https://doi.org/10.5392/JKCA.2019.19.09.476

RFID 요킹증명을 위한 인접태그 정보 획득 기법

A Tag Proximity Information Acquisition Scheme for RFID Yoking Proof

함형민
배재대학교 사이버보안학과

Hyoungmin Ham(neoham12@gmail.com)

요약

RFID 요킹증명은 한 쌍의 태그가 동시에 스캔 되었는지를 증명한다. 단일 리더에 의해 동시에 스캔 된 태그들은 서로 인접해 있기 때문에, 요킹증명은 태그가 부착된 객체들의 물리적 인접성을 검사해야 하는 응용에서 사용된다. 현재까지 제안된 대부분의 요킹증명 기법들은 인접한 태그에 관한 사전정보가 필수적이다. 만약 인접한 태그에 관한 정보를 수집하는 과정에서 오류가 발생하면, 이후의 증명들은 모두 검증에 실패하게 된다. 그러나 현재까지 인접한 태그에 관한 정보를 얻기 위한 구체적인 방법을 제시한 연구는 아직 없다. 이 연구에서 나는 요킹증명 기법을 위한 인접태그 정보 획득 기법인 TPIA을 제안한다. 제안기법은 스캐닝영역 결정과 스캐닝영역 검증의 두 단계로 구성된다. 스캐닝영역 결정 단계에서는 태그들의 위치와 전송범위를 고려하여 태그들을 스캔할 영역의 크기와 위치를 결정하며, 스캐닝영역 검증 단계에서는 고정된 위치의 참조태그를 사용하여 태그 스캐닝이 스캐닝영역 안에서 수행되었는지 여부를 검증한다. 나는 분석에서 제안하는 스캐닝영역이 정상적인 인접태그 정보의 획득을 보장하며, 스캐닝영역 검증이 스캐닝영역의 변형과 이탈을 감지하는 것을 보인다.

■ 중심어 : | RFID | 인접태그 정보 | 스캐닝영역 | 태그위치 | 요킹증명 |

Abstract

RFID yoking proof proves that a pair of tags is scanned at the same time. Since the tags scanned simultaneously by a single reader are adjacent to each other, the yoking proof is used in applications that need to check the physical proximity of tagged objects. Most of the yoking proof schemes require pre-knowledge on adjacent tags. If an error occurs in the process of collecting information about adjacent tags, all subsequent proofs will fail verification. However, there is no research that suggests specific methods for obtaining information about adjacent tags. In this study, I propose a tag proximity information acquisition scheme for a yoking proof. The proposed method consists of two steps: scanning area determination and scanning area verification. In the first step, the size and position of the area to scan tags is determined in consideration of position and transmission range of the tags. In the next step, whether tag scanning is performed within the scanning area or not is verified through reference tags of the fixed position. In analysis, I show that the determined scanning area assures acquisition of adjacent tag information and the scanning area verification detects deformation and deviation of the scanning area.

■ keyword : | RFID | Tag Proximity | Scanning Area | Location of Tags | Yoking Proof |

접수일자 : 2019년 08월 01일
수정일자 : 2019년 08월 23일
심사완료일 : 2019년 08월 25일
교신저자 : 함형민, e-mail : neoham12@gmail.com

I. 서 론

RFID(Radio Frequency Identification) 는 무선통신을 이용하여 자동화된 객체식별을 제공하는 기술이다. RFID는 자동화된 객체식별과 함께 객체의 추적과 모니터링을 요구하는 동물 추적, 물류 관리 같은 응용에서 사용될 수 있으며, 이 같은 장점 때문에 RFID를 이용한 상용솔루션과 연구 결과가 지속적으로 발표되고 있다.

RFID 요킹증명은 한 쌍의 태그가 동시에 스캔 되었는지를 증명하기 위해 제안되었다. 리더에 의해 동시에 스캔 된 태그들은 서로 인접해 있음으로, 요킹증명은 객체들의 물리적 인접성을 검사해야 하는 여러 응용에서 활용될 수 있다. 예를 들어, 약품과 처방전이 하나의 상자에 포장되어 있는지 검사해야 할 경우, 약품과 처방전에 부착된 태그들을 상자 단위로 스캔하여, 구성품들이 상자에 들어있는지를 확인할 수 있다[1]. 다른 예로, 여러 칩셋이 포함된 메인보드의 생산공정에서도, 누락된 칩셋이 없는지 확인하기 위해 요킹증명을 활용할 수 있다. 이 검사과정은 리더와 태그 간의 무선전송을 이용하여, 제품의 포장을 훼손하지 않고 빠르게 수행될 수 있다는 장점이 있다.

