Privacy Enhanced Active RFID Tag

Shingo Kinoshita, Miyako Ohkubo, Fumitaka Hoshino, Gembu Morohashi, Osamu Shionoiri, and Atsushi Kanai
NTT Information Sharing Platform Laboratories, NTT Corporation
1-1 Hikari-no-oka, Yokosuka-Shi, Kanagawa 239-0847 Japan
{kinosita, ookubo.miyako, fhoshino, gembu}@isl.ntt.co.jp,
{shionoiri.osamu, kanai.atsushi}@lab.ntt.co.jp

ABSTRACT
In the coming future ubiquitous society, Radio Frequency Identification (RFID) tags will be affixed to every product and person. This technology is anticipated to be a key technology that will be utilized by various ubiquitous services where these tags will be used to identify things and people and will automatically take advantage of contextual information such as location. On the other hand, a problem is arising where the excellent tracking ability of RFID is abused and personal privacy is being violated. This paper clarifies the active tag privacy problem and proposes a method for protecting personal privacy regarding the active RFID tags. In the proposed method, re-encryption technologies are used to make the tag ID variable. Since variable IDs generated from one ID are cannot be linked to one another by third parties, RFID privacy problems based on a fixed ID can be abated. Furthermore, we introduce an active tag prototype that implements the proposed method and evaluated its effectiveness.

Keywords
RFID, active tag, privacy, security, encryption

1. INTRODUCTION

Radio Frequency Identification (RFID), an automatic recognition technology employing wireless communications, has recently drawn much attention. RFID tags, which are electronic tags that employ RFID technologies, can be broadly classified into passive and active types of tags. The passive type does not incorporate a battery and has a short communications range, but the cost is low. Conversely, the active type incorporates a battery and has a long communications range, but the cost is high.

Although these tags differ in terms of the communications range and cost, they are often attached to products and goods as a means of inventory management. Very recently the number of applications has increased where tags are attached to people. A representative example of this type of application of a passive tag is a facility access card, which is often used by businesses. In Japan, this application is not limited to businesses, it is also used for entry cards to exhibitions [1]. The active tag can be used for marketing, for example, it can be used to track the behavior of customers. Furthermore, for the purposes of security and safety, tracking the behavior of kindergarten children [2], monitoring grade school children on their way to and from school [3,4], and locating wandering or missing elderly people have been initiated.

By using this type of bearer tag, the identification of the bearer and contextual information such as location can be easily obtained with relative certainty. In the future anticipated ubiquitous society, this type of high-level identification will be a very basic technology and play an important role.

On the other hand, in the case that the excellent automatic recognition and tracking abilities of the RFID technology are abused, the privacy violation is a problem. There are already various protest movements that target the use of passive tags [5] and the bearer type active tags [6]. Especially in the case of active tags, which have much longer communications range than passive tags, this is a serious problem.

This paper proposes technological countermeasures that resolve the privacy problem related to active tags and introduces a prototype that we developed.

2. ACTIVE TAG SYSTEM

2.1 What's Active Tag

An active tag is an RFID tag that incorporates a battery, and can communicate with a reader that is several tens of meters away (there are tags that can communicate at several hundreds of meters). While passive tags can only respond to an electromagnetic wave signal emitted from a reader, active tags can also spontaneously transmit an ID. There are various types of transmission opportunities such as the very common periodic transmission type, or the unscheduled transmission type such as when there are changes in vibration or temperature or when a button is pushed. In many cases, the ID data comprise several tens of bits.

Generally, systems that employ active tags comprise the tags, a reader, and a server. The tag spontaneously transmits its ID. For example, if the tag is a periodic transmitting type, the tag transmits its ID once every several seconds. When the reader receives the ID, it

notifies the server of the ID via the network, and based on the ID the server executes the target service.

2.2 Active Tag Applications

This section introduces application examples for active tags.

