제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

Bluetooth 의 키 생성을 위한 안전한 파라미터 교환 프로토콜

김익경, 이석주, 서경룡
부경대학교 컴퓨터 공학과
e-mail : clisp@mail1.pknu.ac.kr

A Secure Parameter Exchange Protocol for the Bluetooth Key Generation

Yik-Kyung Kim, Suk-Joo Lee, Kyungryong Seo
Dept. of Computer Engineering, Pukyong University

요 약

Bluetooth 는 전형적인 무선 네크워크와는 달리 다른 새로운 네트워킹 파라다임으로서 어떠한 고정된 인프라에도 의존하지 않고, 이동 호스트만으로 구성된 네트워크이다. 이는 그 고유의 특성으로 인해 여러 방면에 걸쳐 사용될 수 있는 장점을 가지고 있으나, 외부로부터의 공격에 취약하다는 약점을 가지고 있다. 본 논문에서는 Bluetooth 가 가지고 있는 보안 위협 요소들 중 링크키 생성을 위해 사용되어 지는 파라미터 교환 방식과 각종 키 생성 메커니즘을 분석한다. 또 안전한 파라미터 전달을 위한 프로토콜을 제한하였다. 제안된 프로토콜은 최소한의 메시지 교환만으로 링크키, 조합키, 생성에 필요한 각 파라미터를 안전하게 전달한다.

1. 서론

Bluetooth 는 10 세기경 덴마크와 노르웨이를 통일한 왕의 이름에서 유래한 것으로, 2.4GHz 의 비인가 ISM(Unlicensed Industrial Science Medical)주파수 대역을 사용하여 복잡한 데이터 통신용 유선 케이블을 무선화할 목적으로 개발되었다. 이러한 Bluetooth 는 키보드나 모니터, 마우스와 같은 유선 장치의 케이블을 대처할 뿐만 아니라 저렴하면서 사용편의성, 신뢰성, 저전력의 동작을 제공한다.

Bluetooth 의 특징은 무선 면허가 필요 없는 2.4Ghz 대역을 사용하여 대역폭의 효용성을 얻을 수 있고 대용량의 패킷의 전송이 가능하며 간단한 인터페이스를 사용하여 10m 에서 400m 내에서 1Mbps 정도의 무선 접속이 가능하다. 또한 기존 네트워크 와의 연동성이 원활하여 IrDA, IEEE802.11b 등과 유연하게 연결됨으로써 다양한 프로토콜을 소화할 수 있다 [1].

하지만 Bluetooth 에는 유닛 간의 데이터 전송 전 여러 가지 키 생성 과정에서 파라미터 전달 시 보안에 문제점이 있음을 알 수 있다. 링크키 교환을 위한 해쉬 함수를 사용하는 단순한 키 관리 방법이 제안되었지만 조합키 사용에서는 사용이 불가능하고 보안을 보장하기도 어렵다 [2].

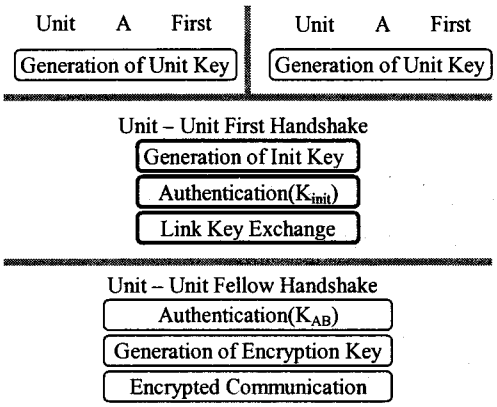
본 논문에서는 각종 키 생성에 필요하지만 보안에 취약한 파라미터 교환 메커니즘을 분석하고 여러 파라미터를 안전하고 효율적으로 교환 할 수 있는 프로토콜을 제안한다.

