논문 13-38C-01-02

한국통신학회논문지 '13-01 Vol.38C No.01
http://dx.doi.org/10.7840/kics.2013.38C.1.12

프라이버시 보호를 위한 개선된 RFID 인증 프로토콜

오 세 진◆, 이 창 희*, 윤 태 진**, 정 경 호***, 안 광 선°

Improved Authentication Protocol for Privacy Protection in RFID Systems

Sejin Oh◆, Changhee Lee*, Taejin Yun**, Kyungho Chung***, Kwangseon Ahn°

요 약

2012년 태그의 고유 식별 정보를 안전하게 숨기고, 매 세션 다른 값을 생성하기 위해서 해시함수와 AES 알고리즘을 모두 사용하는 DAP3-RS(Design of Authentication Protocol for Privacy Protection in RFID Systems)을 제안하였다[7]. DAP3-RS 논문에서 Hash-Lock 프로토콜의 metaID가 고정되는 문제점을 AES(Advanced Encryption Standard) 알고리즘으로 해결하였고, 리더, 태그의 난수로 인증 과정을 거치기 때문에 스푸핑 공격, 재전송 공격, 트래픽 분석 등 다양한 공격에 안전하다고 주장하였다. 그러나 그의 주장과는 달리 고정된 해시 값으로 트래픽 분석이 가능하며, 리더와 태그사이의 동일한 데이터 값으로 인해 공격자임에도 불구하고 인증과정을 통과할 수 있다. 본 논문에서는 DAP3-RS가 공격자의 공격에 취약함을 증명한다. 그리고 AES 알고리즘 기반의 인증 프로토콜을 제안하고, 제안 프로토콜이 DAP3-RS에 비해 안전하고 효율적임을 증명한다.

Key Words : RFID, Protocol, Authentication, AES, Privacy

ABSTRACT

In 2012, Woosik Bae proposed a DAP3-RS(Design of Authentication Protocol for Privacy Protection in RFID Systems) using the hash function and AES(Advanced Encryption Standard) algorithm to hide Tag's identification and to generates variable data in every session. He argued that the DAP3-RS is safe from spoofing attack, replay attack, traffic analysis and etc. Also, the DAP3-RS resolved problem by fixed metaID of Hash-Lock protocol using AES algorithm. However, unlike his argue, attacker can pass authentication and traffic analysis using by same data and fixed hash value on the wireless. We proposed authentication protocol based on AES algorithm. Also, our protocol is secure and efficient in comparison with the DAP3-RS.

Ⅰ. 서 론

RFID(Radio Frequency Identification) 시스템은 무선 주파수를 이용한 차세대 인식 기술로 국방, 축산, 유통 등 다양한 분야에서 사용되고 있다. RFID 시스템 구성은 고유 식별 정보를 담고 있는 태그(Tag)와 태그를 인식 및 판독하는 리더(Reader), 태그의 정보를 관리하는 서버(Server)로 구성된다. 다

※ 이 논문은 2012학년도 경북대학교 학술연구비에 의하여 연구되었음
◆ 주저자 : 경북대학교 전자전기컴퓨터학부 임베디드 시스템 연구실, 170m3@knu.ac.kr, 준회원
° 교신저자 : 경북대학교 IT대학 컴퓨터학부, gsahn@knu.ac.kr, 정회원
* 계명문화대학 컴퓨터학부, chlee@live.co.kr, 정회원
** 경운대학교 모바일공학과, tjyun@ikw.ac.kr, 정회원
*** 경운대학교 컴퓨터공학과, khjung@ikw.ac.kr, 정회원
논문번호 : KICS2012-10-515, 접수일자 : 2012년 10월 30일, 최종논문접수일자 : 2013년 1월 3일

양한 분야에 손쉽고 빠르게 개체의 정보를 관리할 수 있는 RFID 시스템은 리더와 태그 간 무선 주파수를 이용하는 특성으로 인해 도청, 위치추적, 스푸핑 공격, 재전송 공격, 서비스 거부 공격 등 다양한 공격에 취약하다[1-6]. 현재 다양한 공격을 방어하기 위해 해시함수, AES(Advanced Encryption Standard)와 같은 암호학적 방법과 인증절차를 사용한 RFID 보안 프로토콜이 활발히 연구되어지고 있다.

