情報保護學會論文誌
第15卷 第5號, 2005. 10

안전한 유비쿼터스를 위한 확장성 있는 블루투스 피코넷에 관한 연구

서 대 희,†‡ 이 임 영
순천향대학교

A Study on Scalable Bluetooth Piconet for Secure Ubiquitous

Dae-Hee Seo,†‡ Im-Yeong Lee
SoonChunHyang University

요 약

무선 정보 환경의 변화에 따라 사용자가 요구하는 정보의 질적 풍족감이 요구되고 이에 따라 많은 근거리 무선 통신 기술들이 개발되고 연구되어 왔다. 그 중에서도 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 서비스 뿐만 아니라 새로운 형태의 네트워크 구성이 요구된다. 따라서 본 논문에서는 기존 블루투스 통신을 통한 피코넷 구성시 슬레이브 개수의 제한에 대한 취약성을 분석하고 스캐터넷으로 구성하지 않아도 피코넷 내부에서 슬레이브 개수와 무관한 확장된 블루투스 피코넷 구성 방식을 제안한다. 제안 방식은 기존 피코넷의 확장된 형태로써 트리 형태의 구조로 피코넷을 형성하여 기존의 피코넷에서 발생할 수 있는 보안 취약성을 보완 할 수 있는 방식을 제안하였다.

ABSTRACT

Due to the changes in the wireless information environment, there has been an increased demand for various types of information. Accordingly, many wireless communication technologies have been studied and developed. 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, this research analyzed the vulnerability on the limited number of slaves in a piconet configuration through the current Bluetooth communication and proposed an expanded Bluetooth piconet formation method, regardless of the number of slaves inside the piconet even if it is not configured in a scatternet. In the proposed method, we applied a security service and resolved the vulnerabilities of the current piconet by configuring an expanded form of the current tree-shaped structure.

Keywords : *Mobile communication, Bluetootht, Piconet*

접수일 : 2005년 2월 21일 ; 채택일 : 2005년 10월 6일
† 주저자, ‡ 교신저자, patima@sch.ac.kr

Ⅰ. 서 론

최근 모바일 디바이스가 대중화 되어 사용되고 있으며, 각 디바이스의 계층 사이에 통신 채널에 대한 연구들이 진행되고 있다[1]. 따라서 디바이스의 한계를 극복하고 서로의 디바이스들이 통신할 수 있는 무선 환경의 인터페이스에 대한 고려로부터 시작된 연구가 블루투스이다.

블루투스는 1994년 에릭슨의 통신 그룹이 핸드폰과 주변 디바이스 사이의 소비전력이 낮고 가격이 싼 무선 인터페이스를 연구하기 시작하면서 비롯하였다. 블루투스 연구는 1998년에 에릭슨, 노키아, IBM, TOSHIBA, Intel 등으로 구성된 SIG(Special Interest Group)가 발족되면서 본격적인 연구가 진행되고 있다. 블루투스는 고정 또는 모바일성을 가진 각각의 디바이스에 정보를 전송하는 무선 통신 프로토콜로써 채널을 공유한 복수개의 장치들이 1개의 마스터라는 모바일 디바이스를 중심으로 피코넷을 형성하여 스케터넷으로의 확장이 이루어진다.[1-3]

그러나 유비쿼터스와 같은 새로운 환경에서 사용자 주변의 모바일 기기의 증가에 따라 현재의 블루투스를 적용하였을 경우 모바일 디바이스 개수의 제약에 따른 문제점이 제기되고 있다.

따라서 본 논문의 2장에서는 블루투스의 개요와 확장된 형태의 피코넷 구성에 필요한 보안적인 요구사항을 제시한다. 3장에서는 기존 블루투스 통신으로 형성되는 피코넷과 스케터넷이 가질 수 있는 보안적 취약점과 슬레이브 개수의 한계성으로 발생할 수 있는 취약성 분석을 기술하고, 4장에서는 3장에서 제시된 취약성을 보완하기 위해 블루투스를 위한 확장 피코넷 형성 방식을 제안하고자 한다. 5장에서는 제안 방식과 기존 방식을 2장에서 제시한 보안적인 요구사항을 기반으로 분석한 뒤 6장에서 결론을 맺고자 한다.

Ⅱ. 블루투스 기술 분석

본 장에서는 유비쿼터스 통신 기술로 연구가 진행중인 블루투스에 대한 개요와 확장된 형태의 피코넷 형성시 요구되는 보안 사항에 대해 기술하고자 한다.

1) 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성지원사업의 연구결과로 수행되었음

2.1 블루투스의 개요

무선 통신상의 정보교환을 위해서 키 분배 및 인증 등이 필요하며 송/수신된 메시지에 대해 부인봉쇄를 수행할 수 있어야 한다. 또한 제 3자의 불법적 도청으로부터 송신자의 신원 노출을 방지하기 위하여 사용자 기밀성을 확보해야 한다. 다음은 이들에 대한 요구 사항을 기술한 것이다. 우리나라말로 해석하면 '푸른 이빨'이란 뜻으로 해석되는 블루투스는 스칸디나비아 국가인 덴마크와 노르웨이를 통일한 바이킹 해럴드에서 유래되었다. 블루투스는 최초 스웨덴의 에릭슨에서 무선 근거리 통신을 위해 저전력, 저비용으로 무선 인터페이스를 가능하게 하기 위한 기술로서 시작된 프로젝트 이름이었다. 이에 따라 블루투스에 관심을 갖는 회사들은 1998년 5월에 무선 근거리 통신을 위한 하나의 프로젝트 개발을 위해 그룹을 결성하였다. 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, IEEE 802.11, SWAP (Shared Wireless Access Protocol)과 같은 무선 근거리 무선통신들이 많이 등장하였다. 다른 무선 통신 기술과 블루투스를 사용자 관점에서 비교해 볼때 블루투스는 적은 소모 전력으로 휴대폰이나 기타 주변장치들의 무선 연결을 통해 선이 없는 인터페이스를 통해 보다 간편하고 효율적인 측면에서 다가서고 있다. 전체적인 측면에서 블루투스가 주목받는 이유는 정보통신 산업이 무엇을 위해 발전하였는가를 살펴보면 쉽게 알아볼 수 있다. 따라서 보다 자유롭고, 안전하며, 새로운 인터넷 기술과 융합할 수 있는 기술이 블루투스라 할 수 있다.

