랜덤화된 트리워킹 알고리즘에서의 RFID 태그 보안을 위한 백워드 채널 보호 방식

준회원 최 원 준*, 종신회원 노 병 희*, 정회원 유 승 화*, 오 영 철**

Backward Channel Protection Method For RFID Tag Security in the Randomized Tree Walking Algorithm

Wonjoon Choi*, Byeong-hee Roh*, S.W. Yoo*, Young Cheol Oh* ***Regular Members***

요 약

수동형 RFID 태그는 스스로 전력을 갖고 있지 않기 때문에 연산 능력이 매우 미약하고 통신 신호는 크기가 약하고, 도달 거리가 짧다. 이런 특성을 이용하여 대부분의 태그 보안 방법은 태그로부터 리더로 전달되는 무선 경로인 백워드(Backward) 채널은 도청의 가능성이 거의 없다는 가정하에 리더로부터 태그로 정보를 전달하는 포워드(Forward) 채널을 보호하는데 초점을 맞추고 있다. 그러나, 실제로 태그와 가까이에 있는 불법적인 리더는 정보를 불법적으로 수집할 수 있다. 본 논문에서는 이러한 근접거리에서 백워드 채널을 보호할 수 있는 방법을 제안한다. 제안방법은 태그정보의 충돌방지를 위하여 제안된 트리워킹 방식의 도청가능성을 제거하기 위하여 제안된 랜덤화된 트리워킹과 같은 기존 방식들에서 문제점을 해결하여 준다. 제안 방법의 효율성은 분석 모델을 사용하여 보였으며, 표준 코드시스템인 EPCglobal, ISO, uCode의 경우 도청가능성을 거의 '0'에 근접시킴을 보였다.

Key Words : RFID, 정보보호, 백워드채널, 트리워킹

ABSTRACT

Passive RFID tag does not have its own power, so it has very poor computation abilities and it can deliver signals in very short range. From the facts, most RFID Tag security schemes assumed that the backward channel from tags to a reader is safe from eavesdropping. However, eavesdroppers near a tag can overhear message from a tag illegally. In this paper, we propose a method to protect the backward channel from eavesdropping by illegal readers. The proposed scheme can overcome the problems of conventional schemes such as randomized tree walking, which have been proposed to secure tag information in tree-walking algorithm as an anti-collision scheme for RFID tags. We showed the efficiency of our proposed method by using an analytical model, and it is also shown that the proposed method can provide the probability of eavesdropping in some standardized RFID tag system such as EPCglobal, ISO, uCode near to '0'.

* 아주대학교 정보통신전문대학원 ({mecabe, bhroh, swyoo}@ajou.ac.kr)
** 삼성전자 BcN Access개발팀 소속 (ycoh@samsung.co.kr)
논문번호 : KICS2004-12-319, 접수일자 : 2004년 12월 16일
※ 본 연구는 21세기프론티어연구개발사업의 일환으로 추진되고 있는 정보통신부의 유비쿼터스컴퓨팅및네트워크원천기술개발사업의 지원에 의한것임

Ⅰ. 서 론

'비접촉식 개체 인식'을 위해 유일한 일련번호를 RFID 태그에 저장하여 무선 통신으로 읽어들이는 RFID 시스템은 물류시스템, 도서관 관리 시스템, 박물관의 정보 시스템에 응용되고 있으며, 보다 지능화, 자동화, 효율화되고 있다. 현재 주로 개발, 사용하고 있는 RFID 태그는 눈에 보이지 않을 정도로 작은 크기를 가지므로 사물의 외형에 영향을 주지 않고 부착될 수 있으며, 필요한 모든 사물에 부착할 수 있도록 제조 비용을 매우 낮추도록 하는 것을 목표로 하고 있다.

