2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

ECC를 이용한 안전한 piconet에 관한 연구

서대희*, 이임영*, 김영백**, 김해숙**
*순천향대학교 정보기술공학부.
**한국정보보호진흥원 기술부 암호기술팀
e-mail:1636711@hitel.net

A study on secure piconet using ECC

Dae-Hee Seo*, Im-Yeong Lee*,
Yeong-Baek Kim**, Hae-Suk Kim**
*Division of Information Technology Engineering
SoonChunHyang University
**Korea Information Security Agency, Information Security
Technology Division, Cryptographic Team

요약

정보통신의 급속한 발전으로 다양한 정보의 요구는 기존 유선 서비스 환경에서 개인 중심의 무선 서비스 환경으로 변화하고 있다. 그 중에서도 최근 근거리 무선 통신의 중심으로 주목받고 있는 Bluetooth는 이러한 사용자의 요구에 의해 발생되어 많은 연구가 진행중에 있다.

본 논문에서는 Bluetooth Master와 Slave로 이루어진 하나의 작은 네트워크인 piconet의 형성에서부터 유지까지의 보안적 취약점을 분석한 뒤 이를 기반으로 ECC를 적용한 보다 안전하면서 효율적인 Bluetooth piconet 형성 과정 및 유지 과정을 제안하였다.

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 환경에 대한 인터페이스에 대한 고려로부터 시작되었으며 이러한 시스템이 바로 Bluetooth이다. Bluetooth는 고정 혹은 유동성을 가진 각 디바이스에 정보를 전송하는 무선 통신 프로토콜이다. Bluetooth는 채널을 공유한 2개 또는 더 많은 장치들을 1개의 Master를 중심으로 piconet을 형성하여 scatternet으로의 확장이 이루어진다.

본 논문은 Bluetooth의 개요를 살펴보고 Bluetooth에서 자체 제공하고 있는 보안 서비스에 대해서 분석하고 이를 기반으로 piconet에 대한 보안 분석을 통해 새로운 방식을 제안하고 결론을 맺고자 한다.

본 논문은 한국정보보호센터의 "정보보호기반구축지원 사업"의 일환으로 수행되었음.

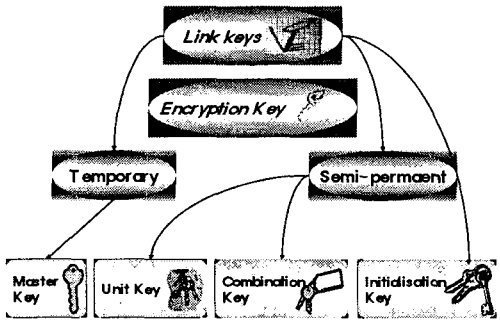
2. Bluetooth 분석

Bluetooth는 컴퓨터 주변기기들간의 선이 없는 통신을 위한 근거리 무선 통신으로 개발되었다.
이를 유동성 디바이스에 적용하여 유동성 디바이스의 무선 활동 영역 뿐만 아니라 자유로운 통신을 제공하는 무선 통신 기술로서 각광 받고 있다.

Bluetooth는 음성, 비디오, 데이터 등 다양한 정보를 10~100m내 거리에서 최대 1Mbps 속도를 전송할 수 있는 기술로 휴대폰, PC 등의 기기간 데이터 송수신뿐만 아니라 근거리 무선 통신망을 통한 무선 인터넷 접속기술로도 이용될 전망이다. Bleutooth 무선 칩은 9mm×9mm의 크기에 세계 어디에서나 사용할 수 있는 2.4GHz의 ISM(Industrial Scientific Medical) 대역폭을 사용한다[1].

2.1 Bluetooth Security 분석

Bluetooth는 보안 서비스 제공을 위해 여러 가지 키를 생성하게 되고 이러한 키를 기반으로 인증, 암호화, 기밀성등을 제공한다.



(그림 1) Bluetooth 키 형태

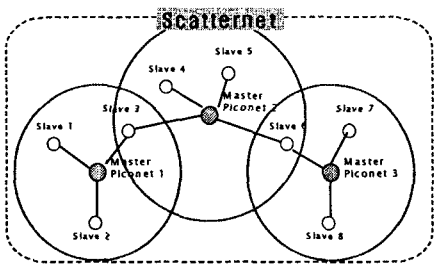
Bluetooth가 제공하는 보안 서비스는 3가지의 보안 모드에서 제공한다[1][2].

