論文 98-23-5-12

CDPD 무선 데이터 통신 시스템의 인증 프로토콜과 가입자 익명성

正會員 이 수 연*, 안 효 범**, 이 동 훈***, 박 창 섭****

Authentication Protocol and Subscriber Anonymity for CDPD Wireless Data Communication System

Suyoun Lee*, Hyobeom Ahn**, Donghoon Lee***, Changseop Park**** *Regular Members*

요 약

본 논문에서는 CDPD 무선 데이터 통신 시스템의 가입자 인증 프로토콜의 문제점을 분석하고 이에 대한 개선 방향을 제시한다. 또한, 가입자 익명성과 관련하여 기존의 접근 방식인 홈 네트워크의 인증 서버에 의해 주도되는 새로운 가명의 생성 및 부여 메커니즘의 대안과 가명 동기화 상실에 따른 복구 방안을 제안한다.

ABSTRACT

We investigate here problems related to a subscriber authentication protocol in CDPD, and suggest an improved alternative. Associated with an anonymity of the subscriber, another method of generating and distributing alias is proposed other than the conventional approach initiated by an authentication server in his home network.

Ⅰ. CDPD 무선 데이터 통신 시스템 개요

CDPD(Cellular Digital Packet Data)[4]는 미국 내의 여러 기업들의 콘소시엄에 의해 무선 데이터 통신 서비스를 위해서 최근에 개발되었다. 명칭에 나타나 있는 것처럼 CDPD는 음성이 아니라 데이터의 전달을 지향하고 있다. CDPD는 데이터를 전송하기 위하여 셀룰라 음성 통신에서 사용되지 않는 유휴 채널을 이용해 데이터를 패킷의 형태로 전송하는 것이다. 무선 데이터 통신 서비스는 기존의 셀룰라 망을 이용하는 CDPD 방식, 보편적인 무선 통신망인 TRS(주파수 공용 통신) 네트워크를 이용하는 TRS 무선 데이터 통신 방식, 그리고 전용 무선 패킷 데이터 통신망을 이용한 방식으로 대별된다. 이 중에서 CDPD 방식은 기존의 이동 전화망을 이용하기 때문에 추가의 설비투자 없이도 비교적 쉽게 무선 데이터 서비스를 제공할 수 있다는 장점을 가지고 있다. 특히, CDPD 방식은 공

*천안외국어전문대 사무자동화과
**국립천안공업전문대 정보통신과
***고려대학교 전산학과
****단국대학교 전자계산학과
論文番號:98065-0216
接受日字:1998年 2月 16日

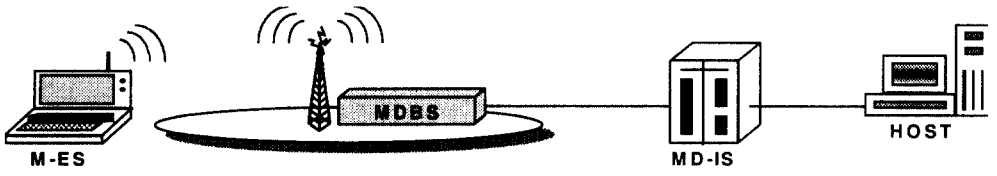

그림 1. CDPD 시스템의 주요 구성요소
Fig. 1 The Primary Components of CDPD system.

개된 표준을 사용하기 때문에 기본적으로 지금까지 유선 데이터 통신 분야에서 사용해 온 전통적인 통신 프로토콜인 TCP/IP나 프레임 릴레이 등을 그대로 무선 분야에 적용시킬 수가 있다. CDPD는 19,200 bps의 속도를 제공하는 변조 방식을 사용하고 또한, 채널 잡음에 따른 재전송(retransmission) 회수를 줄이기 위해 Reed-Solomon 부호를 기반으로 하는 전방 오류 수정(forward error correction) 방식을 채택하고 있다.

그림 1에서처럼 CDPD는 기존의 셀룰라 이동전화 기지국에 MDBS(Mobile DataBase Station)를 추가함으로써 부가적인 무선 데이터 통신 서비스를 이동 단말기 M-ES(Mobile End System)에게 제공할 수 있다. 여러 개의 MDBS는 네트워크 관리, 가입자 인증, 가입자 위치 서비스 및 암호화 기능을 수행하는 MD-IS (Mobile Data Intermediate System)의 제어를 받는다. 그림 2는 CDPD 네트워크 서비스가 제공되는 지역별 구분과 다른 네트워크와의 연동을 보여주고 있다. 한 개의 MDBS에 의해서 관할 되는 지역을 셀(cell)이라고 하고 한 개의 MD-IS가 여러 개의 셀을 관장하고 있다. 특히, MD-IS는 이동 단말기의 현재 위치 정보를 이용하여 라우팅 기능을 수행한다. 다른 사업자의 CDPD 네트워크나 또는 기존의 공중 데이터 네트워크(PDN : Public Data Network)와 인터네트와의 연동은 IS (Intermediate System)를 통해서 이루어 진다. 모든 이동 단말기는 최초에 서비스가 개시될 때 자기의 고유한 홈 네트워크(home network)에 등록된다. 자신의 홈 CDPD 네트워크와 로밍(roaming) 서비스가 협정된 다른 CDPD 네트워크에서도 서비스를 받을 수가 있는 데 이때, 그 네트워크를 방문 네트워크(visiting network)라고 한다.

