(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.^{7}
H04L 9/14

(45) 공고일자 2004년02월26일
(11) 등록번호 10-0419986
(24) 등록일자 2004년02월11일

(21) 출원번호 10-2002-0000683
(22) 출원일자 2002년01월07일

(65) 공개번호 10-2003-0060148
(43) 공개일자 2003년07월16일

(73) 특허권자 한국정보보호진흥원
서울특별시 송파구 가락동 78번지 IT벤처타워 서관

이임영
충남 천안시 쌍용3동 라이프아파트 102동 1103호

(72) 발명자 이임영
충남 천안시 쌍용3동 라이프아파트 102동 1103호

서대희
광주광역시서구풍암동부영2차아파트203동306호

(74) 대리인 특허법인 원전

심사관 : 문태진

(54) 타원곡선 암호알고리즘을 이용한 안전한 피코넷 형성 및유지 방법

요약

근거리 무선 통신의 표준 규격으로 주목 받고 있는 블루투스(bluetooth)는 무선 이동 통신상에서 유동성 디바이스간에 채널을 공유하여 2개 또는 더 많은 장치들이 1개의 마스터를 중심으로 피코넷을 형성한다.
따라서 본 발명에서는 안전한 피코넷을 형성 및 유지하는 방법으로서, ECC를 이용한 키 분배 방식과 서명을 이용하여 안전한 피코넷을 형성하고 비 인가된 디바이스간의 통신 및 연결은 해당 연결 요청 디바이스의 마스터와의 통신을 통해 연결 요청 디바이스를 인증하는 과정으로 이루어진다.

대표도

도 1

색인어

블루투스(bluetooth), 피코넷

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 타원곡선 암호알고리즘을 이용한 안전한 피코넷 형성과정을 나타낸 흐름도,
도 2는 본 발명에 따른 타원곡선 암호알고리즘을 이용한 안전한 피코넷 유지방법을 나타낸 흐름도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 타원곡선암호알고리즘(Elliptic Curve Cryptography: 이하 ECC라고 함)를 이용한 안전한 피코넷 형성 및 유지 과정으로서, 보다 상세하게는 근거리 무선 통신 기술인 블루투스(bluetooth)를 이용하여 피코넷을 형성하게 될 때, 피코넷의 중심이 되는 마스터를 중심으로 안전한 네트워크 형성이 되기 위한 암호화를 수행함에 있어 ECC를 이용함으로서 비인가자의 도청과 전력 소모 공격등을 방지함 과 동시에 안전한 피코넷을 유지하여 스카터넷으로 확장했을 때 안전한 네트워크 형성에 대한 내용이다.

암호화 디지털 서명을 위해 공개키 암호를 사용하는 제품과 표준의 대부분은 RSA(Rivest-Shamir-Adleman)를 사용한다. 안전한 RSA를 위한 비트 길이는 최근 수년동안 증가되어 왔고, 이것은 RSA를 사용하는 응용에서 훨씬 더 많은 계산 능력에 대한 부담을 가져왔다. 이러한 계산 능력에 대한 부담은 특히 안전한 거리를 처리하는 전자 상거래 사이트나 무선 환경에 적용하기엔 많은 부족한 점이 있다. 그러나 1985년에 Miller와 Koblitz에 제안된 타원형 곡선 알고리즘이 각광을 받으면서 이에 대한 표준이 진행중에 있다. ECC는 이산대수 문제를 기반으로 하여 이루어진 알고리즘이다. RSA에 비교하여 ECC의 주요 특징은 훨씬 작은 비트 크기로 동등한 안전성을 제공하여, 처리 오버헤드가 줄어든다는 것이다. 또한 연산 속도가 빠르다는 장점이 있다. 따라서 무선 인터넷이나 스마트 카드와 같은 제한된 환경에 적용하기가 적합하다.

ECDH는 X9.63으로 표준화 작업중에 있으며 Diffie-Hellman 방식을 타원 곡선에 적용한 키 분배 방식이다. 더 자세한 내용은 다음과 같다.

송신자의 비밀키 x_a 를 선택하고 공개키 $Q_a = x_a \times G$를 계산한 후 송신자는 공개키 Q_a 를 전송하고 수신자는 자신의 비밀키 x_b 를 선택하고 공개키 $Q_b = x_b \times G$를 계산한 후 Q_b 를 송신자에게 전송한다. Q_a 를 전송 받은 수신자는 공통된 세션키 생성을 위해 $K = x_a \times Q_b = x_b \times x_a \times G$를 계산하며, Q_b 를 전송 받은 송신자는 $K = x_a \times Q_b = x_a \times x_b \times G$를 계산한다.

따라서, 송신자와 수신자는 공통된 세션키 K를 공유하게 된다.

ECDSA는 타원곡선을 이용한 암호 시스템으로서 X9.62로 표준화된 서명 알고리즘이다.

ECDSA 서명을 서명을 위해서는 서명키와 검증키 쌍 $(d,Q),Q = dG$의 생성이 필요하다. 서명자는 임의의 난수 K에 대해 $(x,y)=KG$를 계산하고 $r = x \bmod n$, $s=(k^{-1} (H(M)+dr)) \bmod n$ 을 계산한다.

검증자는 ECDSA 서명의 검증을 위해 $u=(H(M)s^{-1}) \bmod n$, $v= rs^{-1} \bmod n$ 을 계산하고 $(x,y) = uG + vQ$를 확인한 후, $r = x \bmod n$ 인지 확인하여 서명자의 서명을 검증한다.

이러한 방식의 ECDH와 ECDSA는 RSA에 비해 키의 비트 뿐만 아니라 계산량을 현저히 감소시킬 수 있다. 따라서 유선 환경 뿐만 아니라 무선 환경에 RSA를 대신에 적용하기에 충분하다.

통신시장의 환경이 유선에서 무선으로 이동해가고 있는 시점에 있다. 과거 무선은 가격이 비싸고, 전송 속도도 느리고, 또한 데이터 전송이 불안정하다는 말은 점점 사라져가고 있다.