2. Bluetooth Network Overview

Bluetooth 는 두대 혹은 그 이상의 유닛들이 통신을 하기 위해 기본적으로 해당 장치들 사이에 링크키 생성이 필요하게 된다. 이때 링크키로서 사용되어 질 수 있는 키의 종류는 4 가지로서 보안 레벨과 각 장치의 메모리의 크기, 그리고 키의 용도에 따라 분류되어 사용되어 진다 [3].

링크키로서 가장 많이 사용되는 키는 첫 번째로 유닛키로서, 이는 두 대의 장치 중 한 장치의 유닛키가 링크키의 역할을 수행하게 된다. 두 번째로 사용되어 지는 링크키는 조합키로서 이는 두 대의 장치에서 각

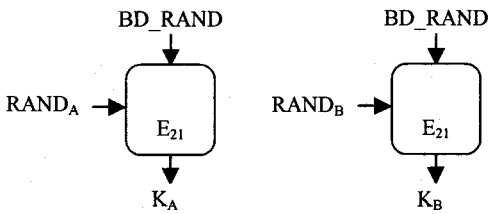
각의 키를 생성해 내고 그 생성된 키를 XOR 을 함으로서 최종 조합키가 생성 되어 진다. [그림 1]은 두 대의 Bluetooth 장치가 통신을 위한 전반적인 동작상태를 나타낸다. 먼저 각각의 장치는 고유의 유닛키를 생성해 내며 First Handshake 를 수행한다. 이때 두 장치는 Initialization Key 생성과 인증이 이루어지며 링크키 교환이 이루어진다.



[그림 1] Bleutooth Network Overview

유닛키의 생성

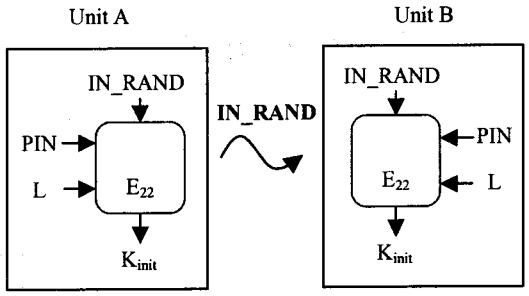
유닛키는 Bluetooth 유닛이 최초 동작시에 생성되어 진다. 이는 BD_ADDR 과 Random number 를 가지고 E_{21} 알고리즘을 통해 생성되어 지며, 이는 생성 이후 비휘발성 메모리에 저장되어 계속적으로 사용되어 질 수 있다. 또 메모리의 용량이 제한적인 장치에 대하여 유닛키는 링크키로서 사용되어 질 수도 있다.



[그림 2] 유닛키의 생성

First Handshake

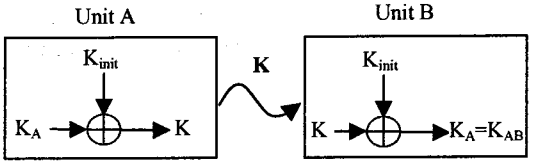
Initialization Key 는 단일 세션을 위하여 사용되는 링크키로서 유닛이 초기화 될 때마다 생성된다. 이 키는 조합키나 유닛키가 아직 교환되지 않았을 때만 사용되며, 인증 과정에서 파라미터로 사용되게 된다.



[그림 3] Initialization Key 의 생성

키의 생성은 각각의 유닛에서 이루어 지며, 각 유닛은 IN_RAND 와 PIN, 그리고 L 을 파라미터로 하여 E_{22} 알고리즘을 통해 생성해 내게 된다.

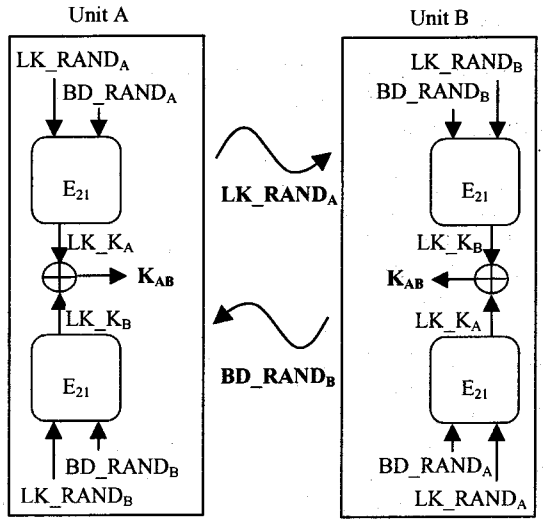
유닛키가 링크키로서 사용되어질 때 각각의 유닛들은 앞서 생성된 유닛키와 Initialization Key 를 통해 링크키로서 사용되어질 유닛키를 교환하게 된다