현재 주로 쓰이고 있는 수동형 RFID 태그는 통신과 연산에 필요한 전력을 스스로 소유하지 못하여, 리더로부터 발생된 전파에 내재되어 있는 에너지를 사용한다. 그러므로 연산 능력과 저장 능력이 매우 미약하고, 리더로부터의 신호 없이 먼저 통신을 개시할 수 없으며, 신호에 뒤따라서 응답하는 형식으로만 통신할 수 있다. 리더는 태그 정보를 읽기 위하여 자신이 읽고자 하는 영역내에 어떤 태그들이 존재하는지를 확인하기 위하여 질의를 전송하는데, 이때 다수의 태그의 동시응답으로 인한 충돌(collision)이 발생하여 리더가 태그들을 인식 못하게 될 수가 있다. 이러한 충돌을 회피하기 위한 다양한 충돌방지(Anti-collision) 방법들이 제안되었다.[1][2] 트리워킹 방식 (Tree Walking Algorithm)[1]은 이러한 충돌방지를 위하여 적용되는 방법들 중의 하나이다. 그러나, 이 트리워킹 방식은 리더가 태그의 ID정보를 비트단위로 확인하는 과정을 수행하게 되어, 제 3자가 태그의 ID정보를 불법적으로 취득하는 것이 가능하며, 이로부터 해당 태그 정보의 도청 또는 변조 위험성을 야기할 수 있다.

기존 통신 시스템에서 정보 보호를 위한 다양한 기술들이 제안되어 있으나, RFID 태그는 앞에서 말한 바와 같이 가격과 크기, 전력의 제약으로 인해, 연산능력이 미약하다는 약점을 갖고 있으므로, 이런 방법들을 적용하기에 적합하지 않다. 위의 트리워킹 방식에서와 같이 리더의 신호가 멀리 전달되는 특성에 의한 도청의 가능성을 막기 위하여 사일런트 트리워킹(Silent Tree Walking)[3], 랜덤화된 트리워킹(Randomized Tree Walking)[4] 방식들이 제안되었으며, 허가받지 않은 리더에 의해 수행되는 트리워킹을 방지하여 태그를 읽어들이지 못하게 하기 위한 방해자 태그 (Blocker Tag)[6] 등이 제안되었다. 이중 사일런트 트리워킹과 랜덤화된 트리워킹과 같은 방법들은 리더로부터 태그로 정보를 전달하는 포워드 채널을 보호함으로써 도청을 방지하고 있지만, 이에 응답하는 태그의 근처에서 태그로부터 리더로의 백워드 채널 신호의 도청에 대한 방어는 할 수 없다.

본 논문에서는 이러한 랜덤화된 트리워킹 방식에서 RFID 태그의 백워드 채널에 대한 도청 문제를 해결하기 위한 방법을 제안한다. 제안하는 방법은 랜덤화된 트리워킹 뿐만이 아니라, 충돌 방지와 ID 정보 전송을 분리한 모든 RFID시스템에 적용가능하다. 제안 방법은 표준 코드시스템들인 EPCglobal, ISO, uCode의 경우 백워드 채널에 대한 도청가능성을 거의 '0'에 근접시킴을 보여 준다.

본 논문의 구성은 다음과 같다. 제2장에서는 본 논문에서 제안하는 방법과 관련있는 트리워킹 기반의 RFID 태그 인식 및 정보 보호 방식들과 이들의 문제점에 대하여 기술한다. 제3장에서는 본 논문에서의 제안 방법을 설명하고, 제4장에서는 제안 방법의 성능 분석 결과를 보인다. 끝으로, 제5장에서는 본 논문의 결론을 맺는다.

Ⅱ. 기존의 트리워킹 기반 태그 정보 보호 방식들

본 장에서는 본 논문에서 제안하는 방식의 배경이 되는 트리워킹 알고리즘과 이의 RFID 태그 정보 도청 방지 문제를 해결하기 위한 사일런트 트리워킹 알고리즘과 랜덤화된 트리워킹 방식들을 소개하고, 이들의 문제점에 대하여 고찰한다.