2012년 배우식은 해시함수와 AES 알고리즘을 동시에 사용한 RFID 시스템에서 프라이버시 보호를 위한 인증 프로토콜 설계(DAP3-RS)를 제안하였다[7]. 그는 Hash-Lock 프로토콜[8]의 고정된 metaID의 문제점을 해결하고자 리더와 태그의 난수를 AES 알고리즘으로 암호화하여 해결하였고, 암호화된 데이터를 활용한 인증과정으로 다양한 공격에 안전하다고 주장하였다. 하지만 그의 주장과는 달리 리더와 태그 사이에 동일한 H(ID) Tn Ek(CD ‖ Rn)가 두 번 전송되는 점과 고정된 해시 값 H(ID)로 인해 태그의 위치추적이 가능하고 공격자임에도 불구하고 인증과정을 통과하는 문제점이 발생하게 된다.

본 논문에서는 배우식이 제안한 DAP3-RS를 분석하고, 문제점을 기술한다. 그리고 제안한 프로토콜과의 보안성, 효율성을 비교분석한다.

Ⅱ. DAP3-RS

RFID 기술은 바코드를 대체할 기술로 각광 받고 있지만 무선을 이용하는 특성으로 인해 도청, 위치추적, 스푸핑 공격, 재전송 공격과 같은 보안상 취약성을 지니고 있다. 이를 해결하기 위하여 암호학적 연구가 필요하다는 것이 입증 되었고, 해시함수를 이용한 프로토콜과 AES 알고리즘을 이용한 프로토콜이 많이 제안되고 있다. 그럼에도 불구하고 잘못된 프로토콜 설계로 보안문제를 지니고 있음이 논문 연구를 통하여 보고되고 있다[1-7].

본 장에서는 2012년 배우식이 제안한 DAP3-RS(Design of Authentication Protocol for Privacy Protection in RFID Systems)를 알아본다. 그림 1과 표 1은 DAP3-RS와 표기법을 나타낸 것이다.

DAP3-RS는 그림 1과 같이 총 6단계로 이루어진다.

◎ Step 1, 2 : 리더는 난수 Rn을 생성하여, Query와 함께 태그와 서버에게 전송한다.

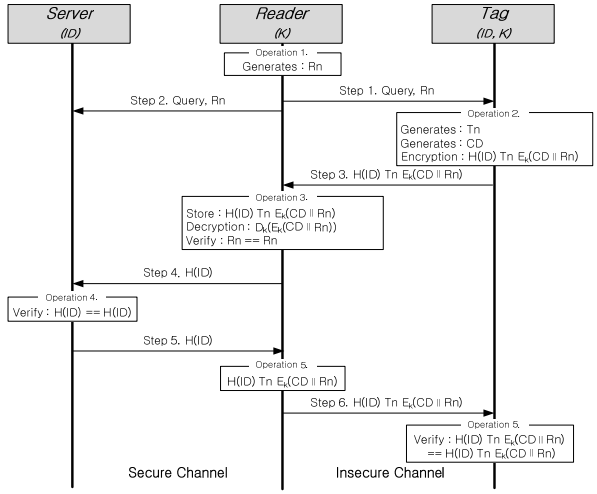


그림 1. DAP3-RS
Fig. 1. The DAP3-RS

표 1. DAP3-RS의 표기법
Table 1. The Notations of the DAP3-RS

Notations	Descriptions
Query	Reader's Query
ID	Tag's Unique Identification
H(x)	Hash Function(SHA-1)
Rn	Reader's Random Number
Tn	Tag's Random Number
CD	Changed Data
$E_k()$	AES Encryption
$D_k()$	AES Decryption
‖	Operation for Concatenation

◎ Step 3 : 리더의 난수 Rn을 전송받은 태그는 태그의 고유정보 ID를 해시한 값과 태그가 생성한 난수를 Tn을 연접한다. 그리고 태그의 CD, Rn을 연접한 값을 비밀키 k를 사용하여 AES로 암호화한 뒤, H(ID) Tn E_k(CD ‖ Rn)을 리더에게 전송한다.

