(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
H04Q 7/20

(11) 공개번호 특2000-0017574
(43) 공개일자 2000년03월25일

(21) 출원번호 10-1999-0035781
(22) 출원일자 1999년08월27일

(30) 우선권주장 9/141,582 1998년08월28일 미국(US)
(71) 출원인 루센트 테크놀러지스 인크
미합중국 뉴저지 머레이 힐 마운틴 애비뉴 600 (우편번호 : 07974-0636)
(72) 발명자 파텔사바
미국뉴저지주07045몬트빌밀러레인34
(74) 대리인 김창세, 장성구

심사청구 : 없음

(54) 이동국 및 네트워크에서의 임시 이동국 식별자 설정 방법

요약

이동국 익명(anonymity) 보호 방법에 있어서, 네트워크는 챌린지와 함께 이동국에 임시 이동국 식별자(temporary mobile identifier: TID) 갱신 요구를 전송한다. 이에 응답하여 이동국은 네트워크의 공개키를 사용한 공개 키 암호화를 통해 그에 대한 고정 ID를 암호화하여 암호화 결과를 네트워크에 전송한다. 또한 이동국은 제 2 챌린지와 제 1 챌린지 응답을 생성한다. 키를 사용하여 제 1 챌린지와 제 2 챌린지에 대해 키 암호화 기능(keyed cryptographic function: KCF)을 수행함으로써, 제 1 챌린지 응답이 생성된다. 이동국은 제 2 챌린지와 제 1 챌린지 응답을 암호화된 고정 ID와 함께 네트워크로 전송한다. 고정 ID를 해독한 후, 네트워크는 고정 ID를 이용하여 이동국과 관련된 키를 액세스한다. 그 후, 키를 사용하여, 네트워크는 제 2 챌린지 및 제 1 챌린지 응답을 사용하여 이동국을 인증한다. 인증되면, 네트워크는 제 1 및 제 2 챌린지를 이용하여 이동국에 대한 TID를 계산한다. 네트워크는 또한 제 2 챌린지 응답을 생성하여 이동국으로 전송한다. 이동국이 제 2 챌린지 응답에 기반하여 네트워크를 인증하면, 이동국은 네트워크가 했던 것과 마찬가지 방식으로 TID를 계산한다.

대표도

도2

명세서

도면의 간단한 설명

도 1은 통상적인 무선 시스템을 도시한 도면,

도 2는 본 발명의 방법에 따른 이동국에 대한 TID를 설정하기 위한 이동국과 네트워크간의 통신을 도시한 도면,

도 3은 본 발명의 방법에 따라 네트워크의 공개키(public key)를 갱신하기 위한 이동국과 네트워크간의 통신을 도시한 도면.

도면의 주요 부분에 대한 부호의 설명

10 : AC/HLR(인증 센터/홈 위치 등록기)

15 : VLR(방문 위치 등록기)

20 : 이동국

관련 출원

1998년 7월 31일에 출원된 하기의 출원, 즉, 표제 출원의 발명자에 의한 "METHOD FOR TWO PARTY AUTHENTICATION AND KEY AGREEMENT"라는 명칭의 출원(출원 번호는 미공지)과, 표제 출원의 발명자에 의한 "METHOD FOR UPDATING SECRET SHARED DATA IN A WIRELESS COMMUNICATION SYSTEM"라는 명칭의 출원(출원 번호는 미공지)과, 표제 출원의 발명자에 의한 "METHOD FOR TRANSFERRING SENSITIVE INFORMATION USING INITIALLY UNSECURED COMMUNICATION"라는 명칭의 출원(출원 번호는 미공지)과, 표제 출원의 발명자에 의한 "METHOD FOR SECURING OVER-THE-AIR COMMUNICATION IN A WIRELESS SYSTEM"라는 명칭의 출원(출원 번호는 미공지)과, 표제 출원의 발명자와 아담 베렌츠바이그(Adam Berenzweig)에 의한 "METHOD FOR ESTABLISHING A KEY USING OVER-THE-AIR COMMUNICATION AND PASSWORD PROTOCOL AND PASSWORD PROTOCOL"라는 명칭의 출원(출원 번호는 미공지)은 표제 출원과 관련된 것으로, 이들 출원은 본 명세서에 전체적

으로 참조로서 인용된다.