오늘날까지 다양한 요킹증명 기법들이 제안되고 있다[1-17]. 요킹증명 기법은 증명의 생성과 검증의 두 단계로 구성된다. 우선 리더는 인접한 한 쌍의 태그를 스캔하고, 스캐닝 결과를 원격지의 검증자에게 전송한다. 검증자는 태그의 ID, 비밀키, 태그의 인접성 같은 사전지식을 통해 태그들이 동시에 스캔 되었는지를 검증한다. 이 중에서도 특히 인접한 태그들에 대한 사전지식은 요킹증명을 검증하기 위해 필수적이며, 이 때문에 초기 단계에서부터 오류없이 정확하게 수집되고 보호되어야 한다. 그러나 인접한 태그들에 대한 사전지식을 얻는 과정에서, 서로 인접하지 않은 태그들이 리더에게 스캔 되거나 인접한 태그 중 일부 스캔 된다면, 사전지식 이 잘못 구축된 태그들은 이후의 모든 검증에 실패하게 된다. 예를 들어, 구성품들이 하나의 박스 안에 포장되었는지 검사해야 하는 경우를 생각해 보자. 주기적인 검사를 위해서, 사전에 각 박스 안에 어떤 구성품들이 포장되어 있는지를 알아내는 과정이 필요하다. 직관적으로, 이 정보는 구성품에 부착된 태그들을 상자 단위로 스캔하여 얻을 수 있다. 이 준비과정에서 태그 스캐닝은 정확하게 상자 단위로 이루어져야 한다. 만약 리더가 한 번에 하나 이상의 상자를 스캔했거나, 상자 안에 구성품 중 일부만 스캔했다면, 이후에 해당 상자들에 대한 검증은 모두 실패하게 된다. 이처럼, 요킹증명 기법에서 인접한 태그에 대한 정확한 사전지식을 얻는 과정은 매우 중요하다. 그러나 현재까지 제안된 요킹증명 기법들[1-17]은 인접한 태그에 대한 사전지식을 얻기 위한 구체적인 방법을 고려하지 않고 있으며, 인접한 태그에 대한 사전지식이 필수적인 기법들[9-17]은 검증자가 검증에 필요한 태그의 그룹키, 그룹 ID 같은 사전지식들을 알고 있다고 가정하고 있다.

이 연구에서는 요킹증명 기법에서 올바른 사전지식 구축을 보장하기 위한 인접태그 정보 획득 기법을 제안한다. 제안기법은 두 가지 핵심단계로 구성된다. 첫 번째는 스캐닝영역 결정이다. 이 단계에서는 태그들의 위치와 전송범위를 고려하여, 리더의 위치와 리더의 전송범위를 결정한다. 두 번째는 스캐닝위치 검증이다. 이 단계에서는 고정된 위치의 참조태그를 통해 리더가 스캐닝한 위치를 검증한다. 나는 제안기법의 건전성을 증명하기 위해 잘못된 사전지식을 획득하게 되는 두 가지 경우를 정의하고, 제안기법이 이 잘못된 경우들을 효과적으로 예방하고 감지할 수 있음을 보인다.

논문의 구조는 다음과 같다. 2절에서 인접태그 정보의 획득을 위한 스캐닝영역 결정문제와 스캐닝영역 검증문제를 정의하고, 3절에서 배경지식과 관련 연구를 소개한다. 다음 4절에서는 인접태그 정보 획득 기법을 제안하고, 5절에서 제안기법이 2절에서 정의한 두 가지 문제를 효과적으로 해결할 수 있음을 보인 후, 마지막으로 결론을 내고 끝을 맺는다.

II. 문제정의

요킹증명을 검증하기 위해, 사전에 어떤 태그들이 서로 인접해 있는지를 아는 것은 매우 중요하다. 직관적으로, 인접한 태그에 관한 정보는 [그림 1]처럼 인접한 두 태그를 단일 리더로 한 번에 스캔하여 얻을 수 있다. 그러나 두 태그 사이의 거리, 리더의 위치, 송수신 범위

를 정의하지 않고 태그를 스캔한다면, 인접한 태그들의 정보를 정확하게 얻는 것은 불가능하다. 구체적으로, 서로 인접한 태그들이 인접하지 않은 것으로 잘못 보고되거나, 인접하지 않은 태그들이 인접한 것으로 잘못 인식될 수 있다. 여기서 인접태그 정보가 잘못 보고되는 두 가지 경우들을 각각 일부 스캔 그리고 원거리 스캔이라고 한다. [그림 1]은 정상적인 인접태그 정보가 획득되는 경우를 보여주고, [그림 2]와 [그림 3]은 어떤 경우에 잘못된 인접태그 정보가 획득될 수 있는지 일부 스캔과 원거리 스캔의 예를 보여준다.

