RFID 시스템에서 Hash-Chain기반 Tag-Grouping을 이용한 안전하고 효율적인 데이터베이스 검색

Secure and Efficient Database Searching in RFID Systems using Tag-Grouping Based on Hash-Chain

이병주*, 송창우*, 정경용**, 임기욱***, 이정현****

인하대학교 정보공학과*, 상지대학교 컴퓨터정보공학부**, 선문대학교 컴퓨터정보공학부***,
인하대학교 컴퓨터정보공학부****

Byeung-Ju Lee(lbju@hanmail.net)*, Chang-Woo Song(ph.d.scw@hanmail.net)*,
Kyung-Yong Chung(kyjung@sangji.ac.kr)**, Kee-Wook Rim(rim@sunmoon.ac.kr)***,
Jung-Hyun Lee(jhlee@inha.ac.kr)****

요약

RFID(Radion Frequency Identification)는 바코드를 대체할 차세대 기술이다. RFID는 무선 주파수를 사용하여 RFID 태그 내부에 있는 ID를 읽어 물체를 식별할 수 있다. 하지만 RFID 태그는 어떤 리더의 요청에도 자신의 고유 ID를 무선 통신으로 응답하기 때문에 도청이나 불법 리더로부터 보안이나 프라이버시에 대한 공격에 취약하다. RFID 인증 프로토콜은 보안과 프라이버시 문제를 해결하기 위해 활발히 연구되고 있으며 태그 검색에도 사용되고 있다. 최근에는 RFID 시스템에서 태그의 수가 증가하고 데이터 수집 비용도 늘어나면서 효과적인 태그 검색에 대한 비중이 더 많아졌다. 본 논문에서는 보안과 프라이버시 보호를 위한 필요조건을 보장하는 Miyako Ohkubo의 hash-chain 메커니즘에서 데이터베이스 연산량이 많은 문제점을 Tag-Grouping을 통해 보완한 효율적인 검색 방법을 제안한다. 실험 결과 데이터베이스에서 10만개의 레코드 수를 기준으로 접근비율이 5이상인 태그 그룹의 우선 검색시 약 30%의 검색시간이 감소하였다.

■ 중심어 : | RFID 시스템 | 보안 | 데이터베이스 검색 |

Abstract

RFID (Radio Frequency Identification) is a next generation technology that will replace barcode. RFID can identify an object by reading ID inside a RFID tag using radio frequency. However, because a RFID tag replies its unique ID to the request of any reader through wireless communication, it is vulnerable to attacks on security or privacy through wiretapping or an illegal reader's request. The RFID authentication protocol has been studied actively in order to solve security and privacy problems, and is used also in tag search. Recently, as the number of tags is increasing in RFID systems and the cost of data collection is also rising, the importance of effective tag search is increasing. This study proposed an efficient search method that solved through tag group the problem of large volume of database computation in Miyako Ohkubo's hash chain mechanism, which meets requirements for security and privacy protection. When we searched first the group of tags with access rate of 5 or higher in a database with 100,000 records, search time decreased by around 30%.

■ keyword : | RFID Systems | Security | Database Searching |

* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음. (NIPA-2009-C1090-0902-0020)

접수번호 : #090730-007

접수일자 : 2009년 07월 30일

심사완료일 : 2009년 08월 03일

교신저자 : 이병주, e-mail : lbju@hanmail.net

I. 서 론

바코드 시스템은 한 번에 하나의 바코드를 인식해야 하기 때문에 대량의 물품을 동시에 처리하는데 많은 시간이 소비된다. 바코드는 단가가 저렴하고 제품의 정보를 파악하는데 유용하지만 실시간으로 대량의 정보를 처리하는 것이 불가능하다. 이러한 문제점을 보안하기 위해 대량의 물품을 동시에 처리할 수 있는 자동인식 시스템이 필요하게 되었다. RFID 시스템은 무선 주파수를 이용하여 RFID 태그 내부에 있는 ID를 읽어서 물체를 식별하며 사물이나 사람과 같은 객체를 직접 접촉하지 않고 자동으로 인식하기 위한 기술이다[1]. RFID 기술은 꾸준히 발전해 왔으며 근래에는 교통요금 지불 시스템, 가축관리, 산업 자동화, 의료분야 등 폭넓은 분야에 활용되고 있다. 미국 식약청은 제약 회사에 향상된 추적 능력을 제공하기 위해서 RFID 태그 부착을 권고하고 있다. RFID 기술은 다른 자동 데이터 획득 기술보다 이점이 많다. 사업현장의 많은 조직들은 비지니스 프로세스에서 RFID 기술을 점진적으로 구현하고 있다. 예를 들면, 월마트, 미국방위청, 식약청 등은 가장 많이 알려져있다[2].

