Mobile Agent Code Updating and Authentication Protocol for Code-centric RFID System

[1]Liang Yan, [2]Hongbo Guo, [3]Min Chen, [1]Chunming Rong, [2]Victor Leung

[1]Department of Electrical Engineering and Computer Science, University of Stavanger, Norway (yanliangtju@gmail.com, chunming. rong@uis.no)
[2]Department of Electrical and Computer Engineering, University of British Columbia, Canada (hongbog, vleung@ece.ubc.ca)
[3] School of Computer Science and Engineering, Seoul National University, Korea (minchen@ieee.org)

Abstract. Traditional identification-centric RFID system (IRS) is designed to provide services of object identification/tracing/locating, but it has some shortcomings when encountering a dynamic environment in which the status of the systems and the service requirements of users/objects may change continuously. Very recently a new Code-centric RFID system (CRS), which is far different from the traditional IRS, is proposed to provide on-demand fashion code re-writing and to suit for more flexible user-centric applications. However, at the current stage the there is no secure and efficient scheme to manage the mobile code updating and authentication process in CRS. In this paper, a new scheme is proposed to provide efficient and dynamic mobile agent code updating management. In addition, to prevent the CRS system form possible attacks from malicious users, an IDPKC-based digital signature generation and authentication protocol is proposed.

Keywords: RFID, Code-centric, Code updating and authentication.

1 Introduction

Radio frequency identification (RFID) is a wireless communication technology for automatic object identification, and it has been receiving more and more attention [6, 9]. In general, an RFID network consists of some readers and many low-cost tags. Each reader is connected with a certain data base that storages the information of the objects. Each RFID tag is programmed with a unique identification (ID). The ID is the information of some object, and the tag is attached to the object. The ID points to some storage of the database. The reader communicates with the tag in a wireless way and collecting its ID. Then the object is recognized by the reader checking the data base that the reader is connected with. RFID tags can be categorized into passive, active, and semi-active (or hybrid) tags, depending on whether they require batteries for operation. On the other hand, RFID tags can also be distinguished depending on their data storage capability: read-only tags or read-and-write tags.

The current RFID system, referred as traditional identification-centric RFID system (IRS) is designed to provide such services as object identification, tracking or

locating. In a dynamic scenario, IRS presents apparent limits. To deal with such dynamic circumstances, very recently a Code-centric RFID system (CRS) [2] is proposed to provide a smart on-demand action for different objects in different situations. As a new concept and new system, the current CRS need some new secure and efficient scheme to manage its mobile codes updating and to provide mobile codes authentication.

The rest of this paper is organized as follows. In Section II the code-centric RFID system (CRS) is reviewed and compared with the traditional IRS RFID system, where particularly the current mobile agent code updating process in CRS is discussed. In Section III the proposed new mobile agent code updating scheme is introduced. In Section IV we discuss how to use an IDPKC-based digital signature generation and verification method to protect the system from security. Section VI concludes this work.

2 Agent based Code-centric RFID system

This section first describes the current CRS system, and then demonstrates possible security threats onto CRS.

2.1 Introduction of Code-centric RFID System (CRS)

The existing RFID system can be summarized as identification-centric (IRS) RFID system. Generally, it utilizes passive information about the object, i.e., the ID information stored in the tag. Then the corresponding action decision is made upon a pre-established database. In IRS RFID system, the applications mainly help answer "where" and "what" questions, such as "where is the object (e.g., a person)" and "who is the person (e.g., the tag serves as electronic passport, and the person's age or marriage status is recorded in the tag memory)". However, the static database cannot be updated in a real-time way for new object types. When information changes, an object database synchronization problem occurs. Thus, the object's profile database must be setup to allow for interactions between a RFID tag and a profile database before the tag is manufactured. If an emergent situation appears and the network access from the reader to the database is blocked, the object identification function of RFID will be also blocked. As a solution for such problems existing in IRS, CRS [2] incorporates code information that is dynamically stored in the RFID tag. It facilitates on-demand actions for different objects in different situations. It is the mobile agent codes that are encoded in the RFID tags, while not simply the static ID. Mobile agent specifies up-to-date services. Furthermore, a high-level language for coding mobile agents is stored in the RFID tags, and the agents will be interpreted by a corresponding middleware layer in the RFID reader. By using this mobile agent-based RFID tag, an object indicates the system to intelligently execute actions in response to the occurrence of specific situations. When the service requirements are put into an RFID tag in one location, the target would be realized in another location through code-centric processing. Fig. 1 shows CRS concept, where CRS extends RFID

message format for the tag. In addition to the traditional tag data (identification information or ID), a mobile agent (code) is stored in the tag.

