韓國 컴퓨터情報學會 論文誌
第11卷 第6號, 2006. 12

2006-11-6-2-7

접근시간 간격 확인 방식을 이용한 RFID 보안강화 프로토콜 설계

김 성 진*, 박 석 천**

Design of RFID Cryptanalysis Strengthening Protocol Using Access Time Interval scheme

Seungjin-KIM*, SeokCheon-PARK**

요 약

RFID의 적용 범위는 점차 그 영역을 확대되고 있으나, 보안과 더불어 개인영역 침해에 대한 연구는 아직은 미흡한 실정이다. 본 논문에서는 기존 RFID 보안 프로토콜을 분석하고 정보보호와 프로토콜의 경량화 문제를 해결하기 위하여 접근시간간격과 경량화 RSA 알고리즘을 이용한 새로운 프로토콜을 제안한다. 제안된 프로토콜을 통해 양방향 정보 송수신에 대한 정보보호 문제를 해결하고 이를 구현하고자 한다.

Abstract

RFID technology has been gradually expanding its application areas however studies on personal space infringement along with security are insufficient. This paper proposes a new security protocol access time interval scheme and RSA algorithm to analyze existing RFID security protocol and attempts to solve the problem of lightweight protocol. Information protection for two-way channels can be enforced through the proposed protocol and other issues of sniffing and man-in-the-middle attacks can be solved by applying a mutual certification technique application among tag readers.

▸ Keyword : RFID, Access Time, Cryptanalysis, Certification

• 제1저자 : 김성진
• 접수일 : 2006.12.01, 심사일 : 2006.12.19, 심사완료일 : 2006. 12.26
* 경원대학교 전자계산학 박사과정 ** 경원대학교 소프트웨어대학 정교수

Ⅰ. 서론

RFID(Radio Frequency Identification) 기술의 발전은 유통, 물류, 위치확인 등에서 비약적으로 적용 범위를 넓혀가고 있다. 일반적으로 태그에 저장된 자료는 단순 식별번호로 이를 도청하는 것은 바코드가 일반인에게 읽혀진다고 문제가 되지 않는 것처럼 구체적인 정보를 알 수 없어 크게 위협이 되지는 않는다. 즉 태그에서 리더로 전달되는 정보는 일종의 일련번호(serial number)에 불과하고 해당 일련번호를 리더가 읽었더라도 그 일련번호에 대응하는 구체적인 정보는 서버를 통해 전달받아야 하기 때문이[1]다. 그러나 신분증이나 여권 등 보안을 필요로 하는 고부가 태그에서는 정보자체가 보호되어야 하는 필요성이 있다. 이는 태그의 움직임을 지속적으로 추적하는 것이 가능하므로 특정인의 위치 추적, 오용 등에 활용될 우려가 있으며 나아가 사생활 침해 문제를 초래할 수 있다. 이와 같은 문제를 해결하기 위해 태그와 리더 간의 통신 내용 자체를 보호하기 위한 도청 방지 기법이 필요하다. 또한, 제한적 자원을 가진 태그내에 보안기능을 구현하기 위해 경량화된 암호화 기능과 프로토콜이 요구된다. RFID 보안 기법에서 요구되는 조건은 첫째, 태그와 리더 간의 양방향 데이터 전송, 둘째, 보안 기법 구현 시 태그의 제한적인 자원과 최소로 한정된 메모리 공간의 사용, 셋째, 실시간 상호작용을 위한 빠른 처리 속도, 넷째, 태그신호간의 상호 간섭 배제 등이다. 최근 이러한 조건을 만족하기 위해 경량화된 보안 프로토콜의 연구가 진행되고 있으며[1,2,3], 본 논문에서는 기존의 경량화 프로토콜을 분석하고, 보안키의 견고성 문제를 해결하기 위해 경량화 암호 알고리즘과 태그 및 리더로의 중간자공격(Man-in-the-Middle Attack)문제를 해결하기 위해 접근시간간격(Access Time Interval, 이하 ATI) 방식을 활용한 새로운 보안강화 프로토콜을 제안한다.