◎ Step 4 : H(ID) Tn E_k(CD ‖ Rn)을 전송 받은 리더는 암호화 된 E_k(CD ‖ Rn)을 비밀키 k로 복호화하여 Rn을 획득한다. 이 때 리더가 생성한 Rn과 태그에서 암호화된 Rn을 비교하여 같으면 태그를 인증한다. 만약 다를 경우 공격자로 간주하고 통신을 중단하며, 태그 인증이 통과하면 H(ID)를 서버에게 전달한다.

◎ Step 5 : 리더로 부터 H(ID)를 전송받은 서버는 데이터베이스에 저장된 ID를 해싱하여 H(ID)에 대해 검증 절차를 진행한다. 검증 절차는 서버의 H(ID)와 리더에게 전송 받은 H(ID)가 같을 때, 리더에게 H(ID)를 전송한다.

◎ Step 6 : 서버에게 H(ID)를 전송받은 리더는 H(ID) Tn E_k(CD ‖ Rn)를 태그에게 전송한다. 이를 전송받은 태그는 리더에게 전송받은 H(ID) Tn E_k(CD ‖ Rn)과 태그에 저장된 H(ID) Tn E_k(CD ‖ Rn)를 비교하여 같으면 인증을 성공적으로 종료한다.

Ⅲ. DAP3-RS의 취약점 분석

본 장에서는 DAP3-RS의 위치추적과 스푸핑 공격 및 재전송 공격으로 인한 취약점을 분석한다. 그림 1에서 리더의 질의에 대한 태그의 응답 값 H(ID) Tn Ek(CD ‖ Rn)을 공격자가 도청 공격을 통해 위치추적이 가능하다. 리더는 항상 Query를 브로드캐스트하며 리더의 인식범위에 위치한 태그는 이에 응답하는 특정을 이용하여, 공격자는 특정 난수 Rn을 생성하여, Query와 Rn을 태그에게 연속적으로 질의하게 되면 항상 동일한 H(ID)를 받을 수 있다.

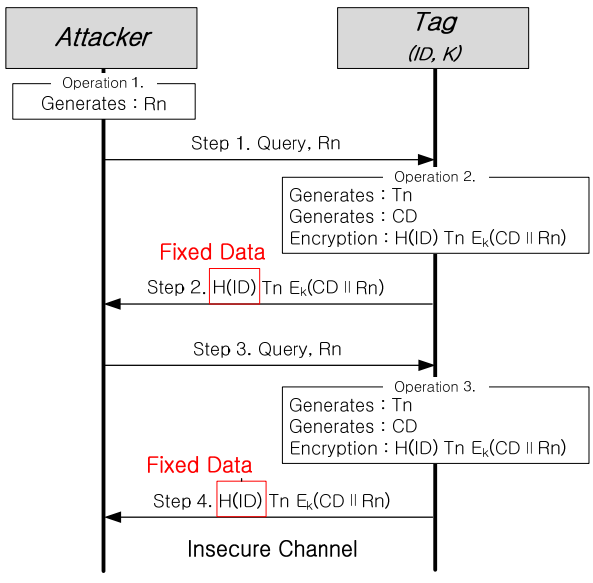


그림 2. DAP3-RS의 위치추적
Fig. 2. The Location Tracking of the DAP3-RS

태그의 첫 번째 응답에서 상위 128 비트는 태그 ID에 대한 매 세션 고정된 해시 값이기 때문에, 해시 값 이후 비트부터 최하위비트 구간에 난수를 이용해 값을 변형 하더라도 위치추적이 가능하다.

