情報保護學會論文誌
第17卷 第4號, 2007. 8

경량 RFID 상호인증 프로토콜 LMAP, M^{2}AP, EMAP에 대한 향상된 취약성 분석

권 대 성,* 이 주 영, 구 본 욱
국가보안기술연구소

Improved cryptanalysis of lightweight RFID mutual authentication Protocols LMAP, M^{2}AP, EMAP

Daesung Kwon,* Jooyoung Lee, Bon Wook Koo
National Security Research Institute

요 약

최근 P. Peris-Lopez 등에 의하여 제안된 일련의 RFID 상호인증 프로토콜 LMAP[10], M^{2}AP[11], EMAP[12]은 간단한 논리 연산에 기반하여 경량 환경에서 높은 구현 효율성을 제공하도록 설계되었다. 그런데, T. Li 등은 [8,9]에서 전송 메시지를 변조하는 능동적 공격으로 위 프로토콜들에 대한 비동기화공격이 높은 확률로 적용됨을 보이고, 태그의 ID를 포함한 일부 비밀 정보를 얻을 수 있음을 보였다. 본 논문에서는 [9]의 일부 오류를 수정하여 비동기화공격이 항상 가능함을 보이고 LMAP에 대한 대폭 개선된 능동적 공격을 제시한다. 한편, M^{2}AP, EMAP에 대한 새로운 분석으로서, 2~3개 연속 세션의 도청으로 태그의 ID를 포함한 일부 비밀 정보를 얻을 수 있음을 보인다. 이들 정보는 태그 추적 외에, M^{2}AP의 경우 태그 위장에도 사용될 수 있어 본고의 공격은 M^{2}AP와 EMAP의 치명적인 결함을 드러낸다고 하겠다.

ABSTRACT

In this paper, we present a security analysis of Lightweight RFID Mutual Authentication Protocols - LMAP[10], M^{2}AP[11], EMAP[12]. Based on simple logic operations, the protocols were designed to be suitable for lightweight environments such as RFID systems. In [8,9], it is shown that these protocols are vulnerable to de-synchronization attacks with a high probability. The authors also presented an active attack that partially reveals a tag's secret values including its ID. In this paper, we point out an error from [9] and show that their de-synchronization attack would always succeed. We also improve the active attack in [9] to show an adversary can compute a tag's ID as well as certain secret keys in a deterministic way. As for M^{2}AP and EMAP, we show that eavesdropping 2~3 consecutive sessions is sufficient to reveal a tag's essential secret values including its ID that allows for tracing, de-synchronization and/or subsequent impersonations.

Keywords : *RFID, 상호인증 프로토콜, 위장 공격, 태그 추적*

접수일: 2007년 5월 30일; 채택일: 2007년 7월 2일
* 주저자, 교신저자: ds_kwon@etri.re.kr

Ⅰ. 서 론

최근 RFID(Radio Frequency IDentification) 시스템이 물류 관리에서 바코드의 역할을 대신하며 각광받고 있는 추세이다. 기존 바코드가 접촉식 리더를 통하여 인식되는 반면, RFID 태그(tag)는 비접촉식 리더(reader)로 인식되는 장점을 갖고 있어, 유통업, 도서관, 승용차 요일제 등으로 급속하게 적용 영역을 확장하고 있다. 그러나 원거리에서 태그를 인식할 수 있다는 성질로 인하여 프라이버시 문제도 꾸준히 제기되는 실정이다. 예를 들어, 제3자가 제품에 부착된 태그를 원거리에서 인식함으로써, 특정 개인이 구매한 제품의 정보를 획득할 수 있고, 나아가 이러한 정보를 개인의 위치 추적 등에 사용할 수도 있다는 것이다. 또한 불법적으로 유출된 정보는 위조 태그의 제조 등 범죄에 이용될 여지도 있다. 이 같은 보안 위협을 막기 위해 태그와 리더에 탑재할 수 있는 인증 프로토콜의 개발이 활발히 진행되고 있다.

지금까지 제안된 인증 프로토콜은 주로 해쉬 함수 또는 블록 암호를 이용하는 방식들이다. 그러나 인증 프로토콜의 주요 적용 환경이라 할 900MHz 대역 RFID 태그는 저가에 대량으로 생산되어야 하기 때문에 이들 방식을 그대로 적용하기에 한계가 있다. 대표적인 해쉬 함수인 SHA-256의 경우 10K게이트까지 구현이 가능하나[2] RFID 환경에서는 여전히 구현 면적이 큰 편에 속한다. 블록 암호 AES의 경우, 3000게이트 정도의 구현이 가능하나[5] 통신 속도 관련 요구 조건인 "초당 100회 이상의 통신"이 가능한 프로토콜은 지원하지 않을 것으로 보인다.

해쉬 함수, 블록 암호 등에 기반한 기존 인증 프로토콜들의 문제점을 해결하고자 하는 연구들이 진행되고 있는데, 대표적인 방향으로 LPN (Learning Parity with Noise) 문제를 이용한 HB 프로토콜 연구[4,6]와 +,⊕,∧, ∨등의 논리 연산만을 이용한 초경량 인증프로토콜 연구[10,11,12]를 들 수 있다. 전자의 경우, 안전성 증명이 제시되어 있는 반면 효율성이 떨어지는 단점을 가지고 있으며, 후자의 경우 매우 높은 효율성을 제공하고 있지만 안전성 주장이 충분하지 못한 단점이 있다.

LMAP, M²AP, EMAP 등의 초경량 프로토콜들[10,11,12]은 안전성이 보장될 경우 기존의 프로토콜보다 매우 높은 효율성을 보장하기 때문에 관심을 끌어왔다. 그런데, 최근 AReS 2007과 IFIP SEC 2007에 채택된 논문들[8,9]에서 이들의 취약성이 발표되었다. 이들 논문에서는 이 프로토콜들에 대한 비동기화 공격(De-synchronization Attack)이 가능함을 보이고, 이를 이용하여, LMAP의 경우 확률적으로 tag의 *ID*를 얻는 능동적 공격을, M²AP의 경우에는 tag의 *ID*를 결정하는 능동적 공격을, EMAP의 경우 연속되는 약 log296개의 리더와 태그 간의 유효 세션을 만들어 tag의 *ID*를 얻는 능동적 공격 방법을 제시하였다. 이 공격들은 인증을 위한 통신 값을 중간에서 변형하고 태그의 인증/에러 여부를 확인하여 태그의 *ID*와 일부 비밀키를 복원하는 방법으로서 프로토콜들의 키 갱신 과정은 이용하지 않고 있다.

이 논문에서는 M²AP, EMAP의 경우 비밀키 갱신과정을 효과적으로 이용하면 연속되는 2~3세션을 도청하는 수동적 공격만으로 태그의 *ID*와 비밀키 일부를 얻을 수 있음을 보인다. 그리고 LMAP의 경우에는 [9]에서 제시한 확률적 태그 *ID* 추출 공격을 개선하여 상대적으로 매우 적은 통신량으로 태그의 *ID*를 결정할 수 있는 공격방법을 제시한다. 이와 더불어, [8,9]에서 제시된 비동기화 공격의 간단한 오류를 수정하여, 공격이 논문의 주장에서와 같이 확률적으로 성공하는 것이 아니라 항상 성립한다는 것을 보인다.

편의상, 비밀키와 *ID*의 크기를 m이라고 할 때, [8,9]에서 제안된 태그 *ID* 추출 공격과 본 논문에서 제안되는 공격의 수동/능동 유형과 요구 통신 횟수 등을 비교하면 표 1과 같다. [표 1]에서 [리더 a, 태그 b]는 각각 공격에 요구되는 공격자-리더 간, 공격자-태그 간의 통신 회수를 표기한다.

