블루투스에서 위치 추적 공격을 방지하기 위한 익명 접속 프로토콜

(Anonymous Connection Protocol against Location Tracking Attacks in Bluetooth Environment)

박 희 진 † 김 유 나 †
(Heejin Park) (Yuna Kim)

김 종 ††
(Jong Kim)

요 약 블루투스(Bluetooth)는 별도의 기반 인증 시설 없이 각 디바이스간의 독립적인 인증과정을 통해 데이타를 서로 전송하는 기술을 사용하고 있다. 이러한 특징 때문에 이전에 기반 인증시설을 이용하는 네트워크에서는 발생하지 않았던 취약점들이 발생할 수 있으며, 가장 대표적인 문제가 위치 추적 공격이다. 따라서 본 논문에서는 디바이스 위치추적공격에 대해 살펴보고 그에 대한 해결책으로 익명모드를 제안한다. 제안된 방법은 발생 가능한 공격시나리오에 대해 분석하고 성능을 평가하였으며, 이를 통해, 기존 방법에 비해 수행 시간과 메모리 소비 측면에서 큰 차이를 보이지 않으면서도 위치 추적 공격에 대해 더 강인하게 동작함을 보였다.

키워드 : 블루투스, 위치 추적 공격, 익명 모드, 가명 인증

Abstract Bluetooth technology provides a way to connect and exchange information between personal devices over a secure and short-range radio frequency without any authentication infrastructures. For this infrastructure-less feature, Bluetooth has several problems which could not occur in other network, and among them location tracking attacks is essential problem which should be solved. In this paper, we introduce the location tracking attack and propose an anonymous connection protocol against it. We also perform security analysis based on possible scenarios of this attack, and estimate both execution time and memory spaces of our scheme and existing methods.

Key words : Bluetooth, location tracking attacks, anonymous mode, pseudonym authentication

· 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었습니다. (IITA-2008-C1090-0801-0045)
· 이 논문은 제34회 추계학술대회에서 '블루투스에서 위치 추적 공격을 방지하기 위한 익명 접속 프로토콜'의 제목으로 발표된 논문을 확장한 것임

† 학생회원 : 포항공과대학교 컴퓨터공학과
parkhj84@postech.ac.kr
existion@postech.ac.kr
†† 종신회원 : 포항공과대학교 컴퓨터공학과 교수
jkim@postech.ac.kr

논문접수 : 2007년 12월 6일
심사완료 : 2008년 2월 14일

정보과학회논문지: 컴퓨팅의 실제 및 레터 제14권 제3호(2008.5)

1. 서 론

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]. 가장 기본적인 블루투스 네트워크 단위를 피코넷(piconet)이라 하며, 이는 하나의 마스터 디바이스와 최대 7개의 슬레이브 디바이스로 구성된다. 하나의 피코넷은 고유한 호핑-시퀀스로 동작되기 때문에 서로 다른 피코넷이 연결되기 위해서는 서로 다른 호핑-시퀀스를 동기화 시켜주기 위한 브릿지 디바이스가 필요하다[1].

블루투스 보안 기술의 궁극적인 목표는 디바이스간에 안전한 데이타 전송을 보장하는 것이다. 이를 저해하는 공격유형으로는 현재 외부에 노출된 패킷을 분석하여 데이타를 엿듣거나(eavesdropping), 디바이스의 고유 주소를 이용하여 개인 위치 정보를 추적하는 경우(location tracking), 암호학적으로 취약한 점을 찾아 공격하는 방법(Cipher vulnerability) 이 있다. 이 중, 위치추적공격(location tracking) 은 기존 네트워크상에서는 발생되지 않았던 문제인 동시에 노출된 데이타를 이용하여 그 디바이스의 사용자에 관한 정보를 악용할 가능성이 높기 때문에 시급히 해결해야 할 문제이다.

따라서 본 논문에서는 피코넷 환경에서 위치추적공격이 가능한 원인과 공격유형에 대하여 알아보고, 이 공격을 해결하기 위한 디바이스의 고유 주소에 익명성을 제공하는 방법을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 위치추적공격이 발생할 수 있는 이유와 동기에 대해서 기술하고, 3장에서는 위치추적공격을 해결하기 위해 제시하는 방안에 대해서 구체적으로 설명한다. 4장에서는 제시한 방안에 대한 분석결과를 제시하고 마지막으로 5장에서는 결론을 맺고 향후 연구방향을 제시한다.