뿐만 아니라 DAP3-RS의 단계 3, 단계 6은 태그가 생성한 값과 동일한 점을 이용하여, 스푸핑 공격과 재전송 공격이 가능하다.

공격자는 Query와 임의의 난수 Rn을 생성하여 태그에게 전송하게 되면, 태그는 H(ID) Tn Ek(CD ‖ Rn)을 공격자에게 전송하게 된다. H(ID) Tn Ek(CD ‖ Rn)을 전송 받은 공격자는 그대로 태그에게 재전송하면, 그림 1의 단계 7에서 비교를 통한 리더 인증과정을 통과하게 된다. 공격자임에도 불구하고 정상적인 리더로 인증을 받는 점은 프로토콜 설계 자체에 큰 오류로 보여 진다. 그림 2와 그림 3은 공격자와 태그 간 공격 시나리오를 나타낸 것이다.

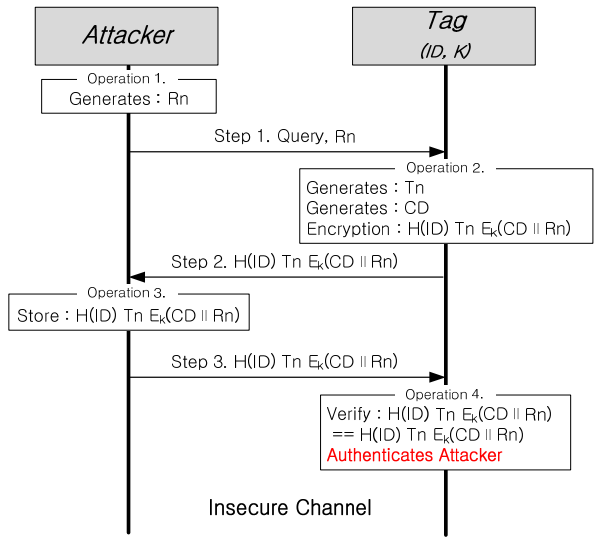


그림 3. DAP3-RS의 스푸핑 공격과 재전송 공격
Fig. 3. The Spoofing and Replay Attacks of the DAP3-RS

Ⅳ. 제안 프로토콜

본 장에서는 DAP3-RS의 문제점을 개선한 RFID 인증 프로토콜을 제안한다. 그림 4는 AES 알고리즘 기반의 RFID 인증 프로토콜을 나타낸 것이다.

4.1. 가정 사항 및 표기법

본 논문에서 제안한 프로토콜은 다음과 같은 가정 하에서 동작하며, 표 2는 제안 프로토콜에서 사용된 표기법 나타낸 것이다.

표 2. 제안 프로토콜의 표기법
Table 2. The Notations of the Proposed Protocol

Notations	Descriptions
Query	Reader's Query
Rn	Reader's Random Number
Tn	Tag's Random Number
ID	Tag's Unique Identification
K	Tag's and Reader's Symmetric Key
Tag Info	Information of the Tag
Ex()	AES Encryption
Dx()	AES Decryption
α, β	Encrypted Data
‖	Operation for Concatenation
⊕	eXclusive-OR