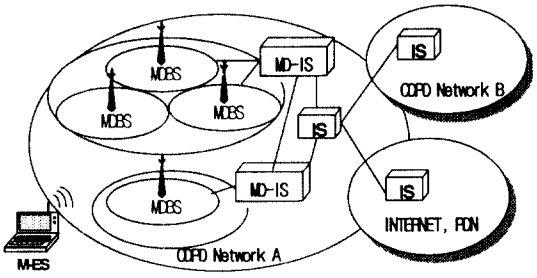

그림 2. CDPD 망의 구성
Fig. 2 Configuration of CDPD Network.

Ⅱ. 무선 데이터 통신 시스템 특성과 보안 서비스

무선 데이터 통신 시스템에 있어서 가입자의 이동성과 통신망에의 무선 접속이라는 특성은 보안적인 측면에서 제 3자에 의한 도청의 가능성 및 불법 접속, 그리고 가입자의 현재 위치와 행적의 노출 등의 문제점을 내포하고 있다. 무선 데이터 통신 시스템에서는 가입자와 무선 데이터 통신 네트워크간의 유선 접속 방식이 존재하지 않기 때문에 무선 접속 서비스의 불법적인 사용이 가능하다. 따라서, 가입자 신분 확인 또는 가입자 인증은 이러한 문제를 해결하기 위해 무선 데이터 통신 사업자가 제공해야 하는 필수적인 보안 기능이다. 최근, 안전한 무선통신 서비스를 제공하기 위하여 각국의 무선 데이터/이동통신 표준화 단체에서는 무선 이동통신 표준화에 인증 기능의 추가를 권고하고 있다. 우리나라의 통신기술협회[8]에서도 디지털 이동전화 무선 인터페이스 표준에 인증 기능을 권고하고 있다.

무선통신의 취약성 때문에 상업용 전파 스캐너를 이용하면 누구나 쉽게 다른 가입자의 통화 내용을 도청할 수가 있다. 이러한 가입자 정보에 대한 도청을 방지하기 위해서는 송수신되는 메시지에 대한 암호화가 요구되어 진다. 암호화를 수행하기 위해서는 송수신자 간에 사용할 공통된 세션 키의 공유가 선행되어져야 하는 데 이를 세션 키 분배라고 한다.

CDPD 무선 데이터 통신 시스템에서는 가입자의 현재 위치가 가입자의 홈 네트워크상의 MD-IS에 의해서 계속 추적되어 진다. 가입자의 단말기가 송신 또는 수신을 위해 켜진 상태에서는 단말기에서 방출되는 가입자의 신원 정보를 통해 가입자의 현재 위치가 네트워크 센터에 의해 등록 또는 갱신되어지고 이 위치 정보는 위치 디렉토리(location directory)라는 데이터베이스에 저장된다. 이러한 가입자의 현재 위치를 추적하는 것은 무선 데이터 통신 서비스를 가입자에게 제공하기 위한 필수적인 기능이지만 가입자의 위치 정보는 결국 가입자의 행적을 추적할 수가 있기 때문에 외부로 노출되어지는 것은 가입자의 프라이버시를 보호한다는 측면에서 바람직하지가 않다. 그러므로, 외부인에 의한 특정 가입자에 대한 추적을 불가능하게 하는 보안 서비스도 선택적으로 사업자가 수용하여야 할 것이다. 이러한 보안 서비스를 추적 불가능(untraceability) 또는 가입자 익명성(subscriber anonymity)이라고 한다. 공중 데이터 네트워크나 인터네트와 같은 고정 네트워크(fixed network)에서는 볼 수 없었던 다음과 같은 무선 데이터 통신 시스템 자체의 구조적인 그리고 운영상의 특성들이 무선 데이터 통신 시스템의 보안에 영향을 미치고 있다.

이동 단말기와 네트워크 센터간의 비대칭성

이동 단말기를 편리하게 휴대하기 위해서는 그 크기가 소형이어야 하고 또한, 다른 대안이 제시되기 전 까지는 배터리에 의해서 그 전원을 공급 받게 될 것이다. 제한된 배터리 용량 때문에 이동 단말기의 처리 속도나 프로세서 사이클은 감소되어야 한다. 이는 결국 적용되는 암호화 알고리즘의 계산 복잡도와 보안 프로토콜에 수반되는 메시지의 개수에 제약을 가하게 된다. 이러한, 이동 단말기와 네트워크 측의 비대칭성으로 인하여 기존의 분산 시스템하에서 적용되는 일반적인 보안 메커니즘의 직접적인 적용에는 어려움이 많다. 또한, 사용자의 보안 관련 데이터를 단말기 자체에 내장하는 것은 여러 가지 측면에서 안전하지 못하고 최근 불법으로 복제된 단말기의 사용이 급증함에 따라서 일반 대중의 신뢰성을 받지 못하고 있다. 따라서, CDPD 시스템에서는 비록 그 용량에는 한계가 있지만 물리적인 보안이 우수한 SIM (Subscriber Identity Module)이라는 스마트 카드에 그러한 정보를 보관하여 사용하는 것을 선택적으로 허용하고 있다.

