비익명성 그룹키를 이용한 안전한 블루투스 피코넷

(A Secure Bluetooth Piconet using Non-Anonymous Group Keys)

서 대 희 † 이 임 영 ††

(Dae-Hee Seo) (Im-Yeong Lee)

요 약 무선 정보 환경의 변화에 따라 다양한 정보에 대한 풍족감이 요구되고 이에 따라 많은 근거리 무선 통신 기술들이 개발 연구되어 왔으며, 그 중에서도 최근 근거리 무선 통신의 표준으로 각광받고 있는 Bluetooth는 많은 관심을 받고 있는 실정이다. 그러나 블루투스가 자체 보안 요소는 좀 더 큰 네트워크에 적용하기엔 많은 취약점을 보이고 있다.

따라서 본 논문에서는 블루투스의 일반적인 개요 및 블루투스의 보안에 관해서 알아보고 취약점을 분석한 뒤 이를 바탕으로 안전한 블루투스 조회과정에서의 안전한 연결을 거쳐 ECDSA와 그룹 키를 이용한 블루투스 피코넷의 형성과 유지 과정을 제안함으로써 블루투스가 가지는 자체 보안성의 취약점을 보완한 안전한 블루투스 시나리오를 제시하였다.

키워드 : 근거리 무선통신, 블루투스, 피코넷, 그룹키

Abstract In accordance with the changes in the wireless communication environment, there has been a great need to satisfy the demand for diverse modes of information exchange. Various types of short-distance wireless communication technology have been developed and studied to meet this demand. Among them, Bluetooth which has recently been acclaimed as the standard for short-distance wireless communication, has been the focus of many such studies. However, Bluetooth has weaknesses in its security features when its in security services are applied to Home networks. The purpose of this study is to propose a safe Bluetooth scenario with an upgraded security feature. This paper first reviews the general characteristics and security features of Bluetooth together with an analysis of its weaknesses, and presents the formation and maintenance process of Bluetooth piconet what is created by using ECDSA and group key in the ACL(Asynchronous Connection-less Link) connection through a safe Bluetooth inquiry process.

Key words : Bluetooth, Piconet, Group-Signaturel

1. 서 론

최근 유동성 디바이스가 많이 사용되고 있으며 각 장비의 계층 사이에 통신 채널에 대한 연구들이 진행되고 있다. 이러한 연구들은 모든 유동성 디바이스가 일정한 장소에 놓여질 수도 있으며 그렇지 않을 수도 있는 한계를 극복하고 서로의 디바이스들이 통신할 수 있는 무선 환경의 인터페이스에 대한 고려로부터 시작되었으며 이러한 시스템이 바로 블루투스이다.

블루투스는 94년 에릭슨의 에릭슨의 통신 그룹이 핸드폰과 주변 디바이스 사이의 소비전력이 낮고 가격이 싼 무선 인터페이스를 연구하기 시작하면서 비롯하였다. 이러한 연구는 98년에 에릭슨, 노키아, IBM, TOSHIBA, Intel 등으로 구성된 SIG(Special Interest Group)가 발족되면서 본격적인 연구가 진행되고 있다

블루투스는 고정 혹은 유동성을 가진 각 디바이스에 정보를 전송하는 무선 통신 프로토콜이며 채널을 공유

† 학생회원 : 순천향대학교 전산학과
earthy6999@empal.com
†† 종신회원 : 순천향대학교 정보기술공학부 교수
imylee@sch.ac.kr
논문접수 : 2002년 3월 28일
심사완료 : 2003년 1월 7일

한 2개 또는 더 많은 장치들을 1개의 마스터를 중심으로 피코넷을 형성하여 스카터넷으로의 확장이 이루어진다[1].

그러나 블루투스에서 자체 제공하고 있는 보안 기능은 현재까지 많은 취약성을 보이고 있으며, 실제 네트워크에 적용했을 경우 사용자의 프라이버시를 침해하여 안전한 통신을 침해할 수 있다. 따라서 현재의 블루투스가 가지는 취약점 중 조회 과정에 따른 취약점을 보완하여야 한다. 취약점을 개선하기 위해 현재의 블루투스에서 제공하는 조회 과정을 보다 안전하게 이루기 위한 새로운 조회 과정과 안전한 피코넷 형성 및 유지에 관한 연구가 선행되어야 한다.

따라서 본 논문은 2장에서 블루투스의 일반적인 개요를 살펴보고 3장에서는 블루투스 표준안 1.1에서 자체 제공하고 있는 보안 서비스와 취약점을 분석한다. 4장에서는 새로운 제안 방식들을 제안하고 5장에서는 제안 방식을 분석한 뒤 마지막으로 6장에서는 결론을 맺도록 한다.

2. 블루투스 개요

최근 블루투스라는 말을 자주 듣게 된다. 우리나라말로 해석하면 '푸른 이빨'이란 뜻으로 해석되는 블루투스는 스칸디나비아 국가인 덴마크와 노르웨이를 통일한 바이킹 해럴드에서 유래되었다.

블루투스는 최초 스웨덴의 에릭슨이라는 회사에서 무선 근거리 통신을 위해 저전력, 저비용으로 무선 인터페이스를 가능하게 하기 위한 기술로서 시작된 프로젝트 이름이었다. 후에 이러한 프로젝트명을 바꿀려고도 하였으나 프로젝트의 이름이 현재의 이름으로 굳어졌다. 이에 따라 블루투스에 관심을 갖는 회사들은 1998년 5월에 무선 근거리 통신을 위한 하나의 프로젝트 개발을 위해 결성되었다. 이러한 그룹은 기존 케이블로 연결된 셀룰러 전화기를 통해서 셀룰러 망에 연결된 다중 통신을 조사하고자 하였으며 이것이 SIG(Special Interest Group)라는 이름으로 시작된 최초의 모임이다.

블루투스 이전에도 IrDA, IEEE802.11, SWAP와 같은 무선 근거리 무선통신들이 많이 등장하였다. 그러나 블루투스가 주목받고 있는 이유는 여러 가지 들 수 있는데 우선 기업 측면에서는 대량 출하수량을 통해 전세계적으로 판매할 수 있다는 점을 들 수 있으며 저가격으로 제조할 수 있다는 장점을 가지고 서로의 상호작용을 일으켜 부품에 대한 저가격화가 가능하고 이에 따라 출하수량이 늘어나는 상승효과를 가져다주고 있다. 또한 사용자 측면에서는 적은 소모 전력으로 휴대폰이나 기타 주변장치들의 무선 연결을 통해 선이 없는 인터페이스를 이루므로 보다 간편하고 효율적인 측면에서 사용자에게 다가서고 있다. 전체적으로 살펴보았을 때 블루투스가 주목받는 이유를 살펴보자면 정보통신 산업이 무엇을 위해 발전하였는가를 살펴보면 쉽게 알아볼 수 있다. 이는 보다 자유롭고, 안전하며, 신뢰성과 최근 급부상하고 있는 인터넷의 확장과 더불어 발전하고 있는 것이며 이를 만족하기 위해 제안된 기술이 블루투스라 볼 수 있다. 블루투스를 간단히 정의한다면 근거리 무선통신을 위한 하나의 기술이다. 중요한 것은 사용자의 요구에서 발생한 기술이라는 점이다. 이는 블루투스가 가져야 하는 여러 가지 특징 중에서 가장 중요한 특징이라고 할 수 있다.