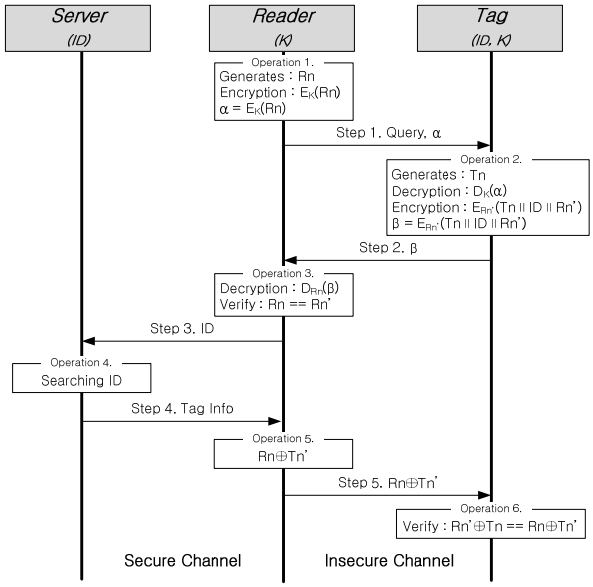


그림 4. 제안 프로토콜
Fig. 4. The Proposed Protocol

① 서버와 리더 사이는 공격자의 공격에 안전한 통신 채널을 이용한다.

② 리더와 태그 사이는 공격자의 공격에 취약한 무선 채널을 사용한다.

③ 리더와 태그는 난수를 생성할 수 있다.

④ 리더와 태그는 AES(Advanced Encryption Standard) 암·복호화 연산이 가능하다.

⑤ 태그는 고유 식별 정보 ID를 가지고 있으며, 리더로 부터 전원을 공급받는 수동형 태그로 가정한다.

4.2. 제안 프로토콜의 인증 절차

제안 프로토콜은 AES 알고리즘과 리더, 태그의 난수를 이용한 인증 절차를 수행한다. 본 절에서는 제안 프로토콜의 인증 절차를 알아본다.

◎ Step 1
리더 : Generates Rn
Encryption $\alpha = E_K(Rn)$
리더 → 태그 : Query, α

리더는 난수 Rn을 생성하여, 비밀키 K로 암호화한 α를 생성한다. α를 생성한 리더는 질의 Query와 함께 태그에게 전송한다.

◎ Step 2
태그 : Generates Tn
Decryption $D_K(\alpha)$
Encryption $\beta = E_{Rn'}(Tn \| ID \| Rn')$
태그 → 리더 : β

α를 전송받은 태그는 난수 Tn을 생성하고, 비밀키 K로 α를 복호화 하여 Rn'을 획득한다. 그리고 태그의 난수 Tn, 태그의 고유 식별 정보 ID, Rn'을 연접하여, AES로 암호화한 β를 생성한다. 이때 태그의 암호화에 사용되는 비밀키는 Rn'이고, β를 리더에게 전송한다.

◎ Step 3
리더 : Decryption $D_{Rn}(\beta)$
Verify Rn == Rn'
리더 → 서버 : ID

β를 전송받은 리더는 리더의 난수 Rn을 비밀키로 사용하여 β를 복호화 한다. 복호화하여 얻어진 Tn ‖ ID ‖ Rn'에서 Rn과 Rn'이 같은지 비교한다. 만약 같다면 정상적인 태그로 인증을 하고, 만약 다르다면 공격자로 취급하고 통신을 중단한다. 태그 인증 후 리더는 태그의 고유 식별 정보 ID를 서버에게 전달한다.

◎ Step 4
서버 : Searching ID
서버 → 리더 : Tag Info

ID를 전송받은 서버는 데이터베이스에서 ID에 해당되는 Tag Info를 찾아 리더에게 전송한다.

◎ Step 5
리더 : Rn⊕Tn'
리더 → 태그 : Rn⊕Tn'

Tag Info를 전송받은 리더는 난수 Rn과 β를 복호화하여 얻은 Tn'을 XOR 연산하여 태그에게 전송한다.

Rn⊕Tn'을 전송받은 태그는 α를 복호화하여 얻은 Rn'과 Tn을 XOR 연산하고, 태그에게 전송된 Rn⊕Tn'와 같은지를 비교하게 된다. 만약 같을 경우 정당한 리더로 인증하고, 다를 경우 공격자로 간주하고 통신을 종료한다.

