블루투스 스캐터넷에서 서로 다른 정책을 지원하는 보안 모델

김태환*, 박용현*, 오세웅**,
*동명정보대학교 정보대학원
**동명정보대학교 멀티미디어공학과

A Security Model supporting different policy for Bluetooth Scatternet Environment

TaeHwan Kim*, YoungHen Park*, SeiWoong Oh**
*Graduate School of Information, Tongmyong Univ. of Information Technology.
**Dept. of Multimedia Engineering, Tongmyong Univ. of Information Technology.

요 약

최근 단거리 무선통신 중의 하나인 블루투스(bluetooth)의 기술이 첨가된 전자결재시스템 등의 출현으로 블루투스의 보안 문제가 대두 되었다. 기존의 블루투스 보안 모델(bluetooth security model)은 하나의 피코넷(piconet)에서만 적용되어지며, 다수의 피코넷으로 구성된 스캐터넷(scatternet)에서는 적용될 수 없다. 본 논문에서는 스캐터넷상에서 서로 다른 보안 정책을 갖고 있는 다수의 어플리케이션을 지원하는 보안 모델을 제안한다.

1. 서론

블루투스(bluetooth)는 하나의 마스터(master) 장치(device)와 7개의 슬레이브 장치(slave device)로 구성되어 있는 피코넷(piconet)과, 그 이상의 장치(device)와 통신하기 위하여 구성되어 있는 스캐터넷이 있다[1]. 현재 블루투스를 이용하여 전자결재 및 쿠폰구매 등과 같은 보안이 필요한 서비스가 등장하여 보안의 중요성이 대두되고 있다.

기존에 보안 모델에서는 보안 협상의 결과가 성공, 실패등과 같은 간단한 에러 이벤트(error event)만을 생성하므로, 실패 시 이에 대해 어플리케이션의 대응이 어렵고, 더욱이 스캐터넷상에서의 보안은 정의가 되어 있지 않아 서로 다른 정책을 갖는 어플리케이션들을 지원할 수 없다.

본 논문에서는 이러한 문제점들을 해결하기 위해 보안 협상 시 응답 이벤트에 상태 정보 뿐만 아니라 각 보안 정책들의 관련 정보를 생성하므로서 각 어플리케이션들이 보안 연결 실패에 대처할 수 있게 하고 또한 스캐터넷에서도 서로 다른 보안 정책을 요구하는 어플리케이션을 지원하는 보안 모델을 제안한다.

본 논문의 구성은 2절에서 기존의 블루투스 보안 모델의 특징과 보안 정책을 설명하고, 기존의 보안 문제점들을 제시하며, 3절에서는 제안된 보안 모델(security model)에 대해서 설명한다. 마지막으로 4절

에서는 결론과 향후 계획을 설명한다.

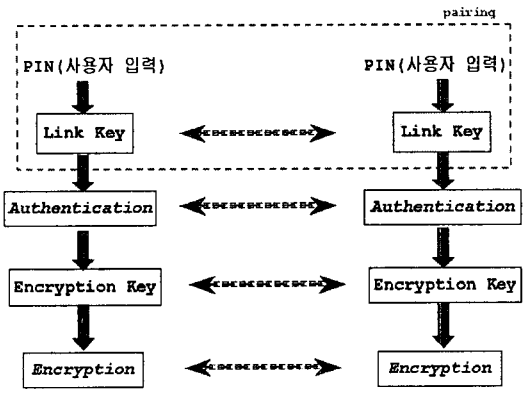
2. 기존의 블루투스 보안 모델

블루투스의 보안 모델에서 피코넷의 권한부여(authorizaton), 인증(authentication), 암호화(encryption) 및 이를 바탕으로 한 보안 절차에 대해 기술하고[3] 기존의 문제점을 제시한다.

2.1 기존 블루투스 보안 모델

그림 1을 보면 블루투스 보안 모델에는 권한부여, 인증, 암호화를 하는 3가지 보안 기술로 이루어져 있다.

권한부여는 리모트 블루투스 장치(remote blueto-oth device)에서 승인 요청이 왔을 때 제공되는 기능으로서 요청을 받은 블루투스에서 각 서비스 허용 여부를 확인하여 승인을 할 것인지를 판단한다. 인증은 권한을 얻은 후 패어링(pairing)과정을 통해 사용자가 입력한 PIN 코드를 가지고, 요청을 한 장치와 똑같은 링크 키를 생성한 후, 이 키를 이용하여 로컬 장치을 입증한다. 마지막으로 암호화는 블루투스 패킷중 어세스 코드(access code), 헤더(header)를 제외한 패이로드(payload) 부분만이 인코딩되는데[1] 이 작업은 인증작업에서 생성 된 링크 키에 의해서 생성된 암호화 키로 작업을 처리한다.