RFID 시스템은 일반적으로 태그, 리더, 데이터베이스 서버로 구성된다. 각각의 태그에는 고유한 ID를 가지고 있으며 ID는 리더기를 통해 데이터베이스로 전송된다. 데이터베이스는 태그 ID로 물품의 정보를 찾아내고 이 정보를 리더에 보내서 리더가 태그의 정보를 파악할 수 있도록 도와준다. 그리고 동시에 여러 개의 태그를 인식할 수 있기 때문에 인식률과 처리율이 우수하다. RFID는 무선 주파수로 통신을 하면서 비접촉 방식으로 물체를 식별할 수 있다는 장점이 있지만 전파를 이용한 통신으로서 도청을 통해 통신 정보를 확인할 수 있는 문제점이 발생된다. RFID 리더를 가지고 있거나 도청기를 가지고 있다면 RFID 태그의 정보를 훔쳐낼 수 있다. 또한 태그의 ID는 고유하기 때문에 위치추적(Location Tracking)문제가 발생할 수 있다.

따라서 본 논문에서는 보안과 프라이버시 보호를 위한 필요조건인 기밀성, 불구분성과 전방위보안성을 보장하는 Miyako Ohkubo의 Hash-Chain 메커니즘 기반에서 데이터베이스 연산량이 많은 문제점을 해결하기 위해 Tag-Grouping을 이용한 효율적인 검색 방법을 제안한다.

본 논문의 구성은 다음과 같다. 기본적인 RFID 시스템과 기존 RFID 시스템에서 보안 문제점을 지적하고 이를 해결하기 위한 조건을 2장에서 구체적으로 설명한다. 3장에서는 Hash-Chain 메커니즘을 설명하고 Tag-Grouping을 이용한 효율적인 데이터베이스 검색 구조를 보여주고 4장에서 실험 및 평가한다. 마지막으로 5장에서는 결론과 향후 연구에 대해 종합한다.

II. 관련 연구

1. RFID 시스템의 구성

RFID란 제품에 부착된 Chip의 정보를 주파수를 이용해 읽고 쓸 수 있는 무선 주파수 인식으로 사람, 상품, 차량 등을 비접촉 방식으로 인식하는 기술을 뜻한다[3]. 라디오 주파수를 사용해 태그와 리더기 사이에 통신이 이루어지는 RFID 기술은 객체 정보의 공유와 추적을 위해서 개발되었다. 기존의 바코드와는 달리 인식을 위해 직접 조준할 필요가 없으며 태그의 정보 변경 및 추가가 자유롭고 일시에 다량의 태그 판독이 가능할 뿐만 아니라 온도, 습기, 먼지 등의 열악한 환경에서도 인식률이 높다.

RFID 시스템은 태그, 리더, 데이터베이스로 구성되어있다. 태그는 능동형 태그와 수동형 태그로 구분된다. 능동형 태그는 자체배터리를 가지고 있으며 먼 거리까지 송신이 가능하고 스스로 동작할 수 있다. 수동형 태그는 자체배터리가 없으며 리더로부터 에너지를 공급받는다. RFID 리더는 태그가 동작할 수 있도록 에너지와 명령을 무선 주파수 신호로 태그에게 전송을 하며 태그로부터의 신호를 복원하는 기능을 수행한다. 데이터베이스는 리더로부터 태그의 ID를 받아 해당 객체 정보를 검색하고 결과를 리더로 반환한다.

1.1 태그(Tag)

리더가 RF신호를 태그에 송신하면 태그는 자체에 저

장된 정보를 리더에게 송신한다. 태그는 배터리를 사용하는 Active 타입인 능동형 태그와 배터리를 사용하지 않는 Passive 타입의 수동형 태그로 나뉜다. Active 타입은 배터리를 내장하고 있어 환경에 따라 사용시간이 제한적이지만 능동적으로 주변의 환경 데이터를 수집 및 처리할 수 있다는 장점이 있다. 반면에 Passive 타입은 배터리를 내장하지 않으며 안테나에서 전송되는 전파에너지로부터 전기에너지를 얻기 때문에 고정된 정보만 저장할 수 있으나 사용시간이 반영구적이고 가격이 저렴하다는 장점이 있다. 전형적인 RFID 태그는 고유한 ID를 갖고 있으며 내장된 실리콘 마이크로칩은 통신으로 추가적인 정보를 저장한다. 마이크로칩은 2Kbyte 정도의 데이터를 저장할 수 있다[4].