[그림 4] 유닛키의 교환

조합키의 생성

조합키는 각각의 유닛이 해당하는 자신의 Random number 를 생성하여 서로 교환을 하게 된다.
각각 교환된 Random number 는 아래의 그림과 같이 E_{21} 알고리즘을 통과하여 각각의 키를 생성의 내게 되고 그 키들을 XOR 하여 최종적으로 조합키를 생성해 낸다.



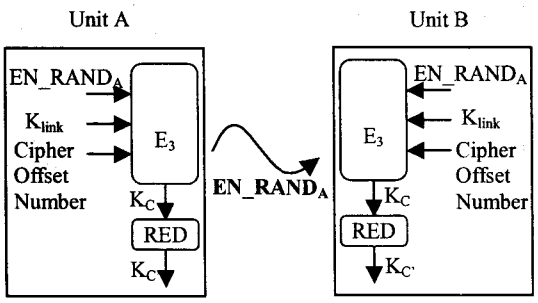
[그림 5] 조합키의 생성

인증

인증의 과정은 먼저 Unit B 는 자신의 BD_ADDR 을 Unit A 에게 전송하고, Unit A 는 인증에 관계된 Random number 를 생성하여 Unit B 에게 전송한다.
이때 각각의 유닛들은 넘겨 받은 파라미터들을 E_{22} 알고리즘을 이용하여 SRES 를 생성해 내게 되는데, Unit B 는 이 SRES' 를 Unit A 에게 전송하게 되고, Unit A 는 전송받은 SRES 값과 자신이 생성한 SRES 값을 비교하여 동일하다면 인증이 이루어 지게 된다

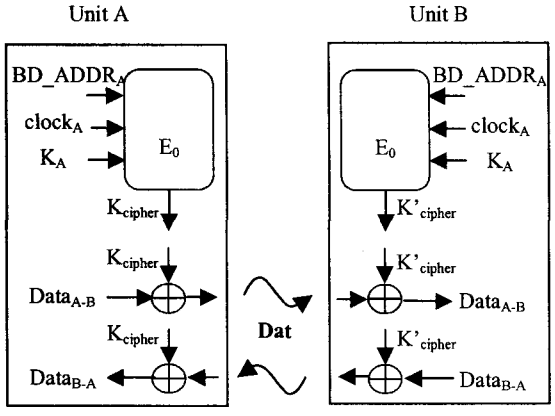
암호화 키의 생성과 통신

암호화 키는 데이터의 안전한 전송을 위해 각각의 유닛들이 가지고 있는 대칭키에 해당된다.
키의 생성을 위한 파라미터들은 앞서 생성된 링크키와 Random number 그리고 COF 로 구성되며, E_3 알고리즘을 통해 최종적인 암호화 키가 생성된다. 그리고 필요에 따라 짧은 암호화 키가 필요 할 경우 RED 를 거쳐 새로운 암호화 키를 만들어 내기도 한다.



