RFID Privacy Using User-Controllable Uniqueness

Inoue, Sozo
System LSI Research Center, Kyushu University

Yasuura, Hiroto
System LSI Research Center, Kyushu University

RFID Privacy Using User-controllable Uniqueness

Sozo INOUE*
sozo@c.csce.kyushu-u.ac.jp

Hiroto YASUURA*
yasuura@c.csce.kyushu-u.ac.jp

Abstract

In this paper, we propose two approaches to protect privacy in the 'Digitally Named World', which is the environment in which 'radio frequency ID's (RFIDs) are attached to any objects in the world, and any objects in the real world can be found by the readers of the RFIDs and the networked database system. One is the approach to conceal the permanent ID under a private ID that users give. The other approach is to assign partial ID sequence to a object, and the rest is given by user-assignable RFID tags. These approaches both attempt to give users the controllability of the uniqueness of IDs from local to global, thereby enabling IDs private or public ones in the required stage of the object's life cycle.

1 Introduction

Recent years' advances in information technology and system LSI technology are penetrating computing resources into ubiquitous places in the real world[4].

Our vision of the future world is the *Digitally Named World*, which is the environment in which 'radio frequency ID tags' (*RFID tags*) are attached to any goods in the world, they can be found anytime via the readers of the RFIDs and the networked database system, and they can be managed throughout their life-cycle. RFID tags are silicon chips with their IDs, radio frequency functions and some additional logic and memory[2]. Most of the RFID tags are supplied with power through radio frequency communication from external readers.

In this paper, we address the problem of privacy in the digitally named world where objects are identified throughout the life cycle, and propose two approaches to protect privacy. The digitally named world can provide highly efficient object management, and will be widely spread, since the application area lies in any domains related to real objects[3]. However, privacy problem is important in the ubiquitous computing world. Careless disclosure of the relationship between a user and an object leads to the privacy invasion.

One of our approaches is to conceal the permanent ID under a private ID that users give. The other approach is to assign partial ID sequence to a object, and the rest is given by user-assignable RFID tags. These approaches both attempt to give users the controllability of the uniqueness of IDs from local to global, thereby enabling IDs private or public ones in the required stage of the object's life cycle.

In the rest of the paper, Section 2 addresses the basic architecture and privacy issue in the digitally named world, and Section 3 describes the methods we propose for protecting privacy in the digitally named world. Section 4 is a conclusion.

[a] System LSI Research Center, Kyushu University 6–1 Kasuga-Koen, Kasuga-Shi, Fukuoka 816-8580 JAPAN

2 Object Identification throughout the life cycle

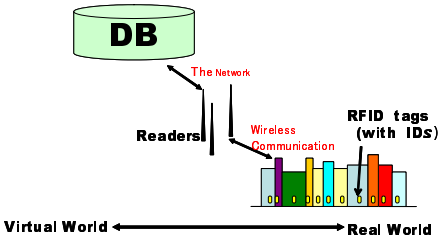

Figure 1: The system architecture

For the digitally named world, we assume the system as briefly shown in Figure 1. In the figure, the RFID tag attached to an object communicate with readers connected to the network. The system architecture we assume above, in which RFID tags have an ID and readers are connected to the network, is considered to widely spread to the world, and close architectures are assumed also in [8, 13].

Figure 2: The life cycle of an object

One of the fundamental features in the digitally named world is the object identification throughout the life-cycle of the object as illustrated in Figure 2. Efficient recycling of an object is realized by embedding the information about the recycling or reusing the object such as materials, how to retrieve the materials, or how to disassemble. Current tagging techniques such as bar-code systems do not manage such information, because of the limitation of the record size and the limitation of the communication distance up to nearly contacted communication.

To our desirable point, object identification throughout the life cycle can contribute to reduce the practical cost of RFID tags, since the cost of the RFID tag attached to an object throughout the life-cycle can be shared by multiple services. Each service, such as manufacturers, distributors, shops, users, and recycling merchants, pay less money if one RFID tag is attached to an object for long time. Thus, object identification throughout the life-cycle of the object is the fundamental feature that strongly promotes digitally naming world.

2.1 Privacy of an ID itself

In the digitally named world, objects passively have abilities to communicate with RFID tags, whereas the contents of the communication can leak to a third party. However, the system can not invade the privacy of the inhabitants in the digitally named world, even if the communication with an object leaks.