표제 출원과 동시에 출원된 하기 출원, 즉, 표제 출원의 발명자에 의한 "METHOD FOR DETERMINING TEMPORARY MOBILE IDENTIFIERS AND MANAGING USE THEREOF"라는 명칭의 출원(출원 번호는 미공지)과 표제 출원의 발명자에 의한 "METHOD FOR ESTABLISHING SESSION KEY AGREEMENT"라는 명칭의 출원(출원 번호는 미공지)은 표제 출원과 관련된 것으로 이들 출원은 본 명세서에 전체적으로 참조로서 인용된다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 전반적으로 무선 시스템에서 이동국 익명성(anonynity)을 보호하는 방법에 관한 것으로, 보다 상세하게는 네트워트가 이동국의 임시 이동국 식별자(temporary mobile identifier: TID)를 인식하는 데 실패한 경우에 TID를 설정하는 방법에 관한 것이다.

현재, 미국에서는 상이한 표준을 갖는 세 개의 주요 무선 시스템을 이용하고 있다. 첫 번째 시스템은 시분할 다원 접속(TDMA) 시스템으로서 IS-136 표준안에 따라 운영되며, 두 번째 시스템은 코드 분할 다원 접속(CDMA) 시스템으로서 IS-95 표준안에 따라 운영되고, 세 번째 시스템은 고 수준 이동 전화 시스템(AMPS)이다. 이들 세 개의 통신 시스템 모두는 시스템간 메시지 통신(intersystem messaging)을 위해, 호 발신, 비밀 공유 데이터(secret shared data) 갱신 등에 대한 인증 절차를 규정하는 IS-41 표준안을 이용한다.

도 1은 인증 센터(authentication center: AC) 및 홈 위치 등록기(home location registor: HLR)(10), 방문자 위치 등록기(visiting location registor: VLR)(15), 이동국(20)을 포함하는 무선 시스템을 도시한다. 두개 이상의 HLR이 하나의 AC와 연계될 수 있지만, 현재는 1:1로 통신이 행해진다. 이에 따라, 도 1에서 HLR과 AC는 분리된 것이지만 단일체로서 나타낸다. 더욱이, 이하의 명세서에서는 설명의 편의상 HLR과 AC를 함께 AC/HLR로서 지칭한다. 또한, VLR은 그와 연관된 다수의 이동 교환국(mobile switching center: MSC) 중의 하나에 정보를 전송하며, 각 MSC는 그 정보를 다수의 기지국(base station: BS) 중의 하나에 전송하여 이동국으로 전송되도록 한다. VLR, MSC, BS는 편의상 VLR이라 지칭하여 도시할 것이다. 네트워크 공급자에 의해 동작되는 AC, HLR, VLR, MSC, BS는 총괄하여 네트워크라 지칭된다.

A키로서 알려진 루트 키(root key)는 AC/HLR(10)과 이동국(20)에만 저장된다. 공유 비밀 데이터(SSD)로서 알려진 보조키는 이동국 로밍(mobile roam)(즉, 이동국이 자신의 본래의 서비스 영역밖에 있는 경우)으로서 VLR(15)에 전송된다. SSD는 암호화 알고리즘이나 기능을 사용하여 A 키 및 랜덤 시드(random seed) RANDSSD로부터 생성된다. 암호화 기능은 가능한 입력 범위에 기반하여 소정 개수의 비트를 갖는 출력을 발생하는 기능이다. 키 암호화 기능(keyed cryptographic function: KCF)은 키에 기초하여 동작하는 암호화 기능의 유형으로서, 예를 들어, 두 개 이상의 인수(argument)(즉, 입력)에 대해 동작하는 암호화 기능인데, 여기서 인수 중의 하나가 키이다. 사용 중인 KCF의 출력과 지식으로부터는, 키가 알려져 있지 않는 한 입력을 결정할 수 없다. 암호화 기능의 유형으로는 암호/해독 알고리즘이 있다. 이들은 의사 랜덤 기능(pseudo random function: PRF)과 메시지 인증 코드(message authentication code: MAC)와 같은 일 방향성 기능이다. $KCF_{SK}(R_N')$의 표현은 세션 키(SK)를 키로서 사용하는 난수 R_N'의 KCF를 나타낸다. 세션 키는 어떤 세션 동안 존속되는 키이며, 세션은 호의 길이와 같은 소정 시간 간격이다. IS-41 프로토콜에 사용된 암호화 기능은 CAVE(Cellular Authentication and Voice Encryption)이다.

