산업기술연구(강원대학교 산업기술연구소 논문집), 제21권 A호, 2001.
Journal of Industrial Technology, Kangwon Nat'l Univ.,Korea, No. 21 A, 2001.

가입자 정보보호를 위한 Virtual Home Environment 시나리오 보안 취약점 분석

A Study of Virtual Home Environment Implementation Scenario for Subscriber Privacy

정 종 민* 이 구 연** 이 용***
Jeong, Jong-Min Lee, Goo-Yeon Lee, Yong

Abstract

Currently, the VHE (suggested for global roaming user to provide personal service environment) implementation scenario is being proposed to realize 3G network requirements. However, developing VHE scenarios are focused on signal flow between node and network, and network and network. this case may result in weakness to protect subscriber's privacy in 3G network which commonly uses visited network. In this paper, we reanalyze a several VHE implementation scenarios for user profile protection, indicate a problem concerning user privacy, and finally, design a procedure to cope with vulnerability in VHE implementation scenario.

Keywords : *VHE, Shadow Home Service, Relay Home Service, Shared Service Control, Direct Home Command, GRE (Global Roaming Environment), PSE (Personal Service Environment)*

1. 서론

3G 이동 통신 환경에서 이기종 망간의 글로벌 로밍(global-roaming)에 관한 사용자의 관심 증가는 가입자 홈 망에서 제공받는 서비스를 여러 망을 이동하는 것과 상관없이 동일한 서비스를 제공받을 수 있는 기술을 요구하게 되었고, 이것은 지역적인 제한에 상관없이 지속적인 사용자 인터페이스를 제공해야 한다는 것을 의미하기도 한다. 따라서 사용자가 가입자 홈 망을 벗어나도 홈 망에서와 동일 서비스 레벨을 제공받을 수 있게 된다.

기존 무선 환경을 3G 망으로 이동시키는 핵심 요소는 망 하부구조의 기술적인 혁신보다는 사용자가 어디에 있든 상관없이 서비스를 수용할 수 있는 새로운 형태의 서비스를 가능하게 하는 것으로, 이는 여러 무선 응용들과 이음세 없는 서비스 뿐만 아니라 서비스 제공자가 새로운 서비스를 생성하고, 이를 가입자의 요구에 맞게 적용하며, 관리하는 서비스 성능이 3G 망의 성공을 좌우하는 요소가 될 것이다.

이러한 글로벌 로밍 및 사용자 홈 서비스 기능을 위해 망에 적용되어야 할 기술들로는 Intelligent Network (IN), Virtual Home Environment (VHE), Open Service Architecture (OSA) 개념들이 거론되고 있으며,[1] 본 논문에서는 VHE에 대해서만 다루게 된다.

VHE는 3G 망에서 사용자가 마치 자신의 가입자 망에 있는 것과 같은 환경을 제공하기 위한 것으로 개인 서비스 환경(Personal Service

* 강원대학교 컴퓨터정보통신공학과 박사과정
** 강원대학교 컴퓨터정보통신공학과 부교수
*** 한국정보보호센터 선임연구원

Environment 이하 PSE)을 가능하게 한다. 이와 관련한 성능 규격(related capabilities)은 IN CS (Capability Set 4)에 포함되어 있고, 1999년 11월에 최종 정의되었다.[2]

현재 VHE의 여러 구현 시나리오가 제안되고 있는 시점인데, 주로 메시지의 흐름에 관련된 요소만을 적용하여 이루어지고 있다. GRE (General Roaming Environment) 구조는 가입자 동작 및 서비스 루틴이 방문 망을 이용하여 이뤄지는 것이 일반적인데, 이 경우 서비스 수행에 필요한 가입자 프로파일 공개 및 등록 정보 등의 가입자 정보가 방문 망에 제공되어야 한다. 이는 가입자 입장에서 개인 정보가 동의되지 않은 상황에서 방문 망에 노출 될 수 있으며, 가입자망의 입장에서는 가입자 정보 보호에 대한 신뢰성을 떨어뜨리는 경우가 되어, 가입자 확보에 치명적인 손실을 가져올 수 있다.

이러한 이유로 인해 VHE의 GRE구조에서 반드시 가입자 정보보호의 요소를 포함시켜야 하며, 이를 위해서는 현재 제안되고 있는 VHE 구현 시나리오에 정보보호의 요구사항을 수용하여 진행되어야 한다.

