EPCglobal Class1 Generation2를 위한 프라이버시 보호 에이전트†

신재동*, 여상수**, 김성권*

*중앙대학교 컴퓨터공학부 , **단국대학교 정보컴퓨터학부

Privacy Protection Agent for EPCglobal Class1 Generation2

Jae-dong Shin*, Sang-Soo Yeo**, Sung Kwon Kim*

*School of Computer Science and Engineering, Chung-Ang University

**School of Information and Computer Science, Dankook University

요 약

RFID(Radio Frequency IDentification) 기술은 리더(reader)가 RF 신호를 사용하여 물품에 부착된 전자 태그(tag)를 식별하는 비접촉 자동인식 기술이다. 그런데 여기에는 RFID 사용자의 프라이버시 보호라는 큰 문제가 존재한다. 이 문제를 해결하기 위하여 현재까지 제안되었던 보안 기법들은 태그와 리더 사이에 암호학적 기법에 중점을 두었다. 하지만, 본 논문에서는 복잡한 암호학적 기법이 아닌 개인 모바일 기기(mobile device)를 제안한다. 이것은 보호되고 있는 태그를 리더가 읽으려 할 때 태그 인식 과정에 관여하여 정당한 리더만이 태그들을 읽을 수 있도록 한다.

I. 서론

RFID(Radio Frequency Identification) 기술은 RF 신호를 사용하여 물품에 부착된 전자 태그를 식별하는 비접촉 기술이다. 이러한 RFID 기술의 확산을 위해서는 태그의 저가격, 저전력, 초소형화 문제, 태그 식별자의 코드 표준화 문제, 다중 태그 식별 문제, 그리고 보안 및 프라이버시 문제 등의 난제들을 해결해야 한다. 이 중에서 특히 프라이버시 문제는 RFID 태그가 인증 프로토콜을 거치지 않고 어떤 리더에게나 태그의 고유한 식별 값(ID)을 응답해주는 데서 기인한다. 프라이버시 문제는 크게 정보 유출과 위치 추적 두 가지로 분류할 수 있다.

첫째, 정보 유출(information leakage)은 태그의 ID가 리더를 가진 아무에게나 읽히므로 개인이 소지하고 있는 물품이 드러나는 것이다. 소지한 물품은 그 사람의 생활환경, 소득수준, 소비경향, 신체조건 등을 반영하기 때문에 태그의 정보 유출로 인한 프라이버시 침해는 상당하다고 보아야 할 것이다[1].

둘째, 위치 추적(location tracking)은 태그가 항상 같은 ID를 송신하는 데서 오는 문제이다. 이로 인해 공격자는 리더를 사용하여 태그 소유자의 위치를 추적할 수 있다. 이런 태그 소유자의 위치 추적, 이동 경로 파악 또한 심각한 프라이버시 침해로 보아야 한다[2].

본 논문에서는 모바일 기기를 사용하여 프라이버시 보호를 하는 기법을 제안한다. 기존의 저가형 태그들은 낮은 연산 능력과 작은 기억용량, 전력 등이 한계가 될 수밖에 없다. 그래서 이런 저가형 태그들을 보호하기 위하여 모바일 기기를 사용하며 이를 통해 좀 더 높은 수준의 작업을 가능하게 한다.

한편, 제안하는 기법에서 태그 인식 프로토콜(singulation protocol)은 18000-6 Type C가 되

† 본 연구는 한국과학재단 특정기초연구 (R01-2005-000-10568-0) 지원으로 수행되었음.

는 EPC Class1 Generation2로 한다. 이것은 현재 RFID 시장에서 가장 많이 사용 될 것으로 예상되는 표준이다.

II. 관련연구

RFID 보안 관련 프로토콜들 중에서 본 논문의 제안 프로토콜과 관련이 있는 연구는 아래의 3가지가 있다.

1. 블로커 태그

블로커(blocker) 태그는 일반 태그를 보호하기 위해 일종의 방어막을 치는 기법이다[3,4]. 여기서는 태그 인식 프로토콜 중 하나인 트리 워킹 프로토콜을 역이용한다. 블로커 태그는 리더의 모든 질의에 응답할 때 항상 0과 1을 모두 대답한다. 모든 질의에 이런 응답을 하기 때문에 리더가 태그를 구분해 낼 수 없게 된다. 결국, 특정 태그의 존재 여부를 숨기고, 리더가 중도에 태그 인식을 포기하게 한다. 하지만, 이 기법은 정상적인 태그도 못 읽게 하는 단점이 있다.