태그에서 리더 인증 절차를 통과하게 되면 이후 프로세스를 진행 할 수 있다.

V. 결 론

본 장에서는 제안 프로토콜과 DAP3-RS를 보안성 측면과 효율성 측면에서 비교 분석한다.

표 3은 제안 프로토콜과 DAP3-RS의 보안성을 비교 분석한 결과이다.

표 3. 제안 프로토콜과 DAP3-RS의 보안성 분석
Table 3. The Security Analysis of the Proposed Protocol and the DAP3-RS

Protocols / Items	DAP3-RS	The Proposed Protocol
Location Tracking	Unsafe	Safe
Spoofing Attack	Unsafe	Safe
Replay Attack	Unsafe	Safe
Eavesdropping	Safe	Safe
Authentication	Not Supported	Mutual Authentication

5.1. 보안성 분석

5.1.1. 위치 추적

위치 추적은 리더의 질의에 항상 동일한 값으로 응답하는 상황을 이용한 공격방법이다.

제안 프로토콜의 태그 응답 값 β는 매 세션 가변적으로 값이기 때문에 위치 추적에 안전하다. 그 이유는 태그에서 β를 생성할 때, 태그에서 매 세션 새로운 난수 Tn을 생성하고 Tn을 포함하여 암호화하기 때문이다. 그러나 DAP3-RS의 태그응답은 특정 비트 구간이 고정되어 있기 때문에 위치추적이 가능하다.

리더 질의에 대한 태그의 응답 값은 H(ID) Tn E_k(CD ‖ Rn)이다. 최상위 비트부터 160번째 비트까지 H(ID)는 각 태그마다 고유한 ID를 해싱한 값으로 값이 변하지 않는 점을 이용해 공격자는 위치추적이 가능해진다.

5.1.2. 스푸핑 공격 및 재전송 공격

본 논문에서 제안한 프로토콜은 매 세션 새로운 리더, 태그의 난수 Rn과 Tn을 이용하여 인증 절차를 수행하기 때문에 공격자는 스푸핑 공격을 할 수 없다. 또한 Rn과 Tn은 매 세션 새로이 생성되기 때문에 공격자가 재전송 공격을 하더라도 인증 절차에서 방어할 수 있다. 하지만 DAP3-RS는 리더와 태그가 동일한 H(ID) Tn E_k(CD ‖ Rn) 데이터로 태그 인증과 리더 인증을 수행하는 오류를 범하고 있다.

5.1.3. 도청 공격

제안 프로토콜은 인증에 사용되는 Rn, Tn, ID를 AES 알고리즘을 통하여 암호화하기 때문에 공격자가 도청 공격을 하더라도 메시지 자체를 해독할 수 없다. DAP3-RS도 태그 ID를 해싱하기 때문에 ID 그 자체를 획득할 수 없고, 인증 절차에 사용되는 CD, Rn 또한 AES 알고리즘으로 암호화하기 때문에 공격자는 CD와 Rn을 획득할 수 없다. 그러므로 제안 프로토콜과 DAP3-RS 모두 도청 공격에 안전하다.

5.1.4. 인증 절차

제안 프로토콜의 인증 절차는 정당한 태그라면 비밀키 K를 가지고 있기 때문에 리더의 난수 Rn을 얻을 수 있다. 그리고 태그가 생성한 α는 리더의 난수 Rn을 비밀키로 사용하기 때문에, 정당한 리더만 α를 복호화하여 마지막 단계의 Rn⊕Rt를 태그에 전달할 수 있게 된다. 이처럼 비밀키 K, 리더 난수 Rn, 태그 난수 Tn을 이용한 인증로 다양한 공격을 방어할 수 있다. 그러나 DAP3-RS는 공격자가 Query와 난수 Rn을 생성하여 태그에게 전달하고, 태그에서 생성한 H(ID) Tn E_k(CD ‖ Rn)를 받아 다시 태그에게 재전송 시 인증과정을 통과하는 매우 위험한 상황이 성립하게 된다. 이는 DAP3-RS의 인증과정은 의미 없는 과정이며, 프로토콜 자체의 오류를 범하고 있다.