무선 이동통신 망의 개방성

무선 데이터 통신 네트워크는 가입자에게 편리함을 제공하지만 반대로 불법적인 도청을 그만큼 용이하게 한다. 무선통신은 기본적으로 방송 통신을 기반으로 하기 때문에 셀 영역의 어디에서도 특정 이동 단말기와 기지국간의 무선통신을 감청할 수가 있다. 따라서, 무선 데이터 통신 네트워크는 인터네트와 같은 개방형 네트워크에서와 같이 물리적인 보안이 지원되지 않기 때문에 별도의 암호 기법을 도입하여 보호되어야 한다. 또한, 특정 서비스 지역을 방문한 이동 단말기들이 과도하게 통신을 시도함으로써 발생되는 네트워크 성능의 저하를 방지할 수가 없다. 이는 결국 네트워크의 혼잡에 따른 다른 이동 단말기에 대한 서비스 거부(denial of service)를 초래하게 된다.

빈번한 접속 해제

무선통신은 잡음(noise)과 간섭(interference)으로 인하여 그리고 통화 중의 셀간 이동 과정에서 종종 접속이 해제된다. 이러한 문제점은 최근 네트워크의 물리적인 계층에서 접속 해제를 최소화하는 방안과 네트워크의 상위 계층에서 접속 해제를 허용하는 방안들을 통해서 접근되어지고 있다. 특히, 이러한 갑작스러운 접속 해제는 제3자에 의해서 유용될 가능성을 내포하고 있다. 최근, TCP/IP 프로토콜 내에서의 인위적인 접속 해제와 이에 따른 불법 접속 공격의 가능성이 보고되고 있다.

핸드-오프

이동 단말기는 여러 셀간을 이동함에 따라서 주파수와 서비스 품질과 같은 서로 다른 물리적인 통신 프로토콜에 동조되어야 한다. 특히, 네트워크의 상위

계층으로 감에 따라서 보안관련 제약과 네트워크 관리 등이 서로 다른 서비스 네트워크를 통과함에 따라서 상이하게 된다. 이러한 현상은 특정 지역의 셀들이 서로 다른 사업자에 의해 운영되어질 경우에 더욱 빈번하게 일어나고 시스템의 관리를 더욱 복잡하게 만드는 요인이 된다. 최근 분산 시스템의 급격한 발전으로 인하여 이러한 복잡함이 어느 정도 해소되어 지고 있으나 이동통신에 있어서 매우 중요한 인증 서비스는 여전히 중앙 집중식으로 이루어 지고 있다.

주파수 대역과 오류 율

무선 망은 유선 망에 비해 전형적으로 낮은 주파수 대역과 높은 채널 오류 율(channel error rate)에 의해서 영향을 받고 결과적으로 무선 망을 통한 데이터의 전달은 고정 망에 비해 비용이 많이 든다. 따라서, 무선 망에 적용되는 보안 프로토콜은 메시지의 개수, 크기, 교환 회수 등을 최소화하는 방안을 고려하여 설계되어져야 할 것이다.

Ⅲ. CDPD 인증 프로토콜의 문제점 분석과 개선안

CDPD의 보안 서비스는 데이터 비밀성, 키 분배, 이동 단말기에 대한 인증 및 외부로부터의 가입자 익명성을 포함하고 있다. CDPD의 각각의 서비스 네트워크 상에서는 독립적인 인증 서버 AS(Authentication Server)가 MD-IS와 같이 위치한다. 이동 단말기 M-ES의 인증은 단말기의 홈 네트워크 상에 있는 인증 서버 AS를 통해 이루어 진다. 인증의 시작은 먼저 MD-IS와 M-ES 사이에 수행되는 Diffie-Hellman 키 분배 프로토콜[1]로부터 이루어 진다. 이 프로토콜의 결과로 이동 단말기 M-ES와 MD-IS는 공통된 세션 키 Ks를 공유하게 된다. 그림 3은 이동 단말기 M-ES가 방문 MD-IS를 경유하여 홈 MD-IS에게 자신에 대한 신분을 확인시키는 인증 프로토콜을 보여주고 있다. M-ES는 자신의 credential [NEI, ARN, ASN]을 RC4 알고리즘에 세션 키 *Ks*를 적용시켜 암호화한 후에 방문 MD-IS로 보내고, MD-IS는 복호화한 후에 credential을 홈 MD-IS로 보낸다. 이때, NEI(Network Equipment Identifier)는 등록된 단말기 번호, ARN(Authentication Random Number)과 ASN(Authentication Serial Number)은 매 세션마다 상이한 값을 부여하여 불법 복제 단말기에 의한 접속 시도를 방지하거나 또는 사후적으로 검출할 목적으로 사용된다. 홈 MD-IS는 수신된 NEI, ARN, ASN의 유효성에 따라서 M-ES에 대한 위치 등록 요청을 결정한다. 선택적으로 MD-IS는 다음에 사용될 ARN'과 ASN'을 생성하여 방문 MD-IS를 경유하여 M-ES에게 전송한다.

CDPD 시스템에서의 보안상의 취약점은 초기에 이동 단말기 M-ES와 방문 네트워크 MD-IS간에 이루어지는 Diffie-Hellman 키 분배 프로토콜의 문제점에 기인한다[9]. 즉, 세션 키의 분배가 방문 MD-IS에 대한 인증 메커니즘이 결여된 상태에서 이루어지기 때문에 불법적인 제3자가 MD-IS로 가장하여 프로토콜에 적극적으로 개입한다면 이동 단말기 비밀 정보의 노출이 가능하게 된다. 또한, 원래의 credential을 소지하고 있는 정당한 M-ES는 외부 공격자가 이미 서비스를 제공받으면서 credential이 변경되기 때문에 더 이상 서비스를 받지 못하게 된다. 따라서, 세션 키의 분배와 더불어 방문 MD-IS에 대한 인증 기능을 포함한 개선된 프로토콜이 선행되어야 한다.