2.1 트리워킹 (Tree Walking) 알고리즘[1]

2.1.1 트리워킹 알고리즘의 개요

ID의 첫번째 비트부터 시작하여 비트 단위로 태그를 구분해서 태그들을 분류해나가 하나의 태그를 선별하는 방법이다. 구현마다 정확한 프로토콜은 약간씩 차이를 보일 수 있지만, 태그를 분류하기 위한 방법의 기반은 같다. 다음은 트리워킹 알고리즘을 기반으로 한 프로토콜의 한 예이다. 태그는 리더의 질의에 응답할 수 있는 'on'상태와 응답할 수 없는 'off'상태를 가질 수 있는데, 먼저 리더는 모든 태그를 'on'상태로 만든다. 그 다음 리더는 첫번째 비트에 대해 질의를 하고, 이에 대해 모든 태그는 응답한다. 이때 첫번째 비트가 '0'인 태그와 '1'인 태그가 함께 존재한다면 '0'과 '1'을 의미하는 응답이 일어남으로써 충돌이 일어난다. 리더는 첫번째 비트

가 '0'인 태그들이나 '1'인 태그들 중 한 쪽을 선택하여 'off'상태로 전환시킨다. 그 다음 'on'되어 있는 태그들을 상대로 두번째 비트를 질의하고, 충돌이 일어날 경우 마찬가지로 한 쪽을 선택하여'off'시킨 후 세번째 비트에 대한 질의를 수행한다. 이를 일반화 시켜 n번째 비트를 질의한다고 하면, 현재 상태에서 'on'되어 있는 태그들이 응답을 하게 되는데 이때 0과 1이 동시에 발생하면 충돌이 일어나게 된다. 응답을 받은 후 리더는 n번째 비트가 '0'인 태그들, 혹은 '1'인 태그들을 지정하여 'off'상태로 변화할 것을 명령하고, 다음 단계에서 다시 리더는 n+1번째 비트에 대해서 질의한다. 각각의 태그 안에 들어있는 ID는 유일하기 때문에 이런 알고리즘을 1번째 비트부터 수행함으로써 태그를 적어도 하나 분류해 내고, 해당 ID를 읽어낼 수 있다. 하나의 태그를 선별해낸 다음에는 최근에 'off'시킨 태그 그룹을 'on'으로 변화시킨 후 같은 알고리즘을 적용하고, 'on'으로 남겨놓았던 태그들을 'off'로 변환시키는 방식으로 위의 알고리즘을 반복함으로써 모든 태그의 ID를 알아낼 수 있다.

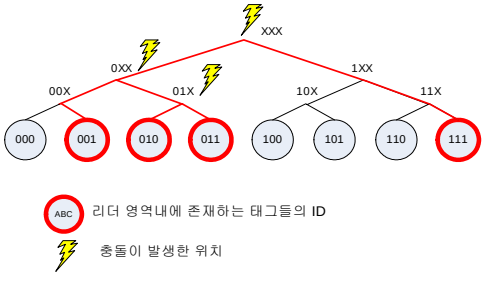

그림 1. 트리워킹 알고리즘의 적용 예

그림 1을 사용하여 3비트로 이루어진 ID를 갖는 태그들에 대하여 적용되는 트리워킹 알고리즘의 동작을 설명하기로 한다. 그림 1은 4개의 ID 001, 010, 011, 111을 갖는 태그들이 리더의 영역내에 존재하는 상황을 가정으로 한다. 그림 1에서 트리 분기점의 값들은 리더가 응답 요청한 태그 ID들의 prefix를 나타낸다. 예를 들어, 0XX는 첫번째 비트가 0인 모든 태그를 의미한다. 처음에 리더는 모든 태그가 응답하도록 XXX를 전송한다. 이 경우 모든 태그가 응답하므로 충돌이 발생한다. 리더는 첫 비트가 '0'과 '1'인 태그들이 존재한다는 것을 인식하고, 다음 단계로 0XX를 전송하게 된다. 이와 같이 하여 태그 ID 001을 찾아가기 위하여 리더가 수행한 ID 요청 순서는 XXX → 0XX → 00X → 001이 된다.