The private information leaks either only via the wired network or involving the communication between an RFID tag and a reader. We focus on the latter problem, since the former problem can be solved in a similar way to the old-fashioned computer networks, such as data encryption.

For the latter problem, placing private information on the memory in an RFID tag, such as writing a credit card number, is obviously dangerous and therefore should be avoided,

since the communication with RFID tags can be easily tapped. Furthermore, other cases related to the latter problem appears, which are unique to the digitally named world:

A. The relationship between the ID of an object and its user is known to a third party through the database system on the network.

B. A user is detected through observation from the real world, such as the location or the shape of an object.

C. The user's behavior becomes clear from the identification history of an ID from one/several reader(s).

These cases lead to the result that the user is monitored, or traced by the third party who can obtain the information of the above two cases.

For A, assume an example of the environment in which readers are located everywhere. After the RFID attached to a product and its consumers are set to be related in a POS (point-of-sale) system, the product can be traced by the readers. This leads to the invasion of the privacy of the consumer, since the consumer will be traced through the location of the product. Although it will be convenient for the consumer if he/she can search the product for his/her own, allowing others to search the product is undesirable from the viewpoint of privacy.

For B, as an example of location, an object located in a private room implies that the object is owned by the resident of the room. Another example, as observation from the real world, if a user walks through a ticket gate embedded with an RFID reader, the gate can detect the object the user accompanies, and a station attendant on the site can relate the object and the user. The attendant cannot detect the name or other private information of the user unless he/she know the information of the commutation ticket, but at least he/she can identify the real entity of the user such as, "Hey, you have such a thing?" These are the relationship between an object and a user, which lead to the same problem in A.

We can easily imagine the case of mixing A and B, in which the products that the person under your eyes can be detected by referring the product-code standards, such as EPC codes by Auto-ID Center[8], or ISO-15963[9] currently discussed, are included in the case A, since the type of a product is deduced from the ID and the standard.

C denotes the problem of leaking the same ID repeatedly even if the relationship between the ID of the product and a user doesn't leak. For example, even if a reward card in a supermarket is not related to the holder, the access of the holder can be traced and used for a POS system. When a product detected in a station is detected in another station, then the movement of the holder of the product can be detected. These are not the matter of *anonymity*, which is the property not to detect the identity of a person, but that of *linkability*, which is the property to detect the movement or the session of a person even if one cannot detect his/her identity[10, 11]. Although linkability must be fomented to be or not to be accepted with social discussion, we can see at least that the damage gets bigger than no linkability when the problem of A or B occurs. For example, if a list of the products and their purchasers leaks, the history of the product shows the purchasers movement.

Moreover, [12] addresses the problem that when the case of B, especially the case of location, and C are compounded, just the existence of an RFID without knowing its ID leads to a privacy problem, such as the movement of a product from a room in which only one RFID with the product exists to the observer's room can be detected from the observer. This im-

plies the problem of population getting small if we consider the location or the observation introduced in B.

2.2 Limitation with low-cost RFIDs

The user can obtain information which relates the object by searching the database system on the network through the ID of the RFID tag. The object and the readers might be placed on the public place many people shares. Therefore, a method to protect users' privacy, that is, "preventing third parties from detecting the user who is related to an object", is necessary. One approach is the authentications for using a reader when a user is to communicate with an RFID tag through the reader. However, this approach is not sufficient to protect privacy, since the following factors can be considered.

- The users who are authenticated to use a reader can communicate with the RFID tags in the zone of the reader. Therefore, the users can identify the objects owned by another person if the objects are located in the zone.

- The users can identify an object on the site with a private reader, which have no authentication to use, even if the reader is not connected to the network.

- The communication between an RFID tag and a reader can be easily tapped, since an encryption is difficult on the current stage. A third party can identify an object by tapping the communication.

Thus, limiting accesses to an RFID tag to the authenticated reader can be assumed to be impossible, and preventing tapping the communication is also difficult.

Weis et. al.[6] proposes the method to realize anonymity and to avoid linkability by embedding hash function and a pseudo-random number generator into RFID tags. This has an advantage that the ID can be automatically changed and that do not need to change it in the secure place as our method. However, the method needs to embed additional circuits for hash function and a pseudo-random number generator, which cost thousands of gates. Even low-cost RFID tags needs privacy protection since the privacy shell chips from thin point.

