# 블루투스에서 위치 추적 공격을 방지하기 위한 익명 접속 프로토콜

박희진 김유나 김종
포항공과대학교 컴퓨터공학과
{ parkhj84, existion, jkim}@postech.ac.kr

# Anonymous Connection Protocol against Location Tracking Attacks in Bluetooth

Hee Jin Park, Yuna Kim, Jong Kim
Department of Computer Science and Engineering
Pohang University of Science and Technology (POSTECH)

**요 약**

블루투스(Bluetooth)는 별도의 인증시설 없이 각 디바이스간의 독립적인 인증과정을 통해 데이터를 서로 전송하므로, 이러한 특징 때문에 기존 네트워크에서는 발생하지 않았던 취약점들이 발생할 수 있다. 따라서 본 논문에서는 이들 취약점 중 하나인 디바이스 위치추적공격에 대해 살펴보고 그에 대한 해결책으로 익명모드를 제안하였다. 제안된 방법은 발생 가능한 공격시나리오에 대해 분석하고 성능을 평가하였으며, 분석과 평가에 있어서 기존 방법에 비해 수행 시간과 메모리 소비 측면에서 큰 차이를 보이지 않으면서도 위치 추적 공격에 대해 더 강인하게 동작함을 보였다.

## 1. 서론

블루투스 (Bluetooth)는 별도의 네트워크 기반시설이나 제어 장치 없이 가정이나 사무실 내에 있는 프린터, 휴대폰 등 정보통신기기나 각종 디지털 가전제품을 무선으로 연결해주는 근거리 무선접속 기술을 말한다[1].

블루투스 디바이스간에 안전한 데이터 전송을 저해하는 공격유형으로는 크게 노출된 패킷을 분석하여 데이타를 엿듣거나, 디바이스의 고유주소를 이용하여 개인 위치 정보를 추적하는 경우, 암호학적 취약점을 찾아 공격하는 방법이 있다. 이 중, 위치추적공격 (location tracking) 은 기존 네트워크상에서는 발생되지 않았던 문제인 동시에 노출된 데이터를 이용하여 그 디바이스의 사용자에 관한 정보를 악용할 가능성이 높기 때문에 시급히 해결해야 할 문제이다.

따라서 본 논문에서는 블루투스에서 위치추적공격의 원인과 공격유형에 대하여 알아보고, 이 공격을 해결하기 위해 디바이스의 고유주소에 익명성을 제공하는 방법을 제시한다.

## 2. 본론

### 2.1. 위치추적공격 (Location Tracking Attack)

블루투스 기술문서 (Bluetooth 1.2 Specification) [2]에 따르면 각 디바이스는 초기에 통신을 수행하기 위해 반드시 키 생성과정을 거쳐야 한다. 이때 이 과정에서 노출된 디바이스의 고유주소를 이용하여 해당 디바이스를 공격하는 것을 바로 위치추적공격이라고 하며 이로부터 유도되는 어떠한 값도 공격대상이 될 수 있다. 따라서, 데이터 전송 과정에서 BD_ADDR의 노출을 어떻게 막느냐 하는 문제가 디바이스의 위치추적문제를 위한 해결책이 될 것이다.

위치추적공격은 다음과 같이 4종류가 있다 [3].

• 질의 공격 (Inquiry Attack)

- 공격자가 공개된 전송매체상에 존재하는 메세지를 분석하여 주변 디바이스의 움직임과 위치정보를 기록하는 것이다.

• 트래픽 분석 공격 (Traffic Monitoring Attack)

- 이 공격에서는 네트워크 트래픽을 분석함으로써 공격대상 디바이스의 정보를 수집하는 공격유형이다.

• 페이징 공격 (Paging Attack)

- 정해진 범위 내에서 이미 알려진 주소를 가지고 공격하고자 하는 디바이스에 페이징 과정을 수행하여 해당 ID 패킷이 리턴되면 이 디바이스가 이 범위 내에 존재한다는 것을 알게 되는 공격 유형이다.

• 프리퀀시 호핑 공격 (Frequency Hopping Attack)

- 이 공격에서는 디바이스 간의 호핑 시퀀스를 관찰하여 BD_ADDR의 LAP와 UAP의 4 LSB를 얻음으로써 마스터 디바이스를 결정할 수 있다.

### 2.2. 제안방법

위치추적공격을 방지하기 위해 가장 쉽게 생각할 수 있는 방법은 BD_ADDR의 노출 가능성을 차단하는 것이다. 하지만 BD_ADDR 자체가 각 디바이스의 신원을 의미하기 때문에 단순히 숨기는 것으로는 문제를 해결할 수 없다. 따라서 본 논문에서는 위치추적공격을 방지하기 위해 두 단계로 이루어진 블루투스의 익명모드를 제안한다. 본래 디바이스들이 연결되기 위해서는 반드시 질의과정 (inquiry procedure) 과 페이징 과정 (paging procedure) 을 수행해야만 한다[4]. 우선, 연결을 원하는 두 디바이스가 수정된 질의 과정과 페이징 과정을 수행하여 상호 인증 한 후, 가명인증을 이용하여 그 연결을 지속적으로 유지한다.