Ⅱ. 배경 연구

2.1 기존 보안 프로토콜

RFID 기술에서 보안 문제를 해결하기 위한 다양한 연구가 진행되고 있다. 이러한 연구의 일환으로 RFID 시스템에서 사용자 프라이버시를 보호를 위해 kill tag, faraday cage, 방해 전파(active jamming), blocker tag 등과 같은 물리적 레벨의 대응 기법[4]과 Hash Lock Scheme(HLS)[5], Extended Hash Lock Sheme (EHLS)[5] 재암호화[6, 7] 등과 같이 암호 기술을 이용한 보호 기법이 제안되고 있다. 본 절에서는 물리적 레벨의 보호 기법이 아닌 암호 기술을 중심으로 한 RFID의 보안 프로토콜을 분석한다.

2.1.1 Hash Lock

Hash Lock의 locking 프로토콜에서 리더는 랜덤키 key를 선택하고, meta ID값으로 hash(key)를 계산한다. 리더는 metaID를 태그 T에 기록한다. 태그는 이때, 잠긴 상태(locked state)에 들어간다. 리더는 (metaID, key)를 저장한다. Hash Lock의 unlocking 프로토콜의 동작 원리는 다음 그림 1과 같다. 리더는 태그에게 태그의 metaID를 질의하고, 리더는 데이터베이스에서 (metaID, key)를 조사한다. 리더는 태그에게 key를 전송한다. 만약 이때, hash(key)와 metaID가 일치하면, T는 잠긴 상태에서 빠져나온다(unlock)[5].

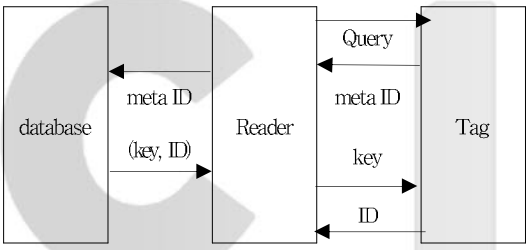

그림 1 Hash Lock 프로토콜
Figure 1. Hash Lock Protocol

일방향 해시 함수의 역함수 계산의 어려움에 기반한 Hash Lock 스킴은 인가받지 않은 리더기가 태그 콘텐츠 읽는 것을 방지할 수 있다. 위장(spoofing)은 방지하지 못하지만 탐지는 가능하다. 공격자는 태그에게 metaID를 요구한 후에 재전송 공격(replay attack)에서 합법적 리더기에게 태그를 위장하는 것이 가능하다. 그러면 합법적 리더기는 위장된 태그에게 키를 주게 된다. 그러나, 리더기는 태그의 ID를 체크하여 백엔드 데이터베이스로부터 적절한 metaID인지를 검증할 수 있다. metaID가 부적절한 경우, 리더기는 적어도 위장이 발생했음을 경고할 수 있다. Hash Lock은 태그에 해시 함수의 구현만을 요구하고, 백앤드에 키관리를 요구한다. 이러한 요구조건은 가까운 장래에 경제적인 것이 될 수 있다. 그러나, 위 방식에서는 metaID가 식별자

처럼 사용되기 때문에 사용자 추적(tracking of individuals)의 위험이 문제가 된다.

2.1.2 Extended Hash Lock

Hash Lock 기법에서 가능한 사용자 추적을 방지하기 위한 방식이다. 태그는 인가되지 않은 사용자에 의한 질의에 대하여 예상 가능한 응답을 하지 않지만, 합법적인 리더기에 의해서는 여전히 식별 가능해야 하는 방식이다. 이 기법에서는 태그에 일방향 해시 함수와 난수발생기(PRNG)가 구축되어있어야 한다. 합법적인 리더기는 태그를 스캔하기 전에 "knows what she owns"를 가정한다. 태그를lock 상태로 만드는 것은 프로토콜이 필요 없는 간단한 과정이나, 태그를 unlock 상태로 하는 프로토콜은 필요하다. 태그를 unlock 상태로 하는 프로토콜의 동작원리는 다음 그림 2와 같다[5].