2. 모바일 기기 기법

프라이버시 보호를 위하여 태그와 리더 이외에 모바일 기기를 사용하여 통신을 중재하는 기법도 있다[5]. 모바일 기기는 기존의 보안 기술을 그대로 적용할 수 있고 태그가 가지기 어려운 능력을 갖출 수 있다. 예를 들어 이런 기기는 새로운 태그나 새로운 리더를 감시하는 역할을 하거나 태그를 대신하는 역할을 한다. 또는 태그를 대신하여 리더가 정당한 리더인지 인증해주는 역할도 한다. 여기에서 모바일 기기는 PDA나 휴대폰이 될 수 있다. 최근에는 RFID 리더가 내장된 휴대폰도 개발이 되어 시판을 앞두고 있다[6]. 그러나 이 방법은 보통 기존 표준들을 많이 변경하거나 새로 만들어야 하는 한계가 있다.

3. 백워드 채널 보호 기법

백워드 채널(backward channel) 보호 기법은 태그가 리더에게 자신의 ID를 보내는 과정에서 ID의 노출을 막는 데 목적이 있다. 이 기법은 그림 1과 같이 태그의 ID 전송 과정에 리더 자신도 랜덤하게 생성한 ID(RID)를 전송한다. 이때, 태그가 전송하는 ID의 비트 타이밍과 리더가 전송하는 RID는 동기화되어 있다고 가정한다. 이와 같은 경우, 일치하지 않는 비트 값들은 충돌이 발생한다. 따라서 도청자는 실제 태그 ID를 인식하기 어려워진다[7].

그러나 리더는 충돌이 일어난 태그 ID의 모든 비트를 그림 2와 같이 함으로써 복원할 수 있다. 즉, 리더가 0을 전송하여 충돌이 일어났다는 것은 태그가 1을 전송하였다는 것이며, 그 반대의 경우도 마찬가지이기 때문이다.

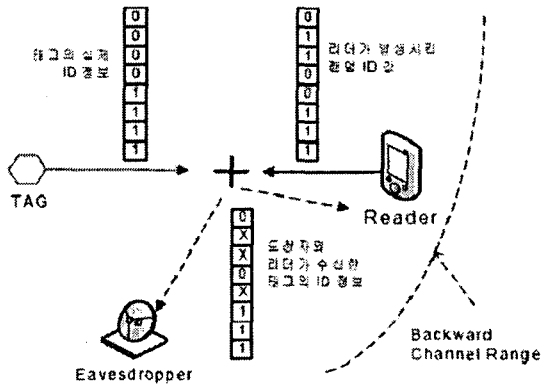

그림 1. 백워드 채널 보호 기법

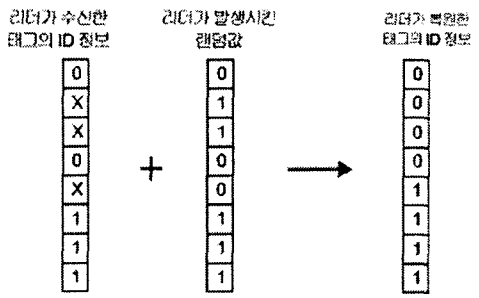

그림 2. 충돌 ID 정보로부터 실제 ID 추출 과정

III. 제안하는 기법

본 논문에서 제안하는 기법에서는 모바일 기기를 에이전트(agent)라 한다. 그리고 이 에이전트는 보호하려는 태그(T_s)와 항상 같이 있는 것을 가정한다. 그리고 인증 과정에서 사용하는 합법적인 리더들의 공개키(PuK) 리스트를 미리 가지고 있다. 즉, 이 리스트의 공개키를 가지고 있는 리더만이 T_s를 읽을 수 있다. 이 리스트는

안전한 채널로 갱신된다고 가정한다.

제안하는 기법의 프로토콜은 크게 리더의 전파 범위 안에 에이전트가 없을 때와 있을 때로 나뉜다. 없는 경우는 그림 3과 같이 기존 태그 인식 과정과 다를 게 없다. 여기에서 태그(T_u)들은 에이전트로부터 보호 받지 못한다.

