Improving the Key Search using Parallelism in RFID Privacy Protection

Myeong-sook Shin* · Choong-woon Kim* · Joon Lee*

ABSTRACT

Abstract. In the ubiquitous environment of the next generation, RFID is predicted to occupy an important technical location and also expected to apply to various fields. However, the properties of tags in itself which is the core of RFID have a dysfunction like an invasion of privacy for user. An existing cryptanalytic protection scheme of the information leakage have a difficult problem to apply to RFID tags for privacy protection. We applied Ohkubo et al.'s scheme to the protection of the tag's information efficiently in the RFID system environment using low-cost tags. But, this method has all informations of tagsto identify tag's ID and then performs the process of identification in sequence in the Back-end server. These processes have lots of computations so that it have problems about a scalability. In this paper, we are based on Ohkubo et al.'s scheme to solve problems, and then analyze the parallelism with the Hellman's tradeoff method, divide it into nodesin parallel. In this paper, we are based on Okubo et al.'s scheme to solve problems, and then analyze the parallelism with Hellman's tradeoff method, divide it into the w node in parallel. as a result, we can reduce the computing complexity of key search to $O(\frac{m^{2/3}n^{2/3}}{w})Z$ seconds from $O(mn)$ seconds . finally we show the results to be enhanced the scalability.

Keywords
RFID, Privacy Protection Scheme, Hash Chain Scheme, Hellman's Tradeoff Method, Parallelism

I. INTRODUCTION

Since it starts to be applied to the various industry as a whole, the importance of privacy has been embossed[1][2]. To solve the problem of privacy invasion in the RFID system should be satisfied with confidentiality, indistinguishability, forward security[3][4]. When applying the privacy protection scheme, an essential factor to guarantee in the Back-end server is a scalability[3][4][5]. Even if the number of total tags to conduct the scalabilityincrease rapidly, it means we should accomplish an identification work in time. Typically, designing the privacy protection scheme, we should increase computingquantity to have to conduct in the Back-end server. If it has much computing quantity of the Back-end server, we are impossible to discriminate tags in real time. We should consider the capability of the server[3][4].

We applied Ohkubo et al.'s scheme to protect the information of tags efficiently in the RFID system environment using low-cost tags[3]. However, this method performs the process of identification in sequence with informations of all tags to identify tag's ID in the Back-end system. So, these processes are so computational that it has problems of the scalability. This paper needs lots of computation ability and storage space in the Back-end server to protect the RFID privacy.

In this paper, we are based on Ohkubo et al.'s scheme to solve problems, and then analyze the parallelism with Hellman's tradeoff method, divide it into four nodes in parallel[6]. As a result, we can

* Dept. of Computer Eng. Chosun Univ.

접수일자 : 2007. 01. 13
심사완료일자 : 2007. 02. 27

reduce the computing complexity of key search. Finally, we show results to be enhanced the scalability.

II. RFID Privacy Protection System

We explain the need of the RFID system and privacy protection scheme based on improving the scalability requires safe the RFID privacy protection scheme. And we raise several problems of RFID certificated protocol and the Back-end server to apply these.

2.1 RFID SYSTEM AND PRIVACY PROTECTION SCHEME

Tags are configured with the chip and antenna. It keeps the unique identification code and the information, so it is device to send and receive own information to readersby the request of readers or existing state of things. Readerstransfer server after reading data received from tags or send tags a signal. The Back-end server has a function to collect, control, manage the various data of transferred tags[7].

The importance of privacy is embossed after RFID starts to be applied to various industries. To solve the invasion of privacy in the RFID system has to contented with indistinguishability and forward security. Ohkubo et al.'s scheme is a secure scheme to guarantee indistinguishability and forward security that the established theory had. In this paper, we suppose to be feasible to RFID tags.

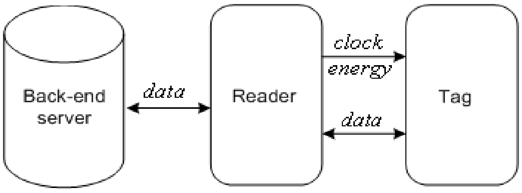

Fig. 1 The RFID system is configured with Tag, Reader, and Back-end server

2.2 RFID AUTHENTICATION PROTOCOL AND BACK-END SERVER

One of the method for the privacy protection is RFID authenticated protocol in the RFID system.