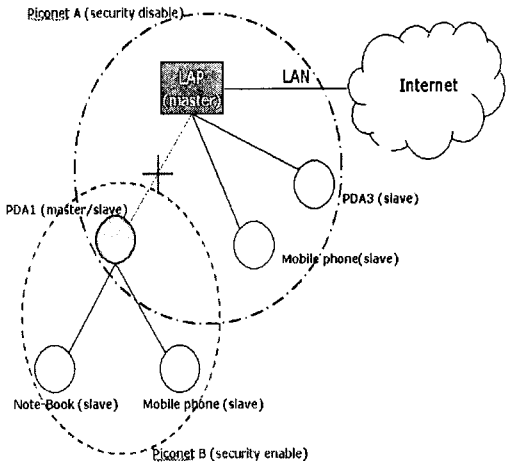
[그림 1] 블루투스(bluetooth) 보안(security) 모델

2.2 피코넷에서의 보안

단일 피코넷망에서 서비스 계층(L2CAP layer 이상)의 보안은 리모트 장치(remote device)로부터 보안이 필요한 서비스의 연결요청이 왔을 때, 로컬 장치(local device)는 요청한 리모트 장치의 보안 정보를 장치 데이터베이스(device database)와 서비스 데이터베이스(service database)를 참조하여 그림 1과 같이 권한 부여 및 인증과 암호화가 일련의 단계들로 구성되어진다[3].

2.3 기존의 보안 모델의 문제점

기존 블루투스의 보안 모델의 문제점 중의 하나는 어떤 보안 정책을 수행하는 피코넷에 새로운 보안 정책을 요청하면, 기존의 블루투스는 not_accepted라는 에러 이벤트(error event)만을 발생시킨다. 만약, 다시 연결을 시도하려고 한다면, 접속하려고 하는 블루투스 장치에 맞는 보안 정책을 설정하여 다시 재접속을 해야 한다.



[그림 2] 스캐터넷(scatternet) 구성망 예

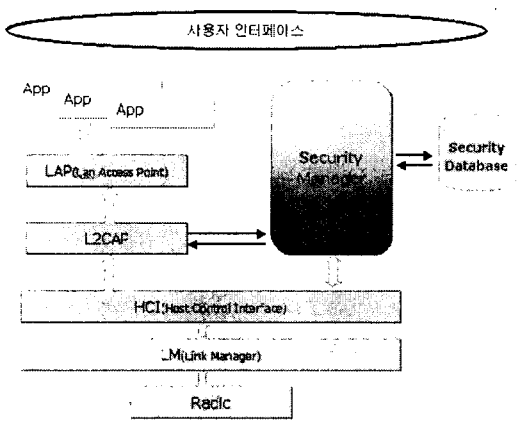
또 다른 문제점으로 피코넷간 보안을 필요로 하는 연결 요청은 그림 2와 같이 블루투스 스캐터넷에서 브리지 역할을 하는 PDA1이 암호화로 인한 작업으로 인하여 부하가 많아지게 되므로 서비스 연결을

하려고 한다면, 보안이 필요하지 않는 서비스들로 이뤄 져야 하거나, 기존의 피코넷 연결을 끊고 새로운 피코넷이 연결되어 보안 정책을 수행해야 하는 것을 들수 있다.

3. 제안된 보안 모델

3.1 블루투스 보안 모델 제안

본 절에서 제안한 보안 모델은 보안 관리자(security manager)와 보안 데이터베이스(security database)로 구성되어 있다. 기존의 보안 모델에서는 보안연결 협상 시 성공, 실패 등의 간단한 정보만 생성하지만[3], 그림 3과 같이 제안된 보안 관리자는 보안 데이터베이스(표1)를 참조하여 관련된 서비스의 보안 정보를 응답 이벤트에 의해 전달해 줌으로써 서로 다른 어플리케이션의 보안 정책이 수행되도록 한다.



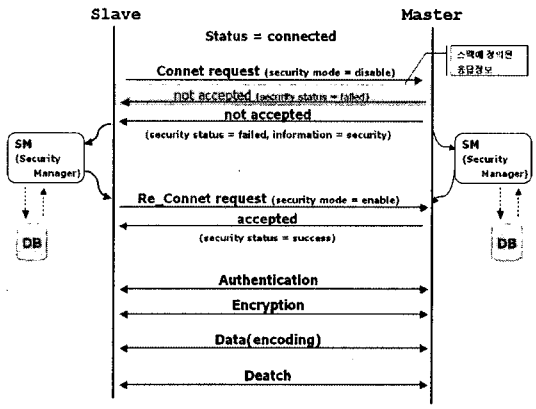
[그림 3] 제안된 보안 모델 구조

Attribute	
1. BD_ADDR	2. PIN code
3. Service Name	4. Link Key
5. PSM / CID	6. Authentication (y or n)
7. Autorization (y or n)	8. Encryption (y or n)

[표 1] 보안 데이터베이스 속성

3.2 블루투스 기기간의 보안

제안된 블루투스 보안 모델에서의 보안 절차에 따른 데이터 교환은 그림 4와 같다. 먼저, connect_request 요청을 하기 전의 상태(status)는 페이징(paging)까지의 작업이 끝난 상태이며 어플리케이션 서비스가 보안 연결 요청을 한다. 마스터는 요청해온 connect_request 명령어내의 정보를 바탕으로 보안 관리자가 보안 데이터베이스를 검색하여, accepted 또는 not_accepted 이벤트에 현재 피코넷의 상태(pass, fail)와 보안 정보(현 피코넷에서의 보안 정보)를 함께 슬레이브에게 보낸다. 슬레이브에서는 not_accepted의 에러 이벤트가 마스터에서 응답이 왔을 경우 리모트 장치의 보안 정보를 가지고 있으므로 슬레이브의 보안 관리자는 재 연결에 대한 과정을 처리한다.



