Improvements over Extended LMAP+: RFID Authentication Protocol

Jitendra B. Gurubani, Harsh Thakkar, and Dhiren R.Patel

Department of Computer Engineering, NIT Surat-395007, India
{jitendra.gurubani,harsh9t,dhiren29p}@gmail.com

Abstract. Radio Frequency Identification (RFID) systems are increasingly being deployed in a variety of applications. Widespread deployment of such contactless systems raises many security and privacy concerns due to unauthorized eavesdropping reader, de-synchronization between reader and tag etc. In this paper, we propose a light weight mutual authentication protocol which is an improvement over Li's extended LMAP+ protocol. In mutual authentication, the tag and the reader of the RFID systems will authenticate each other before transmitting unique ID of tag. The proposed protocol provides protection over traceability and de-synchronization attacks.

Keywords: RFID, Pseudonym, LMAP, Mutual Authentication Protocol

1 Introduction

Radio Frequency Identification (RFID) systems are used for automated identification of objects and people. Applications that use RFID technology include warehouse management, logistics, railroad car tracking, product identification, library books check-in/check-out, asset tracking, passport and credit cards, etc. Most of the RFID systems comprise of three entities: the tag, the reader and the back-end database. The tag is a highly constrained microchip (with antenna) that stores the unique tag identifier and other related information about an object. The reader is a device that can read/modify the stored information of the tags and transfer these data to a back-end database, with or without modification. Back end database stores this information and will keep track of the data exchanged by the reader [1].

The possible security threats to RFID systems include denial of service (DoS), man in the middle (MIM), counterfeiting, spoofing, eavesdropping, traffic analysis, traceability, de-synchronization etc.

The low cost deployment demand for RFID tags forces the lack of resources for performing true cryptographic operations to provide security. Typically, tags can only store few hundred bits and have very limited number of logic gates, out of which very few can be devoted to security tasks. Considering these resource constraints, we aimed for authentication protocol that uses light weight primitives.

The rest of the paper is organized as follows: Background and related work are discussed in section 2. Section 3 describes system design considerations and the pro-

posed protocol. Section 4 shows defense against traceability and de-synchronization attacks with conclusions and references at the end.

2 Related Work

Providing light weight security in RFID systems is not a trivial task. Vajda and L. Buttyan [2] have proposed a set of extremely lightweight challenge response authentication algorithms. These can be used for authenticating the tags, but they may be easily attacked by a powerful adversary. Juels [3] proposed a solution based on the use of pseudonyms, without using any hash function. The RFID tag stores a short list of pseudonyms, which indexes a table (row) where all the information about a tag is stored: it is rotated releasing a different index on each reader query. After a set of authentication sessions, the list of pseudonyms will need to be reused or updated through an out-of-band channel, which limits the practicality of this scheme. In addition to this there are other lightweight mutual authentication protocols proposed in the literature [4-6]. Attacks have been successfully mounted on all of these as demonstrated in literature [7-9].

Peris *et al*. in [10], Proposed a Lightweight Mutual Authentication Protocol called LMAP. They also proposed an extension of this protocol LMAP+. These protocols are extremely lightweight and use only simple bitwise operations. However, attacks are mounted on this as well. It has been discovered that these protocols do not achieve the security they claim [11]. Later, following the LMAP designing strategy, Li [12] proposed a new lightweight protocol which is extension of LMAP proposed by Peris *et al*. in [10]. After that, Safkhani *et al*. in [14] presented two possible attacks on protocol which is extension of LMAP+.

We propose an improvement over Li's protocol [12] LMAP+ - incorporating better security and without compromising performance. Proposed protocol follows the structure and design of LMAP+ [12]; extended to provide defense against traceability and de-synchronization attacks.