이에 본 논문에서는 GRE구조의 3G 망에서 VHE서비스를 제공하기 위해 제안된 구현 시나리오를 분석하고 이를 가입자 정보 보호의 입장에서 재해석하여 보안상의 취약점을 제기하고 이를 해결하기 위한 방안을 설명하여 향후 이뤄지게 될 VHE 환경의 신뢰성 있는 구현을 가능하게 하는 역할을 하고자 한다.

논문의 2장에서는 VHE구현에 대한 요구사항 및 VHE의 개념을 정리하며, 3장에서 현재 제안되고 있는 여러 시나리오를 분석한 후 사용자 개인 정보보호의 관점을 추가하여 문제점을 제시하며, 이를 위한 절차를 설계하고, 5장에서 결론을 맺는다.

2. VHE의 정의

VHE는 단말이 망의 경계를 이동하여 자신의 단말을 사용하지 않더라도 PSE의 이동성을 제공하기 위한 개념으로 정의된다.

이는 사용자가 위치한 장소와 특정 단말과 망에 상관없이 사용자 인터페이스를 제공하며, 동일한 개인 서비스를 지속적으로 제공하기 위해 제안된 것으로 이를 위해 요구되는 핵심 사항은

- 사용자 고유의(Personalised) 서비스 환경
- 사용자 고유의(Personalised) 인터페이스
- 접속 망에 상관없는 지속적인 서비스 제공

으로 VHE를 지원하기 위한 표준은 VHE가 모든 형태의 미래 망에서 적용 가능한 유연성을 지닐 수 있어야 하며 추가적으로 사용자가 지역적인 위치에 상관없이 자신의 등록 서비스를 사용 가능할 수 있게 글로벌 서비스에 관한 기능도 포함해야 한다.[4]

다음 [그림 1]은 VHE의 개념을 설명하기 위해 사용자 관점에서 PSE에 대한 구조를 나타낸 것이다.

*Home environment*는 지속적으로 사용자에게 서비스를 제어하고 공급하게 되며 사용자의 PSE는 사용자가 요구하는 서비스와 사용자의 개인 정보를 조합하는 기능을 하게 된다.

*USER*는 다양한 상황과 필요에 따라 통신을 관리할 수 있도록 여러 개의 *User profile*을 가질 수도 있는데, 이 *User profile*은 **사용자 인터페이스 프로파일**과 **사용자 서비스 프로파일**로 구성되며, 사용자 인터페이스 프로파일에는 메뉴 설정, 터미널 설정, 네트웍 관련 선택 사항 등의 정보를 포함하고, 서비스 프로파일에는 등록한 서비스 목록과 서비스에 관련된 선택 항목 및 현재의 상태 정보(active/deactive)를 포함하고 있다. 하나 혹은 다수의 사용자 인터페이스 프로파일과 여러 개의 사용자 서비스 프로파일을 가질 수 있지만, 사용자 프로파일은 이에 대한 하나의 조합 형태를 갖게 되며, 각 사용자 프로파일은 고유해야 한다.

*USER*와 *Home environment*는 *User profile*로 설명되는 *Personal service environment*의 사용자 특성을 변경할 수도 있는데 이 경우 *Home environment*는 수정된 PSE를 반영하기 위해 분배된 *User profile*을 업데이트 할 수 있어야 한다.

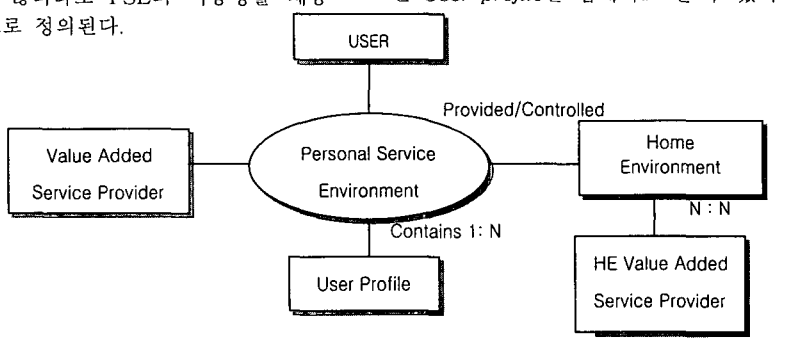

그림1 사용자 관점에서의 개인 서비스 환경 구조

3. VHE 시나리오 분석

본 논문에서 분석하고자 하는 VHE시나리오는 [3]에서 제안된 것으로 VHE 구현 시나리오를 세분하여 상세하게 제안된 논문으로 구현 가능한 시나리오의 총체적인 규격을 살펴보기에 적절하다.

