# u-Vehicle 환경에 적합한 RFID 인증 메커니즘

## Mechanism of RFID Authentication for u-Vehicle

이윤정, 김도현
제주대학교

Yoon-Jung Rhee(rheeyj@cheju.ac.kr), Do-Hyeon Kim(kimdh@cheju.ac.kr)

**요약**

u-Vehicle은, 위치정보에 기반 한 텔레매틱스 서비스뿐 아니라, RFID 기술을 이용하여 움직이는 자동차 안에서의 유비쿼터스 세상을 구축하려는 기술 모델이다. u-Vehicle 환경에서는 RFID가 본래의 목적과 달리 추적, 감시 등 부적절하게 사용될 소지가 크며, 이렇게 될 경우 개인의 프라이버시 침해하게 되는 등, 정보보호 측면이 취약하게 된다. 여기에 사용되는 저가의 RFID 태그는 보안에 취약한 알고리즘을 이용하고 있다. 본 논문에서는 u-Vehicle 환경에서 RFID가 갖는 정보 보안상의 취약점을 도출하였다. 또한 이를 해결하기 위한 방법으로서, 해쉬 함수와 배타적 논리합 연산을 사용하고, 상호인증 단계를 줄여 적은 비용으로 RFID 태그의 안전성을 증가시킬 수 있는 메커니즘을 제시한다.

■ 중심어 : | u-Vehicle | 텔레매틱스 | RFID | 인증 | 정보보호 |

**Abstract**

The concept of u-Vehicle is a technological model that people try to build the ubiquitous world in the car which moves, by using the RFID technology as well as the telematics service based on the location. RFID is weak on the point of information security because RFID has possibility for being abused such as chasing, counterfeiting, and invading personal privacy. RFID's tags use a weak cryptographic algorithm. This paper presents the vulnerabilities of information security under u-Vehicle environments. To solve that, we propose a mechanism enhancing RFID tag's security but with low cost by reducing the number of mutual authentication stages and using the hash function.

■ keyword : | u-Vehicle | Telematics | RFID | Authentication | Information Security |

## I. 서 론

세계는 지금 유비쿼터스 세상을 지향점으로 하여 그에 필요한 기술들을 먼저 선점하고자 앞 다투어 관련 연구에 박차를 가하고 있다[1]. RFID(Radio frequency identification) 은 필요한 모든 것에 RFID 태그를 부착하여(Ubiquitous) 사물을 인식(Identification)하고, 주변의 환경 정보(온도, 습도, 오염정보, 균열정보 등)를 탐지하여 이를 실시간으로 광대역통합망(BcN), 즉 인터넷에 연결하여 정보를 관리하는 것을 의미한다. 좀 더 간단히 말해서, 기존의 인터넷이 사람 중심으로 초고속, 무선, 휴대 인터넷으로 발전을 거듭하여, 앞으로는 사물을 실시간으

* 본 연구는 논문은 2005년도 정부재원(교육인적자원부 학술연구조성사업비)으로 한국학술진흥재단의 지원을 받아 연구되었습니다.(KRF-2005-331-D00374)
접수번호 : #080523-002
접수일자 : 2008년 05월 23일
심사완료일 : 2008년 06월 17일
교신저자 : 김도현, e-mail : kimdh@cheju.ac.kr

로 모니터링하고 제어가 가능한 새로운 유비쿼터스 인터넷이 출현함을 의미한다[2].

텔레매틱스와 RFID 를 결합하는 새로운 서비스 모형인 u-Vehicle의 개념은 다음과 같다. 이동중인 자동차 안에서, 위치정보에 기반 한 텔레매틱스 서비스뿐 아니라 RFID 기술을 이용하여 주위의 RFID를 부착하고 있는 대상을 이용하여 자동차들이 움직임에 따라 시시각각 달라지는 네트워크 속에서도 가능한 통신 서비스를 제공, 즉 자동차 안에서의 유비쿼터스 세상을 구축하려는 기술 모델이라고 정의할 수 있다.

u-Vehicle 기술 모델이 구축되면 다음과 같은 이점이 있다.

- RFID/USN, Telematics, ITS, CDMA, WiBro, CCTV 서비스 복합기기의 테스트베드 제공 및 RFID/USN, 텔레매틱스, ITS 미들웨어간의 서비스 융합 기술 개발을 통한 데이터처리 능력 향상으로 소프트웨어 산업이 활성화
- 기존 GPS 체계를 보완하여 RFID를 기반으로 한 보다 정밀한 위치 보정 서비스 제공
- 차량등록에서부터 폐기까지의 차량관련 각종 업무에서 차량번호, 차대번호, EPC, IPv6 체계 연계 방안 도출을 통해 향후 자동차산업과의 연계 발전 전략 전개 가능
- 도난, 분실차량의 위치 추적 서비스 제공으로 차량 차주에 대한 권익 보호
- 거주자우선주차제 시행에 따른 편리한 차고지 증명 서비스로 확산
- 사고다발지역 통과 차량에 대한 이력 관리를 통하여 인명사고 발생시의 구간 통과 대상 차량에 대한 정보 제공
- 차량인식을 기반으로 한 주차 및 주유서비스 연계로 편리한 차량 서비스 제공
- 민간부문의 보험 및 차량정비 서비스 활성화 기회 제공
- 자동차 회사들이 갖는 차량 출고 이후의 고객관리 연계 시 부가서비스 개선
- 10부제 운행 차량 및 장애인 차량에 대한 우선 주차 등의 제도 개선을 위한 정책 전개용이

