system and our proposed.

	MARP	eMARP Based RFID System	Our Proposed
Eavesdropping	Yes	No	No
Spoofing Attack	No	No	No
Tag Forgery	Yes	No	No
Location Tracking	No	Yes	No
Disclosure	Yes	Yes	No

Second, on computational cost, the mobile agent device can compute operations hash and XOR, which are equal to eMARP and MARP. The total steps of our proposed eMARP-based RFID system, e-MARP and MARP are 3 steps: one between the store database and the mobile agent device, and another two between the mobile agent device and the tag as shown in Figures 2 and Figures 5. The computational costs of tag registration phase for both protocols are shown in Table 3.

The tag computation cost of our proposed protocol is 5 XORs and 5 Hashes. However the mobile agent device computation cost of our protocol is 4 XORs and 4 Hashes, which is higher compared with the eMARP-based protocol and MARP because our protocol is strengthened at Step 3 to protect the $h(Key_t)$ and

Table 3 The performance comparison of tag registration phase for both protocols.

	MARP	eMARP Based RFID System	Our Proposed
Total Steps	3 Steps	3 Steps	3 Steps
Tag Computation	2 XORs + 1 Hashes	2 XORs + 2 Hashes	5 XORs + 5 Hashes
eMARP Computation	1 Hash	1 Hash	1 Hash
Traffic	2 Values	2 Values	3 Values
Memory Size	2 Statics + 1 Variable	2 Statics + 1 Variable	2 Statics + 1 Variable

Uid_t. The traffic cost of eMARP-based RFID system has two values: one value is $PIN_t \oplus Uid_t$ and another is $h(PIN_t) \oplus h(key_t)$, which are between the mobile agent device and the tag. The traffic cost of MARP is the same with eMARP-based RFID system. Our proposed protocol has three values: $M1$, $M2$, and $M3$. To summarize the computation cost, although the computation cost of both the tag and mobile agent device of ours are higher than that of eMARP based RFID system and MARP, our proposed protocol is more secure based on comparison.

Finally, we examine the storage requirement of our proposed protocol; it owns two static values, Uid_t and Key_t, and one updatable value, PIN_t. The memory is required to store 64-bit static value for Uid_t and Key_t, and 128-bit rewritable memory for PIN_t. Therefore, the storage cost of our proposed protocol has the same memory size as eMARP-based RFID system and MARP.

6 Conclusion

In this paper, our contributions are listed as follows: (1) eMARP-based RFID system is insecure in location tracking. We have analyzed the security of eMARP-based RFID system, and then have demonstrated location tracking against the authentication protocol of eMARP-based RFID system in Section 3. (2) Therefore, our proposed protocol has improved the authentication protocol of eMARP-based RFID system, and has shown viable solutions against traceability of the tag. (3) Compared with the authentication protocol of MARP and eMARP-based RFID system, our proposed protocol not only keeps the equivalent condition for memory size and total steps, but it has shown a more secured design than the eMARP-based RFID system. (4) From the system management viewpoint, designing resist traceability of the tag is important to protect personal privacy. In this paper, we have shown that it may be quite dangerous to use authentication protocol under eMARP-based RFID system environment. Therefore, we improve authentication protocol for mobile agent device in RFID. Although our proposed is secure enough, it needs more computation of tag. This problem needs to be solved in future.

Acknowledgements

The authors would like to acknowledge the many helpful suggestions of this paper. We also thank the Editor of this Journal.

References

[1] Tianjie Cao and Peng Shen, "Cryptanalysis of two RFID authentication protocols," *International Journal of Network Security*, vol. 9, pp. 95–100, July 2009.

[2] Jengchung V. Chen and Paul Pfleuger Jr, "Rfid in retail: A framework for examining consumers' ethical perceptions," *International Journal of Mobile Communications*, vol. 6, no. 1, pp. 53–66, 2008.