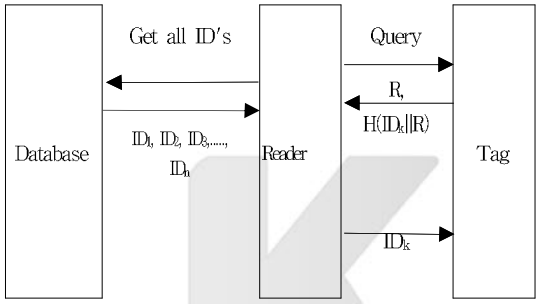

그림 2 Extended Hash Lock 프로토콜
Figure 2. Extended Hash Lock Protocol

우선, 리더(R)는 태그(T)에게 질의를 보낸다. 태그는 랜덤한 난스(nonce)R을 생성하고, hash(ID | | R)값을 계산한다. 태그는 리더에게 (R, hash(ID | | R))을 전송하고, 리더는 모든 알려진 IDi 값에 대해 hash(IDi | | R)을 계산 한다. 만약 hash(IDi | | R) == hash(ID | | R)을 만족하는 IDi를 찾는다면, 리더은 태그에게 IDi 를 전송한다. 만약 IDi와 ID가 일치한다면, 태그는 잠긴 상태에서 빠져나온다. 이 방식은 초당 100~200개의 태그를 읽어야 하는 많은 개수의 태그를 소유한 환경에서는 비현실적이다. 그러나 상대적으로 적은 수의 태그 사용자를 갖는 환경에서는 가능한 방식이다. 소매 상점은 일반 사용자에 비해서 위치 프라이버시와 연관성이 적기 때문에 소매 상인들은 Hash Lock 기법을 적용하고, 구매하는 소비자에게는 Extended Hash Lock 기법을 적용한다. 한 가지 문제는 합법적인 리더기들이 어떻게 그들의 태그를 알게 되느냐는 것이다. 물건이 팔렸을 때, 그것의 ID도 반드시 같이 전송되어야 한다. 그렇지 않으면 새로운 소유주가 태그를 읽을 수 없다. 새로운 소유주가 자신의 태그에 접근하는 한 가지 방식이 printed master key를 사용하는 것이다.

이 방식은 충분히 현실적이지만 이론적으로 완벽하지는 않다. 이는 일방향 함수의 정의가 역함수 계산의 어려움만을 의미하기 때문이다. ID 비트가 노출되지 않음을 보장하기 위해서 보다 강한 프리미티브의 사용이 가능하다. 각 태그는 리더기와 유일한 비밀키를 공유한다고 하고, PRF(Pseudo-Random Function) 앙상블(ensemble)을 지원한다고 가정하면, 이론적으로 ID 비트 노출 방지가 가능하다. 구현상의 문제로 PRF 앙상블을 대칭키 암호화보다 아주 적은 자원으로 구현 가능하냐의 문제가 발생하는데, PRF 앙상블의 최소 하드웨어 복잡도는 open problem이다.

2.1.3 재암호화

ECB(European Central Bank)는 법집행기관(law enforcement agent)에 의한 추적이 가능하도록 2005년부터 RFID를 고액의 유로화에 삽입하도록 제안하였다. 이에 Juels과 Pappu[7]는 지폐의 시리얼 넘버를 법 집행 공개키로 암호화하는 스킴을 제안하였다. 공개키에 의해 암호화된 암호문은 주어진 태그의 연결성(linkability)을 감소시키기 위해 주기적으로 재암호화(re-encryption) 된다. RFID 태그는 제한된 컴퓨팅 리소스를 가지기 때문에, 재암호화는 외부의 계산 기관(computing agent)에서 수행한다. 그러한 재암호화 기관의 정당한 행위는 은행이나 상점에서 지폐를 처리할 때 증명될 수 있다.

재암호화 스킴에서 RFID 태그는 공개키를 이용한 암호 연산을 수행할 수 없기 때문에 재암호화 기관 및 optical verifier에 대한 인프라가 필요하다. 그러나, 이러한 인프라는 부담이 될 수 있다. Golle et al.[6]은 소비자의 상품에 삽입된 RFID 태그의 프라이버시 보호에 보다 적합한 universal re-encryption 스킴을 제안하였다. 이 스킴은 여러 개의 공개키를 사용하며, 연관된 공개키의 정보없이 암호문을 재암호화하는 것이 가능한 ElGamal 암호 의 확장이다. 그러나, 이 기법도 Juels과 Pappu의 기법과 마찬가지로 재암호화 디바이스에 대한 별도의 인프라가 필요하다는 단점이 있다[6,7].