1.2 리더(Reader)

리더는 태그와 무선 주파수 신호로 통신을 하며 태그의 고유 ID를 네트워크와 연결된 데이터베이스로 전달한다. RFID 리더는 수동형 태그가 동작할 수 있도록 전력과 수행할 명령을 무선 주파수 신호로 태그에 전송한다. 그리고 태그로부터 응답을 수신하여 신호를 복원하는 기능을 수행한다.

1.3 데이터베이스(Database)

데이터베이스는 리더로부터 태그의 ID 정보를 받으면 해당 아이디에 맞는 객체를 검색하고 정보를 리더로 보내주는 역할을 한다. 이 때 데이터베이스는 태그 ID와 매칭되는 객체의 정보를 미리 저장하고 있다.

2. RFID 시스템의 보안 문제점

RFID에서의 정보보호를 위해서 기밀성, 불구분성, 전방위보안성이 필요하다. RFID 시스템에서 발생할 수 있는 보안 문제점은 다음과 같다.

2.1 도청(Eavesdropping)

RFID 시스템은 무선 주파수를 사용하기 때문에 통신내용을 중간에서 가로챌 수 있다, 그러므로 도청을 통해 다른 공격에 활용 가능한 어떠한 정보도 얻을 수 없도록 해야 한다.

2.2 통신내용분석(Traffic Analysis)

도청을 통하여 리더의 질의에 대한 태그의 응답을 예측할 수 있으며, 위치추적에 사용할 수 있다.

2.3 위치추적(Location Tracking)

태그 위치의 변화를 감지함으로써 태그 소유자의 이동경로를 파악하는 방법이다.

2.4 스푸핑(Spoofing)

정당하지 않은 객체를 정당한 것처럼 속여 인증과정을 통과하는 방법이다. 공격자가 태그로 위장하여 정당한 리더를 속이는 방법과 공격자가 리더로 위장하여 태그를 속이는 방법이 있다.

2.5 메시지유실(Message Loss)

태그와 리더 사이에 주고받는 통신내용의 일부가 유실될 수 있다. 인증세션의 비정상적인 종료와 둘 사이의 동기가 어긋날 경우 데이터베이스가 태그의 ID를 잃어버리는 문제가 생길 수 있다.

3. 기존 RFID 시스템의 보호 기법

3.1 KILL Command 기법

AutoID센터가 제안한 Kill 태그는 사용자의 프라이버시를 보호하는 가장 일반적인 방법으로 널리 사용된다[5]. 이 기술은 8비트의 패스워드를 가진 Kill 명령을 태그에 전송해 사용자가 물건을 취하기 전에 태그의 기능을 멈추게 하는 방법이다. 하지만 KILL 명령이 태그에 적용된 이후에 태그의 재사용이 불가능 하다는 단점이 있다.

3.2 Active Jamming 기법

Active Jamming은 근처에 있는 RFID 리더의 기능을 차단하거나 혼잡을 줄 수 있는 방해전파를 이용하는 기술이다[5]. Active Jamming 기기의 일정한 구역내의 모든 RFID 시스템에 전파간섭을 통해 사용자의 정보를 보호할 수 있지만 사용해야할 RFID 시스템까지도 영향을 받아 사용할 수 없는 단점이 있다.

3.3 Hash-Lock 기법

MIT는 저가의 태그에서 자원의 제한 문제를 해결하면서 합법한 리더에게만 태그의 정보를 넘겨 줄 수 있는 Hash-Lock 기법을 제안하였다[6-8]. 해시함수의 특성인 역 계산이 어렵기 때문에 Meta ID를 가지고 Key를 계산할 수 없다. 즉, Meta ID만으로는 태그의 정보를 알아내기 어렵기 때문에 해시함수를 사용해서 사용자의 프라이버시를 보호할 수 있다. 태그와 리더의 인증과정은 [그림 1]과 같다.

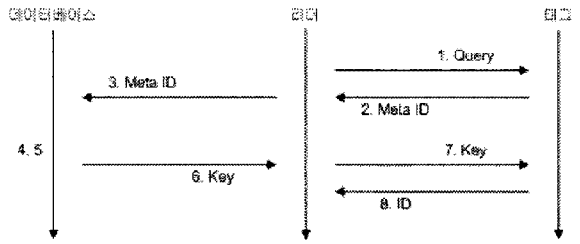

그림 1. Hash-Lock 기법의 태그와 리더 인증과정

1단계: 리더가 태그에게 정보를 요청한다.

2, 3단계: 태그는 Meta ID를 계산한 뒤 리더의 요청에 응답한다.

Meta ID = Hash(key)전송

4, 5단계: 태그의 Lock을 풀기 위해서 리더는 Meta ID값을 데이터베이스로 전송한다. 데이터베이스는 초기화 단계에서 저장되어 있는 Meta ID에 대한 Key를 찾아서 리더에게 전송한다.