- Security Mode 1
  각 디바이스는 어떠한 보안 프로시져도 가지고 있지 않다.
- Security Mode 2
  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.
- Security Mode 3
  각 디바이스는 LMP(Link Manager Protocol) 레벨의 link set-up이 완벽하게 이뤄지기 이전에 보안 프로시져를 가질 수 있다.

2.2 Bluetooth piconet 분석

Bluetooth는 Master를 중심으로 여러개의 Slave가 연결이 가능하며 이러한 경우 piconet이라 부른다. 즉, 한 piconet에서 하나의 Master는 동시에 최대 7개의 Slave 디바이스와 연결할 수 있다. piconet이 형성되었을 경우 상호 채널이 교환되며, 이러한 piconet 여러 개가 서로 연결돼 있을 때 이것을 scatternet이라고 한다.

그러나 piconet이나 scatternet을 위협하는 공격자는 공격자의 디바이스를 piconet이나 scatternet을 구성하는 Master에 계속된 연결 요청을 통한 전력 소모 공격이나 piconet이나 scatternet의 해당 영역에 자신의 Slave를 포함하여 보안적인 연결 과정으로 이루어지지 않는 piconet이나 scatternet을 위협하는 취약점을 가지고 있다[3][4][5].



(그림 2) Piconet과 Scatternet

3. 새로운 제안 방식

본 논문에서는 초기 inquiry과정을 거친 후 PIN 번호의 공유 및 유저의 PIN번호 입력이 올바르게 이루어 졌으며 해당 모바일 디바이스는 PIN번호에 근거해 25시간마다 갱신되는 WPKI 인증서를 가지고 있다는 가정을 바탕으로 ECC를 적용한 안전한 piconet 형성을 제안한다.

3.1 각 객체 및 시스템 계수

다음은 ECC를 이용한 piconet을 구성하는데 필요한 해당 객체와 필요한 시스템 계수를 기술한다.

Bluetooth Master : Piconet 형성의 중심이 되는 Bluetooth Device

Bluetooth Slave : Master에 연결되어 있는 Slave

Bluetooth Master

E : 타원곡선

G : Base Point

n : G의 위수

h_M : Master가 생성한 안전한 해쉬값

t_M : 타임 스탬프

r_M : Master가 생성한 의사난수

R_M : Master가 생성한 ECDSA 서명값

S_M : Master가 생성한 ECDSA 서명값

ID_{info_M} : Master의 정보

K : Master와 Slave 사이의 세션키

p_M : Master의 공개키

q_M : Master의 비밀키

Z_M : 그룹원에게 공개할 시스템 계수

$(Z_M = g^{q_M} \bmod p_M \ [\, g \in GF(p_M)])$

i : 그룹에 할당된 키의 개수 $i \in (1, \ldots, p_M - 1)$

Bluetooth Slave

E : 타원곡선

G : Base Point

n : G의 위수

h_S : Slave가 생성한 안전한 해쉬값

t_S : 타임 스탬프

r_S : Slave가 생성한 의사난수

R_S : Slave가 생성한 ECDSA 서명값

S_S : Slave가 생성한 ECDSA 서명값

ID_{info_S} : Slave의 정보

S_j : 그룹키 서명값

p_S : Slave의 공개키

q_S : Slave의 비밀키

3.2 프로토콜

3.2.1 Master와 Slave의 상호 인증 및 그룹 키 설정 단계

Bluetooth Master와 Slave는 PIN번호를 기반으로 25시간마다 갱신되는 인증서를 가지고 있으며 ECC 기반의 ECDSA 서명을 사용하였으며 그룹키 분배를 위한 세션키 K를 생성은 ECDH를 사용하였다.

단계 1 : Master와 Slave간의 상호인증

step ① Master는 Slave에 전송할 ID_{infor_M}, ECDH를 이용한 세션키 생성을 위한 Q_M로 다음을 계산한다.

$$Q_M = r_M \cdot G$$

$$E_{p_M}(ID_{infor_M} || Q_M || T_M),\ H(E_{p_M})$$

step ② Slave는 전송받은 E_{p_M}와 $H(E_{p_M})$를 확인하고 Slave는 Master에게 전송할 ID_{infor_S}과 ECDH를 이용한 세션키 생성을 위한 Q_S를 다음과 같이 계산하여 Master에게 전송한다.

$$Q_S = r_S \cdot G$$

$$E_{p_S}(ID_{infor_S} || Q_S || T_S),\ H(E_{p_S})$$

단계 2: 서명값 교환 및 그룹 키 설정 단계

step ③ Master : Piconet의 Master는 $n*(p_M/Z_M)$을 계산한 뒤 (p_M/Z_M)과 ECDSA 서명값인 R_M, S_M을 Slave의 단계 1에서 ECDH로 설정된 세션키 K로 암호화하고 안전한 해쉬값을 계산한다.