호 발신, 등록, 비밀 공유 데이터 갱신 등과 같은 절차 동안에, 사용자 신원 정보는 그 통신의 일부로서 이동국으로부터 네트워크로 전송된다. 사용자 신원 정보로는, 예를 들어, 이동국 식별 번호(mobile identification number: MIN) 및/또는 전자 일련 번호(electronic serial number: ESN)가 있다. 설명의 편의상, 고정(permanent) ID가 이동국 신원 정보의 하나 이상의 요소를 처리하는 데에 사용될 것이다. 그러나, 고정 ID를 사용하면, 침입자가 이동국을 비롯하여 이동국 사용자의 신원을 확인하여 추적할 수 있다. 많은 이동국 사용자는 이것이 바람직하지 않다고 생각하고 있다.

이동국의 익명을 보존하고 프라이버시를 보호하는 하나의 기법은 별명이나 임시 ID (TID)를 사용하는 것이다. 이 TID를 사용하여 적당한 때에 통신이 이루어진다. 그러나, 단순히 익명을 사용하는 것은, 침입자가 이동국이 진짜이거나 고정인 ID인지를 드러내게 하는 상황을 시뮬레이션 하도록 할 수 있다는 점에서 효과적이지 못하다.

전형적으로, 네트워크는 이미 TID를 갱신시켰지만 이동국이 갱신된 TID를 확인하지 못하여 이전의 TID에 의존하도록, 침입은 이동국과 네트워크간의 통신의 일부를 차단시킨다. 비동기 갱신으로 인해, 네트워크는 이동국을 인식하지 못하고 이동국은 통신을 재 구축하기 위해서 자신의 고정 ID를 사용한다. 네트워크가 폭주하면 네트워크가 이동국의 TID를 인식하는 데 실패하는 또다른 상황이 발생한다. 결론적으로, 침입자는 네트워크 폭주를 시뮬레이션하여 이동국이 자신의 고정 ID를 드러내도록 강제할 수도 있다.

발명이 이루고자하는 기술적 과제

본 발명에 따른 이동국 익명 보호 방법에 있어서, 이동국 공개키는 그 고정 ID를 암호화하고 네트워크로부터의 TID 갱신 요구 신호에 응답하여 네트워크에 암호화된 고정 ID를 전송한다. 이동국은 TID 갱신 요구와 함께 또한 제 1 챌린지(challenge)를 수신하고 키를 사용하여 제 1 챌린지와 이동국이 생성한 제 2 챌린지에 대해 키 암호화 기능을 수행함으로써 그에 대한 제 1 챌린지 응답을 생성한다. 제 1 챌린지

응답과 제 2 챌린지는 네트워크로 전송된다. 이동국의 고정 ID를 해독함으로써, 네트워크는 제 1 챌린지 응답을 생성하고 이동국을 인증한 키를 액세스할 수 있다.

일단 이동국이 인증되면, 네트워크는 제 1 및 제 2 챌린지에 기반하여 이동국에 대한 TID를 계산한다. 네트워크는 또한 제 2 챌린지에 기반하여 제 2 챌린지 응답을 생성하여 제 2 챌린지 응답을 이동국으로 전송한다. 이동국은 제 2 챌린지 응답에 기반하여 네트워크를 인증한다. 일단 네트워크가 인증되면, 이동국은 네트워크가 했던 것과 마찬가지 방식으로 제 1 및 제 2 챌린지에 기반하여 TID를 계산한다. 이러한 과정의 일부로서 네트워크는 또한 신규 공개키를 이동국에 전달할 수도 있다.

이동국의 고정 ID가 공개 키 암호화를 통해 네트워크에 전달되기 때문에, 이동국의 고정 ID는 침입으로부터 보호된다. 따라서, 침입의 결과에 의한 것이든 시스템 에러의 결과에 의한 것이든, 네트워크가 이동국의 TID를 인식하는 데 실패하면 이동국의 고정 ID는 드러나지 않을 것이다.

발명의 구성 및 작용

본 발명은 단지 예시적인 것으로 주어진 다음의 상세한 설명과 첨부 도면으로부터 보다 충분히 이해될 것이며, 각 도면에서 대응하는 부분은 같은 참조 부호로서 표현된다.

본 발명에 따른 임시 이동국 식별자(temporary mobile identifier: TID)를 설정하는 방법이 도 1의 무선 시스템을 참조하여 설명될 것이다. 본 발명에 따른 방법은 이동국(20)의 고정 ID를 네트워크에 전달하는 것을 포함하지만, 이 노출은 공개 키 암호화를 사용하여 보호된다.