RFID를 기반으로 하는 u-Vehicle 환경에서, 한 정보사회의 요구를 충족시키고 변화에 대처하기 위해서는 RFID 기술의 영향력과 필요성에 비추어 볼 때, 정보보호와 보안에 대한 위협은 미래에 더욱 편리한 유비쿼터스 환경으로 나아가는데 있어 가장 큰 장애가 될 것이다. 따라서 본 논문에서는 안전한 u-Vehicle을 위한 RFID 인증 메커니즘을 제안한다. u-Vehicle 환경에서의 RFID가 본래의 목적과 달리 추적, 감시 등 부적절하게 사용될 소지가 크며, 이렇게 될 경우 국민 생활의 프라이버시를 심각히 침해할 수도 있는 문제점 등, 정보보호 측면에서 취약하다[3-5].

u-vehicle 시스템에 부착되어 있는 태그가 보안 메커니즘이 없는 RFID 태그인 경우, 인근의 인증 받지 않은 불법 리더로부터 데이터 전송 요구 전파를 받게 된다면, 태그는 갖고 있는 고유한 데이터로 응답하게 되어 보안상의 위협이 될 수 있다. 여기서 사용되는 태그들은 설계가 단순하고 저가이며, 단위시간당 다량의 태그 판독이 가능하지만, 보안상 많은 문제점을 갖고 있다.

인증 메커니즘을 포함하고 있는 RFID 태그의 경우는 앞서의 경우보다는 비교적 안전하지만 설계가 더 복잡해지고, 그로 인해 태그 자체 비용이 증가하게 되고, 태그 판독에 드는 시간 또한 상대적으로 증가하면서 판독 시스템 운영에 필요한 전체적인 비용도 증가하게 된다.

이런 문제점들을 해결하기 위한 여러 가지 연구들이 진행되어 왔다. 인근에 위치하고 있는 허가 받지 않은 즉, 불법적인 리더의 도청으로부터 RFID 태그를 보호하기 위한 연구로, 경우에 따라 태그를 비활성화 하는 방법, 재기록 가능 메모리의 응용, 상호인증, 키의 다양화와 같은 방법들이 있다[6][13]. 본 논문에서는 상호인증 단계를 줄이고 해쉬 함수에 배타적 논리합 연산을 추가하여 비용은 줄이면서 더 효율적이고 안전하게 RFID 태그를 보호할 수 있는 메커니즘을 제안한다.

본 연구는 제 1장 서론에 이어 제 2장에서는 RFID 인증에 대한 관련연구를 간략하게 언급하고, 제 3장에서는 본 논문에서 제안하는 u-vehicle 에 적합한 RFID 인증 메커니즘을 설명한다. 마지막으로 제 4장에서는 결론을 맺는다.

## II. 관련연구

RFID 시스템의 보안과 개인정보 보호와 관련된 문제들을 해결하기 위한 기존의 연구들은, 태그의 비활성화 방식과 인가된 리더에만 응답할 수 있게 하는 판독 접근제어로 나눌 수 있다. 고정된 판독 접근제어는 인증 처리로 대표된다. 인증은 중요한 RFID 보안 표준이다.

리더가 태그의 ID를 요구한다면, 태그는 먼저 해당 리더의 인증 여부를 확인해야한다. 인증 처리를 하는 동안 태그는 우선 리더에게 난수를 전송한다. 리더는 자신의 ID와, 태그가 전송한 난수를 정해진 함수로 처리한 값을 태그에게 응답한다. 각각의 질문에 대해 리더가 만들어내는 값은 각기 다르다. 따라서 결과 데이터가 도청된다 하여도 공격자는 그 다음의 질문에서 인증을 통과할 수 없게 된다. 이러한 인증 기반 난수 메커니즘은 위조 및 재전송 공격을 방지할 수 있다.

### 1. 삼단계 상호인증 프로토콜

단순한 RFID 보안 시스템은 일반적으로 리더와 RFID 태그 사이의 도청과 위조 방지 뿐 아니라 상호인증 능력을 가질 수 있게 설계된다. 인증되지 않은 리더는 태그ID를 판독할 수 없고 위조 태그를 구별할 수도 없다.

상호인증은 먼저, RFID 태그가 리더에게 인증되고, 그 후 리더가 RFID에게 인증되는 순서를 따른다. 그 후 서로 간의 통신이 이루어진다. 리더와 RFID 태그 사이의 상호인증은 보통 ISO 9798의 3단계 상호인증 원리를 기반으로 한다. ISO 9798은 [7]을 통하여, 통신의 두 주체는 상대의 비밀키를 확인한다. [그림 1]은 3단계 상호인증을 도식화한 것이다[8].