[Behavior tracking of kindergarten children] [2]

Parents or guardians can view their children in kindergarten via the Internet by utilizing the active tags. Active tags are attached to the nametags of the children, and the classrooms and sports grounds are equipped with a reader and a Web camera. Based on this, by accessing the Internet the children can be viewed in real time and in their actual surroundings. The parents or guardians can automatically select video images of their children.

[Monitoring grade school children on their way to and from school] [3,4]

Since the incidences of abduction and brutalization of children as they are on their way to and from school has increased, the application of active tags has been investigated. The backpacks etc. of the children are equipped with a tag and readers are installed along the route to school and at the school gate. When a child passes by a location that is equipped with a reader, the ID is transmitted and the school and the parents or guardians are notified. By using this system, at an early stage the teachers and the parents or guardians can become aware of any abnormalities in the commute to school.

[Monitoring with the aid of cameras]

Through the cooperation of monitoring cameras and an active tag system, if images are recorded at the same time that the ID is received and recorded as metadata, an effective method for investigating criminal offenses becomes possible. For example, it would be very efficient to use the ID of an abducted person as a search key in an image search.

[Promotion and marketing]

In department stores and supermarkets, if customers bear tags, their behavior can be tracked inside the store, and based on their context history such as moving path or purchasing history, the consumer can take part in promotions that are made possible through the Kiosk terminal inside the store.

[Authentication and settlement]

The use of contact-less IC cards for ticket examination in traffic systems has increased, and the system has become very convenient. To advance this concept further, if active tags can be used in authentication, it would even save the trouble of taking out a card. This type of process would become effortless and the level of convenience would increase even more. Of course, being billed for simply coming into close proximity of these readers would be problematic, and an authentication and settlement scheme that prevents illegal acts such as impersonation is needed.

In this way, applications that use active tags have a wide range and have the potential to become the basic identification method for future ubiquitous services.

3. RFID PRIVACY ISSUES

On the other side of this convenient system, there is the increased anxiety caused by privacy violation stemming from automatic identification using the active tags. This section evaluates the threat to privacy that can occur by transmitting an ID, which at most comprises several tens of bits. First, the characteristics of the many currently used active tags are clarified.

- The active tag transmits its ID without the knowledge of the owner. More specifically, the owner does not have to perform an action such as consciously pushing a button as in the case of an immobilizer. The tag periodically and automatically transmits the ID.
- Anyone that possesses a reader can receive the ID.

These two characteristics lead to the consequence that anyone possessing a reader can receive the ID without the owner being aware. Whether or not this idea can actually be connected to the violation of privacy depends on the characteristic of the ID being disclosed as described below.

3.1 Content Privacy

In the case where the ID contains personal information pertaining to the tag bearer or other related information, there is a risk that others can easily obtain this information. For example, the ID could be assigned information such as the gender of the bearer, birth date, zip code, telephone number, employee number, and student number. For the current active tags, since each service can freely determine the information contained in the ID and there are still many immature service providers that have a low level of awareness of the crisis related to the privacy threat, the possibility cannot be denied that this information may naively be included in the ID.

3.2 Location Privacy

Even if personal information is not included in the ID as mentioned above, if the ID is fixed, there is a danger in that the behavior history of the tag bearer can be disclosed to others based on ID tracking. This danger does not stop at simply the physical tracking of locations visited. All kinds of personal information can be obtained by analyzing the types of places visited such as hospitals, schools, and stores.

Obviously, the ID and the bearer must be connected to be effective. Anyone can very easily obtain the ID information of the bearer by simply coming into close proximity to the bearer and reading the ID using a reader. Conversely, for the ID to specify the bearer is comparatively difficult. The degree of difficulty depends on factors such as whether or not a database (DB) exists to connect the ID to the personal information and the strength of the security of the DB.

Furthermore, it is very dependent on the uniqueness of the ID. As mentioned earlier, in the current state, since each service freely determines the contents of the ID, at best only within the service can the uniqueness be guaranteed. More specifically, when considering local, national, and international levels, the possibility is high that duplication will occur. As the degree of duplication increases the connection between the ID and the tag bearer becomes weaker and it becomes more difficult for a privacy problem to occur.

