https://doi.org/10.5392/JKCA.2019.19.09.637

RFID 그룹증명을 위한 응답손실 감지기법

A Tag Response Loss Detection Scheme for RFID Group Proof

함형민
배재대학교 사이버보안학과

Hyoungmin Ham(neoham12@gmail.com)

요약

RFID 그룹증명은 다수의 태그가 동시에 스캔 되었음을 증명하는 요킹증명의 확장이다. 기존의 그룹증명 기법들은 태그응답의 손실을 검증단계에서 감지하는 지연된 태그손실 감지를 지원한다. 그러나 지연된 태그손실 감지는 태그의 손실을 즉각적으로 감지해야 하는 실시간 응용에는 적합하지 못하다. 이 연구에서 나는 태그의 손실을 빠르게 감지하는 새로운 태그응답손실 감지기법인 TRLD(Tag Response Loss Detection)를 제안한다. 제안기법에서 태그는 응답과 함께 시퀀스번호를 전송하며, 리더는 시퀀스번호를 통해 태그를 식별하는 과정 없이 태그응답의 손실을 감지한다. 안전성 분석에서는 메시지 비구별성 실험을 통해, 시퀀스번호가 특정태그와 태그그룹을 구분하려고 시도하는 메시지 분석 공격에 대해 안전하다는 것을 보인다. 효율성 측면에서 제안기법은 어떤 태그의 응답이 손실되었는지 확정하기 위해 기존의 기법보다 더 적은 수의 통신과 데이터베이스 연산을 요구한다.

■ 중심어 : | RFID | 응답손실 감지 | 그룹증명 | 요킹증명 | 비구별성 |

Abstract

The RFID group proof is an extension of the yoking proof proving that multiple tags are scanned by a reader simultaneously. Existing group proof schemes provide only delayed tag loss detection which detects loss of tag response in a verification phase. However, delayed tag loss detection is not suitable for real-time applications where tag loss must be detected immediately. In this study, I propose a tag response loss detection scheme which detects loss of tag response in the proof generation process quickly. In the proposed scheme, the tag responds with the sequence number assigned to the tag group, and the reader detects the loss of the tag response through the sequence number. Through an experiment for indistinguishability, I show that the sequence number is secure against an analyzing message attack to distinguish between specific tags and tag groups. In terms of efficiency, the proposed scheme requires fewer transmissions and database operations than existing techniques to determine which tags response is lost.

■ keyword : | RFID | Tag Response Loss Detection | Group Proof | Yoking Proof | Indistinguishability |

I. 서 론

RFID 그룹증명은 다수의 태그들이 동시에 스캔 되었음을 증명하는 RFID 요킹증명의 확장이다. RFID 그룹증명은 로컬에서 태그들의 물리적 인접성을 검사하는 여러 응용에 적용될 수 있다. 예를 들어, 다수의 제품

접수일자 : 2019년 08월 04일
수정일자 : 2019년 09월 23일
심사완료일 : 2019년 09월 23일
교신저자 : 함형민, e-mail : neoham12@gmail.com

상자들을 하나의 컨테이너 박스에 넣고 다른 장소로 이동해야 하는 경우, 그룹증명을 이용하여 출발지, 경유지, 목적지에서 콘테이너 박스를 열지 않고 제품 상자들과 내용물을 검사할 수 있다.

그룹증명 프로토콜은 리더가 인접한 태그들을 스캔하는 증명생성과 스캔 결과를 사전정보와 비교하는 검증의 두 단계로 구성된다. 증명생성 단계에서 리더는 태그에게 질의 메시지를 브로드캐스트하고, 태그는 질의 메시지를 받아 무선으로 응답한다. 이 과정에서 태그의 응답이 리더에 전송되는 되지 못하는 태그응답손실이 발생하면, 요킹증명은 검증에 실패하게 된다.

기존의 그룹증명 기법들은 증명이 검증에 실패했을 때 태그응답손실을 감지할 수 있다. 그러나 이처럼 검증과정에서 태그응답손실을 감지하는 지연된 태그응답손실 감지는 객체의 상태변화를 즉각적으로 감지해야 하는 실시간 응용에는 적합하지 않다.