2. 연구 배경

2.1 위치추적공격(Location Tracking Attack)

SIG[2]에서 공개한 블루투스 기술문서(Bluetooth 1.2 Specification)에 따르면 각 디바이스는 초기에 통신을 수행하기 위해 반드시 키 생성과정을 거쳐야 한다. 이때 이 과정에서 디바이스의 고유 주소는 공개된 전송매체에 노출 될 수 밖에 없으며, 이 정보를 이용하여 해당 디바이스를 공격하는 것을 바로 위치추적공격이라고 한다. 대부분의 디바이스는 특정 한 사람에 의해 사용되기 때문에 공격자가 이를 추적할 경우 일단 공격이 한번 성공하면 디바이스 사용자의 모든 고정된 신원(identity)은 잠재적인 프라이버시 공격의 대상이 될 수 있다. 따라서 디바이스의 주소나 이것으로부터 유도되는 어떠한 값도 공격대상이 될 수 있는 것이다.

BD_ADDR은 IEEE 802[1]기준에 따른 디바이스 고유한 주소를 말하며 디바이스가 통신을 위해 연결할 때 서로간의 인증을 위해 사용된다. BD_ADDR은 그림 1과 같은 구성을 가진다.

BD_ADDR은 각 디바이스의 고유한 값이기 때문에 이로부터 유도 되는 모든 값은 바로 특정 사용자를 추적하는데 사용 될 수 있다. 그림 2에서의 키 생성과정을 통해 알 수 있듯이 BD_ADDR은 디바이스간 승인 과정에서 반드시 노출 된다. 따라서 데이타 전송 과정에서 BD_ADDR의 노출을 어떻게 막느냐 하는 문제가 디바이스의 위치추적문제를 위한 해결책이 될 것이다.

LSB MSB

LAP	UAP	NAP
24bits	8bits	16bits

그림 1 BD_ADDR의 구성

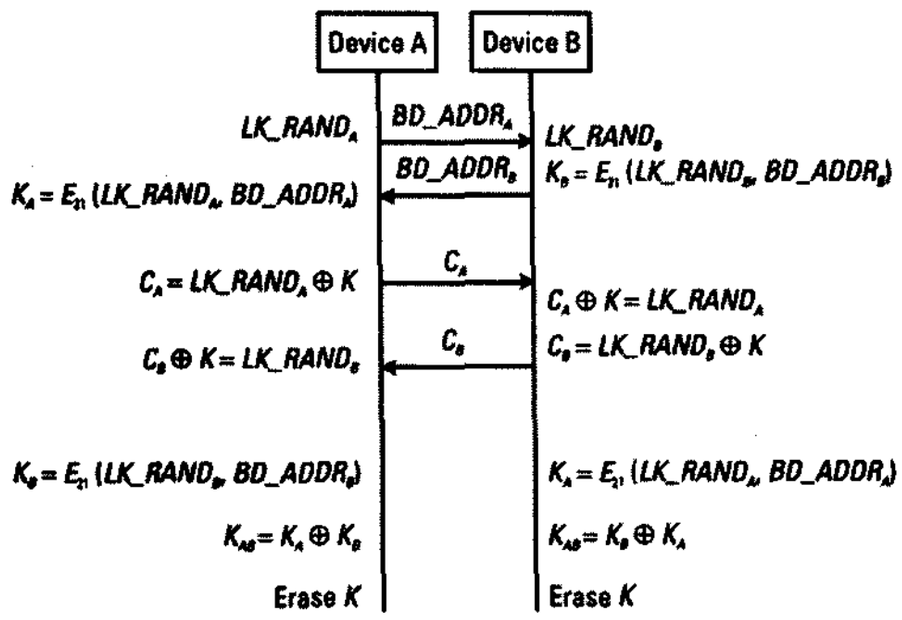

그림 2 A와 B의 키 생성과 승인 과정

2.2 위치추적공격의 종류

위치추적공격은 다음과 같이 4종류가 있다[3].

2.2.1 질의 공격(Inquiry Attack)

공격자가 공개된 전송매체상에 존재하는 메세지를 분석하여 발견 가능 모드(discoverable mode)에 있는 주변 디바이스의 움직임과 위치정보를 기록하는 것이다. 같은 지역에서 자주 통신을 하는 디바이스는 상호간에 서로 연결되어 있을 확률이 더 높기 때문에 가능하며, 이는 가장 단순한 공격유형이라 할 수 있다.

