프라이버시 보호를 위한 RFID 익명화 메커니즘

이동혁*, 송유진*

*동국대학교 전자상거래학과

RFID Anonymization Mechanism for Privacy Protection

Dong-Hyeok Lee, You-Jin Song*

*Dongguk University.

요 약

유비쿼터스 컴퓨팅 환경에서는 센서를 통하여 실시간의 상황인식 서비스를 제공하며, 이를 위해 사용자의 위치 정보 수집이 필요하다. NTT에서는 RFID에 대한 익명화를 통한 프라이버시 보호 메커니즘을 제안하였다. 그러나, 불법적으로 접근하는 리더가 존재할 경우 i값의 비동기화를 통한 태그에 대한 Random Tampering공격이 가능하다. 본 논문에서는 NTT 연구소의 RFID 익명화 방법을 개선하여 태그의 Random Tampering 공격 방지가 가능하고, 태그와 리더 상호간 인증이 가능하며, 연산 과정을 절감시킨 새로운 RFID 익명화 프로토콜을 제안한다. 제안한 방법을 통하여 보다 안전하고 효율적으로 RFID기반 센서 네트워크 환경에서 사용자의 프라이버시를 보호할 수 있다.

I. 서론

유비쿼터스 컴퓨팅 환경에서는 RFID 센서를 통하여 사용자의 위치 및 상황에 맞는 센서 기반 서비스(이동통신 단말기반 자율형, 실시간, 상황인식, Interactive 정보교환 등)이 가능한 상황인식 서비스가 제공된다.

그러나 이러한 유비쿼터스 컴퓨팅의 특성은 데이터의 보안이 취약할 경우 기존 컴퓨팅 환경보다 더 큰 문제로 확대될 것이다. 사용자의 위치를 추적하면서 사용자를 인지하여 서비스를 제공하기 때문에 사용자의 위치 정보의 수집이 필요하게 된다. 수집된 데이터가 노출될 경우 사용자에 대한 감시 시스템(Surveillance System)으로 동작할 것이며, 이러한 문제는 실제 유비쿼터스 컴퓨팅이 현실화되는 데 있어 가장 큰 걸림돌로 작용할 수 있다. 따라서, 유비쿼터스 환경에서는 개인 프라이버시 등의 문제점에 대한 시급한 해결이 필요하다.

이러한 관점에서 NTT 연구소에서는 RFID에 대한 익명화를 통한 프라이버시 보호 메커니즘을 제안하였다[1]. 그러나, NTT 메커니즘은 불법적으로 접근하는 리더가 존재할 경우, i값의 비동기화를 통한 태그에 대한 Random Tampering 공격이 가능하다.

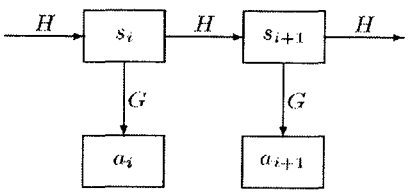
본 논문에서는 NTT의 RFID 익명화 메커니즘을 개선하여 태그의 Random Tampering 공격을 방지하고, 태그와 리더 상호간 인증이 가능하며, 보다 효율적으로 사용자의 프라이버시를 보호할 수 있는 메커니즘을 제안하였다. 제안한 방법을 통하여 보다 안전하고 효율적으로 RFID 기반 센서 네트워크 환경에서 사용자의 프라이버시를 보호할 수 있다.

II. 관련 연구

2.1. Privacy-Friendly Tags[1]

RFID 태그는 각각 유일한 ID를 가지고 있다. 따라서, 무선접속을 통하여 어떤 누구도 쉽게 ID 정보를 알 수 있다. 이러한 방식은 위치 추적과 같은 정보의 처리에 매우 유용하게 활용될 수 있다. 그러나, 만약 태그의 정보로부터 주요한 정보가 유추 가능한 경우, 허가되지 않은 자가 태그에 대한 추적을 시도할 때 사용자에 대한 프라이버시 침해로 이어질 수 있다.

