안전한 유비쿼터스 환경을 위한 확장성 있는 블루투스 네트워크에 관한 연구☆

A Study on Scalable Bluetooth Network for Secure Ubiquitous Environment

백 장 미* 서 대 희**
Baek Jang-mi Seo Dae-hee

요 약

유비쿼터스 혁명이 시작되고 있는 시점에서 초고속 통신망을 기반으로 컴퓨터, 가전, 통신, 방송 등이 하나의 디지털 미디어로 통합되어 새로운 부가가치가 창출되는 디지털 컨버전스가 진행되고 있다. 따라서 새로운 문화와 공간이 창출될 것이며, 이러한 기술의 진화는 '유비쿼터스 사회'라는 독특한 사회적 패러다임으로 변화를 가속화시키고 있다. 그중에서도 최근 유비쿼터스와 관련하여 블루투스에 대한 활발한 연구가 진행되고 있으며, 현실 환경에 적용성을 인정받아 많은 관심을 받고 있다.

그러나 블루투스를 유비쿼터스 혹은 센서 네트워크와 같은 차세대 네트워크에 적용하기 위해서는 현재 블루투스가 제공하고 있는 보안 서비스뿐만 아니라 새로운 형태의 네트워크 구성이 요구된다. 특히, 저자는 2005년 한국정보보호학회 논문지(이하 Kiisc05)에서는 독립된 슬레이브 디바이스를 이용해 확장된 블루투스 피코넷을 제안하였다. 그러나 이는 확장된 형태의 피코넷만을 고려하였으며, 스케터넷으로의 확장은 고려하지 않았다. 따라서 제안 방식은 Kiisc05에서 제안된 방식을 스케터넷으로 확장하여 각각의 브리지에 연결 설정이 안전하게 이루어질 수 있는 방식을 제안하였다.

Abstract

The ubiquitous network revolution is beginning with the onset of digital convergence, whereby computers, home appliances, and communications and broadcast media are being unified into digital media with the founding of the information super high speed. This technical advancement is creating a new culture and a new space and accelerating society's transition to the new and unique social paradigm of a 'ubiquitous society'. In particular, studies on ubiquitous communications are well underway. Lately, the focus has been on the Bluetooth technology due to its applicability in various environments. Applying Bluetooth connectivity to new environments such as ubiquitous or sensor networks requires finding new ways of using it. Thus, the scalable Bluetooth piconet scheme with independent slave device is proposed. It follows from work by Seo et al. But extended scatternet is not considered is Kiisc05 paper. Therefore, we propose secure bridge connection scheme for scalable Bluetooth scatternet.

☞ keyword : Mobile communication, Bluetooth, Piconet, Scalable Scatternet, Ubiquitous Environment.

Ⅰ. 서 론

인터넷의 급속한 확장은 다양한 IT 정보를 기반으로 사용자에게 정보의 풍족감을 제공해주고 있다. 특히, 유비쿼터스 환경은 전기적 공간과 실세계 공간을 하나로 만들어주는 차세대 환경으로 각광을 받고 있다. 특히, 블루투스에 대한 연구는 유비쿼터스 환경에 적용성을 인정받아 연구가 진행되고 있으나 가장 큰 문제점이 보안 부분이다. 따라서 유비쿼터스 환경에서 무선 통신상의 사용자 프라이버시는 다양한 정보를 제공하는 문제와는 차별되는 문제로서 근거리 무선 통신의 보안

* 정 회 원 : Howard university(USA) PH.D
bjm1453@sch.ac.kr
** 정 회 원 : 한국정보보호진흥원 연구원
patima@sch.ac.kr(교신저자)
[2007/05/22 투고 - 2007/06/19 심사 - 2007/10/4 심사완료]
☆이 논문은 2006년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(KRF-2006-214-D00146)

에 대한 연구가 반드시 선행되어야 한다[1][3].

본 논문에서는 Kiisc05의 방식을 기반으로 이루어진 확장 피코넷에서 브리지 슬레이브의 형태에 따라 이루어질 수 있는 확장 스케터넷의 구성 방식을 제안하고자 한다. 본 논문의 2장에서는 유비쿼터스 환경에서 보안의 필요성과 블루투스의 일반적인 개요를 기술하고 확장 피코넷 기반의 스케터넷의 보안 요구사항을 제시하고자 한다. 3장에서는 기존 연구에 대한 보안 취약점을 분석하고 4장에서는 3장에서 제시된 취약점을 보완하기 위해 Kiisc05에서 제안된 방식을 가정으로 확장 스케터넷 형성 방식을 제안하고자 한다. 5장에서는 제안 방식과 기존의 연구들을 2장에서 제시된 보안 요구사항을 기반으로 분석한 뒤 마지막으로 6장에서 결론을 맺고자 한다.

Ⅱ. 기술 개요

본 장에서는 유비쿼터스 환경에서 보안의 필요성과 블루투스의 개요에 대해 기술하고 확장 피코넷 기반의 스케터넷의 보안 요구사항을 제시하고자 한다.

2.1 유비쿼터스 환경에서 보안의 필요성

유비쿼터스 환경은 오늘날 일상생활 속 깊숙이 파고들어 사용자들로 하여금 단일한 데스크톱 앞에서뿐만 아니라 노트북, PDA 등을 통해 정보를 제공받을 수 있게 하였다. 따라서 구체적인 유비쿼터스 환경을 이루기 위한 다양한 영역들에 대한 연구는 매우 의미 있다고 할 수 있다[2][5].