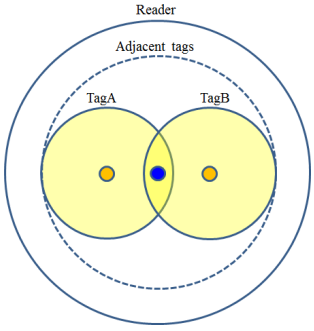

그림 1. 정상적인 인접태그 정보 획득

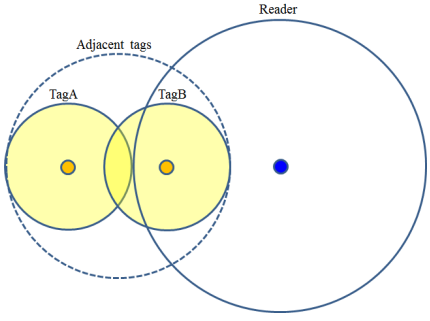

그림 2. 비정상적인 인접태그 정보 획득 (일부스캔)

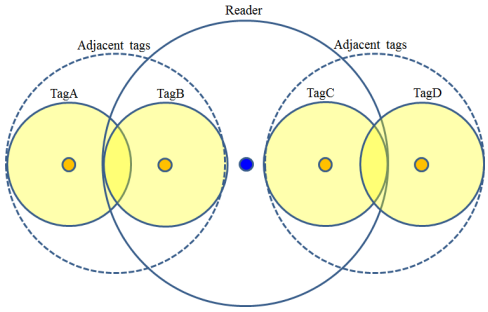

그림 3. 비정상적인 인접태그 정보 획득 (원거리 스캔)

이 절에서는 일부스캔과 원거리 스캔 없이 올바른 인접 태그 정보를 얻기 위해 해결해야 할 두 가지 문제들을 정의한다. 여기서 인접태그는 통신범위가 서로 겹치는 거리에 위치한 한 쌍의 태그이며, 인접태그 정보는 단일 리더로 인접한 태그를 스캔한 결과이다.

스캐닝영역 결정. 인접한 한 쌍의 태그로부터 인접태그 정보를 얻을 수 있는 단일 리더의 스캐닝영역을 결정하는 문제이다. 이 영역에서 단일 리더는 한 번의 태그스캐닝으로, 응답범위가 서로 겹치는 태그들의 응답을 모두 수신할 수 있어야 한다. 여기에 더해서, 이 영역에서는 인접하지 않은 태그의 응답은 수신할 수 없어야 한다. 여기서 나는 인접태그를 서로의 송신범위에 공통영역을 가지고 있는 태그들로 한정한다. 예를 들어, 제품들이 인접태그 단위로 같은 크기의 박스에 포장되어 있거나, 컨베이어 벨트의 위의 제품들이 인접태그 단위로 이동하는 경우들을 고려한다.

스캐닝영역 검증. 단일리더가 지정된 스캐닝영역에서 스캐닝을 했는지 검증하는 문제이다. 이 문제는 검증대상의 위치가 스캐닝영역으로 한정되는 특수한 경우의 위치검증 문제이다.

Ⅲ. 배경지식 및 관련 연구

3.1 요킹증명

최초의 요킹증명 프로토콜[1]은 한 쌍의 태그들이 RFID 리더에 의해 동시에 스캔 되었는지 확인하기 위해 A. Juels에 의해 제안되었다. RFID 리더는 한 태그

의 응답을 다른 태그의 응답을 얻기 위한 요청으로 사용하여 두 태그를 모두 증명에 포함 시킨다. 증명위조를 방지하고 생성된 증명을 검증하기 위해 비밀키와 시간초과라는 두 가지 기능을 사용한다. 각 태그에는 신뢰할 수 있는 검증자와 공유하고 있는 고유한 비밀키가 있으며, 증명은 이 비밀키를 포함하여 생성된다. 이 비밀키를 모르는 공격자는 증명을 생성할 수 없음으로 증명위조를 방지할 수 있다. 여기에 더해, 이 프로토콜은 동시에 스캔 되지 않은 두 개의 응답이 합쳐지는 경우를 방지하기 위해 증명생성 시간을 제한하는 타임아웃을 사용했다. 타임아웃이 발생하면 태그는 증명생성 과정을 종료한다.

[표 1]은 기본적인 요킹증명 프로토콜에서 사용된 표기법을 설명한다. 단순화하기 위해, 나는 증명생성에 참여하는 두 개의 태그를 Tag_A와 Tag_B로 표기한다. 요킹증명 프로토콜은 증명생성을 위해 다음 단계들을 수행한다.