[표 1] 본 논문과 [8,9]의 tag *ID* 복원 공격 비교

프로토콜	[8,9]	본 논문	
	능동 공격	능동 공격	수동 공격
LMAP	[리더 2, 태그 $m+2$] × 수 회	[리더 1, 태그 $2m+2$]	-
M²AP	[리더 1, 태그 $m+1$]	-	연속된 두 세션 도청
EMAP	[리더 1, 태그 4] × (log2m-1)회	-	연속된 두 세션 도청: 2^3개의 *ID* 후보 연속된 세 세션 도청: $2^{3/8}$개의 *ID* 후보

본 논문의 나머지 부분은 다음과 같이 구성된다. 2절에서는 LMAP, M²AP, EMAP을 소개하고, 3절에서는 [8,9]에서 제시된 공격 방법에 대하여 간단히 소개하고, 오류를 수정한다. 4절에서 LMAP에 대한 개선된 능동 공격과 M²AP, EMAP에 대한 수동 공격을 제시한다.

Ⅱ. 경량 인증 프로토콜 LMAP, M²AP, EMAP

RFID 상호 인증 프로토콜 LMAP, M²AP, EMAP은 각각 A Real Light-weight Mutual-Authentication Protocol, A Minimalist Mutual-Authentication Protocol, An Efficient Mutual-Authentication Protocol for Low-cost RFID tags의 약자를 따 명명되었으며, 이들은 모두 다음과 같은 특징을 갖고 있다.

- 고정된 ID 사용(m=96비트)
- 태그 구별을 위한 index-pseudonym(IDS) 사용: 유효 세션 후 갱신됨
- 인증을 위한 4종의 96비트 비밀키 K1, K2, K3, K4 사용: 유효 세션 후 갱신됨
- 인증 및 키 갱신에서 +, ⊕, ∧, ∨ 의 연산만 사용: 경량 및 고속 구현에 적합함

m비트 A의 각 비트를 최하위 비트 $[A]_0$에서 최상위 비트 $[A]_{m-1}$으로 표기하고 $A(k:l)$ $(k>l)$을 l번째 비트부터 k번째 비트까지의 연접 $[A]_k \| \cdots \| [A]_l$ 으로 정의하자. LMAP, M²AP, EMAP은 각각 다음 도식과 같이 진행된다. 진행 과정에서 $n1$, $n2$는 리더가 생성하는 m 비트 난수를 표기한다.

단계 1: Tag identification

(1) 리더 → 태그: hello

(2) 태그 → 리더: $IDS^{(n)}$

단계 2: Mutual authentication

○ LMAP

(1) 리더 → 태그: A||B||C

(2) 태그 → 리더: D

- A= $IDS^{(n)} \oplus K1^{(n)} \oplus n1$,
- B= $(IDS^{(n)} \vee K2^{(n)}) + n1$,
- C= $IDS^{(n)} + K3^{(n)} + n2$,
- D=$(IDS^{(n)} + ID) \oplus n1 \oplus n2$.

○ M²AP

(1) 리더 → 태그: A||B||C

(2) 태그 → 리더: D||E

- A= $IDS^{(n)} \oplus K1^{(n)} \oplus n1$,
- B= $(IDS^{(n)} \wedge K2^{(n)}) \vee n1$,
- C= $IDS^{(n)} + K3^{(n)} + n2$,
- D=$(IDS^{(n)} \vee ID) \wedge n2$,
- E=$(IDS^{(n)} + ID) \oplus n1$.

○ EMAP

(1) 리더 → 태그: A||B||C

(2) 태그 → 리더: D||E

- A= $IDS^{(n)} \oplus K1^{(n)} \oplus n1$,
- B=$(IDS^{(n)} \vee K2^{(n)}) \oplus n1$,
- C= $IDS^{(n)} \oplus K3^{(n)} \oplus n2$
- D=$(IDS^{(n)} \wedge K4^{(n)}) \oplus n2$,
- E=$(IDS^{(n)} \wedge n1 \vee n2) \oplus ID \oplus \bigoplus_{I=1}^{4} KI^{(n)}$

위 과정에서 비밀키를 가진 리더만 올바른 (A,B)쌍을 생성할 수 있으므로, 태그는 (A,B)를 이용하여 리더를 인증하게 된다. 한편, 비밀키를 가진 태그만이 올바른 (D,(E))를 생성할 수 있으므로, 리더는 (D,(E))를 이용하여 태그를 인증하고 ID를 얻는다.

단계 3: IDS와 비밀키 갱신

○ LMAP

- $IDS^{(n+1)} = (IDS^{(n)} + (n2 \oplus K4^{(n)})) \oplus ID$
- $K1^{(n+1)} = K1^{(n)} \oplus n2 \oplus (K3^{(n)} + ID)$,
- $K2^{(n+1)} = K2^{(n)} \oplus n2 \oplus (K4^{(n)} + ID)$,
- $K3^{(n+1)} = (K3^{(n)} \oplus n1) + (K1^{(n)} \oplus ID)$,
- $K4^{(n+1)} = (K4^{(n)} \oplus n1) + (K2^{(n)} \oplus ID)$.

○ M²AP

- $IDS^{(n+1)} = (IDS^{(n)} + (n2 \oplus n1)) \oplus ID$,
- $K1^{(n+1)} = K1^{(n)} \oplus n2 \oplus (K3^{(n)} + ID)$,
- $K2^{(n+1)} = K2^{(n)} \oplus n2 \oplus (K4^{(n)} + ID)$,
- $K3^{(n+1)} = (K3^{(n)} \oplus n1) + (K1^{(n)} \oplus ID)$,
- $K4^{(n+1)} = (K4^{(n)} \oplus n1) + (K2^{(n)} \oplus ID)$.

○ EMAP

- $IDS^{(n+1)} = IDS^{(n)} \oplus n2 \oplus K1^{(n)}$,
- $K1^{(n+1)} = K1^{(n)} \oplus n2 \oplus (ID(95:48) \| F_p(K4^{(n)}) \| F_p(K3^{(n)}))$,
- $K2^{(n+1)} = K2^{(n)} \oplus n2 \oplus (F_p(K1^{(n)}) \| F_p(K4^{(n)}) \| ID(47:0))$,
- $K3^{(n+1)} = K3^{(n)} \oplus n1 \oplus (ID(95:48) \| F_p(K4^{(n)}) \| F_p(K2^{(n)}))$,

· $K4^{(n+1)} = K4^{(n)} \oplus n1 \oplus (F_p(K3^{(n)}) \| F_p(K1^{(n)}) \| ID(47:0))$.

EMAP 키 갱신 과정에서 $F_p(x)$는 4개의 24비트 블록으로 분할된 96비트 $x = x_1 \| x_2 \| x_3 \| x_4$의 블록별 XOR를 표기한다. 즉, $F_p(x) = x_1 \oplus x_2 \oplus x_3 \oplus x_4$으로 정의된다. EMAP 제안 논문[12]에서는 비트 인덱스 표기에 big-endian을 사용하고 있고 여기에서는 little-endian을 사용하고 있어, 키 갱신 과정의 표기가 EMAP 제안 논문의 표기와는 차이가 있다.

이 프로토콜들의 서술에서 태그와 리더의 비밀키 갱신 시점이 명확히 제시되지 않고 있으나, 태그의 비밀키 갱신이 리더의 태그 인증과 무관하게 일어난다면 메시지 차단에 의한 자명한 비동기 공격이 성립하게 된다. 그러므로 본고에서는 태그와 리더의 IDS 및 비밀키 갱신이 상호 인증 완료 후 이루어진다고 가정하겠다. 이러한 가정은 [8,9]에서도 전제되었다.