[7] proposes the idea of blocker tags, which simulates all of the IDs in a desired zone of ID values, and which can selectively protect the zone from being read by malicious readers, with the blocker tag which simulates all of the IDs in the zone. This approach is available in tree-walking protocol widely used in UHF frequency, and is cost effective since RFID tags on objects needs no additional enhancement. Since this approach is to block private information using optional blocker tags, practical requirement that the communication area of a blocker tag must cover that of RFID tags in objects should be solved in the implementation of this approach.

3 Privacy Protection in the Digitally Named World

In this section, two approaches for the privacy problem addressed in Section 3, which is a method for preventing third parties from detecting the relationship between an object and a user, is proposed. The basic concept of these approaches are to give users the controllability of the uniqueness of IDs from local to global, thereby enabling IDs private (without revealing the relationship between the IDs and objects) or public ones in the required stage

of the object's life cycle. Moreover, these approaches try to preserve the clue to recover the permanent IDs, and enable required stage of the object life cycle to get the permanent IDs. This idea can be used on the required stage of the life-cycle. For example, the problem of 1 and 2 is typical in the stage where consumers use the objects, although, the problem is not important in the production, distribution, sale, and recycle stage in Fig. 2. It is rather convenient and totally ecological if the method can be canceled. Proposed mechanism can employ the method as the user needs. The proposed approaches are:

1. to conceal the permanent ID under a private ID that users give onto rewritable memory in an RFID tag, and,

2. assign partial ID sequence to an object, and the rest is split onto other user-physically-assignable RFID tags.

Our approachs selectively use locally-unique ID, instead of losing globally-identifiable IDs. This leads to a problem that an ID conflicts with other IDs in the world. We deal with this problem by using real world information, such as the location/physical shape of objects.

3.1 An approach with rewritable memory

In this section, we describe the 1st method proposed in [1] to restrict object identification to particular users. Figure 3 is the overview of the method.

1. Each RFID tag has a read only memory (ROM) and a rewritable but non-volatile memory (e.g. EEPROM, FRAM).

2. In the ROM, a unique and permanent ID of the RFID tag is set by the producer.

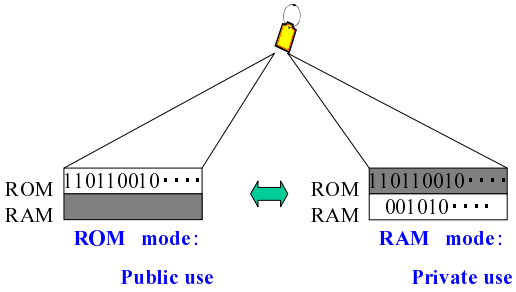

Figure 3: Restriction of identification to limited users

3. ROM and rewritable memory are used only exclusively. A user cannot read the ROM while a value is set to the rewritable memory, and he/she can read the ROM only when the rewritable memory has null value. The *ROM mode*, which is the state that the ROM is readable, and the *RAM mode*, which is the state that the rewritable memory is accessible, are changed by limited users who are allowed to.

For 3, several methods to limit the change the modes exist: to certificate the user for the change, and to restrict the change only via contacted communication or via communication in a short length up to several centimeters. Which method matches the system needs more discussions.

By the method above to limit the accesses to the memories exclusive, the following system manipulation is possible.

- In the ROM mode, unlimited object identification for any users is provided by the identification code of the RFID tag is set to the ROM by the producer.

- In the RAM mode, the restriction of object identification to limited users is

achieved, in which the limited users set a private and temporary identification code which is only known to them to the rewritable memory. That is, the third parties, who is the users other than the limited users, cannot operate the permanent object identification, even if they can know the private and temporary identification code. With the private and temporary identification code, the third parties can not recognize the relation between the code and the object except the visual information about the object which can be obtained by the on-site communication, since the information about the object in the network is distributed accompanying the permanent identification code on the ROM as a key. Therefore, the third parties have nothing to do with the private and temporary identification code. We discuss this further in Section 3.3.