### 2.3. 익명 모드 (Anonymous Mode)의 개요

우선 질의과정 (inquiry procedure) 을 통해 발견되는 BD_ADDR의 노출을 막기 위해 디바이스의 주소를 세가지로 세분화한다.

• BD_ADDR_FIXED

- 기존 블루투스 기술과의 호환성을 위해 익명모드를 제공하지 않는 디바이스의 주소로 사용한다.

• BD_ADDR_ACTIVE

- 질의 과정을 통한 노출을 막기 위해 사용되었으며, 업데이트 함수를 통해 주기적으로 업데이트 된다.

• BD_ADDR_ALIAS

- 디바이스간의 승인과정에서 사용된다. 페이징 과정 이후, 각 디바이스의 연결마다 이전의 BD_ADDR_ALIAS를 해쉬 한 값으로 업데이트된다.

따라서, 이 세 주소를 이용하여 디바이스 주소는 질의 과정 및 페이징 과정에도 계속해서 업데이트 된다. 이를 통해 질의와 페이징 과정을 수행하게 된다.

#### 2.3.1. 수정된 프로세스

2.3.1.1. 질의 과정 (Inquiry Procedure)

BD_ADDR_ACTIVE는 업데이트 함수를 통해 일정 주기마다 임의의 값으로 변한다. 일반적인 BD_ADDR 구성 요소 중 UAP와 NAP는 고정된 값이고 LAP가 변함으로써 하나의 디바이스에 다른 BD_ADDR_ACTIVE가 계속해서 할당 된다.

업데이트 함수를 위한 인자는 $T_{updating\ period}$와 $T_{inquiry\ period}$가 있다. $T_{updating\ period}$는 얼마나 자주 업데이트가 일어날지를 결정하며, $T_{inquiry\ period}$는 일반적인 질의 과정에 소요되는

최소한의 시간이다.

따라서 업데이트과정은 일단 질의 과정 수행 여부를 판단하고, 만일 수행했을 경우$T_{inquiry\ period}$이 경과된 후에 업데이트 함수가 다시 수행 되게 된다. 이렇게 하는 이유는 질의 과정이 끝나기 전에 업데이트가 일어날 경우 상대편 디바이스가 이전의 주소로 페이징을 수행하기 때문이다.

2.3.1.2. 페이징 과정 (Paging Procedure)

질의 과정을 통해 알게 된 BD_ADDR_ACTIVE와 clock정보를 교환하여 호핑-시퀀스를 동기화하고 실제 연결을 맺는다. 원래 블루투스 통신에서는 주기적으로 페이지 스캔하는 과정을 거치는데, 같은 디바이스와의 통신 에서는 첫 번째 연결 이후부터는 질의 하지 않고 "가명 인증 (pseudonym authentication)"을 통해 페이징과정을 수행한다.

### 2.3.2. 가명 인증 (pseudonym authentication)

2.3.2.1. 수행절차

일단 디바이스 A와 디바이스 B는 질의 과정을 통해 알게 된 BD_ADDR_ACTIVE 혹은 이전 모델의 BD_ADDR_FIXED를 이용하여 페이징 과정을 수행했다고 가정한다. [1] 이러한 두 디바이스 간에는 링크키가 설정되어 있으며 같은 해쉬함수를 가지고 있고, 각 디바이스에는 바뀐 주소 값들을 위한 메모리 공간 (alias DB)이 존재한다. 디바이스 A가 자신의 BD_ADDR_ALIAS의 변경을 디바이스 B에게 알리는 과정은 다음과 같다.

1) 디바이스 A는 다음의 정보들을 alias DB에 저장한다.

> **alias DB (디바이스 A)**
> - 자신의 BD_ADDR_ALIAS: 자신의 BD_ADDR
> - 상대방의 BD_ADDR_ALIAS: 처음 페이징 과정을 통해 밝혀진 상대방의 BD_ADDR
> - 링크키: 위 두 주소를 이용하여 생성된 키

2) 디바이스 A가 자신의 $BD_ADDR_ALIAS_A$를 변경하고자 할 때, 저장되어 있는 링크키로 현재 $BD\_ADDR\_ALIAS_B$ 를 암호화하여 디바이스 B에게 보낸다.

3) 디바이스 B는 받은 패킷을 복호화하여 디바이스 A로 부터 받은 $BD_ADDR_ALIAS_B$와 자신의 $BD_ADDR_ALIAS_B$를 비교한다.

4) 위 3)의 결과가 진실이면, 디바이스 B는 alias DB에 저장되어 있는 $BD_ADDR_ALIAS_A$를 아래의 새로운 값으로 갱신하고 그 값을 암호화 하여 디바이스 A에게 보낸다.