Ⅲ. LMAP, M²AP, EMAP에 대한 능동 공격[8,9]

[8,9]에서 LMAP 등에 적용된 분석 방법은 다음과 같이 간단히 요약할 수 있다. 인증 과정에서 전송되는 메시지의 (정해진 위치의) 한 비트를 변형하고, 인증 여부를 확인한 후, 이로부터 비밀키의 해당 비트 정보를 얻어내는 것이다. 좀 더 자세히 서술하면, x, y, r이 미지수이고, $A = x \oplus r$과 $B = y + r$이 주어졌을 때, A, B를 한 비트 씩 변형한 $A' = x \oplus r \oplus [I]_i$, $B' = (y + r) \oplus [I]_i$ ($[I]_i$는 i번째 비트만 1이고 나머지는 0인 비트열)이 유효한 응답 쌍이 될 확률 (즉, $B' = y + (r \oplus [I]_i)$이 될 확률)이 50%라는 점과, A, B, A', B''$= y + (r \oplus [I]_i)$이 주어지면 B'과 B''을 비교하여 $[r]_i$의 정보를 얻을 수 있다는 성질을 이용한다. 전자는 비동기화 공격에 이용되고 후자는 태그의 비밀키 및 ID를 추출하는데 이용된다. 자세한 내용은 [8,9]에 제시되어 있다.

3.1. 비동기화 공격

공격자가 태그로부터 $IDS^{(n)}$를 받고, 리더에게 대신 전달하여 리더로부터 A||B||C를 받았다고 가정하자. 공격 3의 경우를 예로 들면, 공격자는 A, B, C의 한 비트씩을 변형한 A'||B'||C'을 태그에게 보내고, 다시 태그에게서 받은 메시지 D(||E)의 한 비트를 변형한 D'(||E')을 리더에게 보낸다. 양측의 인증이 성공할 경우, 태그와 리더의 공통 정보(IDS 및 비밀키)가 각각 다른 값으로 갱신되어, 이후의 상호 인증이 불가능해진다.

공격 1: C를 수정하여 전송하는 공격
(1) 공격자 → 태그: A||B||C' ($C' = C \oplus [I]_j$)
(2) 태그 → 공격자: D(||E)
(3) 공격자 →리더: D'(LMAP), D'||E(M^2AP)
D'||E'(EMAP)($D' = D \oplus [I]_j$ $E' = E \oplus [I]_j$)

공격 2: A, B를 수정하여 전송하는 공격
(1) 공격자 → 태그: A'||B'||C ($A' = A \oplus [I]_j$, $B' = B \oplus [I]_j$)
(2) 태그 → 공격자: D(||E)
(3) 공격자 → 리더:D'(LMAP), D||E'(M^2AP), D||E'(EMAP) ($D' = D \oplus [I]_j$ $E' = E \oplus [I]_j$)

공격 3: A, B, C를 수정하여 전송하는 공격
(1) 공격자 → 태그: A'||B'||C' ($A' = A \oplus [I]_j$, $B' = B \oplus [I]_j$, $C' = C \oplus [I]_j$)
(2) 태그 → 공격자: D(||E)
(3)공격자 →리더: D'(LMAP),D'||E'(M2AP), D'||E'(EMAP) ($D' = D \oplus [I]_j$ $E' = E \oplus [I]_j$)

공격 1의 경우 C를 변형하면 태그는 $n2$값을 한 비트 변형된 값으로 추출한다. D 또는 E의 해당 비트를 변형하여 리더에 전송할 경우, 태그-리더 사이의 어떤 비밀정보의 해당 비트 값에 따라 리더는 태그를 인증하거나 거부하게 된다. LMAP, M²AP의 경우 50%의 확률로 공격자가 리더에게 전달하는 값이 유효한 값이 된다. 리더가 태그를 인증하는 경우, 리더는 난수 $n2$값을 이용하여 $IDS^{(n)}$와 비밀키를 갱신하고 태그는 $n2 \oplus [I]_j$를 이용하여 $IDS^{(n)}$와 비밀키를 갱신하므로 양측 사이의 동기가 깨지게 된다. EMAP의 경우, $[IDS^{(n)}]_j = 0$이면 100%, 그렇지 않으면 50% 확률로 공격자가 리더에게 전달하는 값(D'(LMAP),D'||E(M^2AP)),D||E'(EMAP))이 올바른 값이 된다. EMAP의 경우, $[IDS^{(n)}]_j = 0$인 j를 찾을 수 있으므로 100% 성공 가능한 공격이라고 할 수 있다.

LMAP, M²AP에 대한 공격 2의 경우, 공격자가 A, B

의 한 비트씩을 변형하여 태그에게 전달하면 태그는 50%의 확률로 공격자를 인증하게 된다. 이 때, 태그의 출력 중 D를 D'=D⊕$[I]_j$로 바꾸어 리더에게 전달하면, 리더는 공격자를 인증하게 되고 $n1$을 이용하여 $IDS^{(n)}$와 비밀키를 갱신한다. 반면, 태그는 $n1$⊕$[I]_j$를 이용하여 $IDS^{(n)}$와 비밀키를 갱신하므로 양측의 동기가 깨지게 된다. EMAP의 경우에는 A, B의 한 비트씩을 변형한 값을 태그에게 전달하면 태그는 항상 공격자를 인증하고 $n1$⊕$[I]_j$를 이용하여 $IDS^{(n)}$와 비밀키를 갱신한다. 공격자는 태그의 출력값 중 E를 E'=E⊕$[I]_j$로 바꾸어 리더에게 전달하는데, 리더가 이를 인증할 확률은 50%가 된다. 이 경우, 리더는 $n1$을 이용하여 $IDS^{(n)}$와 비밀키를 갱신하게 되어 동기가 깨지게 된다.

공격 3은 공격 1과 공격 2를 결합한 공격으로 리더는 $n1$, $n2$를 이용하여 $IDS^{(n)}$와 비밀키를 갱신하고 태그는 $n1$⊕$[I]_j$, $n2$⊕$[I]_j$를 이용하여 비밀키를 갱신하게 되어 비동기 정도가 커지게 된다. 세부적인 내용은 [8,9]를 참조하면 된다.

3.2. Tag *ID* 추출 공격

태그의 *ID* 추출은 비동기화 공격 방법 중 공격 2를 변형한 것이다. 본 논문에서는 [9]에서 제시된 공격 방법을 LMAP 분석에만 이용하므로, LMAP에 대해서만 공격 방법을 간단히 서술한다. 공격 2를 96비트 위치의 각각에 적용하면, 각 비트 위치에 대해 태그는 50%의 확률로 공격자를 인증하거나 에러를 출력할 것이다. 최상위 비트를 제외한 각 비트 위치에 대하여 난수 $n1$의 각 비트 $[n1]_j$는 공격자가 인증되는 경우 $[B]_j$, 에러가 출력되는 경우 $[B]_j$⊕1과 일치하므로 공격자는 $n1$을 복원할 수 있다. [9]에서는 $n1$을 모두 얻을 수 있다고 주장하고 있지만, 최상위 비트가 변형된 경우에는 태그가 공격자를 항상 인증하므로 위와 같은 정보 추출은 성립하지 않는다. 이제 $IDS^{(n)}$와 상호인증 과정의 A, B, $n1$을 이용하여 $K1^{(n)}$의 모든 비트와 $K2^{(n)}$의 일부 비트($IDS^{(n)}$의 해당 비트가 0인 비트)를 계산할 수 있다. 그렇지만, *ID*를 복원하기 위해서는 $n2$를 얻어야 한다.