개인의 입장에서는 자신 이외에 다른 어떤 누구도 태그 정보에 대하여 파악 가능하기를 원하지 않는다. 따라서 RFID 태그에 대한 보호가 필요하다. 이는 태그의 익명화를 통하여 실현 가능하다. NTT가 제안한 메커니즘은 [그림 1]과 같다.



[그림 1] NTT의 태그 익명화 메커니즘

태그의 메모리 내에는 고유값 S에 대한 i회의 해쉬연산을 반복한 값인 S_i가 저장되어 있다. 리더가 태그에 접근하게 될 경우, 태그는 S_i를 읽어들인다. 이후, 해쉬연산 G를 통하여 출력값 a_i를 생성하고 리더에 제공한다. 그리고, S_i는 해쉬연산 H를 통하여 S_{i+1}로서 다시 메모리상에 저장하고, 기존의 S_i는 삭제한다.

한편, Back-end Server는 다음과 같은 절차를 거친다. 서버 내의 데이터베이스에는 ID와 S_1이 각각 연결되어 저장되어 있다. 즉, (ID,S_1)의 형태로 존재하며, a_i가 $G(H^{i-1}(S_1))$, 즉 a^*_i인것을 확인한 이후 ID를 식별할 수 있다. Back-end Server는 [그림 2]와 같은 연산 과정을 거친다.

1. 리더로부터 a_i를 수신한다.
2. 모든 ID에 대하여 a^*_i에 대하여 일치하는 a_i를 찾을때까지 다음을 수행한다.

$S_i = H_{i-1}(S_1)$
$a^*_i = H(S_1)$
$a_i = a^*_i$?
3. 해당 S_1과 연결된 ID를 가져온다.

[그림 2] Back-end Server 연산 절차

이러한 경우, Back-end Server는 한번의 검색시 S_1에 대한 i회의 해쉬 연산이 요구된다. 따라서, f회의 검색이 있을 경우, 총 요구되는 해쉬연산량은 $i \times f$이다.

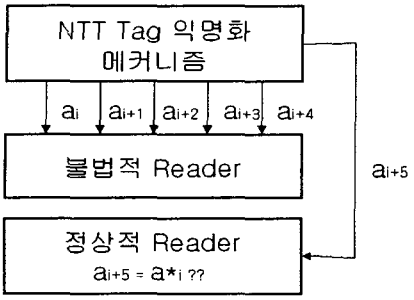
따라서, NTT 메커니즘에서는 태그에 대한 ID 정보는 태그 인식 과정에서 전혀 노출되지 않는다. 따라서, 태그에 대한 익명화가 가능하다.

2.2. 문제 제기

NTT가 제안한 방법은 태그의 판독을 위해서 리더에는 i회의 해쉬 연산이 필요하다. 이러한 방식이 가능하기 위해서 태그와 리더간의 i값에 대한 지속적인 연동이 필요하다.

그러나 여기에는 비동기에 의한 Random Tampering공격 문제가 존재한다. Random Tampering공격이란, i값의 동기화가 되지 않을 경우, 정상적으로 인식이 되지 않는 허점을 이용한 연속적 불법 접근 시도 공격이다. 즉, 불법적인 리더가 접근 시 i의 숫자는 증가하게 되며, 이러한 경우 Back-end Server와 태그가 가진 i의 값이 일치하지 않아서 정상적인 값을 판단할 수 없으며 결과적으로 Back-end Server는 태그의 ID값을 판별할 수 없게 된다.

그 이유는 다음과 같다. 태그에서는 S_i값에 대한 해쉬연산 G를 통하여 생성한 익명화된 태그 식별정보 a_i를 제공한 이후, S_i값이 S_{i+1}로 변경된다. 예를 들어, 5회째 불법적으로 접근하는 리더가 있을 경우, $a_i, a_{i+1}, a_{i+2}, a_{i+3}, a_{i+4}$를 제공하게 되며, 차후 정상적으로 접근하는 리더에 대해서는 a_{i+5}를 제공하게 될 것이다. 따라서, i값의 불일치로 인하여 정상적 리더는 태그의 정보를 식별할 수 없다.([그림 3] 참고)



[그림 3] NTT 메커니즘에 대한 Random Tampering 공격

III. 새로운 메커니즘 제안

본 논문에서 제안하는 메커니즘은 다음과 같다.