현재 무선 멀티미디어 시장에서 가장 주목을 받고 있는 것이 블루투스(bluetooth)이다. 블루투스(bluetooth)가 기존의 무선 통신장비에 비해서 더욱 각광 받는 이유는 통신기능이 없는 디바이스에 간단하고 조그마한 모듈을 첨가함으로써 서로 무선 네트워크로 연결을 할 수 있다는 점이다. 또한 연결 시 서로 무선통신을 할 수 있는 범위 안에만 있으면 연결이 쉽게 되므로 사용상의 간편함을 들 수 있다.

블루투스(bluetooth)는 94년 에릭슨의 이동통신그룹이 휴대폰과 주변기기 사이의 소비전력이 낮고, 가격이 싼 무선(Radio) 인터페이스를 연구하기 시작하면서 비롯되었다. 그후 에릭슨, 노키아, IBM, 도시바, 인텔, 모토로라, 마이크로소프트, 루슨트 테크롤로지, 3Com 등 9개의 주도그룹인 SIG(Special Internet Group)을 중심으로 현재 2000여개 이상의 기업들이 회원으로 가입이 된 상태이다. 또한 국내 참여 기업도 70여 곳에 이르고 있다. 그리고 블루투스(bluetooth) 스펙도 99년 1.0을 발표한 이래로 2001년에 2.0을 공개할 예정으로 있다. 현재 블루투스(bluetooth)는 발전하는 단계에 있다. 블루투스(bluetooth)의 무한한 잠재력을 믿고 국내의 기업 뿐만아니라, 세계의 우수 기업들이 대거 참가를 하고 있다. 하지만 현재 블루투스(bluetooth)는 많은 부분의 보완을 필요로 하고 있다.

현재 블루투스(bluetooth)를 기존의 가전기기에 설치하여 사용하기 위해서는 단가를 낮추어야 하고 짧은 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 방법을 연구 개발하여야 한다.

이처럼 현재 블루투스(bluetooth)는 시작단계에 있는 기술이기 때문에 모든 사람의 욕구를 충족 시킬수는 없다. 하지만 과거 컴퓨터가 연구소나 공공기관에서만 사용하는 전유물에서 현재 누구나 편리하게 이용할 수 있는 개인 생활용품으로 변모했던 것처럼 블루투스(bluetooth)도 앞으로 다가올 첨단 멀티미디어 세상에 커다란 영향을 미칠 기술로 기대되어지고 있다.

근거리 무선 통신의 표준으로 주목받고 있는 블루투스(bluetooth) 통신기술을 좀 더 상세히 설명한다. 정보통신 산업이 무엇을 위해 발전해 왔는가를 생각해보면 알 수 있다. 그것은 자유, 안전, 다기능, 간편함, 신뢰성이다. 하나 더 추가하자면 21세기 최대의 산업인 인터넷 산업 분야에 가장 적합하도록 설계되어 있다는 점이다. 미래에는 인터넷에서 자유로이 여행을 할 수 없다면 그 사람은 무인도에서 사는 자와 다른 바가 없을 것이다.

한 휴대용 PC 사용자의 인터넷 사용기를 예로 들어보자. 2.4GHz 주파수 대역으로 최대 1M의 속도로 휴대용 PC로 주변 10m/100m이내에 유선망(POTS, ISDN, xDSL)이나 유선LAN(10BaseT, 100BaseT, Wireline), 무선망(Cellular, PCS, Paging, Satellite), 무선LAN(802.11, SWAP)등 외부 통로만 있으면 언제든지 접속이 가능하다. 물론 전자우편(E-Mail)도 가능하고 블루투스(bluetooth)는 자체 보안 기능(key운영, Authentication, Encryption 등)을 가지고 있을 뿐만 아니라 1600번의 주파수 도약으로 전자상거래와 같은 높은 보안이 필요한 통신 매체로도 활용할 수 있다.

휴대전화 사용의 경우 무선 귀걸이형 전화(HandSet)만 있으면 전화가 어디 있든 언제든지 전화할 수도 있고, 전화기 한 대로 사무실과 가정에서 전화비용을 낼 필요없이 무선 인터넷폰으로 전화를 사용할 수 있다. 일반전화(PSTN), 휴대전화(Cellular, PCS)까지 사용할 수 있어 전화 하나로 3가지 전화를 쓰는 효과가 된다. 응용 분야는 무궁무진하며 그동안 우리가 생각지도 못했던 아이디어도 블루투스(bluetooth)가 나타남으로 해서 실현 가능해졌다.

일반적인 인터페이스(UART, USB, PCM, PCMCIA등)을 제공하고 ISM Open band로 연결시키는 저가, 소형, 저전력 소모의 블루투스(bluetooth)가 모든 전자분야 개발자들의 관심을 받고 있는 것은 당연한 일이다).

한편, 사용자 보호와 정보 보안을 위해 시스템은 쌍방 환경에 적당한 보안 기능을 제공해야 한다. 즉, 블루투스(bluetooth)에서 각 유닛은 인증과 보안 알고리즘을 같은 방식으로 구현해야 한다.

기본적 수준의 보안이 정의되어 칩 구현에 적당하도록 될 것이고 인증 알고리즘은 처리 기능에 있어서 장치에 무리가 가지 않는 수준에서 제공될 것이다. 암호화 알고리즘에 대한 앞으로의 지원계획은 후방향 호환성(Backward Compatibility)을 지원할 것이며, 제공되는 주요 보안 기능은 다음과 같다.

· Challenge response routine for authentication

· Stream cipher for encryption

· Session key generation - session keys can be changed at any time during a connection

블루투스(bluetooth) 보안 중에서 가장 높은 수준은 Link-Level에서의 보안을 들 수 있다. 블루투스(bluetooth) 개발자들은 블루투스(bluetooth) 기술들의 보안적 위험에 대해서 고려해야 한다. 결과적으로 인증과 암호화를 통해 블루투스(bluetooth) 보안을 이룬다. 인증은 도청을 통해 데이터와 메시지의 생성자를 밝힐 수 있으므로 인증이 반드시 필요하다.