2.1.4 경량화 암호 프로토콜

최근 경량 암호 프로토콜로 Nicholas J. Hopper and Manuel Blum(2001)에 의해 HB 프로토콜이 제안되었으며, Jules 와 Weis에 의해 수정된 HB+가 제안되었다. HB 프로토콜에 사용되는 키를 정의하면 그림 3과 같다.

비밀키(s,s1,s2) : 태그 ID로 리더가 기진 s's개중의 ID 값 중에 하나인 것 확인
쿼리(q) : k개의 2진 스트링, 리더에서 생성되는 비밀키, 하나의 프로토콜 당 하나의 쿼리 생성.
비밀키(γ) : 태그에서 생성되는 비밀키
Epsilon(ε) : 태그로부터 반전되는 값
NU(ν) : epsilon =1
Delta(σ) : 에러 벡터, 태그의 응답에 대한 noise bit
b : blinding Factor

그림 3 HP 키 정의
Figure 3. HP Key Definition

HB 프로토콜의 작동원리는 그림 4와 같다.

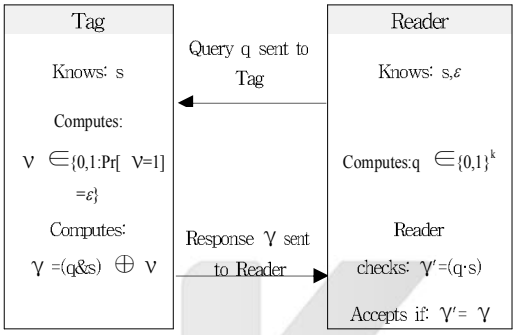

그림4 HP 프로토콜 처리 과정
Figure 4. HP Protocol Process

리더는 q를 계산하여 태그로 전송한다. 태그는 q와 s를 내적연산(&)하고 결과를 nu(ν)와 XOR 하여 결과를 γ에 대입하여 리더에 전송한다. 리더는 q와 s를 내적연산(&)하여 결과에 γ'에 대입하고, γ과 γ '를 비교하여 같을 경우 전송된 값을 기록하고 같지 않으면 거부한다. 태그 리더간 n번의 상호 동작 후, 리더는 태그가 대략 n * ε정도의 에러를 예상한다. 리더는 태그의 응답률이 (n * ε) ∓ δ일 때만, 태그 정보를 받아드린다.

HP 프로토콜에서 개선점은 공격자의 active attack에 대해서는 보안이 되지 않는다는 점이다[8]. 리더로 가장한 공격자가 태그에게 고정된 q를 여러 번 전송하면 s는 쉽게 획득될 수 있다. 또한, 리더는 전송 시마다 서로 다른 쿼리(q)를 전송해야 한다.

HB 프로토콜에서의 개선점인 active attack에 대한 취약성에 대한 대안인 HB+ Protocol은 Juel and Weis(2005)에 의해 만들어졌다. HB+ 프로토콜에서는 각각의 태그에 보안키를 두개(s1, s2)의 쌍으로 사용하였으며, 태그에서 k길이의 이진 쿼리인 브라인트 팩터(blinding factor) 값(b)을 생성하여 보안을 강화하였다. HP+의 작동원리는 그림 5과 같다.