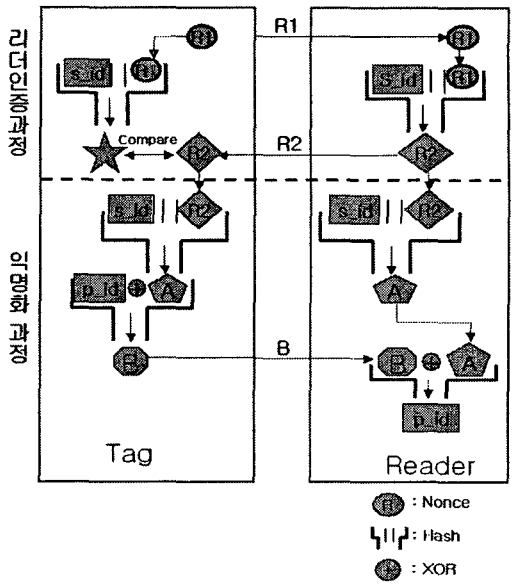
3.1. 초기화 절차

Step 1. 태그 T에 사용자의 고유번호(ID 정보) p_id, 리더 고유번호 s_id를 입력한다. (Tag(T) <- p_id, s_id)
Step 2. 리더 R에 리더 고유번호 s_id를 입력한다. (Reader(R) <- s_id)

3.2. 태그 식별 절차

Step 1. T는 랜덤한 난스(nonce) R1을 생성하고 R에 전달한다. (T -> R : R1)
Step 2. R은 h(s_id||R1)를 통하여 R2를 생성하여 T에 전달한다.(R -> T : h(s_id||R1) = R2)
Step 3. Step 3-1. T는 R2를 기반으로 h(s_id||R2)=A를 계산한다.(h(s_id||R2)=A)

Step 3-2. 계산된 값을 p_id와 XOR연산을 수행한 값 B를 R에 전달한다.(T -> R : A XOR p_id = B)
Step4. R은 h(s_id||R2)를 계산하고 B와 XOR 연산을 수행하여 p_id를 구한다. (R calculate A XOR h(s_id||R2) = p_id)



[그림 3] 제안 메커니즘

IV. 분석

4.1.안전성분석

(1) 태그 Random Tampering 공격 방지

NTT 메커니즘에서, 태그에서는 정상적인 사용자를 판단할 수 있는 메커니즘을 가지고 있지 않으며, 불법적으로 접근하는 RFID리더에 대하여 정당성을 확인할 수 없다. 그러나, 태그의 판독을 위해서 리더에는 i회의 해쉬 연산이 필요하며, 이러한 방식이 가능하기 위해서는 태그와 리더간의 i값에 대한 지속적인 연동이 필요하다. 따라서, NTT 메커니즘은 태그에 대한 Random Tampering 공격을 매우 간편하게 시도할 수 있다. 즉, NTT 메커니즘을 사용함으로써 더욱 태그 Random Tampering 공격이 용이하게 된다.

그러나 제안한 메커니즘은 i값에 따라 해쉬연산량이 증가하는 방식을 사용하지 않으며, 해쉬연산 회수가 태그와 리더 당 각 2회로 고정되어 있다. 따라서, i값이 사용되지 않으며, 연산

회수는 항상 고정되어 있으므로 i값의 비동기화에 따른 Random Tampering공격이 불가능하다.

(2) 리더 인증

NTT 메커니즘에서는 리더에 대한 특별한 인증 방법을 명시하고 있지 않다. 따라서, 리더에 대한 인증이 불가능하다.

그러나 제안한 메커니즘은 3.2.에 명시된 Step 2 과정에서 리더로부터 받은 R2값을 통하여 리더를 인증할 수 있다. R2를 연산하기 위해서 리더는 s_id값이 필요하다. 그러나 불법적인 리더는 s_id를 가지고 있지 않으므로 R2를 연산할 수 없다. 따라서, 태그가 일치하지 않는 R2를 전송받을 시 동일하지 않음을 판별하고 절차를 더이상 진행하지 않는다. 따라서, 태그의 p_id는 노출되지 않게 되며, 리더의 접근을 중단시키므로 태그 ID를 안전하게 보호한다.