5.2. 효율성 분석

DAP3-RS는 해시 함수와 AES 알고리즘을 동시에 사용하는 방법을 제안하였다. 자원이 한정된 RFID 시스템의 태그에 해시 함수와 AES 알고리즘을 연산하는 것은 비효율적으로 보여 진다. 뿐만 아니라 서버의 데이터베이스에서 태그 ID를 찾기 위해 평균 ⌈n/2⌉번의 해시 연산은 서버에 부하를

일으킬 여지가 있다. 제안 프로토콜에서는 AES 알고리즘만을 사용하기 때문에 태그 구현 시 상당히 효율적이다. 그리고 DAP3-RS는 인증에서 CD라는 Changed Data를 생성하고 관리하여야 하나 제안 프로토콜은 리더와 태그의 난수를 이용하는 장점이 있고, 제안 프로토콜의 전체 통신 라운드 수와 리더-태그 간의 송·수신되는 전체 데이터에서 DAP3-RS에 비해 약 15%, 53%정도 줄었다. 표 4는 제안 프로토콜과 DAP3-RS의 효율성에 관한 분석을 표로 나타낸 것이다.

표 4. 제안 프로토콜과 DAP3-RS의 효율성 분석
Table 4. The Efficiency Analysis of the Proposed Protocol and the DAP3-RS

		DAP3-RS	The Proposed Protocol
Tag	Random Number	1	1
	AES	1E	1E, 1D
	Hash	1H	-
	Etc.	1CD	1XOR
Reader	Random Number	1	1
	AES	1D	1E, 1D
	Hash	-	-
	Etc.	-	1XOR
Server	Hash	⌈n/2⌉	-
The Number of Steps		6	5
Data Length		608 bits	288 bits

E: Encryption, D: Decryption, H: Hash Function, CD: Changed Data, Data Length : Between Reader and Tags

Ⅵ. 결 론

RFID 기술은 바코드를 대체하는 기술로 최근 다양한 산업에 사용되면 각광받고 있다. 그러나 무선 주파수를 이용하는 특성으로 도청, 위치추적, 스푸핑 공격, 재전송 공격 등과 같은 공격에 취약하다는 단점이 이슈화 되고 있다. 이러한 문제를 해결하기 위해 암호학적 방법과 인증 절차를 통해 다양한 공격을 방어하는 프로토콜이 지속적으로 연구되어지고 있다. 2012년 배우식은 해시함수와 AES 알고리즘을 태그에 적용한 RFID 시스템에서 프라이버시 보호를 위한 인증 프로토콜 설계(DAP3-RS)를 제안하였다. DAP3-RS는 태그의 고유 식별정보를 해싱하고, 리더와 태그의 난수를 AES 암호화한 데이터를 인증 과정에 사용하여 공격자의 공격에 안전하다고 주장하였다. 그러나 DAP3-RS는 해시된 태그의 고유 식별 정보는 고정된 체 무선 상에 전송되기 때문에 공격자가 위치추적을 할 수 있는 문제점이 존재함을 본 논문에서 증명하였다. 그리고 인증 절차에 사용된 AES로 암호화된 난수 값은 공격자가 태그에게 재전송시 공격자 임에도 불구하고 인증과정을 통과하였다.

본 논문에서는 자원이 제한된 RFID 태그에 AES 알고리즘과 난수를 이용한 프로토콜을 제안하였다. 제안 프로토콜은 AES로 암호화된 리더와 태그의 난수를 인증에 사용하여, 다양한 공격을 방어한다. 뿐만 아니라 DAP3-RS에 비해 연산량 측면에서 효율적임을 증명하였다.