공개 키 암호화가 비대칭 암호화인 반면, 비밀 키 암호화는, 예를 들면, 대칭 암호화이다. 대칭 암호화에 있어서, 암호화 알고리즘 및 비밀키에 대한 지식을 통해 해독이 가능하다. 이와 대조적으로, 공개 키 암호화에 있어서는, 암호화 알고리즘 및 공개키에 대한 지식을 갖고 있더라도 해독이 불가능하다. 이 대신에, 공개 키 암호화를 사용하여 암호화된 정보를 해독하기 위해서는 공개키에 관련된 해독키를 반드시 알고 있어야 한다. 따라서, 본 발명에 따른 방법에 있어서는, 이동국(20)에 관련된 AC/HLR(10)만이 공개키와 관련된 해독키의 지식을 저장하여 갖고 있다.

A키뿐만 아니라, AC/HLR(10)과 이동국(20)은 A키에 기반하여 생성된 M키와 T키로 지칭되는 보조키를 저장한다. M키와 T키는 네트워크 및 이동국(20)에 대해 알려진 값에 A키에 의해 인덱싱된 의사 랜덤 기능(pseudo random function: PRF)을 가함으로써 생성된다. 실제의 잘 알려진 PRF로서는 국가 표준청(national institute of standards: NIST)에 의한 데이터 암호화 표준 씨퍼 블럭 체인(data encryption standard-chipher block chaining: DES-CBC) 알고리즘이 있다. 바람직한 실시예에 있어서, 제 1 알려진 값에 대해 64 비트 A키에 의해 인덱싱되는 DES-CBC가 64 비트의 M키를 생성하고, 제 2 알려진 값에 대해 64 비트 A키에 의해 인덱싱되는 DES-CBC가 64 비트의 T키를 생성한다.

도 2를 참조하여, 본 발명에 따른 TID 설정 방법을 설명한다. 도시된 바와 같이, VLR(15)은 AC/HLR(10)과 이동국(20) 사이의 통신에 대한 통로로서 기능한다. 더 구체적으로는, 본 발명에 따른 TID 설정 방법은 AC와 이동국(20) 사이에서 수행된다. 이동국(20)이 시스템 액세스를 시도한다고 가정하자. 네트워크가 폭주하거나 동기 이탈(out-of-synch)이 존재하는 경우와 같이 이동국(20)이 시스템 액세스를 시도하고 AC/HLR(10)이 시스템 액세스에 내장된 TID를 인식하는 데 실패한 경우, AC/HLR(10)은 시스템 액세스를 처리하지 않는다. 대신에, AC/HLR(10)은 난수(R_N)를 챌린지로서 생성하여 TID 갱신 요구 및 난수(R_N)를 이동국(20)으로 전송한다. 식별을 용이하게 하기 위해, 네트워크에 의해 챌린지로서 생성된 난수는 R_N으로 지칭하는 반면, 이동국(20)에 의해 챌린지로서 생성된 난수는 R_M으로 지칭한다.

TID 갱신 요구에 응답하여, 이동국(20)은 난수(r)를 생성하고 공개키는 네트워크의 공개 키(PK)를 사용하여 이동국(20)에 대한 고정 ID 및 난수(r)를 암호화한다. 이 암호화는 ENC_{PK}(ID, r)로서 표현된다. 바람직하게 사용되는 암호화 알고리즘(ENC)은 라빈(Rabin) 알고리즘 또는 낮은 지수 제곱의 RSA 알고리즘과 같은 고속 공개 키 암호화 알고리즘인데, 다른 임의의 키 암호화 알고리즘도 사용될 수 있다. 난수(r)는 공개키와 함께 암호화되어 암호화 결과가 각 챌린지에 대해 상이할 것이다. 그렇지 않으면 침입자가 암호화 결과를 사용하여 공격을 개시할 수 있다. 난수(r)로 공개키를 암호화하는 것은 일종의 개연성 암호화의 형태이다. 당업자는 전술한 형태의 개연성 암호화 대신에 다른 형태의 개연성 암호화도 이용할 수 있음을 인식할 것이다.