특히, 유비쿼터스 환경과 같이 개체마다 많은 정보를 갖고 있으며, 이에 대한 정보를 수집 분석하여 필요한 서비스를 자동적으로 처리해주는 능동형 환경에서는 필연적으로 개인의 정보를 어떻게 보호할 것이며, 어떠한 방법으로 서비스를 안전하게 제공할 것인지에 대한 연구가 반드시 요구된다. 그러나 최근의 보안에 대한 연구는 단순한 개체의 인증을 통한 연구가 이루어지고 있는 실정으로, 실제 유비쿼터스 환경이 구현 되었을 때 나타날 수 있는 다양한 형태의 보안 연구가 미흡한 실정이다. 현재 유비쿼터스 환경에서 공격자들에 대한 정확한 형태를 파악할 수 없는 상태에서 적용되는 기술의 보안적 취약점은 어떠한 형태로 사용자 프라이버시 정보를 침해할지 예측하기 매우 어렵다. 따라서 다양한 보안 요구사항과 이를 만족하는 보안 프로토콜 개발은 안전한 유비쿼터스 환경에 매우 절실히 요구되는 사항이다[6][17].

2.2 블루투스의 개요

현재 무선 멀티미디어 시장에서 가장 주목을 받고 있는 것이 블루투스이다. 블루투스가 기존의 무선 통신장비에 비해서 더욱 각광받는 이유는 통신기능이 없는 디바이스에 간단하고 조그마한 모듈을 첨가함으로써 서로 무선 네트워크로 연결을 할 수 있다는 점이다. 또한 연결 시 서로 무선 통신을 할 수 있는 범위 안에만 있으면 연결이 쉽게 되므로 사용상의 간편함을 들 수 있다. 그러나, 블루투스를 기존의 가전기기에 설치하여 사용하기 위해서는 단가를 낮추어야 하고 전송거리도 늘려야 한다. 또한 간단한 데이터 전송과 음성 전송만을 할 수 있지만, 화상회의 등 고속의 데이터 전송량을 필요로 하는 장소에서 사용하기 위해서 데이터 전송량을 늘릴 수 있는 방법이 개발되어야 한다[8][12][16].

현재 많이 사용되고 있는 블루투스가 사용자 중심의 네트워크를 형성할 경우 여러 네트워크로의 확장이 가능하지만, 이로 인해 발생되는 보안적인 문제점을 해결하지 않을 경우 새로운 형태로의 네트워크 환경에 적용에 어려움이 따른다.

2.3 확장 스케터넷 보안 요구사항

블루투스와 같이 사용자 중심의 네트워크는 다

양한 형태의 모바일 디바이스로 구성이 가능하며 사용자 프라이버시와 밀접한 관계가 있다. 그러나 현재의 블루투스 네트워크는 확장성이 제한된 형태의 네트워크 형태의 구성이 가능하며, 이로 인해 개인의 디바이스 증가에 따른 네트워크 형성이 어려운 문제점이 발생된다. 또한 블루투스 자체 서비스되고 있는 보안 서비스는 많은 취약점이 발생되고 있다[14][15][16]. 따라서 확장 스케터넷을 제안하기 위해서는 확장 피코넷 방식이 기반이 되어야 하며, 이를 위해 Kiisc05에서 제시된 동일한 보안 요구사항과 확장 스케터넷을 위한 확장 보안 요구사항을 구분하여 기술하고자 한다.

(1) Kiisc05에서 제시된 확장 피코넷의 보안 요구사항

• 상호인증 : 블루투스 초기 보안 키 설정 과정에서의 상호인증과는 별도로 확장 피코넷 형성에 따른 안전한 상호 인증 과정이 필요하다. 블루투스 피코넷상의 상호 인증은 마스터와 마스터간의 상호 인증과 마스터와 슬레이브간의 상호인증으로 구분된다.

  -마스터와 마스터간의 상호인증 : 마스터간의 상호 인증은 동등 레벨에서의 인증과 하위 레벨에서의 인증으로 구분되며, 기존 블루투스 통신을 위한 키 설정과정에서의 인증과는 별도로 수행되어야 한다.

  -마스터와 슬레이브간의 상호인증 : 확장 피코넷에 새롭게 참여하는 모바일 디바이스는 확장 피코넷의 상호인증 방식을 통한 안전한 형태로 확장 피코넷에 참여해야 한다.

• 기밀성과 무결성 : 그룹 통신 과정에서 필요한 보안 요구사항으로써 전송되는 데이터의 기밀성과 무결성 보장을 위해서 암호 알고리즘과 해쉬 함수를 이용해 보안 서비스를 제공해야 한다.

• 키 갱신 범위 : 그룹 키 갱신에 대한 보안 요구사항으로써 그룹 키를 사용하는 모바일 기기의 가입과 탈퇴가 빈번한 특징적인 형태를 고려해 볼 때 키 갱신 범위는 현재 그룹에서 탈퇴하고자 하는 모바일 디바이스만 수행되어야 한다.

• 탈퇴자에 대한 참가자의 보안성 : 피코넷 그룹 통신이 이루어지는 가운데 탈퇴자가 발생된다 할지라도 탈퇴자로 인해 발생되는 보안 취약성이 그룹 참가원들의 보안성을 침해해서는 안 된다. 컴퓨팅 능력을 고려해 볼 때 유선 환경보다 계산량과 통신량 부분에 경량화를 통해 효율성을 유지할 수 있어야 한다.

(2) 확장 스케터넷을 위학 확장된 보안 요구사항

• 상호인증 : 확장 스케터넷 과정에서는 네트워크 구성에 따른 상호 인증이 추가적으로 요구된다. 특히, 이러한 상호 인증 과정은 확장 스케터넷 과정에서의 상호 인증과는 차별화되어야 하며, 브리지를 중심으로 상호 인증 과정이 수행되어야 한다.

  -브리지 노드를 위한 상호 인증 : 상이한 확장 피코넷 사이의 스케터넷 구성 시 브리지 노드를 위한 상호 인증 서비스를 제공해야 한다.

  -동등 레벨 노드간의 상호 인증 : 확장 피코넷에서 이루어지는 동등 레벨간의 상호인증 뿐만 아니라 브리지 노드 설정에 따른 동등 레벨간의 브리지 노드에서도 상호 인증 과정이 요구된다.