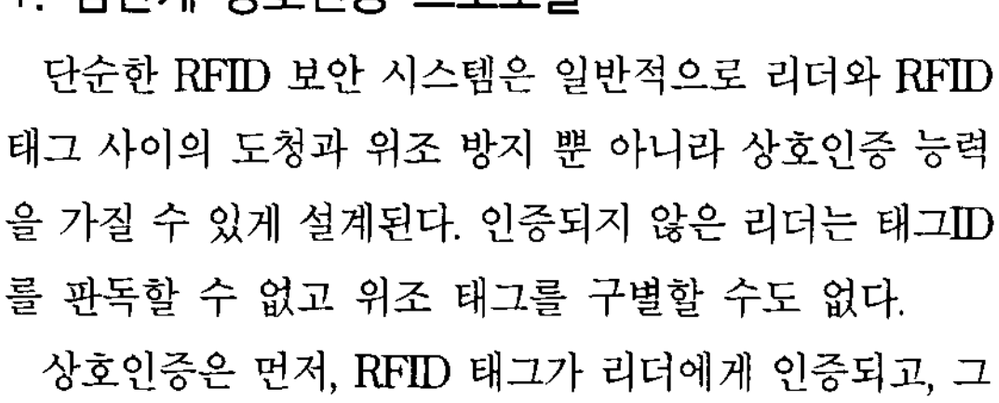


그림 1. RFID 태그와 리더 간의 3단계 상호인증 절차

이 3단계 상호인증 절차에서 태그는 (1) $K_{AB}$ 비밀 키 저장 공간을 갖게 되고, (2) 난수 $R_A$ 생성하며, (3) 암호화 $Token_{AB}$ 및 복호화 $Token_{BA}$ 알고리즘을 이용한다.

이 경우, 통신을 하기 위해서는 리더와 태그 사이에 3단계 인증 처리가 필요하다. 여기서 주요 위험 요소는, 만약 리더와 태그의 사이에 통신이 빈번해지면, 동일한 암호 키 $K_{AB}$을 소유하는 모든 태그가 쉽게 발견될 수 있다는 것이다.

### 2. 키 다양화

3단계 상호인증 메커니즘을 기반으로 하여, RFID 시스템의 보안을 더욱 강화하기 위한 방법 중의 하나는, [그림 2]와 같이, 키 다양화 기법[9]를 적용 것이다. 키 다양화 기법에 기반을 둔 인증 프로토콜의 개념은 아래와 같다[9].

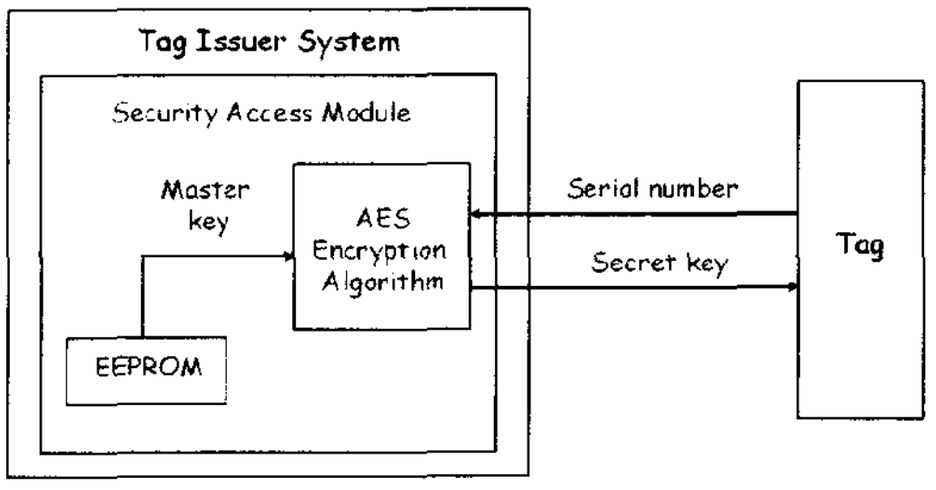


그림 2. RFID태그와 리더 간의 키 다양화 기법

키 다양화 기법은 태그의 일련번호와 비밀 마스터키에 기반을 두는데, 이는 보안상의 이유로 리더의 보안접근 모듈에 저장된다. 이런 방식의 인증은 비밀 마스터키의 사용으로 인하여 리더와 태그 간의 상호인증 메커니즘을 강화시켜줄 수 있으나, 칩의 비용을 증가시킨다. 또한, 한 번의 통신에 요구되는 시간이 다소 증가하기 때문에, 단위시간당 판독되는 태그의 수는 줄어든다.

### 3. 해쉬 함수

인증 기법을 확장하는 방법으로는, 적은 비용으로 프라이버시 제어를 제공하는 해쉬 함수[10][11]을 이용하는 것이다. 여기서 요구되는 것은, [그림 3]과 같이, 해쉬함수

의 이용과 메타 ID 저장이다. 그러나 태그의 응답들이 예측 가능하고, 난수 키와 태그 ID가 부정한 상대에 의해서 도청될 수 있기 때문에 태그가 추적당하는 것에 대한 방지는 불가능하다.