이 연구에서 나는 그룹증명 기법을 위한 빠른 태그응답손실 감지기법을 제안한다. 제안하는 태그응답손실 감지기법은 태그그룹 단위의 시퀀스번호를 활용하여 증명생성 중에 태그응답손실을 감지한다. 제안기법은 기존의 요킹증명 기법들에 적용되어 동작하며 태그의 응답에 시퀀스번호를 포함하는 것 외에 태그에 추가적인 연산을 요구하지 않는다.

나는 특정 그룹에 속한 태그들을 찾을 목적으로 태그응답의 분석을 시도하는 공격자와 태그응답의 비구별성 실험을 정의하고, 이들을 이용하여 제안기법의 안전성을 보인다. 좀 더 구체적으로, 특정 그룹에 속한 태그들을 찾을 목적으로 태그응답의 분석을 시도하는 공격자에게, 시퀀스번호가 주는 정보가 무시할 만 하다는 것을 보이기 위해, 3절에서 공격모델과 비구별성 실험을 정의하고, 5절에서 시퀀스번호의 비구별성을 검증한다. 실험결과는 특정태그와 태그가 속한 그룹을 알아내기 위해 태그응답의 분석을 시도하는 공격자가 시퀀스번호를 통해 얻을 수 있는 정보가 무시할 만 하다는 것을 보여준다.

효율성 측면에서, 제안기법은 태그의 응답메시지에 포함된 시퀀스번호를 제외하고 추가적인 연산을 요구하지 않으며, 기존의 기법들과 동일한 데이터베이스 검색비용과, 더 적은 수의 인증메시지 생성을 요구한다.

논문의 구성은 다음과 같다. 우선 2절에서 태그손실 감지에 관한 문제를 정의하고, 3절에서 태그응답 메시지의 비구별성을 공격하는 공격자 모델을 제시한 다음, 4절에서 배경지식과 관련 연구를 살펴본다. 5절에서 빠른 손실태그 감지기법인 TRLD를 제안하고, 5절에서 해당 기법의 안전성과 효율성을 보인다. 마지막으로 6절에서 결론과 향후 연구를 언급하고 끝을 맺는다.

II. 문제정의

지연된 태그응답손실의 감지. 기존의 그룹증명 기법들은 태그그룹을 스캔하여 증명을 생성하는 과정이 끝난 후에, 검증과정에서 재고의 손실을 감지하고, 손실된 태그를 확인할 수 있다. 그러나 이 같은 지연된 손실감지는 태그의 손실을 즉각적으로 감지해야 하는 실시간 응용에는 적합하지 못하다. 예를 들어, 도난방지를 목적으로 하는 응용에서 일부 물품이 손실되었을 경우, 이 같은 사실은 최대한 빨리 감지되어야 한다. 그러나 기존의 그룹증명 기법들은 증명생성 과정에서 일부 물품의 손실로 인해 잘못된 그룹증명이 생성되고, 검증과정에서 해당 증명이 검증에 실패한 후에 물품의 손실을 감지할 수 있다.

손실된 태그의 확인. 태그응답손실이 감지되면, 어떤 태그그룹에 속한 어떤 태그가 손실되었는지 확인이 필요하다. 예를 들어, 운송 차량에 적재된 물품을 추적하기 위해 그룹증명이 적용된 경우를 생각해 보자. 재고의 손실을 감지했다면 어떤 운송 차량에서 어떤 물품이 손실되었는지 파악해야 한다.

III. 배경지식 및 관련연구

3.1 요킹증명

A. Juels는 [1]에서 기본적인 yoking proof 프로토콜을 제안했다. 기본 요킹증명 프로토콜에서 RFID 리더는 한 태그의 응답을 다른 태그에 대한 챌린지로 사용하여 두 태그를 모두 증명에 포함 시킨다. 이 과정에서 안전한 증명생성 및 검증을 보장하기 위해 비밀키와

시간초과 기능을 사용한다. 이 기법에서 각 태그는 신뢰할 수 있는 검증자와 고유한 비밀키를 공유하며, 이 비밀키를 포함하여 증명을 생성한다. 이로 인해 이 비밀키를 모르는 공격자는 증명을 생성할 수 없다. 여기에 더해, 이 프로토콜은 두 개의 응답이 함께 스캔되었다는 것을 보장하기 위해 세션 시간을 제한하는 타임아웃을 사용했다. 타임아웃이 발생하면 태그는 현재 세션을 종료한다.

