차세대 이동통신시스템에 적용되는 보안 프로토콜의 구성 방식

고재승, 김광조

한국정보통신대학원대학교

Constructing security protocols suitable for next generation mobile system

Jaeseung Go, Kwangjo Kim

Information and Communications University

요 약

본 고에서는 차세대 이동통신시스템에 적용되는 보안프로토콜의 구성방식에 대해서 논의한다. 보안 프로토콜의 구성은 두 단계로 이루어진다. 우선, 단말이용자와 서비스를 제공하는 네트워크간 무선접속구간에서 이용자 익명성과 상호인증 및 안전한 키 합의가 가능한 프로토콜을 제안하고, 이를 기반으로 네트워크 로밍 환경에서 서로 다른 관리영역에 속하는 네트워크간의 두 이동단말 이용자간(end-to-end) 안전한 통신을 위한 보안 프로토콜 구성 방식을 제안한다.

I. 서론

일반 이동전화서비스를 포함하여 이동 컴퓨팅, 이동 멀티미디어 서비스 등 이동통신시스템을 통한 응용서비스 개발과 서비스 제공이 증가함에 따라 이동통신시스템에서 신뢰할 수 있는 보안서비스의 제공의 필요성은 더욱 강조되고 있다. 특히 이동통신시스템의 무선접속구간은 송수신 데이터의 도청이 쉽고, 가용 무선자원이 제한되어 있다는 점에서 유선 네트워크와는 다른 보안 취약점을 가지고 있다. 무선접속구간에서의 이용자 신분 및 위치 정보의 노출, 불법적인 서비스 이용, 송수신 데이터의 도청 및 변경 등은 이용자의 사생활을 침해하고, 전체적인 시스템의 신뢰성을 저하시킬 수 있다. 따라서, 무선환경에서의 보안취약점을 방지할 수 있는 보안서비스 제공이 필요하다.

GSM, CDMA 셀룰라와 같은 기존의 2세대 무선시스템에서 제공하는 보안서비스는 네트워크의 이동이용자 인증, 무선접속구간에서 이용자 데이터와 신호 데이터의 기밀성, 이용자 신분의 부분적인 기밀성 등을 포함한다[1, 2, 3]. 한편, 세계적으로 표준화가 진행중인 UMTS, IMT-2000 과 같은 차세대 이동통신시스템은 유무선 네트워크가 통합된 다중 시스템 환경, 고속의 멀티미디어 서비스 제공, 국내 및 국제적 로밍 서비스 제공 등 2세대 시스템과는 다른 복잡하고 고도화된 응용서비스 제공 환경이 될 것이다[21]. 보편적인 서비스 제공과 네트워크의 복잡성을 고려할 때 차세대 무선시스템에서는 2세대 무선시스템에서 제공하는 보안서

비스를 포함하는 더 넓은 범위의 보안서비스 제공이 필요하다. 이용자와 네트워크간 상호 인증, 무선접속구간에서 강화된 이용자 신분 및 위치정보의 기밀성, 단말이용자간 (end-to-end) 데이터 기밀성 등은 추가적으로 고려되어야 할 보안서비스이다[4, 20].

본 고에서는 차세대 이동통신시스템 환경에서 서로 다른 네트워크 영역에 있는 단말이용자간 안전한 통신을 보장하는 보안 메커니즘과 공개키 암호 알고리즘을 이용한 인증 및 키 합의 프로토콜을 제안한다. 우선 2장에서는 기존에 제안된 이동통신 인증 프로토콜의 보안 메커니즘 및 보안 특성에 대하여 개략적으로 살펴보고, 프로토콜 제안과 관련하여 서로 다른 네트워크에 있는 단말이용자간 통신이 이루어지는 네트워크 환경과 보안구조 관련 기능 시스템 모델을 3장에서 정의하며, 4장에서는 무선접속구간에서 이용자에게 서비스를 제공하는 네트워크 환경에 따른 인증프로토콜과 이를 기반으로 단말이용자간 안전한 통신을 보장하는 인증 및 키 합의 프로토콜을 제안한다.

II. 이동통신 인증 프로토콜 고찰

이동통신시스템에서 보안서비스 제공과 관련하여 가장 중요한 것은 호 설정 절차의 초기에 수행하는 안전하고 효율적인 인증 및 키 설정 프로토콜을 설계하는 것이다. 적합하게 설계된 보안 프로토콜의 수행은 상대 실체를 안전하게 상호 인증하고, 이를 바탕으로 인증된 세션 키를 안전하게 설정하여 뒤따르는 세션의 안전성을 보장한다. 무선접속구간의 이용자와 네트워크간 보안 프로토콜 설계에서 평가되어야 할 보안특성으로는 상호 실체인증, 실체 상호간 세션 키 합의, 합의된 키의 상호 인증, 키 갱신 보증, 이용자 익명성, 과금 데이터에 대한 부인방지 등이 있다[4, 6, 20].

보안 프로토콜은 안전한 암호 알고리즘을 이용하는 기본적인 보안 메커니즘과 세션별로 변경되는 랜덤 수, 타임 스탬프, 시퀀스 등과 같은 시변수값으로 구성되며, 프로토콜 설계시에는 서비스를 제공하는 이동통신시스템의 네트워크 환경과 프로토콜 실체들의 가용자원, 즉 초기 보유지식, 연산능력 등을 고려하여야 한다[15].

최근에 이동통신시스템 환경에서 보안 서비스 제공과 관련하여 여러 가지 인증 및 키 설정 프로토콜들이 제안되었다. 이들 가운데 일부는 기존 2세대 무선시스템의 더욱 강화된 보안특성의 제공을 목적으로 제안되었으며[3, 5, 13, 19], 대다수의 프로토콜은 차세대 무선시스템의 인증 프로토콜로 제안되었다[4, 6, 11, 18]. 또한 제안된 프로토콜의 기본 보안 메커니즘 구성에 적용되는 암호 알고리즘의 형태에 따라 기존의 2세대 무선시스템의 인증 프로토콜과 같이 대칭키 암호 알고리즘을 사용하는 방식[1, 2, 3, 13, 19]과 공개키 인증서 이용을 기반으로 한 공개키 암호 알고리즘을 사용하는 방식[4, 6, 11, 12, 18], 그리고 대칭키 알고리즘과 공개키 알고리즘을 둘 다 이용한 혼합형 방식[5, 17] 등이 있다. 공개키 암호 알고리즘은 대칭키 알고리즘에 비해 상대적으로 훨씬 많은 연산이 필요하지만, 공개키 인증서와 다양한 알고리즘의 적용으로 키 관리 측면에서 확장성을 제공하며, 다양한 보안 응용서비스의 제공이 가능하다. 근래에 암호 연산 마이크로프로세서를 장착한 스마트 카드 기술의 발전과 작은 키 값으로 안전하고 빠른 연산이 가능한 타원곡선 암호 기술의 발달로 무선이동통신구간에서의 공개키 알고리즘의 적용이 훨씬 용이해졌다[6, 12].