블루투스의 또 다른 특징의 하나는 작은 네트워크의 구성이 가능하다는 것이다. 이는 피코넷이라 불리우며 하나의 피코넷에는 2개에서 최대 7개까지의 슬레이브가 가능하다. 이러한 피코넷이 여러개가 모여 서로 연결되어 있을 때 이를 스카터넷이라 한다. 결국 피코넷은 여러 통신장비를 하나의 통신 네트워크로 묶을 수 있다는 장점이 된다.

또한 블루투스는 무선으로 서로 통신하기 때문에 어떤 물리적인 연결이 있을 수 없다. 그래서 주변의 어떤 블루투스 디바이스가 통신 영역에 들어와 있는지 알아내는 방법이 반드시 필요하다. 이렇게 주변의 블루투스 디바이스가 어떤 것이 있는지 알아내는 방법을 "조회"라고 부른다. 조회 과정을 통해 현재 자신이 통신할 수 있는 블루투스 디바이스들의 블루투스 BD_ADDR 리스트를 얻어올 수 있다.

조회 과정은 원 타임(One-Time) 조회와 주기적(Periodic) 조회로 구분된다. 원 타임 조회라는 말 그대로 단 한번 조회를 수행하는 것으로, 호스트의 필요시 조회 명령어를 호스트 컨트롤러에 보냄으로써 조회가 시작된다. 주기적인 조회는 일정 주기마다 호스트의 조회 명령에 관계없이 자동적으로 조회 과정을 수행해 통신이 가능한 주변 블루투스 디바이스의 리스트를 갱신하는 방법이다.

3. 블루투스 표준안 분석

3.1 블루투스 보안 서비스

블루투스 프로파일에서는 3가지 보안 서비스를 제공해주며 다음과 같이 기술된다.

- 보안 모드 1(non-secure)
  각 디바이스는 어떠한 보안 프로시져도 가지고 있지 않다.
- 보안 모드 2(서비스 레벨 보안)
  각 디바이스는 L2CAP(Logical Link Controller and Adaptation Protocol) 레벨에서의 채널 설정 이전에

보안 프로시져를 획득할 수 없다. 이 모드는 응용을 위한 이질적이고 유동적인 access 정책을 허용하는 것으로서, 특히 서로 다른 보안 요구사항을 갖는 응용에서 수용된다.

• 보안 모드 3(링크 레벨 보안)

각 디바이스는 LMP(Link Manager Protocol) 레벨의 링크 초기화가 완벽하게 이뤄지기 이전에 보안 프로시져를 가질 수 있다.

3.2 블루투스 취약성 분석

블루투스가 가지는 취약점은 기술내역서 자체가 가지는 취약점과 실제 블루투스를 적용하였을 때 나타나는 취약점으로 구분하여 볼 수 있으며, 실제 적용시 예측되는 공격은 그림 1과 같다.

가. 블루투스를 실제 적용시 예측되는 공격

블루투스를 실제 적용 하였을때 그림 1과 같은 4가지의 예측되는 공격이 이루어 질 수 있으며 그 중의 하나가 PIN에 대한 공격을 들 수 있다.

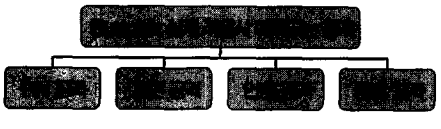

그림 1 실제 적용시 예측되는 공격

① 암호화된 디바이스간의 통신을 도청하거나 PIN의 공격을 통한 공격

일반적으로 블루투스를 통해 당사자들이 중요한 통신을 하기 위해 상호간이 동의하에 암호화된 통신이 이루어진다. 블루투스의 취약점은 디바이스들이 한 쌍이 되는 동안에 교환된 메시지들에 대한 도청을 할 수 있다는 것이다. 즉, 블루투스 계층에서 응용 프로그램 계층에서의 암호화가 수행되지 않으면 공격자에 의한 Man-in-the-middle-attack이 가능하다는 것이다.

블루투스 디바이스들 사이에 이루어지는 첫 번째 프로토콜은 중요한 정보의 교환을 이루는데 만약 첫 번째 프로토콜에서 사용될 정보를 얻지 못할 경우 두 번째 프로토콜이 실행된다. 첫 번째 프로토콜의 목적은 키들을 한정된 메모리의 자원을 가진 디바이스에 저장하기 위해서이다. 첫 번째 프로토콜의 목적이 이루어지지 않을 때 두 번째 프로토콜이 실시된다. 두 번째 프로토콜은 장치들 사이에 서로 다른 링크 키로 첫 번째 과정을 재 실시하는데 이는 PIN 번호와 번지를 생성하여 이루어진다. 그러나 PIN의 코드가 8~128비트로 이루어짐에도 불구하고 사용하지 않는 값을 0으로 채우는 것에 대한 취약점을 보이고 있다.

일단 공격자는 디바이스가 생성할만한 난수를 임의로 생성하여 링크 키를 계산할 수 있으며, 이는 공격자가 디바이스 사이에 이루어지는 정보의 도청이 가능하다. 따라서 공격자는 송신 디바이스와 수신 디바이스 어느 것이든 위장이 가능하다. 만약, 공격자가 디바이스의 유닛 키를 알고 있다면 이것 역시 공격자의 위장이 가능하다고 추정할 수 있다.

나. 블루투스 기술 내역서 1.1의 자체 취약성 분석

블루투스 기술 내역서에서 제공하고 있는 보안 서비스는 그림 2와 같은 취약성을 가지고 있으며 도청과 위장 공격 및 오프라인 PIN 공격에 매우 취약하여 실제 피코넷이나 스카터넷이 구성되었을 경우 보안홀이 생길 수 있다.

그림 2 기술내역서 1.1의 자체 취약성 분석

① 도청과 위장 공격

근본적으로 키 생성 프로토콜이나 키 생성에 대한 프로토콜로서 블루투스의 키 생성 방식은 난수와 PIN 그리고 블루투스 디바이스 주소를 이용하여 계산된다. 만약에, PIN이 유효하지 않거나 유닛간에 전송이 안된다면 공격자는 이를 쉽게 알아낼 수 있다. 이러한 취약점은 PIN의 길이를 충분히 길게 사용한다면 취약점을 보안할 수 있다.