블루투스(bluetooth)와 보안적인 이슈는 크게 암호 알고리즘, 키 관리, 인증 프로토콜로 구분할 수 있다. 먼저 두 개의 장치들이 초기화 통신할 때 초기화 통신을 할 수 있게 하는 믿을 수 있는 인증과 연결키를 만드는 것을 필요로 하게 된다. 이러한 과정을 페어링(pairing) 과정이라 부른다.

초기 연결을 위해서 페어링(pairing) 참여자들은 각각의 장치에 최대 128비트까지 블루투스(bluetooth) 보안키를 사용하도록 요구한다. 두 개의 블루투스(bluetooth) 디바이스들이 통신할 때는 링크 키라는 키를 이용하여 인증과 암호화를 요구하게 된다. 페어링은 이러한 과정이 진행될 때 비밀 공유된 PIN을 out-of-band로 주고받는다.

페어링 과정은 키 관리 혹은 키 교환에 사용된다. 블루투스(bluetooth) 보안이 일시적으로 사용될 경우 128비트 난수를 연결키로 사용되기도 하며 한쌍으로 된 장치들에 동일한 인증을 통해서 한쌍의 장치들 사이에 반영구적으로 사용되기도 한다.

또한 서비스 레벨에서의 보안 모드를 통해 제한된 접근으로 사용자들을 위하여 사용된 서비스와 장치들에 대하여 보안 수준을 정의 내리게 된다. 이것은 서비 스 보안 레벨을 참고하게 된다.

인증과 암호화는 각각 블루투스(bluetooth) 디바이스에 같이 시행되며 이것은 특별한 목적으로 네트워크를 형성하기 위한 특징이기도 한다.

연결은 일방적이기도 하고 일방향(one-way), 양방향(two-way) 또는 인증이 필요 없는 경우도 있다. 인증은 시도 응답 알고리즘에 바탕을 두고 있다. 인증은 블루투스(bluetooth) 시스템에서 매우 중요한 부분이다. 사용자가 다른 사용자의 디바이스와 통신을 하기 위해서는 이러한 시도응답을 통해 믿을 수 있는 연결을 허가하게 된다.

블루투스(bluetooth)의 인증은 다른 장치들 간에 연결이 암호화되기 이전에 암호화키를 가지고 있다는 것을 증명하기 위한 사전과정이다. 또한 연결관리 결과가 서로 다른 암호화키를 사용하는 혼란을 막기 위해서 사용된다.

암호화는 연결의 비밀성을 지키기 위해서 사용된다. 블루투스(bluetooth)는 스트림 암호 알고리즘과 함께 키의 길이는 유동성을 제공한다. 키 관리는 좀 더 높은 소프트웨어 계층에서 제공되는데 서비스의 보안 수준은 3가지로 정의된다.

· 권한부여 요구: 접근에 대한 권한부여가 진행하고 신뢰받고 있는 장치들 혹은 신뢰받고 있지 않는 장치들에 의해 자동적으로 승인된다. 권한부여는 장치로부터의 인증이 다른 것이 아닌지에 대한 증명을 항상 요구하게 된다.

· 인증요구 : 응용 측면에서 연결이 이루어지기 전에 장치에 대한 인증이 이루어져야 한다.

· 암호화 요구 : 이 단계는 서비스로 접근이 가능하기 전에 암호화 방법에 대한 요구가 이루어진다.

이러한 정보는 보안 경영자에 의해 서비스 데이터 베이스에 기록되며 만약 등록이 되지 않으면 일반 보안 수준으로 정의된다. 블루투스(bluetooth) Specification에서는 보안 형태에 따라 다음과 같이 3가지 보안 모드를 정의하고 있다.

· 보안 모드 1 : 디바이스는 어떠한 보안 프로시저(procedure)도 가지고 있지 않다.

· 보안 모드 2 : 디바이스는 L2CAP 레벨에서의 채널 설정 이전에 보안 프로시저를 획득할 수 없다. 이 모드는 응용을 위한 이질적이고 유동적인 access 정책을 허용하는 것으로서, 특히 서로 다른 보안 요구사항을 갖는 응용에서 수행된다.

· 보안 모드 3 : 디바이스는 LMP 레벨의 link set-up이 완벽하게 이뤄지기 이전에 보안 프로시저를 가질 수 있다.

블루투스(bluetooth)는 서로 다른 2개의 디바이스들 사이에 믿을 수 있는 수준을 다음과 같이 3가지 형태로 구별하게 된다.