또한 프로토콜이 적용되는 네트워크 환경, 시스템 모델 및 관련되는 프로토콜 실체에 따라 무선접속구간 인증프로토콜과 단말이용자간 (end-to-end) 인증 프로토콜로 구분할 수 있다[16]. 2세대 무선시스템에서는 무선접속구간의 이용자와 네트워크간 보안서비스의 제공만

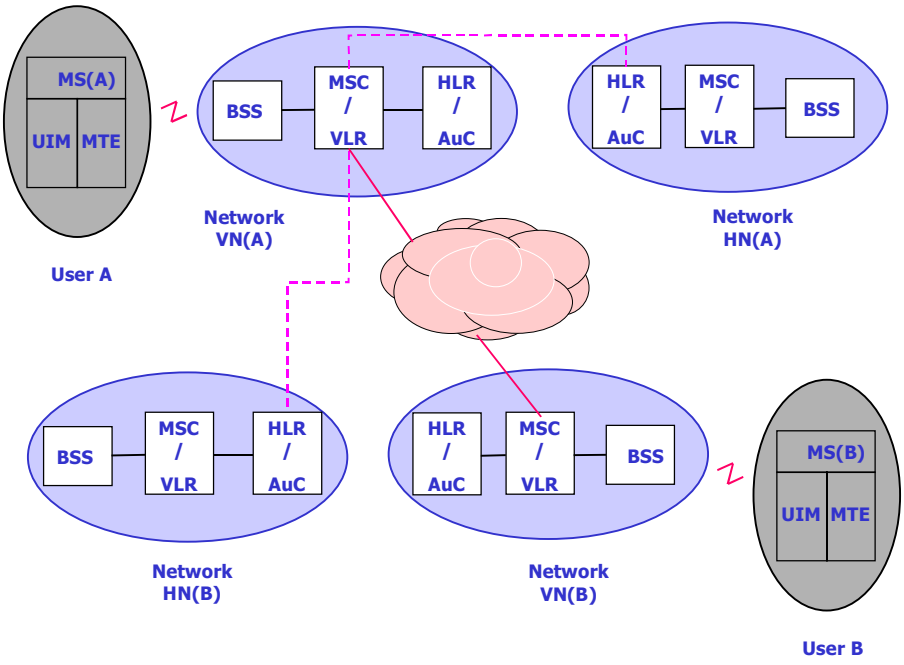
을 고려하였으며, 중간의 유선네트워크 구간은 안전하다고 가정하였다. 보안 프로토콜 설계시에도 전체 시스템에서 유선구간의 네트워크 실체들은 무선접속구간 보안 프로토콜 설계시에 부분적으로 고려되었으며, 유선네트워크 영역에서 이용자 데이터와 신호 데이터는 암호화되지 않는 평문 형태로 전송된다.

차세대 이동통신시스템에서 이용자 데이터의 기밀성을 보장하는 안전한 통신을 위해서는 무선접속구간 뿐만 아니라 두 단말이용자간(end-to-end) 데이터가 안전하게 전송될 수 있는 보안 메커니즘과 프로토콜 구성이 필요하다[16].

III. 네트워크 환경 및 시스템 모델

보안 프로토콜 구성과 관련하여 이동이용자가 서비스를 이용하는 네트워크 환경과 기능 시스템 모델 및 안전한 키 교환과 관련된 보안 모델을 설정한다.

로밍환경에서 서비스를 제공받는 이동이용자의 위치는 시간에 따라 변할 수 있다. 이용자는 현재 자신이 위치한 네트워크 관리영역에서 다른 네트워크 관리영역, 즉 다른 도메인의 상대 이용자와 통신을 수행할 수 있다. (그림 1)은 이동통신시스템의 네트워크 상호간 단말이용자 통신 환경을 보여준다. 홈 네트워크 (*HN*)는 응용서비스를 제공받기 위해 이용자가 초기 가입한 네트워크이며, 방문 네트워크 (*VN*)는 로밍 환경에서 네트워크간을 이동하는 이용자에게 현재 위치에서 서비스를 제공하는 네트워크이다.

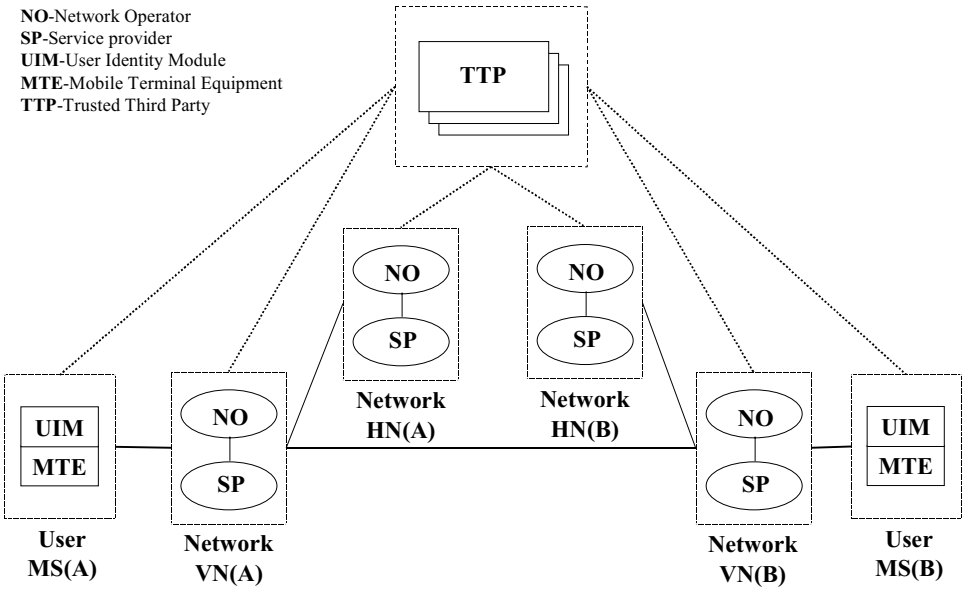


(그림 1) 네트워크 상호간 단말이용자간 통신 환경

보안 프로토콜 설계에서 고려해야 할 보안 구조와 관련된 기능적인 시스템 모델을 가정한다. 차세대 이동통신시스템 보안구조의 프로토콜에 참여하는 통신 실체는 스마트 카드와 같은 이용자신분모듈 (UIM) 과 이동단말(MTE), 네트워크 운용자 (NO) 와 서비스 제공자 (SP),

그리고 제 3의 신뢰기관(TTP) 등이 있다. 본 고에서는 기능 시스템 모델의 프로토콜 실체를 이용자, 네트워크, 그리고 제3의 신뢰기관 (TTP) 등 세가지로 한정한다. 이용자는 UIM 과 MTE 가 결합된 실체이며, 네트워크는 NO 와 SP 가 결합된 실체이다. 이용자 실체의 UIM-MTE간, 네트워크 실체의 NO-SP간의 세부 보안 메커니즘과 보안 파라미터는 고려하지 않는다. 보안구조와 관련된 기능 시스템 모델을 (그림 2) 에 나타내었다.