2.1.2 트리워킹 알고리즘의 도청의 위험성

그림 2는 정상적인 리더와 태그의 신호 전달을 위한 채널들과 신호 전달의 범위, 그리고 이들간의 신호를 도청하는 제3자간의 관계를 도식화 한 것이다.

그림 2에서 리더가 태그에게 질의와 전원 공급의 목적으로 신호를 전달하는 채널을 포워드 채널(forward channel), 태그가 리더에게 신호를 전달하는 채널을 백워드 채널(backward channel)이라고 표현하였다. 리더로 부터의 신호의 전달 거리는 태그에 비하여 매우 길게되므로, 포워드 채널 신호의 전달 영역은 매우 넓게 나타난다. 반면에, 리더로부터의 신호를 에너지원으로 이용하는 태그로부터의 응답 신호가 사용하는 백워드 채널의 거리는 매우 짧게 나타난다. 따라서, 트리워킹 알고리즘을 적용하는 경우, 제3자가 포워드 채널 영역내에 위치하여, 리더가 태그에게 보내는 신호들의 순서를 감지하면, 영역내에 있는 모든 태그들의 정보를 알아내는 것이 가능하다.

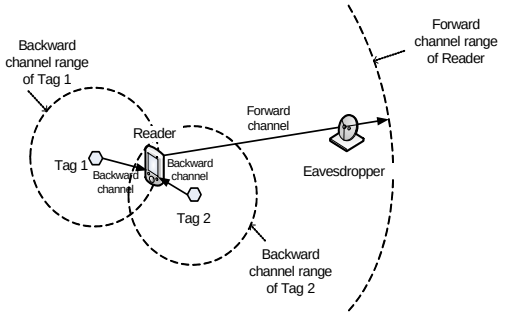

그림 2. 리더와 태그의 신호 전달 범위

2.2 사일런트 트리워킹 (Silent Tree Walking) 알고리즘[3]

2장의 1절에서 설명한 바와 같이 트리워킹 알고리즘에서는 n번째 비트에 대한 질의 후 다음 단계로 이동하기 위해 0 혹은 1을 지정하여 off시켜야 한다. 만약 'on'상태의 모든 태그의 n번째 비트가 같다면 태그들의 응답들은 충돌을 일으키지 않는다. 이런 상황에서 명시적으로 'off' 없이 다음 n+1번째 비트에 대한 질의를 하더라도 동작의 결과는 바뀌지 않는다. 이런 생각을 기반으로 사일런트 트리워킹 알고리즘에서는 n번째 비트에서 충돌이 나지 않으면 이에 대한 정보를 방출하지 않는다. 이렇게 함으로써 멀리 떨어져 있는 도청자는 해당 비트를 알

수 없게 된다. 그리고, 이런 비밀스러운 비트를 기반으로 XOR연산을 사용한 암호화의 열쇠를 만듦으로써, 보다 안전한 암호화를 이루게 된다. 하지만 사일런트 트리워킹의 문제점은 응답시 충돌이 일어나지 않는 동안은 사용할 수 없다는 것이며, 태그와 가까이에 있는 도청자에게는 이 방법이 소용이 없다는 것이다.

2.3 랜덤화된 트리워킹 (Randomized Tree Walking) 알고리즘[4]