3.2 그룹증명

그룹증명은 한 쌍 이상의 태그들이 동시에 스캔 되었다는 것을 증명하는 요킹증명의 확장이다. 현재까지 제안된 그룹증명 기법 중 일부는 다수의 태그로부터 안전한 증명을 생성하기 위해 추가적인 장치를 사용한다. Saito와 Sakurai는 [2]에서 Juels의 기법이 재생공격에 대해 올바른 증거를 생성할 수 없다고 지적하고, 재생공격을 방지하기 위해 타임스탬프를 사용하는 기법을 제안했다. 여기에 더해 그들은 그루핑증명(Grouping proof)이라고 부르는, 한 쌍 이상의 태그들을 위한 확장된 요킹증명 프로토콜을 제안하였다. 이 기법은 태그들을 대신하여 타임스탬프를 발급하고 응답메시지를 암호화하는 팔레트 태그 (Pallet tag)라는 추가장치를 사용한다. 이 기법은 검증과정에서 인접한 태그에 대한 사전정보를 사용하지 않으며. 이 때문에 태그그룹에 속한 일부 태그의 응답이 손실되어도 이 사실을 감지할 수 없다.

Bolotnyy 등은 [4]에서 Juels의 기법을 그룹증명으로 확장하였으며, 추가적으로 태그의 익명성을 고려한 기법을 제안하였다. 그러나 이 기법은 검증과정에서 인접한 태그에 대한 사전정보를 사용하지 않으며, 이 때문에 태그그룹에 속한 일부 태그의 응답이 손실되어도 이 사실을 감지할 수 없다.

Cho 등은 [5]에서 Piramuthu의 기법[3]을 수정하여 전수공격에 강한 저항성을 가지는 요킹증명 기법을 제안하고, 이 기법을 그룹증명으로 확장하였다. 이 기법은 태그에 추가적인 부담을 주지 않으면서 전수공격에 대한 저항성과 그룹증명으로의 확장을 지원한다. 이 기법은 검증과정에서 인접한 태그에 대한 사전정보를 사용하지 않기 때문에 태그의 응답손실을 감지할 수 없다.

Chien 등은 [6]에서 트리기반 매칭 RFID 요킹증명 기법을 제안했다. 이 기법은 태그를 스캔하는 프로세스에서 유효한 증명을 얻기 위해 미리 태그를 그룹화하고, 이 정보를 이용해 스캐닝 결과의 불필요한 데이터를 필터링한다. 이 기법에서는 빠른 식별을 위해 비밀키, ID, 그룹키, 그룹 ID, 트리상의 경로 정보 및 시퀀스 번호 같은 사전지식들을 이진트리에 저장한다. 이 트리 안에 저장된 태그의 식별정보는 상수시간 검색이 보장된다. 증명생성 과정에서, 검증자는 암호화 된 타임스탬프를 생성하여 그것을 판독기에 전송하고, 리더는 암호화 된 타임스탬프를 태그들에게 브로드캐스트한다. 그다음 타임스탬프를 수신한 태그는 응답메시지를 생성하기 위해 해시 함수를 네 번 실행하고 PRNG를 한 번 실행한다. 증명 생성 프로세스 중에 리더는 총 세 번의 태그 스캐닝을 수행하며, 그룹 ID, Tag type ID, 그리고 태그 ID를 그룹 내의 모든 태그에게 전송한다. 이 정보들은 증명을 검증하기 위해 필요한 데이터베이스 검색시간을 감소하기 위해 필요하다. 하지만 트리기반 방식은 증명생성에 참여하는 태그의 수에 비례해서 전송해야 할 메시지의 수가 늘어나므로, 한 그룹에 포함된 태그의 수가 일정 수준 이상으로 증가하게 되면 효율이 크게 저하된다.

Lien 등은 [7]에서 [2]의 기법을 수정하여 팔레트 태그를 사용하는 개선된 그룹증명 프로토콜을 제안했다. 이 기법에서 검증자는 태그들이 스캔되는 순서에 상관없이 증명을 검증할 수 있으며, 이로 인해 더 빠른 증명 생성과 검증이 가능하다. 이 기법은 재전송공격과 증명 위조 공격에 안전하지만, 태그와 검증자가 동일한 난수를 생성하기 위해 동기화가 필요하다. 이 기법은 검증과정에서 인접한 태그에 대한 사전정보를 사용하지 않기 때문에 태그그룹에 속한 일부 태그의 응답이 손실되어도 이 사실을 감지할 수 없다.