차세대 이동통신시스템에서 일부 보안 서비스 제공 및 보안 서비스 초기화는 제 3의 신뢰기관 (TTP) 에 의존한다고 가정한다. TTP가 시스템 보안구조의 일부분이 됨으로써 시스템의 신뢰성과 확장성에 상당한 이점을 제공할 수 있다. TTP는 상호 인증이 필요한 실체들에 대한 공개키 인증서 발급 및 검증에 관여하지만, 이동통신시스템의 보안 프로토콜에 직접 참여하지는 않는다 (off-line).



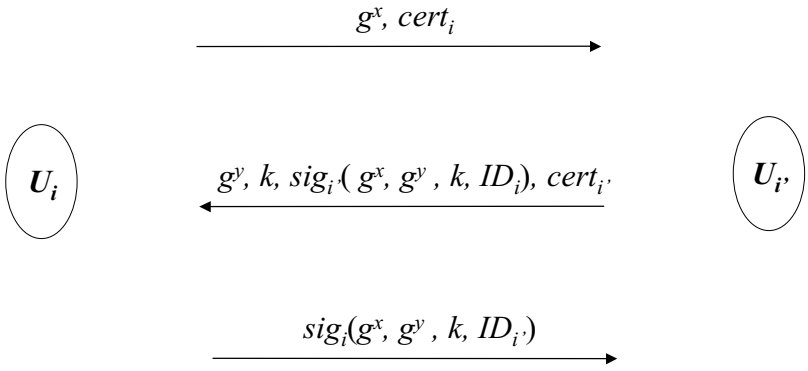
(그림 2) 보안구조 관련 기능 시스템 모델

다음은 인증 프로토콜상의 안전한 세션 키 설정과 관련하여 정형적인 보안 모델을 고려한다. 실체들간의 상호 인증과 안전한 세션 키의 설정은 대부분 동일한 프로토콜상에서 동시에 논의된다. 최근의 연구에서 오래 전부터 인증 및 키 설정 프로토콜의 정형적인 보안 모델에 대하여 많은 연구가 이루어졌으며, 몇 가지 모델이 제안되었다[7, 8, 9].

특히 [9]에서는, 실제 시스템과 이상적인 시스템의 보안 모델을 정의하고 두 시스템의 공격자에 대한 시뮬레이션 가능성(simulatability)에 의하여 키 교환 프로토콜의 안전성을 정의하였으며, Diffie-Hellan 키 교환 및 공개키 암호화 알고리즘을 기반으로 하는 안전한 키 교환 프로토콜 모델을 제안하였다.

본 고에서는 프로토콜 구성시에 [9]에서 제안한 Diffie-Hellman 기반 키 교환 프로토콜 중 (그림 3) 의 DHKE-2 모델을 기반으로 하여, 익명성 강화를 고려한 보안 서비스 제공에 중

점을 두고 보안 프로토콜을 구성하였다.



(그림 3) DHKE-2 키 교환 프로토콜 모델

Ⅳ. 네트워크 상호간 단말이용자를 위한 보안 프로토콜

앞에서 정의한 네트워크 환경과 시스템 모델, 그리고 안전한 키 교환에 대한 보안 모델을 고려한 이동통신 시스템의 보안 프로토콜을 제안한다. 프로토콜의 제안은 두 단계로 구분된다. 첫번째 단계는 무선접속구간에서 보안 프로토콜의 제안이고, 다음 단계는 두 이용자간 서비스 제공에 관계하는 네트워크 실체들을 고려한 무선 이동통신 환경에서 단말이용자간 (end-to-end) 보안 프로토콜의 구성이다.

1. 무선접속구간 인증 프로토콜

우선 이동 이용자와 네트워크간 무선 접속구간에서 공개키 암호 알고리즘을 이용한 인증 및 키 합의 프로토콜을 제안한다. 이동이용자가 서비스를 제공받는 네트워크 환경에 따라 무선접속구간의 인증프로토콜은 두 가지 형태로 구분할 수 있다. 이용자의 위치에 따라 홈 네트워크 관리 영역에 있는 경우와 방문 네트워크 관리 영역에 있는 경우이다. 이용자가 홈 네트워크에 있는 경우, 무선접속구간 인증 프로토콜은 이용자와 홈 네트워크 (*MS-HN*), 두개의 실체간의 메시지 교환이다. 한편, 이용자 로밍의 경우, 즉 이용자가 방문네트워크에 있는 경우에는 이동이용자와 방문 네트워크, 그리고 홈 네트워크 (*MS-VN-HN*) 세 실체간의 프로토콜 메시지 교환으로 구성된다. 본 고에서는 두가지 서비스 시나리오에 대한 프로토콜의 보안 메커니즘을 모두 고려한다.

인증 프로토콜의 설계에 있어서 각 실체에 대한 초기 가정은 다음과 같다. 공개키 인증서

와 관련하여 이용자와 네트워크는 상대 실체가 신뢰할 수 있는 신뢰기관(*TTP*) 이 발행하는 자신의 공개키 인증서를 가지고 있으며, 각각 상대 실체의 인증서 검증이 가능한 신뢰기관(*TTP*) 의 공개키를 가지고 있다. 홈 네트워크(*HN*) 는 서비스 가입시에 이용자에게 초기 임시신분(*TID*) 을 부여하고, 이용자와 홈 네트워크는 고유신분(*UID*) 과 초기 임시신분(*TID*) 을 저장한다.

다음은 프로토콜 제안에 인용한 기호와 그에 대한 설명을 나타낸다.

MS, *VN*, *HN*	이동 이용자와 방문네트워크, 홈 네트워크
p, *q*	큰 소수, *q*는 (*p*-*1*)을 나누는 소수 인수
G	큰 소수의 위수 *q*인 군(group)
$g \in G$	곱셈군 Z_p^*상의 위수 q인 군 *G* 에 대한 생성원
$r_A \in Z_q$	실체 *A* 가 랜덤하게 선택한 비트 스트링
$cert_A$	실체 *A* 의 공개키 인증서
x_A, g^{x_A}	실체 *A* 의 공개키 인증서의 개인키, 공개키
UID, *NID*	이용자와 네트워크의 고유신분
TID	이용자의 초기 임시신분
TID'	프로토콜 수행 후 새롭게 생성된 임시신분
H_j, H_k , H_l	쌍으로 존재하는 독립 해쉬함수
j, *k*, *l*	해쉬함수 지수, 랜덤하게 선택한 특정길이의 비트 스트링
K_{AB}	실체 *A*와 실체 *B*간에 합의된 세션 키
$sig_{x_A}(\bullet)$	실체 *A*의 서명값
$enc_{K_{AB}}(\bullet)$	합의된 세션키 K_{AB}를 이용한 대칭키 암호화

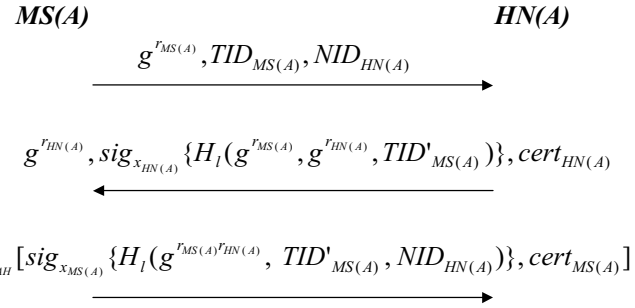
가. 무선접속구간 인증 프로토콜(Ⅰ) – *HN* 과 *VN* 이 동일한 경우

앞에서 설명한 서비스 제공 시나리오중에서 이용자가 홈 네트워크에 있는 경우, 즉 홈 네트워크와 현재 위치에서 서비스를 제공하는 방문 네트워크가 동일한 경우의 프로토콜 구성을 제시한다. 상호 인증과 임시 신분 생성 및 세션키의 합의에 대한 프로토콜 메시지 교환은 (그림 4)에서 보는 바와 같이 이용자와 홈 네트워크 (*MS*-*HN*), 두 실체간에 이루어진다.

