무선 네트워크 연동을 위한 키 관리

조 태 남[†] · 한 진 희[††] · 전 성 익[†††]

요 약

3G 이동통신, 무선랜은 각기 다른 장단점을 가지고 무선 통신 서비스를 제공하고 있다. 현재 이들 서비스의 단점들을 보완하도록 설계한 WiBro 서비스가 개발되었으며, 3중-모드로 작동하는 단말기를 이용하는 사용자가 세 개 망을 편리하게 사용할 수 있도록 하기 위한 3G-WLAN-WiBro 연동 시스템이 제안되었다. 각 망은 보안과 과금을 위하여 사용자와 네트워크 간의 상호 인증 절차를 도입하고 있으나, 서로 다른 인증 프로토콜을 사용하고 있다. 본 논문에서는 3G-WLAN-WiBro 연동 네트워크상에서, 사용자가 동일 사업자의 이종 망으로 이동할 때 이전망에서 사용하던 인증 정보를 활용하면서 새로운 망으로 안전하게 로밍할 수 있도록 지원하기 위한 통합된 인증 및 키 관리 프로토콜을 제안하였다.

키워드 : 무선 네트워크, 이동통신, 휴대인터넷, 인증, 키관리

Key Management for Wireless Interworking

Taenam Cho[†] · Jin-Hee Han[††] · Sung-Ik Jun[†††]

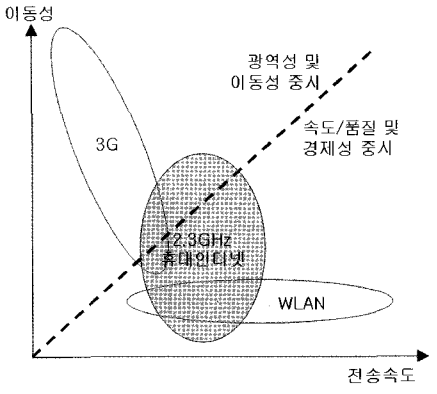
ABSTRACT

3G telecommunication and wireless LAN provide various wireless communication services with their own native advantages and disadvantages. Currently WiBro service was developed to make up for the disadvantages of those services, and 3G-WLAN-WiBro underworking system which enables a user who uses triple-mode terminals to use those three networks was proposed. Even though each network adopts mutual authentication process between users and networks to provide security and accounting, they use different authentication protocols. In this paper, integrated authentication and key management protocol is proposed which makes use of previously used authentication information and supports safe roaming when a user moves from one network to another one under a same service provider on the 3G-WLAN-WiBro interworking network.

Key Words : Wireless Network, Mobile Communications, WiBro, Authentication, Key Management

1. 서 론

기존의 이동통신 무선 망(3G)은 가입자 포화상태에 도달하였기 때문에 증가율이 둔화되는 추세이며, 가입자들은 데이터 서비스를 포함한 신규 서비스를 요구하고 있다. 또한 무선 기술의 발전에 힘입어 랜(LAN: Local Area Network) 기술이 무선랜(WLAN: Wireless LAN)으로 확장되었으며, 이러한 기술력을 토대로 2.3GHz 휴대인터넷(WiBro)이 탄생하였다. 이동통신 무선 서비스는 이동성이 높지만 전송속도가 낮고 요금이 비싸다. 반면에 WLAN 서비스는 높은 전송속도와 저렴한 요금이라는 장점을 갖지만 이동성이 낮다는 단점을 가지고 있다. WiBro는 WLAN에 비해 높은 이동성을 제공하고 3G 이동통신 서비스에 비해 높은 전송속도와 저렴한 요금을 목표로 하고 있다((그림 1) 참조)[1].



(그림 1) 3G, WLAN 및 WiBro의 비교

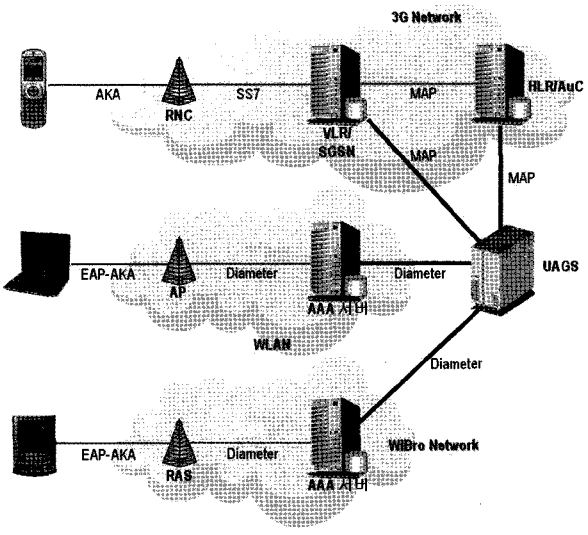
† 종신회원 : 우석대학교 정보보안학과 조교수
†† 정 회 원 : 한국전자통신연구원 무선보안응용연구팀 선임연구원
††† 정 회 원 : 한국전자통신연구원 무선보안응용연구 팀장
논문접수 : 2006년 11월 20일, 심사완료 : 2007년 1월 23일

높은 데이터 전송 속도와 이동성을 동시에 만족시키기 위한 또 하나의 방법으로서, 서로 다른 무선 망들을 연동하여 통합 무선 서비스 체계를 구축하려는 노력이 이루어지고 있다[2-5]. 이종 망을 연동하기 위해서는 인증, 키관리, 로밍/핸드오버 관리 등 여러 가지 측면에서 발생할 수 있는 보안상의 문제를 해결해야 한다[1]. 이러한 보안상의 문제들을 고려하고 기존 시스템의 변경을 최소화하도록 하는 USIM (Universal Subscriber Identity Module) 기반의 무선 네트워크 연동 구조가 제안되었다[6]. 이 연동 구조에서는 통합된 사용자 인증 체계를 지원하며, 이를 위하여 UAGS(USIM Access Gateway System)가 각 망에서의 인증 서버에 대한 프록시 서버 기능과 인증 프로토콜 변환을 수행한다. 본 논문에서는 동일한 사업자가 운영하는 3개 망을 연동하는 시스템에서, 사용자가 이종 망으로 이동할 때 통합된 인증을 위한 키 관리 프로토콜을 제안한다. 본 논문은 다음과 같이 구성된다. 2장에서는 본 논문이 기반하고 있는 연동 시스템의 구조 및 각 망에서의 인증 프로토콜을 설명한다. 3장에서는 연동 시스템에서의 키관리 프로토콜을 제안하고, 4장에서 제안 프로토콜의 안전성 및 효율성을 분석한다. 마지막으로 5장에서 결론을 맺는다.