블루투스의 또 다른 특징의 하나는 작은 네트워크의 구성이 가능하다는 것이다. 이는 피코넷이라 불리우며 하나의 피코넷에는 2개에서 최대 7개까지의 슬레이브(Slave)가 가능하다. 이러한 피코넷이 여러개가 모여 서로 연결되어 있을 때 이를 스케터넷이라 한다. 결국 피코넷은 여러 통신장비를 하나의 통신 네트워크로 묶을 수 있다는 장점이 된다.[1,2,5,6]

2.2 확장 피코넷 보안 요구사항

블루투스는 다양한 환경에 적용 가능한 장점이 있

다. 특히, 2.1에서 기술한 것과 같이 하나의 작은 네트워크 구성 역시 블루투스가 갖는 장점 중에 하나이다.

그러나 최근 유비쿼터스 또는 센서 네트워크와 같은 새로운 환경에 대한 적용성 문제와 모바일 기기의 보편화에 따라 개인이 소유할 수 있는 모바일 디바이스의 증가는 피코넷에서의 슬레이브 개수에 대한 한계성을 취약성으로 지적할 수 있다. 그러나 기존의 연구는 확장된 형태의 스케터넷에 대한 알고리즘 연구나 구성에 대한 연구가 이루어지고 있는 실정이다. 이는 스케터넷을 구성하는 피코넷은 기본 구성으로 하여 구성되고 있다. Maryland 대학에서 이루어지는 연구의 경우 BTCP 연구는 지역내의 비교적 많은 기기들이 가능한 빨리 연결하는 알고리즘 연구를 수행하고 있으며, MIT에서 수행중에 있는 스케터넷 형성 알고리즘에 대한 연구는 스케터넷 형성시 시간과 메시지를 최소화하기 위한 연구를 수행하고 있다. 그러나 두 연구 모두 스케터넷의 기반이 되는 피코넷과 관련된 연구는 미흡한 실정이다. 또한 보안적 측면에서의 고려 보다는 효율성을 높이기 위한 방안들이 지속적으로 제시되고 있는 실정이다.

따라서 개인 중심의 피코넷이 형성될 경우 현재의 피코넷 방식은 디바이스 개수의 제약사항과 개인 프라이버시 보호를 위한 문제점이 발생할 수 밖에 없으며, 이를 보완할 수 있는 방법이 확장된 형태의 피코넷 형성 방법이다. 확장 피코넷이 형성될 경우 슬레이브 개수와는 무관한 피코넷 형성이 가능하며 이는 스케터넷으로 피코넷을 확장할 경우 발생할 수 있는 제약사항을 보완할 수 있는 방식이다.

블루투스를 이용한 확장 피코넷 형성시 하나의 슬레이브는 다른 슬레이브의 마스터(하위 마스터)로 구성이 가능하며, 최상위 마스터와 하위 마스터는 트리 형태로 종속 관계를 유지한다. 이는 기존의 블루투스에 7개의 슬레이브 개수에 대한 제약성을 최대한 14개까지로의 확장이 가능하다. (이는 현재의 블루투스 통신이 가능한 모바일 기기(PTD : Personal Trust Device)의 컴퓨팅 능력을 고려해볼 때의 개수이다.)

따라서 슬레이브 개수의 제약사항을 보완하면서 안전하고 효율적인 피코넷 형성을 제안하기 위해서는 다음과 같은 보안 요구사항을 만족해야 한다.[8-10]

- 상호인증 : 블루투스 초기 보안 키 설정 과정에서의 상호인증과는 별도로 확장 피코넷 형성에 따른 안전한 상호 인증 과정이 필요하다. 블루투스 피코넷에서의 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 해쉬함수를 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.
- 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

본 장에서는 기존의 블루투스 통신시 발생할 수 있는 보안 취약점과 블루투스 통신을 이용해 형성된 네트워크에서의 보안 취약점으로 구분하여 이를 분석하고자 한다.

3.1 블루투스 통신시 발생할 수 있는 보안 취약점 분석

다양한 무선 장비사이에서의 음성과 데이터 통신을 가능하게 하는 기술인 블루투스는 고정된 네트워크 장비가 없는 작은 범위의 지역망에 가장 적합한 기술로 떠오르고 있다. 특히, 매우 저렴한 가격으로

구입할 수 있는 단 하나의 작은 마이크로칩만으로 모든 형태의 휴대 장치와 네트워크 장치를 무선으로 연결 가능케 함으로 인해서 모든 무선 장비 사이의 유선 케이블을 제거할 수 있다. 블루투스 표준에 따르면, 블루투스 네트워크에서의 통신을 위한 기본 구조는 스타형의 단일 홉 네트워크인 피코넷을 구성하는 것이다. 피코넷은 하나의 마스터와 7개 이하의 활성화된 슬레이브 노드를 가지게 된다. 따라서 피코넷 내부의 모든 활성화된 블루투스 노드들은 같은 영역의 1-Mbps Frequency Hopping Spread Spectrum(FHSS) 채널을 시간 분할 다중화 기법(Time Division Multiplexing Scheme)을 이용하여 공유하며 마스터 노드가 시간 분할 다중화 기법을 제어 한다. 만일 다수의 피코넷들이 공통된 영역을 분포하고 있다면, 블루투스 디바이스들은 하나 이상의 피코넷에 참가할 수 있다. 따라서 다수의 피코넷을 연결하는 것이 가능해진다. 하나의 슬레이브는 동시에 여러 피코넷의 슬레이브가 될 수 있으며 동시에 마스터이면서 다른 피코넷의 슬레이브로 동작 할 수도 있다.