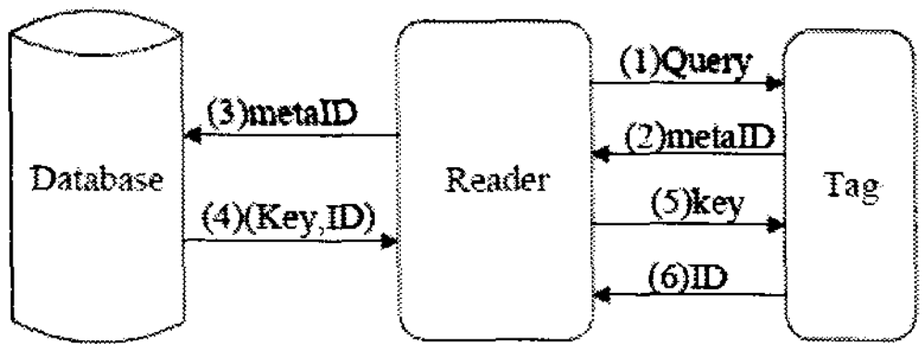


그림 3. 해쉬 잠금

[12]에서는 태그가 추적당하는 것을 피할 수 있는, 랜덤화 된 접근 제어 메커니즘을 기반으로 하는 해쉬 함수를 제안하고 있다. 이 인증 메커니즘은 태그와 리더가 같은 그룹 ID를 공유하는 경우에, 리더가 인증된 그룹에 속해 있다 하더라도 태그가 리더를 인증할 수 있게 한다.

인증이 진행되는 동안, 태그들은 허가되지 않은 리더에게는 응답을 하지 않는다. 태그가 보내는 태그ID (TID)는 일방향 해쉬함수 알고리즘에 의해 만들어진다. 따라서 *[TID, h(TID)]* 는 사전에 데이터베이스에 저장되어야하는데, 이는 최종의 태그ID를 얻기 위함이다. 인증절차는 [그림 4]와 같다.

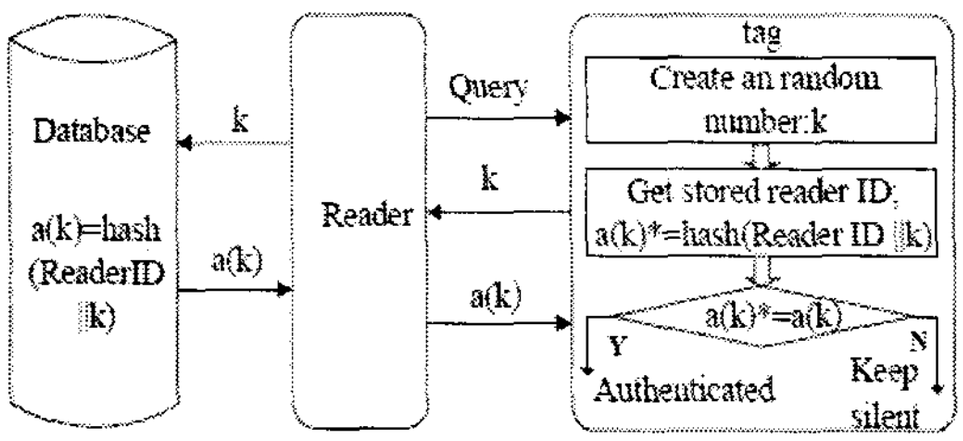


그림 4. RFID태그와 리더 간의 인증 절차에 사용되는 해쉬 함수

이 인증 방식에서 태그는 (1) 난수 $k$ 생성를 생성하고, (2) $h(RID||k)$ 와 $h(TID)$ 의 해쉬 함수를 계산하며, (3) 리더ID 저장을 위한 공간을 갖는다.

이 인증 메커니즘에서 태그는 리더가 허가된 것인지 아닌지를 알아낼 수 있다. 태그들은 인증 절차가 완료될 때마다 리더를 검증하기 위하여 메시지 $h(TID)$를 보내게 된다. 실제 메시지는 해쉬 함수에 의해서 적절히 보호되겠지만, 그럼에도 불구하고, 만일 허가되지 않은 태그가 상시적으로 보내지는 메시지 $h(TID)$를 도청한다면, 이 허가되지 않은 태그는 같은 메시지 $h(TID)$를 리더에게 보낼 수 있게 되기 때문에, 도청의 가능성을 배제할 수 없다.

태그가 확인을 위해 초기마다 리더를 위한 난수 $k$를 생성하지만, 리더가 보내는 인증 코드는 달라진다. 그러나 최종의 인증 과정에서는 $h(TID)$가 고정되고 상시 같은 메시지를 갖기 때문에 태그를 도청의 위험으로부터 보호할 수 없다. 따라서 허가되지 않은 태그가, 메시지 $h(TID)$를 도청하여 리더에게 메시지를 재생함으로써 태그를 위조할 수 있게 된다.

## III. 제안하는 인증 메커니즘

### 1. 2단계 인증 알고리즘

본 논문에서는, 위조방지와 프라이버시 보호[11]를 위해 해쉬 함수의 암호 알고리즘에 배타적 논리합 연산을 추가한 알고리즘을 제안한다.

본 논문에서 제안하는 메커니즘에서 사용할 기호는 다음과 같이 정의하기로 한다.