3.1 보안 취약점 제기 및 해결 방안

VHE의 구현 시나리오는 사용자의 입장에서는 투명(transparent)하게 이루어지지만, 망의 입장에서는 몇 가지의 기술적인 개발과 상업적인 동의가 요구되어 진다. 이러한 VHE 시나리오는 다음과 같은 범주에 근간하여 평가되고 구별된다.[3]

- 서비스 제어 위치
- 서비스 초기화 구조
- 데이터 저장 구조
- 서비스 가용성 정도
- 추가적인 보안적 요소

분석에 이용한 VHE 구현 시나리오는 이중 **서비스 제어 및 서비스 로직 요소의 위치**에 관한 관점에서 설계되었으며 다른 요소들은 적용되지 않았다. 그러므로 보안 관점에서는 여러 문제점을 지니게 된다.

논문에서 제기한 보안 취약점은 가입자 프로파일을 포함한 가입자 정보와 서비스 루틴이 가입자 망이 아닌 타 망에 노출되는 것을 방지하는 것에 초점을 맞춰 분석하였으며, 향후 이동통신 단말에는 데이터 암호화를 위한 정보 및 프로세싱이 포함되어 있음을 전제한다. 또한 암호화 및 인증에 관한 상세 규격은 이 논문에서 제외하고 논리적인 구조를 위주로 설명한다.

(1) 시나리오1 : Shadow Home Service

[구조 설명] 서비스에 필요한 사용자 프로파일, 데이터, 서비스 로직, 음성 패턴을 전부 혹은 일부를 일시적으로 방문 망으로 down/shadow하여 방문 망에서 서비스 프로세스를 수행하는 구조로 인증 절차도 방문 망에서 수행될 가능성이 있다.

[절차 제안] 이 구조의 경우 서비스 수행을 위해 가입자의 프로파일과 서비스 로직이 방문 망으로 다운되기 때문에 가입자 망에서 관리되어야 할 정보가 방문 망에서 일시적 혹은 영구적으로 공개되어지므로 가입자 정보 보호에 대한 책임이 방문 망에 명확히 명시되지 않은 상태라면 이는 가입자 정보 보호의 입장에서 문제점이 발생하게 된다.

이를 해결하기 위해서는 방문 망에서 가입자의 프로파일과 데이터를 읽기 불가능한 상태로 변형(암호화) 후 down/shadow를 시키고 서비스 로직은 기존 형태로 down/shadow 형태를 취하되, 서비스 로직에서 이를 해독하여 가입자가 원하는 서비스를 수행할 수 있게 하면 된다.

이를 위해서는 단말과 가입자 망 사이의 미리 정의된 키와 방문 망의 정보를 기반하여 세션 키 생성 절차가 필요하며, 방문 망에서 수행되는 서비스 로직에 사용자 정보를 복호화 시키는 기능을 내재 시켜야 한다.

이에 추가하여 가입자망은 가입자가 실제로 서비스를 요구한 방문 망에 위치하고 있는 지와 방문 망의 입장에서도 서비스 루틴을 down/shadown 해주는 망이 사용자의 정상적인 가입자 망인지에 관한 상호 인증을 수행해야 한다.

[그림 2]는 shadow home service의 절차를 나타낸 것으로, 사용자의 서비스 요구를 수신한 방문 망은 사용자 인증 절차를 거쳐 사용자와 세션키를 공유하게 되며, 실제 서비스 항목을 공유키로 암호하여 방문 망에 보내면, 방문 망에서 이를 복호 한 후 가입자 망과의 인증을 통해 또다른 공유키를 할당받아 이를 통해 가입자 망에 서비스 요구 메시지를 전송한다. 이를 통해 가입자와 방문 망, 방문 망과 가입자 망의 상호 인증 및 메시지 기밀성을 보장받게 된다. 상호 인증의 절차가 모두 정상적이라면, 각 네트워크 및 노드가 공유한 키로 메시지를 송수신하게 되어 안전한 통신을 이루게 된다.

또한 방문 망에서 다운로드한 로직내에 가입자 프로파일을 복호화 할 수 있는 기능을 내재 시켜 서비스 로직 수행에 필요한 가입자 프로파일의 복호된 형태가 방문 망에 노출되지 않게 한다.

