RFID 기반 개체식별장치의 정보보호를 위한 프로토콜 모델에 대한 연구

강정화*, 김재중**, 곽계달***, 신승중****

*한양대학교 공학대학원 컴퓨터공학과
**한양대학교 신뢰성분석연구센터
***한양대학교 전기전자컴퓨터공학부
****한세대학교 IT 학부

e-mail : expersin@hansei.ac.kr

A Study of A Protocol Model for Information Security of the RFID Base Individual Identification Device

Jung-Hwa Kang*, Jae-Jung Kim**, Kae-Dal Kwack*** and Seung-Jung Shin****

*Division of Electronics and Computer Engineering, Hanyang University
**Reliability Analysis Research Center, Hanyang University
*** Dept. of Electronics and Computer Engineering, Hanyang University
****Dept. of Information Technology, Hansei University

요 약

최근 들어 유전자원의 보존과 효율적인 관리에 대한 요구가 증가함에 따라 이러한 요구에 적합한 무선 인식기술로 RFID 가 주목 받고 있다. 기존의 바코드 기술에 비해 RFID 시스템은 주파수를 이용하여 마이크로 칩이 내장된 태그의 정보를 비접촉식으로 원거리에서도 인식할 수 있으며 대량의 태그 인식 및 판독, 정보의 수정도 가능하여 이러한 장점으로 인해 여러 산업분야에서 사용되기 시작하였다. 이 논문은 축산, 유통 및 동물과 관련된 IT 산업에서 신속 정확한 정보 획득 및 정보 보호의 방안으로 특정 그룹에 포함되는 객체들에 대한 접근이 가능한 태그의 구조를 제안하고 RFID 태그에 저장되어 있는 ID 의 불법적인 유출을 방지하기 위한 프로토콜을 제안한다.

1. 서론

RFID 시스템은 다양한 분야에 적용이 가능하지만 리더와 태그 사이에 물리적인 접촉이 없이 공개된 채널에서 무선 주파수를 사용해 인식하므로 그에 따른 정보 노출로 인한 보안 문제와 개인 정보 침해라는 역기능도 내포하고 있다. 대량의 가축을 사육하는 농가에선 개체별 상세정보를 검색하는 경우와 사육하는 대량의 가축을 관리함에 존재유무 및 안전상태만을 체크하기 위해서 객체 인식이 필요할 경우도 있다. 후자의 경우 상호인증으로 인해 태그 인식을 한다며 시간의 소요와 불필요한 연산량으로 인해 비합리적일 수 있다. 본 논문은 특정 그룹을 포함하는 태그의 구조를 제안하여 그룹 ID 를 이용하여 특정 리더만이 특정 그룹에 포함되는 객체들에 접근이 가능하도록 함으로써 빠르고 정확한 정보의 획득과 ID 의 불법적인 유출의 방지와 효율적인 인식동작을 수행하기 위해 객체 접근방식에 따라 인증 절차를 다르게 수행하도록 하는 프로토콜을 제안한다.

2. 관련 연구

2.1 RFID 시스템

RFID 는 무선주파수를 이용하여 객체를 인식하는 기술이다. 통합된 회로 칩과 안테나를 포함하고 있는 작은 태그(tag)로써, 정보를 전송하고, 처리하고 저장하기 위하여 RFID 리더로부터 전송된 무선전파에 반응하는 능력을 지닌 기술이다[1] 최근에는 RFID 시스템의 구축 비용의 하락과 기술 개발에 따라 기업들은 RFID 기술을 기존 응용시스템과의 결합하려는 시도와 새로운 비즈니스와의 접목을 통해 그 가치가 높아지고 있는 상황이며 앞으로 더욱 넓은 목적으로 활용될 전망이다.[2][3]

2.2 동물식별용 RFID 국제표준 현황

동물의 식별용으로 사용하는 RFID 의 국제적인 규격은 ISO 11784 와 ISO 11785, 그리고 ISO 14223 이다. 수분에 약한 900MHz 대의 고주파가 아닌, 액체와 불순물에도 투과력이 좋은 134.2kHz 대역의 주파수를 사용한다.