- $RID$ : 리더 ID
- $TID$ : 태그 ID
- $r$ : 난수
- $r'$ : 변경된 난수
- $h()$ : 해쉬함수

사전에 태그의 메모리에 허가받은 리더의 ID를 저장해 두고, 태그와 리더 모두에게 저장되어 있는 리더ID를 통하여, 태그는 허가된 리더를 식별할 수 있게 된다. 이 메커니즘은 태그가 태그ID와 동일한 길이를 갖는 난수 $r$ 을 생성할 수 있다.

[그림 5]는 제안한 인증 알고리즘의 개념을 보여준다. 배타적 논리합을 사용하면 연산속도를 향상시키고 태그

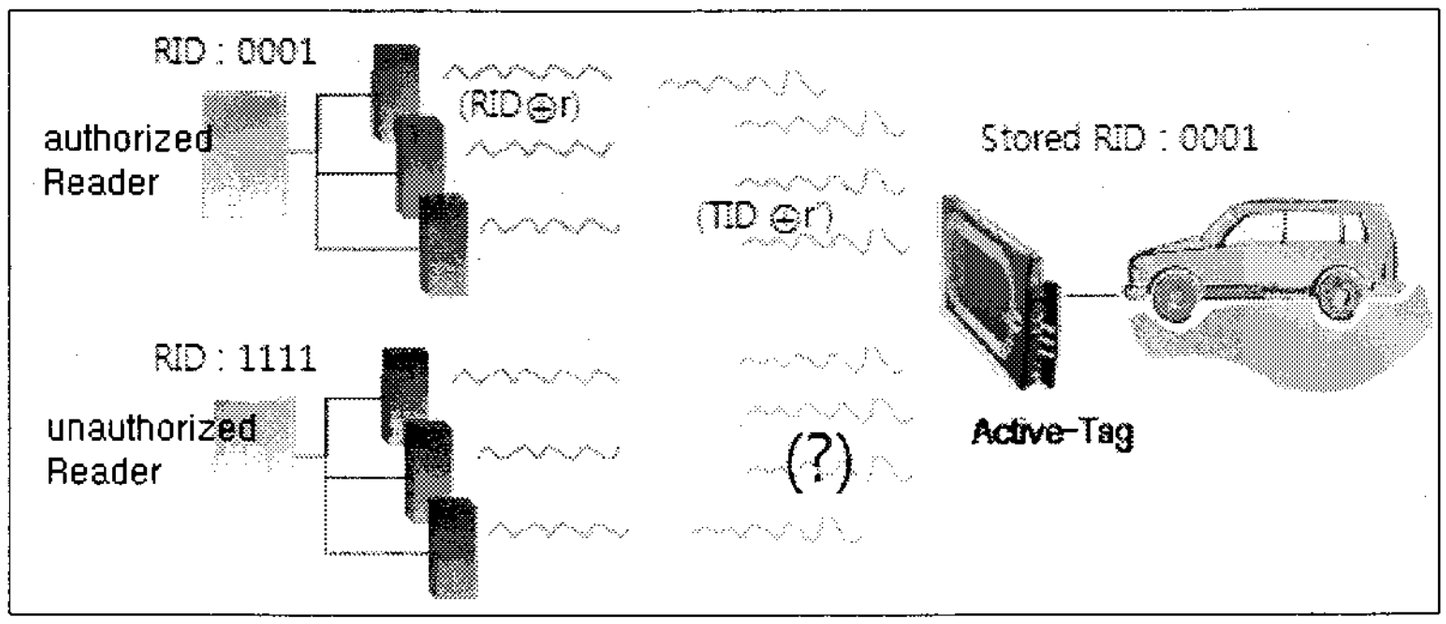


그림 5. 제안하는 인증 알고리즘의 개념

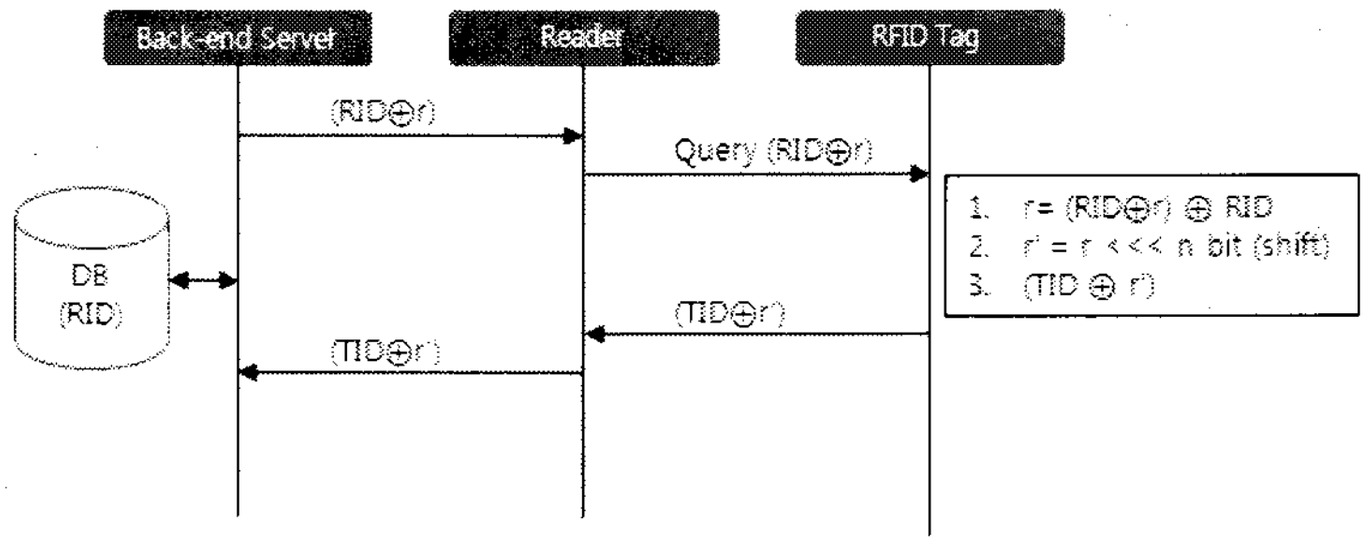


그림 6. 제안하는 인증 메커니즘

의 비용을 감소시킬 수 있다. 배타적 논리합 알고리즘에 따라, 만일 허가되지 않은 리더가 태그에게 ID에 대한 질의를 보낸다면, 리더는 *(TID⊕r')*를 태그로부터 전송받게 되고 이를 다시 미들웨어인 Back-end 서버에게 보낸다. Back-end 서버와 데이터베이스는 태그ID를 다시 리더에게 보내게 된다. 따라서 도청자는 $r$ 을 알 수 없기 때문에 일련의 의미 없는 수만을 얻게 된다. 반대로, 허가받지 않은 리더는 $r$ 과 *(TID⊕r')*를 계산할 수 없으므로 결과적으로, 태그ID(*TID*)를 얻을 수 없게 된다.

[그림 6]은 배타적 논리합 알고리즘에 기반을 둔 2단계 인증 메커니즘을 제안하고 있다. 인증 과정은 다음과 같다.