· 신뢰받고 있는 장치: 블루투스(bluetooth) 디바이스들은 믿을 만한 입증이 사전에 이루어진 장치로서 링크 키는 저장되며 디바이스의 데이터베이스에 신뢰성이 표시된다.
· 믿을 수 없는 장치: 블루투스(bluetooth) 디바이스 장치는 믿을만한 입증이 되어 있으며 링크 키는 저장되지만 디바이스의 데이터 베이스에서 신뢰성이 표기되지는 않는다.
· 알 수 없는 장치 : 보안 정보가 표기되어 있지 않는 장치이다. C. Gamage 등은 대리 서명 방식과 수신자 지정성을 제공하기 위해 제시된 Signcryption 방식을 동시에 적용한 대리-Signcryption 방식을 제안하였다. 사용자가 선정한 대리인으로 하여금 자신을 대신하여 정당한 수신자 지정 서명을 수행할 수 있도록 구성된 방식으로 서명 생성 시 요구되는 계산을 상대적으로 계산 능력이 뛰어난 Proxy Agent에 위탁할 수 있도록 구성되어 있다.
또한 블루투스(bluetooth)는 마스터를 중심으로 여러개의 슬레이브가 연결이 가능하며 이러한 경우 피코넷(piconet)이라 부른다. 즉, 한 피코넷에서 하나의 마스터(Master)는 동시에 최대 7개의 슬레이브 디바이스(Slave device)와 연결할 수 있다. 피코넷이 형성되었을 경우 상호 채널이 교환되며, 이러한 피코넷 여러 개가 서로 연결돼 있을 때 이것을 스카터넷(scatternet)이라고 한다.
그러나 현재의 블루투스(bluetooth)가 제공하고 있는 보안 서비스는 표준안 자체 문제점인 PIN 길이에 따른 취약점 뿐만 아니라 무선 채널 상에 악의있는 공격으로부터 안전성을 유지할 수 없는 문제점을 안고 있다.
또한 안전하지 못한 보안 서비스를 바탕으로 이루어지는 피코넷은 당연히 안전하지 못하는 문제로 귀결된다. 그외에도 스카터넷으로 확장했을 때 전력 소모 공격 및 도청 공격에 매우 취약하기 때문에 무선 통신상에서 여러 응용 분야에 실제 적용하기에는 문제가 있다.
전술한 바와 같은 현재의 근거리 무선 통신 규격으로 많은 연구가 되고 있는 블루투스(bluetooth)는 여러 가지 보안 서비스를 제공하고 있으나 실제 적용하기엔 많은 문제점을 안고 있으며, 무선 통신상에서 사용자에게 큰 악영향을 미칠 수 있는 문제점이 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 근거리 무선 통신상에서 사용자를 중심으로 안전한 피코넷을 형성하여 블루투스(bluetooth)를 실제 적용했을 시 기밀성과 안전성을 확보하기 위한 ECC를 이용한 안전한 피코넷 형성 및 유지 과정과 프로토콜을 제공하는 것을 목적으로 한다.
본 발명의 또 다른 목적은 근거리 무선 통신상에서 사용자를 중심으로 피코넷이 형성 되었을 때 사용자의 프라이버시 보호 뿐만 아니라 블루투스(bluetooth)를 이용한 무선 이동 통신에서 기밀성과 안전성을 제공할 수 있는 ECC를 이용한 안전한 피코넷을 제공하는 것이다.
이러한 목적을 달성하기 위해 본 발명은 이동 통신 단말기를 블루투스(bluetooth) 피코넷 형성을 위해 마스터와 슬레이브로 구분하여 초기 안전한 inquiry 과정을 거친 후 PIN 번호의 공유 및 유저의 PIN 입력이 올바르게 이루어졌으며 PIN에 근거해 25시간마다 갱신되는 WPKI 인증서를 가지는 전제 조건과, 상기 전제 과정을 통해 생성된 정보를 바탕으로 마스터와 슬레이브의 상호 인증 단계인 제 1 과정과, 그룹 키를 이용한 그룹 서명 단계인 제 2 과정과, 마스터간의 비인증된 슬레이브의 접속 요구가 있을 경우 안전한 연결 과정인 제 3 과정과, 마스터 간의 인증이 이루어진 경우 그룹 키를 이용한 인증 과정인 제 4 과정을 포함 하여 이루어지는 것이 특징이다.
본 발명에 따른 ECC를 이용한 안전한 피코넷의 세부적 특징으로는 통신 부하를 줄일 수 있는 ECC를 이용한다는 것과 비익명성 그룹키를 이용한다는 점이다.

발명의 구성 및 작용

이하, 첨부된 도면을 참조로 본 발명을 설명한다. 먼저 본 발명에 의해 구현될 수 있는 블루투스(bluetooth) 피코넷의 요구사항을 살펴보기로 한다.
첫째, 무선 이동 통신 정보 송·수신 시 요구사항
① 비밀성: 송·수신되는 모든 정보는 암호화하여 제 3 자에 의한 불법적인 정보 도용을 방지해야 한다.
② 인증성: 메시지 송·수신시 출처가 누구이며, 전송 도중 불법적인 제 3자로부터 위조 및 변경되지 않았음을 보증하는 것으로서 디지털 서명 기법이 적용된다.
③ 무결성: 각 객체간의 상호인증을 통해 피코넷 형성 주체간의 정보에 대한 무결성이 보장되어야 한다.
둘째, 블루투스(bluetooth)에서의 구성 요소에 대한 요구사항
① 유효성: 무선 이동 통신은 메시지 송·수신을 위해서 일반 네트워크에 비해 상대적으로 계산 능력이 떨어지는 무선 단말기를 사용한다. 따라서 사용자 측면에서도 충분히 사용 가능해야 한다.
② 검증성: 무선 이동 통신에서 메시지 송·수신에 참여하는 개체들이라 할 지라도 위조 및 변조가 불가능해야 한다.
도 1은 본 발명에 따른 안전한 피코넷 형성 절차를 나타낸 흐름도이다. 크게 마스터와 슬레이브의 상호 정보 제공 과정(A1 B3)과, 그룹키 정보의 송/수신 과정(C1 D3)과, 마스터에서의 인증확인 과정(E)으로 이루어진다.
본 발명에서는 안전한 피코넷 형성을 위해 마스터는 ECDH를 이용해 세션키를 생성하여 이용하고 있으며, ECDSA 서명값과 세션키를 이용해 그룹키를 분배함으로서 피코넷이 형성되며, 비인증된 슬레이브의 접속 요구가 있을 경우 해당 접속 요구 슬레이브의 마스터와의 통신을 통해 슬레이브를 인증함으로써 피코넷의 안전한 유지 과정을 제시하고 있다. 따라서 그룹 키를 통한 피코넷 형성은 해당 피코넷 객체들에 대한 인증이 이루어지므로 차후 분쟁이 발생할 경우 비인가된 모바일 디바이스의 부정으로부터 서로를 보호하게 된다. 이렇게 함으로써 스카터넷 확장시 안전한 스카터넷의 형성 및 유지가 가능하다.