2.2.2 트래픽 분석 공격(Traffic Monitoring Attack)

이 공격에서는 공격대상이 발견 가능 모드가 아니더라도 네트워크 트래픽을 분석함으로써 공격대상 디바이스의 정보를 수집하는 공격유형이다. 공격대상 주위의 다른 공격 당한 디바이스를 통해 이와 통신하는 마스터 디바이스를 찾을 수 있기 때문에 마스터 디바이스에 연결된 모든 디바이스에 대한 위치 정보도 찾을 수 있다.

2.2.3 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.

2.2.4 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.

2.3 관련연구

위치추적공격을 막기 위한 방법[4,5]들이 제안되어 있다.

디바이스의 고유 주소를 주기적으로 변환하는 방식[4]에서는 디바이스의 고유주소는 신뢰할 수 있다고 가정한다. 초기에 디바이스 인증을 수행하여 링크키를 생성 한 후, 이 링크키와 난수를 사용하여 주소 값을 계속 변경시키며 마스터와 슬레이브 디바이스간의 연결을 유지한다. 이 경우, 링크키를 생성하기 위한 주소 값이 계속해서 변경되기 때문에 위치 추적에 안전하다고 볼 수 있지만, 처음 신뢰할 수 있다고 가정한 고유 주소 값이 공개될 경우 해당 디바이스는 위치추적공격의 대상이 될 수 있다.

또 다른 연구로는 BA_ADDR뿐만 아니라 이로부터 유도되는 키들도 위치추적공격의 대상이 될 수 있다는 점에서 시작하여, 링크키를 생성할 때마다 알고리즘을 변화시키는 방법[5]이 있다. 이 경우에는 위치 추적 공격에 좀 더 강인하다는 장점이 있는 반면에 디바이스 간의 동기를 맞추기가 어렵다는 단점이 있다.

3. 제안 방법

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 해결

할 수 없다. 따라서 본 논문에서는 위치추적공격을 방지하기 위해 블루투스의 익명모드를 제안한다. 익명모드는 크게 두 단계로 이루어진다. 우선, 연결을 원하는 두 디바이스가 수정된 질의 과정과 페이징 과정을 수행하여 상호 인증 한 후, 가명인증을 이용하여 그 연결을 지속적으로 유지한다.

3.1 익명 모드(Anonymous Mode)의 개요

서로 다른 디바이스들이 연결되기 위해서는 반드시 질의과정(inquiry procedure)과 페이징 과정(paging procedure)을 수행해야만 한다[6]. 질의 과정은 임의의 디바이스가 연결하고자 하는 디바이스를 찾는 과정이며, 즉 디바이스의 주소 BD_ADDR를 획득하며, 페이징 과정은 호핑-시퀀스를 동기화하고 실제 연결을 맺는 과정이다.

따라서 BD_ADDR 은 이 과정에서 외부로 노출될 수 밖에 없다. 이를 막기 위해 디바이스의 주소를 BD_ADDR_FIXED, BD_ADDR_ACTIVE, BD_ADDR_ALIAS 세 가지로 세분화한다.

- BD_ADDR_FIXED
- BD_ADDR_FIXED
  - 일반적인 BD_ADDR와 같고 기존 블루투스 기술과의 호환성을 위해 마련하였다. 따라서 익명모드를 제공하지 않는 디바이스는 디바이스 주소로 BD_ADDR_FIXED를 사용한다.
- BD_ADDR_ACTIVE
  - 질의 과정을 통해 BD_ADDR이 노출되는 문제를 해결하기 위해 사용된다. 이는 업데이트 함수를 통해 주기적, 임의적으로 업데이트 된다(3.2절).
- 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.

3.2 수정된 프로세스

3.2.1 질의 과정(Inquiry Procedure)

BD_ADDR_ACTIVE는 업데이트 함수 그림 3를 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.[1)]