그러나 블루투스 디바이스는 동시에 2개 이상의 피코넷의 마스터가 될 수는 없다. 다수의 피코넷을 연결해서 만들어지는 네트워크를 블루투스에서는 스케터넷이라고 부른다. 스케터넷은 대규모 통신망을 지원하면서 그와 동시에 다른 피코넷의 노드로서 동작하기 위해서 하나의 노드는 다른 피코넷의 주파수 순서로 스위칭해야만 한다. 그러나 유비쿼터스와 센서 네트워크와 같은 새로운 환경에 블루투스를 적용하고자할 경우 피코넷과 같은 네트워크는 다음과 같은 취약성을 내포하고 있다.[1,8,9]

- 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 : 피코넷 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 피코넷 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 : 유비쿼터스와 센서 네트워크와 같이 작은 모바일 디바이스의 네트워크에 적용하기 위해서는 현재의 블루투스의 네트워크보다 확장성을 제공하는 네트워크 형성을 제공할 수 있어야 한다.

3.2 블루투스 통신을 이용한 네트워크 형성시 발생되는 취약성 분석

블루투스 네트워크는 특별한 목적을 위하여 생성되는 네트워크로서 모든 장치들은 무선으로 서로 연결된다. 개인적인 디바이스들은 다른 장치들에 메시지들을 브로드 캐스팅할 때 장치들간에 직접적인 메시지를 받기 위해서는 장치들간에 거리가 문제시된다. 이는 모바일적인 특성을 가진 장치들이 다른 장치들간의 전달 범위의 안팎으로 움직일 때 유동성을 가진다. 블루투스 통신을 통한 네트워크 형성의 특성상 매우 특별한 목적을 위하여 형성된 네트워크이며, 공격에 매우 취약한 구조를 가지고 있다. 또한 매우 복잡한 보안이 필요하게 된다.[9,10]

이러한 블루투스 네트워크의 보안은 크게 시스템의 독립성, 권한부여와 키관리, 기밀성과 무결성으로 나눌 수 있다.

- 시스템의 독립성 : 블루투스로 형성된 네트워크 사이에 모든 장치들은 네트워크에서 이루어지는 브로드 캐스팅된 메시지에 서로 의존한다. 이러한 것은 서비스 거부 공격(Denail of Service) 공격에 매우 취약하다. 또한 블루투스 디바이스들은 장치가 활동중이지 않을 때 전력의 소모를 막기 위해서 전력 모드를 수시로 바꾼다. 따라서

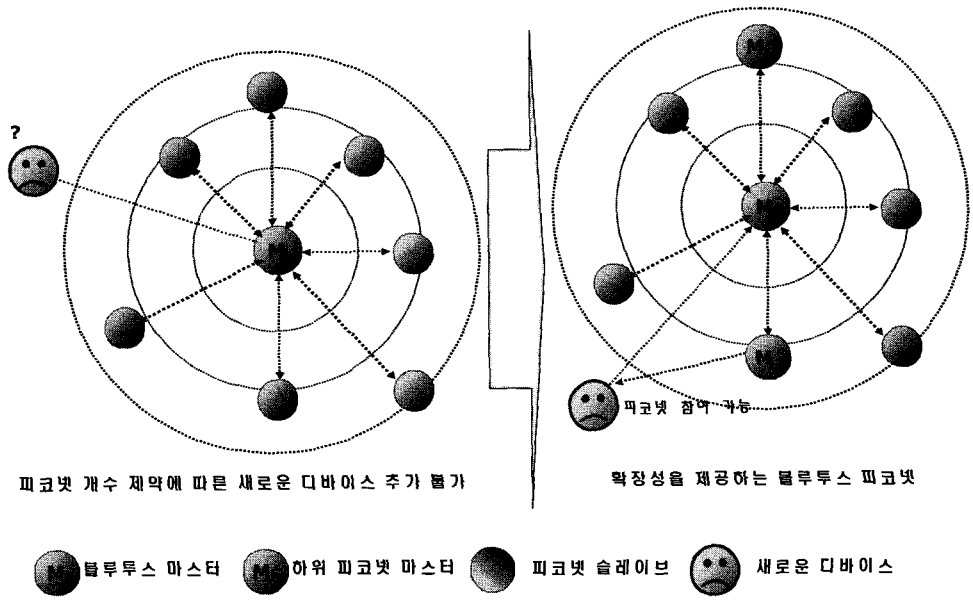

그림 1. 제안방식 시나리오

공격자는 디바이스의 전력 상태를 지속적으로 공격함으로써 사용자의 디바이스가 전력 소모가 많게 하여 결국엔 오프 상태로 만들 수 있다.

- 권한부여와 키 관리 : 블루투스로 형성된 네트워크를 안전하게 하는데 중요한 요소가 권한부여와 키 관리이다. 따라서 신뢰할 수 있는 키 관리 인증 - 키 관리 기술을 기반으로 모든 가능한 공격의 형태에 대해 강력한 인증이 필요로 하게 된다.
- 기밀성과 무결성 : 기밀성과 무결성은 블루투스로 형성된 네트워크에서 매우 취약한 부분이다. 기밀성은 암호화를 통해 유지하게 되는데 피코넷 통신에서 공격자들은 암호화 없이 송신되는 메시지들을 매우 쉽게 취득할 수 있다. 무결성은 안전한 해쉬 함수를 통해 전송 데이터의 변조 및 위조에 대한 취약성을 보완하기 위해서 반드시 요구되는 사항이다.