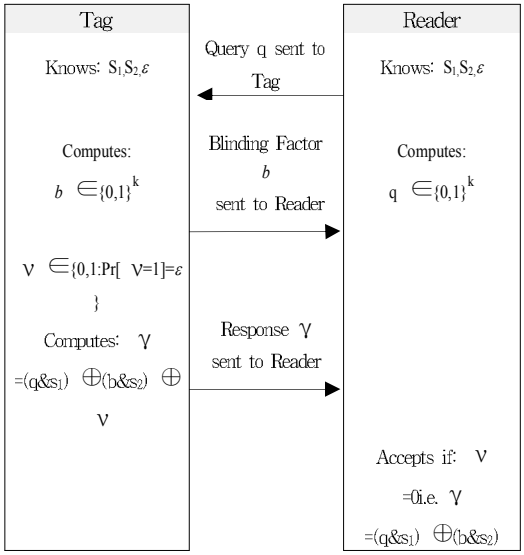

그림 5 HP+ 프로토콜 처리 과정
Figure 5. HP+ Protocol Process

HP+ 프로토콜의 처리과정을 살펴보면 리더는 q를 계산하여 태그로 전송한다. 태그는 blined factor b를 계산하여 리더로 전송한다. 또한, 태그는 q와 s1를 내적연산(&)한 값과 b와 s2의 내적연산 결과를 nu(ν)에 XOR 하여 결과를 γ에 대입하여 리더에 전송한다. 리더는 q와 s1를 내적 연산(&)한 값과 b와 s2의 내적연산 결과를 γ '에 대입하고, γ과 γ '를 비교하여 같을 경우 전송된 값을 기록하고 같지 않으면 거부한다. 태그 리더간 n번의 상호 동작 후, 리더는 태그가 대략 n * ε정도의 에러를 예상한다. 리더는 태그의 응답률이 (n * ε) ∓ δ일때만, 태그 정보를 받아드린다. HB+ 프로토콜의 개선점은 고의적으로 공격하는 중간자 공격에 대해서는 정보보호가 어렵고, 태그의 인증 후 백워드채널(Backward channel)상 태그에서 리더로 r′ 의 정보가 보내질 경우, 공격자는 이 정보로부터 δ를 획득하여 s1을 구할 수 있게 된다[8]. 이후에도 HB++ Protocol이 Bringer et al.(2006)에 의해 제안되었으나, 비밀키(b)를 추가하여 암호의 견고성을 높일 수 있도록 시도하였으나, 여전히 리더 위장 공격에 대해서 정보 보호가 되지 못한다. 기존의 보안 프로토콜의 개선점을 정리하면 표1과 같다.

표 1. 기존 보안 프로토콜의 비교
Table 1. Comparison of Existing Protection Protocol

보안 프로토콜	개 선 점
해쉬-락	위치정보 노출, 재전송 및 스푸핑 공격
확장된 해쉬-락	재전송 및 스푸핑 공격 위험
해쉬-체인	서로 다른 해쉬함수로 태그 가격문제 백-엔드 DB의 많은 계산량 문제
해쉬 기반 ID 변형	스푸핑 공격 위험 및 위치정보 노출
외부 재 암호화	외부장치 필요
기존 RSA	많은 계산량 및 실시간 상호작용의 문제
경량화 암호	구현용이, 중간자공격문제

III. 접근시간간격확인 알고리즘의 적용

본 장에서는 접근시간간격 확인과 경량화 RSA 알고리즘을 리더와 태그에 정보보호에 적용하고자 한다. 리더와 태그의 제한적인 자원을 고려하여 태그에서 인증과정을 생략하여 알고리즘을 경량화하였다. 반면 보안측면을 강화하기 위해 연속적인 불법접근을 경우 거부할 수 있는 기능을 추가하였다.

3.1 단계별 처리 과정

단계별 처리과정을 위한 키 정의는 그림 6과 같다.

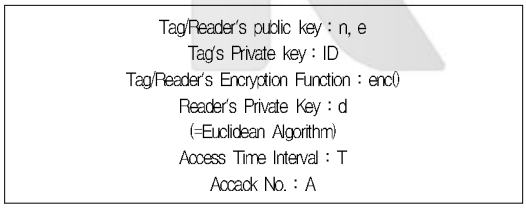

그림 6 ATI-확인 알고리즘 키 정의
Figure 6. ATI-Confirm Algorithm Key Definition

태그의 한정된 연산 능력으로 메시지를 암호화하는 데에는 제약이 따르므로 경량화 공개키 알고리즘을 이용한 공개키(n, e)는 리더로부터 전송받도록 하였다. 공개키를 받은 태그는 공개키를 이용한 암호 코드(ID′)를 만들어 리더로 전송한다. 공격자에서는 개인키가 없으므로 도청자체가 불가능하다. 기존 방식에서는 공개키를 이용하여 ID를 구할 수 있었으나, 본 방식에서는 리더의 개인키(d)는 철저히 보안이 유지되며 공개키(n, e)를 이용하여 p, q를 구하여 다시 d를 구하기는 사실상 불가능하다. 다음으로 각 단계별 절차는 그림 7과 같다.