Brumester 등은 [8]에서 전방향 안전성을 지원하는 요킹증명 기법을 제안하였다. 이 기법은 한 쌍의 태그에 대한 요킹증명의 생성과 검증만을 지원한다. 하지만 이 기법에서는 사전에 인접한 태그들에게 그룹키를 할당하고 검증자가 인접한 태그에 대한 정보를 유지하고 있으므로, 해당기법을 그룹증명 기법으로 확장할 수 있다. 이 기법은 비동기 상태에서 재전송공격에 취약하며,

태그위장과 증명위조 공격에도 안전하지 않다.

Lo등은 [9]에서 그룹증명 지원하는 Online verifier based protocol(OVBP)를 제안하였다. 이 기법에서 리더는 수신한 태그의 응답을 검증자에게 보내고, 검증자는 수신한 태그의 응답과 타임스탬프를 포함하는 해쉬값을 리더에게 송신한다. 리더는 이 값을 다시 태그에게 보내고 수신한 응답을 질의메시지와 함께 다음 태그에게 송신한다. 이 기법은 검증과정에서 인접한 태그에 대한 사전정보를 사용하지 않기 때문에 태그그룹에 속한 일부태그의 응답손실을 감지할 수 없다.

[10]에서 Lopez 등은 기존기법들의 보안 및 프라이버시 문제를 보이고, 그룹증명 프로토콜을 위한 보안지침을 제안했다. 그리고 자신들이 제안한 보안지침을 준수하며 EPCglobal Gen-2 표준에 부합하는 새로운 그룹증명 기법인 Kazahaya 프로토콜을 제안하였다. 이 기법은 초기화 단계에서, 태그를 그룹화하고 비밀 키, ID, 그룹 키 및 그룹 ID를 태그에 할당한 다음, 태그그룹과 할당된 정보들을 백앤드 데이터베이스(back-end database)에 저장한다. 증명생성 단계에서 검증자는 암호화된 타임스탬프를 생성하고, 리더는 암호화된 타임스탬프를 요청 메시지와 함께 브로드캐스트한다. 이 타임스탬프를 수신한 태그들은 리더에 응답하고 리더는 이 응답을 그룹 내의 다른 태그들에 전달한다. 태그들은 그룹 키 및 그룹 ID를 통해 전달받은 응답 메시지를 인증한다. 증명생성이 끝난 후에 증명생성 프로세스의 경과 시간은 암호화된 타임스탬프를 사용하여 검증된다. kazahaya는 메시지 인증과 암호화된 타임스탬프를 통해 증명위조 공격에 안전하지만 태그에게 많은 연산을 요구한다. 좀 더 구체적으로, 증명생성을 위해 리더가 태그를 세 번 스캔하는 동안, 태그는 응답하기 위해 의사 난수 생성기를 14회 실행한다. 이 기법에서 검증자는 그룹키를 통해 인접한 태그들의 그룹을 알 수 있으며, 이 정보를 활용하여, 태그그룹에서 발생한 태그 응답손실을 감지할 수 있다.

[11]에서 Yang 등은 물류 관리에서 다중 리더를 사용하는 그룹 증명 프로토콜을 제안했다. 이 기법에서는 여러 리더들의 스캐닝 결과를 조합하여 하나의 그룹화 증명을 생성하며, 이 증명생성 과정을 "다중계층-리더 그룹증명(Multi-layered readers group proof)이라고 한다. 이 기법은 시계태그라는 추가장비를 사용하여 타임스탬프 값을 생성하고 암호화한다. 증명생성 단계에서 시계태그는 타임스탬프를 생성하고 이를 검증자와 공유하고 있는 비밀키로 암호화한다. 검증자는 암호화 된 타임스탬프를 통해 증명의 유효성을 확인할 수 있다. 이 기법은 DoP 공격(Denial of Proof attack), 재생공격, 태그위장에 대한 보안을 제공한다. 또한 검증과정에서 인접한 태그에 대한 사전정보를 사용하여, 태그응답손실을 감지할 수 있다. 그러나 이 기법은 키 그룹화 코드를 포함한 추가적인 사전지식이 필요하며, 태그가 메시지 암호화, 해시, MAC, 그리고 PRNG 연산을 수행해야 한다.

Ⅳ. 공격모델

이 절에서는 제안기법의 안전성을 평가하기 위해 태그응답의 비구별성 실험을 정의한다. 나는 태그응답의 비구별성을 다음과 같이 정의한다.