6, 7단계: 리더가 데이터베이스로부터 받은 Key를 태그에게 전송하면 태그는 그 값을 Hash하고 Meta ID와 비교해서 일치하는지 체크한다.

8단계: 받은 값과 Meta ID값이 일치하면 태그의 정보를 리더에게 전송한다.

이 기술은 해시함수의 특성인 역으로의 계산이 불가능하기 때문에 Meta ID만으로 태그의 정보를 알아내기가 어려워 사용자의 프라이버시를 보호할 수 있다. 하지만 리더에게 항상 동일한 Meta ID를 전송하기 때문에 위치트래킹 문제에 약하다.

3.4 Randomized Hash-Lock 기법

Hash-Lock 기법에 의사난수 생성기를 추가해서 위치트래킹 문제점을 해결한 방법이다[6-8]. [그림 2]는 Randomized Hash-Lock 기법을 보여준다.

1단계: 리더는 태그에게 질의를 통해 정보를 요청한다.

2단계: 태그는 의사난수생성기를 이용해서 랜덤 수 R을 생성하고 R과 ID_k를 처리한 결과인 hash(R | ID_k) 값을 리더에게 보낸다.

3단계: 합법한 리더는 데이터베이스에 저장되어 있는 모든 ID 값을 받은 R 값과 붙여서 Hash 값을 만들고 받은 Hash 값과 동일한 값을 찾아서 ID_k를 찾아낸다.

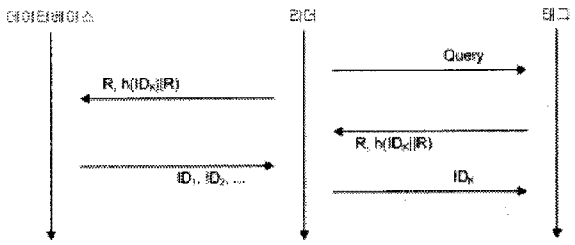

그림 2. Randomized Hash-Lock 기법

Randomized Hash-Lock 기법은 Hash-Lock 기법에서 사용한 Meta ID를 사용하지 않고 랜덤 수 R을 사용하며 리더의 요청시마다 값을 다르게 전달하기 때문에 위치추적 문제를 해결할 수 있다. 하지만 도청을 통해 R 값과 Hash된 값을 계산할 수가 있어서 도청 공격과 전방위보안성 문제에 취약하다.

III. Hash-Chain기반 Tag-Grouping을 이용한 RFID 데이터베이스 처리 시스템

1. RFID 시스템의 보안을 위한 필요조건

RFID 시스템에서 정보유출 문제와 위치추적 문제를 해결하기 위해서 다음과 같은 요건들이 갖추어져야 한다.

1.1 기밀성

기밀성은 전송되는 정보가 공개되지 않게 송신자와 수

신자만 정보를 알아야 한다는 것이다. RFID 시스템에서는 무선 주파수를 사용하기 때문에 암호화를 통해 통신하는 방법을 사용한다.

1.2 불구분성

RFID 시스템에서 태그가 리더의 요청에 의해 전송하는 정보는 동일한 값이 아닌 다른 값을 전송해야 한다. 이러한 정보는 리더 측에서 예측이 불가능해야 하며 예측될 수 있는 값이라면 위치추적의 문제가 발생될 수 있기 때문이다. 이것을 불구분성이라고 한다. 불구분성은 태그를 소유한 사람의 위치 정보를 보호하기 위해서 매우 중요하다.

1.3 전방위보안성

리더의 요청으로 태그에서 보내진 현재 정보가 노출되어도 그 정보로 이전에 생성했던 정보를 알아낼 수 없도록 하는 것을 전방위보안성이라고 한다.

2. Miyako Ohkubo의 Hash-Chain 기법

Miyako Ohkubo는 Hash-Chain을 이용한 보안 프로토콜을 제시했다[9]. 이 기법은 기존에 제안된 다른 프로토콜들에서 해결되지 못한 전방위보안성에 대한 문제를 해결했다. 이 프로토콜은 Hash-Chain을 이용해서 새로운 정보들을 태그에 저장하고 리더에게 보내는 출력값을 일정하지 않게 보내서 불구분성을 보장하게 했다. [그림 3]은 Miyako Ohkubo의 Hash-Chain을 이용한 태그 연산이다.