  -상이한 레벨 노드간의 상호 인증 : 브리지 노드가 동등 레벨이 아닌 경우에 따라 각각의 노드의 상호 인증 서비스를 제공해야 한다.

• 기밀성과 무결성 : 확장 스케터넷은 확장 피코넷의 확장된 네트워크로서 확장 스케터넷 구성 시 확장 피코넷의 사용자 비밀값을 이용해 서로간의 네트워크의 암호키와 이를 이용한 검증시 연관성이 이루어지도록 하여야 하며, 확장 스케터넷만을 위한 별도의 세션키 설립과 전송 값의 검증이 가능한 보안 서비스가 이루어져야 한다.

• 키 갱신 범위 : 그룹키가 생성이 된 경우 확장 피코넷에서 그룹키의 갱신이 이루어지게 되면 그 영향이 확장 스케터넷까지 이루어져야 한다. 따라

서 그룹원에 대한 키 갱신이 아닌 네트워크 측면에서 키 갱신이 이루어지는 서비스가 제공되어야 한다.

• 탈퇴자에 대한 참가자의 보안성 : 확장된 형태의 피코넷을 기반으로 탈퇴자가 발생했을 경우 확장 스케터넷에서는 확장 피코넷의 탈퇴자에 대한 정보만을 그룹 정보에서 제외함으로서 확장 피코넷과 스케터넷의 동일한 보안 서비스가 이루어지도록 해야 한다.

• 효율성 : 무선 환경이라는 제한된 공간과 컴퓨팅 능력을 고려해 볼 때 유선 환경보다 계산량과 통신량 부분에 경량화를 통해 효율성을 유지할 수 있어야 한다.

Ⅲ. 기존 방식 분석

3장에서는 확장 피코넷 기반의 확장 스케터넷을 구성하기 위해 기존 블루투스 통신에서의 네트워크 형성 방식에 대한 보안 취약점을 분석하고자 한다.

3.1 블루투스 통신시 발생할 수 있는 보안 취약점 분석

현재 블루투스 표준에서는 자체 제공되는 보안 방식을 이용하고 있으며, 블루투스의 보안 핸드쉐이크를 통해 다양한 보안키가 생성되고 이를 기반으로 네트워크로의 확장이 이루어진다. 그러나 사용자의 사용 디바이스가 증가하고 있는 시점에서 피코넷의 개수 제한에 의한 취약성과 네트워크 확장에 대한 취약성이 문제시 되고 있다. 따라서 기존의 블루투스 표준을 유비쿼터스 네트워크와 같은 환경에 적용했을 경우 다음과 같은 문제가 발생될 수 있다.

• 상호인증 : 블루투스 초기 보안 키 설정 과정에서의 상호인증 과정은 네트워크 통신에 그대로 적용할 경우 보안 키 길이의 한계성과 평문 메시지 전송에 따른 보안 취약성이 증가하여 개인의 프라이버시 정보 뿐만 아니라 데이터의 안전성에 위협이 될 수 있다.

• 기밀성과 무결성 : 확장된 블루투스 네트워크 형태에서의 데이터 전송은 개인의 정보를 가장 밀접히 관련하는 모바일 단말기에서 전송되는 정보의 기밀성과 무결성 서비스를 제공할 수 있어야 한다. 그러나 블루투스 실제 적용시 취약한 PIN(Personal Identification Number)에 근거해 생성한 보안키의 설립으로 인해 발생되는 취약성이 문제시 된다.

• 키 갱신 범위 : 블루투스 네트워크 형성 후 모바일 디바이스의 자유로운 탈퇴와 효율적인 키 갱신 서비스를 제공해야 한다. 그러나 현재의 블루투스 키 갱신 범위는 현재 그룹에서 탈퇴하고자 하는 모바일 디바이스로 한정되지 않아 그 문제점이 지적되고 있다.

• 모바일 디바이스의 증가 : 현재 블루투스로 구성된 피코넷의 경우 최대 7개까지의 슬레이브를 피코넷 그룹원으로 제어할 수 있다. 그러나 무선 인터넷 사용에 따른 모바일 디바이스의 증가는 7개까지로 규정된 슬레이브 개수에 한정적인 특성으로 인해 적용이 어렵다.

• 새로운 환경에의 적용성 : 유비쿼터스 환경과 같이 작은 모바일 디바이스의 네트워크에 적용하기 위해서는 현재의 블루투스의 네트워크보다 확장성을 제공하는 네트워크 형성을 제공할 수 있어야 한다.

3.2 확장 피코넷의 취약성

Kiisc05에서 제시된 확장 피코넷은 블루투스의 슬레이브 개수를 확장시킨 개념으로서 독립된 형태의 네트워크 구성이 가능하였다[16]. 그러나 피코넷간의 통신이 필요한 경우 스케터넷으로 확장할 수 없어 블루투스의 특징 중에 하나인 스케터넷으로의 확장이 문제시 되고 있다. 따라서 기존의 Kiisc05의 방식에 대한 문제점은 다음과 같이 정리할 수 있다.

• 브리지 노드 연결성 문제 : 확장 피코넷은 스케터넷으로의 확장은 고려되지 않았다. 즉, 확장

된 형태로의 네트워크를 통해 사용자 중심의 네트워크를 구성하였다. 그러나 새로운 네트워크 환경에서 서로 다른 확장 피코넷간의 통신이 요구될 경우 브리지 노드를 설정해야 하며, 이를 기반으로 통신이 이루어져야 한다. 따라서 기존 확장 피코넷에서 브리지 노드 설립을 통한 상호 이질적 피코넷간의 통신을 보장해야 한다.

• 네트워크간의 통신 보안 : 확장 피코넷에서는 기존 블루투스 통신을 이용해 확장된 형태로의 방식을 제안하여 슬레이브 개수의 제한을 보완하였다. 그러나 네트워크간의 통신에 대한 설정이 이루어지지 않아 확장 피코넷간의 통신은 고려되지 않았다. 따라서 네트워크간의 통신을 위한 세션키 설립 및 암호 통신을 위한 부분이 요구된다.