- 비구별성 (Un-distinguishability): 하나의 태그가 생성한 한 개 이상의 메시지들의 집합을 부분집합으로 가지는 전체 태그의 메시지 집합이 있다. 이 집합에서 무작위로 하나의 메시지를 선택한 다음, 이 메시지와 같은 부분집합에 속하는 다른 메시지를 찾을 수 없다면, 이 태그의 메시지는 비구별성을 만족한다.

공격자모델. 태그응답의 비구별성 실험에서 공격자는 리더와 태그 사이의 통신을 도청할 수 있으며, 태그에 질의 메시지를 전송하고, 응답을 얻을 수 있다. 공격시간은 전수공격을 통해 태그의 비밀값을 알아낼 수 있는 시간보다 작다고 가정하며, 태그를 물리적으로 손상시키거나 직접 탈취하는 공격은 고려하지 않는다.

준비단계. 다수의 태그가 포함된 태그집합으로부터 전체 태그의 메시지 집합이 생성된다. 공격자는 전체 태그의 메시지 집합을 생성한 태그집합을 공격대상으로 한다. 공격자의 목적은 전체 태그의 메시지 집합을 분석하여, 특정 태그그룹에 속한 태그의 응답을 구분하는 것이다. 준비단계에서, 공격자는 주어진 시간 동안 자신의 능력을 활용하여 공격에 필요한 정보를 수집한

다.

공격단계. 준비단계가 끝나면, 공격자는 전체 태그의 메시지 집합으로부터 무작위로 하나의 메시지를 선택한다. 이 단계에서, 공격자는 주어진 시간 동안 자신의 능력을 활용하여 선택한 메시지와 같은 부분집합에 속하는 다른 메시지를 찾는다. 즉, 자신이 선택한 메시지를 생성했던 태그가 새로 생성한 메시지를 찾기 위해 시도한다.

주어진 시간이 끝나면 공격자는 최종적으로 한 쌍의 메시지를 선택한다. 이 메시지 쌍이 동일한 부분집합에 속한다면 (즉, 같은 태그에 의해 생성되었다면) 공격은 성공한다. 반대로 이 메시지 쌍이 동일한 부분집합에 속하지 않으면 공격은 실패한다.

Ⅴ. 제안기법

이 절에서 나는 새로운 태그응답손실 감지기법인 Tag Response Loss Detection (TRLD)를 제안한다. TRLD는 기존의 그룹증명 기법에 적용되어 태그응답의 손실감지를 지원하며, 태그의 응답과 함께 전송되는 시퀀스번호의 손실을 확인하는 것으로 태그응답의 손실을 감지한다. 이 과정은 리더가 검증자에게 증명을 제출하기 직전에 수행되며, 태그응답의 손실을 보고받은 검증자는 데이터베이스에서 태그응답이 손실된 태그그룹을 검색하고 응답이 손실된 태그를 확인한다.

[그림 1]과 [그림 2]는 각각 제안하는 기법과 기존의 그룹증명 기법들의 지연된 태그응답손실 감지과정을 나타낸다. 제안기법에서 태그응답손실은 태그스캐닝 중에 리더에 의해 즉각 감지된다. 그에 반해, 기존의 그룹증명 기법들에서 태그응답손실은 태그스캐닝과 증명의 검증이 끝난 다음에 감지되며, 이로 인해 태그손실을 감지하기까지 제안기법에 비해 상대적으로 더 긴 지연이 발생한다.

초기설정. 태그들은 그룹 단위로 시퀀스넘버를 부여받는다. 태그들은 시퀀스넘버에 따라 순차적으로 응답한다. 모든 태그그룹들은 같은 수의 태그로 구성된다. 리더는 그룹 내의 태그의 수를 알고 있다.

같은 태그그룹에 속한 태그들의 사전정보는 시퀀스넘버가 1인 태그와 그 외의 태그들의 링크드 리스트 형태로 데이터베이스에 저장된다. [그림 3]은 태그들의 사전정보를 링크드 리스트 구조로 저장한 데이터베이스 엔트리의 예시이다. 시퀀스넘버가 1인 태그의 사전정보와 그 외의 태그들의 사전정보는 각각 테이블 1과 테이블 2에 저장되어 있으며, 테이블 1의 포인터는 테이블 2에 저장된 엔트리 중에서 자신과 같은 태그그룹인 태그들의 엔트리와 연결되어 있다.