$$E_{K_M}((p_M/Z_M) || R_M || S_M)),\ H(E_{K_M})$$

step ④ Slave : Piconet Slave는 전송받은 E_{K_M}과 $H(E_{K_M})$으로 무결성과 기밀성을 검증하고 임의의 키쌍을 선택하여 $S_j\ (j \in i)$를 수행한 뒤 Slave의 ECDSA서명을 세션키 K로 암호화 한 뒤 안전한 해쉬값을 생성하여 Master에게 전송한다.

$$E_{K_S}(S_j || R_S || S_S),\ H(E_{K_S})$$

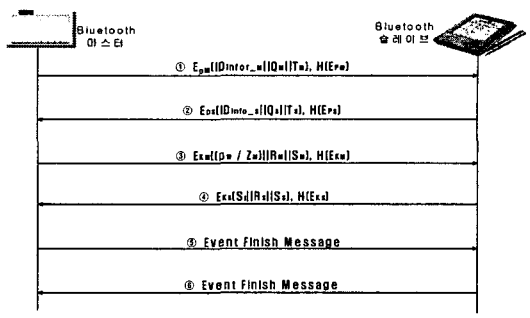
※ 그룹서명의 검증 : Master는 $n*(Z_M)$ 리스트를 검증자에게 제공하며 검증자는 S_j를 검증할 수 있다.

단계 3 : 이벤트 종결 단계

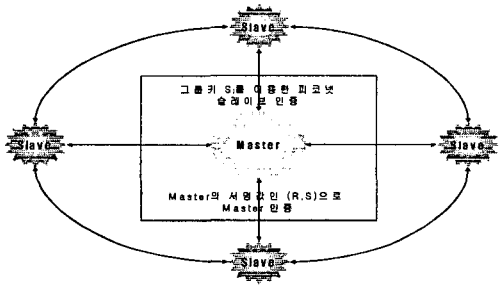
step ⑤ Master는 Slave에게 전송받은 E_{K_S}, $H(E_{K_S})$를 검증하여 무결성과 기밀성을 검증한 뒤 이벤트 종결 메시지를 Slave에게 전송한다.

step ⑥ Slave는 Master에게 이벤트 종결 메시지를 전송한다.

이상의 프로토콜을 기반으로 Master를 중심으로 ECC를 이용한 안전한 piconet이 그림 3과 같이 형성된다.



(그림 3) ECC를 적용한 상호인증 및 그룹서명 단계

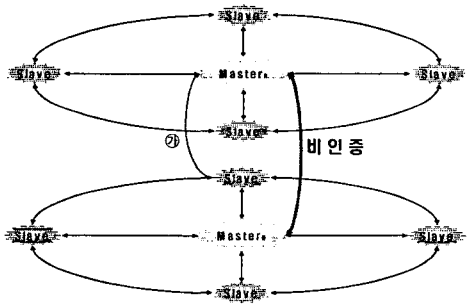


(그림 4) ECC를 적용한 안전한 piconet 형성

3.3 Piconet 프로토콜

ECC를 적용한 piconet이 형성된 후 Slave의 접속에 관한 두 가지 접속 방법을 고려해 볼 수 있다.

3.3.1 Piconet에 포함된 Slave의 접속 요구 (Master간의 비인증)



(그림 5) 인증되지 않는 Slave의 접속요구

step ① Master$_B$의 Slave는 Master$_A$에 자신의 정보인 S_{info}를 전송하여 접속을 요구한다.

step ② Master$_A$는 다음을 계산하여 Master$_B$에 전송한다.

$$E_{P_A}(R_A || S_A || ID_{info_A} || T_A || S_{info})$$

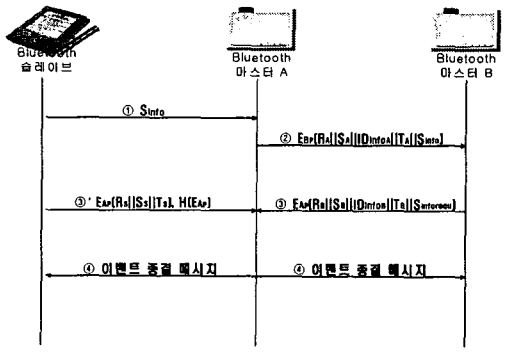
step ③ Master$_B$는 해당 Master$_A$의 ECDSA 서명값을 저장하고 S_{info}를 확인 후 다음을 계산한다.