[그림 4] 개선된 보안 데이터 교환

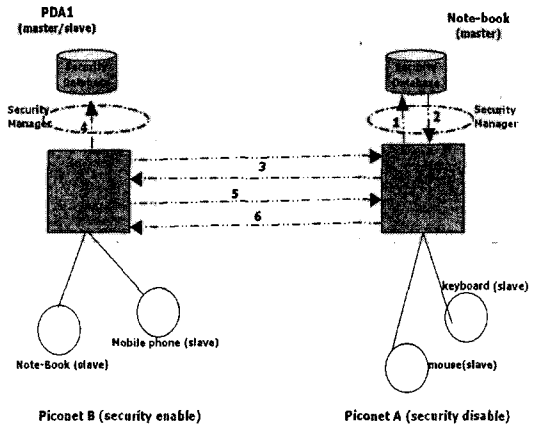
3.3 블루투스 스캐터넷에서의 보안

본 논문에서 제안된 보안 모델을 이용한 스캐터넷상에서의 보안은 보안 정책이 다른 2개의 피코넷 망으로 구성된 그림 5로 설명한다. 그림 5에서 피코넷B의 PDA1이 다른 피코넷의 노트북(마스터)으로 접속을 요청할 때 아래와 같은 방법을 따른다.

1. 보안이 필요한 서비스의 연결 요청을 받은 노트북(마스터)은 접근 정보를 가지고 보안 관리자에 의해서 로컬의 보안 데이터베이스에게 쿼리(query)를 발생시킨다.

2. 노트북의 보안 관리자는 '1'에서 보낸 쿼리문에 대한 받은 각 서비스에 대한 보안 정책 정보를 가지고 응답 이벤트를 판단한다.
3. 노트북의 보안 관리자는 보안 데이타베이스에서 받은 보안 정책 정보를 응답 이벤트에 추가시켜 PDA1로 보낸다.
4. 접속을 요청한 PDA1의 보안 관리자는 응답을 받은 정보를 바탕으로 재 연결 협상을 할 것인지를 어플리케이션과 판단하여 보안 데이터베이스를 업데이트 한다.
5. PDA1의 보안 관리자는 어플리케이션과 협상 되어진 보안 데이터베이스의 정보를 가지고 노트북(마스터)에게 재 연결을 요청한다.
6. 연결 되었다는 accepted 이벤트를 보낸다.

위와 같은 방법으로 보안 협상이 성공적으로 수행되면 어플리케이션들간의 데이터 교환이 이루어진다.



[그림 5] 스캐터넷에서의 개선된 보안 흐름도

4. 결론

기존의 블루투스 보안 모델의 문제점은 보안 연결 협상의 결과로 연결 실패 등과 같은 단순한 정보만 생성하므로 실패 시 어플리케이션의 대응이 어려운 것과 스캐터넷에 서로 다른 보안 정책들을 적용시키는 것이 어려운 것이다. 이러한 문제점을 해결하기 위해 본 논문에서는 보안 관리자가 응답 이벤트에 상태 정보 뿐만 아니라 각 보안 정책들의 관련 정보를 보안 협상 시 생성하므로서 각 어플리케이션들이 보안 연결 실패에 대처할 수 있고, 스캐터넷에서 서로 다른 보안 정책을 갖고 있는 어플리케이션 간의 암호화가 이루어 지도록 보안 모델을 제안 하였다.

향후 계획으로는 제안된 보안 모델을 프로파일(profile)[4] 형식으로 구현하여, 스캐터넷상에서 서로 다른 보안 정책 요구를 가능하게 하는 것이다.

[참고문헌]

[1] Specification of the Bluetooth System -Core-, V.1.1, 2001-02-22

[2] Thomas Muller, Bluetooth Security Architecture, V.1.0 1999-07-15

[3] Christian Gehrmann. Bluetooth Security White Paper, 2002-04-19(Bluetooth SIG Security Expert Group)

[4] Specification of the Bluetooth System -Profile- V1.1, 2001-02-22

[5] Marianthi Alexoudi, Euan Finlayson, Max Griffiths. Security in Bluetooth. 2002-11-08

[6] Marjaana Traskback. Security of Bluetooth: An overview of Bluetooth Security

[7]Robert Morrow. Bluetooth operation and use. 2002.

[8] K. David, M Gordon, S Brian, B Jennifer. Bluetooth Application Developer's Guide