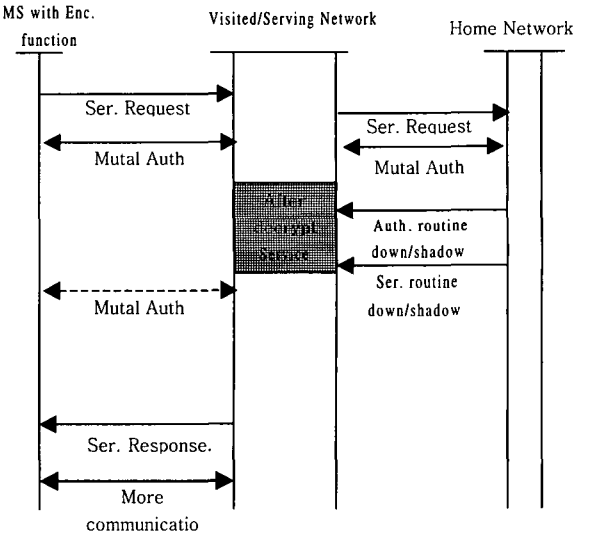

그림 2 Shadow Home Service 시나리오 정보보호 절차

(2) 시나리오2 : Relay Home Service

[구조 설명] 사용자가 요구한 서비스 및 데이터를 방문 망의 SCF(Service Control Function)를 경유하여 가입자 망의 SCF에 전달하게 되면 가입자 망의 SCF에서 서비스를 처리하고 이에 대한 응답도 동일하게 방문 망의 SCF를 통해 사용자에게 전달되는 구조이다.

[절차 제안] 비록 서비스 로직이 가입자 망에 의해서 수행된다 하더라도 서비스를 위한 가입자의 정보와 서비스에 대한 응답이 방문 망을 경유하기 때문에 방문 망은 사용자 프로파일 등의 정보와 서비스 응답 정보를 통해 가입자가 사용한 서비스를 파악할 수 있는데 이는 가입자의 프라이버시 유지에 위배될 수도 있다.

이 문제를 해결하기 위해서는 단말과 가입자 망 간의 통신하는 데이터를 캡슐화시켜 방문 망에서는 실제 데이터를 파악하지 못하는 형태를 취하게 하여 방문 망에서의 정보 노출을 방지해야 할 것이며, 이 시나리오는 shadow home service와 달리 서비스 루틴에 복호 기능을 포함하지 않고 독립적으로 수행해도 될 것이다.

이 구조에서도 가입자와 방문 망, 가입자 망간의 상호 인증 절차가 요구되며, 서비스 수행이 방문 망에서 이루어지지 않기 때문에 정상적인 방문 망임을 확인하는 정도의 인증이 요구 될수 있다. (시나리오 1인 경우 현재 사용자가 방문 망에서 실제 위치하고 있는지에 관한 인증이 요구된다.) 또한 가입자에 대한 인증도 방문 망이 릴레이 시킨 정보를 이용하여 가입자 망에서 수행할 수도 있고, 혹은 방문 망에서 직접 가입자를 인증할 수도 있다. 망의 상태와 방문 망의 자원을 활용한다는 측면에서는 방문 망의 AMF (Authentication Management Function)을 이용하게 되며, 방문 망의 신뢰 정도에 따라 가입자 망에서 직접 수행 할 수 있다.

[그림 3]은 Relay Home Service에 대한 절차를 묘사한 것으로 방문 망의 입장에서는 사용자의 서비스 요구와 가입자 망에서의 수행된 응답 결과만을 단순히 릴레이 시키면 된다. 물론 단말과 가입자 망에서는 암호/복호 기능이 있어 방문 망에서 릴레이 되는 정보는 모두 암호화되어 노출이 방지 되며, 상호 인증이 필요하다.

(3) 시나리오3 : Shared Service Control

[구조 설명] 방문 망과 가입자 망이 미리 정의된 형태로 서비스 로직을 공유하여 Joint Service Control Point의 동작으로 사용자가 요구하는 서비스에 대한 Co-processing을 하는 구조 Specialized Resource Function(SRF)이 가입자 망 혹은 방문 망 중 임의 망에 위치할 수 있다.

