RFID 환경에서 태그 ID의 식별 비트를 이용한 효율적인 태그 인증 기법

장봉임* · 정윤수**· 김용태***· 박길철****

Efficient Tag Authentication Scheme using Tag ID Identification Bits in RFID Environment

Bong-Im Jang* · Yoon-Su Jeong** · Yong-Tae Kim *** · Gil-Cheol Park****

이 논문은 2010년 한남대학교 학술연구조성비 지원에 의하여 연구되었음

요 약

RFID(Radio Frequency IDentification)는 사물 인식을 위한 시스템으로 유통·물류, 의료·보건, 항공・항만 분야 등으로 사용이 확대되고 있다. RFID 시스템은 비접촉식 시스템 환경이고, 동시에 다수의 태그가 인식되므로 태그 인증을 위한 처리 시간의 단축이 중요하다. 그러나 현재까지의 RFID 시스템에 대한 연구는 태그 인증 과정의 보안 취약점 향상을 위한 것이 대부분이었다. 따라서 본 논문에서는 태그 인증 과정에서 보안에도 안전하고 태그 인증 처리 시간의 감소를 위한 효율적인 기법을 제안한다. 본 논문의 제안 기법은 RFID 시스템의 구성요소 중 하나인 데이터베이스에서 태그 ID 검색을 위해 식별 비트를 사용하여 분류된 해당 ID만 검색함으로써 태그 ID 검색 시간을 단축한다. 결과적으로 본 논문의 제안 기법은 데이터베이스의 처리량 및 처리 시간을 감소시켜 태그 ID 인증을 위한 처리 시간을 단축하고, 수동형 태그의 에너지 활용도를 향상시키는 것에 의해, RFID 시스템의 성능 향상을 가져온다.

ABSTRACT

RFID(Radio Frequency IDentification) is a system to identify objects and its usage is being extended to distribution, healthcare, and air&port etc. RFID is a contactless system environment, and reducing tag authentication time is important because multiple tags are identified at the same time. Studies about RFID system so far is, however, mostly to improve security vulnerability in the tag authentication process. Therefore, this paper suggests an efficient scheme to decrease the time of tag authentication which is also safe for the security of tag authentication process. The proposed scheme cuts down on the tag ID search time because it searches only the classified relevant ID in the database, which is one of many components of RFID system, by using identification bits for tag ID search. Consequently, the suggested scheme decreases process time for tag ID authentication by reducing the processing time and the load of the database. It also brings performance improvement of RFID system as it improves the energy applicability of passive tag.

키워드

RFID 시스템, 태그 인증, 해쉬 함수, 데이터베이스

Key word

RFID System, Tag Authentication, Hash Function, Database

* 정회원 : 한남대학교 멀티미디어학과 박사과정(jangg11@nate.com)
** 정회원 : 충북대학교 전자계산학과 네트워크 보안연구실
*** 정회원 : 한남대학교 멀티미디어학부 교수
**** 정회원 : 한남대학교 멀티미디어학부 교수(교신저자)

접수일자 : 2010. 08. 02
심사완료일자 : 2010. 08. 17

Ⅰ. 서 론

최근의 RFID 시스템은 유비쿼터스(Ubiquitous) 환경에서 유용하게 사용되고 있는 사물 인식 및 식별을 위한 기술 중의 하나이며, 유통·물류, 의료·보건, 항공·항만, 금융, 공공분야, 일상생활의 자동화 시스템 등과 같은 다양한 분야에서 폭넓게 응용되고 있다.

RFID 시스템은 현재 사물 인식 시스템으로 사용되고 있는 바코드 시스템과는 달리 한 번에 다수의 개체를 인식할 수 있는 장점을 가지며, 무선 주파수 통신을 사용하므로 개체와 직접적인 접촉 없이 인식이 가능하다. 또한 RFID 시스템은 바코드 시스템보다 효율적인 식별 시스템의 구축이 가능하므로 바코드 시스템을 대체하여 물류 산업, 실시간 재고관리, 산업 자동화, 의료 분야 등의 다양한 분야에서 이용되고 있으며, 앞으로 더욱 활성화 될 것으로 예측된다[1,2,3,4,5].