3 Proposed Protocol: Improved LMAP+

3.1 Design Considerations

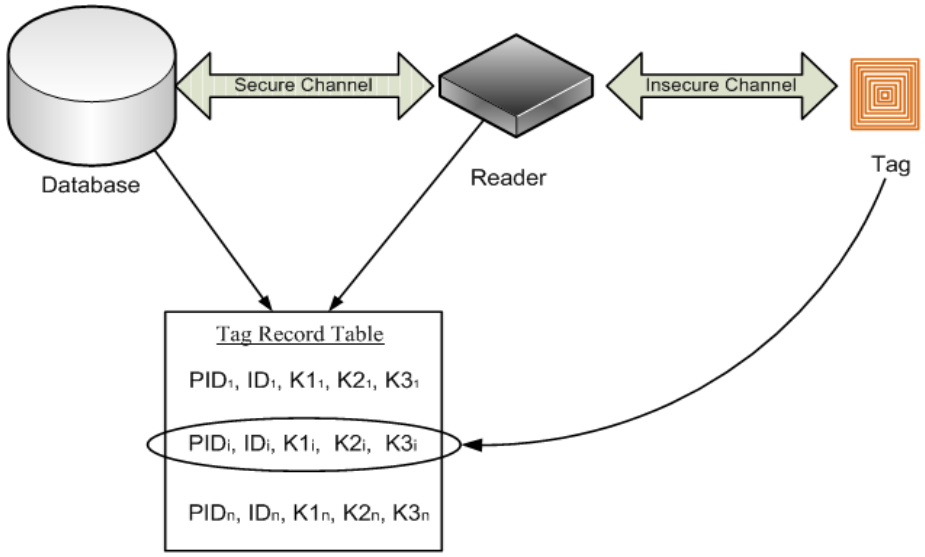

Fig.1. Typical RFID System [12]

Fig.1 shows three main entities (tag, reader and database) of the RFID systems which are involved in the mutual authentication scenarios. Database and reader are connected through a secure wired channel while the tag and reader are connected through wireless channel which is insecure and is our main focus. We will consider database and reader as one unit responsible for maintaining the database where all the tag records are stored in a central table and tag as another unit which is to be authenticated. Before the tags are attached to the objects of the RFID applications, its Unique ID and Pseudo-ID are written in its ROM and EEPROM respectively together with several secret values (for authentication purpose).
The properties of the proposed protocol (Improved LMAP+) are:

- **Privacy**: A tag's Unique ID is never disclosed to an unauthorized reader. Only the authorized reader will identify the Tag by its Pseudo-ID along with its corresponding tag entry in the database. Pseudo-ID and the keys used will be changed after every successful protocol round.
- **Security**: The scheme defends against various attacks like: sniffing attack, spoofing attack, active man-in-the-middle attack, traceability attack and desynchronization attack etc.
- **Compactness**: The proposed protocol uses only ultra-lightweight functions like X-OR and mod 2^m addition as used by Li in [12], whose hardware implementations is very simple.

3.2 Protocol Notations

In the proposed protocol, costly operations such as multiplications and hash evaluations are not used at all, and random number generation is only done at the reader end. Frequently used notations in this paper are listed below:

$ID_{tag(i)}$: Tag's unique identifier.
$PID^n_{tag(i)}$: Tag's dynamic pseudonym at the n^{th}successful run of protocol.
$K1^n_{tag(i)}$, $K2^n_{tag(i)}$ and $K3^n_{tag(i)}$: Tag's secret keys at the n^{th}successful run of protocol.
r : Reader generated pseudorandom number.
A, B, C : Messages transferred between reader and tag.
$\oplus$: XOR operation.
$\|$: concatenation operator.
+ : addition mod2^m.
$(X)_n$: n^{th} Bit of x

All parameters (i.e. ID, PID, K1, K2, K3, r, A, B, C) in the protocol are of 96-bit size- as per EPC class 1 Gen2.

3.3 Initialization

Tag Initialization: Assuming 96-bits as one word, the RFID tag is assigned 5 words which include a Pseudo-ID, a tag unique ID and three keys (*K1*, *K2* and *K3*). Out of these, tag unique ID is static (should be stored in ROM) and the rest are updated on every successful run of protocol (should be stored in EEPROM). Thus, tag requires 96 bits of ROM and 384 bits of EEPROM (4*96). Considering L as word size the tag has 5L bits of storage requirement.

Database Initialization: A central database is built in order to store all the information relevant to the RFID Tags. For each tag, it stores a row [*PID, ID, K1, K2, K3*]. All rows are listed in a single database table. If we have N tags, there will be N records and the total database size will be 5*N*L bits.

3.4 Protocol Description

The protocol has three main stages: tag identification, mutual authentication and updating. These stages are shown in table 1. Equations in first two stages are same as proposed in LMAP+ [12], except last equation in stage 2 – Mutual Authentication.