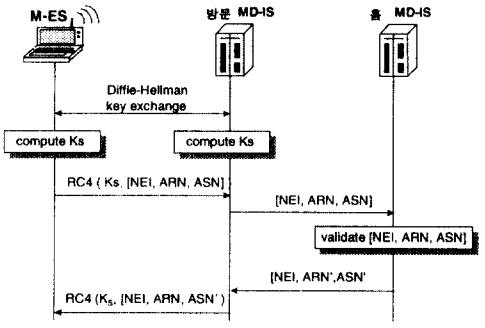

그림 3. CDPD의 보안 프로토콜
Fig. 3 The Security protocol of CDPD

개선된 프로토콜에서는 공개키 방식의 인증서(certificate) 개념을 추가하여 방문 MD-IS가 자신의 신분을 이동 단말기 M-ES에 입증하게 된다. 이때, 고려해야 할 사항은 이동 단말기의 계산 부담을 최소화시켜야 한다는 제약이다. 제안되는 프로토콜에서는 공개키 인증서 발급기관 T의 존재를 가정하여 다음과 같은 유형의 공개키 인증서를 각 네트워크에 부여한다.

각 가입자는 최초 서비스 가입 시에 공개키 인증서를 확인하는 인증서 발급기관의 공개키 P_T를 부여 받는다. 방문 MD-IS의 공개키 인증서 $C_{MD\text{-}IS}$ 구조는 다음과 같다.

$C_{MD\text{-}IS}$ = {MD-IS, $P_{MD\text{-}IS}$, g, p, {MD-IS, $P_{MD\text{-}IS}$, g, p} S_T},
where g, p : Diffie-Hellman 파라메터,
MD-IS : 방문 MD-IS의 ID,
$P_{MD\text{-}IS}$: 방문 MD-IS의 공개키,
{...} S_T : 인증서 발급기관 T의 비밀키 S_T로 {...}을 서명한 값

인증서 발급기관의 공개키 P_T는 이동 단말기 측에서 요구되는 서명의 확인 작업에 소요되는 계산을 최소화하게 선정해야 한다. 이에 대한 대안으로 RSA 공개키 암호시스템에서 공개키의 값을 e=3으로 설정[2]하거나 modular square root 기법[5]을 이용할 수가 있다.

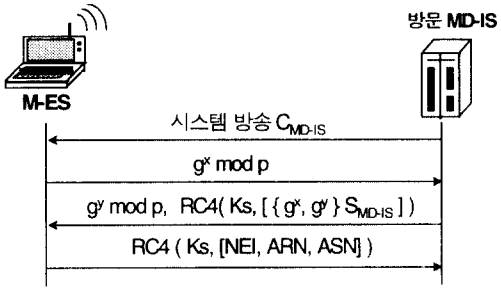

그림 4. 수정된 인증 프로토콜
Fig. 4 Modified Authentication Protocol

그림 4의 개선된 CDPD 프로토콜에서는 방문 MD-IS에서 방송되는 시스템 정보에 포함된 인증서 $C_{MD\text{-}IS}$를 통해서 이동 단말기가 정당한 MD-IS에 대한 확신을 갖게 된다. 먼저 공통된 세션 키 Ks = g^{xy} mod p를 이용해 복호화한 후에 인증서 $C_{MD\text{-}IS}$에 포함된 방문 MD-IS의 공개키 $P_{MD\text{-}IS}$를 이용해서 방문 MD-IS에 의해서 서명 된 {g^x, g^y} $S_{MD\text{-}IS}$를 확인할 수가 있다. 물론, MD-IS의 공개키 역시 이동 단말기의 계산 부담을 감하는 파라메터로 설정되어야 한다. 위의 수정된 프로토콜은 이동 단말기에 단지 인증서 발급기관의 공개키와 공개키 알고리즘만을 추가함으로써 기존의 프로토콜의 변경 없이 사용될 수가 있다. CDPD는 기존의 고정 망은 안전하다는 가정을 하고 있다. 즉, 홈 MD-IS와 방문 MD-IS간의 통신은 평문의 형태로 이루어 지고 있다. 하지만 이 구간의 통신은 특정 M-ES의 credential [NEI, ARN, ASN]을 포함하고 있기 때문에 외부 공격의 가능성을 내포하고 있다. 일단, credential이 노출이 되면 외부 공격자는 특정 M-ES를 가장하여 계속해서 서비스를 제공받을 수 있게 된다. 따라서, MD-IS간의 통신에 있어서도 상호 합의된 방식에 따라서 메시지를 보호할 수 있는 암호화 기법의 도입이 필요하다.

Ⅳ. 무선 데이터 통신 시스템에서의 가입자 익명성

무선 데이터 통신 또는 이동 컴퓨팅 환경에서 나타나는 중요한 보안 문제 중의 하나는 이동 가입자의 신원과 그의 행적을 보호하는 가입자 익명성과 가입자 추적 불가능성이다. 본 논문에서 구체적으로 다루고자 하는 익명성은 가입자의 실제 신원을 제 3자 즉, 불법적인 도청자로 부터 보호하고 경우에 따라서는 서비스를 제공하는 방문 네트워크로부터도 가입자의 실제 신원을 보호하는 것을 의미한다. 가입자의 실제 신원과 행적은 단지 그가 최초로 등록된 홈 네트워크에게만 알려진다. 현재 제공되는 무선 이동 통신 서비스는 가입자에게 후불 방식의 요금 체계를 가정하고 있다. 결과적으로 모든 가입자는 자신의 홈 네트워크가 정의되어지고 자신의 홈 네트워크와 로밍 서비스 협정이 체결된 방문 네트워크 내에서도 서비스를 제공받을 수가 있다. 하지만, 이러한 후불 방식의 요금 체계는 현재 급격히 주목을 받고 있는 전자 현금을 통해 홈 네트워크가 없는 가입자 개념 하에서의 선불 방식 요금 체계와 병행될 가능성이 매우 높다. 이러한 환경 하에서는 결국 홈 네트워크 없이 공중전화 카드를 사용하는 것과 동일하기 때문에 가입자의 행적에 대한 완벽한 비밀성이 보장된다.