1. 리더는 태그에게 질의메시지 left_proof를 전송한다. left_proof를 받은 Tag_A는 랜덤난수 r_A를 생성하고 이것을 자신의 ID A와 함께 리더에게 전송한다.
2. 리더는 r_A를 질의메시지 right_proof와 함께 Tag_B에게 전달한다.
3. Tag_B는 비밀키 xB와 MAC함수를 이용하여 응답메시지 Resp_B=MAC_xB[rA]를 생성하고 이를 자신의 ID B와 랜덤난수 r_B와 함께 리더에게 전송한다.
4. 리더는 r_B를 Tag_A에게 전달한다.
5. Tag_A는 비밀키 xA로 Resp_A=MAC_xA[rB]를 생성하고, 이를 리더에게 전송한다. r_B가 일정시간 안에 수신되지 않았다면 Tag_A는 현재세션을 종료한다.
6. 리더는 Tag_A와 Tag_B의 증명 P_AB=(A,B,Resp_A, Resp_B)를 검증자에게 전송한다.
7. 검증자는 Tag_A와 Tag_B의 ID, 비밀키를 포함하여 증명생성에 필요한 지식들을 사전에 알고 있다. 검증자는 이 사전지식을 통해 수신한 증명과 동일한 증명을 생성하고 이들을 비교한다. 수신한 증명과 생성한 증명이 동일하다면 검증이 성공한 것이다.

표 1. 표기법

표기법	
Tag_A	RFID 태그 A
Tag_B	RFID 태그 B
ID_A	태그 A의 ID
ID_B	태그 B의 ID
rA, rB	태그 A의 난수와 태그 B의 난수
t, r	검증자의 난수들
Delta	Time window
C_A, C_B	태그 A의 카운터와 태그 B의 카운터
xA, xB	태그 A의 대칭키와 태그 B의 대칭키
MAC_x[m]	MAC (Massage Authentication Code) 함수와 대칭키 x를 이용해 생성한 m에 대한 메시지 인증 코드
P_AB	Tag_A와 Tag_B의 요킹증명

3.2 요킹증명 기법들

초기에 제안된 요킹증명 기법들의 목표는 안전한 증명의 생성과 검증이다. [1-7]의 기법들은 증명생성 과정에 발생할 수 있는 공격들과 해당 공격으로부터 안전한 증명생성 및 검증과정을 제안하였다. 예를 들어 [2]는 [1]의 기법이 재전송에 취약하다는 점을 설명하고, 이 문제를 해결하기 위해 증명에 타임스탬프를 포함하였다.

이후에 제안된 요킹증명 기법들은 안전한 증명의 생성과 검증을 보장하면서 다양한 응용으로 요킹증명을 확장하였다. [10][12]의 기법들은 리더와 검증자의 연결이 불안정한 환경에서의 증명생성과 검증을 보장하기 위해 제안되었으며, [13][14]의 기법들은 물류추적 및 관리를 위해 제안되었다. 암호화알고리즘을 수행하는 태그를 사용하는 인증 및 암호화 기반의 요킹증명 기법들[15-17]도 제안되었다. 이 기법들은 암호화알고리즘을 사용하지 않는 다른 기법들보다 더 강력한 안전성을 보장하지만, 시스템 구현에 드는 비용이 상대적으로 높다.

본 논문에서는 요킹증명 기법들을 인접태그 정보의 사용 여부에 따라 두 가지 유형으로 분류한다. 첫 번째는 초기 요킹증명, 다른 하나는 반복적 요킹증명이다.

초기 요킹증명에 해당하는 기법들은 증명생성과 검증을 위해 인접태그 정보를 사용하지 않으며, 증명 생성과정에 참여한 태그들이 동시에 스캔 된 점을 근거로 태그들의 물리적 인접성을 확인하기 위해 사용된다. 초기 요킹증명에서, 검증자는 인접태그에 관한 사전정보가 없기 때문에 현재 스캔한 태그들의 인접성 여부만

확인할 수 있다. 사전에 인접한 태그를 파악하지 않고, 획득한 인접태그 정보를 유지하지 않는 [1-8]의 기법들이 초기 요킹증명에 해당한다.

반복적 요킹증명 기법들은 증명의 생성과 검증을 위해 인접태그 정보를 사용한다. 사전에 획득한 인접태그 정보로 태그를 그룹화하고, 인접태그의 상태를 모니터링하기 위해 사용된다. 사전에 인접한 태그를 파악하고, 그룹ID나 그룹키를 사용하며, 해당 정보를 유지하는 [9-17]의 기법들이 반복적 요킹증명에 해당한다.

반복적 요킹증명에서 요구하는 인접태그 정보는 초기 요킹증명을 통해 얻을 수 있다. 하지만 정확한 정보를 얻기 위해서는 2절에서 정의된 문제들을 해결할 수 있는 별도의 방법이 필요하다.

Ⅳ. 제안기법

이 절에서 나는 요킹증명의 초기 단계에서 올바른 사전지식 구축을 위한 인접태그 정보 획득 기법을 제안한다. 제안기법은 스캐닝영역 결정, 스캐닝위치 검증의 두 가지 단계로 구성된다. 스캐닝영역 단계에서는 인접태그들을 스캔할 영역을 결정하고, 스캐닝영역 검증 단계에서는 지정된 영역에서 태그스캐닝이 수행되었는지 검증한다.