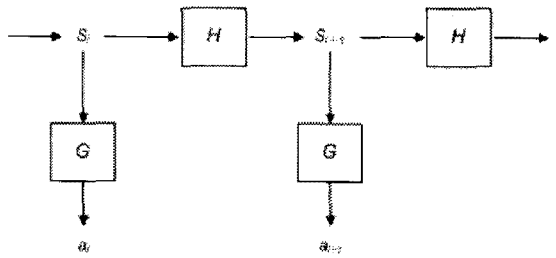

그림 3. Hash-Chain 기법 태그 연산

H와 G는 해시함수이다. 리더는 태그로부터 받은 값을 백엔드 서버(Back-End Server)에 보낸다. 백엔드 서버는 (ID, S_1)의 쌍의 값을 리스트로 가지고 있는다. 그리고, $a'_i = G(H^i(s_1))$의 값을 계산해 놓는다. $a'_i = a_i$인지 체크를 하고 두 값이 동일하다면 a'_i의 쌍인 ID를 반환하게 된다.

위에서 제시된 Miyako Ohkubo의 프로토콜에서 쓰인 H와 G함수는 일방향성 해시함수이기 때문에 불구분성과 전방위보안성을 보장한다. 공격자가 물리적 공격에 의해서 s_{i+1}값을 알았다고 하더라도 해시함수의 특성상 역으로의 계산(s_i를 알아내는 것)은 어렵기 때문이다.

이 기법은 기존의 Hash-Lock 기법의 위치추적 문제와 Randomized Hash-Lock 기법의 전방위보안성 문제점을 해결했으나 모든 태그에 대해 Hash 연산을 수행하므로 데이터베이스에서 연산이 매우 복잡하다는 단점을 가진다.

3. RFID 데이터베이스의 효율적인 검색을 위한 Tag-Grouping

2장에서 언급된 기존의 RFID 프라이버시 보호 기법들은 많은 문제점들을 가지고 있다. Kill Command는 태그를 재사용할 수가 없으며 Active Jamming 기법은 전파방해로 인해 읽어야 하는 태그까지 읽지 못하는 단점이 있다. Hash-Lock 기법은 위치추적 문제를 갖고 있으며 Randomized Hash-Lock 기법은 전방위보안성에 안전하지 못하다는 단점이 있다. Hash-Chain 기법은 기밀성, 불구분성, 전방위보안성을 모두 보호할 수 있는 기법이지만 하나의 태그를 인식하기 위해 많은 데이터베이스 연산이 필요하며 복잡하다는 단점을 가진다. 그러므로 이러한 문제를 해결하기 위해 프라이버시 보호 요건을 만족하며 데이터베이스의 연산량이 적은 프로토콜이 필요하다.

3.1 시스템 가정사항

- tag그룹의 접근비율은 미리 계산되어있다.
- tag그룹은 1000건으로 정의한다.
- 리더 접근비율 범위는 0에서10까지로 정의한다.

- tag의 접근비율이 5이상의 tag만을 먼저 검색한다.
- r : 접근비율
- g : 기준치

RFID 시스템은 태그, 리더, 데이터베이스로 구성이 되어있다. 태그는 제품의 정보를 가진 ID를 가지고 각 제품에 부착하게 되며 태그 내부 연산과 리더의 요청에 응답할 수 있는 상태로 바뀐다. 또한 각각의 태그는 중복되지 않는 ID를 가지고 있다. 제안 기법의 동작은 리더의 요청으로부터 시작된다. 리더는 태그에게 요청을 보내면 태그는 리더의 요청에 의해 자신의 ID를 리더에게 보낸다. 리더는 태그의 ID를 받고 그 정보를 데이터베이스로 보낸다. 데이터베이스는 리더기로부터 요청을 받으면 Tag-Group별 접근비율(r)에 따라 검색할 그룹을 정의한다. 검색된 Tag-Group 범위에서 태그를 검색하여 태그의 정보를 데이터베이스에서 얻어와 리더기로 전송하여 태그의 정보를 파악할 수 있도록 한다.

3.2 데이터베이스 내부 연산

데이터베이스의 검색속도를 향상시키기 위하여 접근비율이 일정 기준치 이상인 그룹과 미만인 그룹을 나누어 검색함으로써 데이터베이스의 검색 효율을 향상시킨다. 제안 시스템은 2단계로 설명할 수 있다. 먼저 접근비율이 높은 Tag-Group을 검색하는 단계와 첫 번째 검색한 그룹에서 해당 Tag-Group을 검색하지 못하였을 경우 접근비율이 높은 Tag-Group을 제외한 나머지 그룹에서 검색을 하는 단계로 구분된다.