RFID 시스템은 무선 통신에 의한 데이터 송수신으로 인해 사용자의 프라이버시 침해를 유발할 수 있는 도청, 위치 추적 공격, 스푸핑 공격, 재전송 공격 등의 악의적인 공격 위협이 존재한다[6,7]. 또한 시스템 환경에 따라 리더와 데이터베이스는 동시에 다수의 태그를 인식해야 하므로 태그 정보 인증 절차의 간소함과 신속함이 요구된다. 현재까지 RFID 시스템의 인증 보안 기법에 대해서는 많은 연구[8,9,10,11,12]가 진행되었지만 태그 검색 및 인증을 위한 처리 시간 단축에 대한 연구는 미흡한 실정이다.

따라서 본 논문에서는 프라이버시 침해 공격으로부터 안전성을 보장하며, 데이터베이스의 태그 검색 과정에서 태그 인증 과정에 대한 처리 시간의 단축을 위하여 식별 비트를 이용하여 태그 ID를 검색하는 개선된 기법을 제안한다.

본 논문의 2장에서는 RFID 시스템의 구성과 각 구성요소의 특징을 살펴보고, 시스템 구성요소 중 하나인 백엔드 데이터베이스에서의 태그 검색 방법에 대해 분석한다. 3장에서는 태그 인증 과정에서의 처리 시간 감소를 위한 개선된 인증 기법을 제안하고, 4장에서는 제안한 기법의 성능 분석 및 평가 결과를 기술한다. 마지막으로 5장에서는 결론과 향후 연구 방향을 제시한다.

Ⅱ. 관련연구

본 장에서는 RFID 시스템의 구성에 대해 기술하고, 데이터베이스에서의 태그 인증 과정에 대한 처리 시간 단축을 위한 기존의 태그 검색 기법들을 분석한다.

2.1 RFID 시스템의 구성

RFID는 무선 주파수를 이용하여 사물을 자동으로 인식하는 기술로, 사물의 정보를 담고 있는 태그(Tag), 태그와 통신하여 태그 정보를 취득하는 리더(Reader), 정보의 저장과 관리를 담당하는 백엔드 데이터베이스(Back-End Data base)로 구성되며, 다음의 그림 1은 RFID 시스템의 구성도를 나타낸다. 일반적으로 RFID 시스템에서의 리더와 백엔드 데이터베이스 사이의 통신 채널은 안전하다고 가정한다.

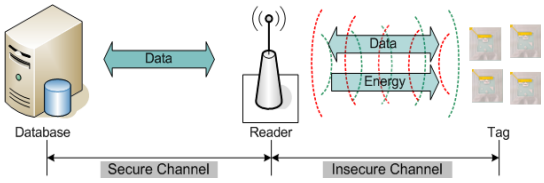

그림 1. RFID 시스템 구성도
Fig 1. RFID system Architecture

RFID 태그는 IC 칩(Integrated Circuit Chip)과 무선 통신으로 데이터를 읽고 쓰기 위한 안테나로 구성되며, 기본적인 연산 및 데이터를 저장하는 역할을 담당한다. 또한 태그는 개개의 사물 인식을 위해 고유한 ID를 가지게 되며, 이러한 태그 ID는 태그를 인증하기 위한 검증 값으로 이용된다.

리더는 무선 주파수를 이용하여 태그와 통신하고 태그로부터 송신된 데이터를 백엔드 데이터베이스에 전송하거나 백엔드 데이터베이스로부터의 전송 결과를 다시 태그에게 전달하는 역할을 한다.

백엔드 데이터베이스는 각 태그를 인증하기 위한 정보를 저장하고 관리하는 장치이고, 리더로부터 전송된 태그 데이터를 기반으로 태그를 인증하고, 인증 결과는 리더를 통해 태그로 전송하는 역할을 담당한다.