랜덤화된 트리워킹 방식에서 태그들은 두가지의 ID를 보유한다. 하나는 실제 태그 ID이고, 다른 하나는 태그 제조 회사 또는 태그 자신이 초기화시 랜덤하게 부여한 ID이다. 리더는 태그의 ID를 찾기 위하여 트리워킹 방식을 적용하는데, 이때 적용하는 ID는 태그의 실제 ID가 아닌 랜덤하게 생성된 ID가 대상이 된다. 이 과정을 통하여 최종적으로 한 태그가 선별되면, 이 태그는 백워드 채널로 자신의 실제 ID를 리더에게 전달하여 리더가 태그의 실제 ID를 인식할 수 있도록 한다. 이 경우, 도청자는 원거리에서 리더로부터 태그들의 포워드 채널상의 신호만 인식하므로, 도청자가 인식하는 ID는 랜덤하게 생성된 ID이므로, 실제 ID는 보호가 가능하다. 이 방식은 도청자가 포워드채널 영역내의 원거리에 있고, 백워드 채널 영역내에 있을 경우에는 효과적으로 태그 정보의 보호가 가능하다. 그러나, 태그와 매우 가까이, 즉, 도청자가 그림 2에서의 백워드 채널 영역내에 있게되면, 태그로 부터의 실제 ID 정보 유출이 가능해지게 되는 문제점을 내포하고 있다.

Ⅲ. 제안하는 백워드 채널 보호 방안

여기에서는 본 논문에서 제안하는 랜덤화된 트리워킹 알고리즘의 마지막 단계인 진짜 ID 전송 단계의 백워드 채널을 보호하는 방법에 대하여 설명한다. 이를 위하여 본 논문에서는 다음을 가정한다. 즉, 통신상에 전송 에러와 같은 정보의 왜곡이 존재하지 않으며, 어떤 2개의 태그도 같은 랜덤값을 생성하지 않는다고 가정한다. 일반적으로 ID의 길이가 n 비트이고, m 개의 태그가 존재시 랜덤 ID 생성시 두 개의 태그 ID가 동일할 확률은 $\binom{m}{2}\frac{1}{2^n}$ 이고, k 개가 같을 경우는 $\binom{m}{k}\frac{1}{2^{n(k-1)}}$ 로 더 작아진다. 표준화된 ID들의 길이는 대개 64비트 이상이므로 이의 확률 값은 0에 근접하여, 위의 가정이 합리적임을 알 수 있다.

본 논문에서 제안하는 방법은 다음과 같다. 태그의 진짜 ID를 전송하는 랜덤화된 트리워킹 알고리즘의 마지막 단계에서, 하나의 태그만이 'on' 되어 있게 되므로 정상적인 경우 해당 태그가 자신의 실제 ID를 전송시 충돌이 발생하지 않는다. 이 단계에서, 제 3자가 백워드채널 범위내의 근접거리에 있게 되면 도청이 가능하게 된다. 이러한 백워드 채널의 도청을 막기 위하여 본 논문에서 제안하는 방법에서는 태그가 실제 ID를 전송할 때 리더가 동시에 랜덤하게 생성한 ID 값을 전송한다. 이때, 태그가 전송하는 ID 정보의 비트 타이밍과 리더가 전송하는 랜덤 ID 정보의 비트 타이밍은 동기화 되어 있다고 가정한다. 이와 같이 할 경우, 일치하지 않는 비트 값들은 충돌이 발생하게 된다. 따라서, 도청자는 충돌이 발생한 비트들을 갖는 정보를 수신하게 되어, 태그 ID의정확한 인식이 어려워지게 된다.

제안 방법의 예를 그림 3에 나타내었다. 그림 3에서는 ID 길이가 8비트인 경우를 예로 들고 있으며, 태그의 실제 ID는 '00001111'이다. 또한 리더가 랜덤하게 발생시킨 ID는 '01100111'이다. 두 ID가 동시에 전송시 백워드 채널의 가청 범위상에 있는 장치들이 수신하게 되는 ID는 '0XX0X111'이 된다. 여기에서 'X'는 충돌이 발생하여 '0' 또는 '1'에 대한 정확한 인식을 할 수 없게 된 비트를 나타낸다. 이러한 신호를 제 3자가 도청하였을 경우, 이 충돌이 발생한 비트를 정확히 재생해 내는 것은 확률적으로 매우 어려우며, ID의 길이가 커질수록 이러한 가능성은 거의 0에 가까워지게 된다. 이러한 상황을 제4장에서 분석을 통하여 보이기로 한다.