Ⅳ. 확장성 있는 블루투스 피코넷 방식 제안

본 제안 방식은 새로운 네트워크 환경에 근거리 무선 통신중의 하나인 블루투스를 적용하기 위해 현재의 블루투스로 형성된 피코넷의 취약성인 슬레이브 개수에 대한 제약 사항을 보완하면서 안전하고 효율적인 형태의 통신 방식을 제안한다. 제안 방식의 구성 개체는 블루투스 마스터, 블루투스 슬레이브로 구성된다. 본 논문에서는 블루투스를 이용한 확장 피코넷을 구성하기 위해서 각각의 모바일 디바이스는 공개키 인증서를 저장하고 있다는 가정을 기반으로 구성된다.(그림 1 참조)

4.1 시스템 계수

다음은 블루투스 네트워크 환경에서 확장성을 갖는 피코넷을 제안하기 위한 시스템 계수를 기술한다.

* : (마스터(M), 슬레이브(S_1, S_2, ,S_n), 새롭게 피코넷에 가입하고자 하는 슬레이브(S_8), 피코넷에서 탈퇴하고자 하는 슬레이브(DEL))

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

e, β, k, α, r : 의사난수

$H()$, $E()$: 안전한 해쉬 함수, 대칭키 암호 알고리즘

n : 각 객체에 공개된 시스템 계수

T_* : *가 생성한 타임 스탬프

BD_ADDR : 모바일 기기의 48bit 고유 주소

$ConnectionRequest$: 접속 요구 메시지

MD_{State} : 모바일 디바이스의 상태

M_w, M_{res} : 피코넷 슬레이브의 상호 인증 메시지, 상호 인증 메시지에 대한 응답 메시지

ID_* : 마스터와 슬레이브 사이에서 공유되어 있는 식별자 ($i=1,2,...,n$)

AID_* : 조합키와 BD_ADDR을 기반으로 계산된 슬레이브의 중간 검증값

4.2 제안방식 프로토콜

4.2.1 그룹 초기화

블루투스 피코넷 마스터는 현재의 피코넷에 포함된 슬레이브들과 사전에 설정한 조합키와 슬레이브들의 공개된 BD_ADDR을 이용하여 각 슬레이브들의 고유 ID 리스트를 다음과 같이 계산하여 피코넷 그룹 통신을 위한 그룹 초기화 단계를 수행한다.

$$(\text{조합키}_{S_i} \oplus \text{BD\_}ADDR_{S_i}) = AID_{S_i} \quad H(AID_{S_i}) = ID_{S_i}$$

전체 슬레이브의 고유 ID 리스트 I는 다음과 같다.

$$I = (ID_{S_1} \| ID_{S_2} \| ID_{S_3} \| ... \| ID_{S_n})$$

4.2.2 새로운 슬레이브 디바이스의 그룹 가입 단계

새로운 모바일 기기가 기존 피코넷에 새로운 개체로 가입을 요청할 경우 해당 슬레이브는 가입하고자 하는 피코넷의 마스터 디바이스와 초기 보안 키 생성 과정을 거쳐 인증 과정을 수행한 뒤 피코넷 마스터의 ID 리스트 I를 갱신하여 이를 추가함으로써 새로운 모바일 디바이스를 자신의 피코넷 개체로 인정한다.

4.2.3 피코넷 통신 단계

① 마스터는 같은 피코넷에 있는 각각의 슬레이브 중의 ID_{S_i}에 해당되는 모바일 기기와 통신을 위해 전체 ID 리스트 I에서 수신 디바이스 ID_{S_i}을 제외한 I'를 생성하여 ID_{S_i}'를 생성한다. (본 과정은 마스터가 피코넷 내부의 슬레이브들과 통신을 수행하기 전에 통신을 수신하는 슬레이브를 내부적으로 확인하는 단계로서, 현재 어떤 통신을 수행하고자하는 슬레이브가 자신의 피코넷 내부에 등록된 슬레이브인지를 확인하는 초기 수행단계이다.)

$$I' = (ID_{S_2} \| ID_{S_3} \| ... \| ID_{S_i}), \quad ID_{S_i}' = (H(I) - H(I))$$

② 마스터는 의사난수 α_M를 생성하여 w_M을 다음과 같이 계산한다. (w_M은 마스터와 슬레이브의 세션키 설립을 위해 마스터에서 생성한 난수를 기반으로 전송되는 세션키 생성정보이다.)

$$w_M = \alpha_M^{ID_{S_i}^{-1}} \bmod n$$

이상의 내용을 기반으로 하여 피코넷의 마스터는 슬레이브(ID_{S_i})에 w_M, α_M을 전송한다.

③ 피코넷의 마스터로부터 전송받은 w_M, α_M을 전송받은 슬레이브는 ID_{S_i}을 이용해 w_{S_i}을 계산한 뒤 마스터로부터 전송된 w_M에 대한 비교를 통해 전송된 정보의 정당성을 확인한다.

$$w_{S_i} = \alpha_M^{ID_{S_i}^{-1}} \bmod n, \quad w_M \equiv w_{S_i} \text{이면}$$

이를 기반으로 세션키 생성을 위한 중간값인 B_{S_i}, T_{S_i}을 마스터에게 전송한다.

$$y_1 = ID_{S_i} * r_{S_i}, \quad B_{S_i} = w_{S_i}^{y_1} \bmod n$$

④ B_{S_i}, T_{S_i}을 전송받은 마스터는 임의의 j개의 그룹 키 쌍을 생성한 후 임의의 그룹 키 쌍 (P_{S_i}, Q_{S_i})를 선택하여 세션키 C_1으로 암호화하여 해당 슬레이브에게 전송한다.

$$C_1 = \alpha_M^{r_{S_i} * AID_{S_i}} \bmod n$$

이상의 단계를 거쳐 마스터는 슬레이브를 해당 피코넷에 추가하기 위한 피코넷 가입 단계를 수행한다.