이를 위하여 공격자는 리더에 다시 $IDS^{(n)}$를 전송함으로써 리더로부터 $A^{\dagger}$,$B^{\dagger}$,$C^{\dagger}$를 얻고 이미 구한 $K1^{(n)}$과 $K2^{(n)}$의 일부 비트를 이용하여 $n1^{\dagger}$이 0이 되는 $A^{\ddagger}$, $B^{\ddagger}$를 계산한다. 그리고 공격자는 태그에게 $A^{\ddagger}\|B^{\ddagger}\|C$를 전송하여 $D^{\dagger}$을 얻는다. 이 세션의 $n2^{\dagger}$이 이전 세션의 $n2$와 다른 점을 이용하여 다음과 같은 식을 얻을 수 있다.

$C=(IDS^{(n)}+K3^{(n)})+n2$,

$D=(IDS^{(n)}+ID)\oplus n1\oplus n2$,

$C^{\dagger}=(IDS^{(n)}+K3^{(n)})+n2^{\dagger}$,

$D^{\dagger}=(IDS^{(n)}+ID)\oplus n2^{\dagger}$

위 식에서 $n2$, $n2'$, $K3^{(n)}$를 소거하면 다음의 식을 얻는다.

$C^{\dagger}-C=(IDS^{(n)}+ID)\oplus D^{\dagger}-(IDS^{(n)}+ID)\oplus n1\oplus D$.

식을 간단히 하기 위해서, $a=D^{\dagger}$, $b=n1\oplus D$, $c=C^{\dagger}-C$, $x=(IDS^{(n)}+ID) \bmod 2^{96}$이라고 놓으면 *ID*를 복원하는 것은 주어진 a,b,c 로부터 다음 식을 만족하는 $x\in\{0,1\}^{96}$를 구하는 문제로 환원된다.

$x\oplus a=x\oplus b+c \ mod\ 2^{96}$.

위 식의 계산에서 상위 비트들은 하위비트 계산에 영향을 미치지 않으므로 x를 상위부터 4비트씩 24개 부분으로 나누고 각 4비트씩 전수조사를 한다. 이 경우 공격량은 $(2^{24}-1)\times$(4비트 전수조사량)이 된다. (이 양은 효율적인 알고리즘의 사용으로 추가적으로 감소할 수 있다.) 그런데, 위 식에서 $[a]_j=[b]_j$인 경우에는 $[x]_j$를 얻을 수 없다. 그러므로 정확한 x를 복원하기 위해서는 상기 공격을 수회 반복하여야 한다. 자세한 내용은 [9]에 제시되어 있다.

3.3. 분석

논문 [8,9]에서 제시한 LMAP 등에 대한 비동기화 공격과 태그 *ID* 추출 공격을 이전 소절에서 살펴보았다. 이제 논문들에서 소홀히 한 점을 지적하고자 한다. 먼저, LMAP, M^2AP의 경우 모든 비트에 대하여 공격 1, 2, 3이 성공할 확률이 50%라고 주장하였는데, 최상위 비트에 대해서는 항상 성공한다. LMAP에 대한 공격 1의 경우

$$[C]_{95}=[IDS^{(n)}]_{95}\oplus[K3^{(n)}]_{95}\oplus[n2]_{95}\oplus carry,$$

$$[D]_{95}=[(IDS^{(n)}_{tag(i)}+ID_{tag(i)})]_{95}\oplus[n1]_{95}\oplus[n2]_{95},$$

이므로 C'=C⊕$[I]_{95}$에 대한 D'=D⊕$[I]_{95}$은 항상 올바른 답이 된다. 그러므로 비동기화 공격이 EMAP 뿐만 아니라 LMAP, M^2AP의 경우에도 항상 성립하게 된다.

비동기화 공격은 좋아지는 반면, 태그 *ID* 추출 공격은 단점을 안게 된다. [9]에서는 공격 2를 이용하면 $n1$ 모든 비트를 얻을 수 있다고 주장하지만, 공격 2가 최상

위 비트에 적용되었을 때, 태그는 항상 공격자를 인증하므로 공격자는 $n1$의 최상위 비트를 얻을 수 없다. 결과적으로 [8,9]에서 제시한 공격 방법은 태그 ID의 최상위 비트를 제외한 모든 비트를 추출하는 공격 방법으로 볼 수 있다.

Ⅳ. 경량 프로토콜 LMAP에 대한 개선된 능동 공격과 M²AP, EMAP에 대한 수동 공격

4.1. LMAP에 대한 개선된 태그 ID 추출 공격

3절에서 소개한 LMAP에 대한 능동 공격[9]의 경우, 리더와의 통신 2회, 태그와의 통신 m+2회로부터 태그의 ID를 확률적으로 얻을 수 있었다. 이 공격에서 공격자는 한 번의 리더와의 통신으로 받은 A, B, C와 이를 이용한 태그와의 통신에서 $n1$만 얻고, $n2$를 얻을 수 없었다. 그러나 본 논문에서는 리더와의 추가적인 통신 없이 태그와의 추가 통신으로 $n2$도 얻을 수 있음을 보인다. 공격자가 동일한 $IDS^{(n)}$를 리더에 반복해서 보내지 않아도 되기 때문에 리더가 공격을 탐지하기 어렵다는 장점이 있다. 또한 우리의 공격은 태그와의 추가적인 m+1회의 통신으로 $n2$를 얻어서 확률적이 아닌 결정적 방식으로 ID를 계산하게 한다. 이러한 면에서 [9]에서 제시한 공격이 대폭 개선됐다고 볼 수 있다.

개선된 공격에는 다음의 보조정리가 이용된다.

보조정리 1([7]). x와 y를 m비트 미지수라고 하자, $i=0,\ldots,m-2$에 대하여 $x\oplus y$, $x\oplus(y+[1]_i)$을 알면 x, y의 최상위 비트를 제외한 모든 비트를 알 수 있다.

보조정리는 $[y\oplus(y+1)]_1=y_0$의 식을 이용하여 증명할 수 있는데, 자세한 증명은 [7]을 참조하면 된다. 이제 공격은 [9]에서 제시한 공격의 일부분을 이용하는 단계와 위의 보조정리를 적용하는 단계로 구성된다.

단계 1: 리더로부터 받은 A, B ,C로부터 $n1, K1^{(n)}$ 복원

이 단계에서 공격자는 3.1의 공격 2를 이용하는 방법을 [9]와 같이 적용하여, 리더와의 통신 1회, 태그와의 통신 m회로 $n1$, $K1^{(n)}$의 최상위 비트를 제외한 모든 비트를 얻는다.

단계 2: $n1, K1^{(n)}$과 리더로부터 받은 A, B, C로부터 $n2, K3^{(n)}, ID$ 복원

보조정리 1을 이용하면 태그의 ID 복원은 다음과 같이 할 수 있다.

먼저, C를 C_j=C+$[1]_j$($j=0,\ldots,m-2$)로 변형하여 태그에 전송하고(m-1회) 응답 D'을 얻는다.

(1) 공격자→태그: $A\|B\|C_j$

(C_j=C+$[1]_j$=$IDS^{(n)}+K3^{(n)}+n2+[1]_j$)

(2) 태그→공격자: D_j

($=(IDS^{(n)}+ID)\oplus n1\oplus(n2+[1]_j)$)

D_j들에 대하여 $x=(IDS^{(n)}+ID)\oplus n1$, $y=n2$로 놓고, 보조정리 1을 이용하면 $(IDS^{(n)}+ID)$와 $n2$의 최상위 비트를 제외한 모든 비트를 얻을 수 있다. $IDS^{(n)}$가 공개된 값이므로, 공격자는 $n2$, $K3^{(n)}$, ID의 최상위 비트를 제외한 모든 비트를 계산할 수 있다.