2.2 데이터베이스에서의 태그 검색 방법

RFID 시스템에서 주로 사용되는 태그는 저가형·수동형 태그로 계산능력이 제한되므로 인증 과정에서 가벼운 연산을 사용하는 기법이 주로 사용되며, 리더와 태그의 무선 통신으로 인하여 악의적인 침입자에 의한 인증 위협이 항시 존재하므로 연산이 복잡하지 않으면서 보안성이 확보되는 기법이 요구된다. 또한 수동형 태그는 내장 배터리가 없어 리더에게 에너지를 제공받는 형태이므로 태그의 에너지 소모를 최소화 할 수 있는 인증 기법이 필요하다. 이에 따라 현재까지 다양한 태그 인증 기법들이 제안[8,9,13]되었다. 제안된 기법들은 태그에서의 연산과정에서 난수 값을 이용하므로 매번 전송 데이터가 달라지고, 태그와 리더사이의 값 전송 시 암호화 된 값을 전송하므로 도청과 위치 추적 등의 무선 주파수의 통신 위협으로부터 안전하지만, 데이터베이스에서의 태그 검색 과정에서 대부분 태그 ID 전체와 연산을 실시하는 전수 검색의 방법을 사용한다. 그러나 이러한 방법은 태그 인증 시간을 증가시켜 시스템 전체의 인증 시간이 증가될 뿐만 아니라 수동형 태그의 에너지 활용에 비효율적이므로 다수의 사물 인증을 위한 RFID 시스템 환경에 적합하지 않은 단점이 있다.

이러한 태그 ID 전수 검증의 단점을 보완하기 위해 데이터베이스에서의 태그 인증에 대한 처리 시간의 단축을 위한 방법으로 Bloom Filter를 이용한 방법[14,15]과 접근비율에 따라 태그를 그룹화하는 방법[16]이 제안되었다.

Bloom Filter란 주어진 원소가 어떤 집합에 속하는지의 여부를 검사하는데 사용할 수 있는 자료 구조[17]로 간단하고 공간 효율성이 뛰어난 반면, 집합에 포함되어 있지 않은 원소를 포함된 것으로 잘못 판단하는 확률인 긍정오류율이 존재하는 단점이 있다[15]. 또한 위의 기법에서 제안한 수식에 따르면 태그 검색의 식별자로 사용되는 Bloom Filter의 개수와 비트수에 따라 데이터베이스에서 수행하는 해쉬 연산의 횟수가 달라지므로, 적정한 Bloom Filter 집합을 구성하는데 어려움이 따른다.

또 다른 방법으로 제안된 태그의 접근비율에 따른 태그 그룹화 기법은 각 태그마다 접근 비율을 달리하여 접근 비율이 높은 태그들을 우선 검색하는 방법으로 데이터베이스의 연산 시간을 감소시켰으나, 태그의 접근 비율 그룹화에 대한 명확한 구분과 계산법이 제시되지 않아 실제 시스템 환경으로의 적용에 어려움이 있으며, 동시에 다수의 태그들이 접근할 경우 시스템의 효율성이 감소되는 단점이 있다.

Ⅲ. 제안 시스템

본 장에서는 RFID 시스템에서 태그 인증에 대한 처리 시간 감소를 위해 태그 ID의 식별 비트를 이용한 태그 인증 기법을 제안한다. 제안 기법의 태그 ID 앞 4비트는 태그를 구분하는 식별 비트로 사용되며, 리더와 데이터베이스 사이의 통신은 안전한 채널이라고 가정한다. 본 논문에서 제안하는 시스템의 전체 구조는 다음의 그림 2와 같다.

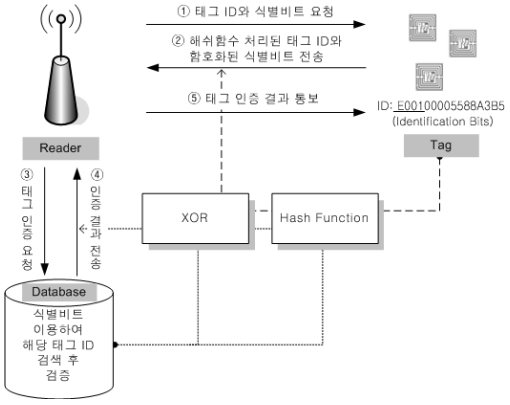

그림 2. 제안시스템의 구조
Fig 2. Structure of Suggested System

제안 시스템은 태그를 인식한 리더가 식별비트로 사용될 값과 태그 인증을 위한 검증값을 태그에게 요청하여 수신된 값을 데이터베이스에게 전송하면, 데이터베이스는 식별비트를 포함하는 태그 ID를 검색하여 태그를 검증하는 절차로 구성된다.