본 장에서는 주어진 보안 환경마다 요구되는 익명성의 정도에 따라서 가입자 익명성에 대한 분류를 하고, 또한 가입자 익명성과 추적 불가능성을 제공하기 위해서 적용될 수 있는 여러 가지 유형의 메커니즘을 분석해 본다. 가입자 익명성을 제공하기 위한 방법은 가입자의 실제 신원을 공개키 또는 개인 키 방식으로

암호화하여 보내거나 또는 각 가입자에게 가변적인 가명(alias)을 부여하여 사용하게 함으로써 가입자의 실제 신원 및 행적을 숨기는 것이다. CDPD에서는 Diffie-Hellman 키 분배 프로토콜에 의해서 설정된 세션 키로 가입자의 실제 신원에 해당하는 NEI를 암호화하여 보낸다. 이번 장에서는 가변적인 가명에 초점을 맞추고 특히, 이와 관련하여 기존의 인증 서버에서 주도되는 가명 갱신 메커니즘의 대안과 가명 동기화가 상실될 경우의 복구 메커니즘을 제시한다.

4.1 가입자 익명성 분류

주어진 무선 데이터 및 이동 통신 환경에서 요구되는 가입자 익명성의 정도는 그러한 보안 서비스가 제공됨으로써 발생될 수 있는 추가 비용, 가입자에게 예상되는 서비스 수준, 그리고 다른 관련 시스템 요소들과의 연동 등을 고려하여 결정되어야 한다. 무선 데이터 통신 환경에서의 가입자 익명성과 추적 불가능성 문제는 요구되는 정도에 따라서 여러 가지 등급[10]으로 구분하여 살펴볼 수 있다. 상위 등급은 하위 등급의 조건을 내포하고 있다.

C1 : 불법적인 외부 도청자로 부터 가입자 신원 은폐

가입자 익명성 문제에 대하여 현재 제시된 대부분의 해결책들은 이 기본적인 요구 조건을 만족하는 것들이다. 이것을 통해서 불법적인 외부 도청자가 가입자의 현재 위치와 실제 신원과의 연관성을 유추해내지 못하게 한다. 가장 보편적인 방법은 가변적인 가명을 사용하는 것이다. GSM 이동 통신 시스템에서 사용되는 TMSI(Temporary Mobile System Identification)가 여기에 해당된다. 정적(static)인 가명을 사용한다면 가입자에 대한 추적이 가능하기 때문에 매 세션마다 다른 가명을 사용하는 것이 보다 안전하다.

C2 : 방문 네트워크로부터 가입자 신원 은폐

C1 등급의 가입자 익명성이 사용되는 환경에서는 방문 네트워크 측으로부터 가입자의 신원과 행적을 보호할 수가 없다. 하지만, 경우에 따라서는 가입자에 대한 신원 정보를 방문 네트워크 측이 알 필요가 전혀 없다. 단지, 방문 네트워크 측이 요구하는 것은 가입자의 대금 지불 능력에 대한 증명과 그 가입자에게 서비스를 제공한 대가로 홈 네트워크 측에 대금 청구를 하는 데에 필요한 정보 뿐이다.

C3 : 가입자의 홈 네트워크를 외부로부터 은폐

보다 강력한 가입자 익명성은 불법적인 도청자가 특정 가입자의 실제 신원을 도출할 수 없게 특정 가입자와 그 가입자의 홈 네트워크와의 연관성을 숨기는 것이다. 또는, 특정 가입자에 대한 이용 요금 청구가 문제가 되지 않거나 혹은 다른 방식의 결제 수단이 존재한다면 방문 네트워크로부터 가입자의 홈 네트워크를 은폐시킬 수도 있다.

C4 : 가입자의 행적을 홈 네트워크로부터 은폐

가장 강력한 가입자 익명성은 가입자의 홈 네트워크에게 조차도 가입자의 행적에 대한 정보를 은폐시킴으로써 가입자의 행동에 대해 완전한 비밀을 보장할 수 있다.

위에서 열거한 4가지 유형의 분류는 단지 가입자 익명성이라는 기능 만을 고려한 것이기 때문에 실제 시스템에 적용되기 위해서는 다른 시스템 요소들과의 충돌 가능성들을 고려해야만 한다. 예를 들어, C4에 해당하는 가입자 익명성이 요구되는 무선 데이터 및 이동통신 환경에서는 홈 네트워크가 가입자의 위치 갱신에 따른 정보를 추적할 수가 없기 때문에 가입자에게로 걸려오는 호 요구는 처리할 수가 없게 된다. 또한, 오프-라인 전자 현금과 같은 지불 방식이 마련되지 않는 한 C4의 가입자 익명성 역시 홈 네트워크에 의한 대금 청구에 문제가 발생한다.