정리하면, 리더와의 통신 1회 태그와의 통신 $(2m-1)$회로 태그 ID 및 일부 키 값의 최상위 비트를 제외한 모든 비트를 얻을 수 있다. [9]에서 제시한 공격이 리더와의 통신 2회, 태그와의 통신 $(m+1)$회로 ID의 일부 비트만을 추출한다는 점에 비춰볼 때 위 공격은 이로부터 대폭 향상된 공격이라고 볼 수 있다.

4.2. M²AP에 대한 새로운 태그 ID 추출 공격

앞에서 제시한 공격들은 리더와 태그가 동시에 상호인증이 된 후에 키 등의 공통 정보를 갱신한다는 가정을 이용하고 있다. 이와 같은 공격을 방지하기 위해 태그가 동일하거나 유사한 값들을 연속적으로 수신했을 때 응답을 거절하도록 하는 방법을 생각해 볼 수 있다. 그리고 올바른 인증이 되지 않는 경우에 에러 대신 랜덤한 값을 응답하도록 프로토콜을 개선할 수도 있을 것이다. 그러나 이 절에서 주어지는 M²AP에 대한 공격은 공격자로 하여금 리더와 태그 간의 연속된 2개 세션의 도청만으로 ID를 얻을 수 있게 한다. 2개 이상의 세션 정보 구분을 위하여 난수 및 리더-태그 간 소통 정보에도 세션 표기를 도입하겠다; n번째 세션의 난수들과 리더-태그 간 소통 정보 각각 $n1^{(n)}$, $n2^{(n)}$, $A^{(n)}$, $B^{(n)}$, $C^{(n)}$, $D^{(n)}$, $E^{(n)}$로 표기한다.

M^2AP의 2개 연속 세션 도청 정보를 이용한 ID와 일부 비밀키 복원

M^2AP은 $\{n1^{(l)}, n2^{(l)}, K1^{(l)}, K3^{(l)}, ID: l=n, n+1\}$의 (j_0-1)이하 비트를 알면 $\{n1^{(l)}, n2^{(l)}, K1^{(l)}, K3^{(l)}, ID: l=n, n+1\}$의 j_0번째 비트를 알 수 있다. $j_0=0$인 경우는 사전 정보 없이 $\{n1^{(l)}, n2^{(l)}, K1^{(l)}, K3^{(l)}, ID: l=n, n+1\}$의 최하위 비트를 알 수 있다. 즉, 두 세션의 도청을 통하여 $n1^{(n)}, n2^{(n)}, K1^{(n)}, K3^{(n)}, n1^{(n+1)}, n2^{(n+1)}, K1^{(n+1)}, K3^{(n+1)}, ID$의 모든 비트를 구할 수 있다.

위 공격의 분석은 다음의 간단한 성질에서 출발한다.

보조정리 2. A, B, C, D가 m비트이고 A와 $(A \wedge B) \vee C$, $(A \vee B) \wedge D$가 공개되어 있다고 하자. $[A]_j=0$인 경우에는 $(A \wedge B) \vee C$로부터 C_j를 알 수 있고, $[A]_j=1$인 경우에는 $(A \vee B) \wedge D$로부터 D_j를 알 수 있다.

예를 들어, $B^{(n)}=(IDS^{(n)} \wedge K2^{(n)}) \vee n1^{(n)}$, $D^{(n)}=(IDS^{(n)} \vee ID) \wedge n2^{(n)}$에 보조정리 2를 적용하면 $[(IDS^{(n)}]_k=0$인 경우에 $[n1^{(n)}]_k$을 얻을 수 있고, $[(IDS^{(n)}]_\ell=1$인 경우에 $[n2^{(n)}]_\ell$을 얻을 수 있게 된다.

이제 위 공격을 $[IDS^{(n)}]_{j_0}$과 $[IDS^{(n+1)}]_{j_0}$의 값에 따라 세 가지 경우로 나누어 분석하겠다. 먼저, 특정 j_0에 대하여, $\{n1^{(l)}, n2^{(l)}, K1^{(l)}, K3^{(l)}, ID: l=n, n+1\}$의 (j_0-1)이하 비트를 안다고 가정하자.

경우 1: $[IDS^{(n)}]_{j_0}=0$인 경우

(1) 보조정리 2를 $B^{(n)}=(IDS^{(n)} \wedge K2^{(n)}) \vee n1^{(n)}$에 적용하여 $[n1^{(n)}]_{j_0}$을 구한다.

(2) $[ID]_{j<j_0}$가 알려졌으므로 공격자는 $(IDS^{(n)}+ID)$의 j_0 위치에 올라오는 캐리 비트를 계산할 수 있다. 이제 $[n1^{(n)}]_{j_0}$와 $A^{(n)}=IDS^{(n)} \oplus K1^{(n)} \oplus n1^{(n)}$, $E^{(n)}=(IDS^{(n)}+ID) \oplus n1^{(n)}$을 이용하여 공격자는 $[K1^{(n)}]_{j_0}$, $[ID]_{j_0}$을 얻을 수 있다.

(3) 이 값을 알면 나머지 값들의 j_0번째 비트들은 리더와 태그 간 소통 정보 및 갱신 식으로부터 알 수 있다. 자세한 계산은 생략한다.

경우 2: $[IDS^{(n+1)}]_{j_0}=0$인 경우

(1) $B^{(n+1)}=(IDS^{(n+1)} \wedge K2^{(n+1)}) \vee n1^{(n+1)}$에 보조정리 2를 적용하여 $[n1^{(n+1)}]_{j_0}$을 구한다.

(2) 경우 1과 같이 $[n1^{(n+1)}]_{j_0}$, $A^{(n+1)}$, $E^{(n+1)}$으로부터 $[K1^{(n+1)}]_{j_0}$, $[ID]_{j_0}$을 얻는다.

(3) $[ID]_{j_0}$을 얻으면, $E^{(n)}=(IDS^{(n)}+ID) \oplus n1^{(n)}$에서 $[n1^{(n)}]_{j_0}$을 구할 수 있고, 경우 1에서와 같이 나머지 값들의 j_0번째 비트들을 알 수 있다.

경우 3: $[IDS^{(n)}]_{j_0}=[IDS^{(n+1)}]_{j_0}=1$인 경우

(1) 이 경우, $D^{(n)}=(IDS^{(n)} \vee ID) \wedge n2^{(n)}$, $D^{(n+1)}=(IDS^{(n+1)} \vee ID) \wedge n2^{(n+1)}$에 보조정리 2를 적용하여 $[n2^{(n)}]_{j_0}$, $[n2^{(n+1)}]_{j_0}$을 구한다.

(2) $C^{(n)}= IDS^{(n)}+K3^{(n)}+n2^{(n)}$, $C^{(n+1)}= IDS^{(n+1)}+K3^{(n+1)}+n2^{(n+1)}$, $[n2^{(n)}]_{j_0}$, $[n2^{(n+1)}]_{j_0}$으로부터 $[K3^{(n)}]_{j_0}$, $[K3^{(n+1)}]_{j_0}$을 구한다. 여기에서도 $K3^{(n)}$, $K3^{(n+1)}$, $n2^{(n)}$, $n2^{(n+1)}$의 j_0 미만 비트들을 알고 있으므로 j_0번째 비트 계산에 영향을 주는 캐리 계산을 할 수 있어 $[K3^{(n)}]_{j_0}$, $[K3^{(n+1)}]_{j_0}$을 구할 수 있는 것이다.