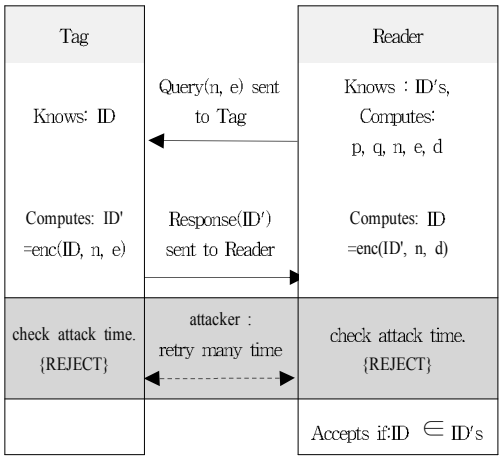

그림 7 제안 프로토콜의 처리 과정
Figure 7. Proposed Protocol Process

3.2 리더기 처리 알고리즘

리더기는 비대칭 쌍의 키를 생성한 후 공개키를 태그로 전송하여 태그에서 암호화된 식별자를 반환 받으면 이를 개인키를 통하여 복호화 하는 처리과정은 그림 8과 같다.

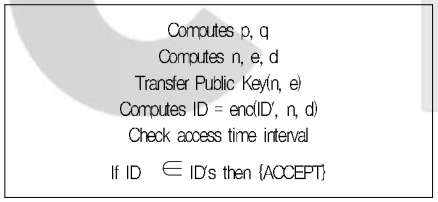

그림 8 리더기 알고리즘
Figure 8. Reader Algorithm

위장된 공격자로부터의 반복적 접근에 대해서는 접근여부를 인정(accept)/거부(reject)할 수 있는 기능을 추가하여 반복접근을 통한 정보획득을 방지하여 리더 보안 기능을 강화한다.

3.3 태그의 처리 알고리즘

태그에는 보유한 고유 식별값(ID)인 비밀키와 수신된 공개키(n, e)를 이용하여 그림 7의 알고리즘과 같이 암호화한다. 암호화 된 ID값을 리더로 전송한다. 태그는 그 자원

에 한계가 있어 고유 식별값(ID)를 비밀키로 사용하였으며, 백워드 보안의 안정성을 위해 암호화 기능을 내장하도록 하였다. 태그의 처리과정은 다음 그림 9와 같다.

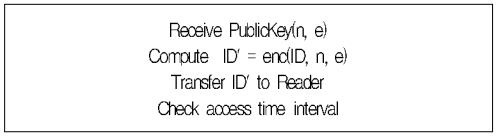

그림 9 태그 처리 알고리즘
Figure 9. Tag Process Algorithm

3.4 반복접근횟수 확인 알고리즘

허가되지 않은 공격자로부터 태그 및 리더로 위장 및 중간자공격과 같은 불법적인 반복공격에 대해 그 접속 형태에 따라 정보전송을 여부를 인정/거부하는 기능을 추가하여 태그 정보 기능을 강화 한다. 다음 그림 10은 ATI확인 알고리즘을 나타낸다.

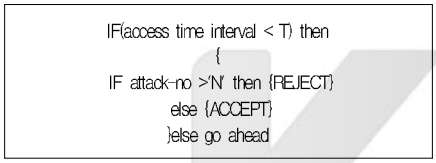

그림 10 ATI 확인 알고리즘
Figure 10. ATI Confirm Algorithm

본 논문에서는 태그 및 리더의 계산량을 고려하여 접근시간간격(T)내에 반복접근 횟수(A)를 이용하여 불법공격에 대응하도록 한다. 예를들어, 동일태그 및 리더로부터 동일시간간격(T)이내에 N이상의 반복접근이 있다면 불법적인 접근으로보고 접근을 거부하는 동작을 수행한다. 이때, 보안경도와 사용 환경에 따라 접근시간간격(T)와 반복 접근수(A)는 별도의 기준을 정한다.

Ⅳ. 성능 평가

본 정에서는 32비트 패스워드 길이, 640Kbps 데이터전송속도상의 프로그램 가능한 규격을 가진 EPC class-1 Generation-2 UHF-RFID(이하 'Gen 2') 규격[10]의 취약점 분석[11]을 바탕으로 다음과 같이 성능 인자를 정의하여 각 항목별로 유사 프로토콜과 성능을 비교하였다.