2.2.1 ISO 11784

동물식별용 RFID 의 코드구조를 정의한 국제표준이다[4]. 동물에 사용되는 64bit 의 인식코드로서 각 나라별로 관리를 한다.

2.2.2 ISO 11785

동물식별용 RFID 의 트랜스폰더와 송수신기 사이의 전송 프로토콜에 대해서 정의한 국제표준으로 트랜스폰더를 구동하기 위한 리더의 규격을 정의한다[5]. 반이중(HDX)과 전이중(FDX-B)의 두 가지 전송 방식을 규정한다.

2.2.3 ISO 14223

동물용 RFID 의 고급 트랜스 폰더(advanced transponder)에 대한 무선인식코드 구조를 규정하며 송수신기와 고급 트랜스폰더 간의 통신규격 및 HF(High Frequency) 접속을 정의한다. ISO 11784 및 ISO 11785 의 확장된 개념이며 호환성 유지와 메모리 용량 증가에 대응하기 위한 확장코드 구조나 암호 처리에 관한 확장코드도 규정하고 있다.

2.3 RFID 공격의 유형

1) 도청(Eavesdropping)

리더와 태그는 무선으로 인식하므로 도청을 통해 태그의 정보를 알아낸 후 도청한 정보를 재 전송함으로써 서버에 접속할 수 있다. 이로써 태그의 상세정보를 알아내는데 이용될 수 있다. 따라서 RFID 시스템은 도청으로 인한 어떠한 정보도 알아낼 수 없도록 설계되어야 하며 이를 전방위 보안성(Forward Security)이라 한다.

2) 위치추적(Location Tracking)

공격자 또는 악의적인 리더가 태그로부터 정상적인 리더에게 전송되는 정보를 가로채고 검사함으로써 태그의 위치 변화를 감지하여 소유자의 이동경로를 파악할 수 있다. 따라서 위치추적에 안전한 RFID 시스템을 위해서는 태그로부터 수신되는 정보를 매 세션마다 변경하여 악의적인 리더가 가로챈 태그의 정보가 동일한 태그의 정보임을 구분할 수 없도록 해야한다.

3) 스푸핑(Spoofing)

공격자가 정당한 태그 및 리더로 가장하여 인증과정을 통과하는 방법으로 수집한 정보로 다른 상세한 정보를 획득할 수 있다. 이에 안전한 RFID 시스템을 위해서는 태그의 정보에 암호화를 하거나 태그에 접근하는 권한에 대해 관리할 수 있는 매커니즘이 필요하다.

4) 전송방해(Interference)

공격자는 RFID 시스템으로부터 어떠한 정보도 수집할 수 없지만 RFID 시스템이 정상적으로 작동하지 못하도록 정보의 전송을 방해할 수 있다. RFID 인증 과정 중에 메시지 유실이 발생되는 경우 현재 또는 다음 세션의 인증이 비정상적인 상태가 발생할 수 있다. 따라서 정보 전송 방해에 대한 공격을 탐지할 수 있는 기능이 필요하다.

3. 제안하는 프로토콜 모델

3.1 제안하는 태그 구조

제안하는 기법은 객체의 용도 및 소속을 구별하기 위한 정보를 gID(group ID)로 정의하고 CA 로부터 gID 를 발급받은 특정 리더가 다수의 태그 중 해당 gID 가 등록된 특정 태그만을 검색하도록 제안한다. 태그 내의 tagID 는 불법적인 태그의 복제 및 정보 해독이 용이하지 못하도록 하기 위해 Fast SEED[6] 암호화 알고리즘을 사용하였으며 이를 통해 생성된 값을 eID(encrypted ID)로 정의하고 태그에 저장한다. 서버에는 태그의 고유한 ID 인 tagID 와 eID 를 함께 저장한다. 특정 리더로부터 질의를 받은 특정 태그는 태그에 저장된 eID 를 사용하여 가변적인 값을 생성하여 응답한다.

