개인 물품 관리 지원 모바일 RFID 시스템

정회원 김 태 성*, 손 경 호*, 윤 강 진*, 종신회원 김 영 용**

A Management Method for Personal Purchases in Mobile RFID System

Tae-sung Kim*, Kyung-ho Sohn*, Kang-jin Yoon* *Regular Members*,
Young-yong Kim** *Lifelong Member*

요 약

RFID 시스템은 무선 전송을 이용하여 물건을 인식하도록 하는 시스템이다. RFID의 응용분야는 그 범위가 매우 다양하고 폭넓은데 그 중 가장 활발하게 적용되는 응용분야는 기업의 공급망 관리이다. 현재는 기업이 RFID 태그가 부착된 물품을 개인에게 판매한 후에는 보안상 문제와 차후 관리의 어려움을 이유로 RFID 태그를 제거하거나 Kill 태그 명령을 내려 RFID 태그의 기능을 정지시킨다. 하지만, 본고에서는 RFID가 부착된 물품이 개인에게 판매되어 소유가 이전될 때 물품의 정보를 전자상품 코드정보 서비스 표준(EPCIS) 서버로부터 개인 물품 관리 서버로 이전하는 시스템 구조를 제안한다. 이 방법을 사용하면 태그를 제거하지 않고도 프라이버시 침해 없이 개인 물품을 관리 할 수 있다. 또한 개인 물품의 위치관리와 그룹관리가 용이한 개인물품관리서버를 제안한다.

Key Words : RFID System, Middleware, EPC, EPCIS

ABSTRACT

Radio frequency identification(RFID) system can identify an object using wireless transmission. RFID applications are numerous and far reaching. The most interesting and widely used applications are supply chain management for companies. Currently, RFID tags must be detached or killed for security and privacy reasons when tagged objects are purchased. In this paper, we present a new architecture that transfers information about products from the electronic product code information services (EPCIS) server of a company to an individual's personal purchases management (PPM) server when products with RFID codes are sold. It solves the security and privacy issues without detaching the tag. Moreover, the PPM server described in this paper allows customers to handle the expiration dates, updates, location management, and group management of products.

Ⅰ. Introduction

Radio frequency identification (RFID) has uses in a variety of applications, including supply chain management, retail[1], and security[2]. As RFID tags continue to decrease in price while offering increased capabilities, manufacturers can manage their products more efficiently.

A RFID system is a chip built into a tag attached to manufactured goods that contains

※ This research was supported by the MKE(Ministry of Knowledge Economy, Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment) (IITA-2008-C1090-0801-0038).
* Yonsei University, Electrical and Electronic Engineering, Wireless & Internet Lab (xinia0214@yonsei.ac.kr)
** Yonsei University, Electrical and Electronic Engineering, Wireless & Internet Lab (y2k@yonsei.ac.kr)
논문번호 : KICS2009-10-505, 접수일자 : 2009년 9월 15일, 최종논문접수일자 : 2010년 2월 8일

information about the whole process of production, distribution, storage, and expenditure. In particular, it connects products with computer networks. The EPCglobal, which was proposed by the MIT AUTO ID CENTER, contained a system architecture for using Internet-based RFID technologies. RFID tags store only minimum information, such as an EPC code (product identification code), and uses product-related specification information that can be located using the Internet. Until now, RFID has mainly been used by companies for applications such as supply chain management, safety management, and distribution management. However, as RFID technology advances, it will find personal uses in addition to its corporate applications. People will manage their purchases with RFID tags connected to the Internet. The RFID system will tell people where their purchases are and what information they need. However, before those applications can reach widespread use, problems of privacy and security must be addressed. RFID information protection technology, such as Tag password, encryption[3], blocking[4] and key distribution, are progressing. However, those methods are cost ineffective or highly complex. Therefore, we propose a new method for managing personal purchases in RFID system by simply adding a personal purchases management(PPM) server. We present an architecture that transfers information about products from a company's electronic product code information services(EPCIS) server to an individual's personal purchases management (PPM) server when products with RFID codes are sold.

We show background materials in section 2, summarizing the EPCglobal network and privacy issues that arise from the deployment of RFID system to PPM. Then we introduce the proposed system architecture and PPM server in sections 3 and 4, respectively. Finally, we provide a conclusion in section 5.

Ⅱ. Related Works

2.1 EPC network

The EPCglobal network is a method for using RFID technology in the global supply chain by using inexpensive RFID tags and readers to pass electronic product code (EPC) numbers and then leveraging the Internet to access large amounts of associated information that can be shared among authorized users. There are five components of the EPCglobal network[5].