[그림 6] 암호화키의 생성

이후 Encryption communication 의 과정은 간단하게 이루어진다. 송신측 유닛은 앞서 생성된 암호화키, K_c 와 전송하고자 하는 데이터를 XOR 하여 암호문을 만들어 내게 되고, 이 암호문을 전송하게 된다.
수신측은 수신된 암호문과 이전에 공유한 K_c 와 다시 XOR 을 하게 되면 최종적인 평문이 생성된다



[그림 7] 암호화 통신

3. 파라미터 교환방법

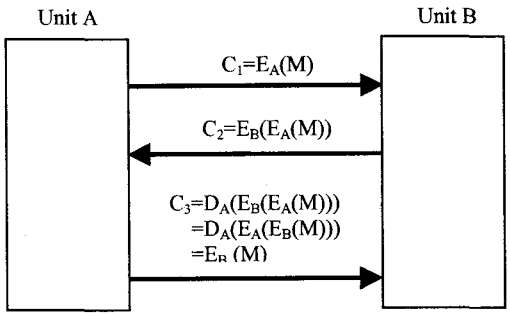
앞서 본 바와 같이 Bluetooth 의 전반적인 통신은 유닛키의 생성 및 교환, 링크키의 생성 및 인증의 절차를 통해 이루어 진다. 하지만 통신시의 데이터의 보안은 암호화 키로 암호화하여 전송하여 보안을 꾀할 수는 있지만, 암호화 키 생성 이전의 각종 키 생성 및 인증의 과정에서 필요한 파라미터들의 전송은 아무런 보안 과정을 거치지 않게 된다.

만약 Initialization Key 생성시 교환되는 파라미터 IN_RAND 와 PIN 이 노출되게 되면 Initialization Key 는 고스란히 공격자에게 노출되게 되고, Initialization Key 의 노출은 곧바로 유닛키를 링크키로 사용시 링크키의 노출로 이어지게 된다.
또 조합키를 링크키로 할 경우 조합키 생성시 교환되는 파라미터인 LK_RAND 이 노출되게 되면, 이후 이어지는 모든 과정 역시 노출되게 된다 [4].

파라미터 전달 프로토콜

앞에서 설명한 대로 Initialization Key 생성을 위하여 Unit 는 IN_RAND 를 UnitB 로 전달하는 First Handshake 를 수행한다. 본 논문에서는 다음과 같은 3-Way Handshake 방식을 사용하여 암호화 하여 IN_RAND 를 전달한다. 제안된 방식은 공유된 키나 공개키가 없는 환경에서 대칭키 방식만으로 키 설정을 가능하게 하는 키 전송 프로토콜이다. 이 프로토콜은 공유된 키를 사용하지 않는 다는 측면에서 Diffie-Hellman 방식과 비슷하지만, 두 개가 아닌 세 메시지를 사용한다는 점과 공개키 방식이 아니라는 점, 키 전송을 제공한다는 점 등이 달라 Bluetooth 에서 파라미터 교환이나 키 교환에 있어 적합하다.

[그림 8] 은 파라미터 전달 동작을 그림으로 보여주고 있는데 Bluetooth 에서 First Handshake 로 사용되거나 [그림 6]의 EN_RAND 전달에 사용 가능하다.



[그림 8] IN_RAND 전달을 위한 3-Way Handshake

먼저 Unit A 는 자신이 전송하고자 하는 파라미터를 자신의 암호화 알고리즘으로 암호화 하여 Unit B 에게 전송한다. 이를 수신한 Unit B 는 다시 자신의 암호화 알고리즘으로 수신된 메시지를 암호화하여 Unit A 에게 전송하게 되고, Unit A 는 수신된 메시지를 자신의 복호화 알고리즘으로 복호화하여 전송하게

된다. Unit B 는 수신된 메시지를 자신의 복호화 알고리즘으로 복호화하게 되면 최종적으로 Unit A 가 전송하고자 하는 파라미터를 얻게 된다.