응답손실 감지. 제안기법에서 응답손실 감지 단계는 증명생성이 완료된 시점에 리더에 의해 수행된다. 응답손실 감지 단계가 수행되는 과정은 다음과 같다.

1. 리더는 태그들에게 질의 메시지를 브로드캐스트한다.
2. 리더의 질의를 받은 태그들은 증명과 시퀀스번호로 응답한다.
3. (응답손실 검사) 리더는 수신한 시퀀스번호를 확인한다. 모든 시퀀스번호가 수신되었다면, 증명을 생

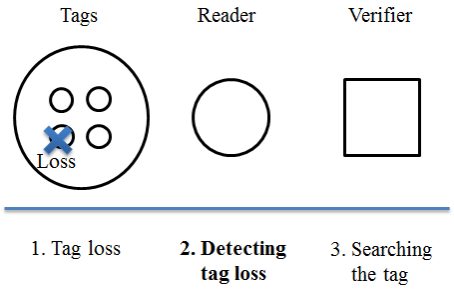

그림 1. 제안기법의 태그응답손실 감지 과정

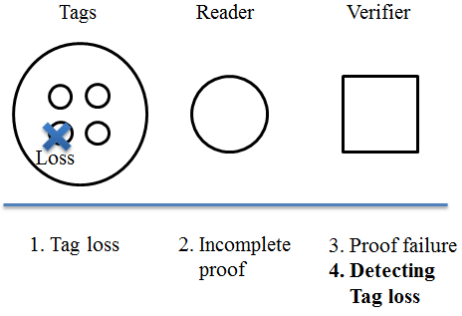

그림 2. 기존 그룹증명 기법들의 지연된 태그응답손실 감지 과정

성한다. 수신되지 않은 시퀀스넘버가 있다면, 수신된 시퀀스번호들, 태그그룹의 응답들, 그리고 태그손실 알림을 검증자에게 전송한다. (현재 스캔중인 태그 중에 초기태그가 있다면, 수신된 시퀀스번호, 초기태그의 응답, 그리고 태그손실 알림을 검증자에게 전송한다.)

태그그룹 검색. 제안기법에서 태그그룹 검색 단계는 검증자가 응답손실 알림을 수신했을 때 수행된다. 태그그룹 검색 단계가 수행되는 과정은 다음과 같다.

4. (태그그룹 검색) 검증자는 태그손실 알림을 통해 태그응답의 손실을 감지한다. 검증자는 태그손실이 발생한 그룹을 알아내기 위해, 데이터베이스에 저장된 태그의 사전정보를 이용해 수신된 태그의 응답과 동일한 방법으로 인증메시지를 생성하고, 이를 수신된 태그의 응답과 비교한다. 이 과정은 수신된 태그의 응답과 동일한 인증메시지를 찾을 때까지 반복한다. 수신된 태그의 응답과 동일한 메시지가 생성되었다면, 태그그룹 검색이 완료된다. 동일한 메시지를 찾지 못했다면, 검색을 종료한다.

손실태그 확인. 태그그룹 검색단계가 끝나면 데이터베이스에 저장된 시퀀스 번호와 수신된 시퀀스 번호를 비교하여 어떤 태그의 응답이 손실되었는지 확인한다. 손실태그 확인 단계가 수행되는 과정은 다음과 같다.

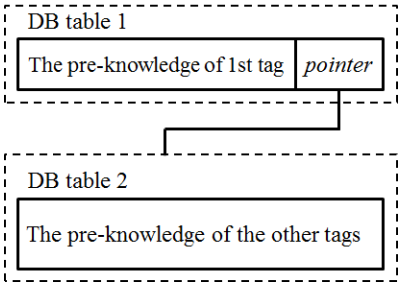

그림 3. 데이터베이스 테이블 엔트리

5. 태그그룹 검색을 통해 태그그룹에 속한 태그들의 사전정보를 얻은 후에, 사전정보에 포함된 태그들의 시퀀스 번호와 수신된 시퀀스번호들을 비교하고 손실된 시퀀스번호를 찾는다. 비교대상이 없는 시퀀스번호에 해당하는 태그는 손실태그로 확인된다.