However, in the future, in the process in which the active tag will be developed as a fundamental device in the global ubiquitous society, the tag ID will also be standardized and made globally unique similarly to telephone numbers, IP addresses, E-mail addresses, RFIDs related UID [7] and EPC codes [8], etc. This global uniqueness will cause a location privacy problem.

4. PRIVACY ENHANCED ACTIVE TAG

4.1 System Architecture

In order to resolve the privacy problem, we adopt the basic architecture shown in Figure 1.

At a transmission opportunity, the tag outputs a temporary ID called an Anonymous-ID. This Anonymous-ID transmits a different random value each time. For this reason, if the Anonymous-IDs are collected and analyzed by eavesdroppers, the IDs can only be recognized as unrelated random number sequences, and they cannot be determined to be from the same ID. Certainly, the frequency that the Anonymous-ID is updated can be changed to satisfy the privacy protection level.

The security server decrypts the Anonymous-ID into the original ID. The decoded results are obtained only by a reader that has the acquisition authorization for that ID. In this way, the threats to content privacy and location privacy caused by readers without authorization having unlimited access can be avoided. The reader authentication, its ID acquisition authorization, and secure communications between the reader and the server, take advantage of the existing Internet security technologies.

4.2 Anonymous-ID Generation Methods

We developed the three schemes described below as methods for generating the Anonymous-ID.

[A: Probabilistic encryption scheme]

Inside the tag, a probabilistic public key encryption scheme is implemented, and this scheme generates a different

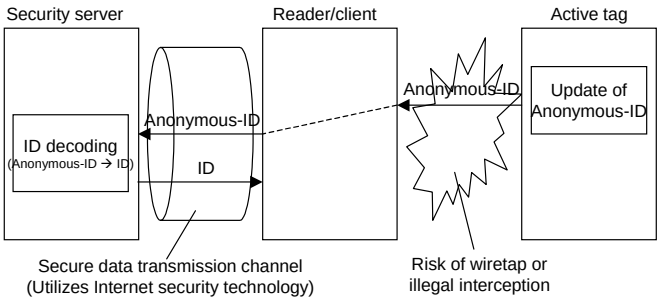

Figure 1. Basic architecture

Anonymous-ID each time. Probabilistic encryption is an encoding scheme in which a different cipher text is generated each time and it is difficult to determine the degree of relatedness among the generated cipher texts. More specifically, even if the same ID is encrypted, the first encryption results and the second encryption results are totally different and unlinkable. Since, in this scheme, information such as the secret key is not stored in the tag it

is highly resistant to tampering. However, since the ID is stored as plain text, it is possible that the ID can be disclosed by tampering. Whether or not this type of self-disclosure can be linked to a threat to privacy depends on the circumstances. For example, as described in Section 3.1, if personal information is stored in the ID, this poses a problem.

In regard to these problems, a function called re-encryption is effective. In this re-encryption function, without decryption one cipher text is generated from another cipher text by using only the public key. Regardless of the number of times re-encryption is performed, the plain text can be obtained by performing decoding once. If this re-encryption function is used, the encrypted ID can be stored inside the tag, and even the danger of disclosing the original ID due to tampering can be abated. For example, the elliptical curve ElGamal is a probabilistic encryption algorithm with such a re-encryption function.

[B: Common key encryption scheme]

When public key encryption, which incurs a large calculation load, is used in the probabilistic encryption scheme, the battery life is curtailed in applications such as the active tag, which has limited calculation resources. To address this, we propose using a method that employs common key encryption, which has a far lower calculation load compared to that for public key encryption. Common key encryption itself does not provide properties such as probabilistic encoding and re-encryption. Common key encryption and random number generation are implemented in the tag, and the original ID and secret key are stored in the tag as well. When the ID is updated, a random number is generated, and then the ID and the random number are combined and encrypted by the secret key. Therefore, each time a different Anonymous-ID can be generated.