이동국(20)은 또한 그 안에 내장된 난수 생성기를 이용하여 난수(R_M)를 생성하며, 챌린지 응답을 획득하기 위한 키로서 M키를 사용하여 난수(R_N 및 R_M), 유형(Type) 데이터, id 데이터(0)에 대한 키 암호화 알고리즘 또는 기능(KCF)을 수행한다. 이 계산 결과는 $KCF_{M\text{-}Key}$(Type, 0, R_M, R_N)로 표현된다. KCF는 바람직하게는 HMAC와 같은 키 메시지 인증 코드이지만 DEC-CBC와 같은 PRF일 수도 있다. 유형 데이터는 수행되고 있는 프로토콜의 유형, 즉 TID 갱신 프로토콜을 나타낸다. 다른 프로토콜 유형은 호 발신, 호 착신, 이동국 등록을 포함한다. id 데이터 0은 통신이 이동국으로부터 발생했음을 표시한다. 이와 대조적으로, id 데이터 1은 통신이 네트워크로부터 온 것임을 표시한다. 이동국(20)은 이어서 난수(r), 암호화 결과(ENC_{PK}(ID, r)), 난수(R_M), $KCF_{M\text{-}Key}$(Type, 0, R_N, R_M)의 챌린지 응답을 AC/HLR(10)에 전송한다.

AC/HLR(10)은 이동국(20)의 고정 ID를 획득하기 위해 네트워크의 공개키와 관련된 해독키와 난수(r)를 이용하여 암호화 결과를 해독한다. AC/HLR(10)은 그에 관련된 이동국에 대한 고정 ID를 사전 저장하고 TID, A키, 보조 키, 기타 각 이동국에 대한 정보를 고정 ID와 관련시킨다. 따라서, AC/HLR(10)이 이동국(20)의 고정 ID를 수신한 경우, AC/HLR(10)은 예를 들어 이동국(20)에 대한 보조키를 안다.

AC/HLR(10)이 TID 갱신 프로토콜을 TID 갱신 요구로서 개시했기 때문에, AC/HLR(10)은 유형 데이터를 알며, 이동국으로부터의 통신이 동일한 id 데이터 0을 포함하기 때문에 이 값도 또한 안다. 따라서, AC/HLR(10)은 수신된 난수(R_M)를 사용하여 $KCF_{M\text{-}Key}$(Type, 0, R_M, R_N)를 계산한다. 이어서 AC/HLR(10)은

KCF_{M-Key}(Type, 0, R_M, R_N)의 계산된 버전이 이동국(20)으로부터 수신된 버전과 정합되는 지의 여부를 검증한다. 정합이 발견되면, AC/HLR(10)은 이동국(20)을 인증한다. 일단 이동국(20)이 인증되면, AC/HLR(10)은 신규 TID를 PRF_{T-KEY}(R_M, R_N)로서 계산하는데, PRF는 바람직하게는 DEC-CBC이다. 그 후, AC/HLR(10)는 KCF_{M-Key}(Type, 1, R_M)를 챌린지 응답으로서 계산하여 계산된 챌린지 응답을 이동국(20)으로 전송하는데, 1은 네트워크의 id 데이터이다.

이동국(20)은 TID 갱신 요구로부터 유형 데이터를 알며, 네트워크로부터의 통신이 id 데이터 1을 포함한다는 것을 안다. 따라서, 이동국(20)은 KCF_{M-Key}(Type, 1, R_M)를 계산한다. 이어서 이동국(20)은 KCF_{M-Key}(Type, 1, R_M)의 계산된 버전이 AC/HLR(10)로부터 수신된 버전과 정합되는 지의 여부를 검증한다. 정합이 발견되면, 이동국(20)은 네트워크를 인증한다. 일단 네트워크가 인증되고 나면, AC/HLR(10)은 AC/HLR(10)이 했던 것과 마찬가지 방식으로 신규 TID를 PRF_{T-KEY}(R_M, R_N)로서 계산한다.

이동국(20)의 고정 ID가 개연성 공개 키 암호화를 통해 네트워크에 전달되기 때문에, 이동국(20)의 고정 ID는 침입으로부터 보호된다. 따라서, 침입의 결과에 의한 것이든 시스템 에러의 결과에 의한 것이든, 네트워크가 이동국의 TID를 인식하는 데 실패하면 이동국의 고정 ID는 드러나지 않을 것이다.

또다른 구체적인 예로서, 네트워크가 이동국의 TID를 인식하는 데 실패한 경우 본 발명에 따른 TID 설정 방법을 수행하는 대신에, 이동국에 의한 각 시스템 액세스를 위한 방법이 수행될 수도 있다. 이런 식으로 TID를 계속 갱신함으로써, 침입의 개시가 더욱 어렵게 된다.