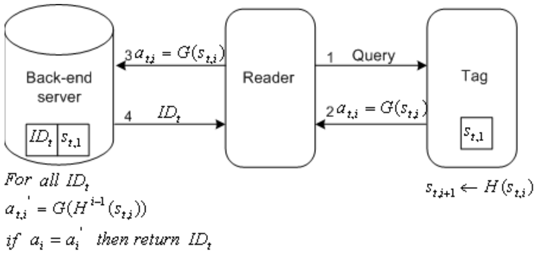

Fig. 2 The authentication in RFID system represent process to prove justice tags and readers.

When readers query a question, tags transmit readersat least information for authenticating itself. Readers transmit the value received from tags to the Back-end server, using the secure channel. The Back-end server transmits value authenticated tags to reader. At last, reader transmits information which tags want to tags. Tegs transmit its own information to reader after it authenticates the transmitted value. Tags/Readers sections are not usually assured security and the wiretapping is possible. But, tags/readers sections suppose that it is the secure block to keep up the security.

The Back-end server is a system to handle information related to tags which is transmitted from several readers. We can operate several servers and manage informations related to tags. Typically, the Back-end server is considered a reliable system as security. When the RFID system apply privacy schemes for the protection, it should guarantee the scalability.

The safest method is authentication protocol to protect privacy among established study. But, computation for identifying tags in the Back-end server is so much that the method to improve the scalability is necessary.

III. Improving Scalability of Back-end server

We discuss improving the scalability of the Back-end server based on problems to be considered in the section 2. The established Ohkubo *et al.'s* scheme is excellent from a privacy aspect, but the solution to this problem is necessary as computing quantity for identifying tags have many problems. We suggest the more elevated method to examine proposed protocol and discuss problems.

3.1 INNER PART OF TAGS FOR SECURE PRIVACY

Ohkubo et al.'s scheme applied to this thesis is technique to find that specified tags belongs to a hash chain through process to construct all hash chain when including all hash chains to have itself for identifying tags in the Back-end server. The inner part of tags to use Ohkubo et al.'s scheme is showed Figure 3.

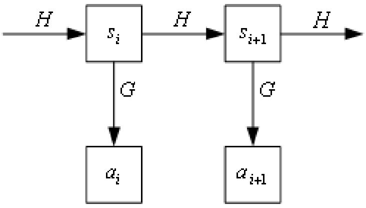

Fig. 3 RFID tags send $a_{t,i}=G(s_{t,i})$, and renew its secret$s_{t,i+1}=H(s_{t,i})$.

In this method, tags save $s_{t,1}$ where H and G are hash functions. And other the Back-end server saves $(ID_t, s_{t,1})$ of hash seed value. Tags send answer $a_{t,i}=G(s_{t,i})$ to readers, and then Tags renew secret update $s_{t,i+1}=H(s_{t,i})$ as determined from previous secret $s_{t,i}$. Reader sends $a_{t,i}$ to the Back-end server. The Back-end server maintains a list of $(ID_t, s_{t,1})$ pairs, where $s_{t,1}$ is the initial secret information and is different for each tag. So, the Back-end server that received tags output $a_{t,i}$ from reader computes $a_{t,i}'=G(H^{i-1}(s_{t,1}))$ for each $s_{t,1}$ in the list, and checks if $a_{t,i}'=a_{t,i}$. We find $a_{t,i}'$, $a_{t,i}'=a_{t,i}$, then return the ID_t, which is a pair of $a_{t,i}'$.

But, in this method, the Back-end server must computes the i times of H and G to all $s_{t,i}$ to find $s_{t,1}$. So, this method must computes all informations of tags to identify tag's ID and then performs the hash operation of n times in sequence in the Back-end server. It is shown in Figure 4. In the worst case, this method is needed the computing complexity of key search of $O(mn)$ as this method computes $a_{t,i}=G(H^{i-1}(s_{t,1})$ of all $1\le t\le m$ and $1\le i\le n$.