(3) $A^{(n)}=IDS^{(n)} \oplus K1^{(n)} \oplus n1^{(n)}$과 $E^{(n)}=(IDS^{(n)}+ID) \oplus n1^{(n)}$의 j_0번째 비트를 다시 표현하면, 적당한 a,b에 대하여, $[K1^{(n)}]_{j_0}=[n1^{(n)}]_{j_0} \oplus a$, $[ID]_{j_0}=[n1^{(n)}]_{j_0} \oplus b$로 쓸 수 있다. 이 식을 키 갱신식 $K3^{(n+1)}=(K3^{(n)} \oplus n1^{(n)})+(K1^{(n)} \oplus ID)$의 j_0번째 비트 식에 대입하면 다음과 같다.

$$\begin{aligned}[K3^{(n+1)}]_{j_0} &= [K3^{(n)}]_{j_0} \oplus [n1^{(n)}]_{j_0} \oplus [K1^{(n)}]_{j_0} \oplus [ID]_{j_0} \oplus c \\ &= [K3^{(n)}]_{j_0} \oplus [n1^{(n)}]_{j_0} \oplus [n1^{(n)}]_{j_0} \oplus [n1^{(n)}]_{j_0} \\ &\quad \oplus a \oplus b \oplus c \\ &= [K3^{(n)}]_{j_0} \oplus [n1^{(n)}]_{j_0} \oplus a \oplus b \oplus c\end{aligned}$$

여기에서 c는 하위 비트들로부터 발생한 캐리이다. 이제 공격자는 $[K3^{(n)}]_{j_0}$, $[K3^{(n+1)}]_{j_0}$과 위 식에서 $[n1^{(n)}]_{j_0}$을 얻고, $[K1^{(n)}]_{j_0}$, $[ID]_{j_0}$을 계산한다.

(4) 나머지 값들의 j_0번째 비트들은 리더와 태그 간 소통 정보 및 갱신 식으로부터 알 수 있다.

위 분석은 공격자가 하위 비트로부터 발생되는 캐리를 알고 있다고 가정하고 있으나 j_0가 lsb인 경우에는 그러한 가정이 필요하지 않다. 그러므로 연속된 2세션의 도청 정보를 이용하면, 공격자는 $n1^{(n)}, n2^{(n)}, K1^{(n)}, K3^{(n)}, n1^{(n+1)}, n2^{(n+1)}, K1^{(n+1)}, K3^{(n+1)}, ID$의 모든 비트를 얻을 수 있게 된다. 이 외의 비밀 정보 $K2^{(n)}$, $K2^{(n+1)}$, $K4^{(n)}$, $K4^{(n+1)}$에 대해서는 $[IDS^{(n)}]_{j_0}$과

$[IDS^{(n+1)}]_{j_0}$에 의존하여 일부 정보만을 알 수 있다. 여기서 중요한 관찰로서 키 $K1$, $K3$의 갱신이 키 $K2$, $K4$와 독립적으로 이루어지고, $K2$, $K4$는 리더의 태그 인증에 사용되지 않는다는 점을 지적한다. 이 점을 이용하면 공격자는 비밀 정보 $n1^{(n+1)}, n2^{(n+1)}, K1^{(n+1)}, K3^{(n+1)}, ID$을 이용하여 도청 세션 이후로 계속해서 태그를 위장할 수도 있을 것이다.

4.3. EMAP에 대한 새로운 태그 *ID* 추출 공격

EMAP에 대한 공격 방법도 M²AP에 대한 공격 방법과 유사한데, M²AP과는 달리 ID와 비밀키들의 일부 비트들을 결정하기 어렵다. 결정할 수 없는 비트 수를 최대한 줄임으로써 ID 후보의 수를 줄이는 것이기 공격의 핵심으로 다음의 보조 정리가 사용된다.

보조정리 3. X, Y, Z, X', Y', Z', S, c 가 $2n$비트 수이고 다음을 만족한다고 하자.

(1) X, X', c와 $X \vee Y$, $X \wedge Z$, $X' \vee Y'$, $X' \wedge Z'$이 알려져 있다.

(2) $Y'=Y \oplus S$, $Z'=Z \oplus S \oplus c$인 관계가 있다.

(3) $Y \oplus Z \oplus S$와 $G_p(Y), G_p(Z)$도 추가적으로 주어져 있다. 여기에서 $2n$비트 x에 대하여 G_p는 상위 n 비트와 하위 n비트의 XOR, 즉 $G_p(x)=x(2n\text{-}1:n) \oplus x(n\text{-}1:0)$이다.

그러면, X, X'의 비트들에 대하여

$[X]_j \oplus [X']_j=0$ 또는 $[X]_{j+n} \oplus [X']_{j+n}=0$ 또는 $[X]_j \oplus [X]_{j+n}=1$을 만족하는 $j(0 \le j \le n-1)$번째 비트에 대하여, $[Y]_j, [Y]_{j+n}, [Z]_j, [Z]_{j+n}, [S]_j, [S]_{j+n}$을 구할 수 있다.

보조정리 3에서 (1)은 리더와 태그 간 소통 정보에 대한 식, (2)는 키 갱신식이고 (3)은 공격 단계에서 얻을 수 있는 값들이다. 이 보조정리의 증명은 공격 방식 이후에 서술하기로 한다.

이제 연속된 2개의 세션을 도청하여 얻은 소통정보에 보조정리 2와 보조정리 3을 적용하여 EMAP 프로토콜을 분석해보자.

단계 1: $K1^{(n)}$, $K1^{(n+1)}$ **복원**

보조정리 2를 $D^{(n)}$과 $B^{(n)}$에 적용하면, 모든 $j(0 \le j \le m)$에 대하여

- $[IDS^{(n)}]_j=0$인 경우, $D^{(n)}$로부터 $[n2^{(n)}]_j$을 얻고, $IDS^{(n)}$의 갱신식으로부터 $[K1^{(n)}]_j$을 얻는다.
- $[IDS^{(n)}]_j=1$인 경우, $B^{(n)}$로부터 $[n1^{(n)}]_j$을 얻고, $A^{(n)}$로부터 $[K1^{(n)}]_j$을 얻는다.

즉, $IDS^{(n)}$으로부터 $K1^{(n)}$를 얻을 수 있다. 같은 방법으로, $IDS^{(n+1)}$로부터 $K1^{(n+1)}$을 얻을 수 있다.

단계 2: $K3^{(n)}$, $n1^{(n)}$, $n2^{(n)}$, $K3^{(n+1)}$, $n1^{(n+1)}$, $n2^{(n+1)}$ **복원**

$K1^{(n)}$, $K1^{(n+1)}$을 복원하면, $A^{(n)}$, $A^{(n+1)}$, $C^{(n)}$, $C^{(n+1)}$와 $IDS^{(n)}$의 갱신식으로부터 위 값들을 다음과 같이 구할 수 있다.

- $n1^{(n)} = A^{(n)} \oplus IDS^{(n)} \oplus K1^{(n)}$,
- $n1^{(n+1)} = A^{(n+1)} \oplus IDS^{(n+1)} \oplus K1^{(n+1)}$,
- $n2^{(n)} = IDS^{(n+1)} \oplus IDS^{(n)} \oplus K1^{(n)}$,
- $n2^{(n+1)} = IDS^{(n+2)} \oplus IDS^{(n+1)} \oplus K1^{(n+1)}$,
- $K3^{(n)} = C^{(n)} \oplus IDS^{(n)} \oplus n2^{(n)}$,
- $K3^{(n+1)} = C^{(n+1)} \oplus IDS^{(n+1)} \oplus n2^{(n+1)}$.