> $BD\_ADDR\_ALIAS_A$ = **HASH** (이전$BD_ADDR_ALIAS_A$)

5) 디바이스 A는 3)과 같은 방법으로 저장된 $BD\_ADDR\_ALIAS_A$ 와 받은 $BD\_ADDR\_ALIAS_A$ 를 비교하여 같다면 해쉬함수를 수행하여 $BD\_ADDR\_ALIAS_A$ 를 교체한다.
6) 두 디바이스는 각각 링크 키를 갱신한다.

반대로 디바이스 B의 $BD_ADDR_ALIAS_B$변경을 디바이스 A에게 알릴 때에도 위의 1)~6) 과정을 거친다.

## 3. 결론

### 3.1. 시나리오 분석

앞에서 소개한 각 위치추적공격들이, 앞의 3가지 과정을 수행하는 중에 해결되는지 분석한다.

• 질의 공격

- 같은 디바이스라고 하더라도 매 질의 과정마다 해당하는 응답 메세지의 주소 값이 모두 다르므로 이 값을 이용하여 디바이스의 움직임이나 관련정보를 판단할 수 없다.

• 트래픽 분석 공격

- 이 공격이 성공하려면 이전에 질의 공격을 통한 공격된 디바이스가 있어야 한다. 그러나 질의 공격 자체가 불가능하므로 이 공격 또한 성립하지 못한다.

• 페이징 공격

- 특정 BD_ADDR로 정해진 범위 내에 해당 디바이스의 존재 여부를 판단하는 공격이므로, 주소의 지속적 변경으로 인해 이러한 값이 존재될 수 없으므로 공격이 성립 될 수 없다.

• 프리퀀시 호핑 공격

- 고정된 BD_ADDR이 아니라 BD_ADDR_ACTIVE의 업데이트 과정과 가명 인증을 통해 계속해서 변하는 BD_ADDR로 호핑 시퀀스가 정해지기 때문에 이를 이용하여 마스터 디바이스를 결정한다는 것을 불가능하다.

### 3.2. 성능평가

3.2.1. 속도

제안한 모델에서는 기존에 불필요했던 주소의 업데이트 과정과 가명 인증과정이 필요하기 때문에 이에 대한 추가적인 수행 시간이 필요하다. 하지만 일반적으로 각 디바이스가 통신을 하기 위해 수행하는 여러 암호화와 키 생성과정에 비해 이를 위한 난수생성기나 해쉬함수의 수행시간은 큰 비율을 차지하지 않는다.

3.2.2. 메모리

하나의 피코넷을 예로 들었을 때 한 디바이스가 최대로 연결될 수 있는 디바이스의 개수는 6개 이다. 메모리 효율을 높이기 위해 링크키를 따로 저장하지 않을 경우 다음과 같은 메모리 크기가 필요하지만 대부분 디바이스는 이 정도는 무시할 만한 정도의 메모리를 가지고 있다.

> **기존 모델**: 7 * 48bits = BD_ADDR + 6 * BD_ADDR
> **제안하고자 하는 모델**: 13 * 48bits
> = BD_ADDR + 6 * (자신과 상대방의 BD_ADDR_ALIAS)

### 3.3. 맺음말

블루투스가 실생활에 좀더 안전하게 사용되기 위해서, 개인의 위치가 노출되는 위치추적 공격은 반드시 해결해야 하는 문제이다. 본 논문에서는 이 문제를 해결하기 위해 디바이스의 고유주소에 익명성을 제공하는 방식으로 문제를 해결하였다.

익명성을 보장하기 위한 방안으로는 BD_ADDR_ACTIVE의 주기적인 업데이트와 가명 인증을 제안하였다. 전자를 통해 고정된 BD_ADDR이 노출되지 않아 디바이스 고유정보가 노출되지 않았고, 후자를 통해 계속해서 업데이트되는 BD_ADDR을 이용하면서도 디바이스간 연결 유지를 보장할 수 있었다.

블루투스에 이 익명모드를 적용할 경우 기존 방법에 비해 수행시간과 메모리 소비 측면에서 큰 차이를 보이지 않으면서도 개인 사생활 보호 및 데이터 전송 중 위치추적공격에 대한 안전성을 보장해 줄 수 있다.

### 감사의 글

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었습니다.
(IITA-2007-C1090-0701-0045)

### 참고문헌

[1] IEEE standard for Local and Metropolitan Area Networks: Overview and Architecture, IEEE, IEEE std. 802-2001,2002
[2] The Bluetooth SIG, http://www.bluetooth.com/Bluetooth/SIG/
[3] Markus Jakobsson and Susanne Wetzel, "Security Weaknesses in Bluetooth", RSA Conference'01
[4] Tom Karygiannis, Les Owens, NIST, "Wireless Network Security 802.11, Bluetooth and Handheld Devices"

[1] BD_ADDR_ACTIVE와 BD_ADDR_FIXED를 모두를 앞으로 BD_ADDR라고 가정한다.