· gID(group ID) : 각 객체의 용도 및 소속 등 필요에 의해 객체의 종류를 구별하기 위한 ID이다. 제안하는 RFID 검색 프로토콜에서는 CA로부터 gID를 리더에 발급받아 질의문에 gID를 포함시켜 특정 태그만을 검색한다.

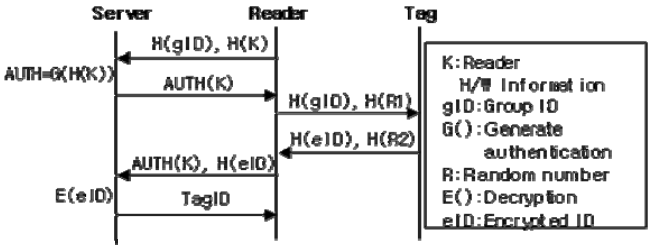
· tagID : 각 태그의 고유한 ID이며 gID와 eID를 생성하기 위한 기본 키이다. 제안하는 RFID 검색 프로토콜에서는 서버에 tagID를 저장하고 태그에는 해당하는 tagID를 저장하지 않고 Fast SEED 알고리즘에 의해 암호화된 값인 eID를 태그에 저장한다.

· eID(encrypted ID) : 태그의 고유한 ID인 tagID를 Fast SEED 알고리즘에 의해 암호화하여 생성된 값이다. 서버와 태그에 각각 저장되며 특정 리더의 질의시 응답으로 eID 를 사용한다.

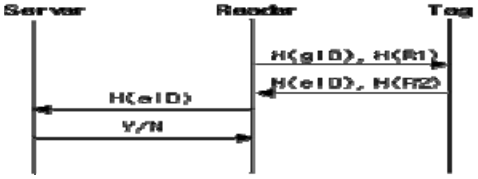
3.2 제안 프로토콜

본 논문에서 제안하는 프로토콜은 gID 를 적용한 태그 구조에 적합하면서 태그의 검색 목적에 따라 인식 절차가 다르게 동작하도록 한다.

· 고수준 보안이 적용된 프로토콜



· 저수준 보안이 적용된 프로토콜



4. 안전성 비교 분석

제안하는 프로토콜은 다음과 같은 공격에 대해서 안전성을 보장할 수 있다. <표 2>는 기존의 인증기법들과 제안 프로토콜과의 안전성을 비교 분석하였다.

<표 2> RFID 공격 유형에 대한 안전성 비교

	재전송	스푸핑	전송방해	위치추적
Hash Lock	X	X	X	X
Randomized Hash Lock	O	X	O	O
Hash Chain	X	O	O	O
제안프로토콜	O	O	O	O

5. . 결론 및 향후 과제

본 논문에서 제안한 RFID 태그의 구조와 프로토콜은 빠르고 정확한 정보의 획득과 효율적인 인식동작을 위한 접근 방식에 따라 인증 절차를 다르게 수행하도록 제안하였다. 그러나 본 논문은 실제 RFID 시스템의 환경과 다소 상이할 수 있으니 실제 환경에서 적용할 수 있는 시스템을 구현해야 한다.

REFERENCES

[1] Wu, N. C., Nystrom, M.A., Lin, T,R., & Yu, H.C. Chanllenges to global RFID adoption. Technovation. 26, 1317-1323, 2006

[2] G. Avoine, and P. Oechslin, “RFID Traceability: A Multilayer Problem,” EPFL, Oct. 2004.

[3] K. Finkenzeller, “RFID Handbook,” John Wiley & Sons, 1999.

[4] International Standardization Organization, ISO 11784: Agricultural equipment – Radio frequency identification of animals – Code structure, 1996, 2004

[5] International Standardization Organization, ISO 11785: Agricultural equipment – Radio frequency identification of animals – Technical concept, 1996

[6] Ko, H., Kim, J., Jung, j., Lee, Y., Joe, S., and Chang, Y., “A Study on the RFID Tag Encryption using Fast SEED,” Proceedings of the international Methods in Science and Engineering 2007 (ICCMSE 2007), Vol. 2, Parts B, 2007, PP. 571-574.