4.2 가명을 이용한 가입자 익명성

가장 직접적인 가입자 익명성 제공 방안은 가명(alias)을 이용하는 것이다. 일반 패스워드도 안전성을 높이기 위해서는 정기적으로 갱신이 요구되어지는 것처럼 매 세션마다 가변적인 가명을 사용하는 것이 권장된다. 따라서, 매 세션마다 그 다음 세션에 사용될 새로운 가명을 갱신하는 메커니즘이 요구된다.

이미 언급한 바와 같이 가명을 고정적으로 사용한다면 가입자의 실제 신원은 노출될 가능성이 적다고 할지라도 해당 가입자의 행적은 추적되어질 수가 있다. 따라서 매 세션마다 가명을 변화시켜주는 메커니즘이 요구된다. 그림 5는 i번째 세션에 수행되는 가입자 인증과 세션 키의 분배가 이루어 진 직후에 새로

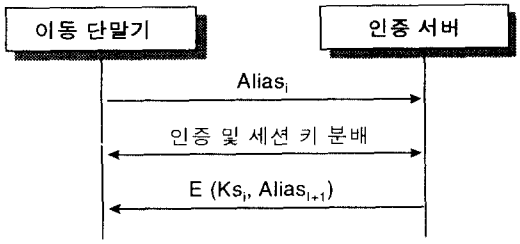

그림 5. 인증 서버에 의한 새로운 가명의 부여
Fig. 5 Distributing a new alias by an Authentication Server.

운 가명을 인증 서버 측에서 부여하는 가명 갱신 프로토콜을 보여주고 있다.

이동 단말기는 (i-1)번째 세션에서 부여받은 가명 $Alias_i$를 이용하여 가입자 인증 및 세션 키 Ks_i의 분배를 수행하고 i번째의 인증 세션 종료 전에 (i+1)번째 세션에 사용될 가명 $Alias_{i+1}$을 인증 서버로부터 부여받게 된다. 이때, 인증 서버는 새로이 선정한 가명을 해당 세션에서 합의된 세션 키 Ks_i를 이용하여 대칭형 암호 알고리즘 E를 통해 암호화한 후에 부여한다. 그림 5의 새로운 가명을 부여하는 프로토콜은 마지막 단계의 메시지가 오류 없이 이동 단말기에 의해 수신이 되어진다는 보장이 되어야 한다. 만약, 마지막 메시지의 수신이 통신 장애로 인하여 완료되어지지 못한다면 추가의 복구 메커니즘을 통해서 가명의 동기화를 회복하여야 한다. 현재, GSM 이동전화 시스템[3]에서는 이러한 유형의 가명 갱신 메커니즘을 이용하고 있다.

4.3 인증 기능을 동반한 새로운 가명 갱신 메커니즘의 제안

그림 5에서처럼 새로운 가명의 생성과 분배가 어느 한쪽에 의해서 수행되어지는 경우에는 새로운 가명의 분배에 따른 추가의 메시지 교환이 필수적이다. 이의 대안으로서 쌍방간에 합의된 가명 갱신 메커니즘을 이용한다면 가명 갱신과 관련된 추가의 메시지 교환의 필요는 없게 될 것이다. 이미 제안된 방안[6] 중의 하나는 쌍방간에 약속된 일방향 함수 h()를 이용하여 일정한 시간 간격을 두고 이동 가입자가 서비스 최초 가입 시에 부여 받은 비밀키 K와 해당 시간에 대한 함수 값을 다음에 사용할 가명으로 합의하는 것이다. 즉, $Alias_{j+1} = h(K, Time_j)$. 이때, $Time_j$에서의 j는 몇 초나 몇 분 단위가 아니라 몇 시간 정도의 시간 대역으로 설정한다. 결국, 인증 서버 측에서는 일정한 시간대 별로 각 가입자의 새로운 가명을 갱신하는 작업이 요구되어 진다. 경우에 따라서는 미리 그 해당 날에 필요로 하는 모든 가명을 미리 생성하여 미리 보유할 수도 있다. 가입자 측에서는 필요할 때마다 해당 시간대 값을 적용하여 생성된 가명을 이용할 수가 있게 된다. 시간대 별로 새로운 가명을 계속 갱신해주는 작업은 서버 측에서는 매우 큰 부담이라고 할 수가 있다. 또한, 빈번하게 접속을 요구하지 않는 이동 가입자의 가명을 일괄적으로 갱신한다는 것도 매우 비효율적인 방식이라고 할 수가 있고 반면에 주어진 시간대 내에서 연속적으로 통화 접속을 요구하는 이동 가입자에게 대해서는 부분적이나마 추적의 가능성을 내포하고 있다. 따라서, 접속이 종료될 때에 이동 단말기와 인증 서버간에 일정한 알고리즘에 따라서 새로운 가명을 각각 동기적으로 갱신하는 메커니즘이 보다 효율적이고 안전하다고 볼 수가 있다. 예를 들어 i번째의 세션 종료 전에 (i+1)번째에 사용할 가명 $Alias_{i+1} = h(K, Alias_i, Time_i)$, i = 0, 1, 2, ...이 계산된다. 이때, $Time_i$는 i번째 세션의 현재 시각의 시간 대 값이고 $Alias_0$는 이동 단말기의 실제 신원 ID_M을 나타내는 정보를 의미한다. 즉, 최초 서비스 가입 시에 이동 단말기에는 비밀키 K, 실제 신원 정보 ID_M 그리고 $Alias_0$이 기록, 저장된다. 인증 서버의 데이터베이스에도 가입된 이동 가입자의 실제 신원, 비밀키 그리고 가입자의 현재 가명이 저장되어 진다. 이러한 가명 갱신 메커니즘을 기반으로 한다면 그림 6에서와 같이 기존의 추가 인증 프로토콜의 필요성은 없어진다.