References

[1] A. Juels, “RFID security and privacy: a research survey,” *IEEE J. Sel. Area Comm,* vol. 24, no. 2, pp. 381-394, Feb. 2006.

[2] J. Aragones-Villella, A. Martinez- Balleste, and A. Solanas, “A brief survey on RFID privacy and security,” in *Proc. IAENG World Congress on Eng. (WCE)*, vol. 2, pp. 1488-1493, Jul. 2007.

[3] S. E. Sarma, S. A. Weis, and D. W. Engels, “RFID systems and security and privacy implications,” in *Proc. Cryptographic Hardware and Embedded Systems (CHES), LNCS,* vol. 2523, pp. 454-469, Aug. 2003.

[4] B. Koo, G. Ryu, S. Yang, T. Chang and S. Lee, “Low-cost AES implementation for RFID tags” *J. of Korea Institute of the information Security and Cryptology (KIISC),* vol. 16, no. 5, pp. 67-77, Oct. 2006.

[5] D. Kwon, J. Lee, and B. W. Koo, “Improved cryptanalysis of lightweight RFID mutual authentication protocol LMAP, M2AP, EMAP”, *J. of Korea Institute of the information Security and Cryptology (KIISC),* vol. 17, no. 4, pp. 103-113, Aug. 2007.

[6] H. Ahn, E. Yoon, K. Bu and I. Nam,

"Secure and efficient DB security and authentication scheme for RFID system", *J. of Korea Information and Communications Society (KIISC)*, vol. 36, no. 4, pp. 197-206, Apr. 2011.

[7] B. W. Sik, "Design of an authentication protocol for privacy protection in RFID systems", *J. of Digital Policy and Management*, vol. 10, no. 3, pp. 155-160, Apr. 2012.

[8] S. A. Weis, S. E. Sarma, R. L. Rivest and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification system," in *Proc. Security in Pervasive Computing (SPC)*, LNCS 2802, pp. 201-212, Mar. 2003.

오 세 진 (Sejin Oh)

2009년 2월 경운대학교 컴퓨터공학과 학사
2011년 2월 경북대학교 전자전기컴퓨터학부 석사
2011년 3월~현재 경북대학교 전자전기컴퓨터학부 박사과정
<관심분야> RFID, 정보보호, 임베디드 시스템

이 창 희 (Changhee Lee)

1992년 2월 경북대학교 컴퓨터공학과 학사
1994년 2월 경북대학교 컴퓨터공학과 석사
1998년 8월 경북대학교 컴퓨터공학과 박사
1998년 9월~현재 계명문화대학 컴퓨터학부 교수
<관심분야> RFID, 임베디드 시스템, 시험구조

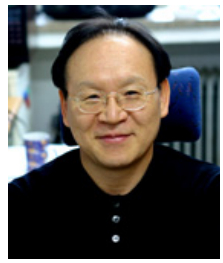
윤 태 진 (Taejin Yun)

1994년 2월 경북대학교 컴퓨터공학과 학사
1996년 2월 경북대학교 컴퓨터공학과 석사
2012년 2월 경북대학교 컴퓨터공학과 박사
1999년 3월~현재 경운대학교 모바일공학과 교수
<관심분야> 정보보안, 센서 네트워크, 임베디드

정 경 호 (Kyungho Chung)

2000년 2월 대구대학교 컴퓨터정보공학과 학사
2002년 2월 경북대학교 컴퓨터공학과 석사
2011년 2월 경북대학교 컴퓨터공학과 박사
2005년 3월~현재 경운대학교 컴퓨터공학과 교수
<관심분야> 임베디드 리눅스, RFID, 정보보호

안 광 선 (Kwangseon Ahn)



1972년 2월 연세대학교 전기공학과 학사
1975년 2월 연세대학교 전자공학과 석사
1980년 2월 연세대학교 전자공학과 박사
1977년 3월~현재 경북대학교 컴퓨터공학과 교수
<관심분야> 임베디드 시스템 설계, RFID 시스템