② 오프라인 PIN의 취약점

두 디바이스간에 키를 수립하는 결정에 대한 도청적인 공격을 고려해 볼 수 있다. 이는 현재 블루투스 버전에서 유닛간의 키 교환 전에 PIN 번호를 결정 지을 때 공격자가 공격할 수 있는 여지가 있다고 볼 수 있다. 이렇게 강탈한 PIN 번호에 대한 정보는 피공격자의 키를 유추할 수 있는 토대가 될 수 있다.

공격자는 첫 번째 PIN을 추측하여 수행하고 있는 키에 대한 정보를 얻은 다음 부정하지 않는 정보를 흘려 피공격자의 디바이스가 동작하는 결과를 본 뒤 정확한 PIN에 대한 추측을 행할 수 있다. 이로 인해, 피공격자의 응답이 정확하다면 공격자는 공격자가 원하는 초기화키를 계산할 수 있게 된다. 초기화 키의 획득에 대한 문제는 검증 알고리즘의 문제이며 우리들은 일단 공격자가 시도 응답에 대한 쌍을 얻으면 이러한 공격이 수행되었다고 볼 수 있다[3] [4] [5].

4. 제안방식

본 장에서 각 모바일 디바이스는 공개키 암호 알고리즘

을 기반으로 자신의 피코넷 블루투스 마스터에게는 비익명성을 제공하면서 다른 피코넷의 마스터 디바이스에게는 익명성을 제공하는 안전한 피코넷 형성으로 기존 블루투스 조회과정의 취약점을 극복하여 블루투스 링크 계층에서의 보다 안전한 조회 과정을 제안하였다.

제안방식은 다음과 같은 4개의 객체로 구성되어 있다.

- 중앙 서버 : 초기 안전한 조회 과정에서 개인 PC가 인증해주는 블루투스 슬레이브(피코넷 형성시 피코넷 슬레이브 역할을 하는 모바일 디바이스)를 인증하는 하면서 이를 제어하고 관리하는 홈 네트워크의 중앙 서버
- 개인 PC : 홈 네트워크의 중앙서버의 제어를 받는 객체로서 중앙 서버가 인증하는 블루투스 슬레이브(피코넷 형성시 피코넷 마스터의 역할을 하는 모바일 디바이스)를 인증하는 홈 네트워크의 한 객체
- 블루투스 마스터 : 홈 네트워크에 위치해 있는 사용자의 모바일 디바이스로서 중앙 서버와의 상호 인증과정을 거쳐 안전한 조회 과정이 이루어진 후 안전한 피코넷 형성시 피코넷 마스터의 역할을 수행하는 모바일 디바이스 객체
- 블루투스 슬레이브 : 홈 네트워크에 위치해 있는 사용자의 모바일 디바이스로서 블루투스 마스터보다는 컴퓨팅 파워와 전력이 낮은 기기이다. 블루투스 슬레이브는 개인 PC와의 상호 인증과정을 거쳐 안전한 조회과정을 통해 안전한 피코넷 형성시 피코넷 마스터 중심의 피코넷 슬레이브가 되는 모바일 디바이스 객체

4.1 각 객체 시스템 계수

다음은 각 객체의 시스템 계수이다.

$*$: H - 중앙서버, I - 개인 PC, M - 블루투스 마스터, S - 블루투스 슬레이브

p_*, q_* : $*$가 생성한큰 소수 ($p, q \geq$ 512비트)

x_*, y_* : RSA 암호 알고리즘을 기반으로한 $*$의 개인키, 공개키

a_*, c_* : ECC 암호 알고리즘을 기반으로한 $*$의 공개키, 개인키 ($a \geq$ 128비트, [$a = cP, P \in E(Z_p)$])

g, η : 중앙 서버가 공개한 시스템 계수

Ψ_*, Ξ_* : $*$의 객체가 생성한 ESIGN 서명값

$H()$: 안전한 해쉬 함수

h_* : $*$가 생성한 안전한 해쉬값

r_* : $*$가 생성한 의사 랜덤수

$PINLg_*$: $*$의 PIN 코드 길이

$PINcode_*$:$*$의 PIN 코드

T_* : $*$의 타임 스탬프

EC : 타원곡선 암호 알고리즘

ER : RSA 암호 알고리즘

E : 관용 암호 알고리즘

G : ECC에서 사용되는 Base Point

$V*\_@\#$: #로 암호화 되어 $*$에서 @로 전송되는 암호화된 값

R_*, S_* : $*$가 생성한 ECDSA 서명값

ID_{info_*} : $*$의 정보

Z : 블루투스 master가 피코넷 그룹원에게 공개하는 시스템 계수($Z = g^{c_M} \bmod \eta$ $[g \in GF(a_M)]$)

i : 블루투스 master가 피코넷 그룹원에게 할당된 키의 개수

($i \in (1, \ldots, a_M - 1)$)

BD_ADDR_* : $*$의 48비트 블루투스 주소

S_j : 블루투스 피코넷 그룹키 서명값

$(\xi)_*$: $*$가 생성한 연접값

S_{info} : 블루투스 피코넷에 접속을 요구하는 블루투스 슬레이브 정보

S_{info_w} : S_{info}를 전송 받은 해당 블루투스 피코넷의 응답값

R_{BS}, S_{BS} : 블루투스 피코넷에 접속을 요구하는 블루투스 슬레이브 ECDSA 서명값

(p_{Mi}, n_{Mi}) : 그룹 서명값 생성을 위해 블루투스 마스터에서 생성한 임의의 공개키, 개인키 쌍

ζ : 피코넷을 형성하는 블루투스 슬레이브 개수

4.2 비익명성 그룹키를 이용한 안전한 블루투스 피코넷 프로토콜

비익명성 그룹키를 갖는 안전한 블루투스 피코넷을 구성하기 위해서는 다음과 같은 단계를 거쳐 이루어진다.

- 사전단계 1 : 세션키 설정단계
- 사전단계 2 : 중앙서버와 개인 PC 서명값 생성 단계
- 중앙서버와 개인 PC와의 상호인증 단계
  - 중앙서버 & 블루투스 마스터 사이에 링크 키가 요구될 경우 중앙서버와 블루투스 마스터 사이에 현재 BD_ADDR과 난수를 교환하는 단계
  - 중앙서버와 블루투스 마스터 사이에 PIN 코드가 요구될 경우 BD_ADDR값 뿐만 아니라 PIN과 연관된 값을 전송하는 단계
  - 사용자가 모바일 디바이스에 직접 PIN입력을 통해 초기 조회 과정이 이루어질 경우 이루어지는 단계
- 블루투스 마스터와 슬레이브 통신단계

- 블루투스 마스터와 슬레이브 상호 인증 단계
- 서명값 교환 및 그룹 키 설정단계
- 이밴트 종결 단계
- 피코넷 프로토콜 단계

이상의 단계는 그림 3과 같은 순서에 따라 진행되어 비익명성을 제공하는 안전한 블루투스 피코넷이 형성된다.