Ⅵ. 분석

6.1 안전성

비구별성. 기존 그룹증명 기법들은 공격자가 메시지 분석을 통해 특정태그와 태그그룹을 구분할 수 없도록 암호학적 연산을 통해 태그의 응답메시지를 보호한다. 태그의 응답메시지와 함께 기존에 없던 정보를 포함하여 전송하면, 이 정보를 통해 새로운 취약점이 발생할 가능성이 있다. 나는 3절의 공격모델을 통해 제안기법에서 사용하는 시퀀스번호가 비구별성을 만족하는 것을 보이고, 이를 통해 제안기법이 특정태그와 태그그룹을 구분하려는 공격에 대해 안전하다는 것을 보인다.

정리. 태그그룹의 수가 하나 이상일 때, 응답 메시지에 포함된 시퀀스번호는 비구별성을 만족한다.

증명. 같은 수의 태그를 포함하는 두 개의 태그그룹 TA와 TB가 있고, 태그들이 시퀀스번호로 응답한다고 가정하자. TA와 TB를 스캔하면, 서로 동일한 시퀀스번호의 집합 ScanA와 ScanB를 얻을 수 있다. ScanA와 ScanB를 합친 결과를 ScanAB라고 하자.

우선 공격자는 ScanAB중에서 무작위로 한 태그의 응답 Seqx을 선택한다. 이 태그가 속한 태그그룹을 TGA, 다른 태그그룹을 TGB 라고 하자.

이제 공격자는 두 개의 태그그룹을 새로 스캔한 결과 ReScanAB에서, TGA에 속한 태그의 응답 Seqx를 다시 선택해야 한다. 선택한 Seqx가 TGA에 속한다면 공격은 성공한다. 그러나, 공격자는 시퀀스번호의 모임인 ScanAB와 ReScanAB로부터 Seqx가 TGA에 속해 있는지 여부를 확인할 수 없다. 그러므로, 시퀀스번호는 비구별성을 만족한다. □

그 외의 공격들. 그룹증명의 안전성을 위협하는 다양한 공격들이 존재한다. 기존에 알려진 그룹증명의 안전성을 위협하는 공격들은 공격목적에 따라 태그위장과 증명위조로 분류될 수 있다. 여기서 태그위장은 태그의 응답을 위조하는 공격들을 의미하며, 재전송공격이 가능한 기법들[2][3][8][9]은 태그위장 공격에 대해 안전하지 않다. 증명위조는 인접하지 않은 태그들의 그룹증명을 생성하는 공격을 의미하며, 인접한 태그들에 대한 사전지식을 활용하지 않는 기법들[2][3][5]은 증명위조 공격에 취약하다. [표 1]은 제안기법을 적용하기 전과

후에 태그위장과 증명위조에 대한 그룹증명 기법들의 안전성을 비교한 것이다. 태그위장과 증명위조에 해당하는 공격들은 [2][3][8][10][12]를 참고하였으며, 공격자의 능력은 앞서 3절에서 정의된 공격자모델을 따른다. 4.1절에서 언급한 것처럼, 제안기법에서 태그들이 전송하는 카운터 값은 비구별성을 만족하므로 제안기법을 기존기법들에 적용하기 전과 후의 안전성에 차이가 없는 것을 확인하였다.

6.2 효율성

이 절에서는 태그응답손실 감지를 위한 태그그룹 감지, 태그그룹 검색, 그리고 태그그룹 인증 비용을 분석한다. [표 2]는 제안기법과 기존의 그룹증명 기법들의 손실태그 감지 비용을 비교한 결과이다. 여기서 분석대상들의 데이터베이스는 4절에서 소개한 제안기법의 데이터베이스와 동일한 링크드리스트 구조라고 가정하며, 태그그룹의 태그 중 한 태그의 응답이 손실된 경우를 고려하였다. 한 태그그룹의 증명생성 과정을 고려하며, 그룹 내의 태그 중 가장 먼저 응답하는 초기태그가 필수적인 기법들[2][3][5][9]과의 비교를 위해서, 초기태그가 손실된 경우는 고려하지 않는다. 분석결과는 제안기법이 적용된 경우가 기존기법들 단독으로 수행되는 경우보다 더 효율적이라는 것을 보여준다. 제안기법은 손실태그 감지를 위해 기존의 그룹증명 기법들보다 더 적은 통신횟수와 인증메시지 생성 횟수를 요구하며, 특히 손실태그 확인 단계에서 태그응답을 인증하는 과정이 필요하지 않다.