• 확장 스케터넷의 기밀성과 무결성 : 확장 스케터넷의 기밀성과 무결성은 블루투스 기본 보안 통신과 확장 피코넷과는 차별화가 되어야 한다. 이는 확장 스케터넷이 블루투스 기본 통신과 확장 피코넷을 기본으로 구성되나 확장 피코넷상에서 통신을 위한 안전성을 유지하기 위해서는 전송 메시지에 대한 기본적인 보안 요구사항을 만족해야 한다.

Ⅳ. 확장성 있는 블루투스 스케터넷 방식 제안

Kiisc05에서 제안된 확장 피코넷 형성 이후 독립된 확장 피코넷이 스케터넷을 구성할 경우 기존의 방식과는 차별화된 스케터넷 구성방식이 요구된다. 따라서 제안된 방식은 Kiisc05의 확장 피코넷이 이루어짐을 가정으로 구성되며, 확장 피코넷이 구성된 후 다음과 같은 프로토콜로 확장 스케터넷이 구성된다.

4.1 시스템 계수

다음은 확장 스케터넷 구성을 위한 시스템 계수를 기술하고자 한다.

* : (확장 피코넷 1의 최상위 마스터(HM_1), 확장 피코넷 2의 최상위 마스터(HM_2), 브리지 노드로 설정된 슬레이브 (BS))

P_j, Q_j : 디바이스에 저장된 공개키, 개인키 쌍 (피코넷 디바이스의 경우 피코넷 마스터에서 생성한 임의의 j개의 공개키, 개인키 쌍중의 하나)

α,r : 의사난수

$H()$, $E()$: 안전한 해쉬 함수, 대칭키 암호 알고리즘

g, n : 각 객체에 공개된 시스템 계수

T_* : *가 생성한 타임 스탬프

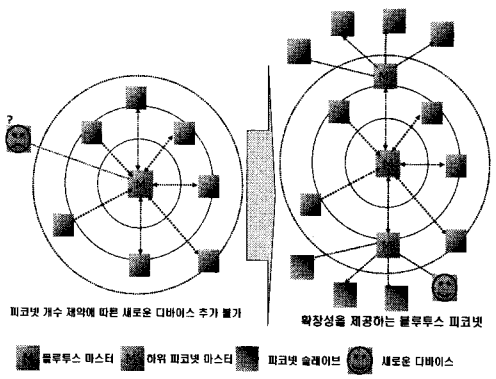
BD_ADDR : 모바일 기기의 48bit 고유 주소

SK_* : 확장 피코넷 암호 통신을 위한 세션키

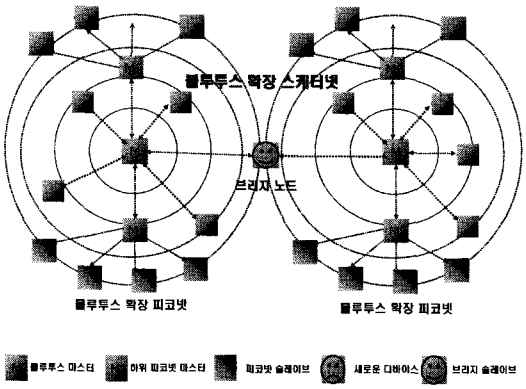
ID_* : 확장 피코넷에 참여하는 블루투스 디바이스의 ID로써 다음의 계산 과정을 통해 생성된다. 조합키$_{BS_1}$ ⊕ BD_$ADDR_{BS_1}$)= AID_{BS_1}, $H(AID_{BS_1}) = ID_{BS_1}$

4.2 확장 스케터넷 프로토콜

확장 스케터넷이 구성될 경우 상이한 확장 피코넷 사이의 브리지 노드가 마스터 혹은 슬레이브로 설정 될 수 있으며, 각각 서로 다른 브리지 설정 및 암호 통신을 위한 세션키 설립이 필요하다.



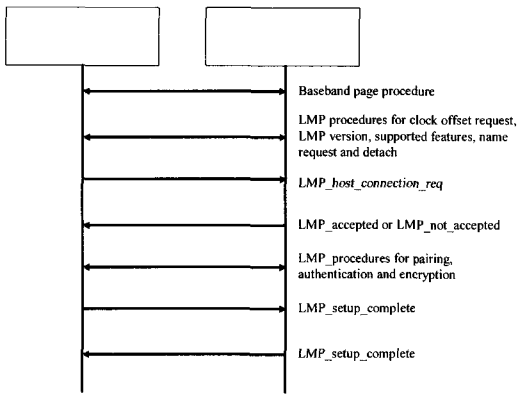
(그림 1) Kiisc05의 확장 피코넷 방식



(그림 2) 확장 피코넷 기반의 스케터넷 구성

(1) 브리지 설정

브리지 연결 설정을 위해 연결 설정은 블루투스 표준에 기반하며 그 과정은 다음과 같은 과정으로 이루어진다[1][12].



(그림 3) Connection establishment

(2) 슬레이브가 브리지 노드로 설정될 경우

브리지 노드로 슬레이브가 설정될 경우 슬레이브가 확장 피코넷의 하위 마스터인지 혹은 슬레이브인지에 따라 다른 설정과정이 요구된다.