3.1 태그 ID 상호 인증 과정

본 논문에서 제안한 태그 ID의 식별 비트를 이용한 RFID 시스템의 태그 인증 과정은 그림 3과 같으며, 각 부분별 역할에 따른 인증 절차는 다음의 그림 3과 같다.

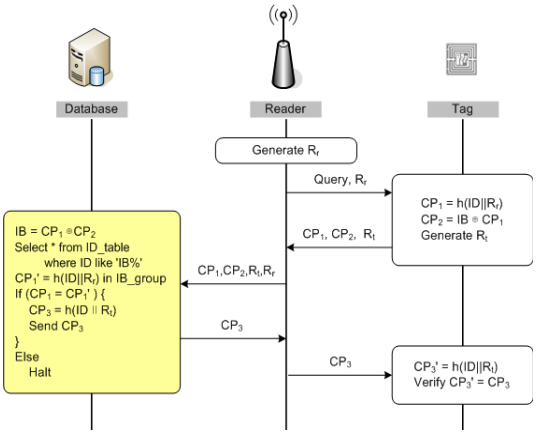

그림 3. 상호 인증 과정
Fig 3. Authentication Process

- h( ) : 해쉬 함수
- ⊕ : XOR 연산
- R_r : 리더가 생성한 난수
- R_t : 태그가 생성한 난수
- CP : h(ID ‖ 난수) 연산 결과 값
- IB : 태그 ID 식별 비트(Identification Bits)

첫째, 리더는 자신의 인식 범위 내에서 태그의 존재가 인식되면 난수 R_r을 생성한 후 태그에게 R_r과 질의를 전송한다. 리더의 질의를 받은 태그가 자신의 ID와 R_r을 연접 해쉬 함수 처리하고, 식별비트의 XOR 연산 과정을 수행한 후 생성된 결과 값을 리더에게 전송하면 리더는 수행된 결과 값을 데이터베이스에게 전송한다. 또한 리더는 데이터베이스의 태그 인증과정이 종료되면, 데이터베이스로부터 해당 태그를 정당한 태그로 인증한 인증결과 값을 태그에게 반환하는 역할을 담당한다.

둘째, 태그는 리더로부터 수신된 R_r과 자신의 ID를 연접 해쉬 함수로 처리하여 CP_1값을 생성한다. 또한 전체 태그 ID 중에서 식별 비트로 사용되는 1~4번째 비트의 코드와 CP_1을 XOR 연산 수행하여 자신이 생성한 난수 R_t와 연산을 처리한 2개의 값 CP_1, CP_2를 함께 리더에게 전송한다. 그리고 마지막 절차에서는 리더로부터 수신된 CP_3이 정당한 값인지 검증한 후 전체 인증 과정을 마친다.

셋째, 데이터베이스는 리더로부터 수신된 CP_1과 CP_2의 값으로부터 IB를 획득한 후, 전체 태그 ID를 검증하는 대신, IB를 포함하는 태그 ID그룹 내에서 태그 ID와 리더의 난수 R_r을 연접 해쉬 함수 처리하여 검증 연산을 수행하고, 태그의 연산 값과 일치하는 값을 검색한다. 그 결과 태그로부터 전송된 CP_1과 일치하는 CP_1'값이 검색되면 태그 정보를 정당한 정보로 판단하고, 태그의 난수 R_t와 태그 ID와의 연접 해쉬 함수를 처리한 결과 값인 CP_3을 리더에게 전송한다.