이에 반하여, 리더는 충돌이 일어난 비트를 포함하는 태그 ID의 모든 비트를 다음과 같이 함으로써 정확히 알 수 있다. 리더는 충돌이 일어난 비트에

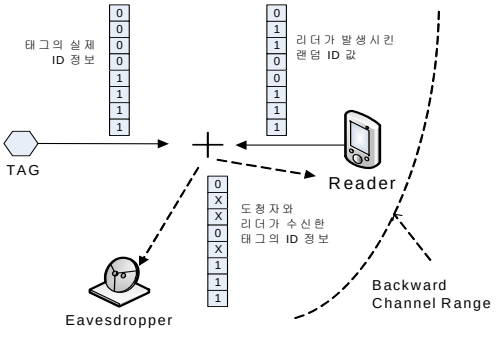

그림 3. 제안방법의 적용 예

대해서 해당 타이밍에 자신이 전송한 비트의 반대 비트를 적용하여 전체 ID를 알아낼 수 있다. 즉, 리더가 '0'을 전송하여 충돌이 일어났다는 것은 태그가 '1'을 전송하였다는 것이며, 그 반대의 경우도 마찬가지이다. 그림 4는 그림 3의 예에 대하여 리더가 충돌이 난 비트를 포함하여 태그의 모든 비트를 얻는 것을 보이고 있다. 앞에서 설명한 바와 같이, 정상적인 비트들은 그대로 적용하고, 충돌이 발생한 비트들은 리더가 발생시킨 비트의 반대값을 적용한다. 이와 같이 하여 복원된 태그의 ID 정보는 태그의 실제 ID와 동일하게 됨을 볼수 있다. 그러나, 도청자는 리더가 발생시킨 랜덤값을 알수가 없으므로, 이와 같은 정확한 복원이 거의 불가능하게 된다.

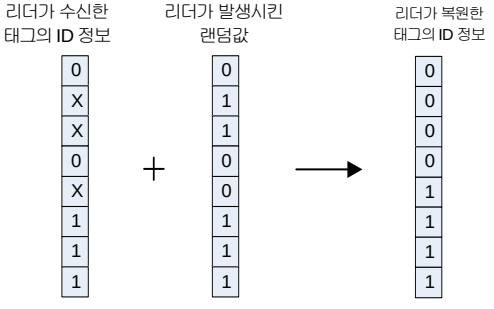

그림 4. 충돌 ID 정보로부터 리더가 실제 ID를 추출하는 과정

Ⅳ. 성능 분석

4장에서는 분석 모델을 사용하여 제안방법이 어느 정도 수준으로 태그 정보를 보호할 수 있는지를 보인다. 우선 1절에서 ID만을 전송하는 경우 순수한 수학적 분석을 통해 아이디 유출의 확률을 구하고, 2절에서는 CRC를 추가적으로 전송하는 경우에 대하여 수치적 방법으로 분석한다.

태그의 ID 길이를 l 비트라고 하고, 각 비트에서 충돌이 발생할 확률을 p_c라고 하기로 한다. 이때, l 개의 비트 중 k 개의 비트에서 충돌이 발생할 확률을 $p_c(l,k)$라 하면, 이는 다음과 같이 나타낼 수 있다.

$$P_c(l.k) = \binom{l}{k} P_c{}^k (1-p_c)^{l-k} \qquad (1)$$

또한, k개의 충돌된 비트로부터 제3자가 이를 원래의 태그 ID의 해당 비트값과 동일한 값들을 추정해 낼 확률 $P_f(k)$는 다음과 같다.

$$P_f(k) = \frac{1}{2^k} \qquad (2)$$

따라서, l 비트의 ID크기를 갖는 태그에서의 충돌 발생시 제3자가 태그 ID를 정확히 유추해 낼 수 있는 평균 가능성 $E(l)$은 다음과 같다.