[세부 단계 1 : 브리지 개체가 확장 피코넷 하위 마스터일 경우]

① 확장 피코넷 1의 최상위 마스터 HM_1은 브리지 노드로 설정된 블루투스 슬레이브 BS에 확장 스케터넷 통신을 요청한다.

$$Brigde\_Connection\_Request$$

② 확장 스케터넷 통신을 수신한 브리지 슬레이브 BS는 확장 피코넷 통신 단계에서 계산된 α_{BS}를 이용해 x_{BS}, y_{BS}를 다음과 같이 계산하여 확장 피코넷 1의 최상위 마스터 HM_1에 전송한다.

$$x_{BS} = H(\alpha_{BS}),$$
$$y_{BS} = H(\alpha_{BS} \oplus BD\_ADDR)$$

③ x_{BS}, y_{BS}를 전송받은 확장 피코넷 1의 최상위 마스터 HM_1은 BS와의 피코넷 설정과정에서 등록된 α_{BS}와 BD_ADDR을 확장 피코넷 주소 테이블을 기반으로 검색하여 이를 확인 한 뒤 x_{HM_1}을 계산하여 x_{HM_1}, T_{HM_1}을 브리지 슬레이브 BS에 전송한다.

$$x_{HM_1} = \alpha_{HM_1} g^{r_{HM_1}} \bmod n$$

④ 브리지 슬레이브 BS는 α_{BS}^{-1}를 이용해 $g^{r_{HM_1}}$을 추출한 뒤 이를 기반으로 x_{BS}', y_{BS}'를 계산하여 확장 피코넷 2의 최상위 마스터 HM_2에 이를 전송한다.

$$v_{BS} = g^{r_{HM_1}} \bmod n,\ x_{BS}'' = v_{BS}^{ID_{BS}^{-1}} \bmod n,$$
$$y_{BS}' = H(v_{BS}) x_{BS}' \bmod n$$

⑤ 브리지 슬레이브 BS로부터 x_{BS}', y_{BS}'를 전송받은 확장 피코넷 2의 최상위 마스터 HM_2는 확장 피코넷 (3) 피코넷 통신 과정의 ID_{BS}를 이용해 v_{BS}를 추출하여 전송된 정보를 검증한다. 만약 올바른 경우 x_{HM_2}, T_{HM_2}를 브리지 슬레이브 BS에 전송한다.

$$x_{HM_2} = \alpha_{BS} g^{r_{HM_2}} \bmod n$$

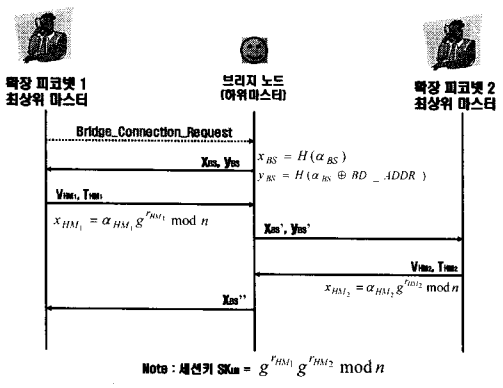
⑥ x_{HM_2}, T_{HM_2}를 전송받은 브리지 슬레이브 BS는 확장 피코넷 통신 과정에서 설정된 α_{HM_2}를 이용해 v_{BS}'을 계산한 뒤 이를 확장 피코넷 1의 최상위 마스터에 x_{BS}'', y_{BS}''을 계산하여 전송한다.

$$v_{BS}' = g^{r_{HM_2}} \bmod n,\ x_{BS}'' = v_{BS}^{ID_{BS}^{-1}}{}' \bmod n,$$
$$y_{BS}'' = H(v_{BS}')x_{BS}'' \bmod n$$

⑦ 확장 피코넷 1의 최상위 마스터 HM_1은 브리지 슬레이브 BS로부터 전송된 x_{BS}'', y_{BS}''에서 v_{BS}'를 추출하고 y_{BS}''를 검증한 한다.

이상의 과정을 수행한 뒤 확장 스케터넷 통신을 요구하는 HM_1과 HM_2는 다음과 같은 세션키 SK_{LM}를 생성해 암호 통신을 수행한다.

$$SK_{LM} = g^{r_{HM_1} r_{HM_2}} \bmod n$$



(그림 4) 확장 피코넷의 하위마스터가 브리지 개체일때의 세션키 설립

[세부 단계 2 : 브리지 개체가 확장 피코넷의 슬레이브일 경우]

① 확장 스케터넷 통신을 요구하는 확장 피코넷 1의 최상위 마스터 HM_1은 스케터넷 통신 요청 메시지를 브리지 슬레이브 BS에 전송한다.

Bridge_Service_Request

② 통신 요청을 수신한 브리지 슬레이브 BS는 확장 피코넷 1의 최상위 마스터 HM_1과 확장 피코넷 프로토콜에서 설정된 세션키 C를 이용해 다음을 계산한 뒤 x_{BS}, y_{BS}를 HM_1에 전송한다.

$$x_{BS} = E_C(BD\_ADDR \| \alpha_{BS}),$$
$$y_{BS} = H(\alpha_{BS} \oplus BD\_ADDR)$$

③ x_{BS}, y_{BS}를 수신한 HM_1은 확장 피코넷 통신과정에서 등록된 세션키 C를 이용해 x_{BS}를 복호화 한 뒤 BD_ADDR과 α_{BS}를 추출하고 y_{BS}를 검증하여 올바른 경우 다음을 계산하여 V_{HM_1}, T_{HM_1}을 브리지 슬레이브 BS에 전송한다.

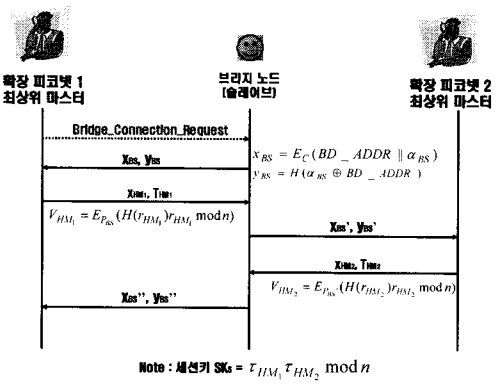
$$\beta_{HM_1} = ID_{BS} * r_{HM_1},\ \tau_{HM_1} = g^{\beta_{HM_1}} \bmod n$$
$$V_{HM_1} = E_{P_{BS}}(H(\tau_{HM_1}) r_{HM_1} \bmod n)$$