4.1 스캐닝영역 결정

스캐닝영역 결정 단계에서는, 인접한 태그들을 스캔하기 위한 리더의 위치와 송신범위를 결정한다. 이 영역은 태그의 통신범위와 통신범위의 교점을 고려하여 결정되며, 이 영역에서 리더는 한 번의 태그스캐닝으로 인접한 태그들을 스캔할 수 있다. 나는 이 조건을 만족하는 스캐닝영역을 다음과 같이 정의한다.

정의 (스캐닝영역). 태그의 통신(송수신)범위는 반지름이 r인 원 R_Tag이다. 인접한 태그 R_TagA와 R_TagB사이에 공통영역 (Common Region) CR_TagAB가 있다면, 두 태그의 중심점을 잇는 직선 L_TagAB는 반드시 CR_TagAB 를 통과한다. 이 직선 L_TagAB의 길이를 length(L_TagAB)라고 했을 때, 스캐닝영역은 반지름 r의 길이가 length(L_TagAB)/2 이고, 중심점이 L_TagAB의 중심점과 같은 원형의 영역으로 정의된다. [그림 4]는 서로 공통영역을 가지는 인접태그와 스캐닝영역의 관계를 보여준다.

리더는 인접태그로부터 인접태그 정보를 얻기 위해, 두 가지 조건을 만족해야 한다. 1) 우선 리더는 정의된 스캐닝영역과 동일한 크기의 통신범위를 가져야 한다. 즉, 리더의 통신범위는 반지름 length(L_TagAB)/2 의 원 R_Rd 이다. 2) 또한 리더는 L_TagAB의 중심에 위치해야한다. 즉, 리더는 R_TagA의 중심점으로부터, length(L_TagAB)/2의 지점에 위치해야한다.

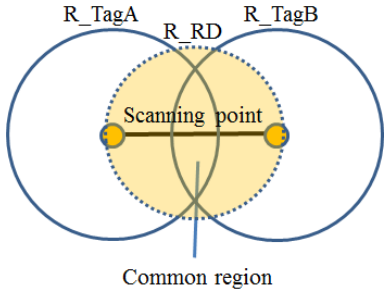

그림 4. 인접태그와 스캐닝영역

4.2 인접태그 스캐닝

인접태그의 스캐닝영역이 결정되면, 리더는 해당 영역에 배치된다. [그림 5]는 공통영역을 가지는 한 쌍의 인접한 태그 TagA와 TagB 사이에 정의된 스캐닝 영역과 동일한 스캔 범위를 가진 리더를 배치한 예시를 보여준다. 스캐닝 영역에 배치된 리더는 인접태그 정보를 얻기 위해 태그를 스캔한다. 이 과정은 다음과 같다.

1. 리더는 타임스탬프를 생성하고, 타임스탬프와 질의메시지를 브로드캐스트 한다.
2. 태그들은 타임스탬프와 질의메시지를 수신하고, 자신의 ID와 타임스탬프로 응답한다.
3. 리더는 인접태그들의 응답을 수신하고 두 번째 타임스탬프를 생성한다. 수신한 태그의 응답들과 두 개의 타임스탬프를 인접태그 정보로 저장한다.

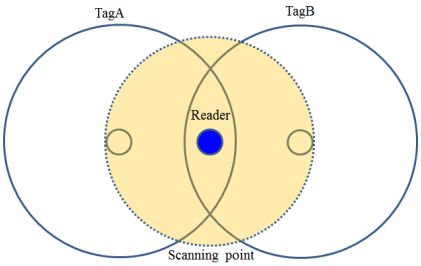

그림 5. 인접태그 정보 획득을 위한 인접태그와 리더의 배치

4.3 스캐닝영역 검증

지정된 스캐닝영역을 벗어난 리더의 스캐닝결과는 사전지식에 포함되지 않아야 한다. 스캐닝영역 검증은 고정된 위치의 참조태그를 통해, 리더가 스캐닝영역에서 태그를 스캔했는지 검증한다. 좀 더 자세하게, 스캐닝영역 검증은 다음 두 가지 잘못된 경우를 감지한다.

- 일부 스캔: 서로 인접한 두 태그 중 일부 (둘 중 하나)만 스캔한 경우를 의미한다.
- 원거리 스캔: 서로 인접하지 않은 두 태그 (공통영역이 없는 태그들) 를 스캔한 경우를 의미한다.

제안하는 스캐닝영역 검증기법은 위의 두 가지 잘못된 경우를 감지하기 위해 두 종류의 참조태그를 사용한다. 첫 번째는 스캐닝영역 내부의 참조태그이고, 두 번째는 스캐닝영역 외부의 참조태그이다. 이 두 종류의 태그들을 각각 내부참조태그 (Inside Reference Tag)와 외부참조태그 (External Reference Tag)로 부른다. 두 태그의 특징은 다음과 같다.