본 발명에 따른 TID 설정 방법을 기술함에 있어서, 이동국(20)이 네트워크의 공개키를 사전에 획득했다고 가정한다. 예를 들면, 이동국(20)은 공개키를 서비스 제공의 일부로 획득했을 수도 있다. 이동국(20)이 주어진 네트워크를 통해 통신하도록 설정된 경우(즉 서비스 제공), A키 및 다른 정보가 이동국(20) 내에, 전형적으로는 네트워크 제공자의 업무 공간에서, 프로그램된다. 이 과정 중에, 네트워크의 공개키가 이동국(20)에 주어진다.

이와 달리, 공중 서비스 제공(over air service provisioning: OTASP)으로서 지칭되는 공중 용 이동국을 제공하고 민감한 정보를 공중을 통해 안전하게 전달하기 위한 기법도 또한 구현했다. 예를 들면, IS-41 프로토콜은 OTASP 프로토콜을 제공한다. 이들 기법의 어느 것도 네트워크의 공개키를 이동국(20)에 제공하는 데 이용될 수 있다. 앞서 언급한 관련 참조 출원의 하나로서 본 명세서에서 전체적으로 참조로서 인용되는 것에 기술된 민감성 정보의 전달을 위한 기법은 바람직하게는 네트워크의 공개키를 이동국(20)에 제공하는 데 사용된다.

네트워크 서비스 제공자는 또한 공개키를 주기적으로 갱신하는 것을 원할 수도 있다. 도 3은 본 발명에 따른 TID의 설정에 사용된 공개키의 갱신 방법을 도시한다. 도시된 바와 같이, AC/HLR(10)은 난수(R_N)를 챌린지로서 생성하여 난수(R_N) 및 신규 공개 키(PK)를 이동국(20)에 전송한다.

이에 응답하여, 이동국(20)은 난수(R_M)를 생성하며, 챌린지 응답을 획득하기 위한 키로서 M키를 사용하여 난수(R_N 및 R_M), 유형(Type) 데이터, id 데이터(0), 공개 키(PK)에 대한 KCF를 수행한다. 이 계산 결과는 KCF_{M-Key}(Type, 0, R_M, R_N, PK)로 표현된다. KCF는 바람직하게는 HMAC와 같은 키 메시지 인증 코드이지만, DEC-CBC와 같은 PRF일 수도 있다. 이동국(20)은 이어서 난수(R_M)와 KCF_{M-Key}(Type, 0, R_N, R_M, PK)의 챌린지 응답을 AC/HLR(10)에 전송한다.

AC/HLR(10)은 수신된 난수(R_M)를 사용하여 KCF_{M-Key}(Type, 0, R_M, R_N, PK)를 계산한다. 이어서 AC/HLR(10)은 KCF_{M-Key}(Type, 0, R_N, R_M, PK)의 계산된 버전이 이동국(20)으로부터 수신된 버전과 정합되는 지의 여부를 검증한다. 정합이 발견되면, AC/HLR(10)은 이동국(20)을 인증한다. AC/HLR(10)이 이동국(20)을 인증할 수 없으면, AC/HLR(10)은 공개 키 갱신 프로토콜을 다시 시작한다.

그 후, AC/HLR(10)는 KCF_{M-Key}(Type, 1, R_M)를 챌린지 응답으로서 계산하여 계산된 챌린지 응답을 이동국(20)으로 전송하는데, 1은 네트워크의 id 데이터이다.

이동국(20)은 또한 KCF_{M-Key}(Type, 1, R_M)을 계산한다. 이동국(20)은 KCF_{M-Key}(Type, 1, R_M)의 계산된 버전이 AC/HLR(10)로부터 수신된 버전과 정합되는 지의 여부를 검증한다. 정합이 발견되면, 이동국(20)은 네트워크를 인증한다. 이동국(20)이 네트워크를 인증하면, 이동국(20)은 네트워크에 대한 공개키를 신규 공개키로 갱신한다.

전술한 공개 키 갱신 프로토콜은 도 2에 대해 서술된 TID 갱신 프로토콜의 일부로서 수행될 수도 있다. 예를 들어, 신규 공개키는 AC/HLR(10)에 의해 TID 갱신 요구와 함께 전송되며 신규 공개키는 이동국(20)에 의해 고정 ID를 암호화하는데 사용된다. 또한, 이동국(20)에 의해 생성된 챌린지 응답은 신규 공개키를 인수로서 포함한다.