④ 브리지 슬레이브 BS는 HM_1으로 할당 받은 그룹키 쌍중 개인키에 해당되는 Q_{BS}를 이용해 V_{HM_1}을 복호화 한 뒤 τ를 검증하고 올바른 경우 x_{BS}', y_{BS}'를 HM_2에 전송한다.

$$x_{BS}' = E_{C'}(BD\_ADDR' \| \alpha_{BS}' \| \tau_{HM_1}),$$
$$y_{BS}' = H(\alpha_{BS}' \oplus BD\_ADDR')$$

⑤ x_{BS}', y_{BS}'를 전송받은 HM_2는 확장 피코넷 통신과정에서 등록된 세션키 C'를 이용해 x_{BS}'을 복호화하여 y_{BS}'을 검증한 뒤 올바른 경우 τ_{HM_1}을 임시 저장하고 V_{HM_2}, T_{HM_2}를 계산하여 브리지 슬레이브 BS에 전송한다.

$$\beta_{HM_2} = ID_{BS}' * r_{HM_2},\ \tau_{HM_2} = g^{\beta_{HM_2}} \bmod n$$
$$V_{HM_2} = E_{P_{BS}'}(H(\tau_{HM_2}) r_{HM_2} \bmod n)$$



(그림 5) 확장 피코넷 슬레이브가 브리지 개체일때의 세션키 설립

⑥ 브리지 슬레이브 BS는 전송된 정보를 HM_2로부터 할당된 그룹키 쌍중의 비밀키 Q_{BS}'을 이용해 복호화 한 뒤 τ_{HM_2}를 세션키 C로 암호화하여 x_{BS}''을 HM_1에 전송한다.

$$x_{BS}'' = E_C(BD\_ADDR \| \alpha_{BS} \| \tau_{HM_2})$$

⑦ HM_1은 세션키 C로 복호화한 뒤 τ_{HM_2}를 추출한다.

이상의 과정을 거쳐 확장 스케터넷의 브리지가 슬레이브일 경우 HM_1과 HM_2는 다음과 같은 세션키 SK_S를 생성하고 이를 기반으로 암호 통신을 수행한다.

$$SK_S = \tau_{HM_1}\tau_{HM_2} \mathrm{mod} n$$

(3) 마스터가 브리지 노드로 설정될 경우

브리지 노드로 슬레이브가 설정될 경우 2가지의 슬레이브가 확장 피코넷의 최상위 마스터인지 혹은 하위 마스터인지에 따라 서로 다른 설정과정이 요구된다.

[세부 단계 1 : 브리지 개체가 확장 피코넷 최상위 마스터일 경우]

브리지 개체가 확장 피코넷 최상위 마스터일때 확장 피코넷 내부에서 사용되는 암호 통신을 위한 키를 활용할 경우 사용자의 프라이버시 정보가 다른 피코넷 사용자에게 전송되는 취약성이 발생할 수 있다. 따라서 확장 스케터넷에서 사용되는 암호키는 확장 피코넷에서 사용되는 키와는 별도의 세션키 설립 과정이 요구된다.

① 확장 스케터넷 통신을 요구하는 HM_2는 난수 r_{HM_2}를 생성하고 확장 피코넷 통신에서 계산된 w_{HM_2}를 이용해 y_{HM_2}, e_{HM_2}, V_{HM_2}를 HM_1에 전송한다.

$$y_{HM_2} = (BD\_ADDR_{HM_2} \oplus w_{HM_2})$$

$$e_{HM_2} = H(g^{r_{HM_2}} \| y_{HM_2}),$$

$$V_{HM_2} = E_C(g^{r_{HM_2}} \| BD\_ADDR_{HM_2})$$

② y_{HM_2}, e_{HM_2}를 수신한 HM_1은 난수 r_{HM_1}을 생성하고 확장 피코넷 통신에서 계산된 w_{HM_1}을 이용해 V_{HM_1}, T_{HM_1}을 HM_2에 전송한다.

$$V_{HM_1} = E_C(g^{r_{HM_1}} \| BD\_ADDR_{HM_1})$$

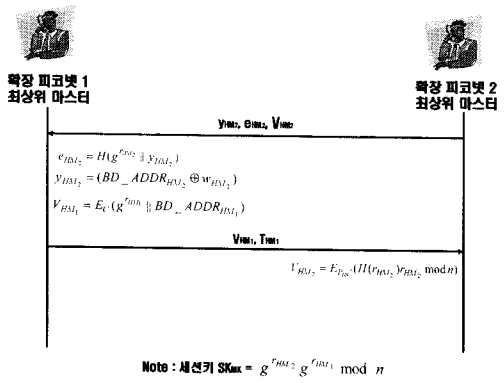
③ HM_2는 HM_1의 확장 피코넷 내부에 존재하는 개체이므로 (BD_ADDR, w값에 대한 검증은 확장 피코넷 설정과정에서 사전에 가능하다) 세션키 C를 이용해 V_{HM_1}을 복호화 한 뒤 확장 스케터넷 세션키 정보인 g^{HM_1}을 추출한다.

이상의 과정을 거쳐 최상위 마스터가 확장 스케터넷의 브리지로 연결될 경우 암호 통신을 위한 세션키 SK_{HM}은 다음과 같이 계산한다.

$$SK_{MK} = (g^{r_{HM_2}} * g^{r_{HM_1}}) \mathrm{mod} n$$

[세부 단계 2 : 브리지 개체가 확장 피코넷의 하위 마스터일 경우]

확장 스케터넷의 브리지 개체가 하위 마스터일 경우, 세부 단계2 과정을 수행하여 브리지 개체간의 암호 통신을 위한 통신 과정을 수행한다.



(그림 6) 확장 피코넷의 최상위 마스터가 브리지 개체일때의 세션키 설립

Ⅵ. 제안 방식 분석

제안 방식은 다음과 같은 특징을 가지고 있다.