3.2 식별 비트를 이용한 태그 ID 검색 과정

RFID 시스템에서 사용하는 태그 ID는 각 태그를 구분하기 위한 고유한 코드체계이다. 제안 시스템에서 사용한 태그 ID는 표 1과 같이 16진수 16비트의 숫자 코드로 구성되며, 특히 1~4번째 코드는 데이터베이스에서의 빠른 태그 검색을 위한 식별 비트로 사용한다.

표 1. 태그 ID 코드 체계
Table 1. Composition of Tag ID code

태그 구분	식별 비트	태그 ID
태그 1	E001	E00100005588A3B5
태그 2		E00100005588ABC1
태그 3		E00100005588ABC2
태그 4		E00100005588ABD1
태그 5	E010	E01011C032A3B500
태그 6		E01011C032A3B511
태그 7		E01011C032A3B5AA
태그 8		E01011C032A3B5AC
태그 9	E011	E0110110A3F44000
태그10		E0110110A3F44005
. .	. .	. .

제안 시스템에서는 태그 인증을 위한 데이터베이스의 연산 과정 중에서 태그로부터 전송된 해쉬 함수의 처리 값과 일치하는 값을 검색하기 위하여 일반적으로 사용되는 태그 ID의 전체를 이용하여 검증하는 방법을 사용하지 않는다. 본 논문에서의 제안 기법은 XOR 연산을 사용하여 태그의 검증을 위한 리더의 난수와 태그 ID와의 해쉬 함수 처리값 CP_1과 태그 ID의 식별비트를

암호화 한 CP_2의 값으로부터 $IB=CP_1 \oplus CP_2$ 연산을 수행하여 식별 비트로 사용될 태그 ID의 1~4번째 코드를 획득한다. 그리고 태그 ID 리스트 테이블 내에서 해당 코드를 포함하는 태그 ID를 검색하여 $CP_1'=h(ID \| R_r)$의 연산을 수행한다. 연산의 검증 결과 태그로부터 수신된 값과 일치하는 값이 검색되면 태그를 인증하고, 마지막 인증 절차를 위해 태그 ID와 태그의 난수 R_t를 연접 해쉬 함수 처리하여 리더에게 전송한다.

Ⅳ. 성능 분석 및 평가

본 장에서는 제안 기법의 성능을 분석하기 위하여 기존의 전체 태그 ID를 검색하는 기법과 본 논문에서 제안하는 ID의 일부를 식별 비트로 사용하여 해당 ID만 검색하는 기법과의 태그 인증을 위한 처리 시간을 비교하였다.

4.1 성능 분석

데이터베이스에서의 태그 ID 검색 및 태그 인증에 대한 성능 평가를 위하여 본 논문에서는 태그 ID 식별 비트 분류 비율 그리고 태그 개수의 변화에 따라 각각의 성능을 비교 분석한다. 태그 ID 검색 및 태그 인증에 대한 처리 시간 분석을 위하여 표 2와 같은 파라미터를 설정하였다.

표 2. 시스템 파라미터
Table 2. System Parameter

사항	내용
T_num(태그 개수)	1,000개~10,000개
IB_rate(태그 ID 식별 분류 범위)	25%~100%
AP_t(태그 ID 검색 및 인증처리 시간)	240ms(carrier frequency : 13.56MHz)

첫 번째 분석방법은 태그 ID 식별 비트 분류 비율에 따른 태그 ID 인증을 위한 처리 시간의 변화에 대한 비교이다. 태그 ID 식별 비트 분류 비율은 모든 태그를 인식할 경우는 100%로 설정하고, 그 외의 분류 비율을 각각 50%, 25%로 설정하였다. 태그 ID 개수는 1,000개부터 10,000개까지 매 단계별 1,000개씩 증가시켜 실험하였다.

두 번째 분석방법은 태그 개수의 변화에 따른 태그 ID 인증을 위한 처리 시간의 차이를 검증한다. 실험을 위하여 태그 개수는 각각 1,000개, 5,000개, 10,000개의 3가지 경우로 분류하고, 각 개수별 태그 ID 식별 비트 분류 비율을 100%, 50%, 25%로 구분하여 처리 시간 변화의 차이를 분석하였다.

