Journal of Network and Computer Applications 41 (2014) 37–46

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

An ultralightweight RFID authentication protocol with CRC and permutation

Lijun Gao [a,b], Maode Ma [c,*], Yantai Shu [a], Yuhua Wei [b]

[a] School of Computer Science and Technology, Tianjin University, Tianjin
[b] Department of Computer Science and Technology, Shenyang Aerospace University, Shenyang, China
[c] School of Electrical & Electronic Engineering, Nanyang Technological University, Singapore

ARTICLE INFO

Article history:
Received 11 May 2013
Received in revised form
24 August 2013
Accepted 13 October 2013
Available online 31 October 2013

Keywords:
RFID
Ultralightweight
Permutation
Desynchronization
SPIN

ABSTRACT

Radio Frequency Identification (RFID) technology will become one of the most popular technologies to identify objects in the near future. However, the major barrier that the RFID system is facing presently is the security and privacy issue. Recently, an ultralightweight RFID authentication protocol with permutation has been proposed to provide security and prevent all possible attacks. However, it is discovered that a type of desynchronization attack can successfully break the proposed scheme. To overcome the vulnerability under the desynchronization attacks, we propose an approximate ultralightweight RFID authentication protocol which integrates the operation of the XOR operator, build-in CRC-16 function, the permutation and secret key backup technology to improve the security functions without increasing any security cost. We formally verify the security functionality of the proposed scheme by using Simple Promela Interpreter (SPIN). Analysis shows that our proposal has a strong ability to prevent existing possible attacks.

1. Introduction

Radio frequency identification (RFID) is a technology for automated identification of objects and people (Juels, 2006). An RFID application contains three key elements: RFID tags, RFID readers, and a back-end database server that has the ability to identify objects with increased speed and accuracy. The reader is used to query the tag identify (TID) and forwards it to the back-end server. Once the tag is found valid, the back-end server will check the information kept by the tag for further processing. RFID tags are classified into three types: active, semi-passive, and passive. Active tags need batteries to operate so that they can actively communicate with the readers. Semi-passive tags also need batteries to work but they have to wait for the reader's query. As for passive tags, the power supply comes from the reader. In a basic RFID system, the information transmitted in the air between the tag and the reader could easily be intercepted and eavesdropped due to its radio transmission nature.

A Generation 2 (Gen2) tag contains a pseudorandom number generator (PRNG) and protects message integrity via Cyclic Redundancy Code (CRC-16). The memory space is separated into four banks: the reserved memory, Electronic Product Code (EPC) memory, TID memory, and the user memory. It harvests power from the readers through the antenna, and hence, cannot perform complex computations. EPCglobal class-1 generation-2 (Gen2 in brief) was approved as ISO18000-6C in July 2006. It is widely believed that Gen2 tags will be the mainstream for the developing RFID applications because the effective reading range is larger (Sun and Ting, 2009).

Currently, the RFID security and privacy protection mechanisms mainly can be classified into two major categories: physical approaches and encryption mechanisms and protocols. The proposals on the physical security mechanisms for the RFID tags mainly include the Faraday Cage (Sarma et al., 2003), kill command mechanism (Weis, 2003), and the locker tag (Juels et al., 2003). Further research results indicate that although the physical security approaches can achieve some degree of security, it will cause the increase of the cost of an entire RFID system. On the other hand, the encryption technology based security protocols have shown to be more attractive to the development of the RFID systems, which will be soon widely adopted. The encryption technology based security protocols can be classified into four classes. The first class called "full-fledged class" refers to those protocols that demand the support of conventional cryptographic functions like symmetric encryption, ryptographic one-way function, or even the public key algorithms. The second class called "simple" refers to those protocols that should support random number generator and one-way hashing function on tags. The third class called "lightweight" protocols refers to those protocols that require a random number generator and simple functions.

* Corresponding author. Tel.: +65 67904385; fax: +65 67920415.
E-mail addresses: emdma@ntu.edu.sg, Maode_Ma@pmail.ntu.edu.sg (M. Ma).

1084-8045/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jnca.2013.10.014

The fourth class called "ultralightweight" that only nvolve simple bitwise operations (like XOR, AND, OR, etc.) or some built-in function in tags. Analysis shows that simple, lightweight and ultralightweight RFID authentication protocols are more effective and efficient. They have attracted much more attention from researchers because the full-fledged RFID authentication protocols cannot meet the requirement of a low-cost RFID system, although they have strong security functionality (Chien, 2007).

In terms of simple protocols, the hash-Lock scheme has been introduced in Sarma et al. (2003a, 2003b) used $metaID=H(K)$ to hide the real ID of a tag, where K is the shared secret between the tag and the back-end server, H is a one-way hash function. Although this scheme offers certain level of reliability at low cost, an adversary can easily track the tag via its *metaID* and thus the transaction secret or privacy would be at risk. Furthermore, since the key shared between the tag and the back-end server is sent in plaintext, even an inactive adversary can easily sniff the channel to spoof the tag later. The hash based ID variation protocol in Henrici and Muller (2004) is similar as the hash chain protocol, which uses a random number to refresh the tag identifier dynamically. The random number increases in every successful authentication session so that this improved protocol can defend against the replay attacks. The protocol can resolves the location attacks by making the ID of a tag randomized in every interrogation. It is reliable to prevent data loss because it can restore the data from the previous record. Unfortunately, this protocol cannot resist man-in-the-middle attacks. The behaviors of the intermittent position tracing attacks and desynchronization attacks have been defined in Gao et al. (2013). And the vulnerability of the protocol under the desynchronization attacks has been reported in Zhou et al. (2010) while a novel RFID security protocol (RIPTA-DA) has been designed, which employs a stochastic dynamic multi-key mechanism to encrypt the information and introduces the noise disturbance technology to overcome the vulnerabilities under the both attacks.