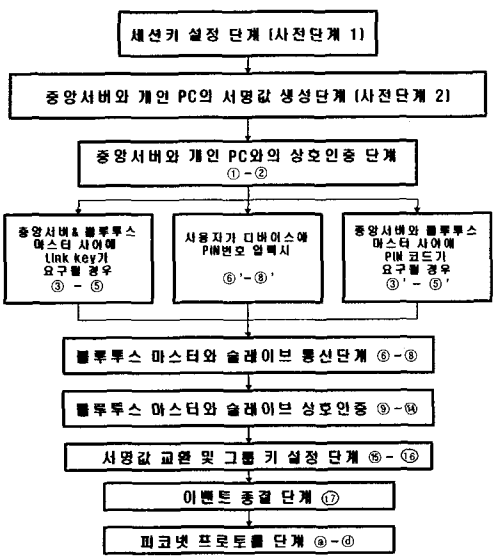

그림 3 제안방식 프로토콜 순서도 (①~ⓓ 내부 프로토콜 진행단계)

사전단계 1 : 세션키 K 설정 단계

세션키 K를 생성하는 사전단계는 중앙서버와 개인 PC사이에 비밀스럽게 공유할 수 있는 세션키를 설정하는 단계이다.

- 중앙서버 : 랜덤 수 r_H를 생성한 후 이를 이용하여 K를 생성후 개인 PC에 전달한다.

$$K = g^{r_H} \bmod \eta$$

- 개인PC : 랜덤 수 r_I를 이용하여 Y를 생성 후 중앙서버에 전송한다.

$$Y = g^{r_I} \bmod \eta$$

- 중앙서버는 개인 PC에게 X를 다음과 같이 계산하여 전송한다.

$$X = Y^{r_H} \bmod \eta$$

- 개인 PC는 다음을 계산하여 K=K임을 증명함으로써 세션키 K를 생성한다.

$$r_I^{-1} = y$$

$$K' = X^y \bmod \eta$$

중앙서버와 개인 PC 사이의 세션키 K의 설정은 중앙서버가 인증하는 블루투스 슬레이브(피코넷 형성시 중앙서버가 인증하는 블루투스 슬레이브는 형성된 피코넷의 블루투스 마스터가 된다.)를 개인 PC가 인증하고, 개인 PC가 인증하는 블루투스 슬레이브(개인 PC가 인증하는 블루투스 슬레이브는 사용자 중심의 피코넷 형성시, 형성된 피코넷의 블루투스 슬레이브가 된다.)를 중앙 서버가 인증하기 위한 사전 단계이다.

사전단계 2 : 중앙서버와 개인 PC 서명값 생성 단계

사전단계 2에서는 중앙서버와 개인 PC가 각각 고유한 ESIGN 서명값을 생성하는 단계이다.

- 중앙서버는 서명값 Ξ_H, Ψ_H를 생성한다.

$$\Psi_H \geq (h_M - (r_H)^K \bmod \eta) / (p_H * q_H)$$

$$\Xi_H = r_H + ((\Psi_H / K * (r_H)^{K-1})^{-1} * \bmod p_H) * (p_H * q_H)$$

- 개인 PC은 서명값 Ξ_I, Ψ_I를 생성한다.

$$\Psi_I \geq (h_I - (r_I)^K \bmod \eta) / (p_I * q_I)$$

$$\Xi_I = r_I + ((\Psi_I / K * (r_I)^{K-1})^{-1} * \bmod p_I) * (p_I * q_I)$$

- 이후 단계에서 사용되는 서명값은 수신자가 $(\Xi_*)^K \bmod \eta$을 계산한다. 만약 $h_*(m) \leq \Xi_*^K \bmod \eta$ 이고 $h_*(m) \leq \Xi_* \leq h_*(m) + 2^{(\frac{2}{3}\log \eta)}$이면 서명은 유효하다고 간주한다.

단계 1 : 중앙서버와 개인 PC와의 상호인증 단계

단계 1은 중앙서버와 개인 PC사이에 사전에 공유된 세션키 K를 기반으로 상호인증을 위한 단계이다.

Step ① 중앙 서버: 안전한 해쉬 값을 생성하고 세션키 K로 암호화한 후 VH_IK를 개인 PC에 전달한다.

- $(\xi_1)_H = (\Xi_H \| \Psi_H \| T_H)$
- $Z_H \equiv ((\xi_1)_H)^{r_H} \bmod \eta$
- $VH\_IK = E_K(Z_H \| r_H)$

Step ② 개인 PC: 안전한 해쉬 값을 생성하고 세션키 K로 암호화한 후 VI_HK를 중앙서버에 전송한다.

- $(\xi_1)_I = (\Xi_I \| \Psi_I \| T_I)$
- $Z_I \equiv ((\xi_1)_I)^{r_I} \bmod \eta$
- $VI\_HK = E_K(Z_I \| r_I)$

이와 같은 과정을 통하여 중앙서버와 개인 PC 사이에 상호 인증과정이 수행되며 블루투스 통신을 위한 초기화 단계가 수행된다.

<중앙서버와 블루투스 마스터 사이에 링크 키가 요구

될 경우>

Step ③ 블루투스 마스터는 안전한 해쉬 값을 생성하고 중앙서버의 공개키로 암호화한 후 $(VM_HyH \| h_M)$를 중앙서버에 전송한다.

- $(\xi_1)_M = (BD\_ADDR_M \| r_M \| T_M)$
- $h_M = H((\xi_1)_M)$
- $VM\_HyH = ER_{y_H}((\xi_1)_M)$

Step ④ 중앙서버: 블루투스 마스터의 BD_ADDR_M을 확인하고 다음을 계산한 뒤 $(VH_MrM \| VH_MK \| h_H)$를 블루투스 마스터에 전송한다.

- $(\xi_2)_H = (BD\_ADDR_H \| T_H)$
- $h_H = H((\xi_2)_H)$
- $VH\_MK = E_K(g^{r_H r_M} \bmod \eta \| \Xi_H \| \Psi_H)$
- $VH\_MrM = E_{r_M}((\xi_2)_H)$

블루투스 마스터는 전송해온 해쉬 값에서 중앙서버의 BD_ADDR_H 확인 후 VH_MK를 임시 버퍼에 저장한다. 저장된 VH_MK는 블루투스 마스터와 슬레이브 상호 인증 단계에서 개인 PC가 인증한 블루투스 슬레이브를 중앙서버가 인증하기 위하여 사용된다.

Step ⑤ 중앙서버와 블루투스 마스터 사이에 링크 키가 요구될 경우의 이벤트에 대한 종결 메시지를 중앙서버에게 전송한다.