본 발명에서 표기되는 기호들은 다음과 같이 정의한다.

*: M: 블루투스(bluetooth) 마스터, S : 블루투스(bluetooth) 슬레이브

· p_{*} : ECC 암호 알고리즘을 기반으로한 *의 공개키 (p≥128비트)

· q_{*} : ECC 암호 알고리즘을 기반으로한 *의 비밀키 ($q = aP, P \in E(Z_P)$)

· g, eta : 중앙 서버가 공개한 시스템 계수

· h_{*} : *가 생성한 안전한 해쉬값

· r_M , r_S : 각 해당 객체의 의사 랜덤수

· T_{*} : *의 타임 스탬프

· EC : 타원곡선 암호 알고리즘

· G : Base Point

· n : G의 위수

· R_{*} , S_{*} : *가 생성한 ECDSA 서명값

· ID_{infor} : *의 정보

· E : 관용 암호 알고리즘

· Z : 블루투스(bluetooth) 마스터가 피코넷 그룹원에게 공개할 시스템 계수
(Z= g^{q_m} mod η [g∈GF(p_M)])

· i : 블루투스(bluetooth) 마스터가 피코넷 그룹원에게 할당하는 키의 개수
($i \in (1,....,p_M -1)$)

· S_j : 블루투스(bluetooth) 피코넷 그룹키 서명값

· ξ* : *가 생성한 연접값

· S_{info} : 블루투스 피코넷에 접속을 요구하는 블루투스 슬레이브 정보

· $S_{info_{req}}$: 블루투스 피코넷에 접속을 요구하는 블루투스 슬레이브의 S_{info} 의 응답값

· R_{BS} , S_{BS} : 블루투스(bluetooth) 피코넷에 접속을 요구하는 블루투스(bluetooth) 슬레이브 서명값

· (p_{Mi} , n_{Mi}) : 그룹키 생성을 위해 블루투스(bluetooth) 마스터에서 생성한 임의의 키쌍

ζ : 피코넷을 형성하는 Bluetooth slave 갯수

*V*_@#* : #으로 암호화 되어 *에서 @로 전송되는 암호화된 값

블루투스(bluetooth) 마스터와 슬레이브는 PIN번호를 기반으로 25시간마다 갱신되는 인증서를 가지고 있으며 ECC 기반의 ECDSA 서명을 사용하였으며, 그룹키 분배를 위한 세션키 K의 생성은 ECDH를 사용하는 것을 전제로 한다.

먼저 마스터(Master)는 무작위 추출값(random)(r)을 사용하여 타원곡선 암호 알고리즘을 기반으로 한 비밀키 Q_M 을 생성하고(A-1) $Q_M = r_M \cdot G$)(A-1), 자신의 정보(ID_{infor_M})와의 연접값 ($\xi^M = (Q_M \| ID_{infor_M})$)을 구한다. 이후, 연접값(ξ^M)에 해쉬를 취하고(A-2), 그 값($h_M = H (\xi^M$))을 슬레이브의 공개키(EC_{q_M})로 암호화하여 $V_{M\text{-}S_{Q_M}}$ 을 계산하고 이를 슬레이브에 전송한다. ($V_{M\text{-}S_{Q_M}} = EC_{q_M}(\xi^M \| h_M)$)(A-3)

슬레이브(Slave)는 전송받은 $V_{M\text{-}S_{Q_M}}$ 을 확인하고 마스터와 유사한 방식으로 $V_{S\text{-}M_{Q_S}}$ 을 계산하여 마스터에게 전송한다.

$Q_S = r_S \cdot G$

$\xi^S = (Q_S \| ID_{infor_S})$ ·························(B-1)

$h_S = H (\xi^S)$ ·························(B-2)

$V_{S\text{-}M_{Q_S}} = EC_{q_S}(\xi^S \| h_S)$ ·························(B-3)

마스터는 슬레이브로부터 제공받은 수식의 정상여부를 확인하여, 비 정상적 수식인 경우, 슬레이브의 정당한 디바이스 정보와 세션키 정보를 재생성할 것을 요구하는 메시지를 전송한다.

마스터는 ζ* (p_{Mi} , n_{Mi})을 계산한 뒤 임의의 키쌍들인 (p_{Mi} , n_{Mi})과 ECDSA 서명값인 R_M ,S_M 을 생성하고(C-1), 생성된 각 값을 연접하여 이를 안전한 해쉬 값으로 계산한 뒤(C-2) 세션키 K 로 암호화하여 $V_{S\text{-}M_K}$ 를 슬레이브에게 전송한다(C-3).

$(\xi_1)^M = ((p_{Mi}/n_{Mi}) \| R_M \| S_M)$

$h_M = H((\xi_1)^M)$

$V_{M\text{-}S_k} = E_K((\xi_1)^M \| h_M)$

슬레이브는 전송받은 $V_{M\text{-}S_K}$ 과 h_M 으로 무결성과 기밀성을 검증하고 임의의 키쌍을 선택하여 서명값 $S_j(j \in i)$ 를 수행한 뒤(D-1) 슬레이브의 ECDSA서명을 기반으로 안전한 해쉬값을 생성하고(D-2) 세션키 K 로 암호화 한 뒤 $V_{S\text{-}M_K}$ 를 블루투스 마스터에게 전송한다(D-3).

$(\xi_1)^S = (S_j \| R_S \| S_S \| T_S)$

$h_S = H((\xi_1)^S)$

$V_{S\text{-}M_K} = E_K((\xi_1)^S \| h_S)$

여기에서 ECDSA 서명값은 이후 블루투스 피코넷 프로토콜에서 블루투스 슬레이브를 인증하기 위하여 사용된다.