2 3G-WLAN-WiBro 연동 구조 및 인증 프로토콜

2.1 연동 구조

본 논문에서 기반하고 있는 연동 구조는 (그림 2)와 같다. 이 구조는 기존의 각 3개 망의 변경을 최소화하도록 제안된 구조로서[6], 3G 망의 인증 센터인 HLR/AuC(Home Location Register/Authentication Center)를 이용하여 통합된 과금, 인증 및 로밍을 위해 필요한 정보를 관리한다. HLR/AuC는 인증에 필요한 정보와 보안을 위한 키재료(key material)인 인증벡터(AV: Authentication Vector)를 생성하여 3G망의 VLR/SGSN(Visited Location Register/Serving GPRS Support Node)과 WLAN과 WiBro 망의 AAA(Authentication, Authorization and Accounting) 서버로 전달한다. 사용자와 네트워크간의 상호 인증을 수행하는 주체인 VLR/SGSN과 AAA 서버는 HLR/AuC로부터 전달 받은 인증벡터를 이용하여 사용자와 네트워크간의 인증 프로토콜을 수행한다. 사용하는 인증 프로토콜은 서비스 망에 따라 다르다. 3G 망에서는 AKA(Authenticated Key Agreement) 프로토콜을[7,8] 사용하며, WLAN과 WiBro에서는 EAP-AKA(Extensible Authentication Protocol-Authentication Key Agreement)를 [9] 사용한다. 연동 시스템에서 통합된 서비스를 지원 받는 사용자는 3중-모드(3G, WLAN, WiBro를 모두 지원) 단말을 필요로 한다. (그림 2)에서 보는 바와 같이, VLR/SGSN과 HLR/AuC간에는 MAP(Mobile Application Part) 프로토콜을 사용하며, AAA 서버는 Diameter 프로토콜을[10] 사용한다. UAGS는 HLR/AuC와 AAA 서버간의 인증 벡터 송수신 시, 이들 간의 프로토콜 변환을 수행한다.



(그림 2) 연동 시스템 구조

2.2 AKA 프로토콜

본 절에서는 3G 망에서 인증 프로코콜로 사용하는 AKA 프로토콜을[7,8] 설명한다. AKA에서는 사용자와 네트워크가 사전에 공유한 키(preshared key) K를 가지고 있다. AKA 프로토콜을 이용한 인증 처리 흐름은 (그림 3)과 같다(부가적 설명을 위하여 각 단계에서 전송되는 메시지에 번호를 부여하였다). 인증은 크게 사용자 식별 단계((그림 3)에서 1~3단계), 사용자와 네트워크간의 인증 및 키 합의 단계(AKA 프로토콜 수행 단계로서 (그림 3)에서 4~15단계), 그리고 기지국 장치로의 키 전달 단계((그림 3)에서 16~17단계)의 3단계로 구성된다. 각 단계별로 처리흐름을 기술하면 다음과 같다.

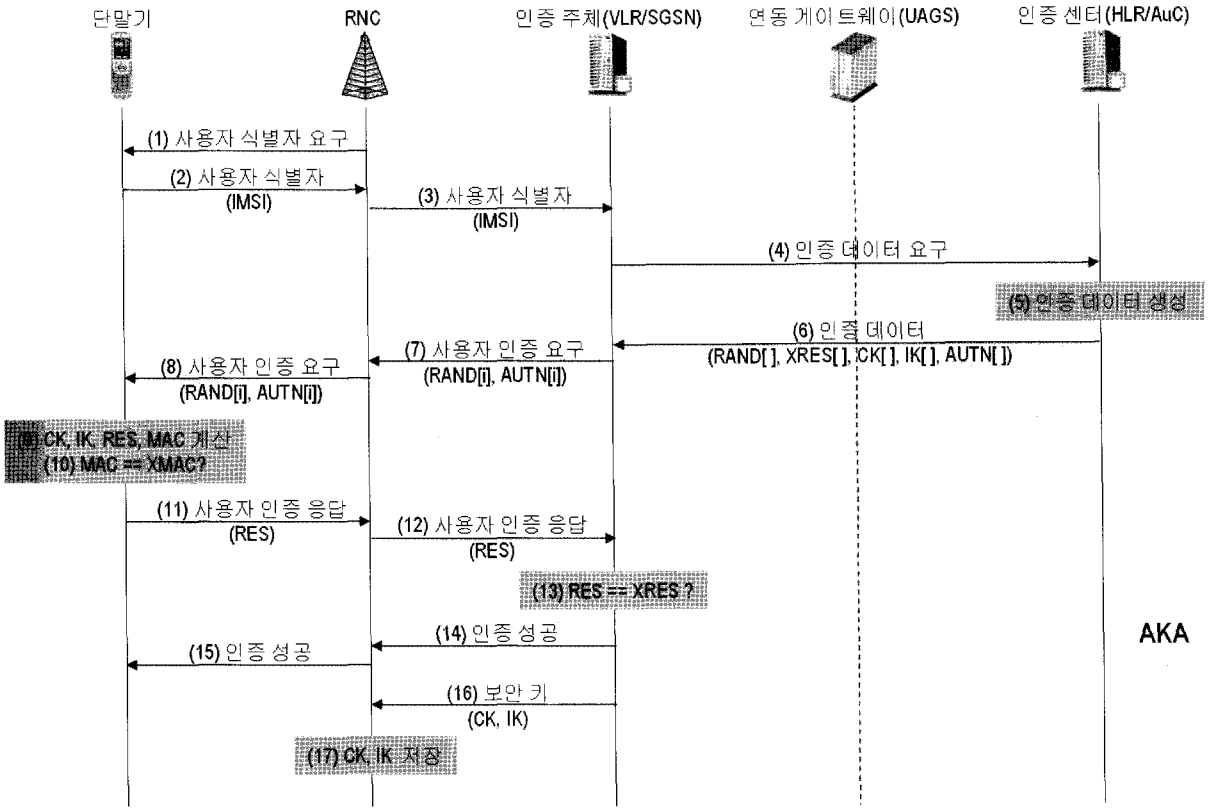
(1) 인증 주체(authenticator)인 VLR/SGSN이 사용자에게 식별자를 요구하면서 인증이 시작된다.