[3] Jiann-Liang Chen, Ming-Chiao Chen, Chien-Wu Chen, and Yao-Chung Chang, "Architecture design and performance evaluation of RFID object tracking systems," *Computer Communications*, vol. 30, no. 9, pp. 2070–2086, 2007.

[4] Peter D. DeVries, "The state of rfid for effective baggage tracking in the airline industry," *International Journal of Mobile Communications*, vol. 6, no. 2, pp. 151–164, 2008.

[5] S. L. Garfinkel, A. Juels, and R. Pappu, "RFID privacy: An overview of problems and proposed solutions," *IEEE Security & Privacy*, vol. 3, no. 3, pp. 34–43, 2005.

[6] Shin-Yuan Hung, She-I Chang, and Chi-Ping Ting, "Unerstanding the key success factors of rfid use in supply chain management: A delphi study," *International Journal of Mobile Communications*, vol. 8, no. 3, pp. 313–333, 2010.

[7] Min-Shiang Hwang, Chia-Hui Wei, and Cheng-Yee Lee, "Privacy and security requirements for RFID applications," *Journal of Computers*, vol. 20, no. 3, 2009,Corrected Proof.

[8] Wen-Shenq Juang and Jing-Lin Wu, "Robust and efficient authenticated key agreement in mobile communications," *International Journal of Mobile Communications*, vol. 7, no. 5, pp. 562–579, 2009.

[9] Ari Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communication*, vol. 24, no. 2, pp. 381–394, 2006.

[10] Ari Juels and Stephen A. Weis, "Defining strong privacy for RFID," *ACM Transactions on Information and System Security*, vol. 12, no. 1, pp. 7:1–7:23, 2009.

[11] Soo-Cheol Kim, Sang-Soo Yeo, and Sung Kwon Kim, "MARP: Mobile agent for RFID privacy protection," *Lecture Notes in Computer Science*, vol. 3928, pp. 300–312, 2006.

[12] Chun-Liang Lai, Kwoting Fang, and Shou-Wei Chien, "Enhanced monitoring of tuberculosis patients by using rfid technologies," *International Journal of Mobile Communications*, vol. 8, no. 2, pp. 244–256, 2010.

[13] M.R. Rieback, B. Crispo, and A.S. Tanenbaum, "The evolution of RFID security," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 62–69, 2006.

[14] Panagiotis Rizomiliotis, Evangelos Rekleitis, and Stefanos Gritzalis, "Security analysis of the song-mitchell authentication protocol for low-cost RFID tags," *IEEE Communications letters*, vol. 13, no. 4, pp. 274–276, 2009.

[15] C. M. Roberts, "Radio frequency identification (RFID)," *Computers & Security*, vol. 25, no. 1, pp. 18–26, 2006.

[16] P. Rotter, "A framework for assessing RFID system security and privacy risks," *IEEE Pervasive Computing*, vol. 7, no. 2, pp. 70–77, 2008.

[17] S. Spiekermann and S. Evdokimov, "Critical RFID privacy-ehancing," *IEEE Security & Privacy*, vol. 7, no. 2, pp. 56–62, 2009.

[18] Chiu C. Tan, Bo Sheng, and Qun Li, "Secure and serverless RFID authentication and search protocols," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1400–1407, 2008.

[19] Chia-Hui Wei, Min-Shiang Hwang, and Augustin Yeh-Hao Chin, "An authentication protocol for low-cost rfid tags," *International Journal of Mobile Communications*, vol. 9, no. 2, pp. 208–223, 2011.

[20] Sang-Soo Yeo, Soo-Cheol Kim, and Sung Kwon Kim, "Protecting your privacy with a mobile agent device in RFID environment," *Wireless Personal Communications*, vol. 51, no. 1, pp. 165–178, 2009.

[21] Xiaolan Zhang and Brian King, "Security requirements for RFID computing systems," *International Journal of Network Security*, vol. 6, pp. 214–226, Mar. 2008.