Fig.1. Extended RFID message in CRS

The mobile code will be changed or re-written in an on-demand fashion so as to provide on-demand quality of service. Usually, the goal of the updating action is some operation or adjusting according to the changing surrounding environment. Particularly when the tag is attached onto a non-human object, this object will have no intelligence to update code by itself. As a result, some other malicious devices or attackers get opportunities in the updating, and the security problem emerges in the updating stage. To sum up, a security mechanism for the updating process of the CRS agent based tag is a critical issue.

2.2 Problems about Mobile agent code updating

One of the most important characteristics of CRS system is that the memory of each tag in this system consists of two parts: original fields and extension fields as shown in Fig.1. Original fields include identification information and description information, which will not be changed. Extension fields that include code priority and mobile agent can be re-written in an on-demand fashion to provide on-demand quality of service.

There are three kinds of code updating modes: passive mode, active mode, and hybrid mode.

(1) *Passive Mode:* In RFID systems, the tag can be generally attached to human and non-human objects (e.g., product, animal, etc.). Non-human objects are not intelligent enough to update agent codes by themselves.
(2) *Active Mode:* If the object is a human being, then he/she may have specific requirements on service types and qualities. These users can update the codes actively by themselves through portable RFID readers.
(3) *Hybrid Mode:* This is the combination of both passive mode and active mode.

In current CRS system,there is no security scheme to manage this codes updating procedure. As a result, there exist some possible security threats in CRS system.

(1) Denial of service attack
Because RFID tag has limited memory and there are no efficient schemes to manage mobile codes updating, malicious users can launch denial of service attack by writing a large amount of mobile codes into tag memory. If the memory is full, new updating codes from tag user cannot be written into tag memory anymore..
(2) Unauthorized access attack

In a CRS system, updating mobile codes may come from different readers. The system must ensure that readers do not update and modify the mobile code if they have no authorization to access to the mobile codes. Otherwise, malicious attackers are able to use a reader to write malicious codes into tag memory or modify the original code. Malicious codes like a virus may cause system failure, whereas modified codes with wrong information may bring loss or inconvenience for tag owners.

3 Mobile agent code updating scheme

In this part, a modified tag data structure and a proposed mobile agent code updating procedure is proposed to solve the problems in the current CRS system.

3.1 Modified tag data structure

In order to manage mobile agent code updating procedure, a new RFID tag data structure is proposed. In this new tag data structure, a code update time and a digital signature are added for each mobile agent code as shown in Fig. 2. Digital signature will be generated from this mobile agent code by tag owner. The detail of digital signature generation will be introduced in part IV.

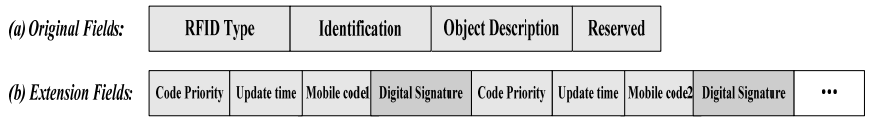

Fig.2. Modified RFID tag data structure in CRS

3.2 Mobile Agent code updating procedure

When a new mobile agent code comes if the tag has enough free memory for this code, this code will be written into tag's memory. On the other hand if there is not enough free memory, the code may be discarded, not written into tag memory, and not sent to the code information manager. In this section, we propose a new scheme to manage this mobile agent code updating process as shown in figure 3. Given that tags are usually low-cost and without enough computation resource to perform digital signature verification, the proposed mobile agent code updating management scheme are designed to be performed by RFID reader.

(1) The Reader reads all the tag information from tag memory, which includes both the original fields and extension fields.
(2) The Reader checks if there is enough free memory for the new coming code. If yes, reader will write this code into memory of this tag.
(3) If there is not enough free memory for this new code, the reader will check the codes stored in the memory one by one and erase the codes that are not from this tag's owner. Here the code checking process is a code authentication process,

which recognizes whether this code is from owner of this tag. An IDPKC-based digital signature generation and verification scheme is used.

(4) If there is still not enough free memory for the new code, reader will compare the processing priority and update time of all codes to make sure that codes with higher processing priority and new update time will be stored in the tag memory.