- 제안기법에서 내부참조태그 는 리더의 위치를 확인하기 위해 사용되며, 스캐닝 결과에 포함되어야 한다. 내부참조태그는 스캐닝영역의 중앙에 위치하며, 전송범위는 인접태그의 공통영역과 같다.
- 외부참조태그는 리더의 전송범위가 스캐닝영역을 초과하지 않는지 확인하기 위해 사용되며, 스캐닝 결과에 포함되어서는 안 된다. 외부참조태그는 스캐닝영역의 바깥쪽에 위치하며, 전송영역은 인접정보 수집 대상인 태그와 같다.

[그림 6]은 제안기법에서 스캐닝영역과 그에 따른 참조태그들의 위치를 보여준다. 그림에서 원들은 태그들의 통신범위이다. 가운데 위치한 원과 R_IRTag는 각각 내부참조태그와 송신범위를, 사면에 위치한 삼각형과 R_EXTag는 각각 외부참조 태그와 송신범위를 나타낸다. 내부참조 태그의 송신범위는 스캐닝영역 R__Rd에 포함되며, 외부참조 태그들은 스캐닝영역의 외부에 배치된다.

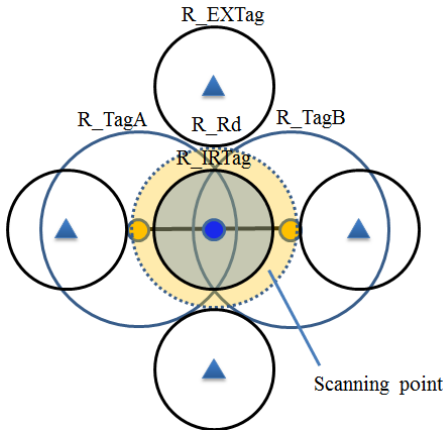

그림 6. 스캐닝영역 검증을 위한 참조태그의 배치

위치검증 단계. 검증자는 참조태그의 ID, 비밀키, 위치를 알고 있다. 위치검증은 다음 단계들로 수행된다.

1. 리더는 스캐닝포인트에서 태그를 스캔한다.
2. 검증자는 스캐닝결과에 내부참조태그가 포함되었는지 확인한다. 내부참조태그가 포함되지 않은 스캐닝결과는 무시한다.
3. 검증자는 스캐닝결과에 외부참조태그가 포함되었는지 확인한다. 외부참조태그가 포함된 스캐닝결과를 무시한다.

V. 분석

5.1 스캐닝영역의 정당성

주장 1. 스캐닝영역을 따르는 리더는 일부스캔 없이 인접한 두 태그로부터 올바른 인접태그 정보를 얻을 수 있다.

증명(일부 스캔 방지). 통신범위에 공통영역을 가진 인접한 두 태그를 인접태그라고 하자. 스캐닝영역을 따

르는 리더는 인접태그의 공통영역의 중앙에 위치하며, 스캐닝영역과 동일한 통신범위를 가진다. 스캐닝영역의 중심점이 인접태그의 공통영역의 중앙에 위치해 있을 때, 이 영역은 인접태그들의 송신범위에 포함된다[그림 4]. 스캐닝영역은 인접태그들의 송신범위에 포함되어 있음으로, 스캐닝 영역을 따르는 리더는 일부 스캔 없이 인접한 두 태그의 응답을 얻을 수 있다. □

주장 2. 스캐닝영역을 따르는 리더는 원거리 스캔없이 인접한 두 태그로부터 올바른 인접태그 정보를 얻을 수 있다.

증명(원거리 스캔 방지). 스캐닝영역은 인접태그들의 송신범위만 포함하며 원거리 태그들의 송신범위는 포함하지 않는다[그림 6]. 그러므로, 스캐닝 영역을 따르는 리더는 원거리 스캔 문제없이 인접한 두 태그의 응답을 얻을 수 있다. □

5.2 스캐닝영역 검증의 정당성

주장 3. 스캐닝영역 감지기법은 스캐닝영역을 확장하여 인접하지 않은 태그들의 응답을 인접태그 정보로 위조하려고 시도하는 리더를 감지한다.

증명. 전송범위를 확장하여 스캐닝영역의 바깥에서 인접한 두 태그를 스캔하는 리더를 생각해보자. 제안기법에서, 스캐닝영역의 바깥쪽 경계면은 외부참조태그의 수신범위로 커버된다[그림 5]. 그러므로, 스캐닝영역의 바깥쪽 경계면에서의 태그스캐닝결과는 외부참조 태그의 응답을 포함하게 된다. 검증자는 외부참조 태그의 응답을 통해 리더가 스캐닝영역 바깥에서 태그스캐닝을 수행한 사실을 감지할 수 있다. □

5.3 효율성

이 절에서는 제안하는 인접태그 정보 획득 기법의 효율성을 보이기 위해, 제안기법의 태그응답 및 태그연산 횟수를 기존에 제안된 요킹증명 분석 프로토콜들의 비용과 비교 분석한다. 기존의 기법들은 인접태그 정보를 획득하기 위한 별도의 방법이 없음으로, 인접한 태그들의 증명생성과 동일한 과정을 통해 인접태그 정보를 획득한다고 가정한다. 이 때 리더는 스캐닝영역에서 증명을 생성하며 인접태그들은 일부스캔과 원거리스캔 문제없이 스캔 되었다고 가정한다.