첫번째 메시지에서 이동 이용자 *MS*(*A*)는 랜덤 비트 스트링 $r_{MS(A)}$ 를 선택, $g^{r_{MS(A)}}$ 를 계산하고, 임시 신분 $TID_{MS(A)}$ 및 $NID_{HN(A)}$와 함께 홈 네트워크 *HN*(*A*)로 보낸다. *HN*(*A*)는 데이터베이스를 검색하여 *MS*(*A*)가 정당한 가입자인지 확인한 후, 프로토콜을 계속 수행한다.

두번째 메시지에서 *HN*(*A*)는 랜덤 비트 스트링 $r_{HN(A)}$ 를 선택하여, $g^{r_{HN(A)}}$ 를 계산하고, $g^{r_{MS(A)}}$, $g^{r_{HN(A)}}$, *MS*(*A*)의 고유신분 $UID_{MS(A)}$ 을 이용하여 새로운 임시신분 $TID'_{MS(A)} = H_j(UID_{MS(A)}, g^{r_{MS(A)}r_{HN(V)}})$ 과 키 $K_{AH} = H_k(g^{r_{MS(A)}r_{HN(V)}}, g^{r_{MS(A)}x_{HN(V)}})$ 를 계산한다. 이후 $g^{r_{MS(A)}}$, $g^{r_{HN(A)}}$, $TID'_{MS(A)}$ 에 대한 서명값을 생성하고, $g^{r_{HN(A)}}$ 과 서명값, 그리고 자

신의 인증서 $cert_{HN(A)}$를 $MS(A)$로 보낸다. 이 과정에서 $g^{r_{MS(A)}}$, $TID'_{MS(A)}$ 에 대한 서명은 $MS(A)$에 대한 암시적인 신분확인 및 실체인증을 제공하고, $g^{r_{MS(A)}}$, $g^{r_{HN(A)}}$ 에 대한 서명은 암시적인 키 인증 및 이어지는 세션에서의 키 갱신을 보증한다.



$*\ MS(A)$ computes,

$$TID'_{MS(A)} = H_j(UID, g^{r_{MS(A)}r_{HN(A)}}), K_{AH} = H_k(g^{r_{MS(A)}r_{HN(A)}}, g^{r_{MS(A)}x_{HN(A)}})$$

$*\ HN(A)$ computes,

$$TID'_{MS(A)} = H_j(UID, g^{r_{MS(A)}r_{HN(A)}}), K_{AH} = H_k(g^{r_{MS(A)}r_{HN(A)}}, g^{r_{MS(A)}x_{HN(A)}})$$

(그림 4) 인증 프로토콜(Ⅰ) – HN 과 VN 이 동일한 경우

$MS(A)$는 두번째 메시지를 받았을 때, $g^{r_{MS(A)}}$, $g^{r_{HN(A)}}$, $UID_{MS(A)}$ 을 이용하여 새로운 임시신분 $TID'_{MS(A)}$과 세션키 K_{AH} 를 계산한 후, $HN(A)$의 인증서의 공개키를 이용하여 서명값을 검증하고, $g^{r_{MS(A)}}$, $g^{r_{HN(A)}}$, $TID'_{MS(A)}$ 와 $HN(A)$의 신분 $NID_{HN(A)}$의 해쉬값에 서명한 후, 서명값과 자신의 인증서 $cert_{MS(A)}$를 세션키로 암호화하여 세번째 메시지를 보낸다. 세번째 메시지에서 $MS(A)$는 $NID_{HN(A)}$에 서명함으로써 $HN(A)$에 대한 신분 확인을 제공하며, $g^{r_{MS(A)}}$, $g^{r_{HN(A)}}$, $TID'_{MS(A)}$ 에 서명함으로써 실체 인증과 명시적인 키 인증 및 키 갱신을 보증하고, 키 교환에 의해 설정된 세션 키 K_{AH}를 이용하여 메시지 및 인증서를 암호화하여 명시적인 키 확인 및 신분확인을 제공한다.

제안된 프로토콜의 실행이 끝난 후에 세션에 참여하는 통신 실체간 상호 실체 인증, 암시적인 키 인증에 의한 안전한 키 합의 및 키 확인, 세션별 키 갱신 보증, 그리고 이용자 익명성 등 이동통신 시스템의 인증 프로토콜 목표를 달성할 수 있다. [4]

프로토콜 초기에 임시 신분 $TID_{MS(A)}$에 의해 네트워크가 이용자를 확인하고, 프로토콜 실행 중 $UID_{MS(A)}$와 랜덤하게 선택한 비트 스트링을 입력으로 하는 해쉬함수를 이용하여

새로운 임시신분을 상호 계산하며, 새로운 임시신분 $TID'_{MS(A)}$을 다음 세션의 인증 프로토콜에 이용하여 임시신분의 세션별 갱신을 보증한다. 또한, 이용자의 고유 신분 $UID_{MS(A)}$은 무선접속구간의 프로토콜 메시지 교환 과정에서 누설되지 않기 때문에 이용자의 익명성을 보장한다.

나. 인증 프로토콜(Ⅰ)의 키 합의에 대한 안전성 분석

제안된 프로토콜(Ⅰ)은 랜덤하게 선택한 비트 스트링을 이용하는 도전-응답(challenge-response) 방식에 의한 Diffie-Hellman 기반 키 교환 프로토콜이다. DDH(decisional Diffie-Hellman) 가정과 서명 알고리즘, 암호학적 해쉬 함수, 대칭키 암호 알고리즘에 대한 안전한 암호 프리미티브를 선택시 안전한 키 교환 방식에 의한 인증 프로토콜이다[9].

제안된 프로토콜의 키 합의에 대한 안전성과 관련하여,본 고에서는 프로토콜에 참여하는 실체의 장기 비밀키(long-term secret key)를 얻을 수 있는 능동적인 공격자의 경우를 가정하였다. 제안된 프로토콜(Ⅰ)에서 공격자의 능동적인 공격방식에 안전할 수 있는 프로토콜의 보안특성을 분석한다[10].