$$E(l) = \sum_{k=0}^{l} P_c(l,k) \cdot P_f(k) \qquad (3)$$

이때, $p_c = \frac{1}{2}$ 이므로 식 (3)은 다음과 같이 나타낼 수 있다.

$$E(l) = \sum_{k=0}^{l} \binom{l}{k} \cdot 2^{-k} \cdot 2^{-l} = 2^{-l} \sum_{k=0}^{l} \binom{l}{k} \times 2^{-k} \qquad (4)$$

식 (4)의 우측항의 합부분은 1과 1/2의 두개의 인자로 구성된 다항식으로서 표현 가능하므로, 이를 간략히 할 수 있다.

$$E(l) = 2^{-l} \sum_{k=0}^{l} \binom{l}{k} \cdot l^{l-k} \cdot (2^{-1})^k = \frac{(1+2^{-1})^l}{2^l} = \left(\frac{4}{3}\right)^l \qquad (5)$$

식 (5)의 결과에 대한 직관적인 해석은 다음과 같다. 어떤 비트에 대하여 충돌이 일어나는 사건을 E_c, 해당 비트를 정확하게 알거나 추론을 하여 맞는 사건을 E_t라고 하자. 어떤 한 비트에 대해 올바르게 추측할 확률 $\Pr\{E_t\}$은 총 확률 정리(total probability theorem)에 의하여 $\Pr\{E_t \mid E_c\} \times \Pr\{E_c\} + \Pr\{E_t \mid E_c{}^C\} \times \Pr\{E_c{}^C\}$과 같이 된다. 이때, $E_c{}^C$은 사건 E_c의 여집합을 나타낸다. $\Pr\{E_t \mid E_c\} = \Pr\{E_c\} = \Pr\{E_c{}^C\} = 1/2$, $\Pr\{E_t \mid E_c{}^C\} = 1$이므로, $\Pr\{E_t\} = 3/4$가 된다. 각각의 비트가 제3자에 의해 해석될 확률은 서로 독립이기 때문에 길이 l에 대한 모든 비트를 정확히 추측하게 될 확률은 식 (5)와 같이 $(3/4)^l$ 이 된다.

그림 5는 제안방법을 사용시 ID의 길이가 l인 태그에 대하여, 제3자가 도청시 충돌된 비트들로부터 원래의 ID 정보를 정확히 유추해낼 가능성 ($E(l)$)을 보여준다. 식 (5)에 나타낸 바와 같이, ID 길이 l이 증가함에 따라 도청에 성공할 확률은 지수 급수로 계속 급격하게 떨어지고 있음을 볼수 있다. 특히, EPCglobal[7], uCode[8]등에서 제시하고 있는 표준 코드 길이가 64, 96, 128 비트인 경우 도

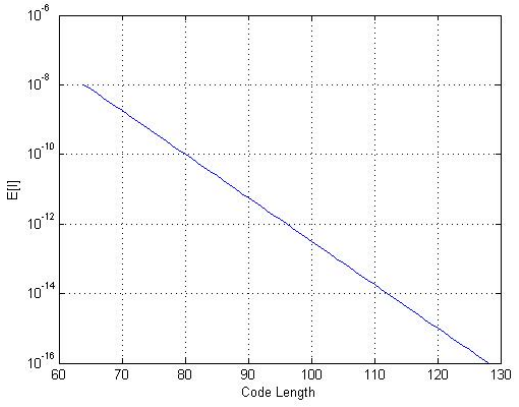

그림 5. 길이(l)에 따른 충돌 비트의 정확한 복원 가능 확률

청 가능성은 각각 $1.01*10^{-8}$, $1.01*10^{-12}$, $1.03*10^{-16}$으로서 도청 가능성이 거의 '0'에 가깝게 됨을 알 수 있다.