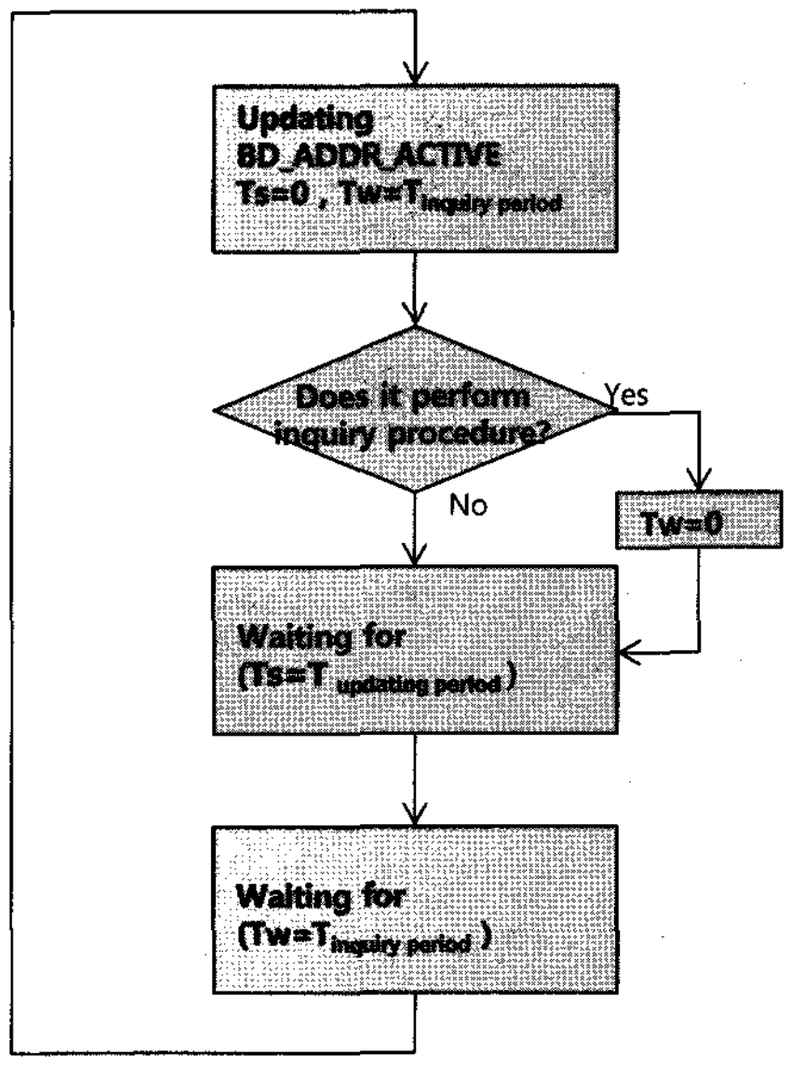

그림 3 BD_ADDR_ACTIVE의 업데이트 알고리즘

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 그림 3과 같이 업데이트과정은 다음과 같다. 질의 과정 수행 여부를 판단하고, 만일 수행했을 경우 $T_{inquiry\ period}$이 경과된 후에 업데이트 함수가 다시 수행되게 된다. 이렇게 하는 이유는 질의 과정이 끝나기 전에 새로운 BD_ADDR_ACTIVE가 생성될 경우 상대편 디바이스가 이전의 BD_ADDR_ACTIVE로 페이징을 수행하기 때문이다. 여기서 Ts와 Tw는 계속해서 증가하는 timer를 말한다.

3.2.2 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 페이징 과정을 수행한다.

3.3 가명 인증(pseudonym authentication)

3.3.1 수행 필요성

가명 인증이란 디바이스가 물리적 주소에 의한 링크가 아닌 BD_ADDR_ALIAS를 사용하여 서로를 승인하는 과정을 말한다[7].

가명 인증 과정을 수행하는 이유는 크게 두 가지 이다. 첫 번째 이유는 위치추적문제 해결을 위해 BD_

1) LAP에서 0x9E8B00~0X9E8B33까지는 예약된 특정 값이다. 따라서 생성되는 LAP값은 이 범위 밖의 값이 되어야 하며, 이 범위 안에 들 경우 업데이트 과정을 다시 수행하여 새로운 값을 생성한다.

ADDR을 계속 변경하는 방법이 궁극적으로 서로의 신원 파악을 저해하는 요소가 되기 때문이다. 임의의 두 디바이스 간의 연결은 한번 연결되었다고 해서 그 연결이 계속 유지되는 것이 아니기 때문에 연결된 이후에도 계속해서 연결 유무를 판단하는 과정이 필요하다. 따라서 이 연결 유무를 판단하는 과정에서 변경된 주소는 서로의 신원 여부를 판단할 수가 없다.

두 번째 이유는, 익명모드를 지원하지 않는 디바이스에서는 BD_ADDR_FIXED가 노출되면서 여전히 위치추적 문제가 발생 할 수 있기 때문이다. 따라서 가명 인증 과정을 통해 비록 완벽한 익명성을 보장해주지는 못하지만 위치추적문제를 어느 정도 해결 할 수 있다.