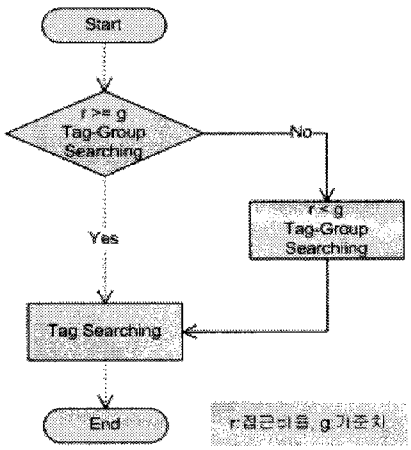

그림 4. Tag-Grouping 과정

[그림 4]는 제안한 RFID 시스템에서 Tag-Grouping 과정을 보여준다. 데이터베이스의 연산량을 단축하기 위하여 데이터베이스에서 태그 정보에 대한 접근비율 (r)이 (g)이상인 Tag-Group을 우선 검색함으로써 검색 범위를 축소시킨다. 만약 접근비율 (r)이 (g)이상인 Tag-Group에서 태그 정보를 검색하지 못하였을 경우 접근비율 (r)이 (g)미만인 그룹만 다시 검색하도록 한다.

IV. 실험 및 평가

MS-SQL 데이터베이스에서 태그 일련번호, 태그 ID, Tag-Group ID, 태그 접금비율 필드를 생성한다. 최소 5만개의 최대 10만개 까지 태그 레코드를 다양하게 생성한다. 생성된 태그의 테이블에 태그의 데이터와 Tag-Group의 데이터를 생성하여 Tag-Group의 정보를 검색할 수 있도록 질의를 수행한다. 접근비율이 상대적으로 높은 Tag-Group으로 범위를 축소한 후 검색을 하며 첫 번째 그룹에서 검색하고자 하는 Tag-Group을 찾지 못하였을 때 접근비율이 상대적으로 낮은 나머지 Tag-Group에서 검색하도록 한다.

표 1. 하드웨어 구성

CPU	Pentium IV 1.6GHz
RAM	2GB
HDD	5G 이상의 여유공간
OS	Windows xp Professional
데이터베이스	MS-SQL Server

표 2. TAG 데이터 생성 필드

ⓐ TAGNO	ⓑ TAGID	ⓒ TAGGROUPID	ⓓ ACCESSRATE
일련번호	태그 ID	Tag-Group ID	태그 접근비율

ⓐ TAGNO: 태그가 생성된 수만큼 증가.
ⓑ TAGID: 태그의 ID는 최소 5만개부터 10만개까지 생성시킨다.
ⓒ TAGGROUPID: Tag-Group ID를 0부터 1000 까지 차례대로 생성한다. Tag-Group ID는 중복되지 않도록 차례대로 생성시킨다.
ⓓ ACCESSRATE: 태그의 접근비율을 0부터 10까지 난수를 발생시켜 생성한다.

표의 실험환경에서 데이터베이스 내부에 태그의 정보를 생성한 후 접근비율을 적용하기 전과 후의 쿼리

비용을 비교하면 [그림5][그림 6]과 같다.

접근비율을 적용하지 않고 전체 데이터를 대상으로 실행한 [그림 5]의 쿼리 처리비용이 56.11%인 것에 비해 전체 데이터 중 접근비율이 5이상인 레코드만을 대상으로 실행한 [그림 6]의 쿼리는 43.89%로 상대적으로 적은 비용을 가지는 것을 확인할 수 있다.

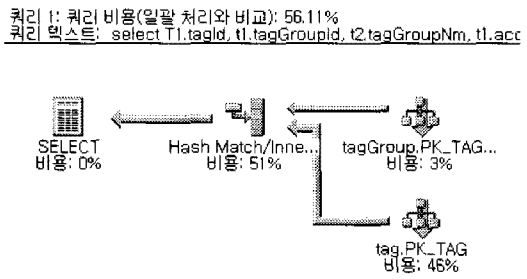

그림 5. Tag-Grouping 적용 전 쿼리 비용

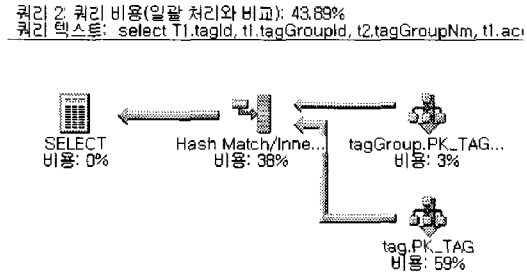

그림 6. Tag-Grouping 적용 후 쿼리 비용

[그림 7]은 데이터베이스의 검색시간을 측정하기 위해서 데이터베이스에 연결한 후 결과를 가져오는데 걸리는 시간을 DateTime.Now.Millisecond 함수를 이용하여 시작 시간과 종료 시간을 체크하여 총 걸린 시간을 체크하는 소스 코드이다.

```
DataSet ds;
lbSearchTimeStart.Text =
    DateTime.Now.Millisecond.ToString();

string strSql = getQueryStr();
ds = con.GetDataSet(strSql);
dataGridView1.DataSource = ds.Tables[0];
lbSearchTimeEnd.Text =
    DateTime.Now.Millisecond.ToString();
lbTotalSearchTime.Text =
    Convert.ToString(
        Convert.ToInt16(lbSearchTimeEnd.Text)
        - Convert.ToInt16(lbSearchTimeStart.Text)
    ).ToString();
```