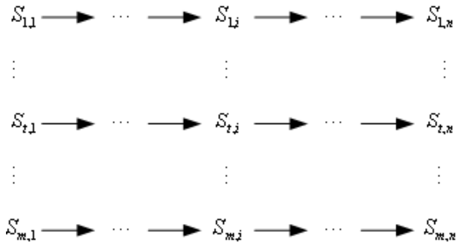

Fig. 4 The Back-end server performs the hash operation of n-th in sequence

So, as this method computing quantity to identify tags in the Back-end server, if the number of tags increase over some, there are problems for tag's indentification to be impossible.

3.2 Improving Scalability using Parallelism

To improve problem of Ohkubo et al.'s scheme, we applied Hellman's tradeoff method and then analyze the parallelism, divide it into nodes. As a result, we also discuss methods to reduce computing quantity.

3.2.1 ANALYSIS OF PARALLELISM

We should handle lots of the computing quantity to identify tags in the Back-end server. To this method, we use Hellman's tradeoff method to find out key in cryptanalytic.

If $a_{t,i}$ is transmitted in the Back-end server, we will find unanimous value to compare the new value and apply H and G to $a_{t,i}$. We can define function to $f=(t,i)->a_{t,i}=G(H^{i-1}(s_{t,1}))$ where $s_{1.1}$ is SP(Start Point) and $s_{1,n}$ is EP(End Point).

$$SP_1 = S_{1,1} \xrightarrow{f} S_{1,2} \xrightarrow{f} S_{1,3} \xrightarrow{f} \cdots\cdots \xrightarrow{f} S_{1,n} = EP_1$$

$$SP_2 = S_{2,1} \xrightarrow{f} S_{2,2} \xrightarrow{f} S_{2,3} \xrightarrow{f} \cdots\cdots \xrightarrow{f} S_{2,n} = EP_2$$

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

$$SP_m = S_{m,1} \xrightarrow{f} S_{m,2} \xrightarrow{f} S_{m,3} \xrightarrow{f} \cdots \xrightarrow{f} S_{m,n} = EP_n$$

Fig. 5 This show that m SP repeat n times in sequence.

Figure 5 repeat m SP n times in the sequence, create EP and sort created EP, and then, save (EP, SP) and make tables. When it is $m=2^{32}$ and $n=2^{32}$, we create 2^{64} ideally. Like this, as we save only (EP, SP)in process of computation to apply Hellman's tradeoffmethod, reduce working hours by much by reducing the necessary time to create (EP, SP).

In this way, the process to compute EP from SP independently in the preceding computed process is like Figure 5. Because there is not intervention or subordination in the process to compute EP from different SP, it is possible to computeto apply going side by side. So, it is possible to carry out applying to key searching process and preceding computed process in nodes.

3.2.2 DIVISION OF PARALLELISM

We saw a preceding computed process extract concurrence like Figure 6. We divide all operations to carry out using parallelism into operation of w to carry out side by side. And then, if divided operation is disposed of parallelism, the time completed operation can be reduced. Figure 6 represent the way to divide at nodes after collecting an arbitrary SP. Nodes divided like this compute a pair of (SP, EP)in parallel. The number of SP collecting to each node is m/wif it gives operation in each nodes without discrimination because nodes of w carry out dividing if the number of SP is m.

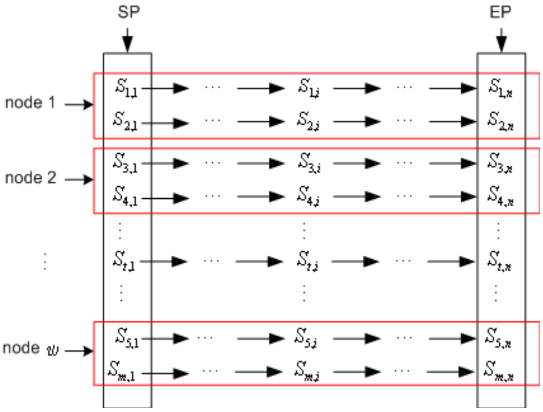

Fig. 6 A work divides using Hellman's tradeoff method to w nodes.