역으로, BD_ADDR_ACTIVE의 업데이트 과정 없이 가명 인증 만으로 익명성을 보장해 주지 못하는 이유는, 가명 인증에 사용하는 주소 값인 BD_ADDR_ALIAS가 BD_ADDR의 초기 값을 가지고 해쉬 함수를 이용하여 생성된 값이기 때문에 단순히 고정된 BD_ADDR로 이를 수행한다면 임의의 디바이스 A와 연결된 서로 다른 두 디바이스 B, C에서의 $BD_ADDR_ALIAS_A$는 항상 같게 된다.

3.3.2 수행절차

가명 인증 수행과정 이전에 디바이스 A와 디바이스 B가 질의 과정을 통해 알게 된 BD_ADDR_ACTIVE 혹은 이전 모델의 BD_ADDR_FIXED를 이용하여 페이징 과정을 수행했다고 가정한다.[2] 페이징 과정을 거친 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 현재의 $BD_ADDR_ALIAS_B$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 두 값이 같으면, 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.

4. 분 석

앞서 제안한 익명모드를 검증하기 위해 디바이스간의 승인과정을 통해 이를 분석한다.

4.1 시나리오

디바이스 A와 B가 각각의 익명성을 보장 하며 성공적인 데이타 전송을 수행하기 위해서는, 질의과정, 페이징과정, 가명 인증을 수행해야 한다. 2장에서 소개한 각 위치추적공격들이, 앞의 3가지 과정을 수행하는 중에 해결되는지 분석한다.

4.1.1 질의 공격

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

4.1.2 트래픽 분석 공격

이 공격이 성공하려면 이전에 질의 공격을 통한 공격된 디바이스가 있어야 한다. 그러나 질의 공격 자체가 불가능하므로 이 공격 또한 성립하지 못하며, 공격된 디바이스가 있다 하더라도 이와 연결된 다른 디바이스 정보에 대해 알 수 없다.

4.1.3 페이징 공격

이미 알려진 BD_ADDR로 정해진 범위 내에 해당 디바이스의 존재 여부를 판단하는 공격이다. 주소의 지속적 변경으로 인해 이미 알려진 BD_ADDR이 없으므로 공격이 성립 될 수 없다.

4.1.4 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.

4.2 성능평가

4.2.1 속도

제안한 모델에서는 기존에 불필요했던 BD_ADDR_ACTIVE의 업데이트 과정과 가명 인증과정이 필요하기

2) BD_ADDR_ACTIVE와 BD_ADDR_FIXED를 모두를 앞으로 BD_ADDR라고 가정한다.

때문에 이에 대한 추가 수행 시간이 필요하다. 하지만 일반적으로 각 디바이스가 통신을 하기 위해 수행하는 여러 암호화와 수 많은 키 생성과정[3]에 비해 주소의 업데이트 과정 및 가명 인증과정 중에 사용하는 난수생성기나 해쉬함수의 수행시간은 큰 비율을 차지하지 않는다.

4.2.2 메모리

하나의 피코넷을 예로 들었을 때 하나의 마스터 디바이스에 최대로 연결될 수 있는 슬레이브 디바이스의 개수는 7개이다. 메모리 효율을 높이기 위해 링크키를 따로 저장하지 않을 경우 마스터 디바이스는 다음과 같은 메모리가 필요하다.

> **기존 모델**: BD_ADDR + 7 * BD_ADDR = 8 * 48bits
> **제안하고자 하는 모델**: BD_ADDR + 7 * (자신의 BD_ADDR_ALIAS + 다른 디바이스의 BD_ADDR
> = 15 * 48bits

대부분의 블루투스 디바이스는 최소 512MB에서 최대 40GB의 메모리를 가지고 있다 따라서 288bit 정도의 메모리 사용은 무시할만하다.

5. 결 론

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 데이타 전송 중 위치추적공격에 대한 안전성을 보장해 줄 수 있다.

참 고 문 헌

[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] Ford-Long Wong and Frank Stajano, "Location Privacy in Bluetooth," ESAS 2005, LNCS 3813, pp. 176-188, 2005.
[5] F.-L.Wong, F. Stajano and J. Clulow, "Repairing the Bluetooth Pairing Protocol," 13th International Workshop in Security Protocols, Apr 2005.
[6] Tom Karygiannis, Les Owens, NIST, "Wireless Network Security 802.11, Bluetooth and Handheld Devices".
[7] Nikhil Anand, SANS Institute 2002-2002, "An Overview of Bluetooth Security," c2004.

3) 일반적으로 블루투스 통신을 하기 위해 각 디바이스는 링크키(link key), 암호화키(encryption key), 조합키(combination key), 마스터키(master key)와 같은 키를 주어진 암호화 알고리즘을 통해 생성한다.