인증 서버는 i번째 세션에 이동 단말기로부터 수신된 가명 $Alias_i$를 자신의 데이터 베이스에서 검색을 한다. 만약, 그러한 가명이 현재 존재한다면 그러한 가명을 보내온 이동 단말기의 가입자는 정당한 가입자가 되고 결국 인증 과정은 성공적으로 종료된다. 이때, 인증 서버는 그 이동 가입자의 새로운 가명 $Alias_{i+1} = h(K, Alias_i, Time_i)$을 계산하여 데이터 베이스로부터 갱신을 한 다음에 이동 단말기에 회답 Ack을 하면 이동 단말기 역시 약속된 가명 갱신 알고리즘에 따라서 동기화 된 새로운 가명 $Alias_{i+1}$을 계산하게 된다. 여기서 제안한 익명성이 보장된 인증

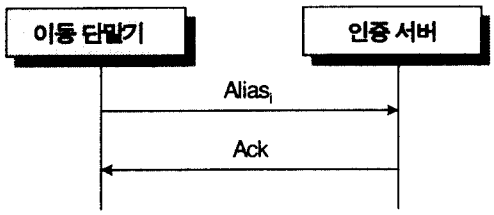

그림 6. 익명성이 보장된 인증 프로토콜
Fig. 6 The Authentication Protocol which secured anonymity

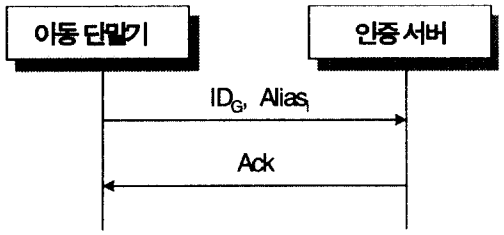

그림 7. 그룹 번호를 동반한 인증 프로토콜
Fig. 7 The Authentication Protocol With Group ID.

기법을 사용할 경우에 인증 서버의 데이터 베이스에는 비록 그 가능성은 매우 희박하지만 동일한 가명이 하나 이상 존재할 수도 있다. 또한, 불법 외부 침입자가 임의의 가명을 사용하여 연속해서 접속을 시도할 가능성도 있다. 가명에는 인증에 필요한 모든 정보가 함축해 있기 때문에 외부 침입자의 이러한 공격이 성공할 가능성은 최소화되어야 한다. 이에 대한 해결책으로 가입된 이동 가입자들을 그룹으로 나누어 각 그룹에 속하는 가입자들에게 그룹 번호 ID_G와 그룹 비밀키 K_G를 부여한다. 이때, 동일한 그룹에 속하는 가입자라고 할지라도 서로 상이한 그룹 번호를 할당하여 임의의 두 그룹 번호가 동일한 그룹에 해당하는 것인지를 알 수 없게 한다. 하지만 인증 서버는 이러한 서로 다른 그룹 번호가 동일한 그룹에 속하는 번호라는 사실을 아는 유일한 객체가 된다. 따라서, 이동 가입자가 네트워크에 접속을 요구할 때에는 그림 7에서와 같이 가명과 더불어 그룹 번호를 함께 보내게 된다. 이 경우에 위에서 논의된 위험성은 최소화될 수가 있다. 외부 침입자의 경우에는 각 그룹마다 모든 가능한 가명을 시도해야 하기 때문에 성공 가능성은 매우 희박하게 된다.

기존의 CDPD에서 가입자의 익명성이 제공되는 방식은 가입자의 실제 신원을 나타내는 등록된 가입자 단말기의 NEI가 암호화되어져 교환되기 때문에 외부로부터의 익명성이 보장된다. 하지만, 방문 MD-IS에 대해서는 익명성이 보장되지 않는다. 특히, MD-IS 간에는 안전한 채널이 존재하지 않기 때문에 여기서 제시한 가명 기법을 이용한다면 CDPD가 지니는 보안상의 취약점을 해결할 수가 있게 된다.

4.4 가명 동기화 상실에 따른 복구 메커니즘

전 절에서 논의한 가명 갱신 메커니즘의 경우에도 가명의 동기화가 상실될 수가 있다. 일반적으로 가명에 대한 동기화가 상실되었을 경우에는 GSM에서처럼 가입자의 실제 신원을 통해서 인증 및 가명 동기화가 수행된다. 결국, 동기화가 상실되었을 경우에는 가입자의 익명성 역시 상실된다고 할 수 있다. 이번 절에서는 가입자의 실제 신원을 노출함이 없이 새로운 가명으로 동기화 되는 복구 프로토콜을 제시한다.

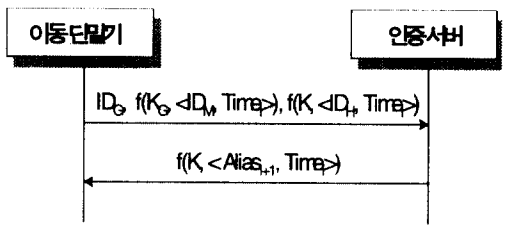

그림 8. 동기화 된 가명 복구 메커니즘
Fig. 8 Synchronized Alias recovery mechanism.