1) EPC: A unique number identifies a specific object in motion in the supply chain.

2) ID system: The ID system consists of EPC tags and EPC readers. EPC tags are RFID devices that contain a microchip and an antenna attached to a substrate. The EPC is stored on this tag, which is applied to cases, pallets and/or items. EPC tags communicate their EPCs to EPC readers using RFID. EPC readers communicate with EPC tags via radio waves and deliver information to local business information systems using EPC middleware.

3) EPC middleware: EPC middleware manages real-time read events and information services (EPCIS) and company's other existing information systems. EPCglobal is developing a software interface standard for services enabling data exchange between an EPC reader or network of readers and information systems.

4) Discovery services: A suite of services that enables users to find data related to a specific EPC and to request access to that data. The object naming service (ONS) is the one component of discovery services.

5) EPC information services (EPCIS): EPCIS enables users to exchange EPC-related data with trading partners through the EPCglobal network.

2.2 Privacy threats in RFID system

The majority of consumers today and for the foreseeable future will come in direct contact with EPC tags only if they are buying cases of goods from a retailer who uses the EPCglobal network. It will take some time before item-level tagging is implemented on a large scale, and thus consumer contact with EPC tags will remain limited until that point. This provides the necessary time to properly analyze any perceived privacy risks associated with EPC-tagged objects owned by consumers and to develop appropriate strategies for addressing those concerns.

For example, in a shopping mall, a seller usually eliminates the RFID tag from an article or stops its function with a “kill tag” order after selling it because of security problems or control difficulties. If a RFID tag is active without security after being sold, other people could get a lot of information about the article, which would violate the owner’s privacy. To solve this privacy problem, the MIT AUTO ID CENTER, which is having proposed the EPC code, presents a method to stop the function of an RFID tag with an 8-bit “kill tag” order. However, disabling the tag is also a significant disincentive for businesses because they can no longer access RFID data, which limits marketing opportunities. To solve the privacy issues, several methods have been proposed[6].

Tag passwords: A tag could emit important information only if it receives the right password. The paradox here is that a reader can’t know which password to transmit to a tag unless it knows the tag’s identity.

Encryption: Encrypting a tag identifier seems to be a good solution to address problems of privacy, but it does not solve all problems because the encrypted identifier is itself just another identifier. This method is also expensive.

Blocking: A blocker tag prevents unauthorized scanning of tags mapped into the privacy zone[6]. But blocker tags need a circuit modification.

Those methods are cost ineffective or highly complex. Therefore, we propose a new method for managing personal purchases in RFID system by simply adding a personal purchases management(PPM) server.

Ⅲ. Proposed RFID system

3.1 Personal purchases management RFID system

We introduce the overall construction of support for personal purchases management RFID system in Fig. 1. At first, we apply the identification of persons to the existing RFID system. Identification of persons consists of an ID RFID tag and an ID EPCIS server. To classify who possesses the tagged item, we should identify the person with an RFID tag called an ID RFID tag.

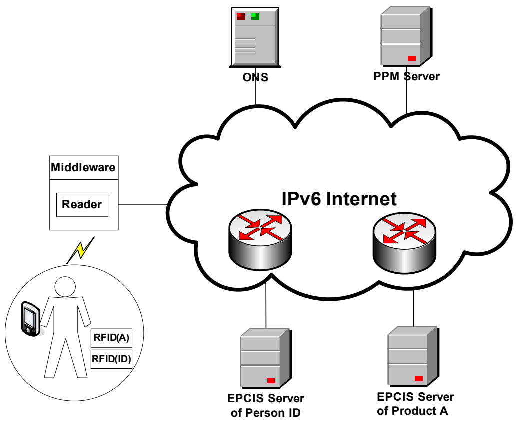

Fig. 1. Personal purchases management RFID system

ID RFID tag uses a tag blocker in order to avoid being read by unrelated reader. As the EPCIS product server has the information about the product, the person ID EPCIS server has the information about the person corresponding to each ID. However, it has only the URL information for the PPM server corresponding to each person. The ID EPCIS server should have confidentiality, authentication and integrity for all middleware queries about the URL of a PPM server. To manage a product at the item level, each consumer will need a PPM server. Just as e-mail service requires an e-mail account in its server, personal purchases management needs either a centralized or distributed PPM server. This PPM server registers the reader of the owner and the tag while transferring possession after buying. We assume a person has a mobile RFID phone supported by MIPv6, equipped with an RFID reader and Internet access.

3.2 Signal flow of transferring information about products

As shown in Fig. 2, the procedure of transferring information about a product uses the following steps.