On the other hand, in terms of lightweight protocols, Hopper and Blum (HB), HB+, HB++ protocols have been proposed in Blurn et al. (1993), Juels and Weis (2005), Bringer et al. (2006) and Piramuthu (2007)) as a family, which has used Learning Parity in the Presence of Noise (LPN) to provide stronger security functionality. However, it is found that if an aggressor replays challenges on a tag with $O[(1-\eta)/(1-2\eta)^2]$, where η is a noise parameter. Each tag has a noise generator, the probability of generating a noise is $\nu=\{0, 1|\text{prob}\ [\nu=1]=\eta\}$, $\eta\in(0, 1/2)$, where ν is a vector, which is a binary string, η is the probability of the number of "1" in the binary string ν times. It is possible to obtain the value of $a.x$, where . is a point multiplication operation, with very high probability. A synchronization-based communication protocol for RFID devices has been presented in Duc et al. (2006). The protocol targets to protect the EPC Global Class-1 Gen-2 RFID tags which support only simple cryptographic primitives like PRNG and CRC. It can prevent the cloned tags and malicious readers from impersonating attacks and abusing legitimate tags, respectively. In addition, the protocol is able to provide that each RFID tag emits a different bit string (pseudonym) when receiving each query from different readers. Therefore, it makes possible for the tracking activities and personal preferences of a tag's owner impractical to provide the user's privacy. It's possible for a malicious reader can get $M_1=\text{CRC}(\text{TID}\|r_1)\oplus K_i$, and $M_2=\text{CRC}(\text{TID}\|r_2)\oplus K_i$, where k represents string concatenation and r_1, r_2 are nonce values. In this way, the attacker can identify the tag by the following way $M_1\oplus M_2=\text{CRC}(\text{TID}\|r_1)\oplus\text{CRC}(\text{TID}\|r_2)$. Once the tag is queried by a valid reader which causes the key update, the attacker can restart the attack. Although the protocol is defective, the application of CRC function in the design has opened a new way to design a low cost RFID system. In Doss et al. (2013, 2012), three solutions have been proposed for the authentication and privacy in the RFID systems base on the quadratic residues technology. But due to the employment of high cost hash functions and complex encryption algorithms, they are not suitable to the low-cost RFID systems.

In terms of ultralightweight protocols, a minimalist mutual-authentication protocol (M^2AP) for low-cost RFID tags has been proposed in Lopez and Castro (2006) based on some simple operations such as XOR, OR, AND, and sum of modulo. A tag and a reader can share a pseudonym session identifier (SID) and four keys K_1, K_2, K_3, and K_4. During each session, the reader generates two random numbers n_1 and n_2. Let "$\vee$" denote OR operation, "$\wedge$" for AND, and "$+$" for modular summation. By this protocol, the tag verifies the reader by checking the n_1 value extracted from the first two messages. The tag then responds to the reader if it is correct. Both SID and four keys must be updated after each session to provide forward secrecy. Recently, an attack to break the M^2AP protocol has been reported in Bárász et al. (2007). By this attack, an adversary could discover the tag's identity and some shared secrets in two rounds of eavesdropping. Furthermore, the attacker can undertake desynchronization attacks by using the known key.

An interesting lightweight authentication protocol has been proposed providing strong authentication and strong integrity (SASI) for low-cost RFID tags in Chien (2007). An index-pseudonym (IDS), the tag's private identification (ID), and two keys (k_1/k_2) are stored both on the tag and in the back-end database. Simple operation functions such as bitwise XOR ($\oplus$), bitwise AND ($\wedge$), bitwise OR ($\vee$), addition 2^m and left rotate Rot(x,y) are required on the tag. Additionally, a PRNG is required at the reader. The proposed scheme is ultralightweight, while the active tracking attacks are possible among two valid readers because the IDS in SASI is a static value. It is also shown that a desynchronization attack on the SASI scheme can succeed with at most 96 trials (Sun et al., 2011). A Gossamer protocol has been introduced in Peris-Lopez et al. (2009), which has a very good security performance to keep the confidentiality and integrity of data in the authentication procedure with a forward security characteristic due to a rotation operation, which is a combined function with circular shift function and the Mixbits function. The Gossamer protocol has shown to have an extremely lightweight nature, as only bitwise right shift ($\gg$) and additions have been employed. The abovementioned protocols have certain security functionality equipped with simple operations at a low cost, while they are not able to resist some desynchronization attacks (Ahmed et al., 2010).

A new ultralightweight RFID authentication protocol with permutation (UAPP) has been proposed in Tian et al. (2012). It has avoided using unbalanced OR and AND operations and has introduced a new operation named permutation. A tag only involves three operations: bitwise XOR, left rotation and permutation. The performance evaluation illustrates that since the UAPP scheme only uses fewer resources on the tags in terms of computation operation, storage requirement and necessary communication, the total cost of the UAPP scheme is low. The security analysis in Tian et al. (2012) has claimed that the UAPP scheme can resist to all possible existing attacks. However, one type of the desynchronization attacks has been found to be able to break the protocol.

It is obvious that the simple authentication protocols can effectively resist to various attacks due to the employment of the complicated hash functions. Then, the security cost of them is high. Although the lightweight authentication protocols have not been equipped with complex hash functions, the security cost is relative higher due to the random number generator introduced. The design of RFID ultralightweight authentication protocols to have high security functionality with a low cost becomes very important and attractive. In this paper, the UAPP scheme, which is the newest ultralightweight protocol, has been reviewed to explore its vulnerability under one type of the desynchronization