1) 데이터베이스와 연결되어 있는 Back-end 서버가 난수 $r$ 을 생성한다. 먼저 $r$ 과의 배타적 논리합 연산을 위해 데이터베이스로부터 리더ID(*RID*)를 요구한다. 이어서 *(RID⊕r)*를 리더에게 전달하고, 리더가 질의 문에 포함하여 태그에게 방송된다.
2) 태그가 질의를 받으면 *(RID⊕r)*를 미리 저장되어 있는 리더ID(*RID*) 값과의 배타적 논리합 연산을 통하여 난수 $r$ 를 얻게 되는데, 리더ID는 미리 태그에 저장되어 있다. 그 후 태그가 $r$ 을 n 비트 왼쪽 쉬프트 하여 난수 $r'$ 를 생성한다. 그 후 태그 ID로 배타적 논리합 연산을 하여 *(TID⊕r')* 얻는다. *(TID⊕r')* 는 리더에게 다시 전송된다.
3) 리더는 $r'$의 계산을 위해 *(TID⊕r')* 를 Back-end 서버에게 전달한다. 최종적으로 $r'$ 와 리더ID와의 배타적 논리합 연산을 통해 태그ID가 얻어진다.

이 2단계 인증 메커니즘은 태그는 (1) $r$ 을 비트 쉬프트하여 난수 $r'$ 를 생성할 수 있고, (2) 배타적 논리합을 이용하여 *(TID⊕r')*를 계산하며, (3) 리더ID를 저장하기 위한 저장 공간을 가지고 있다.

또한, 제안된 인증 메커니즘에서는, 태그는 인증 절차가 완료 될 때마다 리더를 확인하기 위하여 *(TID⊕r')* 를 전송하게 되고, 이를 통해 허가받은 리더를 식별할 수 있게 된다. *(TID⊕r')* 메시지는 최종 단계에서 리더에게

전송되고 또한 가변적이기 때문에 도청을 방지 할 수 있다.