4.2.4 피코넷 탈퇴 과정

피코넷을 탈퇴하고자 하는 모바일 디바이스의 경우 피코넷 탈퇴를 요구하는 메시지를 해당 피코넷 마스터 디바이스에게 전송한다.

① 탈퇴하고자 하는 디바이스는 세션키 C_1을 이

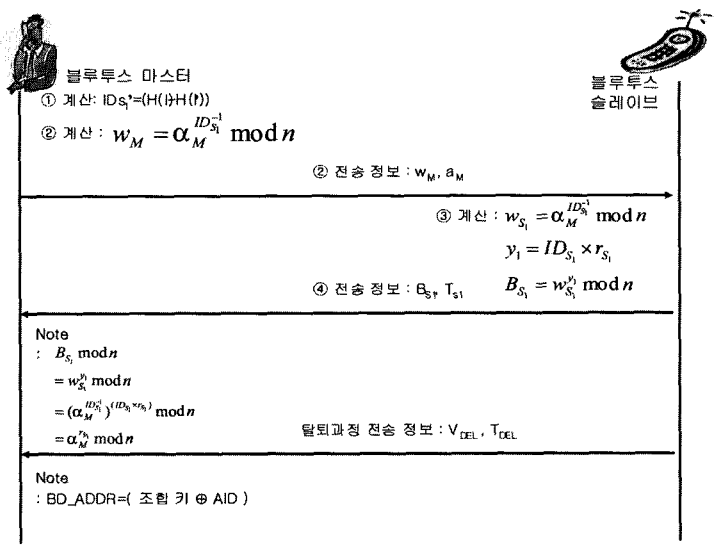

그림 2. 블루투스 피코넷 설정 과정 및 탈퇴 과정

용해 V_{DEL}를 계산한 뒤 해당 마스터에 V_{DEL}, T_{DEL}를 전송함으로써 피코넷 탈퇴 과정을 수행한다.

$$V_{DEL} = E_{C_1}(H(AID_{DEL} \oplus 조합키_{DEL}))$$

② V_{DEL}, T_{DEL}를 전송받은 블루투스 마스터는 XOR 연산을 수행하여 해당 ID에 대응되는 H(BD_$ADDR_{DEL}$)과의 동일성을 검증한다.

$$(조합키_{DEL} \oplus AID_{DEL}) = \text{BD\_}ADDR_{DEL}$$
$$H(조합키_{DEL} \oplus AID_{DEL}) \stackrel{?}{=} H(\text{BD\_}ADDR_{DEL})$$

이상의 과정이 올바른 경우 생성된 BD_ADDR에 대응되는 슬레이브의 해당 ID를 전체 ID 리스트 I에서 삭제하여 피코넷 탈퇴 서비스를 제공한다. 이상의 프로토콜은 그림 2와 같이 요약해 볼 수 있다.

4.2.5 확장 피코넷 초기 설정 단계

최대 슬레이브 개수가 7개인 피코넷이 설정된 후 제 8의 정당한 모바일 기기가 해당 피코넷에 접속을 요청할 경우 피코넷을 확장해 제 8의 정당한 모바일 기기를 피코넷 개체로 구성하는 초기 단계이다.

① 제 8의 정당한 모바일 기기는 접속 요구 메시지(*ConnectionRequest*)와 공개키 P_{S_8}을 해당 마스터에 전송한다.

② 접속 요청을 받은 해당 피코넷 마스터는 제 8의 모바일의 P_{S_8}과 접속 요청 메시지를 확인하고 현재 자신의 피코넷 슬레이브의 상태(파워상태, 컴퓨팅 능력, 메모리)에 대한 메시지를 요청하는 브로드캐스팅 메시지(*Broadcasting Message Request*)를 전송한다.

③ 브로드캐스팅 메시지를 수신한 해당 피코넷 슬레이브들은 요청 메시지에 해당되는 파워상태, 컴퓨팅 능력, 메모리에 대한 메시지를 다음과 같은 연산 과정을 거쳐 P_*, V_*를 피코넷 마스터에 전송한다.

$$V_* = E_{C_*}(MD_{state} \| T_*)$$

④ 피코넷 슬레이브의 정보를 각각 전송받은 피코넷 마스터는 피코넷 슬레이브에 대한 정보를 비교하여 가장 높은 파워상태, 컴퓨팅 능력, 메모리를 보유하고 있는 모바일 디바이스를 선택하여 제 8의 모바일 디바이스와 하위 피코넷 형성을 위한 통신을 요청한다. (ID_{S_3}'은 마스터에서 통신을 수행하는 슬레이브를 확인하는 값이며, 3번째 슬레이브 (ID_{S_3})가 가장 높은 상태를 유지하고 있을 경우, V_M, T_M을 전송)

$$I' = (ID_{S_1} \| ID_{S_2} \| ID_{S_4}, ..., \| ID_{S_7})$$
$$ID_{S_3}' = (H(I) - H(I')), V_M = E_{C_{S_3}}(ID_{S_3} \oplus \alpha_M)$$

4.2.6 하위 피코넷 설정단계

하위 피코넷 설정단계는 상위 피코넷 마스터로부터 하위 피코넷 형성을 위한 통신을 요청받은 상위 피코넷 슬레이브는 제 8의 모바일 기기와 하위 피코넷 형성을 위한 4.2.2의 과정을 수행하고 초기 설정 단계를 실시한다.