(3) 프라이버시 보호

사용자의 신원 확인은 태그 ID확인을 통하여 가능하다. 그러나, 본 논문에서 제안하는 메커니즘은 ID의 익명화의 방법으로서, Back-end-Server와의 태그 인식 과정에서 전달되는 해쉬 처리된 값을 통하여 p_id를 계산하며, 네트워크상에는 고유 ID정보를 전혀 노출시키지 않는다. 따라서, 태그와 무선 접속이 가능한 거리에 불법적인 리더가 위치하더라도 태그 정보를 읽을 수 없다. 이것은 태그 ID 인식을 통한 사용자 개인정보(위치정보 등)을 인지할 수 없음을 의미하며, 이를 통하여 사용자의 프라이버시를 안전하게 보호할 수 있다. [표 1]

[표 1] 안전성 비교

	태그 Random Tampering 공격 방지	리더 인증	프라이버시 보호
NTT 메커니즘	×	×	○
제안 메커니즘	○	○	○

×: 제공 ○: 제공안함

4.2. 효율성 분석

NTT 메커니즘은 태그에 대한 해쉬 연산이 2회 요구된다. 그러나, Back end Server에서는 검색 회수당 i회의 해쉬 연산이 요구되므로, 메커니즘 과정에서 총 요구되는 해쉬 연산의 회수는 (i×f)+2회이다. 이는 i값의 증가에 따라 재초기화의 번거로움을 가져오게 될 수 있다. 또한, 고유 태그 정보는 각각의 Hash값과 연결되어 있으며, i회의 해쉬 결과값과 연결된 고유 태그정보의 검색이 필요하다.

한편, 제안 메커니즘은 태그상에서 해쉬연산이 2회 소요되며, 1회의 XOR연산이 소요된다. 또한, Back-end Server에서 소요되는 연산량은 태그에서 요구되는 연산량과 일치하며, 메커니즘 과정에서 총 요구되는 양은 4회의 해쉬연산과 2회의 XOR연산이 소요된다.

[표 2] 효율성 비교

	Tag	Back-end Server	Total
NTT 메커니즘	Hash : 2회	Hash : i×f회	Hash (i×f)+2회
제안 메커니즘	Hash : 2회 XOR : 1회	Hash : 2회 XOR : 1회	Hash : 4회 XOR : 2회

i : 해쉬연산회수 f : 검색 회수

V. 결론

본 논문에서는 NTT의 RFID 익명화 메커니즘을 개선하여 태그의 Random Tampering 공격을 방지하고, 태그와 리더 상호간 인증이 가능하며, 보다 효율적으로 사용자의 프라이버시를 보호할 수 있는 메커니즘을 제안하였다. 제안한 방법을 통하여 보다 안전하고 효율적으로 RFID

기반 센서 환경에서 사용자의 프라이버시를 안전하고 효율적으로 보호할 수 있다.

[참고문헌]

[1] Miyako Ohkubo, Koutarou Suzuki and Shingo Kinoshita, Cryptographic Approach to "Privacy-Friendly" Tags, RFID Privacy Workshop, MIT, 2003.

[2] Ari. Juels, "Privacy and Authentication in Low-Cost RFID Tags", RFID Privacy Workshop, MIT, 2003.

[3] Ari. Juels, Ravikanth. Pappu, "Squealing euros: Privacy protection in RFID-enabled banknotes", In Proceedings of Financial Cryptography - FC'03, 2003.

[4] Shingo Kinosita, Fumitaka Hoshino, Tomoyuki Komuro, Akiko Fujimura and Miyako Ohkubo, "Nonidentifiable Anonymous-ID Scheme for RFID Privacy Protection", CSS 2003 in Japanese.

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

[6] Stephen A. Weis, Sanjay E.Sarma, Ronald L. Rivest and Daiel W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", First International Conference on Security in Pervasive Computing, 2003.