## 2. 인증 절차

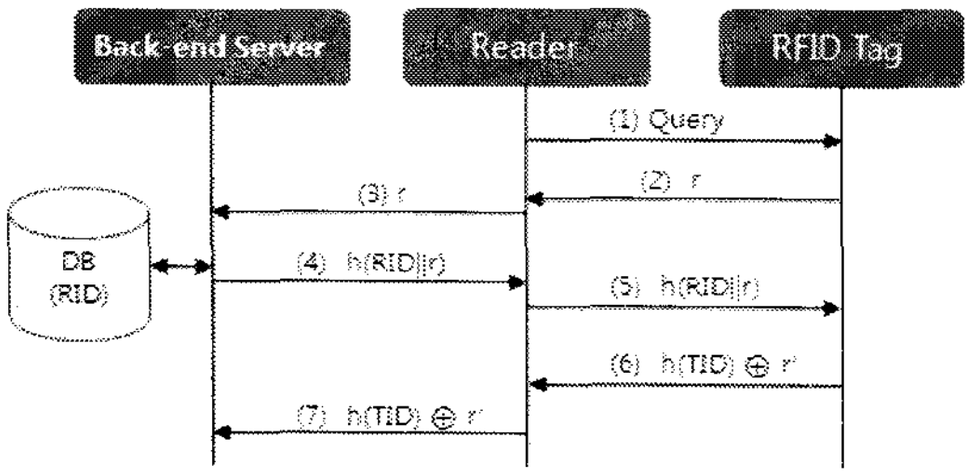


그림 7. 제안하는 인증 메커니즘의 인증 절차

[그림 7]은 제안된 메커니즘에서 사용되는 RFID 태그와 리더, back-end 서버 사이에 일어나는 인증 절차를 도식화 하고 있다. 제안된 메커니즘은[12]의 $h(TID)$을 $h(TID \oplus r')$ 로 대체하였고, 특히 난수 $r$ 을 쉬프트를 통하여 $r'$로 변형하였다. 위조된 태그가 우연히 동일한 $h(TID) \oplus r'$를 전송한다 해도 태그ID를 계산하기 위한 $r$ 이 이 위조된 태그의 API 내부에 저장되어 있지 않기 때문에 $h(TID)$를 알아내기 어려우며, 결과적으로 $h(TID)$의 도청을 방지할 수 있다.

## 3. 메커니즘 분석 및 비교평가

### 3.1 성능 분석

제안된 메커니즘의 인증 절차 과정의 연산 오버헤드를 분석하였다. 태그는 해쉬 연산 1회, 배타적 논리합 1회, n 비트 시프트 연산을 하게 된다. 배타적 논리합을 사용하여 태그의 연산속도를 향상시키고 태그의 비용을 감소시킬 수 있다. 또한 [8][9][12]와 비교할 때 인증 단계가 두 단계로 줄어들기 때문에 속도가 빠르다.

본 메커니즘에서 고려해야할 점은, 태그에서 요구되는 메모리가 다소 증가한다는 점이다. 난수 $r$ 과 리더ID의 데이터 길이는 태그ID와 같아야한다. 태그에 리더ID를 저장하기 위해서는 태그의 메모리가 일반적으로 두 배 이상 되어야한다. 56비트의 ID 길이를 갖는 태그가 있다면 난수 $r$ 과 리더ID의 데이터 길이도 56 비트이다. 이 경우, 태그에서 요구되는 메모리는 128 비트이다. 태그에 메모리 추가로 인해 약간의 비용 상승에 대한 우려가 있을 수 있으나, 현재의 메모리 기술로 본다면 그 수준은 미미할 것으로 판단된다.

[표 1]는 연산 오버헤드, 메모리 오버헤드의 측면에서 앞서의 연구들과 제안된 메커니즘에 대한 성능 분석을 하였다.

표 1.연산 오버헤드와 메모리 요구량 분석

| 특성 | | 삼단계 상호인증[8] | 키 다양화 [9] | 해쉬함수 [12] | 제안된 프로토콜 |
|---|---|---|---|---|---|
| 해쉬 연산 횟수 | 태그 | 0 | 0 | 1 | 1 |
| | B-e서버 | 0 | 0 | 1 | 1 |
| 난수생성 횟수 | 태그 | 1 | 1 | 1 | 1 |
| | 리더 | 0 | 0 | 0 | 0 |
| | B-e서버 | 1 | 0 | 0 | 1 |
| 인증 단계 수 | | 3 | 3 | 3 | 2 |
| 메모리 필요량(L) | 태그 | L | N * L (N:키갯수) | L | 2L |
| | 리더 | L | L | L | L |
| | B-e서버 | L | N * L | L | L |

### 3.2 안전성 분석

제안하는 메커니즘에서는, 인증 과정 중에 만일 부정한 상대가 리더의 결과물 $h(TID) \oplus r$ 을 도청한다 해도, 그 다음의 인증 과정에서 허가된 인증 리더로 가장할 수 없게 된다. 요구되는 $h(TID) \oplus r$ 값은 매 인증 과정마다 바뀌기 때문이다. 전자의 인증값 $h(TID) \oplus r$ 은 다음의 인증에서는 쓸모가 없어지므로 재전송 방지를 할 수 있다.

인증 후에, 태그는 자신의 태그 ID 대신 태그ID에 대한 해쉬값을 출력한다. 해쉬 함수는 역함수가 존재하지 않기 때문에, 결과 값이 부정한 상대에 의해서 도청된다 해도 태그ID는 보호될 수 있으므로 위조 방지를 할 수 있고, Back-end 서버와 리더, 태그에 대한 상호 인증도 보장된다.

태그가 새로운 리더ID를 태그 메모리에 업데이트하고자 할 때도, 새 리더ID는 기존의 리더ID로 암호화되기 때문에 태그의 익명성이 보장된다.

인증 절차에 해쉬 함수 $h(TID) \oplus r$ 와 $h(TID \oplus r')$를 사용하고 있기 때문에 데이터 무결성이 보장된다.

제안하는 알고리즘에서, 태그는 인증된 리더에게만 응

답한다. 또한 부정한 리더는 인증된 리더로 가장할 수 없다. 태그가 응답하지 않기 때문에 태그가 부착된 자동차의 행로를 추적할 수 없게 된다. 따라서 자동차 운전자의 위치 정보를 부정한 리더로부터 추적을 방지할 수 있다.