<중앙서버와 블루투스 마스터 사이에 PIN 코드가 요구될 경우>

Step ③′ 블루투스 마스터: 안전한 해쉬 값 생성하고 중앙서버의 공개키로 암호화한 뒤 $(VM_HyH \| h_M)$를 중앙서버에 전송한다.

- $(\xi_2)_M = (BD\_ADDR_M \| r_M \| T_M)$
- $h_M = H((\xi_2)_M)$
- $VM\_HyH = ER_{y_H}((\xi_2)_M)$

Step ④′ 중앙서버: 전송된 VM_HyH에서 BD_ADDR_M을 저장한 후 다음을 계산하여 $(VH_MK \| VH_MrM \| h_H)$를 블루투스 마스터에 전송한다.

- $(\xi_3)_H = (BD\_ADDR_H \| PINLg_H \| PINcode_H \| T_H)$
- $h_H = H((\xi_3)_H)$
- $VH\_MK = E_K((g^{r_H r_M} \bmod \eta) \| \Xi_H \| \Psi_H)$
- $VH\_MrM = E_{r_M}((\xi_3)_H)$

블루투스 마스터는 $BD_ADDR_H, PINLg_H, PINcode_H$를 확인하고 VH_MK값을 임시 버퍼에 저장한다. 저장된 VH_MK는 블루투스 마스터와 슬레이브 상호 인증 단계에서 개인 PC가 인증한 블루투스 슬레이브를 중앙서버가 인증하기 위하여 사용된다.

Step ⑤′ 중앙 서버와 블루투스 마스터 사이에 PIN 코드가 요구될 경우의 이벤트에 대한 종결 메시지를 중앙서버에게 전송한다.

< 사용자가 디바이스에 직접 PIN 번호 입력시 >

Step ⑥′ 블루투스 슬레이브: 안전한 해쉬값을 계산한 후 개인 PC의 공개키로 암호화하여 $(VS_IyI \| h_S)$를 개인 PC에 전송한다.

- $(\xi_1)_S = (BDADDR_S \| T_S \| r_S)\_$
- $h_S = H((\xi_1)_S)$
- $VS\_IyI = ER_{y_I}((\xi_1)_S)$

Step ⑦′ 개인 PC: 블루투스 슬레이브에 전송된 값으로 BD_ADDR_S을 저장하고, 다음을 계산한 뒤 $(VI_SK \| VI_SrS \| h_I)$를 블루투스 슬레이브에 전송한다.

- $(\xi_2)_I = (BD\_ADDR_I \| PINLg_I \| PINcode_I \| T_I)$
- $h_I = H((\xi_2)_I)$
- $VI\_SK = E_K(g^{r_I r_S} \bmod \eta \| \Xi_I \| \Psi_I)$
- $VI\_SrS = E_{r_S}((\xi_2)_I)$

블루투스 슬레이브는 전송된 값으로 개인 PC의 BD_ADDR_I, $PINLg_I$, 를 확인하고 VI_SrS값을 임시 버퍼에 저장한다. $PINcode_I$

Step ⑧′ 사용자가 디바이스에 개인 PIN 번호를 직접 입력 했을 때의 이벤트에 대한 종결 메시지를 개인 PC에 전송한다.

단계 2 : 블루투스 마스터와 슬레이브의 통신단계

블루투스 마스터와 슬레이브의 안전한 조회 과정을 위한 통신 단계로서 세션키를 설정하고 중앙서버와 개인 PC와 비밀스럽게 공유한 VH_MK, VI_SK를 전송하는 통신단계이다.

Step ⑥ 블루투스 마스터: 안전한 해쉬 값을 계산하여 다음을 계산한 뒤 $(VM_S\rho \| \rho)$를 블루투스 슬레이브에 전송한다.

- $(\xi_3)_M = (VH\_MK \| r_M \| T_M)$
- $h_M = H((\xi_3)_M)$
- $\rho = g^{r_M} \bmod \eta$
- $VM\_S\rho = E_\rho((\xi_3)_M \| h_M)$

Step ⑦ 블루투스 슬레이브: 전송된 $(VM_S\rho \| \rho)$을 저장하고 다음을 계산하여 $(VS_M\tau \| \tau)$를 블루투스 마스터에 전송한다.

- $(\xi_2)_S = (VI\_SK \| r_S \| T_S)$

- $h_S = H((\xi_2)_S)$
- $\tau = g^{r_S} \bmod \eta$
- $VS\_M\tau = E_r((\xi_2)_S \| h_S)$

Step ⑧ 블루투스 마스터: 전송된 ($VS\_M\tau \| \tau$)을 임시 저장하고 다음을 계산하여 블루투스 슬레이브에 ($\Lambda \| T_M$)를 전송한다.

- $\Lambda = \tau^{r_M} \bmod \eta$

블루투스 슬레이브는 다음을 계산하여 $\rho' = \rho$임을 증명한다.

$$r_S^{-1} = \omega$$

$$\rho' = \Lambda^{\omega} \bmod \eta$$

만약 모든 과정이 옳다면 $\rho = \rho'$이다. 따라서 마스터와 슬레이브는 임시 저장한 값을 복호화하여 r_M, r_S를 확인하고 VH_MK, VS_IK를 저장한다.

단계 3 : 블루투스 마스터와 슬레이브 상호 인증 단계

블루투스 마스터와 슬레이브의 상호 인증 단계는 중앙서버, 개인 PC가 통신 단계에 참여하여 블루투스 마스터와 슬레이브를 상호 인증하는 단계이며 이상의 프로토콜을 마지막으로 안전한 inquiry 과정이 종료되며, 마스터와 슬레이브는 새로운 세션키를 생성하게 된다.

Step ⑨ 블루투스 마스터: 안전한 해쉬 값을 생성 후 중앙서버의 공개키로 암호화하여 VM_HyH을 전송한다.

- $(\xi_4)_M = (VH\_MK \| T_M \| ID_M)$
- $h_M = H((\xi_4)_M)$
- $VM\_HyH = ER_{y_H}((\xi_4)_M \| h_M)$

Step ⑩ 블루투스 슬레이브: 안전한 해쉬 값을 생성 후 개인 PC의 공개키로 암호화하여 VS_IyI를 전송한다.

- $(\xi_3)_S = (VI\_SK \| T_S \| ID_S)$
- $h_S = H((\xi_3)_S)$
- $VS\_IyI = ER_{y_I}((\xi_3)_S \| h_S)$

Step ⑪ 중앙서버: 초기 세션키 K를 생성할 때 생성된 사용한 난수 r_H와 블루투스 마스터에서 생성한 r_M을 사용하여 다음을 계산한 뒤 안전한 해쉬 값을 생성하고 개인 PC의 공개키로 암호화하여 ($VH\_IyI \| h_H$)를 개인 PC에 전송한다.