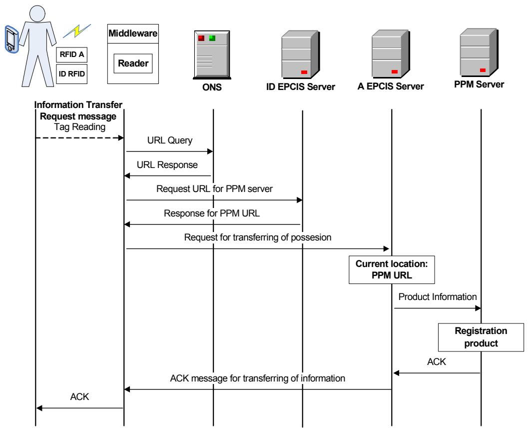

Fig. 2. Procedure of transferring possession

1) At the cash desk, a reader reads the RFID tag of product A and the buyer's ID RFID tag.

2) Middleware generates the procedure to transfer possession. It sends a URL query for both RFID tags to the ONS for the receiving URL of the EPCIS servers.

3) After the middleware gets the URLs, it sends a message to the ID EPCIS server for the receiving URL of the PPM server.

4) After the middleware gets the URL of the PPM server, it sends an information transferring request message to the EPCIS of the product. The message includes the URL of the PPM server.

5) The EPCIS of product A records the ownership of the product to the URL of the personal purchases server, and then it sends the product information data to that PPM server.

6) The PPM server saves the product information and sends ACK message to the EPCIS of product A.

7) The EPCIS of product A sends ACK message to the middleware for completion of information transferring.

8) The middleware delivers ACK message to the buyer.

When a buyer registers several products simultaneously, the steps of products information transferring are as follows. For example, a man purchases 3 products such as shaver, MP3 player, and milk at major supermarkets. In order that he registers 3 items in his PPM, the procedure of transferring possession from step2 to step7 is performed repeatedly by each item. In step 8, after the middleware receives all ACK messages from three EPCISs, it sends one ACK message to the buyer. To save wireless resources, three EPCISs send ACK messages to buyer through middleware not directly. Throughout the procedure of transferring possession, unauthorized users who try to access the EPCIS service can not obtain the information about the product because the EPCIS server has recorded the possession of the product. The role of the middleware is important because it makes the possession transfer procedure possible without an additional hardware system. The software platform on the middleware requires not only existing generic RFID functions but also information transferring functions such as getting URLs, authentication with the ID EPCIS, information transfer requests, and event notification.

3.3 EPCIS data

EPCIS data[7] can be divided into two big categories. First, static data, which does not change over the life of a physical object, includes class-level static data and instance-level static data. Second, transactional data, which does grow and change over the life of a physical object, includes instance observations, quantity observations, and business transaction observations. Among the five data categories, the EPICS sends class-level static data, instance-level static data and instance observations to the PPM server when it transfers information about the product. Quantity observations and business transaction observations are useless in a PPM server because they are related to product management in a company. Instance observations, which record events such as time, location, one or more EPCs, and business process step, are just recorded at the final location to the PPM server's URL. Class-level static data, which is the same afor all objects of a given class, is required to classify the personal purchases in a PPM server. Instance-level static data, which includes such things as date of manufacture, lot number, expiration date and so forth, is needed to manage the product using the PPM service.

Ⅳ. Personal purchases Management Server

4.1 Personal purchases Management Server

Fig. 3 shows the function of the PPM server. PPM server manages registered personal RFID readers and RFID tags. Throughout the possession transfer procedure, tags are registered in the PPM server. Variable RFID readers belonging to a person will be also registered to his or her PPM server. For example, a refrigerator that manages the freshness of the food and a home-automation server that maintains updated services for home digital devices and a mobile RFID reader that manages the tags in its sensing range can all be registered to a single PPM server. A scheduling function based on instance-level static data from the EPCIS and context-aware event management sends alarm messages about expiration dates to the registered RFID reader based on a time scheduling table. In case of registered product is milk, it is classified food according to a static data. PPM gets storage method and expiration time of milk from instance observation. Based on this, PPM server makes the time scheduling. Context-aware event management sends alarm messages to the refrigerator based on a time scheduling table.

For a mobile RFID system, RFID tag location is measured by the RFID reader because RFID tags do not have communication modules. Therefore, a registered RFID reader sends the location of tagged items in its sensing range.

A group management function groups all tagged item by current location and item class. Current location is based on the address of a subnet of MIPv6, and item class is based on class-level static data from the EPCIS.