(2-3) 사용자의 단말기에 있는 USIM 카드는 사용자 식별자인 *IMSI*(International Mobile Subscriber Identity)를 [8,11] 기지국인 RNC(Radio Network Controller)를 거쳐 VLR/SGSN으로 보낸다. 이 때, 사용자의 식별자 보호를 위해 이후의 인증부터는 *TMSI*(Temporary Mobile Subscriber Identity)를 사용할 수 있다.

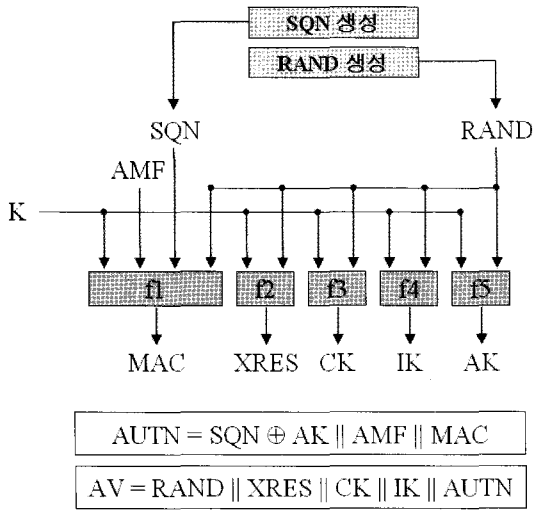
(4) VLR/SGSN은 인증 서버인 HLR/AuC에게 사용자 식별자에 해당하는 인증 데이터를 요구한다.

(5) HLR/AuC는 (그림 4)와 같이 랜덤값 *RAND*와 시퀀스 번호 *SQN*(SQuence Number)을 생성하고 사용자와의 공유키 K 등을 이용하여 *MAC*(Message Authentication Code), *XRES*(eXpedted RESponse), *CK*(Cipher Key), *IK*(Integrity Key) 및 *AK*(Anonymity Key)를 계산하여, 인증 벡터 *AV*를 생성한다.

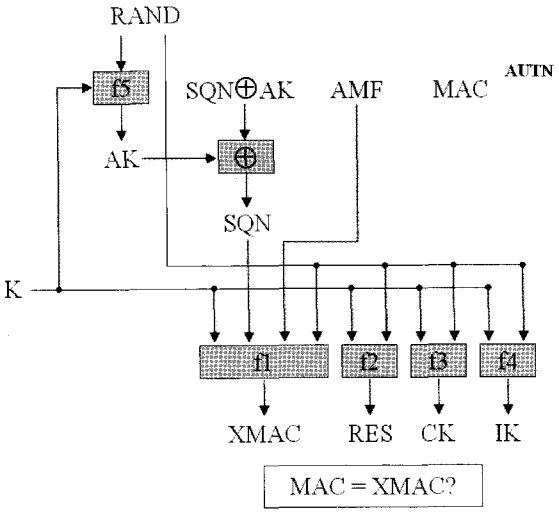
(6) 이 인증 벡터는 HLR/AuC의 부하를 줄이기 위하여, 한 번에 최대 5세트를 만들어 VLR/SGSN으로 전달한다 [8,12,13]. 이 때, *SQN*의 일부 비트는 여러 인증 벡터들을



(그림 3) AKA 프로토콜 흐름도



(그림 4) HLR/AuC의 인증 벡터 생성



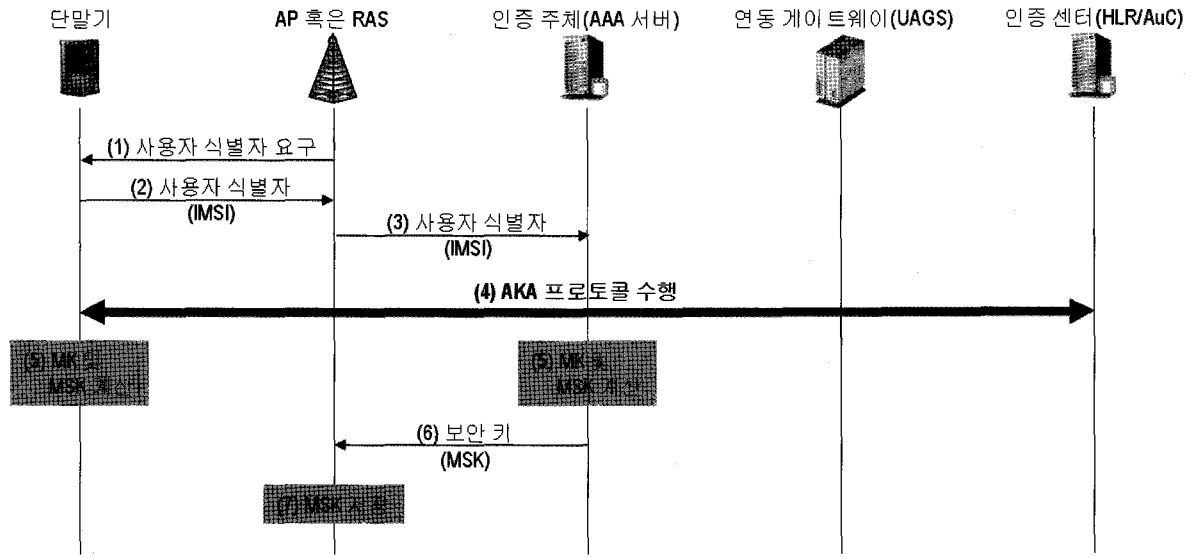
(그림 5) 사용자의 인증 벡터 검증

구분하는 식별자인 *KSI*(Key Set Identifier)로 사용된다 [14].