Ⅶ.결 론

이 연구에서 나는 그룹증명 기법을 위한 빠른 태그응답손실 감지기법인 TRLD를 제안하였다. 제안기법은 태그그룹에 부여된 시퀀스번호를 활용하여 증명생성 단계에서 태그응답의 손실을 감지하며, 이것은 증명생성 단계가 끝나고 검증과정에서 태그응답의 손실을 감지할 수 있었던 기존의 기법들보다 더 빠른 태그손실 감지를 가능하게 한다. 제안기법은 태그의 응답메시지에 시퀀스번호를 함께 전송하는 것을 제외하면, 태그에 추가적인 연산이나 메시지 전송을 요구하지 않는다. 나는 제안기법의 안전성을 보이기 위해, 메시지 비구별성 실험을 제안하고, 추가된 시퀀스번호가 특정태그와 태

표 1. 그룹증명 기법들의 안전성 (TRLD 적용 전과 적용 후)

	태그위장 공격		증명위조 공격	
	제안기법 미적용	제안기법 적용	제안기법 미적용	제안기법 적용
Grouping proof[2]	X	X	X	X
Generalized yoking[4]	X	X	X	X
Enhanced yoking[5]	O	O	X	X
Tree-based matched yoking proof[6]	O	O	O	O
Reading order independent GP with pallet tag[7]	O	O	O	O
A robust GP for two tags[8]	X	X	X	X
OVBP[9]	X	X	X	X
Kazahaya[10]	O	O	O	O

O: 안전 X: 공격가능

표 2. 손실태그 확인 비용

	응답손실감지 (리더/태그의 통신횟수)		태그검색 (태그응답 인증횟수)		손실태그 확인 (태그응답 인증횟수)	
	제안기법 미적용	제안기법 적용	제안기법 미적용	제안기법 적용	제안기법 미적용	제안기법 적용
Grouping proof[2]	2	1	O(n-1)	O(n-1)	O(TG-1)	-
Generalized yoking[4]	TG	2	O(n-1)	O(n-1)	O(TG-1)	-
Enhanced yoking proof for tag group [5]	3	2	O(n-1)	O(n-1)	O(TG-1)	-
Reading order independent GP with pallet tag[7]	4	1	O(n-1)	O(n-1)	O(TG-1)	-
OVBP[9]	TG	2	O(n-1)	O(n-1)	O(TG-1)	-
Kazahaya[10]	TG	2	O(n-1)	O(n-1)	O(TG-1)	-

n: 태그그룹의 총 수, TG: 한 그룹안의 태그 수

그그룹을 구분하려는 공격에 안전한 것을 보였다. 효율성 측면에서, 제안기법을 기존기법에 적용한 경우가 기존기법들을 단독으로 사용한 경우보다 더 빠르게 태그 손실을 감지하며, 기존기법들과 동등한 데이터베이스 검색비용과 더 적은 계산비용을 요구한다. TRLD는 기존의 그룹증명 연구에서 고려하지 않았던 태그응답 손실에 대한 효과적인 대응책이며, 향후 태그응답 손실을 고려한 다른 그룹증명 연구에 활용될 수 있을 것으로 기대된다. TRLD는 태그 그룹 단위의 시퀀스번호를 태그와 데이터베이스에 유지하는 것으로 기존의 그룹증명 기법들에 비교적 손쉽게 적용 가능하며, 이 같은 확장성은 그룹증명이 다양한 산업 분야에서 활용될 가능성을 높여준다. TRLD는 현재까지 제안된 그룹증명 기법들 대부분에 적용 가능한 것을 확인하였으나, 태그에 공개키 기반 암호화 연산을 요구하는 일부 기법들에 대한 적용은 추가적인 연구가 필요하다. 향후에는 제안기법을 공개키 기반 암호화 연산을 사용하는 그룹증명 기법들에 적용하고 그룹증명 생성에 미치는 영향을 추가로 분석할 필요가 있다.

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] 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, WAINA'08, pp.1591-1596, 2008.

[6] H. Chien, "Tree-Based Matched RFID Yoking Making It More Practical and Efficient," International Journal of Computer Network and Information Security, Vol.1, pp.1-8, 2009.

[7] Y. Lien, X. Leng, K. Mayes, 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] 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.

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

[10] 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.

[11] 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.

[12] 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," Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, pp.55-60, 2007.

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 핀테크보안연구소(책임연구원)
- 2019년 8월 ~ 현재 : 배재대학교 사이버보안학과 전임강사

〈관심분야〉 : 정보보안, IoT, 블록체인, 스마트컨트랙트