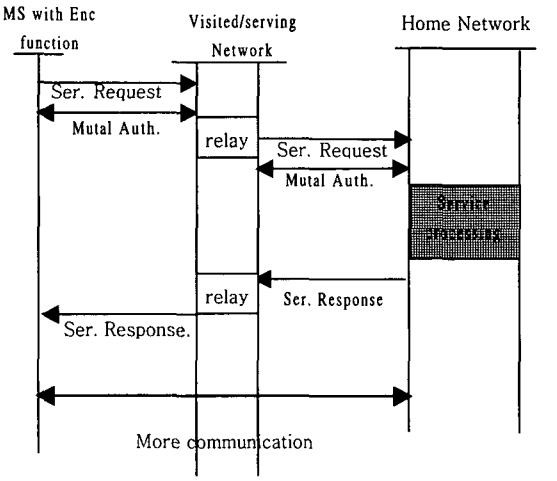

그림 3 Relay Home Service 시나리오 정보보호 절차

[절차 제안] 우선적으로, 방문 망과 가입자 망에서 처리되어질 로직을 정의하는데 있어, 방문 망에서 보안수준이 낮은 데이터 및 그 데이터를 이용한 서비스 로직을 두게 되는데, 이의 정의가 명확해야 하며 가입자 및 사업자 간의 동의가 요구되어진다. 방문 망의 서비스 로직을 가입자 망에서 구현하여 분배시키는 경우는 방문 망의 서비스 로직을 신뢰할 수 있지만, 방문 망에서 수행되는 로직을 방문 망 자체에서 구현된 것을 이용할 경우 방문 망의 악의에 의해 가입자 정보 등이 노출될 수 있다.

이의 해결을 위해서는 방문 망에서 수행되는 서비스 로직은 보안 레벨이 낮은 사용자 프로파일을 요구하는 로직을 두게 하며, 가능하다면 방문 망의 모든 서비스 로직을 가입자 망에서 구현하여 이를 분배하는 형태를 취해야 한다.

가입자와 가입자 망 사이에 방문 망에서 수행될 응용과 가입자 망에서 수행될 것을 구분하여 동의를 얻는 과정이 필요하며, 방문 망에서 수행되는 로직의 구현을 가입자 망에서 구현하여야 한다.

[그림 4]는 Co-processing하는 로직 분배 결정에 관한 절차를 포함한 Shared Service Control의 구조를 보여준다. 마찬가지로 노드와 네트워크간의 상호 인증이 선행되야 하며, 각 인터페이스간의 공유 세션키를 이용하여 기밀성을 유지해야 한다.

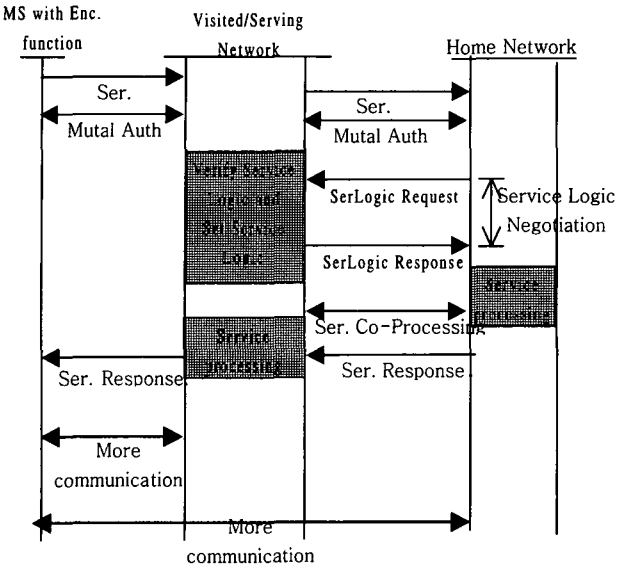

그림 4 Shared Home Service 시나리오 정보보호 절차

(4) 시나리오4 : Direct Home Command

[구조 설명] 이 구조는 서비스 로직을 제어하기 위해 가입자 망의 SCF를 바로 접속 요구하는 구조로 방문 망의 SCF는 어떠한 릴레이나 데이터 전송을 수행하지 않으며 사용자의 서비스 프로파일이나 서비스 로직을 down/shadow하지도 않는다. 즉 이 시나리오에서는 방문 망의 SCF는 없어도 무방한 구조이다. 방문 망에 가입자의 정보 노출이나 서비스 구조를 공개하지 않는다는 입장에서는 가입자 프라이버시 보호에 가장 적절한 구조로 여겨질 수 있다.([그림 5]참조)