(7-8) VLR/SGSN은 HLR/AuC로부터 받은 인증 벡터 중 *RAND*와 *AUTN* 하나를 RNC를 거쳐 사용자에게 보낸다(VLR/AuC는 인증 프로토콜이 수행될 때마다 HLR/AuC로부터 받은 여러 개의 인증 벡터 중에서 하나씩 차례로 사용한다).

(9) 사용자는 수신한 *RAND*와 *AUTN* 및 *K*를 이용하여 (그림 5)에서와 같이 *CK*, *IK*, *RES* 및 *XMAC*(eXpected MAC)을 계산하고,

(10) 계산한 *XMAC*과 수신한 *AUTN* 내의 *MAC* 값이 같은지 비교함으로써 네트워크를 인증한다.



(그림 6) EAP-AKA 풀인증 프로토콜 흐름도

(11-12) 이 값이 일치할 경우 계산된 *RES*(RESponse)값을 RNC를 거쳐 VLR/SGSN으로 보낸다.

(13) VLR/SGSN은 사용자가 보낸 *RES* 값과 HLR/AuC로부터 받은 *XRES* 값이 일치하는지 확인하고,

(14-15) 일치할 경우, 인증 성공 메시지를 RNC를 통하여 사용자에게 전송함으로써 인증절차가 성공적으로 종료된다.

(16) 인증 프로토콜 AKA가 성공적으로 완료되면, VLR/SGSN은 RNC에게 *CK*와 *IK*를 전송한다.

(17) RNC는 *CK*와 *IK*를 저장하고, 이후의 사용자와의 데이터 통신에서 암호화와 무결성 검증 키로서 각각 *CK*와 *IK*를 사용한다.

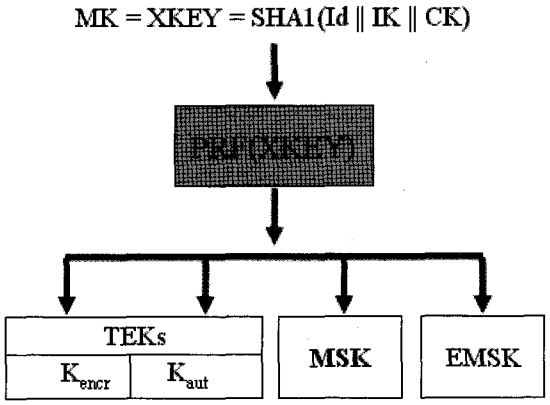
만약 단계 (10)에서 *MAC*과 *XMAC*이 일치하지 않거나, 단계 (13)에서 *RES*와 *XRES*가 일치하지 않으면 인증은 실패로 종료한다. 인증이 성공적으로 종료하면 사용자는 현재 위치를 식별하는 *LAI*(Local Area Identifier)를 네트워크에 요청하여 자신의 위치정보를 저장한다.

2.3 EAP-AKA 프로토콜

본 절에서는 WLAN과 WiBro 망에서 인증 및 키 설정 프로토콜로 사용하는 EAP-AKA 프로토콜을[9] 기술한다. EAP-AKA는 인증 및 키 분배 프로토콜로서 AKA를 사용하는 EAP(Extensible Authentication Protocol)[15] 메커니즘이다. EAP-AKA는 필수적인 풀인증(full authentication) 방법과 옵션인 빠른 재인증(fast re-authentication) 방법을 제공한다. 풀인증의 처리 흐름은 (그림 6)과 같으며, 각 단계별 수행 내용은 다음과 같다.

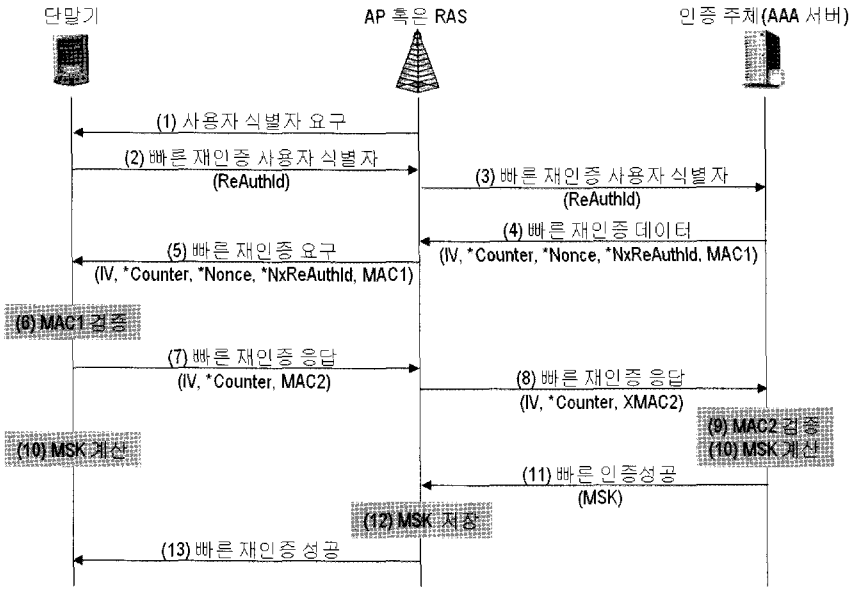
(1-3) 사용자 식별자 인식 후, AKA 프로토콜을 수행한다. 이 때, 사용자의 식별자 보호를 위해 *IMSI* 대신 Pseudonym을 사용할 수 있다.

(4) AAA서버가 HLR/AuC에게 인증 벡터를 생성을 요구하면, HLR/AuC는 인증벡터들을 생성하여 AAA서버로 전달한다. 인증벡터 생성 요구나 인증 벡터 전송 메시들은 프로토콜 변환을 위해 UAGS를 경유하게 된다. AAA 서버는 사용자와 AKA 프로토콜을 수행하여 상호 인증하고, *CK*와 *IK*를 서로 공유한다.