① 피코넷의 마스터 디바이스가 설정해준 슬레이브는 제 8의 모바일 디바이스와 초기 보안 키 생성 과정을 거쳐 인증 과정을 수행한 뒤 확장 피코넷 마스터으로써의 I_1을 생성하여 ID_{S_8}을 추가함으로써 새로운 모바일 디바이스를 자신의 피코넷 개체로 포함한다.

$$I_1 = (ID_{S_3} \| ID_{S_8})$$

② 하위 피코넷 형성에 따른 피코넷 내부 통신은 4.2.3~4.2.4의 과정을 수행한다. 그림 3은 4.2.5의 과정을 도해시한 그림이다.

4.2.7 상위 마스터와 하위 마스터 통신의 경우-1

확장 피코넷에서 최상위 마스터 A와 하위 마스터 B(=슬레이브 3)와의 통신이 요구될 경우 다음과 같은 과정을 거쳐 보안 통신 서비스 초기화 단계가 수행된다.

① 하위 마스터 B는 난수 k_{S_3}를 선정하여 최상위 마스터 A에 전송한다.

② 최상위 마스터 A는 난수 k_{S_3}를 수신한 후 X를 계산하여 하위 마스터에 b, X를 전송한다. ($\beta_{S_3} \in \{0, 1, 2\}$)

$$X = k_{S_3}^{\beta_{S_3}} g^b \bmod n,\ b = H(ID_{S_3} \oplus \beta_{S_3})$$

- X는 β의 값에 따라 g^b, $k_{S_3} g^b$, $k_{S_3}^2 g^b$ 값을 갖게 된다.

③ 최상위 마스터는 비밀정보 확인을 위해 b를 하위 마스터에 전송한다. 하위 마스터는 $g^b \bmod n$을 계산하여 그 값이 X이면 $\beta_3 = 0$이고, X가 아니면, $g^b \bmod n$에 k_{S_3}를 곱한값이 X인지 또는 $g^b \bmod n$에 $k_{S_3}^2$를 곱한 값이 X인지 확인하여 b를 확인한다.

각각의 k_{S_3}의 값에 따라 블루투스 보안 서비스를 선택하게 된다.

- 보안 서비스 1($k_{S_3}^0$) : 인가와 인증을 요구한다. 자동 접근이 신뢰 장비에 대해서만 허용된다. 비신뢰 장비는 수동인가가 요구된다.(초기 접속 시 보안 서비스 1의 형태로 제공되지만, 인증 이후 지속적인 연결이 있을 경우 자동적으로 보안 서비스 3형태로의 전환을 제공할 수 있는 부가적 서비스를 제공한다.)
- 보안 서비스 2($k_{S_3}^1$) : 인증만을 요구한다. 인증 프로시저를 거친 후에 어플리케이션에 대한 접근이 허용된며, 인가는 요구되지 않는다.
- 보안 서비스 3($k_{S_3}^2$) : 모든 장비에 대해 개방적

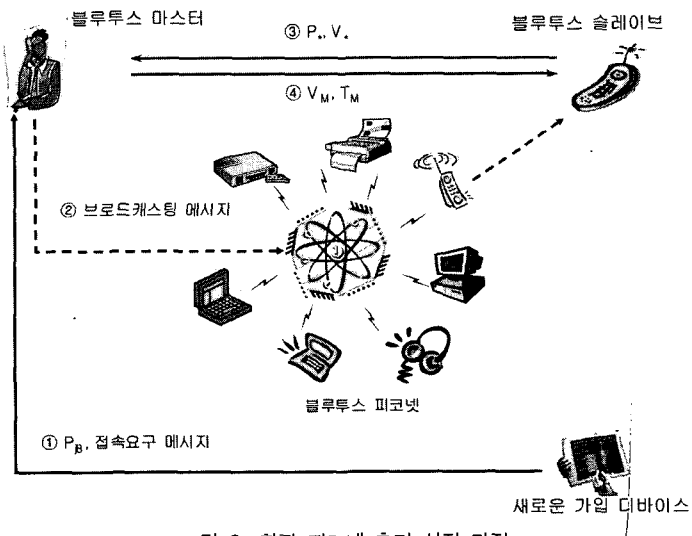

그림 3. 확장 피코넷 초기 설정 과정

이다. 인증이 필요하지 않으며, 개체에 대한 접근이 자동적으로 허용된다.

이상의 과정을 거쳐 상위 마스터와 하위 마스터간의 통신 초기화 과정을 수행한다.

4.2.8 동등 레벨의 하위 마스터끼리의 통신을 위한 인증-2

동등 레벨에서의 하위 마스터끼리의 통신이 이루어지기 위해서 상위 마스터의 검증 과정을 거쳐 통신이 이루어지도록 한다. (통신을 요청하는 송신자 하위 마스터를 A, 통신을 수신하는 수신자 하위 마스터를 B(=최상위 마스터 피코넷의 슬레이브 3)라함)

① 하위 마스터 A는 다)과정에서 최상위 마스터와 통신 과정에서 전송받은 α_M를 이용하여 v_{S_3}를 계산한다.

$$v_{S_3} = \alpha_M^2 \bmod n$$

v_{S_3}를 계산한 후 임의의 난수 r_{S_3}를 생성한뒤 다음을 계산하여 최상위 마스터에 v_{S_3}, X_{S_3}를 전송한다.

$$X_{S_3} = r_{S_3}^2 \bmod n$$

② 최상위 마스터는 의사난수 $e_i(e_i=(0,1), i=(1,....,k))$을 생성하여 하위 마스터 A에 전송한다.