The process performing with parallelism to use parallelism draws up EP after calculating EP to collect SP of m/w first. And we perform the process to search key in using Hellman's tradeoff method. As it performs this process each nodes of w, we reduce the computing time.

3.2 ANALYSIS OF THE COMPUTING COMPLEXITY OF KEY SEARCH

We exlain the elevation precision of the scalability through analyzing the computing quantity that identify tags in the Back-end server to apply this proposed method. We suppose to give the same operation in each node after we divide it into nodes of w if the number of SP is m. The number of SP is n/w in this proposed method. When we analyze the computing complexity of key search for identifying tags, existing Okubo *et al.'s* scheme is $O(mn)$ and this proposed method is $O((m^{2/3}n^{2/3})/w)$.

IV. CONCLUSION

In this paper, we describe method to improve the scalability at the server among the method to solve the infringement of privacy in the RFID system.

We apply Okubo et al.'s scheme to tags for solving the infringement of privacy in the RFID system[3]. But, this proposed method have problems of the scalability which have many computing quantity for identifying the infringement of privacy in the RFID system[3][4][5]. We used Hellman's tradeoff method for solving this problem[6]. Dependent does not exist to different among the process to find out the key in this method. We abstracted concurrence to use that each SP is done at once. We separated the arbitrary SP of w. And then, we reduced computing time by means of doing process computed and key process searched about w.

In this paper, When we analyze the computing complexity of key search for identifying tags, existing Okubo et al.'s scheme is $O(mn)$ and this proposed method is $O((m^{2/3}n^{2/3})/w)$ in this proposed method for solving the scalability of the Back-end server. We make certain of taking the better scalability with stability like Okubo *et al.'s* scheme. Applying to identify various tags for the ubiquitous computing environment realization, it was necessary to handle between system and network environment in parallel. If this proposed method is applied, handling lots of data in the distributed environment is expected because apply to the grid.

REFERENCE

[1] S. Sarma, S. Weis, and D. Engels, "The RFID System and Security and Privacy Implications", In CHES 2002, Vol. 2523 of LNCS, pp.454-469, Aug. 2002.

[2] M. Feldhofer, S. Dominikus and J. Wolkerstorfer, "Strong Authentication for RFID Systems using the AES Algorithm", In CHES 2004, Vol. 3156 of LNCS, pp.357-370, Aug. 2004.

[3] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic approach to “privacy-friendly" tags", In RFID Privacy Workshop, MIT, USA, 2003.

[4] Gildas Avoine and Philippe Oechslin, "A scalable and provably secure hash based RFID protocol", In IEEE International Workshop on Pervasive Computing and Communication Security - PerSec 2005, Kauai Island, Hawaii, USA, IEEE, IEEE Computer Society Press, March 2005.

[5] P. Oechslin, "Making a faster cryptabalytic time-memory trade-off", In Advanced in Cryptology-CRYPTO'03, LNCS, Springer, 2003.

[6] M. Hellman, "A cryptanalytic time-memory trade off", IEEE Transactions on Information Theory, Vol. IT-26, No. 4, pp.401-406, 1980.

[7] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems", In Proceedings of the 1st International Conference on Security in Pervasive Computing, 2003.

저자 소개

신명숙(Myeong-sook Shin)

1992년 2월 광주대학교 전자계산학과(공학사)
1996년 2월 광주대학교 전자계산학과(공학석사)
2005년 12월 조선대학교 컴퓨터공학과 박사과정(수료)
※ 관심분야 : 시스템소프트웨어, 유비쿼터스컴퓨팅, 정보보호

김충원(Choong-woon Kim)

1982년 2월 한양대학교 전자공학과(공학사)
1984년 2월 한양대학교 전자공학과(공학석사)
1989년 2월 한양대학교 전자공학과(공학박사)
※ 관심분야 : 영상처리

이 준(Joon Lee)

1979년 2월 조선대학교 전자 공학과(공학사)
1981년 2월 조선대학교 대학원 전자공학과(공학석사)
1997년 2월 숭실대학교 대학원 전자계산학과(공학박사)
1982년 3월 조선대학교 전자정보공과대학 컴퓨터공학부 교수(현)
※ 관심분야 : 운영체제, 정보보호, 유비쿼터스컴퓨팅