• 상호인증 : 제안방식은 블루투스 기본 인증을 기반으로 각각의 디바이스가 생성하는 의사난수와 ID를 기반 $I=(ID_{S_2}\|ID_{S_3}\|....\|ID_{S_i})$ 과 $ID_{S_1}'=(H(I)-H(I))$을 생성하여 확장 피코넷에서의 상호 인증이 수행된다. 또한 확장 피코넷 기반의 스케터넷 구성시 최상위 마스터를 이용한 상호 인증 방식을 통해 브리지 노드에 대한 인증을 수행한다. 특히, 상호 인증에 사용되는 키 사이즈는 너무 커지지 않는한 안전성과 효율성을 유지할 수 있다. 따라서 타원곡선 암호화와 같은 키 사이즈가 효율적인 암호 알고리즘 적용이 가능하다.

• 기밀성과 무결성 : 피코넷 형성시 세션키 생성은 다음과 같은 검증과정을 거쳐 상호 기밀성을 유지할 수 있다. 초기 세션키 생성을 위한 검증과정은 $B_{S_1}\bmod n = w_{S_1}^{y_{S_1}}\bmod n = (\alpha_M^{ID_{S_1}^{-1}})^{(ID_{S_1}*r_{S_1})}\bmod n = \alpha_M^{r_{S_1}}\bmod n$로 수행된다. 제안방식의 검증과정에서와 같이 자신의 아이디의 역승을 이용한 이산대수 문제에 근거한 기밀성을 제공할 수 있으며, 데이터 전송의 무결성은 브로드 캐스팅된 메시지를 제외한 메시지의 경우 안전한 해쉬 함수를 이용한 무결성 서비스를 제공한다. 또한 스케터넷 구성시 피코넷 구성과는 다른 세션키 설립을 위해 피코넷 형성시에 생성된 세션키 C를 이용해 각각의 브리지 노드에 대한 세션키 $SK(SK_{LM}=g^{r_{HM_1}}g^{r_{HM_2}}\bmod n,\ SK_S=\tau_{HM_1}\tau_{HM_2}\bmod n,\ SK_S=\tau_{HM_1}\tau_{HM_2}\bmod n)$를 브리지 노드의 역할에 따라 별도로 구성함써 스케터넷만을 위한 암호 통신 서비스를 제공하였다.

• 키 갱신 범위 : 그룹 키에 대한 갱신 부분으로써 그룹 키를 사용하는 모바일 기기의 탈퇴로 인한 빈번한 모바일 기기의 특징적인 형태를 고려해 볼 때 키 갱신 범위는 현재 그룹에서 탈퇴하고자 하는 모바일 디바이스에 한정되어야 한다. 본 제안 방식에서는 그룹 환경에서 그룹 키에 대한 갱신이 이루어질 경우 해당 디바이스와의 탈퇴 통신을 통해 피코넷 마스터에 등록된 ID리스트에서 해당 디바이스의 ID를 삭제함으로써 다른 디바이스와는 지속적인 통신이 가능하도록 하였다. (조합키$_{DEL}\oplus AID_{DEL}$)=BD_$ADDR_{DEL}$을 이용한 키 갱신의 범위를 탈퇴 하는 모바일 디바이스만을 ID리스트에서 삭제한 후 갱신하는 방식을 도입하여 갱신의 범위를 최소화하였다.

• 탈퇴자에 대한 참가자의 안전성 : 피코넷 통신에서 발생되는 탈퇴자는 매 세션마다 생성되는 세션키 C의 생성에서 B를 계산 할 수 없으므로 해당 세션키를 계산할 수 없다. 따라서 탈퇴자가 발생한다 할지라도 현재의 참가자들과의 통신에 보안적 취약점을 제공하지 않는다.

• 전력 소모 공격으로부터의 안전성 확보를 위한 시스템의 독립성 : 제안 방식의 경우 블루투스 형태의 네트워크에서 예측될 수 있는 전력 소모 공격에 대한 안전성을 제공할 수 있다. 이는 공격자의 다바이스가 지속적인 전력 상태를 위한 연결 요청을 수행할 경우 Bit Comment 방식으로 이루어지는 보안 서비스 설정과정에서 인증되지 않는 모바일 디바이스의 *BD_ADDR*을 등록하여 이를 초기에 차단함으로써 지속적인 연결 요청과 같은 전력 소모 공격에 안전성을 제공할 수 있다.
• 효율성 : 제안 방식은 무선 환경이라는 점을 고려해 볼 때 지수승 연산을 최소한으로 지양하고 해쉬 함수와 XOR 연산을 기반으로 효율성을 높이고자 하였다. 그러나 논문의 전체적인 프로토콜에서 사용되는 지수승 연산은 많은 오버헤드를 발생시킬 수 있어 기존 블루투스와 비교해볼 때 효율적인 특성은 낮다고 할 수 있다.

제안방식에 대한 안전성을 기존 블루투스 네트워크 구성방식과 비교해 볼 때 표 1과 같이 정리할 수 있다.

표 1에서의 취약(X)는 보안 서비스를 제공하지 않는 경우이며, 보통(△)은 보안 서비스를 제공하나 취약성을 내포하고 있는 경우이며, 안전(O)은 안전한 통신 서비스가 가능한 경우이다.