인증 서버는 그룹 번호 ID_G를 통해서 그 이동 가입자가 속한 그룹과 그에 해당하는 비밀 키 K_G를 이용하여 이동 가입자의 실제 신원 ID_M을 파악하고 그의 비밀키 K로 $f(K, \langle ID_H, Time_i \rangle)$을 복호화 한다. 이때, ID_H는 이동 가입자가 속한 네트워크의 실제 신원을 나타내고 $f(K, \langle ID_H, Time_i \rangle)$은 이동 가입자에 대한 인증의 목적으로 사용될 수가 있다. 인증 서버는 새로운 가명 $Alias_{i+1} = h(K, ID_M, Time_i)$을 계산하여 이것을 암호화한 $f(K, \langle Alias_{i+1}, Time_i \rangle)$을 이동 단말기에 보낸다. 이동 단말기 역시 동기화 된 새로운 가명

$Alias_{i+1}$을 계산하고 수신된 가명과 비교하여 동기화를 이룬다. 이때, $f(K, \langle Alias_{i+1}, Time_i \rangle)$은 인증 서버에 대한 인증 역할을 하게 된다. 이 경우에 가입자의 실제 신원에 대한 노출은 없게 된다.

V. 결 론

본 논문에서는 CDPD 무선 데이터 통신 시스템의 보안상의 취약점을 지적하고 그것을 보완하기 위한 해결책을 제시하였다. 특히, 가입자의 익명성과 관련하여 효율적인 가명 갱신 메커니즘의 제안과 동기화가 상실된 가명을 복구하는 메커니즘 역시 제시되었다. 특히, 제안된 가변적인 가명 기법은 그 자체가 인증에 필요한 모든 정보를 내포하기 때문에 추가의 인증 프로토콜이 요구되지 않는 매우 효율적인 기법이라고 할 수 있고 CDPD에도 적용될 수가 있다. 이미 언급한 바와 같이 현재의 CDPD 상의 보안 프로토콜은 많은 허점을 지니고 있기 때문에 상당한 수정이 가해져야 할 것으로 사료된다.

참 고 문 헌

1. W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. on Inform. Theory, vol. 22, pp. 644-655, 1976.
2. M. Tatebayashi, N. Matsuzaki, and D.B. Newman, "Key Distribution Protocol for Digital Mobile Communication Systems", Advances in Cryptology, Proceedings of Crypto'89, pp. 324-334, 1989.
3. ETSI-GSM, Technical Specification GSM 03.20, "Security Related Network Functions," Version 3. 3.2 (Release 92, Phase 1), 1992.
4. Cellular Digital Packet Data (CDPD) System Specification, Release 1.0, July 19, 1993.
5. M.J. Beller, L.F. Chang, and Y. Yacobi, "Privacy and Authentication on a Portable Communication System", IEEE Journal on Selected Areas in Communications, vol. 11, no. 6, pp. 821-829, Aug. 1993.
6. A. Herzberg, H. Krawczyk, and G. Tsudik, "On Traveling Incognito," Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, Santa Cruz, Ca., Dec. 8-9, 1994.
7. D. Samfat and R. Molva, "A Method Providing Identity Privacy to Mobile Users during Authentication," Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, Santa Cruz, Ca., Dec. 8-9, 1994.
8. 한국통신기술협회, TTA Interim Standard:800MHz 대 디지탈 이동전화 무선 인터페이스, 제 1 판, 1994.
9. Y. Frankel, A. Herzberg, P.A. Karger, H. Krawczyk, C.A. Kunzinger, and M. Yung, "Security Issues in a CDPD Wireless Network," IEEE Personal Communication, vol. 2, no. 4, pp. 16-27, Aug. 1995.
10. D. Samfat, R. Molva, and N. Asokan, "Anonymity and Untraceability in Mobile Networks," Proc. of the ACM International Conference on Mobile Computing and Networking, Nov. 1995, Berkeley, Ca.

이 수 연(Suyoun Lee) 정회원

1990년 2월:단국대학교 전자계산학과 학사

1993년 2월:단국대학교 전산통계학과 석사

1996년 2월:성균관대학교 정보공학과 박사수료

1997년~현재:천안외국어전문대 사무자동화과 전임강사

※주관심분야:암호와 부호 이론, 정보 보호 기술, 무선통신망 프로토콜 설계 및 성능 분석

안 효 범(Hyobeom Ahn) 정회원

1992년 2월:단국대학교 전자계산학과 학사

1994년 2월:단국대학교 전산통계학과 석사

1996년 2월~현재:단국대학교 전산통계학과 박사 수료

1997년 9월~현재:국립천안공업전문대 정보통신과 전임강사

※주관심분야:네트워크 성능분석, 컴퓨터 성능평가, 암호이론

박 창 섭(Changseop Park) 정회원

연세대 경제학사
미국 LEHIGH 전산학 석사, 박사
현재 : 단국대학교 전자계산학과 부교수
※주관심분야 : 암호 및 부호 이론, 보안 프로토콜

이 동 훈(Donghoon Lee) 정회원

1984년 : 고려대학교 경제학과 학사
1988년 : Oklahoma대학 전산학과 석사
1992년 : Oklahoma대학 전산학과 박사
1992년 : 단국대학교 전자계산학과 전임강사
1993년~1997년 : 고려대학교 전산학과 조교수
1997년~현재 : 고려대학교 전산학과 부교수
※주관심분야 : 정보보안 및 계산 이론