Tag Identification
Reader → Tag: Hello
Tag → Reader: $PID^{n}_{tag(i)}$

Mutual Authentication
Reader → Tag: $A \,||\, B$
Tag → Reader: C
Where,
$A = PID^{n}_{tag(i)} \oplus K1^{n}_{tag(i)} + r$
$B = PID^{n}_{tag(i)} + K2^{n}_{tag(i)} + r$
$C = PID^{n}_{tag(i)} \oplus (K3^{n}_{tag(i)} + r)$ *

Updating
By both Reader and Tag
$PID^{n+1}_{tag(i)} = PID^{n}_{tag(i)} \oplus r + (K1^{n}_{tag(i)} + K2^{n}_{tag(i)} + K3^{n}_{tag(i)})$ *
$K1^{n+1}_{tag(i)} = K1^{n}_{tag(i)} \oplus r + (PID^{n+1}_{tag(i)} + K2^{n}_{tag(i)})$ *
$K2^{n+1}_{tag(i)} = K2^{n}_{tag(i)} \oplus r + (PID^{n+1}_{tag(i)} + K3^{n}_{tag(i)})$ *
$K3^{n+1}_{tag(i)} = K3^{n}_{tag(i)} \oplus r + (PID^{n+1}_{tag(i)} + K1^{n}_{tag(i)})$ *

Table 1. Improved LMAP+: n^{th} Protocol Run between Tag and Reader (* shows modified or improved equations)

- **Tag Identification**: To start the protocol for mutual authentication, the reader has to identify the tag. The reader will initiate the protocol by sending a hello message to the tag, which will be responded by the tag sending its current pseudonym (PID). By means of this PID, only an authorized reader is able to search the database and access the tag's corresponding secret keys ($K = K1|K2|K3$), which are needed to carry out the next authentication stages.
- **Mutual Authentication**: Initially the reader generates a random number *r*. Using *r* along with the keys *K1* and *K*2; the reader generates the messages *A* and *B*, and then sends them to the tag. Thus, the reader actually conveys a random challenge to the tag. At the tag side, upon receiving the messages *A* and *B*, the tag can calculate two random numbers (*r1* from *A* and *r2* from *B*) using secret keys *K*1 and *K*2 respectively. If *r1* equals to *r2*, the tag can obtain *r* correctly and prepare the response message *C* as detailed by Li in [12]. On the reader side it calculates the value of *C* according to the equation in the table 1, as it has all required parameters and compares the calculated *C* value with the one received from the tag. If both are equal, the tag is authenticated. Then using the PID value, the reader retrieves the unique tag ID from the database table and considers the tag with this ID as detected. Hereafter that reader proceeds with update operations. If the reader is not authenticated, the authentication protocol is aborted. This makes the tag identification by the reader without actually transmitting the unique ID of the tag.

- **Updating:** Major improvements over LMAP+ are incorporated in this stage. After the reader and the tag have authenticated each other, they carry out the pseudonym and keys updating operations at both sides synchronously as mentioned by the equations in table 1.

The mechanism for synchronization is same as described by Li [12]. Both reader and tag contain a status bit in the protocol denoted by *s*. In each run, if the protocol is successfully completed, *s* will be initialized with 0 otherwise it is set to 1. Hence, *s* = 1 indicates that the protocol was aborted. So it should be reset or restarted.

4 Security against traceability and de-synchronization attacks

According to Li's protocol in [12]:

$$A = PID^{n}_{tag(i)} \oplus K1^{n}_{tag(i)} + r \quad (1)$$

$$B = PID^{n}_{tag(i)} + K2^{n}_{tag(i)} \oplus r \quad (2)$$

$$C = (PID^{n}_{tag(i)} + ID_{tag(i)} \oplus r) \oplus (K1^{n}_{tag(i)} + K2^{n}_{tag(i)} + r) \quad (3)$$

Our protocol reflects improvements as indicated by * in table 1.

4.1 Traceability defense

According to Safkhani *et al.* [14], if we consider only last significant bit (LSB) then the modular additions mod 2^m can be replaced by bitwise XOR. Therefore, any adversary can extract and trace the last significant bit of tag unique ID by knowing $PID^{n}_{tag(i)}$, *A*, *B* and *C* as follows:

$$(ID_{tag(i)})_0 = (A)_0 \oplus (B)_0 \oplus (C)_0 \oplus (PID^{n}_{tag(i)})_0$$

Our proposal (Improved LMAP+) provides defense against this attack as the actual unique ID of the tag is not transmitted and hence it will not be extracted by the adversary.