(그림 7) EAP-AKA 풀인증에서의 키 유도

(5) EAP-AKA에서는 *CK*와 *IK*를 데이터 통신에 이용하지 않고, 공유한 *CK*와 *IK*를 이용하여 새로운 키를 유도한다. (그림 7)에서와 같이 사용자와 AAA서버는 *CK*와 *IK* 및 사용자 식별자 *Id*를 파라미터로 하여 해쉬 알고리즘인 SHA1(Secure Hash Algorithm 1)을[16] 수행하고, 그 값으로 의사난수생성함수(PRF: Pseudo Random Function)를[17] 수행시켜 *MK*(Master Key)와 *MSK* (Master Session Key) 등 여러 가지 키들을 생성한다. 생성한 키들 중 X_{encr}과 X_{aut}은 인증 프로토콜의 메시지를 암호화하거나 무결성을 검증하기 위해 사용되는 키이다.



(그림 8) EAP-AKA 빠른 재인증 프로토콜 흐름도

(6) 키 생성이 완료되면, AAA 서버는 마스터 세션키인 *MSK*를 기지국인 AP(Access Point) 혹은 RAS(Radio Access Station)에게 전송하고,

(7) AP 혹은 RAS는 *MSK*를 저장한다. 이와 같이 공유한 *MSK*의 일부를 데이터 통신용 암복호화키나 무결성키로 사용한다.

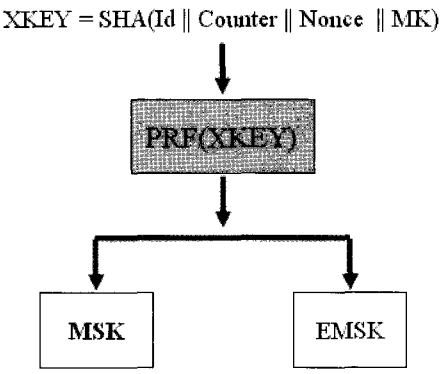
EAP-AKA에서는 인증 절차가 빈번하게 수행되는 환경에서의 효율적인 인증을 위해 빠른 재인증(fast re-authentication) 프로토콜을 옵션으로 지원한다. 빠른 재인증 프로토콜에서는 새로운 인증 벡터를 이용하지 않고, 풀인증에서 생성한 *MK*를 이용하여 서버와 사용자가 동일한 방법으로 다음 세션키인 *MSK*를 유도하여 공유한다. 앞에서 기술한 풀인증(full authentication) 프로토콜을 수행하기 위해서는 인증 센터인 HLR/AuC로부터 인증 벡터를 받아와야 하므로, 인증 센터의 계산 부하와 네트워크 부하를 줄이기 위한 방법이다. 빠른 재인증을 지원하려면, 풀인증 프로토콜에서 서버가 재인증용 식별자(next fast re-authentication identity)를 보냈을 경우에만 가능하다. 빠른 재인증의 처리 흐름은 (그림 8)과 같으며, 각 단계별 수행 내용은 다음과 같다.

(1) AP 혹은 RAS의 사용자 식별자 요구에 대하여,

(2) 사용자가 빠른 재인증용 식별자를 답변함으로써 프로토콜이 시작된다.

(3) AP 혹은 RAS이 사용자 식별자를 AAA서버로 전달하면,

(4-5) 서버는 암호화된 랜덤값 *Nonce*, 빠른 재인증 반복 횟수 *Counter*, 다음 빠른 재인증용 사용자 식별자 *NxReAuthId*와 암호화에 사용되는 초기화 벡터 *IV* (Initialization Vector), 그리고 메시지에 대한 인증 코드 *MAC1*을 사용자에게 보낸다. 그림에서 *은 암호화된 정보를 나타낸다.



(그림 9) EAP-AKA 빠른 재인증에서의 키 유도

(6) 사용자는 *MAC1*을 검증함으로써 네트워크를 인증한다.

(7-8) 검증에 성공하면 사용자는 수신한 *IV*와 *Counter*를 암호화한 값과, 이에 대한 인증 코드 *MAC2*를 서버에게 전달한다.

(9) 서버는 *MAC2*의 값을 확인함으로써 사용자를 인증한다.

(10) 검증에 성공하면 서버와 사용자는 (그림 9)와 같은 방법으로 새로운 *MSK*를 계산한다.

(11) 서버는 계산된 *MSK*를 AP 혹은 RAS로 전달하고,

(12) 사용자에게 인증이 완료되었음을 알린다.

3 연동을 위한 키 관리

본 논문에서 제안하는 키관리 메커니즘은, 사용자가 동일 사업자 망 내의 다른 망으로 이동할 경우에 기존에 생성된 인증 및 키 재료들을 효율적이고 안전하게 사용하기 위한 방법이다. 사용자의 이동 범위가 동일 사업자 망이라는 것은,

인증 벡터를 관리하는 HLR/AuC가 동일할 뿐 아니라 사용자와 HLR/AuC가 하나의 키를 공유하고 있다는 것을 의미한다. 즉, 동일한 사업자 망 내에서는 상호 인증을 위해 생성되는 인증 벡터가 동일함을 의미한다. 현재, 한 사업자의 3G 망 내에서 사용자가 이동할 경우, 이동하기 이전의 해당 VLR/SGSN이 새로운 지역의 VLR/SGSN에게 아직 사용되지 않은 인증 벡터들과 현재의 키들을 전송하도록 되어 있다[8]. 그러나 연동 시스템에서는 각 망에서 사용하는 키들이 상이하기 때문에 현재의 킷값을 전달하는 것만으로는 해결되지 않는다. 새로운 망으로 이동하였을 때, 별도의 절차 없이 HRL/AuC에게 새로운 인증벡터를 생성하도록 요구하고 기존의 인증 프로토콜을 수행할 수도 있다. 그러나 각 망에서 사용하는 상이한 키들은 동일한 파라미터로부터 생성되기 때문에, 이전망에서 생성된 인증 벡터들을 새로운 망에서 효율적으로 사용할 수 있다.

3.1 설계 개요

사용자가 동일 사업자의 이종 망으로 이동한 경우에 대한 키 관리 요구사항은 다음과 같이 요약될 수 있다.