4.1 보안 분석

Gen2의 취약점에 대한 대응능력에 대해 평가하면 표 2와 같다. 상호 인증 기법에서는 제안된 프로토콜은 태그 및 리더에서 연속 접근횟수를 체크하는 방식으로 2회의 인증을 수행한 반면 표준에서는 인정이 사용되지 않고 있다. 또한 복제 및 복제 공격에 대해서는 제안 프로토콜에서는 태그 ID를 전송간에 암호화하여 전송함으로서 어떠한 형태로든 노출하지 않았으며, 복제 태그 탐지 문제와 중간자 공격, 백워드 채널 보호, 도청문제는 제안된 프로토콜에서는 비밀키에 의해 암호화하고 리더에서 복호화함으로서 해결하였다.

표 2 제안된 프로토콜 성능 분석
Table 2. Proposed Protocol Performance Analysis

프로토콜 / 평가항목	EPCglobel Gen2	제안한 프로토콜
상호 인증 기법	×	○(2회)
복제 및 복제공격	×(ID 노출)	○(ID 봉인)
복제 태그 탐지	△ (Kill 패스워드 태그 당 1회)	○(ID 봉인)
중간자 공격 대처 능력	×	○(ID 봉인, 불법공격횟수검사)
백워드 채널 보호	×	○
도청공격	× (Access 패스워드 노출)	○(ID 봉인)

○: 만족 △: 보통 × : 미흡

표 3에서 제안된 프로토콜과 보안 요구 사항[12]에서 작성한 분석을 바탕으로 제안한 프로토콜과 비교하였다.

표 3 제안된 프로토콜 보안 분석
Table 3. Proposed Protocol Security Analysis

프로토콜	HLS[6]	EHLS[6]	HBM[5]	제안안
비밀성	×	△	△	○
태그 익명성	×	△	△	○
데이터 통합	△	△	○	○
상호인증	△	△	△	○
포워드 보안	△	△	○	○
중간자공격	△	△	×	○
반복공격	△	△	○	○
위조방지	×	×	×	○
데이터 복구	×	×	○	○

○: 만족 △: 보통 ×: 미흡

4.2 성능 분석

태그와 리드내의 오버헤드를 통한 성능 분석은 다음과 같다.

• 계산 오버헤드(Computational Overhead)

태그내의 제한된 계산 능력과 메모리 공간내에서 복잡한 암호 기능을 구현하기 어렵다. 본 논문에서는 태그는 인증 처리과정을 생략하고, 연속적 접근에 불법 접근에 의해 ID 도용의 이뤄진다는 전제하에, 제한된 시간내에 일정 수 이상의 연속적인 불법접근이 있을 경우 접근 차단하는 방법으로 계산 오버헤드를 줄였다. 이때, 사용되는 계산은 접근자의 인식번호에 접근수를 카운트하는 ADD 연산과 XOR 연산으로 계산 오버헤드를 줄인다.

• 저장 오버헤드(Storage Overhead)

제안된 프로토콜의 메모리 사이즈를 비교하기 위해 모든 암호와 관련한 해쉬함수 생성 및 랜덤값 생성등의 컴포넌트의 길이를 각각 L 비트로 가정한다. 제안된 프로토콜은 태그의 저장공간을 최소화하기위해 인증 처리절차를 최소화하고, ATI 및 접근자 인식정보를 기록 하고 접근수를 카운트하는 최소 공간을 활용한다. 암호화를 위한 저장 오버헤드는 암호레벨에 따라 사용여부를 선택적으로 조정한다.

• 통신 오버헤드(Communication Overhead)

제안된 프로토콜은 표 4에서 보는 것과 같이 태그 리더간의 최소 4회 이상의 상호 인증 과정을 요구한다. 그러나 본 연구에서는 태그 리더간의 인증 과정을 생략하고 공개키 알고리즘을 통한 ID 암호화와 접근시간간격 확인방법으로 인증절차를 최소화하여 통신 오버헤드를 경량화 하였다.