태그 인증을 위한 처리시간의 계산을 위해 각 분류별 T_num×IB_rate×AP_t의 식을 사용했으며, 태그 인식 과정에서의 충돌은 없는 것으로 가정한다.

4.2 성능 평가

본 절에서는 위와 같은 분석방법으로 기존 태그 ID 검색 기법과 제안 기법의 효율성을 비교 평가하였다.

첫 번째 분석 방법에 따른 태그 ID의 식별 비트 분류 비율 증가와 데이터베이스에서의 태그 ID 인증을 위한 처리 시간과의 관계에 대한 결과는 그림 4와 같다. 그림 4에서 나타나는 것과 같이 데이터베이스에서 전체 태그 ID를 검색한 100% 추세선의 태그 인증을 위한 처리 시간 증가율과 태그 ID의 50%, 25%를 검색한 각각의 추세선 증가율이 큰 차이를 보인다. 특히, 태그 ID 식별 비트 분류율이 25%일 경우의 태그 개수 증가에 따른 처리 시간 증가율과 전체 태그 검색의 처리 시간 증가율을 비교했을 때, 약 4배 정도의 증가 폭 차이를 나타낸다. 이러한 결과는 태그 ID 식별 비트 분류율이 세분화 될수록 제안 시스템이 더욱 효과적으로 사용될 수 있음을 나타낸다.

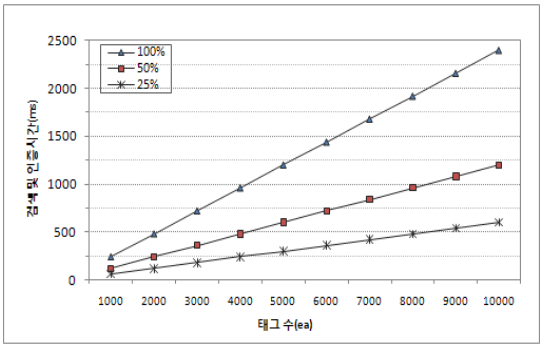

그림 4. 식별 비트 분류율에 따른 인증처리시간
Fig 4. Tag Authentication Time by Identification Bits classification rate

그림 5는 태그 개수 증가에 따른 태그 인증을 위한 처리 시간 증가율의 변화에 대한 결과를 나타내며, 동일한 태그 개수 내에서 식별 비트 분류율에 따른 처리 시간의 증감폭을 나타낸다.

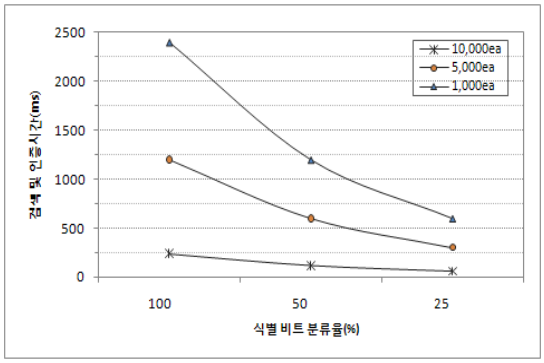

그림 5. 태그 개수 증가에 따른 인증처리시간
Fig 5. Tag Authentication Time by Tag increasing

태그 ID의 개수가 10,000개 일 경우, 전체 태그 ID의 인증을 위한 처리 시간과 식별 비트 분류 비율이 25%일 경우의 처리 시간 차가 2,160ms 정도인 반면, 태그 ID의 개수가 1,000개 일 경우, 처리 시간의 차이가 200ms 정도로 나타난다. 따라서 태그의 개수가 증가할수록 식별 비트 분류 비율에 따른 처리 시간의 증가폭이 비례하여 감소함을 나타낸다. 이는 제안 기법이 다수의 태그 ID 인증 환경에서 더욱 효율적으로 활용될 수 있음을 나타낸다.