③ 하위 마스터 A는 다음의 Y_{S_3}를 계산하여 최상위 마스터에 전송한다.

$$Y_{S_3} = r_{S_3} \sum_{i=1}^{k} \alpha_M^{e_i} \bmod n$$

④ 최상위 마스터는 다음을 계산하여 검증 과정을 수행한다.

$$Y_{S_3}^2 = X_{S_3} \sum_{i=1}^{k} v_{S_3}{}^{e_i} \bmod n$$

수행 과정이 올바른 경우 그 결과를 하위 마스터 B에 전송한다.

이상의 과정은 하위 마스터 B도 반복 수행해야 하며, 프로토콜 수행이 완료될 경우, 최상위 마스터를 통한 상호 인증 과정을 수행한다.(그림 4 참조)

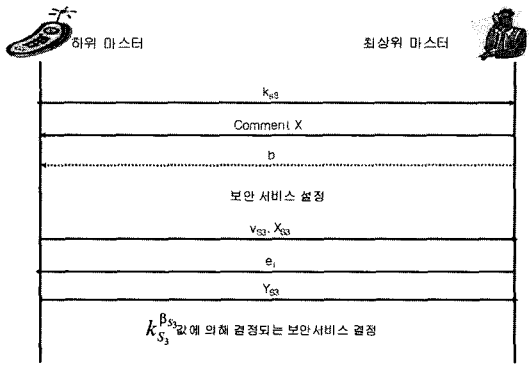

그림 4. 확장 피코넷에서 보안 서비스 및 인증 서비스

4.2.9 확장 피코넷내의 동등 레벨에서 모바일 디바이스간의 통신(슬레이브-슬레이브)

확장 피코넷 내의 동등 레벨에서 슬레이브 - 슬레이브간의 암호 통신이 필요한 경우 상호 인증과 세션키 설정을 위해 다음과 같은 과정을 수행한다.

[세부 단계 1] 상호 인증 과정

① 동등 레벨의 모바일 슬레이브 1은 슬레이브 2와 암호화 통신을 위한 값 V_{S_1}과 상호인증을 위한 X_{S_1}, 상호 인증 메시지 M_{S_1}, 타임스탬프 T_{S_1}을 블루투스 슬레이브 2 디바이스에 전송한다.

$$V_{S_1} = E_{P_{S_2}}(g^{r_{S_1}}),\ X_{S_1} = H(M_{S_1} \| g^{r_{S_1}}) \bmod n$$

② 슬레이브 디바이스 2는 전송받은 V_{S_1}을 자신의 개인키로 복호화한 뒤 다음을 계산하여 전송된 값의 무결성과 기밀성을 검증하고 슬레이브 1과의 상호 인증 초기화 과정을 수행한다.

$$X_{S_1}' = H(M_{S_1} \| g^{r_{S_1}}) \bmod n$$

$X_{S_1} = X_{S_1}'$이면 슬레이브 1의 인증 메시지 M_{S_1}에 대한 응답 메시지 M_{res}를 생성하고 다음을 계산하여 슬레이브 1에 $V_{S_2}, M_{res}, X_{S_2}, T_{S_2}$를 각각 전송한다.

$$V_{S_2} = E_{P_{S_1}}((M_{res}) \| g^{r_{S_2}}),\ X_{S_2} = H(M_{res} \| g^{r_{S_2}}) \bmod n$$

③ 슬레이브 1은 슬레이브 2가 전송한 암호화된 값 V_{S_2}를 자신의 개인키로 복호화하여 기밀성을 검증하고 X_{S_2}'를 생성하여 전송된 X_{S_2}를 비교한 뒤 무

결성과 인증 데이터를 검증한다. 이상의 단계를 기반으로 슬레이브 1과 슬레이브 2의 상호 인증을 위한 초기 과정을 수행한다.

〔세부 단계 2〕 세션키 설정 단계

다음은 상호인증을 위한 초기 과정을 수행한 뒤 슬레이브 1과 슬레이브 2가 세션키 설정 단계이다.

① 슬레이브 1은 슬레이브 2와 암호화 통신을 하기 위한 세션키 생성 정보인 Z_{S_1}와 타임스탬프 T_{S_1}을 슬레이브 2에 전송한다.

$$Z_{S_1} = H(r_{S_1} \oplus T_{S_1})$$

② 슬레이브 2는 슬레이브 1으로부터 전송된 Z_{S_1}, T_{S_1}을 임시 저장하고, 슬레이브 1과의 동적 세션키 설정을 위해 슬레이브 2의 세션키 생성 정보인 Z_{S_2}, 타임스탬프 T_{S_2}를 슬레이브 1에 전송한다.

$$Z_{S_2} = H(r_{S_2} \oplus T_{S_2})$$

③ 슬레이브 1과 슬레이브 2는 세션키 K를 다음과 같이 생성한다.

$$K = H(Z_{S_2} \oplus g^{r_{S_1}} \| Z_{S_1} \oplus g^{r_{S_2}})$$

이상의 진행과정을 그림으로 도식화하면 다음과 같은 그림 5로 표현할 수 있다.