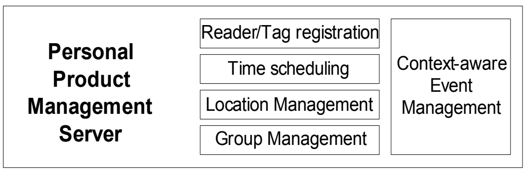

Fig. 3. Personal Purchases Management Server

The PPM server can be either a centralized server system similar to an e-mail server or a distributed server system similar to a home-automated server.

4.2 Group location management

The IETF Network Mobility (NEMO) WG is defining requirements and developing NEMO standards[8]. We are easily handling group location management using a NEMO protocol with MIPv6. The RFID tags in the sensing rage of a personal mobile reader can exploit the group mobility management. The mobile reader, as a group leader, manages the location information of the RFID tags in its sensing range. When a person moves from one sub-network to an adjacent one, the mobile reader obtains the address of the new sub-network using MIPv6, and then it sends a new address and information about the RFID tags to the registered PPM server. Using that procedure, the PPM server can manage group mobility and track the location of its RFID tags. When a person moves into an adjacent sub-network leaving a tagged item behind, the PPM server sends a lost message to the person.

Ⅴ. Conclusion

This paper proposes a method to support an item-level RFID system without changing current network protocols or system architecture. Our proposed system transfers the information about products from the EPCIS server of a company to a PPM server when products with RFID codes are sold. The system makes it possible for customers to handle expiration dates, updates, location management and group management of products. RFID will become more useful by allowing customers to use RFID tags after buying products. Location management and group mobility management of products can be performed easily because the system is based on MIPv6. In the future works, we need to supplement proposed system in diverse circumstances such as rental, gift, and take back.

References

〔1〕 George Roussos, "Enabling RFID in retail" Volume 39, Issue 3, March 2006 Page(s):25-30 Digital Object Identifier 10. 1109/MC.2006.88.

〔2〕 T. Phillips, Karygiannis, R. Kuhn, "Security Standards for the RFID Market", Security & Privacy Magazine, IEEE Volume 3, Issue 6, Nov.-Dec. 2005 Page(s):85-89 Digital Object Identifier 10.1109/MSP.2005.157.

〔3〕 K. P. Fishkin and S. Roy, "Enhancing RFID Privacy via Antenna Energy Analysis", IRS-TR-03-012, Intel Research Seattle.2003.

〔4〕 A. Juels, R. L. Rivest and M. Szydlo, "The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy", In Proceedings of 10th ACM Conference on computer and Communications Security(CCS 2003), 2003.

〔5〕 http://www.epcglobalinc.org/about/media_centre/Network_Security_Final.pdf

〔6〕 L. Hyanjin, K. Jeeyeon, "Privacy threats and issues in mobile RFID", Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on 20-22 April 2006 Page(s):5 pp. Digital Object Identifier 10.1109/ARES.2006.96

〔7〕 K. Traub, G. Allgair, H. Barthel,"The EPCglobal Architecture Framework", EPCglobal Final Version of 1 July 2005, http://www.epcgloblinc.org/standards/Final-epcglbal=arch-20050701.pdf.

〔8〕 http://www.ietf.org/rfc/rfc3963.txt"Network Mobility (NEMO) Basic Support Protocol"

김 태 성 (Tae-Sung Kim) 정회원

2004년 2월 연세대학교 전자공학과 학사졸업
2004년 3월~현재 연세대학교 전자공학과 석박사 통합과정
<관심분야> 차세대 이동통신 시스템, Multicast 전송기법

손 경 호 (Kyung-Ho Sohn) 정회원

2002년 2월 연세대학교 전자공학과 학사졸업
2004년 2월 연세대학교 전자공학과 석사졸업
2004년 3월~현재 연세대학교 전자공학과 박사과정
<관심분야> Radio Resource Management, 차세대 네트워크, Multicast System

윤 강 진 (Kang-Jin Yoon) 정회원

2004년 2월 연세대학교 전자공학과 학사졸업
2006년 2월 연세대학교 전자공학과 석사졸업
2006년 3월~현재 연세대학교 전자공학과 박사과정
<관심분야> Self-organizing 네트워크, Femtocell 네트워크

김 영 용 (Young Yong Kim) 종신회원

1991년 2월 서울대학교 전자공학과 학사 졸업
1993년 2월 서울대학교 전자공학과 석사 졸업
2000년 2월 University of Texas at Austin 전기컴퓨터공학과 박사 졸업
1998년~2000년 Telcordia Technologies 연구원
2000년~2005년 연세대학교 전기전자공학부 조교수
2005년~현재 연세대학교 전기전자공학부 부교수
<관심분야> 차세대 이동통신 시스템, 차세대 인터넷