공개 키 갱신 프로토콜은 또한 SSD 갱신 프로토콜과 같은 다른 갱신 프로토콜의 일부로서 수행될 수도 있다.

이상에서 본 발명에 대해서 설명하였는데, 다양한 방식으로 변경될 수 있음은 자명할 것이다. 그러한 변경은 본 발명의 사상과 범주를 벗어나지 않는 것으로 간주되어야 하며, 그러한 모든 변형은 첨부한 특허 청구 범위 내에 포함되는 것으로 고려되어야 한다.

발명의 효과

따라서, 본 발명에 따르면, 이동국과 방문 위치 등록기 모두가 갖고 있는 TID 리스트를 사용 중인 TID가

확인될 때마다 갱신함으로써, 이동국 자신의 ID가 침입자에게 노출되는 것을 방지할 수 있다.

(57) 청구의 범위

청구항 1

이동국에서의 임시 이동국 식별자(temporary mobile identifier: TID)를 설정하는 방법에 있어서,

① 제 1 코드를 수신하는 단계와,

② 제 2 코드를 생성하는 단계와,

③ 네트워크의 공개키를 이용하여 상기 이동국에 대한 고정 ID를 암호화하는 공개 키 암호화 단계와,

④ 상기 제 2 코드 및 상기 암호화된 고정 ID를 상기 네트워크에 전송하는 단계와,

⑤ 상기 제 1 코드에 기반하여 TID를 설정하는 단계를 포함하는

이동국에서의 임시 이동국 식별자 설정 방법.

청구항 2

제 1 항에 있어서,

상기 단계 ①이 상기 네트워크로부터 상기 제 1 코드 및 TID 갱신 요구를 수신하며,

상기 단계 ④ 및 ⑤가 상기 TID 갱신 요구에 응답하여 수행되는

이동국에서의 임시 이동국 식별자 설정 방법.

청구항 3

제 1 항에 있어서,

상기 제 1 코드가 챌린지(challenge)이며,

상기 단계 ②가 키를 사용하여 상기 제 1 코드에 대해 키 암호화 기능을 수행함으로써 상기 제 2 코드를 챌린지 응답으로서 생성하는

이동국에서의 임시 이동국 식별자 설정 방법.

청구항 4

제 1 항에 있어서,

상기 제 1 코드가 챌린지이며,

상기 단계 ②가 상기 키를 사용하여 상기 제 1 코드 및 유형 데이터에 대해 키 암호화 기능을 수행함으로써 상기 제 2 코드를 챌린지 응답으로서 생성하되, 상기 유형 데이터가 상기 네트워크 및 상기 이동국에 의해 수행되고 있는 프로토콜의 유형을 나타내는

이동국에서의 임시 이동국 식별자 설정 방법.

청구항 5

제 1 항에 있어서,

⑥ 챌린지를 생성하는 단계를 더 포함하되,

상기 단계 ④가 상기 챌린지, 상기 제 2 코드, 상기 암호화된 고정 ID를 상기 네트워크에 전송하는

이동국에서의 임시 이동국 식별자 설정 방법.

청구항 6

제 5 항에 있어서,

⑦ 상기 네트워크로부터 챌린지 응답을 수신하는 단계와,

⑧ 상기 챌린지 응답에 기반하여 상기 네트워크를 인증하는 단계를 더 포함하되,

상기 단계 ⑧이 상기 네트워크를 인증할 경우 상기 단계 ⑤가 상기 TID를 설정하는

이동국에서의 임시 이동국 식별자 설정 방법.

청구항 7

제 5 항에 있어서,

상기 단계 ⑤가 상기 챌린지 및 상기 제 1 코드에 기반하여 상기 TID를 설정하는

이동국에서의 임시 이동국 식별자 설정 방법.

청구항 8

제 1 항에 있어서,

상기 단계 ①이 상기 네트워크로부터 상기 제 1 코드 및 상기 공개키를 수신하는

이동국에서의 임시 이동국 식별자 설정 방법.

청구항 9

제 8 항에 있어서,

상기 단계 ②가 키를 사용하여 상기 제 1 코드 및 상기 공개키에 대해 키 암호화 기능을 수행함으로써 상기 제 2 코드를 생성하는

이동국에서의 임시 이동국 식별자 설정 방법.