[표 2]는 제안기법 TPIA와 기존의 요킹증명 기법들의 인접태그 정보 획득 비용을 비교한 결과이다. 인접태그 정보 획득 비용은 태그의 통신횟수와 태그가 증명생성 과정에서 수행해야 하는 연산의 종류와 각 연산수행 횟수로 비교하였다. f, MAC, PRNG, XOR, Shift, Nun은 각각 암호학적 해쉬함수, MAC함수, 의사난수생성기, XOR연산, Shift연산, Lightweigt PRNG[5]를 의미하며, 각 연산들의 f, MAC, PRNG의 수행비용이 XOR, Shift, Nun보다 상대적으로 높다고 가정한다. 암호화와 복호화가 가능한 태그를 사용하는 [12-17]의 기법들은 비용분석에서 제외하였다. TPIA는 기존기법들과 비교했을 때 상대적으로 가장 낮은 수준의 통신횟

표 2. 최초 인접태그 정보 획득을 위한 통신횟수와 계산비용

	Communication	Computation of tags	
		TagA	TagB
Yoking proof[1]	3	1f+1MAC+2shift+1PRNG	1MAC+1shift
Yoking proof using timestamp[2]	2	1MAC	1MAC
Modified proof[3]	3	1MAC+1PRNG	1MAC+1PRNG
Generalized yoking[4]	3	1f+1shift+1MAC	1MAC+1shift
Clumping proof[5]	3	1Nun+2MAC+1XOR+1shift	1Nun+1MAC+1XOR+1shift
Enhanced yoking[6]	2	1PRNG+1MAC	1PRNG+1MAC
Reading order independent GP with readers power[7]	2	1PRNG+1MAC	1PRNG+1MAC
A robust GP for two tags[9]	4	2f+1shift	1f
OVBP[10]	4	1Nun+2PRNG+3XOR+1MAC	1Nun+2PRNG+2XOR+1MAC
Kazahaya[11]	3	14PRNG+12XOR	11PRNG+9XOR
TPIA (인접태그 정보 획득 기법)	1	1MAC	1MAC

f: 암호학적 해쉬함수, MAC: MAC 함수, PRNG: Pseudo Random Number Generator,
XOR: Exclusive or operation, Shift:: Shift operation, Nun: Lightweight PRNG

수와 연산횟수를 요구하는 것을 확인할 수 있다.

제안기법은 기존의 요킹증명 기법들이 지원하지 않는 일부스캔과 원거리 스캔 문제를 감지하기 위해 두 종류의 참조태그들을 사용한다. 그러나 이 참조태그들은 스캔영역이 정의된 후에 스캔영역 주변에 배치되면 반영구적으로 사용되며, 인접태그 정보 획득을 위해 스캔 되어야 하는 태그들의 메모리, 통신횟수, 그리고 연산횟수에 영향을 끼치지 않는다.

Ⅵ. 결 론

이 연구에서 나는 요킹증명 기법을 위한 인접태그 정보 획득 기법인 TPIA을 제안하였다. 제안기법은 인접한 태그들의 위치와 전송범위를 기반으로 정의된 스캐닝영역과, 스캐닝 영역 주변에 배치된 참조태그를 통해 일부스캔 문제와 원거리 스캔 문제가 없는 인접태그 정보 획득을 보장한다. 나는 분석에서 TPIA가 정상적인 인접태그 정보의 획득을 보장하며, 스캐닝영역의 변형과 이탈을 효과적으로 감지할 수 있다는 것을 보였다. 효율성 측면에서 TPIA는 기존의 기법들과 비교했을 때 태그에 추가적인 메시지 전송과 연산을 요구하지 않는다. 이 같은 TPIA의 특성들은 태그인접정보가 필수적인 요킹증명 기법들의 안전한 증명생성을 보장한다. 또한 다양한 산업분야에 요킹증명 기법의 적용을 용이하게 하며, 실시간 물류 추적과 제품 검수의 정확도 향상에 도움을 줄 것으로 기대된다. TPIA는 스캐닝영역을 2차원 평면으로 가정하고 있으나, 실제 환경에서는 태그 쌍, 참조태그, 그리고 리더들의 위치에 고저 차가 존재할 수 있으며, 환경에 따라 제안기법의 성능에 변동이 있을 가능성이 있다. 향후에는 제안기법의 정확한 성능을 분석하고 개선하기 위해, 표준규격의 RFID 장비들을 이용하여 시스템을 구현하고 다양한 관점에서 성능분석을 위한 실험이 수행되어야 할 것이다.