4.2 De-synchronization defense

The main aim in this attack is to convince the tag and reader to update their common parameters to different values. With different values of common parameters; tag and reader will not be able to authenticate each other for future transactions. According to Safkhani *et al.* [14], if we assume that $(PID^{n}_{tag(i)})_0$, $(K1^{n}_{tag(i)})_0$, $(K2^{n}_{tag(i)})_0$ and $(ID_{tag(i)})_0$ are zero then adversary can mount the attack by toggling the LSBs of *A*, *B* and *r*. It will have no impact on the correctness of above equations 1, 2 and 3. Only the random number retrieved at tag side will be different than the one sent by the reader. Tag and reader will authenticate each other and up-

date their common parameters to different values as both have different *r* value which will be used in updating stage.

In our proposal, the random number *r* is used only once in the formation of equation *C*. Therefore, if the adversary changes the LSBs of *A*, *B* and *r* then the calculated value of *C* from tag will differ from the expected *C* value. Reader will not authenticate this tag and the transaction will be aborted. So, the de-synchronization attack is defended.

5 Conclusion

Improvements in Mutual authentication protocol for low cost RFID systems are proposed in this paper.

As it is an extension over LMAP+ protocol, it inherits security against tag cloning, spoofing and man in the middle attack as provided by LMAP+ protocol. In addition it is secure against traceability and de-synchronization attacks for which LMAP+ was not secure as shown by Safkhani *et al*. in [14]. The improved protocol is secure (more trustworthy than LMAP+) and uses ultra light weight bitwise operations.

References.

1. V. D. Hunt, A. Puglia, and M. Puglia: RFID: A Guide to Radio Frequency Identification. Wiley-Inter science (2007).
2. I. Vajda and L. Buttyan.: Lightweight authentication protocols for low-cost RFID tags. In: *Proc. of UBICOMP'03* (2003).
3. A. Juels.: Minimalist cryptography for low-cost RFID tags. In: *Proc. of SCN'04*, volume 3352 of LNCS, pages 149–164. Springer-Verlag (2004).
4. Sadighian and R. Jalili.: Afmap: Anonymous forward-secure mutual authentication protocols for rfid systems. In: Third IEEE International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2009), pages 31–36 (2009).
5. Sadighian and R. Jalili.: Flmap: A fast lightweight mutual authentication protocol for rfid systems. In: 16th IEEE International Conference on Networks (ICON 2008), pages 1–6, New Delhi, India (2008).
6. H.-Y. Chien. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. In: IEEE Transactions on Dependable and Secure Computing, 4(4):337–340 (2007).
7. M. Safkhani, M. Naderi, and N. Bagher.: Cryptanalysis of AFMAP. In: IEICE Electronics Express, 7(17):1240–1245 (2010).
8. M. Safkhani, M. Naderi, and H. Rashvand.: Cryptanalysis of AFMAP. In: International Journal of Computer & Communication Technologys, 2(2):182–186 (2010).
9. M. B´ar´asz, B. Boros, P. Ligeti, K. L´oja, and D. Nagy: Passive Attack Against the M2AP Mutual Authentication Protocol for RFID Tags. In: First International EURASIP Workshop on RFID Technology, Vienna, Austria (2007).

10. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda.: Lmap: A real lightwight mutual authentication protocol for low-cost rfid tags. In: Proceedings of RFIDSec06 Workshop on RFID Security, Graz,Austria, 12-14 (2006).
11. T. Li and G. Wang.: Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols. In: IFIP SEC 2007, Sandton, Gauteng, South Africa (2007).
12. T. Li.: Employing lightweight primitives on low-cost rfid tags for authentication. In: *VTC Fall*, pages 1–5 (2008).
13. Ben Niu; Hui Li; Xiaoyan Zhu; Chao Lv.; Security Analysis of Some Recent Authentication Protocols for RFID. In: Computational Intelligence and Security (CIS), 2011 Seventh International Conference on, vol., no., pp.665-669 (2011).
14. Safkhani, Masoumeh; Bagheri, Nasour; Naderi, Majid; Sanadhya, Somitra Kumar; Security analysis of LMAP^{++}, an RFID authentication protocol. In: Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, vol., no., pp.689-694 (2011).