단계 3: $ID(95:48)$, $F_p(K2^{(n)})$, $F_p(K4^{(n)})$**복원**

$K1^{(n)}$, $K3^{(n)}$, $n1^{(n)}$, $n2^{(n)}$, $K1^{(n)}$, $K3^{(n+1)}$, $n1^{(n+1)}$, $n2^{(n+1)}$을 복원하면, $K3^{(n)}$의 갱신식으로부터 위 값들을 다음과 같이 구할 수 있다.

- $ID(95:48) \| F_p(K4^{(n)}) \| F_p(K2^{(n)})$
  $= K3^{(n+1)} \oplus K3^{(n)} \oplus n1^{(n)}$

단계 4: $K2^{(n)}$, $K4^{(n)}$**의 상위 48비트 복원**

$E^{(n)}=(IDS^{(n)} \wedge n1^{(n)} \vee n2^{(n)}) \oplus ID \oplus K1^{(n)} \oplus K2^{(n)} \oplus K3^{(n)} \oplus K4^{(n)}$에서 이미 구한 값들을 제외하면 남는 값은 다음과 같다.

$ID \oplus K2^{(n)} \oplus K4^{(n)}$

보조정리 2로부터 각 비트에 대하여 $K2^{(n)}$와 $K4^{(n)}$ 중 하나를 알 수 있고, $ID(95:48)$을 알고 있으므로, $K2^{(n)}$, $K4^{(n)}$의 상위 48비트를 얻을 수 있다.

단계 5: 다음의 조건들

$[IDS^{(n)}]_j \oplus [IDS^{(n+1)}]_j = 0$ **또는**

$[IDS^{(n)}]_{j+24} \oplus [IDS^{(n+1)}]_{j+24} = 0$ **또는**

$[IDS^{(n)}]_j \oplus [IDS^{(n)}]_{j+24} = 1$

에서의 $j(0 \le j \le 23)$비트에 대한 $[K2^{(n)}]_j$, $[K4^{(n)}]_j$, $[ID(47:0)]_j$, $[K2^{(n)}]_{j+24}$, $[K4^{(n)}]_{j+24}$, $[ID(47:0)]_{j+24}$ 복원

보조정리 3의 적용을 위하여 다음과 같이 치환한다.

$X=IDS^{(n)}(47:0)$, $X'=IDS^{(n+1)}(47:0)$,

$Y=K2^{(n)}(47:0)$, $Y'=K2^{(n+1)}(47:0)$,

$Z=K4^{(n)}(47:0)$, $Z'=K4^{(n+1)}(47:0)$,

$S=ID(47:0) \oplus n2^{(n)}$, $c=n1^{(n)} \oplus n2^{(n)}$.

$B^{(n)}$,$B^{(n+1)}$, $D^{(n)}$,$D^{(n+1)}$, $K2^{(n)}$, $K4^{(n)}$의 갱신식을 새로운 변수로 치환하면 보조정리 3의 (1), (2)를 얻고 단계 4의 결과에 적용하면 (3)을, 위 조건에 적용하면 보조 정리 3의 조건을 얻는다. 그러므로 위 조건을 만족하는 $j(0 \le j \le 23)$비트에 대하여 $[K2^{(n)}]_j$, $[K4^{(n)}]_j$, $[ID(47:0)]_j$, $[K2^{(n)}]_{j+24}$, $[K4^{(n)}]_{j+24}$, $[ID(47:0)]_{j+24}$ 을 구할 수 있다.

단계 6: $K2^{(n)}$, $K4^{(n)}$, $ID(47:0)$의 복원

단계 5의 조건을 만족하지 않을 확률이 1/8이고, j $(0 \le j \le 23)$비트에 대하여 $[K2^{(n)}]_j$, $[K4^{(n)}]_j$ 중 하나를 알 수 있어, $K2^{(n)}(23:0)$, $K4^{(n)}(23:0)$의 결정되지 않는 비트 수의 합은 평균은 3이다. 23개의 $(K2^{(n)}(23:0),\ K4^{(n)}(23:0))$후보들을 결정하면, $F_p(K2^{(n)})$, $F_p(K4^{(n)})$에 의하여 $K2^{(n)}$, $K4^{(n)}$가 완전히 결정되고, $E^{(n)}$으로부터 $ID(47:0)$도 복원할 수 있다. 즉, 평균 23개의 ID후보를 얻는다.

만일, k개의 연속된 세션을 도청하였다고 가정하자. 그러면 단계 5의 조건은 <두 순열 $([IDS^{(n)}]_j,\ldots, [IDS^{(n-k+1)}]_j)$, $([IDS^{(n)}]_{j+24},\ldots,[IDS^{(n-k+1)}]_{j+24})$에서 0 또는 1이 연속으로 나오는 경우가 적어도 한번 있거나 $\{([IDS^{(n)}]_j,[IDS^{(n)}]_{j+24}),\ldots,([IDS^{(n+k-1)}]_j,\ [IDS^{(n+k-1)}]_{j+24})\}$ 중에 (0,1) 또는 (1,0)의 쌍이 있어야 한다>로 바뀐다. 이 경우 조건을 만족하지 않을 확률은 $1/2^{3k-2}$가 되어 공격자는 평균 $2^{48/2^{3k-2}}$개의 ID후보를 얻게 된다. 예를 들어, 3개의 연속된 세션을 도청하면 공격자는 평균적으로 2개 이하의 ID후보를 얻게 된다.

보조정리 3의 증명.

조건이 3가지 경우이므로 경우 별로 나누어 증명하기로 한다.

경우 1. $[X]_j \oplus [X']_j=0$ $(0 \le j \le n-1)$일 때 $[Y]_j$,$[Y]_{j+n}$,$[Z]_j$,$[Z]_{j+n}$,$[S]_j$,$[S]_{j+n}$의 복원

이 경우는 다시 $[X]_j=[X']_j=0$인 경우와 $[X]_j=[X']_j=1$인 경우로 나뉜다. 먼저 $[X]_j=[X']_j=0$인 경우 (1)로부터 $[Y]_j$, $[Y']_j$를 얻을 수 있다. (2)로부터 $[S]_j$를 구하고 (3)의 $G_p(Y)$를 이용하면 $[Y]_{j+n}$을, $Y \oplus Z \oplus S$를 이용하면, $[Z]_j$를 계산할 수 있다. 마지막으로 $G_p(Z)$를 이용하면 $[Z]_{j+n}$을, $Y \oplus Z \oplus S$를 이용하면 $[S]_{j+n}$을 계산할 수 있다.

$[X]_j=[X']_j=1$인 경우에는 (1)로부터 $[Z]_j$, $[Z']_j$를, (2)로부터 $[S]_j$를 구하고 (3)의 $G_p(Z)$를 이용하면 $[Z]_{j+n}$을, $Y \oplus Z \oplus S$를 이용하면, $[Y]_j$를 계산할 수 있다. 마지막으로 $G_p(Y)$를 이용하면 $[Y]_{j+n}$을, $Y \oplus Z \oplus S$를 이용하면 $[S]_{j+n}$을 계산할 수 있다.

경우 2. $[X]_{j+n} \oplus [X']_{j+n}=0$ $(0 \le j \le n-1)$일 때 $[Y]_j$,$[Y]_{j+n}$,$[Z]_j$,$[Z]_{j+n}$,$[S]_j$,$[S]_{j+n}$의 복원

이 경우는 경우 1의 증명에서 비트 인덱스 j와 $j+n$을 치환하여 증명할 수 있다.