참 고 문 헌

[1] A. Juels, “Yoking proofs for RFID tags,” Proceedings of the 2nd IEEE Annual Conference on Computing and Communication Workshops, pp.138-143, 2008.

[2] J. Saito and K. Sakurai, “Grouping proof for RFID tags,” Proceedings of the 19th International Conference on Advanced Information Networking and Applications, Vol.2, pp.621-624, 2005.

[3] S. Piramuthu, “On existence proofs for multiple RFID tags,” Proceeding of ACS/IEEE International Conference on Pervasive Services, pp.317-320, 2005.

[4] L. Bolotnyy and G. Robins, “Generalized yoking proofs for a group of RFID tags,” Proceeding of the 3rd International Conference on Mobile and Ubiquitous Systems Workshops, pp.1-4, 2006.

[5] P. Peris Lopez, J. C. Hernandez Castro, J. M. Estevez Tapiador, and A. Ribagorda, “Solving the simultaneous scanning problem anonymously: clumping proofs for RFID tags,” Proceedings of the 3rd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, pp.55-60, 2007.

[6] J. S. Cho, S. S. Yeo, S. C. Hwang, S. Y. Rhee, and S. K. Kim, “Enhanced yoking proof protocols for RFID tags and tag groups,” Proceedings of the 22nd International Conference on Advanced Information Networking and Applications Workshops, WAINA08, pp.1591-1596, 2008.

[7] Y. Lien, X. Leng, K. Mayes, and J. Chiu, “Reading order independent grouping proof for RFID tags,” Proceedings of the IEEE International Conference on Intelligence and Security Informatics, pp.128-136, IEEE, 2008.

[8] D. Trçek, “Wireless sensors grouping proofs for medical care and ambient assisted-living deployment,” Sensors, Vol.16, No.1, pp.33, 2016.

[9] M. Burmester, B. Medeiros, and R. Motta, “Provably secure grouping proofs for RFID tags,” Proceedings of the 8th IFIP international

conference on Smart Card Research and Advanced Applications, pp.176-190, Springer Verlag, Berlin, Heidelberg, 2008.

[10] N. Lo and K. Yeh, "Anonymous coexistence proofs for RFID tags," J. Inf. Syst. Edu. Vol.26, No.4, pp.1213-1230, 2010.

[11] P. Peris Lopez, A. Orfila, J. C. Hernandez Castro, Van der Lubbe, and C. A. Jan, "Flaws on RFID grouping-proofs: Guidelines for future sound," J. Netw. Comput. Appl. Vol.34, No.3, pp.833-845, 2011.

[12] C. Ma, J. Lin, Y. Wang, and M. Shang, "Offline RFID grouping proofs with trusted timestamps," Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp.674-681, 2012.

[13] C. L. Chen, C. Y. Wu, F. Y. Leu, and Y. L. Huang, "Using RFID yoking proof to design a supply-chain applications for customs check," IT CoNvergence PRActice (INPRA), Vol.1, No.2, pp.34-53, 2013.

[14] M. H. Yang, J. N. Luo, and Y. Lu, "A novel multi-layered RFID tagged cargo integrity assurance scheme," Sensors, Vol.15, No.10, pp.27087-27115, 2015.

[15] S. Cheng, V. Varadharajan, Y. Mu, and W. Susilo, "An efficient and provably secure RFID grouping proof protocol," In Proceedings of the Australasian Computer Science Week Multiconference (ACSW '17), pp.1-7, 2017.

[16] S. Rostampour, N. Bagheri, M. Hosseinzadeh, and A. Khademzadeh, "An authenticated encryption based grouping proof protocol for RFID systems," Security and Communication Networks, Vol.9, No.18, pp.5581-5590, 2017.

[17] Z. Zhou, P. Liu, Q. Liu, and G. Wang, "An anonymous offline RFID grouping-proof protocol," Future Internet, Vol.10, No.1, pp.1-15, 2018.

저 자 소 개

함 형 민(HyoungMin Ham) 정회원

- 2007년 2월 : 배재대학교 컴퓨터공학과(공학사)
- 2009년 2월 : 한양대학교 컴퓨터공학과(공학석사)
- 2018년 2월 : 연세대학교 컴퓨터과학과(공학박사)
- 2018년 4월 : 충남대학교 핀테크 보안연구소(책임연구원)
- 2019년 8월 ~ 현재 : 배재대학교 사이버보안학과 전임강사

〈관심분야〉 : 정보보안, IoT, 블록체인, 스마트컨트랙트