In comparison to the probabilistic encryption scheme, the common key encryption scheme has a small calculation load; however, since the secret key must be stored in the tag, it is extremely vulnerable to tampering. Since the secret key must be shared among multiple tags, when disclosing the secret key other tags can also be decrypted and privacy can no longer be protected. The reason that the secret key must be shared is described in the following. If the secret keys are individualized, the server must know which secret key to use for the decoding. In order to make that discrimination, additional information such as an ID key number must be included, and the fixed and unique characteristics of this form would cause new privacy violations.

[C: Hash-chain scheme]

In order to address the issues related to the probabilistic encryption scheme and common key encryption, we believe that applying the Hash-chain scheme [9], which we previously developed for the passive tag, is effective. Hereafter, a simple explanation of the function of the Hash-chain scheme is given using Figure 2. When the tag updates the ID, (1) local variable α is input into Hash function H and (2) α is updated. Next, (3) α is input into Hash function G, and (4) Hash value β is updated as the Anonymous-ID. At the next transmission opportunity, the tag transmits β. The corresponding relationships between the original ID and the initial value of α are safely managed in the server as secret information.

Based on the randomness of Hash function G, the Anonymous-IDs, β, generated each time are different and unlinkable to one another. Since this process is one way, there is no way to retrieve the internal secret information, α, from β. The secret information inside the tag, α, is updated one-way each time α is read using Hash function H. For this reason, even if a third party knows α through tampering, the third party cannot know the retroactive values of α. As a result, previous values of the Anonymous-ID, β, cannot be investigated.

In this way, even if tampering of the secret information in the tag occurs, the previous information up to that point (cipher text, signature, etc.) is protected by the characteristic called forward security. The Hash-chain scheme provides this characteristic.

However, the main issue of this scheme is the limited scalability of resolving the IDs at the security server. Different from encryption, hash functions are one-way functions. For this reason, to resolve the original ID, the server must repeat its calculation until it obtains the identical match to the Anonymous-ID (β) received from the tag by retesting the same procedures that are performed by the tag for each of the initial values of α, which has a one-to-one correspondence to the original ID. As a result, as the number of IDs managed at the server increases the decoding processing time increases. However, if the server disk capacity is sufficiently large that the corresponding tables for all of the β values and IDs can be generated beforehand, the IDs can be resolved in a $\log_2 (N \times M)$ level of retrieval processing time, where N is the number of IDs and M is the envisioned maximum number of reads.

Among the three schemes described above, there are advantages and disadvantages in terms of the calculation load of the tag, safety, and the server load. The results are given in Table 1. We can select the appropriate scheme among the three according to the system requirements.

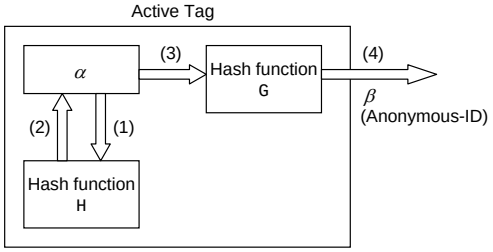

Figure 2. Hash-chain scheme

Table I. Comparison of Privacy Protection Schemes

		A: Probabilistic encryption scheme	B: Common key encryption scheme	C: Hash-chain scheme
Privacy	Content privacy	Protected (o)	Protected (o)	Protected (o)
	Location privacy	Protected (o)	Protected (o)	Protected (o)
	Vulnerability to tamper	Tamper free (o)	Vulnerable (x)	Tamper free (o)
Calculation load	RFID Tag	High (x)	Low (o)	Low (o)
	Security server	Low (o)	Low (o)	High (x)

4.3 Prototype System

In the currently commercialized version of the active tag, some limited functions are provided such as initializing the ID or changing the transmission timing. However, there have been no tags in which a software program for the above-proposed privacy protection schemes can be implemented. For this reason, we developed an active tag that integrates a microprocessor (Figure 3).