(표 1) 제안방식 분석

보안 요구사항			블루투스 표준 v1.1	Kiisc05 방식	제안 방식
상호 인증	마스터와 마스터		△	O	O
	마스터와 슬레이브		△	O	O
	브리지 노드	노드 인증	X	X	O
		동등 레벨간의 인증	X	X	O
		상이한 레벨 노드간의 인증	X	X	O
기밀성과 무결성	전송 데이터		△	O	O
	저장 데이터		△	O	O
키 갱신 범위			X	O	O
탈퇴자에 대한 참가자의 안전성			X	O	O
전력 소모 공격으로부터의 시스템의 독립성			X	O	O
시스템의 확장성			X	X	O
효율성			소형화 디바이스에서 구현 가능	PID와 같은 보안 디바이스에 구현 가능	PID와 같은 보안 디바이스에 구현가능

[X : 취약, △ : 보통, O : 안전]

Ⅶ. 결 론

유비쿼터스는 우리의 일상이 네트워크로 연결되어 있는 상태를 의미하며, 모든 정보가 공유되고 누구나 쉽게 접근할 수 있다. 따라서 이와 관련된 연구가 국내외적으로 활발히 진행되고 있어 유비쿼터스 사회의 실현은 현실로 다가오고 있다. 이미 국내에서는 홈네트워크 시범사업이나 u코리아 추진 전략 등을 통해 구체적으로 현실화 되고 있다. 유비쿼터스를 구체화하기 위한 연구 중에서 블루투스는 필요 기술로 선정된 후 새로운 형태로의 적용을 위한 다양한 연구가 절실히 요구되고 있다. 이에 본 논문에서는 기존의 블루투스 표준에 대한 보안 분석을 통해 사용자 중심의 네트워크 구성과 확장에 대한 연구의 연장선상에서 확장 피코넷 기반의 확장 스케터넷에 대한 연구를 수행하였다. 제안 방식은 2005년에 제안된 Kiisc05에 제안된 확장 피코넷 이후의 확장된 네트워크의 구성이 발생할 수 있는 보안 취약성을 보완하기 위해 브리지 노드 형태에 따라 보안 서비스 제공을 위한 새로운 구성 방법과 보안 서비스 설정 방법을 제시함으로써 블루투스가 갖는 특징적인 네트워크의 전체적인 확장 방법을 제시하였다. 그러나 효율성 측면에서는 기존 Kiisc05 방식의 가장 큰 문제점인 슬레이브 개수 증가에 따른 블루투스 주소 비트의 확장에 대해서는 여전히 고려되지 않고 있으며, 스케터넷으로 확장

되었을 때 여러 형태의 그룹 보안 요구사항을 만족하지 못하고 있는 실정이다. 따라서 향후 연구 방향으로는 확장된 형태의 블루투스 네트워크 구성시 주소 비트를 확장시켜 각각의 주소 비트에 대한 추가적인 정의와 이를 기반으로 이루어지는 보안 문제점들에 대해 보다 심도있는 연구가 필요할 것으로 사료된다.

참 고 문 헌

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

[2] Bluetooth Security Architecture, 1999.

[3] Specification of the Bluetooth System, 1999.

[4] M.Hermelin and K. Nyberg. Correlation Properties of the Bluetooth Combiner Generator. In ICISC'99, volume 1787 of LNCS. Springer Verlagg, 2000.

[5] S. Fluhrer and S. Lucks, "Analysis of the E0 Encryption System" available from S.Lucks' website at http://th.informatik.uni-mannheim.de /People/Lucks/papers/e0.ps.gz, agnu-zipped Postscript file

[6] Bluetooth SIG, Specification of the Bluetooth system, Profiles" , Version 1.1, February 22, 2001, available at http://www.bluetooth.com/

[7] Bluetooth SIG, Specification of the Bluetooth system, Core ", Version 1.1, February 22, 2001, available at http://www.bluetooth.com/

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

[9] http://www.cs.hut.fi/Opinnot/Tik-86 .174/sectopics .html (Ullgren T, "Security in Bluetooth Key management in Bluetooth", 2001)

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

[11] http://mmlab.snu.ac.kr/research/publication/docs/ KISS2002_jklee.pdf

[12] http://csdl.computer.org/comp/proceedings/hicss/ 2003/1874/09/187490314b.pdf

[13] 서대희, 이임영, 김해숙, "홈 네트워크에 적용한 Bluetooth Security에 관한 연구," 한국통신학회 하계 학술발표회, Vol23, No1, pp32-35, 2001.

[14] 서대희, 이임영, 김해숙, 김영백, "Bluetooth Security에 관한 고찰" 한국정보보호학회지, 제 11권 4호, pp76-86, 2001.

[15] 서대희, 이임영, 김해숙, 김영백, "ECC를 이용한 안전한 piconet에 관한 연구" 한국정보처리학회 추계 학술 발표 논문집, 제 8권 제 2호, pp911-914, 2001.

[16] 서대희, 이임영, "안전한 유비쿼터스를 위한 확장성 있는 블루투스 피코넷에 관한 연구", 한국정보보호학회, 제 15권, 제 5호, pp 13-24, 2005.

[17] 최용락, 소우영, 이재광, 이임영 "통신망 정보 보호", 도서출판 그린, 1997.2.

[18] 이만영, 김지홍, 류재철, 송유진, 염흥렬, 이임영 "전자상거래 보안 기술", 생능출판사, 1999.8.

[19] 최용락, 소우영, 이재광, 이임영 "컴퓨터 통신 보안", 도서출판 그린, 2001.2

[20] 이임영 "전자상거래 보안입문", 생능출판사, 2001.8

◐ 저 자 소 개 ◑

백 장 미(Baek Jang-Mi)
2001년 순천향대학교 컴퓨터학 졸업(학사)
2003년 순천향대학교 대학원 전산학과 졸업(석사)
2006년 순천향대학교 대학원 전산학과 졸업(박사)
2007년 Post-Doc of Howard University
관심분야 : 임베디드 시스템, 유비쿼터스 네트워크, 유비쿼터스 컴퓨팅
E-mail : bjm1453@sch.ac.kr

서 대 희(Seo Dae-hee)
2001년 동신대학교 전기전자공학과 졸업(학사)
2003년 순천향대학교 대학원 전산학과 졸업(석사)
2006년 순천향대학교 대학원 전산학과 졸업(박사)
2007년 Post-Doc of Howard University
관심분야 : 네트워크 정보보호, 암호학, 유비쿼터스 컴퓨팅
E-mail : patima@sch.ac.kr