**표 2. 메커니즘 비교**

| 특성 | 삼단계 상호인증[8] | 키 다양화 [9] | 해쉬함수 [12] | 제안된 메커니즘 |
|---|---|---|---|---|
| 위조 방지 | X | △ | △ | ○ |
| 태그 익명성 | X | △ | △ | ○ |
| 데이터 무결성 | △ | ○ | △ | ○ |
| 상호 인증 | ○ | ○ | △ | ○ |
| 재전송 방지 | X | X | X | ○ |
| 추적 방지 | ○ | △ | △ | ○ |

** 표기 X:지원하지 않음 △:약간 ○:지원함

[표 2]에서는 위의 사항들을 기준으로 기존의 연구들과 제안된 메커니즘을 비교한다.

## IV. 결론

본 논문에서는 u-Vehicle 환경에서의 정보 보안상 취약점을 도출하고, 이를 해결하기 위한 방법을 제시하였다. 위조방지와 프라이버시 보호를 위해 해쉬 함수의 암호 알고리즘에 배타적 논리합 연산을 추가한 알고리즘을 제안 하였다. 사전에 태그의 메모리에 허가받은 리더의 ID를 저장해 두고, 태그와 리더 모두에게 저장되어 있는 리더ID를 통하여, 태그는 허가된 리더를 식별할 수 있게 된다. 또한, 상호인증 단계를 줄여 적은 비용으로 RFID 태그의 안전성을 증가시키고자 하였다. 결과적으로 제안된 메커니즘에서는 매번의 인증 과정마다 리더에게 요구되는 값이 바뀌기 때문에 리더에 의해서 행해지는 위조를 방지할 수 있고, 자동차 운전자의 위치 정보를 부정한 리더로부터 보호할 수 있어 추적방지의 효과를 얻을 수 있으며, 태그에서 배타적 논리합 연산을 사용하므로 저렴하면서도 향상된 보안 서비스를 제공할 수 있다.

## 참 고 문 헌


[1] J. Deng, "Security Support for In_Network Processing in Wireless Sensor Networks," Proc. SASN, 2003.

[2] ETRI, *RFID/USN 출현의 시사점과 부작용 극복 방안 모색*, 2004

[3] L. Tieyan and D. Robert, "Vulnerability Analysis of EMAP-An Efficient RFID Mutual Authentication Protocol," Reliability and Security (ARES'07), 2007.

[4] KISA, *RFID/USN Security Issues & Stepwise Approach*, 제9회 정보보호 심포지움, 2004

[5] 박종욱, 주학수, 이재일, 이동훈, "유비쿼터스 센서 네트워크의 정보보호 이슈와 동향", 통신학회지, 2004(6).

[6] K. Finkenzeller, *RFID Handbook Second Edition*, Wiley&Sons, 2002.

[7] BSI Report, *Security Aspects and Prospective Applications of RFID Systems*, 2005.

[8] Z. Lan and Z. Huaibei, "An Improved Approach to Security and Privacy of RFID Application System," Wireless Communications, Networking and Mobile Computing, Proceedings, 2005 International Conference on, Vol.2, pp.1195-1198, 2005.

[9] G. C. Chang, "A Feasible Security Mechanism for Low Cost RFID Tags," Mobile Business, ICMB2005 International Conference, pp.675-677, 2005.

[10] S. A. Weis, S. E. Sarma, and L. Ronald, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," First International Conference on Security in Pervasive Computing, 2003.

[11] H. Dirk and M. Paul, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers,"

Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, pp.149-153, 2004.

[12] G. Xingxin, X. Zhe, W. Hao, S. Jun, H. Jian, and S. Song, "An Approach to security and privacy of RFID system for supply chain," IEEE International Conference on E-Commerce Technology for Dynamic E-Business, pp.164-168, 2004.

[13] L. Tieyan, W. Guilin, and H. D. Robert, "Security Analysis on a Family of Ultra-lightweight RFID Authentication Protocols," Journal of software, Vol.3, No.3, 2008.

## 저 자 소 개

**이 윤 정(Yoon-Jung Rhee)** 정회원

- 1993년 2월 : 숙명여자대학교 전산학과(이학사)
- 1998년 8월 : 숙명여자대학교 전산학과(이학석사)
- 2002년 8월 : 고려대학교 컴퓨터학과(이학박사)
- 현재 : 제주대학교 전산통계학과 조교수

<관심분야> : 유무선 통신보안

**김 도 현(Do-Hyeun Kim)** 정회원

- 1988년 2월 : 경북대학교 전자공학과 공학사(정보통신전공)
- 1990년 2월 : 경북대학교 전자공학과 공학석사(정보통신전공)
- 2000년 8월 : 경북대학교 전자공학과 공학박사(정보통신전공)
- 1990년 3월 ~ 1995년 3월 : 국방과학연구소 연구원
- 1999년 3월 ~ 2004년 8월 : 천안대학교 정보통신학부 조교수
- 2004년 9월 ~ 현재 : 제주대학교 통신컴퓨터공학부 부교수

<관심분야> : 무선 센서 네트워크, 위치기반 서비스, 텔레매틱스, WBAN, WPAN