$$E_{P_B}(R_B||S_B||R_{BS}||S_{BS}||T_B||S_{info_{request}})$$

step ③′ 접속요구 Slave는 다음을 계산하여 Master$_A$를 전송한다.

$$E_{P_A}(R_S||S_S||T_S),\ H(E_{P_A})$$

step ④ Master$_A$는 Slave에서 전송된 값과 Master$_B$에 전송된 값의 무결성가 기밀성을 확인한 후 Slave에게 전송되어온 서명값과 Master$_B$에게 전송되어온 해당 Slave의 서명값을 확인 후 접속요구 Slave를 인증한다.



(그림 6) 인증되지 않는 Slave 인증 방식

3.3.2 Piconet에 포함된 Slave 접속 요구 (Master간의 인증이 이루어진 경우)

step ① Master간의 인증이 이루어진 경우 접속요구 Slave와 단계 1 ~ 3까지의 과정이 진행된다.

4. 특징 및 비교분석

본 제안 방식은 다음의 특징을 통해 Bluetooth Security 요구 사항들을 만족하고 있다.

- 비밀성 : 송·수신되는 모든 정보는 수신자의 공개키로 암호화되며 제 3자는 이를 확인 할 수 없다.
- 인증성 : 각 해당 객체는 PIN 번호에 근거한 인증서를 가지고 ECDSA 서명을 수행하여 이에 근거한 상호 인증이 이뤄진다.
- 무결성 : 디지털 서명과 Time stamp를 이용한 정보의 무결성이 보장된다.
- 검증성 : ECDSA를 이용한 상호인증과 piconet 형성의 그룹 서명은 믿을 수 있는 제 3자에 의해 검증이 가능하다.

<표 1> 제안방식 분석

	Bluetooth specification V1.1	제안방식
비밀성	△	○
인증성	○	○
무결성	△	○
검증성	△	○

5. 결론

정보통신의 급속도로 발전하고 있는 가운데 사용자 중심의 무선통신에 대한 연구가 빠르게 진행되어 가고 있으며 이를 기반으로 컴퓨터 분야 뿐만 아니라 많은 무선 환경에서 적용할 수 있는 무선통신 기술이 필요하게 되었다. 이러한 무선통신 기술이 데이터 뿐만 아니라 음성 서비스까지 특정한 보안 절차 없이 사용자에게 제공되었을 경우 사용자의 프라이버시 뿐만 아니라 무선 기반 서비스 자체의 위험성을 내표하고 있다.

따라서 본 논문에서는 최근 근거리 무선 통신의 표준으로 자리잡고 있는 Bluetooth가 자체 제공하고 있는 보안 서비스를 바탕으로 하나의 소규모 네트워크인 piconet의 형성에서부터 유지를 위해 기존의 piconet 형성의 취약점을 보완하여 ECC기반의 키 분배와 디지털 서명방식을 이용한 보안적인 piconet 형성 방식을 제안하였다.

향후 Bluetooth 뿐만 아니라 근거리 무선통신이 적용된 네트워크 구성에 관한 기초 자료로 활용될 수 있으리라 기대한다.

6. 참고문헌

[1]. http://www.bluetooth.com (Bluetooth White Paper)
[2]. "Bluetooth Message Sequence Charts" Bluetooth Sepcification Section Appedix IX.
[3]. Bluetooth Security Juha T. Vainio Department of Computer Science and Engineering Helsinki University of Technology 2000.05.25
[4]. http://www.cs.hut.fi/Opinnot/Tik-86.174/sectopics.html (Ullgren T. Security in Bluetooth: Key management in Bluetooth)
[5]. http://www.bell-labs.com/user/markusj/bt.html (Jakobsson M., Wetzel S. Security Weakness in Bluetooth: RSA 2001)
[6]. 최용락, 소우영, 이재광, 이임영 "통신망 정보보호", 도서출판 그린, 1997.2.
[7]. 이만영, 김지홍, 류재철, 송유진, 염흥렬, 이임영 "전자상거래 보안 기술", 생능출판사, 1999.8.
[8]. 최용락, 소우영, 이재광, 이임영 "컴퓨터 통신 보안", 도서출판 그린, 2001.2
[9]. 이임영 "전자상거래 보안입문", 생능출판사, 2001.8
[10]. Alfred J. Menezes, Paul C.van Oorschot, Scott A. Vanstone "HANDBOOK of APPLYED CRYPTOGRAPHY", CRC, 1996.11.