(1) HLR/AuC의 계산량 및 통신량을 최소화하기 위하여, 로밍 이전망의 VLR/SGSN이나 AAA 서버에 저장된 인증 벡터들을 폐기하지 않고 활용할 수 있어야 한다.
(2) 사용자의 계산량을 최소화기 위하여, 새로운 인증 절차 없이 로밍 이전의 키를 사용할 수 있어야 한다.
(3) 로밍 후, 사용자가 올바른 키를 가지고 있음을 확인할 수 있어야 한다.
(4) 새로운 망으로 이동한 후에는, 이동망에 적합한 인증 키 및 인증 방식을 사용할 수 있어야 한다.
(5) 이전망으로 되돌아가거나 다른 새로운 망으로 이동하는 경우에도, 이동한 망의 인증 방식을 지속할 수 있어야 한다.

위와 같은 요구사항을 만족하기 위하여, 본 논문에서는 다음과 같이 키 관리 프로토콜을 설계하였다. 자세한 프로토콜 흐름은 다음 절에서 기술한다.

(1) HLR/AuC의 계산량 및 통신량 절감을 위하여, 이전망의 VLR/SGSN이나 AAA 서버에 저장되어 있으나 사용되지 않은 인증 벡터들을 이동망의 AAA 서버나 VLR/SGSN으로 전달한다.
(2) 사용자의 계산량을 최소화기 위하여, 이전망에서 사용하던 키들을 이동망으로 전송하거나, 이전망에서 사용하던 키들을 계산할 수 있는 키-재료들을 전송한다. 3개의 망에서 동일한 키를 사용하지는 않으나, *CK*, *IK*를 사용하거나 이로부터 유도한 *MSK*를 이용하고 있다. 따라서, 최근 *CK*, *IK* 및 EAP-AKA에서 사용될 수 있는 빠른 재인증 정보들을 전달한다.
(3) UAGS는 프로토콜 변환 뿐 아니라, 이전망에서 생성된 인증벡터들을 이동망으로 전달해 주는 역할도 수행한다.
(4) 이동망에서 키를 성공적으로 공유하고 나면, 새로운 위치정보를 단말기의 USIM 카드에 저장한다.

제안 프로토콜은 다음과 같은 사항을 전제하였다. 이 사항들은 AKA와 EAP-AKA 프로토콜에서 기반하고 있는 가정 사항들이다.

(1) 사용자의 단말기는 현재 위치하고 있는 위치 정보를 가지고 있다.
  - 3G망에서는 지역정보(LAI)와 임시 식별자로 자신을 식별한다[8,11].
  - WLAN과 WiBro망에서는 mobile IP 주소를 위치정보로 사용한다.
(2) UAGS는 단말기가 가지고 있는 지역 정보로부터 해당 VLR/SGGN이나 AAA 서버를 인식할 수 있는 매핑 테이블을 관리한다.
(3) 인증이 시작되면, 인증이 완료되거나 실패하기 전에는 로밍이 발생하지 않는다. 즉, 인증 프로토콜 수행 중에는 로밍이 발생하지 않는다. 만일 발생한다면 인증과정을 다시 실행한다.
(4) VLR/SGSN, AAA 서버 및 UAGS는 서로 신뢰한다.
(5) 인증 후, 사용자 및 인증 주체(VLR/SGSN 혹은 AAA 서버)는 사용된 키들(*CK*, *IK* 혹은 *MSK*)과 *KSI* 및 지역 정보를 다음 변경 때까지 캐싱하고 있다[8].
(6) 사용자와 기지국간의 무선 구간을 제외한 각 개체 간 구간에서의 통신은 안전한 채널을 통하여 이루어진다고 가정한다[8].

3.2 제안 프로토콜

제안 프로토콜은 현재 사용하고 있는 인증 프로토콜과의 일관성을 유지하고, 구현을 용이하게 하기 위하여, 기존 인증 프로토콜인 EAP-AKA와[9] AKA[7,8] 프로토콜을 확장하여 사용하도록 설계하였다. 사용자가 새로운 망으로 이동하면, 인증 프롤토콜에서와 같이 인증 주체가 "사용자 식별 요구" 메시지를 보낸다. 이 때 사용자는 응답 메시지로서 "로밍 요구" 메시지를 전송함으로써 로밍을 위한 키관리 프로토콜이 시작된다.

프로토콜의 단계별 처리 절차는 다음과 같으며 (그림 10)에 도식화하였다.

(1) 새로운 이동망의 인증 주체인 VLR_n/$SGSN_n$ 혹은 AAA_n이 사용자에게 사용자 식별을 요구한다.
(2-3) 사용자는 사용자 식별자 *Id*와 함께 이전망에서의 위치 정보 Loc_o를 기지국을 경유하여 VLR_n/$SGSN_n$ 혹은 AAA_n에게 전송한다. 사용자 식별자는 이전망에서 사용했던 Pseudonym이나 *TMSI*이며, 이전망에서의 위치 정보 Loc_o는 mobile IP이거나 *LAI*이다.
(4) VLR_n/$SGSN_n$ 혹은 AAA_n가 이전망에서의 인증 주체로부터 인증 벡터를 전달 받기 위해 UAGS로 수신한 메시지를 전달한다.

(5) UAGS는 수신한 위치 정보로부터 이전망의 인증 주체인 AAA_o 혹은 $VLR_o/SGSN_o$를 인식하고, 사용자의 식별정보를 AAA_o 혹은 $VLR_o/SGSN_o$로 전송한다.

(6) AAA_o 혹은 $VLR_o/SGSN_o$는 수신 정보로부터 사용자 정보를 검색하고, 사용자의 *IMSI*, 사용되지 않은 인증 벡터들, 사용 중이던 *CK*, *IK*, 연계된 *KSI*, *MSK*와 EAP-AKA에서 빠른 재인증에 필요한 정보로서 *Counter* 최종값, *NxReAuthId*를 UAGS로 전송한다. *MSK*와 빠른 재인증에 필요한 정보는 이전에 설정된 적이 없다면 생략된다. 만약 AAA_o 혹은 $VLR_o/SGSN_o$가 소유한 데이터베이스에 사용자 식별자가 없으면, 로밍은 실패로 종료한다.