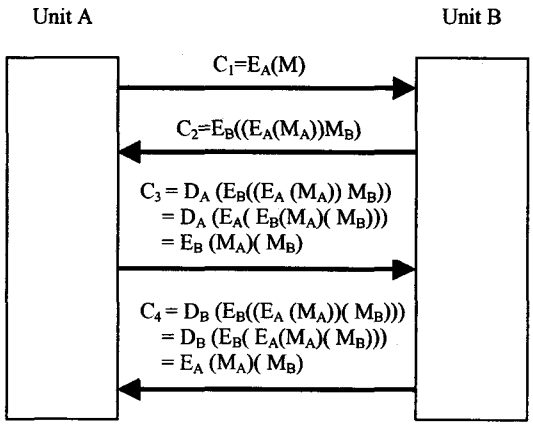
파라미터 교환 프로토콜

조합키를 생성하기 위하여 Unit A 는 LK_RAND_A 를 Unit B 에 전달해야 하고 Unit B 는 BD_RAND_B 를 Unit A 에 전달하여야 한다. 이 경우 앞에서 제안한 IN_RAND 전달 프로토콜을 사용하여도 무방하지만, 2 번의 3-Way Handshake 를 수행하여야 한다. 이를 개선하여 아래와 같은 4-Way Handshake 프로토콜을 제안하였다.

[그림 9]에서 조합키 생성시의 2 가지의 파라미터 교환 프로토콜을 보이고 있다.

먼저 Unit A 는 자신의 암호화 알고리즘으로 보내고자 하는 파라미터(M_A)를 암호화하여 전송한다. 이를 수신한 Unit B 는 자신이 보내고자 하는 파라미터(M_B)와 수신된 메시지를 함께 암호화 알고리즘으로 암호화하여 다시 Unit A 에게 전송한다. Unit A 는 수신된 메시지를 자신의 복호화 알고리즘으로 복호화하여 메시지를 Unit B 에게 보내게 되고, 이를 수신한 Unit B 는 최종적으로 자신의 복호화 알고리즘으로 복호화하여 Unit A 의 파라미터(M_A)를 얻게 되고, 다시 메시지를 전송하게 된다.

따라서 제안된 프로토콜은 LK_RAND_A, BD_RAND_B 의 전달을 단 4 번의 메시지 교환만으로 암호화하여 안전하게 수행할 수 있다.



[그림 9] 파라미터 교환을 위한 4-Way Handshake

4. 결 론

본 논문에서는 다양한 이기종 간의 무선으로 근거리에서 통신할 수 있도록 하는 기술인 Bluetooth 의 파라미터 교환을 통한 키 생성 메커니즘을 보이고 안전한 파라미터 전달을 위한 프로토콜을 제안하였다.

링크키 생성에 필요한 파라미터 전달은 3-Way Handshake 를 사용하여 파라미터 및 링크키 교환의 비밀성과 무결성을 보장 할 수 있다. 이 경우 안전한 전송을 위하여 3 번의 메시지 교환이 이루어 진다.

조합키를 생성하기 위하여 각 유닛은 자신의 파라미터를 상대방에게 서로 전달하여야 하는데, 이를 위하여 제안된 프로토콜은 4 번의 메시지 전달만으로 파라미터를 안전하게 교환할 수 있다. 이 결과 2 회의 3-Way Handshake 를 사용할 때 보다 메시지 교환 횟수가 2 회 줄게 되므로 효율적이다.

참고문헌

[1] Jennifer Bray and Charles F Sturman, "Bluetooth : Connect without cable" Peason Education, Inc 2001

[2] Hsu-Tun Teng and Ching-Nung Yang "Enhanced Mechanism of Key Management for Bluetooth Security" http:// sna.csie.ndhu.edu.tw/~cnyang/paper/17.pdf

[3] "The Bluetooth Specification, v.1.1" Volumes 1 and 2 http://www.bluetooth.com

[4] Gregory Lamm, Gerlando Falauto, Jorge Estrada and Jag Gadiyaram, "Bluetooth Wireless Networks Security Features" Proceedings of the 2001 IEEE Worshop on Information Assurance and Security. Online available. http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperW2A2(26).pdf

[5] 강주성, 김재헌, 박상우, 박춘식, 지성택, 하길찬, 한재우 공저 "현대 암호학" 경문사 2000

[6] L.Buttyan and J. P. Hubaux. "Report on a Working Session on Security in Wireless Ad Hoc Networks", Mobile Computing and Communications Review, Vol. 6, Number 4, 2003.