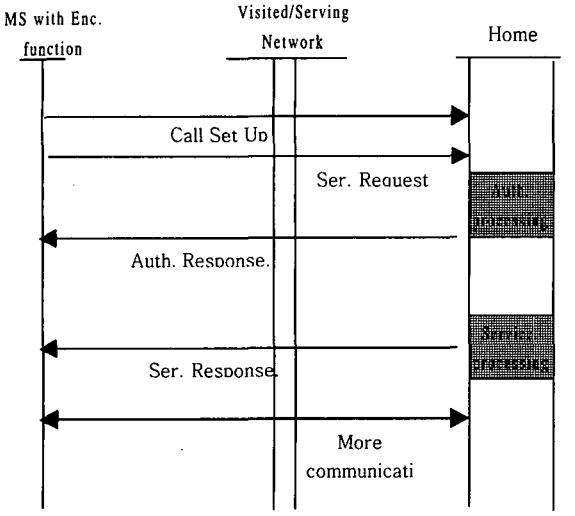

그림 5 Ditect Home Command시나리오 정보보호 절차

분석한 VHE구현 시나리오는 서비스의 로직 및 서비스 요소들이 가입자 망에서 처리되는 것과 방문 망에서 처리되는 것, co-processing하는 것으로 구분될 수 있는데 방문 망을 주로 의존하는 시나리오인 경우 특히 가입자 정보보호를 위한 구조 정의가 요구되어 진다.

GRE환경 및 자원 활용 측면에서 방문 망의 사용은 일반적인 것이나, 방문 망에 서비스 루틴에 관한 많은 권한을 부여한다면, 그 만큼의 정보 보호를 위한 프로세싱이 요구되어 진다.

기본적인 요구 사항은 암호화와 인증을 통한 엔티티간의 접근 권한 확인 및 통신 데이터의 보호가 실현되어야 하며 이는 가입자 혹은 가입자 망에서 방문 망을 인증하는 형태의 단일 인증과 각 노드 및 네트워크간의 상호 인증이 요구 되며, 노드와 방문 망간의 무선 링크 구간에서의 메시지 기밀성을 위한 암호화가 필요한데, 무선 전송 매체의 환경적인 특성을 적절히 파악하여 최적의 절차를 설계해야 할 것이다. 이와 아울러 이기종 망간의 연동이 이루어지는 VHE구조에서 방문 망을 이용한 서비스 수행 시 가입자 정보 보호 기술이 반드시 요구되어 진다.

4. 결론

본 논문에서는 핵심 암호/인증 기술과 실제 이를 이용하여 동작하게 되는 구조를 세부적으로 정의하지는 않았다. 물론 현재 3GPP, 3GPP2등의 사실적 표준화 단체에서 핵심 암호/인증 기술을 제안하고 정의하고 있으며 이 기술들이 향후 3G 네트워크에서의 보안 서비스의 핵심 기술들이 될 것이다.

본 논문에서의 주안점은 3G 네트워크 서비스로 요구되는 VHE의 현 개발단계가 단순히 메시지의 흐름에 관한 사항을 기준으로 하여 진행되고 있는데, GRE 환경에서 필연적으로 이용하게 되는 방문 망에서의 가입자 정보보호에 관한 중요 요소를 제외하고 제안되고 있는 시점에서 향후 거론하게 될 보안 구조에 관한 연구를 선행하여 3G 네트워크의 가입자 보안 기술에 관한 기술을 습득하기 위해 현재 제안되고 있는 VHE의 구현 시나리오에 가입자 프로파일 보호의 입장에서 각 구조에 대해 취약점을 살펴보고, 이를 해결하기 위한 절차를 설계하였다.

향후 3GPP에서 3G 이동 통신 암호 기술로 정의한 KASUMI[6] 등의 핵심 암호/인증 기술을 이용하여 네트워크와 노드 혹은 네트워크와 네트워크간의 상호 인증 및 메시지 기밀성을 제공할 수 있는 상세 규격 및 절차적인 프로토콜을 제안해야 할 것이다.

감사의 글

본 논문은 정보통신부에서 주관하는 2001년도 대학기초 연구 지원사업에 의하여 수행되었음

참 고 문 헌

[1] M. Torabi, "A Shift in the Mobile Network Service Provisioning Paradigm", *Bell Labs Tech. Journal*, 2000

[2] Sugiyama, Nakada, Suzuki, "A Study of Virtual Home Environment in IMT-2000", *IEICETRANS.*, VOL.E82-A, 1999

[3] M. Torabi, Rolfe E.Buhrke, "Third Generation Mobile Telecommunications and Virtual Home Environment", *Bell Lab Tech. Journal*, 1998

[4] "3rd Generation Partnership Project : The Virtual Home Environment(3G TS22.121 ver 3.1.0)", 3GPP Technical Spec. 1999

[5] "User Service requirements for Global VH E" , TSG-SA Working Group1, ETSI , 1999

[6] "3rd Generation Partnership Project : General Report on the Design, Specification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms", 3GPP Technical Spec. 2000