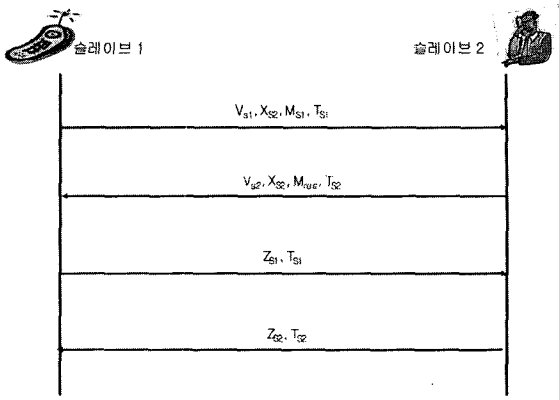

그림 5. 확장 피코넷내의 동등 레벨에서의 모바일 디바이스 간의 인증 및 키 설정

V. 제안 방식 분석

제안 방식은 다음과 같은 특징을 가지고 있다.

- 상호인증 : 제안방식은 블루투스 기본 인증을 기반으로 각각의 디바이스가 생성하는 의사 난수와 ID를 기반 $I' = (ID_{S_2} \| ID_{S_3} \| \ldots \| ID_{S_7})$과 $ID_{S_1}' = (H(I) - H(I'))$을 생성하여 상호 인증이 수행된다. 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 $B_{S_1} \bmod n = w_{S_1}^{y_1} \bmod n = (\alpha_M^{ID_{S_1}^{-1}})^{(ID_{S_1} * r_{S_1})} \bmod n = \alpha_M^{r_{S_1}} \bmod n$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.
- 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 *ID*리스트에서 해당 디바이스의 *ID*를 삭제함으로써 다른 디바이스와는 지속적인 통신이 가능하도록 하였다. (조합키$_{DEL} \oplus AID_{DEL}$) $=$BD_$ADDR_{DEL}$을 이용한 키 갱신의 범위를 탈퇴 하는 모바일 디바이스만을 *ID*리스트에서 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 비교해 볼 때 효율적인 특성은 낮다고 할 수 있다.

제안방식에 대한 안전성을 기존 블루투스 피코넷과 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	제안방식
상호인증	마스터와 마스터	△	O
	마스터와 슬레이브	△	O
기밀성과 무결성	전송 데이터	△	O
	저장 데이터	△	O
키 갱신 범위		X	O
탈퇴자에 대한 참가자의 안전성		X	O
전력 소모 공격으로부터의 시스템의 독립성		X	O
효율성		소형화 디바이스에서 구현 가능	PTD와 같은 보안 디바이스에 구현가능

〔X : 취약, △ : 보통, O : 안전〕

Ⅵ. 결 론

최근 차세대 IT 기술인 유비쿼터스 컴퓨팅과 관련되어 근거리 무선 통신 기술중 블루투스가 새로운 요소 기술로 적용되면서 활발한 연구가 지속되고 있다. 블루투스가 초기 제시되었던 여러 가지 취약성을 보안하면서 새로운 형태로의 적용을 위해서는 기존의 블루투스 기술의 취약성을 보완할 수 있는 방안에 대한 연구가 절실히 요구된다.

특히, IEEE와 SIG와 같은 표준 그룹에서 이루어지고 있는 새로운 블루투스 표준안에서 기존의 블루투스가 갖는 여러 가지 문제점을 해결하기 위한 연구와 표준화 방향이 제시되고 있는 것이 현실이다.

따라서 본 논문에서는 기존의 블루투스가 갖는 취약성을 분석하고 블루투스 통신을 통해 피코넷이라는 네트워크가 형성되었을 경우 이를 그룹으로 정의하고 스케터넷으로 확장하지 않고 피코넷 내부에서의 확장성을 갖는 새로운 형태의 방식을 제안하였다.

이와 더불어 피코넷 그룹 상태에서의 가입과 탈퇴 및 갱신에 대한 내용을 기술함으로써 보안적인 재구성이 필요할 경우에 따라 안전한 형태의 방식을 제안하였다. 그러나 효율성 측면에서 기존 블루투스와 비교해볼 때 지수승 연산의 증가에 따른 구현에 대한 비현실성을 제시할 수 있다. 또한 한 피코넷에서 슬레이브 개수를 증가시키기 위해 주소 비트가 확장되어야 하는 문제점도 내포하고 있는 실정이다. 따라서 향후 본 연구에서 제시된 방향을 기반으로 효율성을 높일 수 있는 프로토콜의 재수정을 통한 구현 연구와 병행하여 주소 비트 확장에 따른 문제점을 해결하고, 여러 형태의 그룹 보안 요구사항을 제시하고 이를 적용함으로써 다양한 형태로 보안사항을 고려한 연구가 지속되어야 될 것으로 사료된다.

참 고 문 헌

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

〔2〕 S. Fluhrer and S. Lucks, "Analysis of the E0 Encryption System" available from S.Lucks' web site at http://th.informatik.uni-mannheim.de/People/Lucks/papers/e0.ps.gz, agnu-zippedPost-script file.

[3] http://www.bluetooth.com (Bluetooth White Paper)
[4] Bluetooth Security Architecture, 1999, available at http://www.bluetooth.com/.
[5] Specification of the Bluetooth System, 1999, available at http://www.bluetooth.com/.
[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/markusj/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

〈著者紹介〉

서 대 희 (Dae-Hee Seo)
2003년 2월: 순천향대학교 전산학 전공 석사
2004년 3월~현재: 순천향대학교 전산학과 박사과정
〈관심분야〉 암호이론, 정보이론, 컴퓨터 보안

이 임 영 (Im-Yeong Lee)
1981년 8월: 홍익대학교 전자공학과 졸업
1986년 3월: 오사카대학 통신공학 전공 석사
1989년 3월: 오사카대학 통신공학 전공 박사
1989년 1월~1994년 2월: 한국전자통신연구원 선임연구원
1994년 3월~현재: 순천향대학교 정보기술공학부 교수
〈관심분야〉 암호이론, 정보이론, 컴퓨터 보안