그림 7. 데이터베이스의 검색시간을 측정하는 코드

데이터베이스에서 태그의 데이터를 DataSet으로 가져오기까지의 시간을 측정해 보았다. 전체 레코드의 수를 다양하게 증가시키면서 접근비율이 5미만인 Tag-Group을 대상으로 태그 레코드 수에 따른 검색시간을 체크하여 (ms)단위로 정리하면 다음과 같다.

표 3. 태그 레코드 수에 따른 검색시간 체크 결과

태그 레코드 수 / 검색시간(ms)	5만	6만	7만	8만	9만	10만
전체데이터대상	54	59	65	72	85	92
제안기법 적용 후 접근비율 5미만인 그룹	45	48	52	57	59	65

데이터베이스의 태그 레코드 수가 많아질 경우 검색시간의 차이를 알아보기 위해 태그 레코드의 수를 5만, 6만, 7만, 8만, 9만, 10만 건으로 늘려 제안기법 적용하기 전 전체 데이터를 대상으로 실행한 검색시간과 제안기법을 적용한 후 접근비율 5 미만인 그룹을 비교해 보았다. 검색된 레코드 수의 변화에 따른 검색시간의 비교 결과는 [그림 8]와 같다.

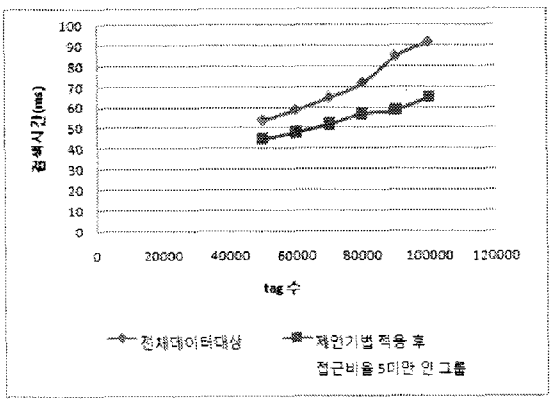

그림 8. 전체 태그 레코드 수에 따른 검색시간 비교

태그 레코드의 수가 커질수록 제안기법 적용 후 검색시간이 전체데이터를 대상으로 검색하는 것보다 상대적으로 줄어드는 결과를 확인할 수 있다.

V. 결론 및 향후연구

RFID 시스템은 광범위한 부분에서 적용되고 있지만

안전한 태그 검색 및 데이터 수집에 불안한 요소들이 많다. 본 논문에서는 보안과 프라이버시 보호를 위한 필수요건을 보장하는 Miyako Ohkubo의 Hash-Chain 메커니즘에서 데이터베이스 연산량이 많은 문제점을 Tag-Grouping을 이용한 효율적인 검색 방법을 제안하였다. 데이터베이스에서 Tag-Group을 검색할 때 태그의 정보에 접근비율 정보를 추가하고 이 접근비율을 이용하여 Tag-Group을 검색할 경우 데이터 전체를 대상으로 검색하는 것이 아니라 기준치 이상의 접근비율을 가진 그룹을 우선 검색함으로써 검색시간을 단축시켰다. 전체 Tag-Group만을 대상으로 검색한 결과와 제안기법 적용 후 5미만의 Tag-Group을 검색할 경우 태그의 레코드 수가 증가할수록 시간차이가 발생한다. 이때 데이터베이스에서 10만개의 레코드 수를 기준으로 접근비율이 5이상인 태그 그룹의 우선 검색 결과 약 30%의 검색시간이 감소하였다.

다만 소량의 레코드를 가진 태그의 데이터 정보를 처리할 경우 태그의 데이터를 검색하는데 큰 효율을 보이지 못하였으나 데이터양이 많아질수록 태그의 접근비율을 이용하여 검색하고자 하는 범위를 축소시킴으로써 전체 태그 데이터를 대상으로 검색하는 것보다 효율적으로 Tag-Group을 검색할 수 있었다. 그러나 태그의 접근비율을 어떻게 계산하여 적용시키는 것에 따라 대용량 데이터베이스에서 원하는 Tag-Group을 검색할 때 검색성능에 영향을 미칠 수 있다. 또한 검색하고자 하는 태그가 어떤 접근비율의 그룹에 포함되어 있는지에 대한 효율적인 계산법이 필요하다.