The specifications for the developed active tag are given in Table 2. The transmission period and ID update timing are specified so that they are independent of each other. Based on this, requirements such as the level of privacy protection and battery life can be flexibly satisfied. There are two choices for transmission timing, the periodic transmission type and the ultrasound response type in which an ultrasound is received from an outside source and when there is a transmission opportunity a response is transmitted. The ultrasound response type is appropriate for real-time systems such as automatic ticket examination, and

Table 2. Specifications for active tag prototype

General specifications		Wireless specifications		MPU specifications	
Exterior	30x70x15 mm	Transmission frequency	315 MHz±40 KHz	MPU	Motorola 8 bit MPU
Consumed electrical Current (Waiting)	Less than 20 μA	Transmission speed	19.2 kbps	MPU execution frequency	20 MHz
Consumed electrical current (Transmitting)	Approx. 6 mA	Transmission output	500 μV/m@3m	Memory	Flash 60 KB, RAM 4 KB

for event driven systems such as changing the ID transmission interval when entering a store and ID update.

Table 3 presents the implemented Probabilistic encryption and Hash-chain schemes and their respective encryption or hash algorithms and processing time results for updating the ID. From these results, in the Probabilistic encryption scheme it is difficult to update the ID in a short period such as a second, and even if the period is extended to several seconds, since the conditions are such that the processor must constantly be in operation, the battery life becomes extremely short. Since the speed at which people move is limited, an ID update per hour should be more than sufficient. For these requirements, practical application is more than possible. Furthermore, if the encryption processor used in IC cards is employed, calculation at high-speed and with low power consumption is possible in public key encryption.

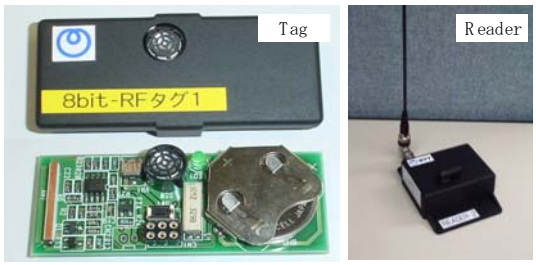

Figure 3. Active tag prototype

Table 3. Processing time

	Encryption / Hash algorithms	Tag processing time
Probabilistic encryption scheme	Elliptic curve ElGamal (key length 160 bits)	6 sec
Hash-chain scheme	SHA-1, MD5	Less than 1 sec

5. CONCLUSION

By using the bearer type active tag, identifying people and providing personal contextual information such as location will become easier and more certain. This type of high-level identification or contextual information collection will become important as a very fundamental technology in the anticipated ubiquitous society. However, a problem is arising where the excellent tracking ability of active tags is abused and personal privacy is being violated.

This paper clarified the active tag privacy problem and proposed three schemes each with different characteristics from the viewpoints of safety, tag calculation cost, and server calculation cost. Furthermore, we constructed an active tag prototype that enables ID encryption and restriction-less update control, implemented two proposed schemes, and evaluated them.

In the future, with the view of achieving a safe ubiquitous society, we plan to intensify the analysis of the application areas for active tags and refine the requirements while investigating a way to achieve the optimal privacy protection scheme.

REFERENCES

1. NIKKEIBP, http://itpro.nikkeibp.co.jp/free/NBY/NEWS/20040630/2/ (in Japanese).
2. RFID journal, “Surveillance System Links Video to RFID Tags”.
3. CNET News.com, “Japan school kids to be tagged with RFID chips”.
4. The Mercury News, “ID Badges on Children”.
5. CASPIAN’s homepage, http://www.spychips.com/
6. Electronic Frontier Foundation, “Mandatory Student ID Cards Contain RFIDs”.
7. ISO/IEC 15963, “Information technology -- Radio frequency identification for item management -- Unique identification for RF tags”, 2004.
8. EPC global, “EPC Tag Data Standards Version 1.1”, 2004.
9. M. Ohkubo, K. Suzuki, S. Kinoshita, “Cryptographic Approach to “Privacy Friendly” Tags,” RFID Privacy Workshop @ MIT, Nov. 2003.

   http://www.rfidprivacy.org.