- $(\xi_4)_H = (VH\_MK \| r_H \| r_M \| T_H)$
- $h_H = H((\xi_4)_H)$
- $VH\_IyI = ER_{y_I}(h_H \| (\xi_4)_H)$

Step ⑫ 개인 PC: 블루투스 슬레이브에서 전송된 값으로 개인 PC는 초기 세션키 K를 생성할 때 생성된 사용한 난수 r_I와 블루투스 슬레이브에서 생성한 r_S를 사용하여 다음을 계산한 뒤 안전한 해쉬 값을 중앙서버의 공개키로 암호화하여 ($VI\_HyH \| h_I$)를 중앙서버에 전송한다.

- $(\xi_3)_I = (VI\_SK \| r_I \| r_S \| T_S)$
- $h_I = H((\xi_3)_I)$
- $VI\_HyH = ER_{y_H}(h_I \| (\xi_3)_I)$

Step ⑬ 중앙서버: 중앙서버는 다음을 계산하여 블루투스 마스터에게 VH_MrM를 전송한다.

- $(\xi_5)_H = (K \| T_H)$
- $h_H = H((\xi_5)_H)$
- $VH\_MrM = E_{r_M}(h_H \| (\xi_5)_H)$

Step ⑬ 개인 PC: 개인 PC는 다음을 계산하여 블루투스 슬레이브에게 VI_SrS를 전송한다.

- $(\xi_4)_I = (K \| T_I)$
- $h_I = H((\xi_4)_I)$
- $VI\_SrS = E_{r_S}(h_I \| (\xi_4)_I)$

Step ⑭ 블루투스 마스터와 슬레이브는 VH_MK 와 VS_IK를 복호화한 뒤 중앙서버와 개인 PC의 서명을 확인 후 이벤트 종결 메시지를 송신한다. 이후 블루투스 마스터와 슬레이브는 $K \oplus \rho = x$ 계산하고 x를 세션키로 암호화 통신을 시작한다. 그림 4와 5는 사전단계에서 단계 3까지의 흐름을 나타낸다.

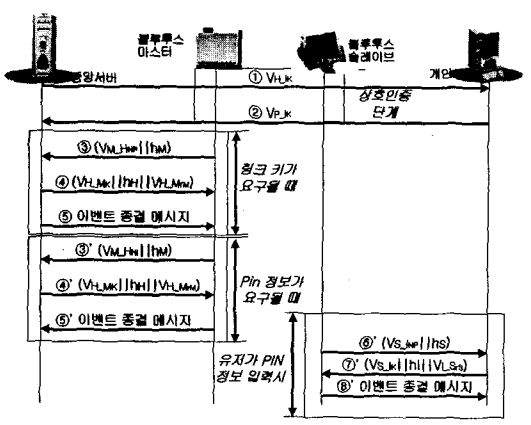

그림 4 New ACL Connection setup with pairing-1

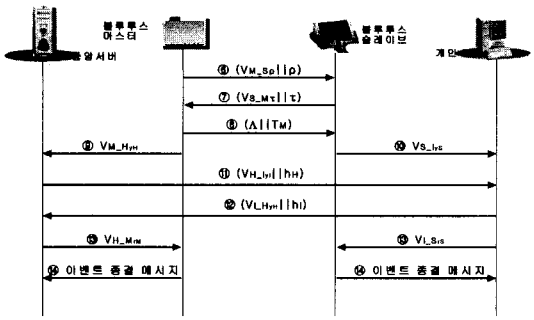

그림 5 New ACL Connection setup with pairing-2

단계 4 : 서명값 교환 및 그룹 키 설정 단계

단계 4는 블루투스 피코넷 구성을 위해 피코넷 마스터와 슬레이브간에 서명값 교환 및 그룹키 설정을 위한 초기 단계이다.

Step ⑮ 블루투스 마스터: 피코넷의 마스터는 ζ개의 (p_{Mi}, n_{Mi})을 계산한 뒤 임의의 그룹 키쌍인 (p_{Mi}, n_{Mi})과 ECDSA 서명값인 RM_i, S_M을 생성하고 안전한 해쉬 값을 계산한 뒤 세션키 x로 암호화하여 $VMA_S\chi$를 블루투스 슬레이브에게 전송한다(ζ개의 그룹 키 쌍중에서 임의의 그룹 키쌍을 선택하는 것은 블루투스의 피코넷 형성시 최대 7개까지의 슬레이브가 피코넷에 참가할 수 있다. 따라서 모바일 디바이스의 가입/탈퇴 뿐만 아니라 피코넷 슬레이브 개수의 유동성과 그룹 키에 대한 갱신 및 재분배에 대한 문제를 최소화 하기 위해서이다).

- $(\xi_1)_{M_A} = ((p_{Mi}, n_{Mi}) \| R_M \| S_M)$
- $h_{M_A} = H((\xi_1)_{M_A})$
- $VMA\_S\chi = E_x((\xi_1)_{M_A} \| h_{M_A})$

Step ⑯ 블루투스 슬레이브: 피코넷 슬레이브는 전송받은 $VMA_S\chi$를 복호화 하여 기밀성을 검증하고 안전한 해쉬 값 h_{M_A}로 무결성을 확인한 후 임의의 키쌍을 선택하여 서명값 $S_j\,(j \in i)$를 수행한 뒤 슬레이브의 ECDSA서명을 기반으로 안전한 해쉬 값을 생성하고 세션키 x로 암호화 한 뒤 $VS_MA\chi$를 블루투스 마스터에게 전송한다.

- $(\xi_4)_S = (S_j \| R_S \| S_S \| T_S)$
- $h_S = H((\xi_4)_S)$
- $VS\_MA\chi = E_x((\xi_4)_S \| h_S)$

- ECDSA 서명값은 이후 블루투스 피코넷 프로토콜에서 블루투스 슬레이브를 인증하기 위하여 사용된다.
- 그룹서명의 검증: 마스터는 ζ개의 그룹 키 (p_{Mi}, n_{Mi}) 리스트를 검증자에게 제공하며 검증자는 S_j를 검증할 수 있다.
- 그룹 키와 그룹 서명은 현재 형성된 피코넷의 정당한 모바일 디바이스인지를 검증할 수 있는 값으로써 그룹 키 값은 현재 모바일 디바이스가 참여하고 있는 피코넷 마스터가 생성한 뒤 임의의 그룹 키쌍을 선택하여 이를 피코넷 슬레이브에게 전송하여 그룹 서명값을 전송 받음으로써 제 3의 공격자로부터 안전한 피코넷 형성 및 유지 할 수 있게 한다.

단계 5 : 이벤트 종결 단계

단계 5는 그룹 서명키와 서명값 교환이 끝난 뒤 현재 이벤트를 종료하는 이벤트 종결 단계이다.