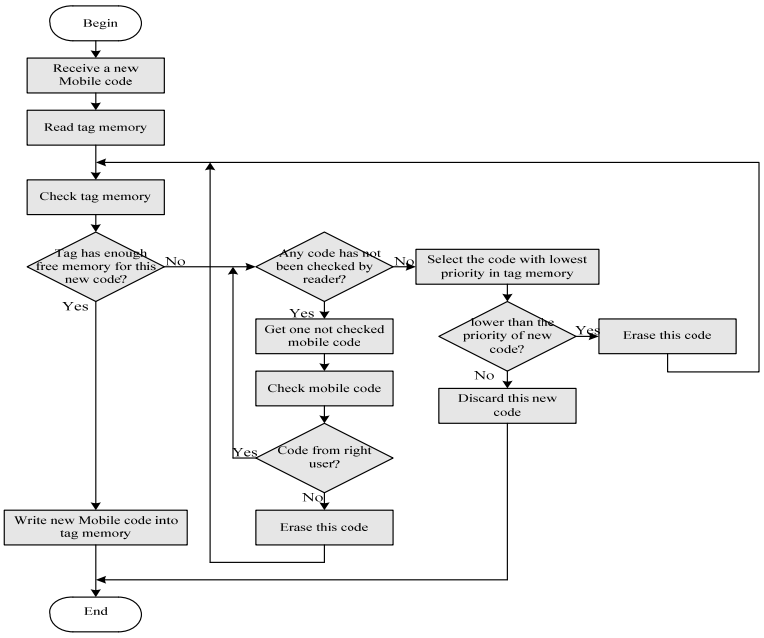

Fig.3. Mobile Agent code updating procedure

By comprehending this new mobile agent code updating procedure into the current CRS system, the code from the right tag owner will be kept in tag's memory with high processing priority and new update time.

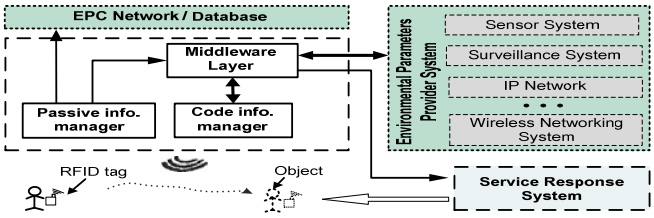

Fig.4. Functional components of CRS

From Fig. 4, we see that when a reader reads the tag memory, the identification and description data will be sent to the passive information manager. The mobile agent code is forwarded to the code information manager, which will deliver the agent

to the middleware layer for interpreting. By way of this agent code updating protocol, the new code from the tag owner is appropriately updated. But it cannot make sure that all codes are from the tag owner. In order to avoid this, each code should be authenticated when it is read. A fundamental technique for demonstrating the authenticity and integrity of a mobile code is to use a signing code. Typically, mobile code signing involves a public key cryptography. In a Public Key Infrastructure (PKI) system, the public keys are made publicly available by using of certificates. To sign a code, the code should first pass through a hash function to generate a code digest, and then the digital signature is generated by encrypting this code digest with the singer's private key. Because both the private key and the code digest are unique, this digital signature authenticates not only the origin of the code but also the code integrity. In a CRS system, each mobile code has a digital signature and this digital signature will be generated by the owner of the tag and be written into the tag memory together with this mobile code. Although this traditional PKI system is widely used in some mobile agent systems [3, 4, 5, 8], it has some drawbacks in certificates and public key management and is not suitable for this CRS system. In this paper, an Identity-based Public Key Cryptography (IDPKC) is adopted to provide digital signature generation and verification service in CRS system.

4 IDPKC-based digital signature and verification

4.1 IDPKC-based digital signature and verification

In a CRS system, a digital signature scheme is adopted to authenticate the integrity of a mobile agent code and to verify whether a mobile agent code is from the tag owner. Normally, a digital signature scheme typically employs a type of public key cryptography and consists of three parts. Each part is described by an algorithm:

(1) Key generation algorithm that generates a private key and a corresponding public key for the user.
(2) Signing algorithm that generates a digital signature from a digital message with user's private key.
(3) Signature verifying algorithm that authenticates the received message with message, user's public key and digital signature.

In [7], an IDPKC-based signature generation and verification scheme is introduced. The key generation center uses sender's identity to generate a signature generation key and pass this key to sender. Digital signature will be generated using this signature generation key and this message. This digital signature can be verified with the signature verification key that is generated from sender's identity.

4.2 Identity-based digital signature and verification in CRS

In a CRS system, an IDPKC-based digital signature generation and verification scheme is used for the reader to authenticate the integrity of a mobile agent code and if a mobile agent code is from the right tag owner or not. The process of this IDPKC-based digital generation and verification is shown in Fig. 5.