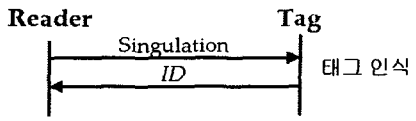

그림 3. 에이전트가 없는 프로토콜의 전체 구조

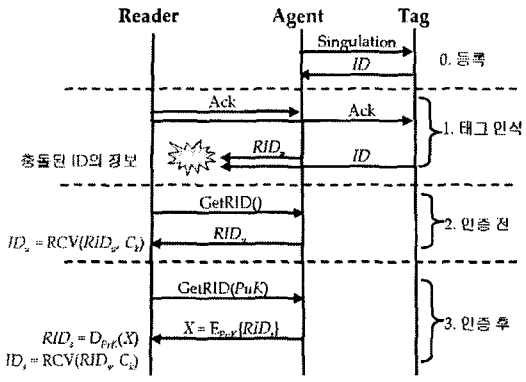

그림 4. 에이전트가 있는 프로토콜의 전체 구조

하지만, 에이전트가 있으면 그림 4와 같이 기존 방법이 크게 변한다. 여기에는 크게 등록, 태그 인식, 인증 전, 인증 후의 4단계가 존재한다. 먼저 등록 과정에서 소유자는 보호하려는 태그들을 미리 에이전트에 등록한다. 등록은 T_s의 ID를 에이전트가 저장하는 것이다. 이 과정에선 기존 태그 인식을 사용한다. 이때 다른 공격자는 없으며 안전한 환경 하에서 등록한다고 가정한다.

그 후 실질적인 프로토콜 부분으로 들어간다. 리더의 태그 인식 과정은 EPCglobal C1G2의 태그 인식 과정대로 진행한다. 리더는 태그 인식 과정 중에 태그의 실제 ID를 알아내기 위해 'Ack 명령어'를 보낸다. 태그는 이 'Ack 명령어'에 따라 응답을 하는데, 이때 에이전트는 동시에 RID_n를 보낸다. 여기서 RID_n은 n번째 RID를 뜻한다. 이러면 리더는 'Ack 명령어'의 응답으로 충돌이 난 결과(C_k)를 받게 된다. 이 결과만으로는 무슨 ID인지 알 수가 없다. 하지만, 리더는 이 응답을 버리지 않고 기억해 둔다. 이런 태그 인식 과정이 끝나면 리더는 에이전트에게 RID_u를 'GetRID 명령어'를 통해 요청한다. 에이전트는 'GetRID 명령어'의 인자가 비어 있다면 RID_u를 전송한다. RID_u는 T_u의 ID를 복원하기 위한 RID들의 집합이다. 리더는 이것을 에이전트로부터 얻어 T_u의 ID를 복원(RCV;Recover)할 수 있다. 이렇게 함으로써 인증되지 않은 리더라 하더라도 보호되지 않은 태그들은 인식할 수 있게 된다. 이것을 가능하게 하려는 이유는 에이전트의 목적이 블로커 태그처럼 모든 것을 막는 게 아니라 보호되는 태그들만 막는 데 있기 때문이다.

한편, 보호되는 태그를 읽고 싶은 리더가 있다면 자신의 공개키(PuK)를 'GetRID 명령어'의 인자로 해서 에이전트에게 전송한다. 에이전트는 리더가 보낸 공개키가 자신이 가지고 있는 공개키 리스트에 있는지 확인한다. 있다면 합법적인 리더라고 판단하고 이 공개키로 RID_s를 암호화하여 리더에게 전송한다. RID_s는 보호되는 태그를 복원할 때 필요한 RID들의 집합이다. 그럼 리더는 그것을 자신의 비밀키(PrK)로 복호화해서 RID_s를 얻어내고 이것을 통해 보호되는 태그들의 ID도 복원할 수 있게 된다. 하지만, 만일 에이전트의 공개키 리스트에 없는 공개키가 리더로부터 전송된다면 불법적인 리더라 판단하고 아무것도 전송하지 않는다.

RID_n은 RID_u와 RID_s의 합집합이다. 그리고 RID_u와 RID_s는 서로 겹치는 게 없다. RID_u와 RID_s의 구분은 1단계 태그 인식 과정에서 에이전트가 RID를 보낼 때 충돌 난 ID를 에이전트도 듣고 방금 보낸 RID의 조합을 통해 태그의 실제 ID를 알아낸다. 이 실제 ID가 에이전트에 등록된 태그라면 RID_s 집합에 넣고 그렇지 않다면 RID_u 집합에 넣는다.