1) 알려진 키에 대한 안전성(known session keys)

제안된 프로토콜은 이전 세션에서 사용되었던 세션 키를 알고 있는 공격자에 대하여 다른 세션에서 합의된 세션키에 대한 안전성을 보장한다. 프로토콜(Ⅰ)에서 합의된 세션키는 랜덤 수를 입력으로 하며, 세션별로 독립적으로 선택하는 랜덤 수의 변경에 따라 세션 키 역시 변경된다.

2) 전향적 보안성(forward secrecy)

프로토콜에 참여하는 실체의 장기 비밀값($x_{MS(A)}$ 또는 $x_{HN(A)}$)이 노출된 경우에도 이전 세션에 대한 안전성에 영향을 미치지 않는다[11]. 랜덤한 입력값에 의해 계산된 세션키 $K_{AH} = H_k(g^{r_{MS(A)}r_{HN(V)}}, g^{r_{MS(A)}x_{HN(V)}})$ 와 임시신분 $TID'_{MS(A)} = H_j(UID_{MS(A)}, g^{r_{MS(A)}r_{HN(V)}})$ 에서 DDH가정과 안전한 해쉬 함수의 사용을 가정하면 세션키 K_{AH}와 변경된 임시신분 $TID'_{MS(A)}$의 계산 및 확인이 불가능하다.

3)미지의 키 공유(unknown key-share)

프로토콜의 수행과정에서 공격자가 프로토콜의 중간에서 네트워크 *HN(A)*의 공개키 $g^{x_{HN(A)}}$를 알아내어, 신뢰기관에서 공개키 인증서를 발급 받은 후에 이용자 *MS(A)*와 프로토콜을 수행하며, 동시에 *HN(A)*로 하여금 *MS(A)*와 프로토콜을 수행하고 있다고 믿게 만드는 경우를 고려한다.

두번째 메시지에서 *HN(A)*이 서명문에 $TID'_{MS(A)} = H_j(UID_{MS(A)}, g^{r_{MS(A)}r_{HN(A)}})$ 을 포함시켜 송신하는 경우, 공격자가 $TID'_{MS(A)}$를 그대로 중계한다 할지라도 DDH가정에 의해 $TID'_{MS(A)}$에 포함된 *HN(A)*의 임시 비밀값 $r_{HN(A)}$ 을 이용한 세션키의 계산이 불가능하므로, 단지 중계 역할만 가능하며, 프로토콜의 세번째 메시지 내용을 알아낼 수 없으므로 프로토콜을 손상시킬 수 없다.

4)키 위장에 대한 안전성(key-compromise impersonation)

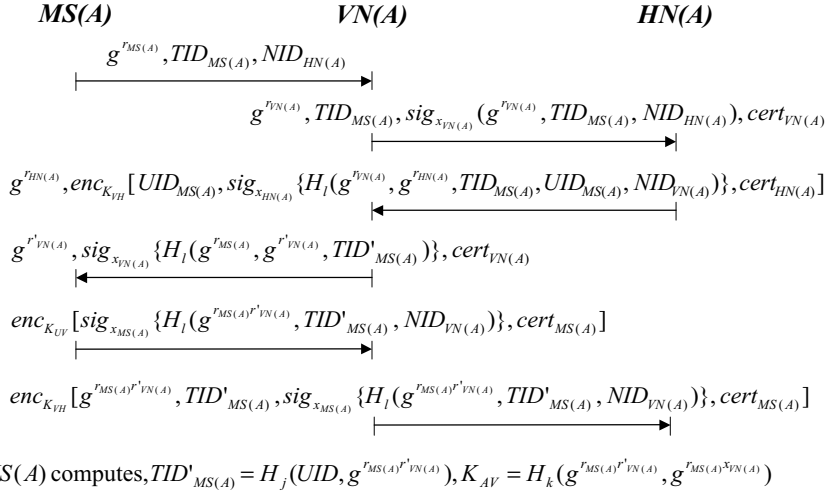
이용자 *MS(A)*의 장기 비밀값 $x_{MS(A)}$ 이 손상되어, 공격자가 네트워크 *HN(A)*에 대하여 *MS(A)*

로 위장하거나, *MS(A)*에 대하여 *HN(A)*로 위장하는 경우를 고려한다. 먼저 공격자가 *HN(A)*에 대하여 *MS(A)*로 위장하는 경우에, 공격자는 첫번째 메시지에서 유효한 $TID_{MS(A)}$를 제시할 수 없으므로 *HN(A)*에 의한 신분확인에서 실패한다. 또한 마찬가지로 공격자가 *MS(A)*에 대하여 *HN(A)*으로 위장하는 경우, 공격자는 *MS(A)*에 대한 $UID_{MS(A)}$를 알 수 없으므로 $TID'_{MS(A)}$를 계산할 수 없으며, 두번째 메시지를 수신한 후 *MS(A)*의 서명 검증시 실패하게 된다.

위에서 본 바와 같이 제안된 프로토콜은 능동적인 공격자의 이미 알려진 몇 가지 공격방식에 대하여 안전하다.

다. 무선접속구간 인증 프로토콜(Ⅱ) – *HN* 과 *VN* 이 다른 경우

한편, 이용자가 이동하여 방문 네트워크에 있는 경우, 즉 홈 네트워크와 방문 네트워크가 다른 경우의 무선접속구간 인증프로토콜(Ⅱ)를 (그림 5)에 나타내었다. 이용자 임시 신분확인 및 새로운 임시 신분의 생성에는 이용자와 방문 네트워크, 홈 네트워크 (*MS-VN-HN*)가 모두 관여하며, 안전한 세션키 설정과 인증된 메시지 교환을 위하여 이용자와 방문 네트워크간 (*MS-VN*), 방문 네트워크와 홈 네트워크간 (*VN-HN*) 보안 메커니즘이 필요하다.



(그림 5) 인증 프로토콜(Ⅱ) – *HN* 과 *VN* 이 다른 경우

*VN(A)*과 *HN(A)*간의 보안 메커니즘을 중심으로 프로토콜(Ⅱ)를 살펴보면 다음과 같다. 두번째 메시지에서 *VN(A)*는 *MS(A)*가 보낸 값 $TID_{MS(A)}$, $NID_{HN(A)}$와 자신이 계산한 값 $g^{r_{VN(A)}}$에 대한 서명값을 계산하고, 인증서 $cert_{VN(A)}$와 함께 *HN(A)*로 보낸다. 메시지 수신 후 *HN(A)*는 서명값을 검증하고, *MS(A)*의 임시신분에 대한 데이터베이스를 검색하여, 정당한 가

입자임을 잠정적으로 확인한다. 이후 *HN(A)*는 랜덤 비트 스트링 $r_{HN(A)}$ 를 선택하여 계산한 $g^{r_{HN(A)}}$ 과, $g^{r_{VN(A)}}$ 를 이용하여 *VN(A)*와 *HN(A)*간의 안전한 통신을 위한 세션키 $K_{VH} = H_k(g^{r_{VN(A)}r_{HN(V)}}, g^{r_{VN(A)}x_{HN(V)}})$ 를 계산한다.