마스터는 슬레이브에게 전송받은 $V_{S\text{-}M_K}$, h $_S$ 를 검증하여 무결성과 기밀성을 검증한다. 이때, 마스터는 자신이 생성한 임의의 키 쌍들과 슬레이브가 서명한 서명값을 믿을 수 있는 제 3 자 혹은 제 3 기관 등의 검증자에게 전송하여($\zeta^*(n_M)$ 리스트) 자신의 슬레이브에게서 받은 서명에 대한 검증을 수행한다. 만일, 서명이 정상적인 것이 아닌 경우, 슬레이브의 개인서명값과 그룹키 서명을 재전송할 것을 슬레이브에게 요구하는 메시지를 전송한다. 정상적인 경우, 이벤트 종결 메시지를 슬레이브에게 전송하고, 슬레이브로부터 이벤트 종결에 관련한 메시지를 수신함으로써 안전한 네트워크를 형성한다.(E)

이상에서 설명한 바와 같이, 마스터는 그룹키 서명값(S $_j$)을 이용하여 피코넷 슬레이브를 인증하고, 슬레이브는 마스터의 서명값(R, S)으로 마스터를 인증함으로써 마스터를 중심으로 안전한 피코넷을 형성한다.

이와 같이 형성된 네트워크(피코넷)을 형성한 후 슬레이브의 접속요구에 대하여 두 가지 처리 방법이 있을 수 있다.

서로 인증이 이루어지지 않은 상태에서 비인증된 피코넷에 포함된 슬레이브로부터의 접속 요구와 서로 인증이 완료된 피코넷의 슬레이브로부터 마스터로의 접속 요구가 있는 경우이다.

도 2는 본 발명에 따른 안전한 피코넷을 유지방법을 나타낸 흐름도이다.

먼저 접속을 요구한 슬레이브가 인증된 피코넷에 포함되어 있는 지 아니면 비인증된 피코넷에 포함된 슬레이브인가 여부를 확인한다.(S1 과정)

마스터간에 서로 인증이 된 경우에는 해당 슬레이브에 대한 특별한 인증과정없이 접속 요청이 있을 경우 그룹키를 분배하여 자신의 피코넷에 포함시키면 된다.(S6)

그러나, 비인증된 피코넷의 슬레이브로부터 접속요구가 있는 경우는 다음과 같은 처리절차를 거치게 된다.

마스터(A)는 $V_{M_A\text{-}M_B K}$ 를 계산하여 마스터(B)에 전송한다. 마스터(A)가 마스터(B)에게 접속요구 슬레이브로부터 제공된 정보의 정당성을 확인하기 위한 절차이다.(S2)

$$(\xi)^{M_A}=(R_A \| S_A \| ID_{info} \| T_A \| S_{info})$$

$$h_{M_A}=H((\xi)^{M_A})$$

$$V_{M_A\text{-}M_B K}=E_K((\xi)^{M_A} \| h_{M_A})$$

마스터(B)는 해당 마스터(A)의 ECDSA 서명값을 저장하고 S_{info} 를 확인 후 안전한 해쉬 값을 계산하고 마스터(A)의 공개키로 암호화한 뒤 $V_{M_B\text{-}M_A p_{M_A}}$ 를 마스터(A)에게 전송한다.(S3)

$$(\xi^{M_B})=(R_B \| S_B \| R_{BS} \| S_{BS} \| T_B \| S_{info_{req}})$$

$$h_{M_B}=H(\xi^{M_B})$$

$$V_{M_B\text{-}M_A p_{M_A}}=EC_{a_{M_A}}((\xi^{M_B} \| h_{M_B})$$

접속요구 슬레이브는 $V_{S\text{-}M_A p_{M_A}}$ 를 계산하여 마스터(A)에 전송한다.(S4)

$$(\xi_2)^S=(R_S \| S_S \| T_S)$$

$$h_S=H((\xi_2)^S)$$

$$V_{S\text{-}M_A p_{M_A}}=EC_{a_{M_A}}((\xi_2)^S \| h_S)$$

마스터(A)는 슬레이브로부터 전송된 값($V_{S\text{-}M_A p_{M_A}}$)과 마스터(B)로부터 전송된 값의 무결성과 기밀성을 확인한 후, 슬레이브에게 전송되어온 서명값과 마스터(B)에게 전송되어온 해당 슬레이브의 서명값의 동일 여부를 확인한다.(S5)

만일 동일하지 않은 경우 에러(error)처리하고(S7), 정상적인 슬레이브로 확인된 경우 접속요구 슬레이브를 인증하고 그룹키를 분배한다.(S6)

이상에서 본 발명에 대한 기술 사상을 첨부 도면과 함께 서술하였지만 이는 본 발명의 가장 양호한 실시 예를 예시적으로 설명한 것이며 본 발명을 한정하는 것은 아니다. 또한, 이 기술 분야의 통상의 지식을 가진 자이면 누구나 본 발명의 기술 사상의 범주를 이탈하지 않는 범위 내에서 다양한 변형 및 모방이 가능함은 명백한 사실이다.

발명의 효과

이상에서 설명한 바와 같이 본 발명은 종래의 블루투스(bluetooth) 피코넷 형성에서 나타나는 보안적 취약점을 극복하고자 하였다. 또한 무선 단말기에서의 계산량 증가에 따른 효율성 저하를 방지하기 위하여 ECC를 이용하여 해결하고 있으며, 피코넷 형성 및 유지 뿐만 아니라 더 큰 네트워크로 확장시 안전성을 확보하기 위해 하나의 네트워크마다 고유의 그룹 키 쌍을 생성함으로써 안전성을 유지하고 있다. 또한, 컴퓨터 네트워크 및 이동 통신의 발전으로 향후 정보화 사회는 전자 상거래 서비스들을 비롯하여 더욱 다양한 응용 서비스들을 제공하게 될 것이다.

이러한 이동 통신 환경 상에서 기밀성 및 인증성을 제공하는 안전한 피코넷 형성과 유지과정에 대한 제안은 전자 상거래 서비스 및 응용 서비스들의 발전에 기여하는데 큰 효과가 있을 것이라 판단된다.

(57) 청구의 범위

청구항 1.