(7) UAGS는 AAA_o 혹은 $VLR_o/SGSN_o$로부터 수신한 정보를 $VLR_n/SGSN_n$ 혹은 AAA_n 로 전달한다.

(8) 이동한 망이 WLAN이나 WiBro망일 경우, AAA_n 은(그림 7)에서와 같이 수신한 *CK*, *IK* 및 사용자 *Id*를 이용하여 *MSK*, K_{encr}, K_{aut}를 계산한다. 만약 수신한 *MSK*가 계산된 값과 다를 경우에는 빠른 재인증을 수행한 경우이므로, 수신한 값으로 대체한다.

(9) $VLR_n/SGSN_n$ 혹은 AAA_n 은 기지국으로 사용할 키 값들과 지역정보를 전송한다. 즉, $VLR_n/SGSN_n$은 *KSI*, *CK*, *IK*를 기지국에 보내고, AAA_n 은 *KSI*, *MSK*, K_{encr}, K_{aut}를 보낸다.

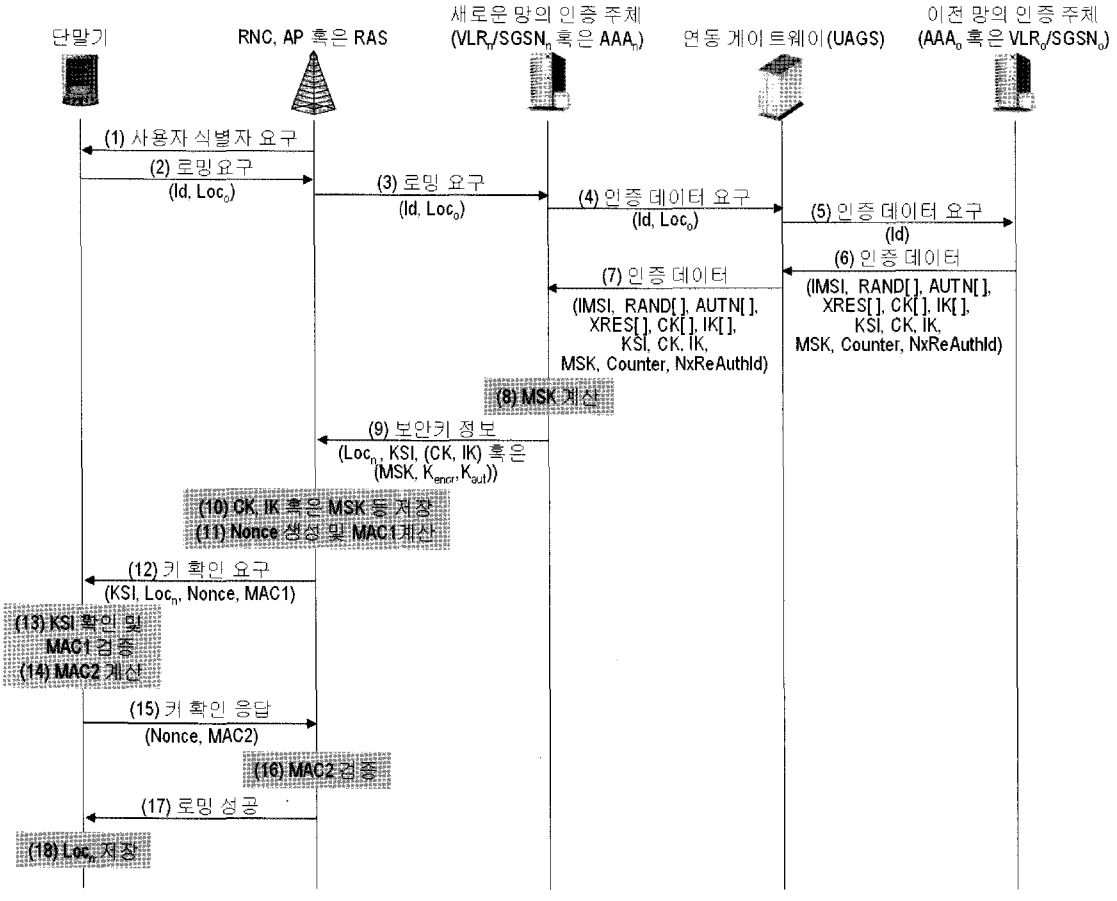
(10-12) 기지국은 수신한 키값들을 저장한 후, 랜덤값 *Nonce*를 생성하여 *KSI*, Loc_n, *Nonce*를 포함한 메시지를 구성한다. 또한 메시지에 대한 인증 코드 *MAC1*을 계산하여 메시지에 추가한다. *MAC1* 계산에 사용되는 키는, 이동한 망이 3G인 경우에는 *IK*를 이용하고 WLAN이나 WiBro망인 경우에는 K_{aut}을 이용한다. 생성한 메시지와 인증코드를 사용자에게 전송한다.

(13) 사용자는 수신한 *KSI*와 보유하고 있던 *KSI*가 일치하는지 확인한다. *KSI*가 일치하면, 대응되는 무결성 키(*IK* 혹은 K_{aut})로 *MAC1*을 검증한다. 만약 수신한 *KSI*가 소유한 *KSI*와 일치하지 않거나 *MAC1* 검증에 실패하면, 사용자는 로밍을 거부함으로써 로밍 실패로 종료한다.

(14-15) 검증이 성공한 사용자는 키 확인 응답 메시지를 만들고, 메시지 및 수신한 *Nonce*에 대한 인증 코드 *MAC2*를 생성하여 기지국으로 전송한다.

(16) 이를 수신한 기지국은 수신한 메시지와 (12)에서 보낸 *Nonce*에 대한 *MAC2*값을 검증한다.

(17-18) 검증 코드가 일치하면, 기지국은 로밍이 성공되었다는 메시지를 사용자에게 송신하고, 사용자는 (12)에서 받은 새로운 위치정보를 저장함으로써 로밍 절차가 완료된다.