- An RFID tag can be used in both limited and unlimited identification, and they can be switched for the requirements from the services. For example, an RFID tag on an object can provide unlimited identification with the ROM mode for total management at its production, distribution, and sale stage, and can be switched to RAM mode by a consumer when the object is handed to him/her. Afterward, the object can be identified only by the consumer. Moreover, the RFID tag can be switched to ROM mode again by a scrap merchant when the object is discarded, and the merchant can obtain the information about the object from the network with the permanent identification code, and utilize it for recycling. Such a cycle is realized by the double mode of a single RFID tag.
- The limited user who sets a private and temporary identification code can obtain the permanent identification code by once removing the value of the rewritable memory before setting the private identification code onto the ROM, and they can obtain the information of the object from the databases on the network.

3.2 An approach with physical ID separation

The 2nd method is not to use rewritable memory on RFID tags. This approach adopts non-unique IDs for each RFID tag, but achieves locally-unique IDs by combining 2 or more RFID tags. That is, to say, we alternate the rewritable memory in the 1st approach using physically independent RFID tags.

In this method, an RFID sequence for naive assignment for globally-unique ID is divided into two fields as follows (Figure 4).

- *Class ID*: the field which can itself be related to the information of the database or public standards about the information about the object, such as UPC/EAN codes used in barcodes.
- *Pure ID*: the rest of the ID, but which is necessary for the full ID to be globally unique, such as serial numbers or lot numbers.

We can easily see that only a Pure ID cannot achieve global uniqueness because there is a conflict with others, such as the same serial number of different type or company of product.

When the owner of a product in a stage of the life cycle (e.g. a retailer) is to pass his/her ownership to the next stage (e.g. a consumer), he/she takes off the Class ID. For this, several ways can be expected: to kill only the Class ID electrically in the case of holding the both IDs in one RFID tag, or to take off the RFID tag for Class ID in the case of separately assigning

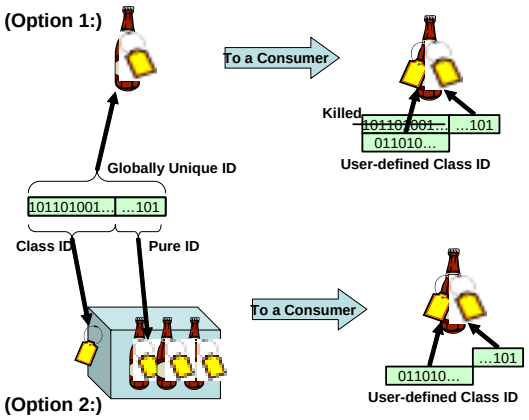

Figure 4: Physical separation of IDs

the both IDs to 2 tags. In the latter case, the Class ID tag can be assigned to the case or the container of the product, a price tag, or an anti-theft tag which are taken off when the product is paid.

The owner of the next stage (e.g. a consumer) prepares RFID tags with several user-assigned Class IDs, in the form of, for example, a sticker. Attaching the tags to the products of his/her own makes the concatenation of his/her ID and the Pure ID an ID which is relatable only for the owner, if he/she desires, to the information of the product. User-assigned Class IDs can be variable according to the privacy and usability the owner desires.

- If the owner assigns his/her ID unique ID for him/her as the user-assigned Class IDs. The concatenation of the user-defined Class ID and the Pure ID can be globally unique, but the owner of the product can be easily guessed. Although there are problems to be discussed, i.e., how to generate the unique ID for the owner, and how to prevent counterfeiting, it is useful when such a case that the product must be traced when it is stolen.
- If the owner assigns user-assigned Class IDs without paying attentions to the others' IDs, the product can not be clear whose product it is except for the owner, and it is easy to achieve local uniqueness by choosing several user-assigned Class IDs not to conflict in the products he/she owns. However, the conflict from the point of global uniqueness still occurs.

Moreover, this method can realize the way to complement global IDs, in the scope of currently socially accepted way of identification, by deducing the Class ID of the product, in such a way of judging the product type through the shape, or scanning the barcode of the product in the stage of a producer recalling it for repairing. This seems to be dangerous from the point of privacy protection as well, but it is more costly than the automatic identification by RFID.

Another merit of the method is the visibility of the privacy control for users, using physically separated multiple RFID tags.