향후 연구에서는 태그의 접근비율을 효과적으로 산출해 내는 방법과 해당 Tag-Group의 접근비율을 효율적으로 계산하는 연구가 필요하다.

참 고 문 헌

[1] K. Finkenzeller, *RFID Handbook-Second edition*, John wiley & Sons, 2001.

[2] H. H. Huang and C. Y. Ku, "A RFID Grouping Proof Protocol for Medication Safety of Inpatient," Journal of Medical Systems, 2008.

[3] 박승창, "RFID/USN 국제 표준화 동향과 국내 기업의 대응 전략", EIC IT리포트, 2004.

[4] G. Hornback, A. Babu, B. Martin, B. Zoghi, M. Pappu, and R. Singhal, "Automatic Attendance System," Automatic Attendance System Journal, Smart Distributed Systems Group RFIDSensNet Lab., 2001.

[5] J. I. Kang, J. S. Park, and D. H. Nyang, "Privacy Protection Scheme on RFID System," Korea Institute of Information Security and Cryptology paper, Vol.14, No.6, 2004(12).

[6] S. Sarma, S. Weis, and D. Engels, "RFID Systems and Security and Privacy Implications," In CHES 2002, Vol.2523 of LNCS, pp.454-469, 2002(8).

[7] S. Weis, "Security and Privacy in Radio-Frequency Identification Devices," In Master Thesis, 2003(5).

[8] 유성호, 김기현, 황용호, 이필중, "상태기반 RFID 인증 프로토콜", 정보보호학회 논문지, 제14권 제6호, 2004(12).

[9] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic Approach to "Privacy-Friendly" Tags," In RFID Privacy Workshop, MIT, 2003(11).

저 자 소 개

이 병 주 (Byeung-Ju Lee) 정회원

- 2004년 8월 : 한서대학교 컴퓨터공학과(공학사)
- 2006년 8월 ~ 현재 : 인하대학교 정보공학과 석사과정

<관심분야> : RFID/유비쿼터스 시스템

송 창 우(Chang-Woo Song) 정회원

- 2004년 8월 : 한국교육개발원 학점은행제 컴퓨터공학 전공(공학사)
- 2007년 2월 : 인하대학교 컴퓨터·정보공학과(공학석사)
- 2007년 3월 ~ 현재 : 인하대학교 정보공학과 박사과정

<관심분야> : 임베디드/유비쿼터스 시스템, 데이터마이닝

정 경 용(Kyung-Yong Chung) 정회원

- 2000년 2월 : 인하대학교 전자계산공학과(공학사)
- 2002년 2월 : 인하대학교 컴퓨터정보공학과(공학석사)
- 2005년 8월 : 인하대학교 컴퓨터정보공학과(공학박사)
- 2005년 9월 ~ 2006년 2월 : 한세대학교 IT학부 교수
- 2006년 3월 ~ 현재 : 상지대학교 컴퓨터정보공학부 교수

<관심분야> : 유비쿼터스 컴퓨팅, 인공지능시스템, 데이터마이닝, U-CRM

임 기 욱(Kee-Wook Rim) 정회원

- 1977년 2월 : 인하대학교 전자공학과(공학사)
- 1987년 2월 : 한양대학교 전자계산학(공학석사)
- 1994년 8월 : 인하대학교 전자계산학(공학박사)
- 1977년 ~ 1988년 : 한국전자통신연구소 시스템소프트웨어 연구실장
- 1989년 10월 ~ 1996년 12월 : 한국전자통신연구원 시스템연구부장, 주전산기(타이컴)III,IV 개발사업 책임자
- 2001년 7월 ~ 1999년 12월 : 한국전자통신연구원 컴퓨터소프트웨어 연구소장
- 2000년 ~ 현재 : 선문대학교 컴퓨터정보학부 교수

<관심분야> : RDBMS, 운영체제, 시스템구조

이 정 현(Jung-Hyun Lee) 정회원

- 1977년 2월 : 인하대학교 전자과(공학사)
- 1980년 9월 : 인하대학교 전자공학과(공학석사)
- 1988년 2월 : 인하대학교 전자공학과(공학박사)
- 1979년 ~ 1981년 : 한국전자기술연구소 연구원
- 1984년 ~ 1989년 : 경기대학교 전자계산학과 교수
- 1989년 1월 ~ 현재 : 인하대학교 컴퓨터공학부 교수

<관심분야> : 자연어처리, HCI, 음성인식, 정보검색, 고성능 컴퓨터구조