경우 3. $[X]_j \oplus [X]_{j+n}=1$ $(0 \le j \le n-1)$일 때 $[Y]_j$, $[Y]_{j+n}$,$[Z]_j$,$[Z]_{j+n}$,$[S]_j$,$[S]_{j+n}$의 복원

이 경우는 $[X]_j=0$,$[X]_{j+n}=1$과 $[X]_j=1$,$[X]_{j+n}=0$인 경우로 나뉜다. 먼저, $[X]_j=0$,$[X]_{j+n}=1$인 경우에는 (1)로부터 $[Y]_j$, $[Z]_{j+n}$을 얻을 수 있다. (3)의 $G_p(Y)$, $G_p(Z)$로부터 $[Y]_{j+n}$,$[Z]_j$를 구할 수 있고 $Y \oplus Z \oplus S$를 이용하면 $[S]_j$,$[S]_{j+n}$을 계산할 수 있다. $[X]_j=1$,$[X]_{j+n}=0$인 경우에도 증명이 유사하므로 생략한다.

V. 결 론

본 논문에서는 LMAP, M^2AP, EMAP 에 대해 T. Li 등이 제안한 확률적 비동기화 공격[8,9]의 오류를 수정하여 항상 비동기화 공격이 가능함을 보이고, [9]의 LMAP에 대한 태그 ID 및 일부 비밀정보 복원 공격을 대폭 개선하였다. [9]에서는 리더와의 통신 2회 태그와의 통신 $(m+2)$회를 수회 반복하여 최상위 비트를 제외한 태그 ID의 각 비트를 확률적으로 얻는 공격을 제시

하였으나, 본 논문에서는 리더와의 통신 1회 태그와의 통신 (2m-1)회로 태그 ID의 최상위 비트를 제외한 모든 비트를 완전하게 복원할 수 있음을 보였다. 그리고 M²AP, EMAP에 대해서는 [8,9]에서 제시된 능동 공격이 아닌 연속된 2~3개 세션의 정보 수집만으로 태그 ID와 일부 비밀키를 복원할 수 있음을 보였다. [8,9]에서는 리더와 태그의 통신값 만으로 M²AP, EMAP에 대한 공격을 구성한 반면, 본 논문에서는 키갱신 과정의 단점을 추가로 이용하여 수동 공격이 가능하였다.

LMAP 등은 +,⊕,∧,∨ 등의 연산만으로 이루어진 매우 효율적인 프로토콜이나, HB⁺[4] 등과 달리 안전성을 보장할 수 있는 기반 문제에 대한 고려가 없었다. 결과적으로, 비동기화 공격을 비롯하여 태그 ID 및 일부 비밀키를 복원할 수 있는 단점이 발견되었다. LMAP에 대한 공격은 태그의 인증 여부가 중요한 요소로 작용하므로 태그는 인증 거부 메시지 대신 랜덤값 등을 응답하여 이러한 공격에 대응할 수 있다[9]. 그러나 M²AP, EMAP에 대한 공격은 유효한 세션의 도청만 요구하므로 이러한 대응 방안이 적용될 수 없다.

RFID 시스템에서는 암호화가 아닌 인증이 주요 목적이므로, 해쉬 함수, 비밀키 암호를 사용하지 않고 간단한 연산만으로 인증 프로토콜을 구성하는 것이 흥미 있는 연구 방향이나, [10,11,12]에서와 같이 안전성을 충분히 고려하지 않는다면 쉽게 취약점이 발견될 수 있다. 향후 안전성을 고려하여 프로토콜을 구성하면, 매우 효율적인 RFID 인증 솔루션이 될 수 있을 것이다.

참고문헌

[1] J. Bringer, H. Chabanne, E. Dottax, "HB⁺⁺: A Lightweight Authentication Protocol Secure against Some Attacks," *Proceedings of SecPerU* 2006, pp.28-33.

[2] M. Fredhofer and C. Rechberger, "Case Against Currently Used Hash Functions in RFID Protocols", *Proceedings of Workshop on RFID Security* 2006. pp.372-381.

[3] International Standard ISO/IEC 18000-6: Information technology - Radio frequency identification for item management - Part 6: Parameters for air interface communications at 860MHz to 960MHz, 2004.

[4] A. Juels and S. Weis, "Authenticating Pervasive Devices with Human Protocols", *Proceeding of CRYPTO* 2005, LNCS3621, pp.293-308, 2005.

[5] M. Jung, H. Fiedler and R. Lerch, "8-bit microcontroller system with area efficient AES coprocessor for transponder applications", *Ecrypt Workshop on RFID and Lightweight Crypto*, Proceeding, Graz, pp.32-43, 2005.

[6] J. Katz and J. S. Shin, "Parallel and Concurrent Security of the HB and HB⁺ Protocols", *Proceeding of EUROCRYPT* 2006, LNCS4004, pp.73-87, 2006.

[7] D. Kwon, D. Han, J. Lee and Y. Yeom, "Vulnerability of an RFID Authentication Protocol Proposed at SecUbiq 2005", *Proceeding of SecUbiq* 2006, LNCS4097, pp.262-270, 2006.

[8] T. Li, R. H. Deng. "Vulnerability Analysis of EMAP-An Efficient RFID Mutual Authentication Protocol". *Proceeding of AReS* 2007, April 2007.

[9] T. Li, G. Wang. "Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols", *Proceeding of IFIP SEC* 2007. May 2007.

[10] P. Peris-Lopez, J. C. Hermandez-Castro, J. M. Estevez-Tapaidor, A. Ribagorda, "LMAP: A Real Leightweight Mutual Authentication Protocol for Low-cost RFID tags." *Workshop on RFID Security*, RFIDSec 06, pp.137-148, July 2006.

[11] P. Peris-Lopez, J. C. Hermandez-Castro, J. M. Estevez-Tapaidor, A. Ribagorda, "M²AP: A Minmalist Mutual- Authentication Protocol for Low-cost RFID tags." *Proceedings of UIC* 2006, pp.912-923, 2006.

[12] P. Peris-Lopez, J. C. Hermandez-Castro, J. M. Estevez-Tapaidor, A. Ribagorda, "EMAP: An Efficient Mutual- Authentication Protocol for Low-cost RFID tags." *Proceedings of OTM Federated Conferences and Workshop: IS Workshop* 2006. pp. 352-361, 2006.

〈著者紹介〉

권 대 성 (Daesung Kwon) 정회원
1992년 2월 : 서울대학교 수학과 졸업
1994년 2월 : 서울대학교 수학과 석사
1999년 2월 : 서울대학교 이학박사
1999년 4월 ~ 2001년 2월 : 고등과학원 박사 후 연구원
2001년 3월 ~ 현재 : 국가보안기술연구소 선임연구원
<관심분야> 공개키 암호, RFID

이 주 영 (Jooyoung Lee) 정회원
1996년 2월 : 서울대학교 수학과 졸업
1998년 2월 : 서울대학교 수학과 석사
2005년 8월 : Waterloo 대학 암호학 박사
2005년 11월 ~ 현재 : 국가보안기술연구소 선임연구원
<관심분야> RFID, 센서네트워크

구 본 욱 (Bon Wook Koo) 정회원
2001년 2월 : 한양대학교 수학과 졸업
2003년 2월 : 한양대학교 수학과 석사
2006년 2월 : 한양대학교 수학과 박사과정 수료
2006년 11월 ~ 현재 : 국가보안기술연구소 연구원
<관심분야> RFID, 블록암호