예를 들어 전체 태그 T = {ID_0, ID_1, ID_2, ID_3}로 존재하고 에이전트에 등록된 태그 T_s = {ID_0, ID_1}, T_u = {ID_2, ID_3}라고 하자. 태그 인식 과정에서 에이전트는 (RID_0, ID_0), (RID_1, ID_1), (RID_2, ID_2), (RID_3, ID_3) 충돌을 내고 이에 대한 리스트를 가지고 있다. 후에 에이전트는 리더에게 인증 전에는 RID_u = {RID_2, RID_3}만 전송하

고 인증 후에는 RID_s = {RID_0, RID_1}를 전송하게 된다.

IV. 안전성 분석

본 논문에서 제안한 에이전트를 사용한 기법을 처음에 제시한 프라이버시 보호의 2가지 큰 문제에 대하여 분석해 보겠다. 먼저 정보 유출 문제는 에이전트가 보호되는 태그의 ID를 일부로 RID와 충돌시켰기 때문에 도청자는 이 충돌된 정보에서 태그의 실제 ID를 알기는 어렵다. 물론 태그의 전체 ID 비트 수가 작고 게다가 충돌 난 비트 수가 작다면 충돌 난 ID로부터 실제 ID를 추측하는 것이 가능하겠지만 ID 비트가 길면 점차 어려워지게 된다. ID 비트 길이는 현재 많이 사용하고 있는 EPCglobal은 64비트, ISO 18000에서는 96비트이다. 논문 [7]에 의하면 이 정도 길이면 충분히 길므로 도청 가능성이 거의 0에 가깝다고 한다.

한편, 리더가 에이전트에게 보내는 'GetRID명령어' 안의 공개키를 도청자가 들어도 공개키 자체로는 어떤 복호화도 할 수 없으므로 소용이 없다. 그리고 에이전트는 RIDs를 공개키로 암호화해서 전송하기 때문에 도청자는 암호화된 RIDs를 비밀키를 몰라 복호화를 할 수 없으며 공개키를 전송한 합법적인 리더만 이것을 복호화하여 RIDs를 얻어낼 수 있다. 이것은 리더의 인증이 되기도 한다.

두 번째로 위치 추적 문제를 보면 태그의 ID는 고정되어 있으므로 리더에게 그냥 전송하면 위치 추적이 될 수 있다. 하지만, 에이전트가 매번 다른 랜덤한 값인 RID와 충돌을 내어 실제 ID의 값을 감추므로 같은 ID가 전송되지 않는다. 그러므로 이러한 변화되는 값으로 인해 공격자의 위치 추적은 힘들어 진다.

V. 결론

본 논문에서는 RFID 환경에서 프라이버시 보호를 위해 리더와 태그에 에이전트를 넣어 보호되는 태그들은 합법적인 리더만이 읽을 수 있게 만들었다. 제안한 방법은 에이전트가 없다면 기존 리더와 보호되지 않는 태그 사이에서는 변화가 없으므로 표준의 변경이 없고 에이전트가 있으면 리더에게만 약간의 확장을 하면 적용이 가능하게 만들어졌다.

앞으로는 기존 프로토콜을 좀 더 변형하지 않으면서 목적한 프라이버시 보호를 강화하는 연구를 하려 한다.

[참고문헌]

[1] R. Anderson and M. Kuhn, "Low cost attacks on tamper resistant devices", In Proceeding of the International Workshop on Security Protocols - IWSP, vol. 1361 of LNCS, pp. 125-135, April 1997.

[2] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems", In Proceedings of the 1st International Conference on Security in Pervasive Computing - SPC 2003, vol. 2802 of LNCS, pp. 454-469, March 2003.

[3] A. Juels, Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", In Proceeding of the Conference on Computer and Communications Security - ACM CCS 2003, ACM, pp. 103-111, October 2003.

[4] A. Juels, J.Brainard, "Soft Blocking: Flexible Blocker Tags on the Cheap", In Proceeding of the Workshop on Privacy in the Electronic Society - WPES 2004, pp. 1-7, October 2004.

[5] M. Rieback, B. Crispo, and A. Tanenbuam, "RFID Guardian; A battery-powered mobile device for RFID privacy management", In Proceedings of the Australasian Conference on informaiton Security and Privacy - ACISP 2005, vol. 3574 of LNCS, pp. 184-194, July 2005.

[6] http://economy.hankooki.com/lpage/industry/200602/e2006020717192070260.htm

[7] 최원준, 노병희, 유승화, 오영철, "랜덤화된 트리 워킹 알고리즘에서의 RFID 태그 보안을 위한 백워드 채널 보호 방식", 한국통신학회논문지 2005-5 Vol.30 No.5C