세번째 메시지에서 *HN(A)*는 *VN(A)*에서 수신한 값과 자신의 계산값 $g^{r_{HN(A)}}$ 및 이용자 고유신분 $UID_{MS(A)}$ 과 이에 대한 서명값을 계산하고, 인증서 $cert_{HN(A)}$를 세션키 K_{VH} 로 암호화하여 *VN(A)*로 보낸다. *VN(A)*는 *HN(A)*로부터 메시지 수신 후 다른 랜덤 값 $r'_{VN(A)}$를 선택하여 $g^{r'_{VN(A)}}$ 를 계산하고, $g^{r_{MS(A)}}$, $g^{r'_{VN(A)}}$, $UID_{MS(A)}$ 를 이용하여 새로운 임시신분 $TID'_{MS(A)} = H_j(UID_{MS(A)}, g^{r_{MS(A)}r'_{VN(A)}})$ 를 계산하고, *MS(A)*와 메시지 교환을 계속하며, 그 과정은 프로토콜(Ⅰ)과 유사하다. 마지막 메시지에서 *HN(A)*는 이용자의 서명값을 검증하여 고유신분을 명시적으로 확인하며, 이전 임시신분을 새로운 임시신분으로 갱신한다.

프로토콜(Ⅱ)에서 프로토콜(Ⅰ)과 다른 점은 이동이용자 *MS(A)*의 신분확인을 위해 방문 네트워크 *VN(A)*와 홈 네트워크 *HN(A)*간의 프로토콜 메시지 교환이 수행되는 보안 메커니즘이 필요하다는 것이다. 이용자 임시신분의 확인 및 갱신은 *MS(A)*와 *VN(A)*간, *VN(A)*와 *HN(A)*간에 수행되며, 이 과정에서 *VN(A)*은 중간에서 인증된 메시지의 확인 및 전달자의 역할을 한다. *VN(A)*와 *HN(A)*간의 메시지 교환시에는 상대 실체의 상호인증과 안전한 세션키의 설정 및 새로 생성된 *MS(A)*의 임시신분 $TID'_{MS(A)}$ 의 기밀성을 유지하기 위하여 프로토콜(Ⅰ)과 유사한 보안 메커니즘을 이용한다.

2. 무선이동통신 단말이용자간(end-to-end) 보안 프로토콜

무선이동통신 서비스환경에서 두 이용자 *MS(A)*와 *MS(B)*간에 주고 받는 데이터의 기밀성을 보장하는 보안서비스를 제공하기 위해서는 단말이용자간 상호 인증 및 안전하고 인증된 세션 키를 설정하는 보안 프로토콜이 필요하다.

가. 단말이용자(end-to-end)간 보안 프로토콜(Ⅲ) 구성

앞에서 제안한 무선접속구간 인증 프로토콜(Ⅰ), (Ⅱ)를 기반으로 하여 서로 다른 네트워크에 있는 무선이동통신 단말이용자간(end-to-end) 안전한 통신을 위한 보안 프로토콜을 제안한다.

(그림 1)의 네트워크 환경에서 이동이용자 *MS(A)*는 자신의 홈 네트워크 *HN(A)*에서 이동하여 현재 서비스를 제공하고 있는 방문 네트워크 *VN(A)*에서 서비스를 받고 있으며, 다른 시스템 관리영역에 속하는 방문 네트워크 *VN(B)*에서 서비스를 제공받는 홈 네트워크가 *HN(B)*인 이동이용자 *MS(B)*와 호를 설정하고 데이터를 주고 받기를 원한다고 가정한다.

기존의 이동통신 시스템에서 *MS(A)*와 *MS(B)*간의 호 설정 경로는 *MS(A)-VN(A)-HN(A)-HN(B)-VN(B)-MS(B)*의 순으로 구성된다. 그러나 차세대 이동통신 시스템에서 최적 경로 설정방식을 적용했을 때의 호 설정 경로는 *MS(A)-VN(A)-VN(B)-MS(B)*의 순으로 구성될 수 있다[22]. (그림 2)의 보안구조 관련 기능 시스템 모델에서 두 이용자간의 호 설정 절차를 고려하여 보안 프로토콜을 구성한다.

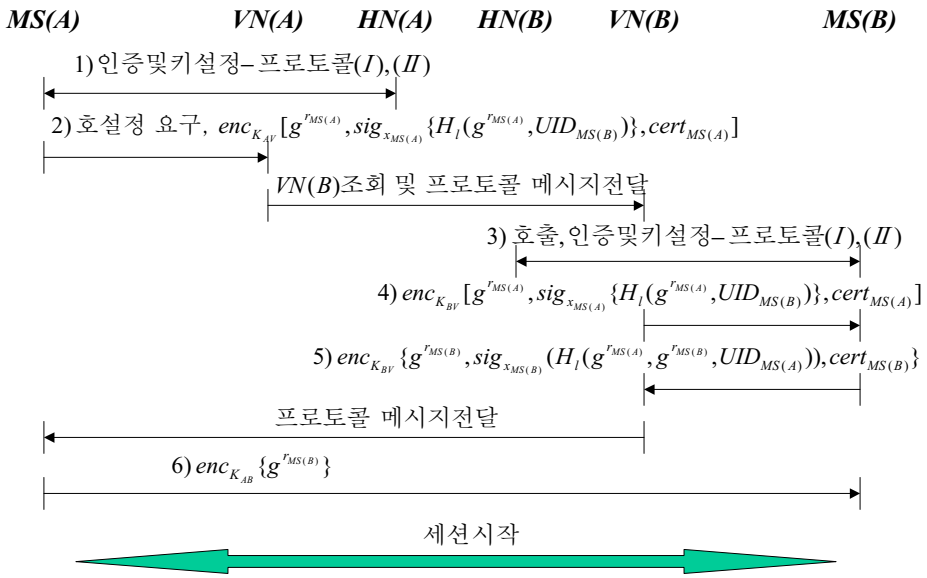
호 설정 절차를 단계별로 설명하면 다음과 같다. *MS(A)*와 *VN(A)*간에 초기 무선채널이 설정된 후, *MS(A)*는 *VN(A)*에게 *MS(B)*로의 호 설정을 요구한다. *VN(A)*는 *HN(B)*에 현재 *MS(B)*의

*VN(B)*를 조회하여 알아낸 다음 *VN(B)*로 호 설정 요구를 전달한다. *VN(B)*가 *MS(B)*를 호출하고, 할당된 무선채널을 통하여 호 설정요구가 전달되면, *MS(A)*와 *MS(B)*간의 연결이 설정된다. 단계별 보안 프로토콜 구성 과정을 (그림 6)에 나타내었다.

각각의 호 설정 단계에 따라 보안 프로토콜을 구성하면 다음과 같다.

1) *MS(A)*-*VN(A)* : 인증 및 키 설정 - 프로토콜(Ⅰ) 또는 (Ⅱ)

*MS(A)*와 *VN(A)*간에 초기 무선채널이 설정되면, 앞에서 제안된 프로토콜(Ⅰ), (Ⅱ)를 이용하여 *MS(A)*와 *VN(A)*간에 무선접속구간에서의 상호 인증 및 인증된 키 설정 프로토콜을 수행한다.