V. 결 론

본 논문에서는 트리워킹 방식의 도청 가능 문제를 해결하기 위하여 제안된 방식들의 문제점인 근접거리에서의 백워드 채널영역에서의 도청을 방지하기 위한 효율적인 방안을 제안하였다. 제안 방식의 성능은 표준 태그 ID 시스템의 경우 거의 '0'에 근접함을 분석을 통하여 보였다. 기존의 트리워킹을 기반으로 한 방식들이 포워드 채널의 보존에 초점을 맞추어 졌는데 반하여, 제안 방식은 백워드 채널에 대한 보안을 제공하므로, 이들을 RFID 시스템에 적용함으로써 양방향 채널의 보호를 이룰 수 있으며, 이를 통하여 RFID 응용의 보급 활성화에 기여할 수 있을 것으로 기대한다.

참 고 문 헌

[1] M. Jacomet, A. Ehrsam, U. Gehrig, "Contactless Identification Device With Anticollision Algorithm," proc. IEEE CSCC'99, Athens, Greece, July 1999

[2] H. Vogt, "Efficient Object Identification with Passive RFID Tags," Intn'l Conference on Pervasive Computing, Zürich, 2002

[3] S.A. Weis, S.E. Sarma, R.L. Rivest, and D.W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," Security in Pervasive Computing, LNCS 2802, 2003

[4] S.A. Weis, "Security and Privacy in Radio-Frequency Identification Devices," Masters Thesis. MIT. May, 2003

[5] Auto-ID Center, "Draft protocol specification for a 900 MHz Class 0 Radio Frequency Identification Tag," Auto-ID Center, Feb. 2003

[6] A. Juels, R.L. Rivest, M.Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," 8th ACM Conf. Computer and Commun. Security, 2003

[7] D. Brock, C. Cummins, "EPCTM Tag Data Standards Version 1.1 Rev.1.24", Auto-ID center, April 2004

[8] Ubiquitous ID Center, http://www.uidcenter.org/

최 원 준 (Wonjoon Choi) 준회원

2003년 2월 아주대학교 정보 및컴퓨터 공학부 졸업
현재 아주대학교 정보통신전문대학원 석사과정
<관심분야> 유비쿼터스, 트래픽 혼잡 제어 제어, RFID

노 병 희 (Byeong-hee Roh) 종신회원

1987년 2월 한양대학교 전자공학과 졸업
1989년 2월 한국과학기술원 전기및전자공학과 석사
1998년 2월 한국과학기술원 전기및전자공학과 박사
1989년 3월~1994년 3월 한국통신 통신망 연구소
1998년 2월~2000년 3월 삼성전자
현재 아주대학교 정보통신전문대학원 부교수
<관심분야> 유/무선 인터넷, 멀티미디어 통신 및 응용, 트래픽 제어, 유비쿼터스 네트워킹, RFID 네트워킹

유 승 화 (S.W. Yoo) 정회원

1972년 2월 서울대학교 응용수학과 졸업
1980년 5월 University of Kansas Computer Science 석사
1983년 5월 University of Kansas Computer Science 박사
1974년 7월~1976년 9월 한국과학 기술 연구소
1976년 10월~1978년 9월 금성 통신
1983년 6월~1988년 8월 AT Bell 연구소
1988년 9월~1989년 8월 Amdahl Corporation
1989년 8월~1999년 2월 삼성 전자
현재 아주대학교 정보통신전문대학원 교수
<관심분야> 유/무선 인터넷, 멀티미디어 통신 및 응용, 트래픽 제어, 유비쿼터스 네트워킹, RFID

오 영 철 (Young Cheol Oh) 정회원

1980년 경북대학교 전자공학과 졸업
1993년 LSU(Luisiana State Univ.) 전기및컴퓨터공학석사
1996년 LSU 전기및컴퓨터 공학박사
1980년 삼성반도체통신 입사
2000년~ 삼성전자 Broadband Access개발팀장, 연구위원(상무)
<관심분야> BcN Access Network, FTTH, Home Network, Sense Network