그림 5의 분석 결과, 제안 기법은 다수의 태그 인식이 필요한 상품 인식 및 물품 관리 등의 유통 분야와 재고 관리 등의 물류 분야에서 유용하게 적용 가능함을 나타낸다. 특히, 기존 기법과는 달리 태그 ID를 분류하고 필터링 하는 방법이 매우 간단하여 구현이 쉽다는 장점을 갖는다. 이는 결과적으로 전체 시스템의 총 처리량과 연산시간을 감소시켜 수동형 태그의 에너지 효율을 증가시킨다. 또한 태그의 인증 절차를 강화하여 무선 주파수 통신을 사용하는 RFID 시스템의 취약점인 프라이버시 침해에도 안전한 기법을 제공한다.

위와 같이 제안된 기법은 기존 연구들에서 사용되던 태그 ID의 전수 검색 대신에 식별 비트를 이용하여 분류된 해당 태그만을 검색함으로써 데이터베이스에서의 태그 검증 시간을 효과적으로 감소시키는 장점을 갖는다.

V. 결 론

최근 RFID 시스템이 물류·유통 분야에서 바코드 시스템을 대신한 상품인식의 도구로 사용이 활성화 되면서 다수의 태그 인식을 필요로 하는 환경에서의 태그 인증을 위한 처리 시간 감소에 대한 연구가 필요하다. 태그 인증을 위한 처리 시간의 단축은 태그의 에너지 소모를 최소화 할 수 있으므로 비용적인 측면에서 활용이 유용한 수동형 태그를 사용하는 시스템에서 더욱 중요하다. 또한 RFID 시스템은 무선 주파수 통신을 이용하므로 프라이버시 침해의 위협이 존재한다. 따라서 프라이버시 침해의 위협으로부터 안전하고, 태그의 에너지 활용 능력 향상 및 데이터베이스의 연산 처리량 감소에도 효율적인 연산 기법에 대한 연구가 요구된다. 이러한 문제점을 해결하고자 본 논문에서는 기존의 기법들을 보완한 효율적인 인증 기법을 제안하였다.

제안 기법은 데이터베이스에서의 태그 데이터 검증 과정에서 기존의 전체 ID를 검색하던 방법과는 달리 일정 ID를 추출 할 수 있는 식별 비트의 사용으로 검색의 효율성을 높였다. 또한 복잡한 연산 절차 없이 1회의 XOR 연산만으로 식별 비트를 산출할 수 있어 태그와 데이터베이스의 연산량을 최소화 하였으며, 프라이버시 침해에도 안전한 검증 기법으로 RFID 시스템의 보안 취약점을 강화하였다. 제안 기법의 분석 결과, 태그 ID 전수 검색 기법에서의 태그 인증을 위한 처리 시간과 식별 비트를 사용한 처리 시간의 편차가 태그 수가 많을수록 크게 나타나 다수의 사물 인증을 위한 RFID 시스템 환경에서의 효과적인 적용이 기대된다. 결과적으로 제안 기법의 적용은 시스템 전체의 처리 시간 감소 효과로 저가형·수동형 태그의 에너지 활용도를 높여 전반적인 RFID 시스템의 성능 향상을 가져온다.

향후 연구에서는 데이터베이스 내에서의 태그 인증을 위한 처리 시간뿐만 아니라 태그와 리더간의 인증 시간까지 고려한 시스템 전체의 처리 시간에 대한 연구가 필요하다.

참고문헌

[1] Stephen A. Weis, Sanjay E. Sarma, R. L. Rivest, and D. W. Engels, “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems”, *Security in Pervasive Computing 2003,* LNCS 2802, pp.201-212, 2004.

[2] Klaus Finkenzeller, *RFID Handbook,* Second Edition, John Wiley& Sons, 2003.

[3] G. Avoine and P. Oechslin, “RFID Traceability: A Multilayer Problem”, *In Proceeding of the Financial Cryptography* ’05 - FC’05, LNCS 3570, pp.125-140, 2005.

[4] S. Sarma, S. Weis and D. Engels, “Radio- Frequency identification: security Risks and Challenges”, *RSA Laboratories Cryptobytes,* Vol.6, No.1, pp.2-9, 2003.