(그림 6) 단말이용자간(end-to-end) 보안 프로토콜(Ⅲ)

2) *MS(A)*-*VN(A)* : 호 설정 요구 및 보안 파라미터 전달

MS(A)-*VN(A)*간에 1)의 과정이 성공적으로 수행되면 *MS(A)*는 *VN(A)*에게 *MS(A)*-*MS(B)*간 호 설정을 요구하는 메시지를 전송한다. 호 설정 요구시 *MS(A)*는 *MS(B)*와 인증 및 키 설정을 위해 랜덤 비트 스트링 $r_{MS(A)}$를 선택, $g^{r_{MS(A)}}$를 계산하고, $g^{r_{MS(A)}}$, $UID_{MS(B)}$에 대한 서명값을 계산하여, 인증서 $cert_{MS(A)}$와 함께 세션 키 K_{AV}를 이용 암호화하여 *VN(A)*로 보낸다. *VN(A)*는 수신한 메시지를 복호화하고, 현재 *MS(B)*의 *VN(B)*를 *HN(B)*에 조회하여 알아낸 다음 *VN(B)*로 전달한다.

VN(A)-*HN(B)*간 *VN(B)*에 대한 조회와 *VN(A)*-*VN(B)*간 *MS(A)*의 메시지 전달에 대한 보안서비스 제공은 서로 다른 네트워크 시스템 관리 영역간 합의된 보안 메커니즘에 의존한다고 가정한다.

3) *VN(B)*-*MS(B)* : 호출, 인증 및 키 설정 - 프로토콜(Ⅰ) 또는 (Ⅱ)

호 설정 요구 메시지 수신 후, *VN(B)*는 할당된 무선채널상에서 *MS(B)*를 호출하는데, 이 과정에서 *VN(B)*-*MS(B)*간 프로토콜(Ⅰ), (Ⅱ)를 이용한 상호인증 및 인증된 키 설정 프로토콜을 수행한다.

4) *VN(B)*-*MS(B)* : *MS(A)*의 보안 파라미터 전달

VN(B)-*MS(B)*간에 3)의 과정이 성공적으로 수행되면 *VN(B)*는 *MS(B)*에게 *MS(A)*와의 상호 인증 및 키 설정에 필요한 *MS(A)*의 보안 파라미터, 즉 $g^{r_{MS(A)}}$와 $g^{r_{MS(A)}}$, $UID_{MS(B)}$에 대한 서명값 및 $cert_{MS(A)}$를 K_{BV}로 암호화하여 전달한다.

5) *MS(B)*-*VN(B)*-*VN(A)*-*MS(A)* : *MS(B)*의 보안 파라미터 전달

*MS(B)*는 4)에서 수신한 메시지를 K_{BV}를 이용, 복호화하고, 서명값을 검증한다. 메시지 검증 후, 인증 및 키 설정을 위해 랜덤 비트 스트링 $r_{MS(B)}$를 선택하여 $g^{r_{MS(B)}}$와 세션 키 $K_{AB} = H_k(g^{r_{MS(A)}r_{MS(B)}}, g^{r_{MS(A)}x_{MS(B)}})$를 계산한 다음, $g^{r_{MS(A)}}$, $g^{r_{MS(B)}}$, $UID_{MS(A)}$에 대한 서명값을 계산하여, $g^{r_{MS(B)}}$, 서명값, 인증서 $cert_{MS(B)}$를 세션 키 K_{BV}로 암호화하여 *VN(B)*로 보낸다.

*VN(B)*는 수신 메시지를 *VN(A)*로 전달하며, *VN(A)*는 *MS(A)*에게 전달한다.

6) *MS(A)*-*VN(B)*-*VN(A)*-*MS(B)* : 보안 프로토콜 완료 및 세션 시작

*MS(A)*는 메시지 수신 후, 서명값 검증 및 K_{AB}를 계산하고, $g^{r_{MS(B)}}$를 K_{AB}로 암호화하여 *MS(B)*에 전송한다. *MS(B)*는 메시지 수신 후, 키 K_{AB}를 이용하여 복호화 및 $g^{r_{MS(B)}}$를 확인한다. 이 단계부터 네트워크 실체 *VN(A)*, *VN(B)*의 암호 알고리즘 연산은 필요하지 않으며, *MS(A)*와 *MS(B)*간의 상호 계산된 세션키를 이용한 암호 알고리즘 연산만으로 구성된다.

나. 프로토콜 비교 및 평가

최근에 이동통신시스템의 단말이용자간 안전한 통신을 위한 보안 프로토콜로 몇 가지 방식이 제안되었다. [12, 13, 17] 공유 비밀키와 대칭키 암호 기술을 이용하여 단말이용자간 암호화 키를 분배하는 방식 [13, 17] 과 인증서 기반의 공개키 암호 기술과 Diffie-Hellman 키 교환을 이용하여 키를 합의하는 방식 [12] 으로 구분할 수 있다. 본 논문에서 제안한 프로토콜(Ⅲ)과 이전에 제안된 단말이용자간 프로토콜들을 비교한 것을 (표 1)에 나타내었다. [12], [13], [17] 에서 제안된 프로토콜을 각각 [CSP97], [LHY99], [VM97]로 표시하였다.

[13] 에서는 GSM 시스템의 단말이용자간 데이터의 기밀성을 보장하는 보안 프로토콜에 대해서 네트워크간의 공유 비밀키를 이용하는 방식을 제안하고 있는데 두 이용자간 데이터 암호화를 위한 세션키 계산 방식만을 제안하고 있으며, 상대 이용자에 대한 신분확인 및 실체 인증은 고려하지 않았다. [17] 에서는 이용자 키 분배시에는 대칭키 암호기술을, 그리고 홈 네트워크와 방문 네트워크간 메시지 인증시에는 공개키 암호기술을 이용하였다. 그러나 착신측 단말이용자와 그 홈 네트워크간의 상호 인증은 고려되지 않았다. 한편, [12] 에서는 이용자의 홈 네트워크에서 발급한 이용자의 공개키 인증서와 Diffie-Hellman 키 교환 방식을 이용하여 각각의 방문 네트워크에 있는 두 단말이용자간 상호 실체 인증 및 인증된 세션키 설정방식을 제안하고 있다. 그러나, 무선접속구간에서 이동이용자와 네트워크간 인증 및 키 설정시 각 단말이용자의 홈 네트워크와 방문네트워크간, 즉 *HN*-*VN*간의 보안 메커니즘은 고

려하지 않았다.