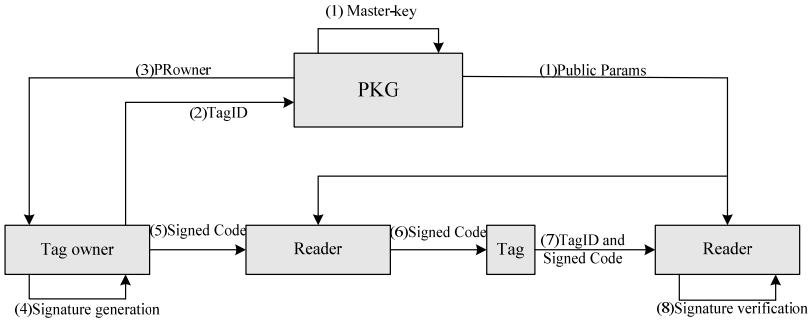

Fig. 5. IDPKC-based digital signature generation and verification in CRS system

(1) PKG generates a master-key and public Params and sends public Params to the readers.
(2) Tag owner sends the tag identity (TagID) to PKG.
(3) PKG generates a private key for this TagID and it to the tag owner.
(4) Tag owner hash mobile agent code to generate a hash code.
(5) Tag owner uses the private key to encrypt the hash code and gets a digital signature for this mobile agent code.
(6) Tag owner sends this mobile agent code together with its digital signature to a RFID reader.
(7) Reader writes this mobile agent code and its digital signature into the memory of the tag.
(8) Reader reads the TagID and signed code from tag memory.
(9) Reader uses TagID and Public Params to generate the public key of this tag and uses this public key to verify the digital signature.

Compared with traditional PKI system, the advantages of using IDPKC-based digital signature generation and verification scheme in a CRS system are:

(1) One important advantage of IDPKC system is that if there is only finite users in the system, the private key generator can be destroyed after all users have been issued with their private keys.
(2) Scalability becomes a significant concern with a growing number of RFID tags whose associated information needs to be stored in the database. Failures in the database and/or networking infrastructure may render the system unusable. Therefore, in a CRS system, in order to realize the system decentralization, the mobile code processing is performed locally by an interpreter attached to the RFID reader and the RFID reader does not need to be connected with the backend database.
(3) One inherent disadvantage with PKI is the management of the certificate and associated key. Fortunately IDPKC can overcome this problem because it allows a user to generate the public key of any user without having to search a directory or request a copy of its key from the user..

(4) Another advantage of using IDPKC for digital signature verification is the system can develop more lightweight implementations at the reader. This is because the reader need not store separate certification, identification and keying information to generate the verification key.
(5) IDPKC offers a useful feature by adding additional information to the tag identity. For example, a tag user can specify a code expiration data and use this timestamp and tag identity to generate the private key and public key.

5 Conclusion

In this paper, we first reviewed the traditional identification-centric RFID system (IRS), some disadvantages of IRS in dynamic environments, and a recently emerged code-centric RFID system (CRS). Based on the review, we analyzed some mobile updating modes and their problems with current mobile code updating procedure in a CRS system. To solve these problems, a new mobile code updating protocol is proposed. By way of this proposed protocol, CRS guarantees that the mobile codes from the right tag owner or from the tag owner with higher processing priority not be discarded, especially when free tag memory is not enough for a new coming mobile code. In order to prevent the system from being attacked by malicious users and protect the tag owner's rights and interests, we propose the code authentication adopts singed code. In the IDPKC-based digital signature generation and authentication scheme, any RFID reader can generate the verification key from the tag identity and it is more suitable for our CRS system compared with traditional PKI based approach.

References

1. D. Boneh and M. Franklin. "Identity-based encryption from the Weil pairing," Advances in Cryptolog, CRYPTO2001, volumen 2139 of LNCS, 213-219(2001)
2. M. Chen, S. Gonzalez, Q. Zhang, and Victor Leung, "Code-Centric RFID System Based on Software Agent Intelligence, " IEEE Computer Society, March/April 2010 (Vol, 25 no.2) 12-19(2010)
3. Robert S. Gray, "Agent Tcl: A Flexible and Secure Mobile-Agent System, "Proceedings the of Fourth Annual Tcl/Tk Workshop (TCL 96), 9-23, (1996)
4. G. Karjoth, Danny B. Lange, and M. Oshima, "A Security Model For Aglets," IEEE Internet Computing, 68-77(1997)
5. Foster N. Karnik, "Security in Mobile Agent Systems," Ph.D. Dissertation, Department of Computer Science, University of Minnesota, (1998)
6. B. Nath, F. Reynolds, and R. Want, "RFID Technology and Applications," IEEE Pervasive Computing, vol. 5, no. 1, 22-24(2006)
7. A.Shamir. "Identity-based cryptosystems and signature schemes," In Advances in Cryptology – CRYPTO '84, volume 196 of *LNCS*, pages 47-53. Springer-Verlag,(1984)
8. J. Tardo and L. Valente, "Mobile Agent Security and Telescript," Proceedings of IEEE COMPCON'96, Santa Clara, California, pp. 58-63, February 1996
9. Http://www.rfid.org/