청구항 10

네트 워크에서의 임시 이동국 식별자(temporary mobile identifier: TID) 설정하는 방법에 있어서,

① 이동국으로부터 제 1, 제 2, 제 3 코드를 수신하는 단계 - 상기 제 3 코드가 상기 네트워크의 공개키를 사용하여 상기 이동국에 대한 고정 ID의 공개 키 암호화임 -와,

② 상기 제 3 코드를 해독하여 상기 이동국에 대한 상기 고정 ID를 획득하는 단계와,

③ 상기 이동국에 대한 상기 해독된 고정 ID에 기반하여 상기 이동국과 관계되고 상기 네트워크에 의해 저장되어 있는 키를 액세스하는 단계와,

④ 상기 키 및 상기 제 2 코드에 기반하여 상기 이동국을 인증하는 단계와,

⑤ 상기 이동국이 인증되면 상기 제 1 코드에 기반하여 상기 이동국에 대한 TID를 설정하는 단계를 포함하는

네트워크에서의 TID 설정 방법.

청구항 11

제 10 항에 있어서,

⑥ 제 1 챌린지를 상기 이동국에 전송하는 단계를 더 포함하되,

상기 단계 ①이 상기 제 1 챌린지에 대한 챌린지 응답을 상기 제 2 코드로서 수신하는

네트워크에서의 TID 설정 방법.

청구항 12

제 11 항에 있어서,

상기 단계 ①이 상기 제 2 챌린지를 상기 제 1 코드로서 수신하는

네트워크에서의 TID 설정 방법.

청구항 13

제 12 항에 있어서,

상기 단계 ⑤가 상기 제 1 및 제 2 챌린지에 기반하여 상기 TID를 설정하는 네트워크에서의 TID 설정 방법.

청구항 14

제 11 항에 있어서,

상기 챌린지 응답이 키를 이용하여 상기 제 1 코드 및 상기 제 1 챌린지에 대해 키 암호화 기능을 수행한 결과인

네트워크에서의 TID 설정 방법.

청구항 15

제 11 항에 있어서,

상기 챌린지 응답이 키를 이용하여 상기 제 1 코드 및 유형 데이터에 대해 키 암호화 기능을 수행한 결과이되, 상기 유형 데이터가 상기 네트워크 및 상기 이동국에 의해 수행되고 있는 프로토콜의 유형을 나타내는

네트워크에서의 TID 설정 방법.

청구항 16

제 11 항에 있어서,

상기 단계 ⑥이 상기 네트워크 및 상기 챌린지에 대한 신규 공개키를 상기 이동국에 전송하는

네트워크에서의 TID 설정 방법.

청구항 17

제 16 항에 있어서,

상기 챌린지 응답이 키를 이용하여 상기 제 1 코드 및 상기 신규 공개키에 대해 키 암호화 기능을 수행한 결과인

네트워크에서의 TID 설정 방법.

청구항 18

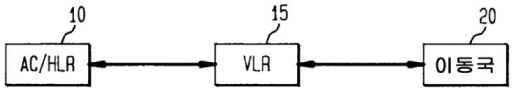
제 11 항에 있어서,

상기 단계 ⑥이 TID 갱신 요구 및 상기 챌린지를 전송하는

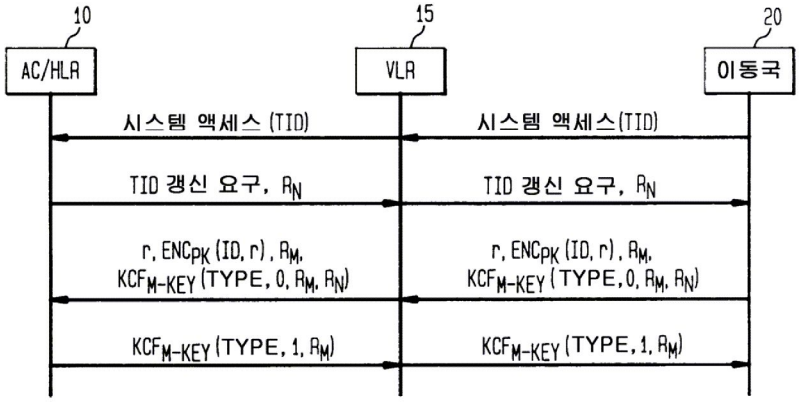
네트워크에서의 TID 설정 방법.

도면

도면1



도면2



도면3