[5] S. E. Sarma, S. A. Weis and D. W. Engels, “RFID systems, security & privacy implications”, *Cryptographic Hardware and Embedded Systems-CHES 2002,* LNCS 2523, pp.454-469, 2003.

[6] Yuichi Kobayashi, Toshiyuki Kuwana, Yojitanigughi and Norihisa Komoda “Group Management of RFID Passwords for Privacy Protection”, *Electronics and Communications in Japan,* Vol. 92, No. 10, pp.24-31, 2009.

[7] Alex X. Liu, LeRoy A. Bailey, ″PAP: A Privacy and authentication protocol for passive RFID tags″, *Computer Communications,* 32, pp.1194-1199, 2009.

[8] Hung-Yu Chien, Chen-Wei Huang, ″A Lightweight Authentication Protocol for Low-Cost RFID″, Journal of Signal Processing Systems, 59, pp.95-102, 2010.

[9] Woo-Sik Bae, Shin-Hyeong Choi, Kun Hee Han ″RFID Security Authentication Protocol for the Ubiquitous Environment″, Korea Society of Computer Information, Vol. 12, No. 4, pp.69-75, 2007.

[10] H. Chien, C. Chen, “Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards”, Computer Standards & Interfaces, Vol. 29, pp.254-259, 2007.

[11] Soo-Young Kang, Deok-Gyu Lee, Im-Yeong lee, ″A study on secure RFID mutual authentication scheme in pervasive computing environment″, Computer Communications, Vol. 31, pp.4248-4254, 2008.

[12] Hung-Yu Chien, Chi-sung Laih, ″ECC-based lightweight authentication protocol with untraceability for low-cost RFID″, Journal of Parallel and Distributed Computing, Vol. 69, pp.848-853, 2009.

[13] 안해순, 부기동, 윤은준, 남인길, “RFID/USN 환경을 위한 개선된 인증 프로토콜”, 전자공학회 논문지, 제46권 CI편, 제1호, pp.1-10, 2009.

[14] 김진호, 서재우, 이필중, “저비용 RFID 시스템에 적합한 효율적인 인증 방법”, 정보보호학회, 제18권, 제2호, pp.117-128, 2008.

[15] 원태연, 천지영, 박춘식, 이동훈, “수동형 RFID 시스템에 적합한 효율적인 상호 인증 프로토콜 설계”, 정보보호학회, 제18권, 제6(A)호, 2008.

[16] 이병주, 송창우, 정경용, 임기욱, 이정현, “RFID 시스템에서 Hash-Chain 기반 Tag-Grouping을 이용한 안전하고 효율적인 데이터베이스 검색”, 한국콘텐츠학회논문지, Vol. 9, No. 9, pp.9-17, 2009.

[17] Andrei Broder and Michael Mitzenmacher, ″Network Applications of Bloom Filter: A Survey″, *Internet mathematics,* Vol. 1, pp.485-509, 2004.

저자소개

장봉임(Bong-Im Jang)

2003 한남대학교 멀티미디어학과 공학석사

2008-현재 한남대학교 멀티미디어학과 박사과정

※관심분야 : RFID/USN, 센서 웹, 멀티미디어, 웹서비스

정윤수(Yoon-Su Jeong)

2000 충북대학교 전산학과 석사
2008 충북대학교 전자계산학 이학박사

※관심분야 : 센서 보안, 암호 이론, Network Security, 이동통신 보안

김용태(Young-Tae Kim)

1984 한남대학교 계산통계학과 학사
1988 숭실대학교 전산학과 공학석사
2008 충북대학교 전산학과 이학박사
2002-2006 (주)가림정보기술 이사
2006-현재 한남대학교 멀티미디어학부 교수
※관심분야 : 모바일 웹서비스, 정보보안, 센서 웹, 모바일 통신보안, 멀티미디어

박길철(Gil-Cheol Park)

1983 한남대학교 계산통계학과 학사
1986 숭실대학교 전산학과 공학석사
1998 성균관대학교 정보공학과 박사
2006 UTAS, Australia 교환교수
1998-현재 한남대학교 멀티미디어학부 교수
※관심분야 : multimedia and mobile communication, network security