무선 이동통신상에서 유동성 장치간에 채널을 공유하여 다수의 장치들이 하나의 마스터를 중심으로 피코넷을 이루는

블루투스(Bluetooth) 통신 프로토콜 상의 안전한 네트워크 형성방법에 있어서;
마스터(master)가 타원곡선암호알고리즘(ECC)을 기반으로 한 비밀키를 생성하는 과정(A-1)과,
상기 비밀키 값에 마스터의 정보를 연접하여 이를 해쉬함수로 계산한 값을 추출하는 과정(A-2)과,
상기 A-2과정에 의한 결과값을 타원곡선암호 알고리즘(ECC)을 이용하여 암호화하여 슬레이브에게 전송하는 과정(A-3)으로 이루어지는 마스터 암호정보 제공과정(A)과,
슬레이브(Slave)는 마스터로부터 제공받은 마스터 암호 정보를 확인하고, 타원곡선암호알고리즘(ECC)을 기반으로 한 비밀키를 생성하는 과정(B-1)과,
상기 비밀키 값에 슬레이브의 정보를 연접하여 이를 해쉬함수로 계산한 값을 추출하는 과정(B-2)과,
상기 B-2과정에 의한 결과값을 타원곡선암호 알고리즘(ECC)을 이용하여 암호화하여 마스터에게 전송하는 과정(A-3)으로 이루어지는 슬레이브 암호정보 제공과 정(B)과,
마스터가 그룹키(group key) 생성을 위해, 피코넷을 형성하는 블루투스 슬레이브(Bluetooth slave)의 수에 해당하는 임의의 키쌍들과, 타원곡선을 이용한 암호시스템(ECDSA)을 이용한 서명값을 생성하는 과정(C-1)과,
임의의 키쌍값과 서명값을 연접하여 안전한 해쉬 값을 계산하는 과정(C-2)과,
세션키(K)로 암호화하여 슬레이브에게 전송하는 과정(C-3)을 포함하여 이루어지는 그룹키정보 송신과정(C)과,
슬레이브에서 상기 그룹키정보 송신과정을 통해 마스터로부터 제공받은 정보의 무결성과 기밀성을 검증하는 과정(D-1)과,
임의의 키쌍을 선택하여 서명값을 생성하고 타원곡선을 이용한 암호시스템(ECDSA)을 기반으로 안전한 해쉬 값을 생성하는 과정(D-2)과,
세션키(K)로 암호화하여 마스터에게 전송하는 과정(D-3)을 포함하여 이루어지는 그룹키정보 수신과정(D)과,
마스터에서 슬레이브로부터 수신한 정보의 무결성과 기밀성을 검증하여 확인 메시지를 전송하는 이벤트 종결과정(E)을 포함하여 이루어지는 타원곡선 암호알고리즘을 이용한 안전한 네트워크 형성방법.

청구항 2.

제 1 항에 있어서;
상기 슬레이브 암호정보 제공과정(B)을 통해 마스타에게 제공된 수식이 정당하지 않은 경우, 마스터가 슬레이브에게 슬레이브의 정당한 디바이스 정보와 세션 키 정보의 재생성을 요구하는 과정이 부가되는 것을 특징으로 하는 타원곡선 암호알고리즘을 이용한 안전한 네트워크 형성방법.

청구항 3.

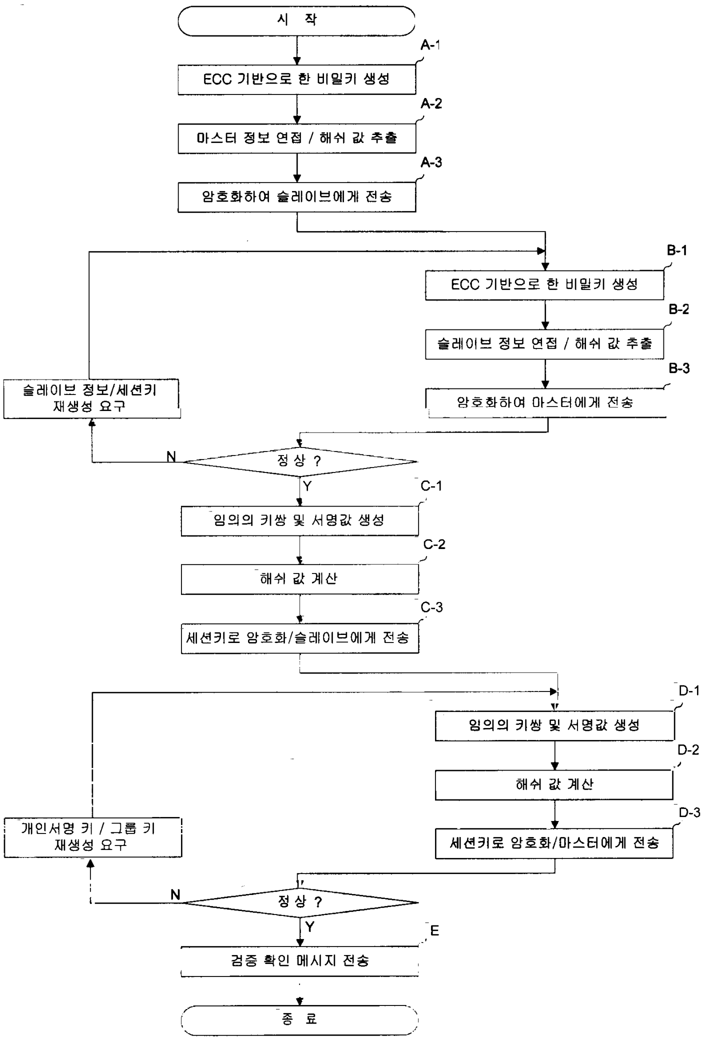
제 1 항에 있어서,
상기 이벤트 종결과정(E) 중 수식이 정당하지 않은 경우 마스터가 슬레이브의 개인 서명 값과 그룹 키 서명 재전송을 요구하는 과정이 부가되는 것을 특징으로 하는 타원곡선 암호알고리즘을 이용한 안전한 네트워크 형성방법.