표 4 프로토콜 오버헤드 비교
Table 4. Comparison of Protocol Overhead

프로토콜	Entity	EHLS[6]	HBVI[5]	제안안
암호화 동작수	T	2	3	1
	R(B)	n	3	1
키해쉬 동작수	R(B)	-	-	-
랜덤값 생성수	T	1	-	1
	R(B)	-	1	1
암호	B(T)	-	-	1
복호	R	-	-	1
인증단계		5	5	2
오버헤드 합계		18	12	7
메모리크기	T	1L	3L	(3L)
	R	-	-	3L
전체메모리		10	30	30(60)

• n : 태그수, L : 컴포넌트 메모리 사이즈, B : DateBase,
- : not required,

• 가격 오버헤드(Cost Overhead)

[3]에서 일반적으로 보안을 위해서 게이트의 수는 2.5~5k 개의 게이트 수를 넘어서는 실용화에 문제가 된다. 본 논문에서는 태그에서 암호화되는 정보는 좌표값을 나타낼수 있는 최소 비트를 사용하며, 암호화를 위한 최소연산으로 XOR 및 ADD 연산을 이용하여 접근자수, 접근간격을 기록하여 게이트 수를 최소화하였다.

본 논문에서는 [12의 메모리평가방법을 이용하여 태그수(n)와 암호관련 컴포넌트의 메모리 크기(L)를 정수값 10으로 각각 고정하여 태그와 리더 및 데이터베이스에서의 오버헤드를 합산하여 프로토콜간의 오버헤드수를 비교하였고 내용은 표 4와 같다.

V. 결론 및 향후 과제

본 논문에서는 ATI 확인 알고리즘을 이용하여 태그 리드간의 정보보호 기능을 가진 경량화된 프로토콜을 제안하였다. 제안한 경량화 프로토콜은 Gen2의 취약점을 해결할 수 있으며, 정보보호측면에서 태그-리더의 사용환경에 따라 태그-리더로의 접근시간간격과 연속접근 횟수를 정하여, 보안강도에 따라 탄력적으로 암호기법을 적용할 수 있는 방안으로 보안 강화와 오버헤드를 상황에 따라 조절할 수 있는 방안을 제시하였다.

참 고 문 헌

[1] Piramuthu, Selwyn.HB and Related Lightweight Authentication Protocols for Secure RFID Tag/Reader Authentication.(CollECTeR Europe Conference, June 2006)

[2] Tassos Dimitriou. A Lightweight RFID Protocol to protect against Traceability and Cloning attacks.(SecureComm, September 2005)

[3] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, Arturo Ribagorda. LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags. (Workshop on RFID Security, July 2006)

[4] A. Juels et al., "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy,"

ACM CCS'03, pp.103-111.
[5] D. Henrici and P. Muller. "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," In Proc. of PERSEC'04, pages 149 - 153. IEEE Computer Society, 2004.
[6] P. Golle et al., "Universal Re-encryption for Mixnets," CT-RSA 2004, LNCS 2964, pp.163-178.
[7] A. Juels and R. Pappu, "Squealing Euros: Privacy Protection in RFID-enabled Banknotes," Financial Cryptography 2003, LNCS 2742, pp.103-121.
[8] Piramuthu, Selwyn. "HB and Related Lightweight Authentication Protocols for Secure RFID Tag/Reader Authentication" CollECTeR Europe Conference, June 2006
[9] Ari Juels and Stephen Weis. "Authenticating Pervasive Devices with Human Protocols", Crypto, August 2005
[10] EPCTMRadio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version1.0.9
[11] Ari Juels, "Strengthening EPC Tags against Cloning", In submission, Available at http://www.rsasecurity.com/rsalabs/node.asp?id=2780
[12] J. Yang, J. Park, H. Lee, K. Ren, and K. Kim. "Mutual authentication protocol fol Low-cost RFID," Encrypt Workshop on RFID and Lightweight Crypto, 2005.

저 자 소 개

김 성 진

1996년 : 서경대학교 컴퓨터과학과(공학사)
1998년 : 경원대학교 대학원 전자계산학과(공학석사)
2006년 : 경원대학교 대학원 전자계산학과(공학박사 수료)
1999~현재 : 현대전문학교 컴퓨터정보학과 교수
관심분야 : 유비쿼터스 컴퓨팅, 정보보호, RFID etc.

박 석 천

1977년 : 고려대학교 전자공학과 학사
1982년 : 고려대학교 대학원 컴퓨터공학 석사
1989년 : 고려대학교 대학원 컴퓨터공학 박사
1979년~1985년 : 금성통신연구소
1991년~1992년 : University of California, Irvine Post Doc.
1988년~현재 : 경원대학교 소프트웨어학부 정교수
관심분야 : 차세대 인터넷, 멀티미디어 통신, IMT-2000