Step ⑰ 마스터는 슬레이브에게 전송받은 $VS\_MA\chi$, h_S를 검증하여 세션키 χ를 이용하여 전송된 값의 기밀성과 무결성을 검증한 뒤 이벤트 종결 메시지를 슬레이브에게 전송한다.

Step ⑰ 슬레이브는 마스터에게 이벤트 종결 메시지를 전송한다.

이상의 프로토콜을 기반으로 마스터를 중심으로 안전한 피코넷이 그림 6과 같이 형성된다.

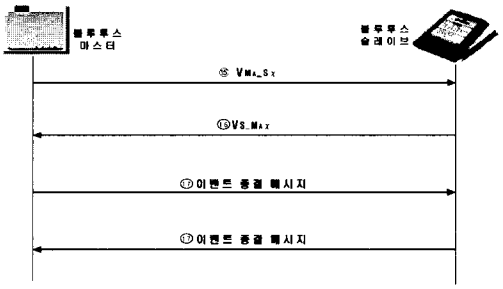

그림 6 마스터와 슬레이브간의 상호인증 및 그룹서명 단계

4.3 피코넷 프로토콜

그룹키를 적용한 피코넷이 형성된 후 슬레이브의 접속에 관한 두 가지 접속 방법을 고려해 볼 수 있다.

가. 피코넷에 포함된 슬레이브의 접속요구(마스터간의 비인증)

다음은 두 개의 피코넷이 존재하게 될 경우 모바일 슬레이브가 블루투스 마스터간 비인증된 피코넷에 접속을 요청할 경우의 프로토콜이다(마스터$_A$와 마스터$_B$는 서로 독립된 피코넷의 마스터로서 마스터$_A$는 사용자 중심으로 형성된 피코넷 마스터이며 마스터$_B$는 인증되지

않은 피코넷의 마스터이다).

Step ⓐ 마스터$_B$의 슬레이브는 마스터$_A$에 자신의 정보인 S_{info}를 전송하여 접속을 요구한다.

Step ⓑ 마스터$_A$는 $VMA_MB\chi$를 계산하여 마스터$_B$에 전송한다.

- $(\xi_2)_{M_A} = (R_A \| S_A \| ID_{M_A} \| T_{M_A} \| S_{info})$
- $h_{M_A} = H((\xi_2)_{M_A})$
- $VMA\_MB\chi = E_x((\xi_2)_{M_A} \| h_{M_A})$

Step ⓒ′ 마스터$_B$는 해당 마스터$_A$의 ECDSA 서명값을 저장하고 ID_{M_A}를 확인 후 안전한 해쉬 값을 계산하고 마스터A의 공개키로 암호화한 뒤 VMB_MAaMA를 마스터A에게 전송한다.

- $(\xi)_{M_B} = (R_B \| S_B \| R_{BS} \| S_{BS} \| T_{M_B} \| S_{info_{PN}})$
- $h_{M_B} = H((\xi)_{M_B})$
- $VMB\_MAaMA = EC_{a_{M_A}}(((\xi)_{M_B}) \| h_{M_B})$

Step ⓒ 접속요구 슬레이브는 VS_MAaMA를 계산하여 마스터$_A$에 전송한다.

- $(\xi_5)_S = (R_S \| S_S \| T_S)$
- $h_S = H((\xi_5)_S)$
- $VS\_MAaMA = EC_{a_{M_A}}((\xi_5)_S \| h_S)$

Step ⓓ 마스터$_A$는 슬레이브에서 전송된 값과 마스터$_B$에 전송된 값의 무결성과 기밀성을 확인한 후 슬레이브에게 전송되어 온 서명값과 마스터$_B$에게 전송되어 온 해당 슬레이브의 서명값을 확인하여 접속요구 슬레이브를 인증한다(그림 7 참조).

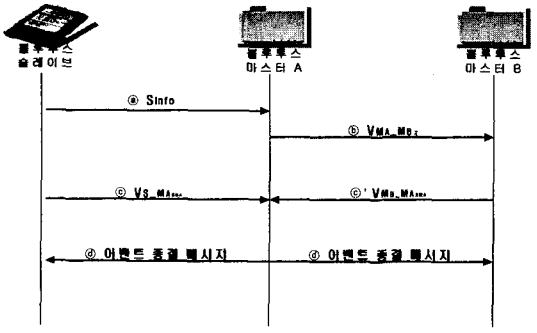

그림 7 인증되지 않는 슬레이브 인증 방식

나. 피코넷에 포함된 슬레이브 접속 요구(마스터간의 인증이 이루어진 경우)

마스터간의 인증이 이루어진 경우 접속 요구 슬레이브와 단계 4~5까지의 과정이 진행된다.

5. 제안방식 분석

본 논문에서는 홈네트워크에서 안전한 조회 과정을 거쳐 피코넷 형성을 이루는 과정을 제안하였다. 제안된 방식은 현재 블루투스 스팩에서 가지고 있는 여러 가지 문제점을 보안할 뿐만 아니라 실제적으로 사용자 중심의 안전한 서비스를 위해 반드시 필요한 피코넷 형성에 안전성을 추가하였다.

기존 블루투스 스팩에서 기술한 조회 과정에서 나타나는 취약점을 공개키 암호 알고리즘과 Hughes 키 분배 알고리즘을 통한 안전한 과정이 되도록 하였으며 실제 블루투스를 적용하기 위한 안전한 피코넷에 대한 연구는 피코넷의 마스터에서 분배하는 그룹키를 바탕으로 이루어지는 그룹 서명으로 피코넷의 참여 객체들이 안전한 피코넷을 유지하도록 하였다.

특히, 제안 방식의 분석은 블루투스 표준안 v1.1에서 제공되는 보안 서비스를 기반으로 실제 블루투스를 이용했을 때 예측되는 공격들에 대한 분석과 일반적인 보안 서비스에 대한 분석을 통해 제안 방식에 대한 전체적인 안전성을 분석하였다.

- 키 관리 : 기존 블루투스 스팩에서는 PIN번호 길이에 대한 취약성으로 인해 실제 암호 통신을 위한 키의 관리와 분배에 대한 취약성을 제안방식에서는 Hughes 키 분배와 동적 세션키를 이용해 안전한 PIN번호 유지 뿐만 아니라 키 관리 측면까지 고려하였다[6].
- 암호화 : 블루투스 스팩에서는 피코넷 형성시 암호 통신키를 브로드캐스팅 하여 제 3자에 의한 도청이나 위장 공격에 취약하나 제안 방식에서는 응용 계층의 보안 협상에서 공개키와 세션키를 이용한 전송되는 메시지의 암호화 통신을 제공함으로써 보다 안전한 통신 및 피코넷 형성이 가능하게 하였다.
- 인증 : 블루투스 스팩에서 제시하고 있는 인증은 사용자의 인증이 아닌 단지 모바일 디바이스가 블루투스 통신이 가능한지를 확인하는 인증이 수행되는 반면, 제안 방식은 PIN번호에 근거한 사용자의 서명을 이용한 사용자 인증을 제공함으로써 블루투스 통신이 가능한 디바이스 자체에 대한 인증뿐만 아니라 사용자의 인증까지 제공한다.
- 지역 공격 : 블루투스 스팩에서는 사용자 주변에 흩어져 있는 모바일 디바이스의 피코넷 형성시 공격자가 자신의 모바일 디바이스를 이용한 지역 공격이 가능하게 하는 취약성을 제안 방식에서는 그룹 키를 이용해 해당 피코넷에 인증된 슬레이브간의 통신으로 안전하게 디바

이스를 컨트롤 할 수 있도록 하였다.