청구항 4.

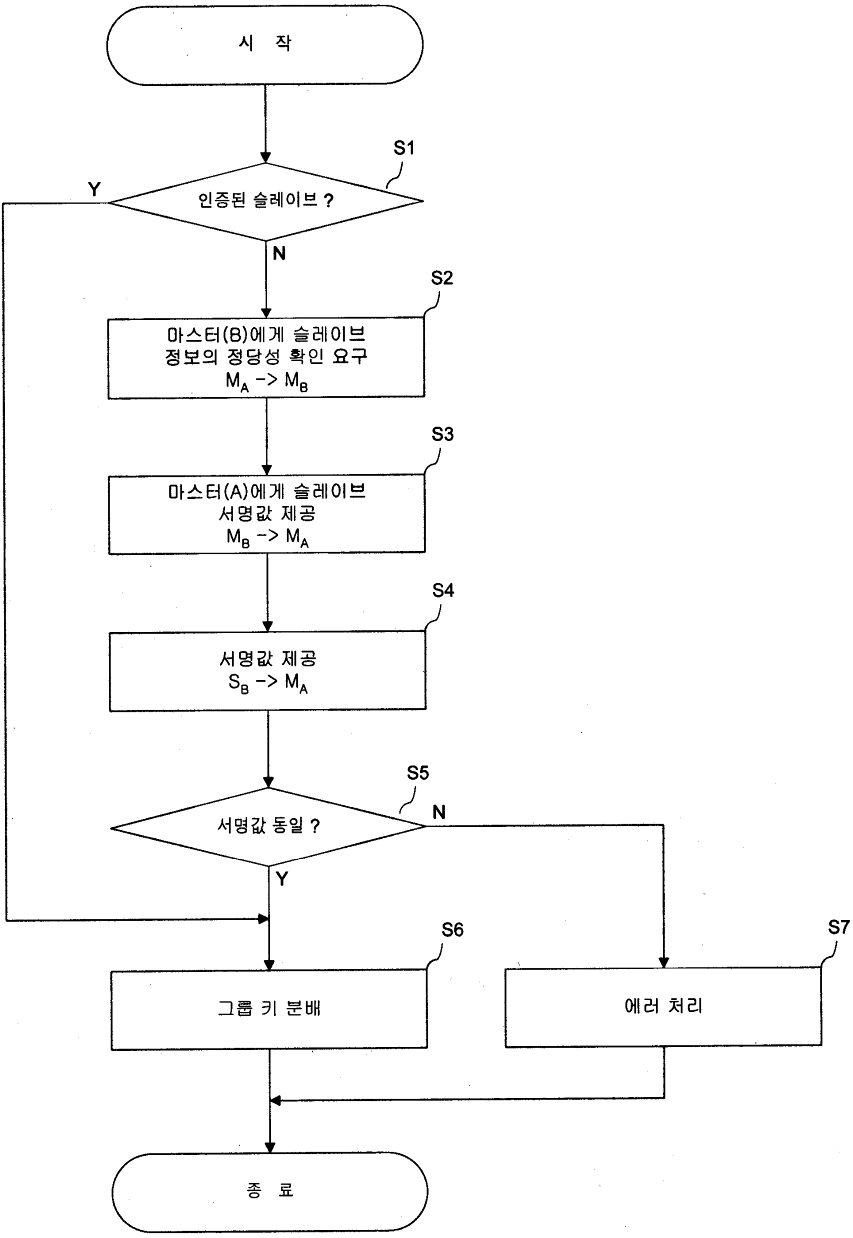
슬레이브로부터 접속요구가 있을 때의 안전한 네트워크 유지방법에 있어서;
접속을 요구한 슬레이브의 인증 여부를 확인하는 과정과,
비인증 피코넷으로부터의 접속인 경우 해당 피코넷의 마스터에게 접속요구 슬레이브 정보의 정당성 확인을 요구하는 과정과,
해당 피코넷의 마스터로부터 접속요구 슬레이브의 서명값을 수신받는 과정과,
접속요구 슬레이브로부터 서명값을 제공받는 과정과,
해당 피코넷의 마스터로부터 제공받은 서명값과 접속요구 슬레이브로부터 제공받은 서명값의 일치여부를 확인하는 과정과,
서명값이 일치하거나 인증된 슬레이브의 접속요구인 경우 그룹키를 분배하는 과정을 포함하여 이루어지는 타원곡선 암호알고리즘을 이용한 안전한 네트워크 유지방법.

도면

도면1


시 작
A-1
ECC 기반으로 한 비밀키 생성
A-2
마스터 정보 연접 / 해쉬 값 추출
A-3
암호화하여 슬레이브에게 전송
B-1
ECC 기반으로 한 비밀키 생성
B-2
슬레이브 정보 연접 / 해쉬 값 추출
B-3
암호화하여 마스터에게 전송
슬레이브 정보/세션키 재생성 요구
N
정 상 ?
Y
C-1
임의의 키쌍 및 서명값 생성
C-2
해쉬 값 계산
C-3
세션키로 암호화/슬레이브에게 전송
D-1
임의의 키쌍 및 서명값 생성
D-2
해쉬 값 계산
D-3
세션키로 암호화/마스터에게 전송
개인서명 키 / 그룹 키 재생성 요구
N
정 상 ?
Y
E
검증 확인 메시지 전송
종 료

도면2


시 작
S1
인증된 슬레이브 ?
Y
N
S2
마스터(B)에게 슬레이브 정보의 정당성 확인 요구
M_A -> M_B
S3
마스터(A)에게 슬레이브 서명값 제공
M_B -> M_A
S4
서명값 제공
S_B -> M_A
S5
서명값 동일 ?
N
Y
S6
그룹 키 분배
S7
에러 처리
종 료