3.3 Discussion

Using the methods shown in Section 3.1 or 3.2, we can prevent the problem, which we addressed in Section 2.1, that the relationship between the ID of an object and its user is known to a third party through the database system on the network, or observation from the real world. For example, a consumer can prevent an object of his/her from being identified by a shop, by setting the value of the rewritable memory or replacing the RFID for Class ID after the shop registers the relationship between the user and the object. Even if the value of the user-defined value is read by a reader by one of the methods shown in Section 2.2, users other than the user who set the

value can not know the relation between the value and the object.

On the other hand, the user who sets the value can know the object, the value, and the permanent ID when he/she sets the user-defined ID. Therefore, he/she can search both of the database about the value of the object on the network and the object in the real world.

Additionally, the system dependability against pretenders and data manipulation can be realized by our method, in the world where readers are ubiquitously spread. By continuously monitoring RFID tags by readers, and by the readers notifying an update of user-defined IDs to its related user, the related user, can detect if it is a manipulation or an update by himself/herself. However, it needs more discussion in the case of semi-ubiquitous readers where readers cannot always monitor RFID tags.

Thus, we can prevent the problem that "the relationship between the ID of an object and its user is known to a third party through the database system on the network", however, this is not enough to prevent the problem that "the user who relates to the object would be detected by the third party". As addressed in C in Section 2.1, we must consider the problem of a combination of B and C, that is, once the private/pure ID is known to a third party, tracing a user by the third party is possible after the relationship between the private/pure ID and the user is known. For the problem, changing the private/pure ID frequently is required and must be worked further.

Conflict management of private/pure ID is also required in such situation in which users frequently change the private/pure ID of objects. One of the simple solutions is to make a particular area of the ID the ID of the user who is related to the object, and to make the rest the user-defined ID for the object. However, this method is not appropriate, since a third party can know the user who is related to the object, and can not prevent the close relationship between the object and the user. For this, we must manage the private ID such as, although applicable only for the 1st approach, hashing the ID including relation to the user, and to design the whole system which is tolerant to a conflict of the private IDs.

4 Conclusion

In this paper, we addressed the privacy issue in the digitally named world, in which objects in the real world can be detectable for computers by RFID tags. In the digitally named world, privacy issue arises when an object and a user are carelessly related. We proposed the method for protecting privacy by each user setting private and temporary identification code to each object. This method enables object management throughout the life-cycle of the object, since the permanent identification code can be utilized at the recycling stage, and therefore contributes to ecology.

Acknowledgment

This work has been supported by the Grant-in-Aid for Creative Scientific Research No.14GS0218 and for Young Scientists No.15700100 of the Ministry of Education, Science, Sports and Culture (MEXT) from 2002 to 2006. We are grateful for their support.

References

[1] S. Inoue, S. Konomi, H. Yasuura, "Privacy in the Digitally Named World with RFID Tags", Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, 2002.

[2] P. Hewkin, "Smart Tags - The Distributed Memory Revolution". IEEE Review (1989).

[3] R. Want, K. P. Fishkin, A. Gujar, B. L. Harrison, "Bridging Physical and Virtual Worlds with Electronic Tags". Proc. Int'l Conf. CHI 99 (1999) pp. 370–377.

[4] M. Weiser, "Some Computer Science Issues in Ubiquitous Computing". Communications of the ACM, 36(7) 1993, pp. 75–84.

[5] Finkenzeller, K. , 「RFID Handbook」, Nikkan Kogyo Pbl. Japan (2001).

[6] S. A. Weis, S. E. Sarma, R. L. Rivest, D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Int'l Conf. Security in Pervasive Computing, (2003).

[7] A. Juels, R. Rivest, M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", http://theory.lcs.mit.edu/ rivest/, (2003).

[8] MIT AUTO-ID Center Homepage, http://www.autoidcenter.org/.

[9] ISO/IEC, SC31, WG2, http://usnet03.uc-council.org/sc31/sc31_wg2.cfm.

[10] D. Chaum, "Untraceable electronic mail, return address, and digital pseudonyms", Communications for the ACM, 1981.

[11] S. Seys, et al., "Anonymity and Privacy in Electronic Services Deliverable 2 - Requirement study of different applications", APES Documents, https://www.cosic.esat.kuleuven.ac.be/apes/

[12] A. R. Beresford, F. Stajano, "Location Privacy in Pervasive Computing", IEEE Pervasive Computing Magazine, pp.48–57, Jan-Mar. 2003.

[13] Ubiquitous-ID Center Homepage, http://uidcenter.org/.