- 인증 공격 : 블루투스 스팩에서는 단순한 디바이스 인증으로 피코넷 형성시 해당 피코넷 슬레이브의 인증 공격이 가능하였으나, 제안 방식에서는 세션키와 그룹키를 기반으로 피코넷 형성으로 피코넷 슬레이브의 안전한 유지를 통한 무작위적 인증 공격을 예방하였다.
- PIN 공격 : 블루투스 스팩 버전 1.1에서는 PIN에 대한 여러 가지 공격에 취약하지만 제안 방식에서는 응용계층에서 암호화 수행으로 Man-in-the-middle-atttack에 대한 보완과 안전한 해쉬함수 및 공개키 암호화로 통한 PIN 공격에 대한 안전성을 확보하였다.
- 기밀성 : 블루투스 스팩에서 자체 제공하고 있는 보안키는 PIN에 기반해 생성되므로 PIN의 취약성과 더불어 보안 키에 대한 취약성까지 연관된다. 따라서 제안 방식에서는 세션키와 공개키 암호화를 통한 기밀성을 확보하였다.
- 무결성 : 무선 통신에서 반드시 필요한 무결성 보안 서비스를 제안 방식에서는 안전한 해쉬값과 타임 스탬프를 이용한 무결성 서비스를 제공하고자 하였다.
- 사용자 인증 : 기존 블루투스에서는 사용자의 인증서비스를 제공하지 않아 이에 대한 취약성이 문제시 되었지만 제안 방식에서는 사용자의 PIN 번호에 근거한 네트워크 형성으로 해당 디바이스 인증뿐만 아니라 사용자의 인증 기능까지 제공하였다.

표 1은 이상의 내용을 블루투스 표준안 v1.1과 제안 방식을 비교하였다.

표 1 제안방식 분석

	블루투스 표준안 v1.1	새로운 제안방식
키관리	△	○
암호화	×	○
인증	△	○
지역 공격	△	○
암호 공격	△	○
PIN 공격	△	○
기밀성	△	○
무결성	△	○
사용자 인증	×	○

× : 위험, △ : 취약, ○ : 안전

6. 결 론

최근 정보통신의 급속한 발전으로 개인 정보통신의 수요는 날로 증가하고 있다. 이에 따라 사용자의 요구에 의해 많은 근거리 무선 통신에 대한 연구가 진행되고 있으며 블루투스도 이러한 요구에 의해 주목받고 있는 연구분야이다. 그러나 다양한 데이타 서비스를 안전하게 제공하기 위한 보안적인 연구는 미흡한 실정이다.

따라서 본 논문에서는 근거리 무선 통신의 표준으로 자리잡고 있는 블루투스를 홈 네트워크에 적용함으로써 블루투스 표준안 v1.1에서 가지고 있는 보안적 취약점과 실제 네트워크 구성에 따른 취약점을 보안하여 안전한 피코넷 형성 및 유지에 관하여 제안하였다.

제안된 방식은 최근 모바일 커머스의 급속한 확산에 따라 개인 모바일 디바이스를 이용한 여러 가지 서비스가 상용화 되고 있다. 특히, 블루투스를 이용한 모바일 상거래 환경에서의 모든 서비스에서 안전한 조회 과정을 거쳐 안전한 디바이스 통신 초기 과정 설정과 안전한 피코넷 형성으로 공격자로 의심되는 제 3자로부터 자신의 정보를 저장하고 있는 모바일 디바이스의 안전한 구성으로 안전한 모바일 응용 서비스를 가능하게 한다.

향후 제안된 방식에서 고려하지 않은 통신량에 대한 내용까지도 고려한 통신 방식의 연구를 통해 Ad-hoc 네트워크와 IMT-2000에서 좀더 안전한 방식의 블루투스를 적용할 수 있으리라 사료된다.

참 고 문 헌

[1] http://www.bluetooth.com (Bluetooth White Paper)

[2] http://www.bluetooth.or.kr (Bluetooth Sepcification v1.1)

[3] http://www.niksula.cs.hut/fi/~jiitv/bluesec.html (Juha T.Vainio, "Bluetooth Security," jssmd 2000)

[4] http://www.cs.hut.fi/Opinnot/Tik-86.174/sectopics.html(Ullgren T, "Security in Bluetooth Key management in Bluetooth," 2001)

[5] http://www.bell-labs.com/user/markusj/bt.html (Jakobsson M and Wetzel S, "Security Weakness in Bluetooth," RSA, 2001)

[6] E. Hughes, "An Encrypted Key Transmission Protocol," presented at the rump session of CRYPTO '94, Aug 1994.

[7] 서대희, 이임영, 김해숙 "홈 네트워크에 적용한 Bluetooth Security에 관한 연구", 한국통신학회 하계종합학술발표회논문집(상) Vol23, No.2, pp.36~39, 2001.

[8] 서대희, 이임영, 김영백, 김해숙 "ECC를 이용한 안전한 Piconet에 관한 연구", 한국정보처리학회2001년도 추계학술발표 논문집, 제 8권 제 2호, pp.911 ~ 914, 2001.

[9] 최용락, 소우영, 이재광, 이임영 "컴퓨터 통신보안", 도서출판 그린, 2001.2.

[10] 이임영 "전자상거래 보안입문", 생능출판사, 2001.
[11] Alfred J. Menezes, Paul C.van Oorschot and Scott A. Vanstone "HANDBOOK of APPLIED CRYPTOGRAPHY", CRC.

서 대 희

2001년 2월 동신대학교 전기전자공학과 졸업. 2001년 3월~현재 순천향대학교 전산학과 석사과정. 관심분야는 암호이론, 정보이론, 컴퓨터 보안

이 임 영

1981년 8월 홍익대학교 전자공학과 졸업 1986년 3월 오사카대학 통신공학전공 석사. 1989년 3월 오사카대학 통신공학전공 박사. 1989년 1월~1994년 2월 한국전자통신연구원 선임연구원. 1994년 3월~현재 순천향대학교 정보기술공학부 부교수. 관심분야는 암호이론, 정보이론, 컴퓨터 보안