(표 1) 단말이용자간 보안 프로토콜 비교

프로토콜 / 구성방식	VM97	LHY99	CSP97	프로토콜(Ⅲ)
세션키 설정 방식	키 분배	키 분배	키 합의	키 합의
암호화 방식	대칭키+공개키	대칭키	공개키	공개키
익명성 보장 여부	○	×	○	○
단말이용자간 상호 인증	○	×	○	○
이용자-홈 네트워크간 상호 인증	△	×	○	○
*HN-VN*간 보안 메커니즘 고려 여부	○	×	×	○

○ : 만족, △ : 부분만족, × : 불만족

프로토콜(Ⅲ)은 인증서 기반의 공개키 암호기술과 Diffie-Hellman 키 교환을 이용하는 서로 다른 관리영역의 네트워크에 있는 단말이용자간 안전한 통신을 위한 보안 프로토콜이다. 프로토콜(Ⅲ)의 무선접속구간의 이용자와 네트워크간에는 방문 네트워크와 홈 네트워크간의 보안구조를 고려하여 제안된 프로토콜(Ⅰ), (Ⅱ)를 이용하여 상호 인증 및 인증된 키의 안전한 설정이 이루어지며, 이를 기반으로 서로 다른 네트워크에 있는 두 단말이용자간(end-to-end) 상호 실체인증 및 인증된 키의 설정이 가능하다.

Ⅴ. 결론 및 연구과제

본 고에서는 인증서 기반 공개키 암호 기술과 Diffie-Hellman 키 교환을 기반으로 이동통신시스템의 무선접속구간에서의 이용자-네트워크간에 이용자 익명성과 상호 실체인증, 인증된 키 합의를 보장하는 프로토콜(Ⅰ), (Ⅱ)을 제안하였고, 이를 기반으로 서로 다른 네트워크에 있는 두 이동 단말이용자간의 안전한 통신을 위한 상호 인증 및 키 합의가 가능한 보안 프로토콜(Ⅲ)의 구성을 제안하였다.

프로토콜(Ⅰ), (Ⅱ)의 설계시에 이동통신시스템의 서비스 시나리오별 네트워크 환경에 적합한 안전하고 효율적인 인증 및 키 설정 프로토콜의 정형 모델에 대한 향후 계속적인 연구와 공개키 암호 알고리즘 이용에 따른 연산량을 고려하여 안전하고 효율적인 암호 기본요소, 즉 해쉬 함수, 서명 및 암호화 방식에 대한 적합한 선택이 필요하며, 프로토콜(Ⅲ)의 구성시에 두 이용자의 방문네트워크간 안전한 프로토콜 메시지의 전달과 관련하여 네트워크 시스템 관리 영역간 합의된 보안정책에 대한 연구가 필요하다. 또한 제안된 보안 프로토콜 구성에서 이용자 데이터의 기밀성 유지와는 상반된 보안특성이긴 하지만, 통신로상의 중대 범죄 방지 또는 국가 보안을 위해 특정한 경우에 정부 기관에 의한 합법적인 도청을 가능하게 하는 안전한 키 위탁 및 키 복구 메커니즘을 고려가 필요하며, 이는 앞으로의 연구 과제이다.

참고문헌

[1] M. Y. Lee, CDMA cellular mobile communications network security, Prentice Hall PTR, 1998.

[2] GSM 03.20 version 6.0.1, Digital cellular telecommunications system (Phase 2+): Security related network functions, release 1997.

[3] A. Mehrotra and L.S. Golding, " Mobility and Security Management in the GSM System and some Proposed Future Improvements", Proceedings of the IEEE, Volume 86, Issue 7, pp. 1480-1497, July 1998.

[4] G. Horn, K.M. Martin and C.J. Mitchell," Authentication Protocols for Mobile Network Environment Value Added Services", available as http://isg.rhbnc.ac.uk/cjm/ - Listofpublications

[5] H.Y. Lin and L. Harn," Authentication Protocols for Personal Communication Systems", Proceedings of ACM SIGCOMM'95, pp. 256-261, August 1995.

[6] G. Horn and B. Preneel, " Authentication and Payment in Future Mobile Systems", Computer Security – ESORICS'98, Lecture Notes in Computer Science, 1485, pp. 277-293, 1998.

[7] M. Bellare and P. Rogaway, " Provably Secure Session Key Distribution - the Three Party Case", In 27th Annual ACM Symposium on Theory of Computing, pp. 57-66, 1995.

[8] M. Bellare, R. Canetti, and H. Krawczyk, " A Modular Approach to the Design and Analysis of Authentication and Key Exchange Protocols", In 30th Annual ACM Symposium on Theory of Computing, pp. 419-428, 1998.

[9] V. Shoup, " On Formal Models for Secure Key Exchange (version 4)", revision of IBM Research Report RZ 3120(April 1999), November 15, 1999.

[10] S. Blake-Wilson, D. Johnson, and A. Menezes, " Key Agreement Protocols and their Security Analysis", 6th IMA International Conference on Cryptography and Coding, LNCS 1355, pp. 30-45, 1997.

[11] D.G. Park, C. Boyd and S.J. Moon, " Forward Secrecy and Its Application to Future Mobile Communications Security", PKC 2000, Springer-Verlag, pp. 433-445, 2000.

[12] C.S. Park, " On Certificate-based Security Protocols for Wireless Mobile Communication Systems", IEEE Network Volume: 11 Issue: 5, pp. 50-55, Sept.-Oct. 1997.

[13] C.H. Lee, M.S. Hwang, W.P. Yang," Enhanced Privacy and Authentication for the Global System for Mobile Communications, Wireless Networks 5, pp. 231-243, 1999

[14] M.J. Beller, L. Chang and Y. Yacobi, " Privacy and authentication on a portable communications system, IEEE J. on Selected Areas in Comms. 11, pp. 821-829, 1993.

[15] L. Chen, D. Gollmann and C. Mitchell, " Tailoring Authentication Protocols to Match Underlying Mechanisms", Information Security and Privacy, Springer-Verlag LNCS 1172, pp.121 – 133, 1996.

[16] C. Boyd and A. Mathuria, "Key Establishment Protocols for Secure Mobile

Communications: A Selective Survey", Information Security and Privacy (ACISP98), Lecture Notes in Computing Science, Vol. 1438, Springer-Verlag, pp. 344-355, 1998.

[17] V. Varadharajan, Y. Mu, " Preserving Privacy in Mobile Communications: a Hybrid Method", IEEE International Conference on Personal Wireless Communications, pp. 532-536, 1997.

[18] K.H. Lee and S.J. Moon, " AKA Protocols for Mobile Communications", ACISP 2000, LNCS 1841, pp. 400-411, 2000.

[19] R. Molva, D. Samfat and G. Tsudik, " Authentication of Mobile users", IEEE Network , Volume: 8 Issue: 2 , pp. 26-34, March-April 1994.

[20] C.J. Mitchell, " Security in Future Mobile Networks", in Proceedings of the Second International Workshop on Mobile Multi-Media Communications (MoMuC-2), Bristol, April 1995.

[21] ETSI TS 122.101 V3.10.0, Universal Mobile Telecommunications System (UMTS); Service aspects; Service principles (3G TS 22.101 version 3.10.0 release 1999), 2000. 6.

[22] ETSI TS 122.079 V3.0.1, Universal Mobile Telecommunications System (UMTS); Support of Optimal Routeing (SOR); Service definition - Stage 1 (3G TS 22.079 version 3.0.1 release 1999), 2000. 1.