(그림 10) 로밍을 위한 프로토콜 흐름도

4. 제안 프로토콜 분석

제안 프로토콜은 사용자가 이종 망으로 이동하였을 때, 기존의 인증 프로토콜을 새로 수행하지 않고 이미 생성된 인증 벡터를 새로운 망으로 이동시키고, 사용자가 가지고 있던 기존의 키를 그대로 사용할 수 있도록 하기 위한 프로토콜이다. 제안한 프로토콜은 인증 프로토콜의 안정성을 감소시키지 않으면서도, 이동망에서 기존의 인증 프로토콜을 다시 수행하는 것보다 HLR/AuC와 사용자의 계산량 및 전송량을 줄임으로써 효율성을 증대시키도록 설계하였다.

4.1 안전성 분석

본 절에서는 EAP-AKA의 안전성을 기준으로 제안 프로토콜을 분석한다.

(1) 사용자 식별자 보호(identity protection)

정규 인증 프로토콜에서는 사용자 가입 후 처음 인증 프로토콜을 수행할 때는 영구 식별자를 보냄으로써 사용자 식별자를 보호하지 못하고, 이후의 인증 프로토콜에서는 일회용 pseudonym이나 *TMSI*를 보냄으로써 사용자 식별자를 보호한다. 제안 프로토콜은 인증이 한번 이상 수행한 사용자가 이동할 경우에 대한 프로토콜이기 때문에, 영구 식별자를 사용하지 않고 pseudonym이나 *TMSI*만을 사용한다. 따라서 제안 프로토콜은 사용자 식별자를 보호할 수 있다.

(2) 상호 인증(mutual authentication)

제안한 프로토콜은 사용자와 네트워크가 이미 상호 인증을 수행한 후, 사용자가 이종 망으로 이동한 경우에 대한 키 관리 프로토콜이다. 따라서, 본 프로토콜을 통하여 상호 인증을 수행하기 보다는, 인증되지 않은 사용자나 네트워크가 인증된 사용자나 네트워크로 가장할 수 있는지를 분석하는 것이 적합할 것이다. 사용자는 여러 개의 키 세트를 가지고 있을 수 있기 때문에, 네트워크가 *KSI*를 보냄으로써 사용할 키를 확인한다. 사용자와 네트워크는 서로 공유하고 있는 무결성 키인 *IK* 혹은 K_{aut}으로 메시지에 대한 인증코드를 생성하여 송수신하고, 이를 검증함으로써 간략하게 상호인증한다.

(3) AuC 플러딩 공격(flooding AuC)

모든 인증 서버들은 HLR/AuC로부터 인증 벡터들을 가져와야 하기 때문에 HLR/AuC는 서비스 거부 공격(denial of service attack)의 대상이 될 수 있다. 이러한 이유로 EAP-AKA 표준은 AuC로의 트래픽을 제한하도록 권한다. 제안 프로토콜에서는 미사용된 인증 벡터를 이동한 영역의 서버로 전송함으로써 사용자의 이동으로 인한 HLR/AuC의 부가적 계산이 발생하지 않도록 하였다. 또한 인증 서버들이 UAGS를 통하여 인증 벡터들을 전송하도록 함으로써 HLR/AuC로의 트래픽을 생성을 방지하였다. UAGS는 이종 망간의 메시지에 대한 프로토콜 변환이 주요 기능으로서, 인증의 주요 계산을 담당하고 있는 HLR/AuC에 비하여 작업량이 적기 때문에 HLR/AuC을 경유하는 것보다 트래픽의 분산을 유도할 수 있다.

(4) 재생 공격(replay protection)

제안 프로토콜은 인증 프로토콜이 수행되고 나서 다음 인증 프로토콜이 수행되기 이전까지 두 번 이상의 이동이 발생할 수 있음을 가정하였다. "상호 인증" 분석에서 기술한 바와 같이, 사용자와 네트워크는 공유한 무결성 키로 메시지에 대하여 인증 코드를 생성하고 이를 검증한다. 무결성에 검증 키인 *IK*나 K_{aut}은 인증 프로토콜을 수행해야만 갱신된다. 로밍 후, 인증 프로토콜 수행 없이 다시 로밍이 발생할 경우에는 동일한 *KSI* 및 무결성 키를 사용하게 된다. 이로 인하여 제안한 프로토콜의 단계 12와 15에서 동일한 *MAC* 값이 생성된다면 재생공격이 가능하다. 이를 방지하기 위하여, 로밍 때마다 기지국은 새로운 랜덤값 *Nonce*를 생성하고 *MAC*을 계산할 때 *Nonce*가 포함되도록 하였다. 따라서 로밍으로 인한 재생 공격은 방지된다.

(5) 중간자 공격(man-in-the-middle attack)

인증 및 키 합의 프로토콜에 대한 표준 프로토콜인 AKA 및 EAP-AKA에서는 중간자 공격과 세션 가로채기 공격을 막기 위해서는 물리적으로 안전하지 않은 망에서는 무결성이 보장되도록 요구하고 있다. 본 논문에서 제안한 프로토콜은 AKA 및 EAP-AKA의 가정 사항에 기반하여 설계하였다. 따라서, 3.1절에서 기술한 바와 같이 사용자와 기지국 간의 무선 구간을 제외한 구간은 안전한 채널로 가정하고 있다. 제안 프로토콜에서 전송 무선 구간에서 송수신되는 정보는 *KSI*, 위치정보, 네트워크가 매번 새로 생성하는 *Nonce*로서 공개될 수 있는 값이며, 이들 정보를 포함한 메시지에 대하여 네트워크와 사용자만이 공유한 무결성 키로 인증코드를 태깅하여 보내기 때문에, 무선 구간에서의 중간자 공격은 불가능하다.

4.2 효율성 분석

서로 다른 서비스 특성과 사용자를 가지고 있는 각 무선망을 연동하려는 시도가 이루어지고 있다. 3G 이동통신과 WLAN 2개의 망을 연동하기 위한 규격들은 3GPP 그룹에서 제정하고 있고[2-5], 3G 이동통신과 WLAN 및 WiBro 망을 연동하기 위하여 한국전자통신연구원에서 그 구조를 제안하였다[6]. 그러나 3개 망의 연동 시스템에서의 로밍을 위한 키관리 프로토콜은 아직 제안된 바가 없다. 따라서, 제안 프로토콜의 효율성 분석을 통하여, 사용자가 다른 망으로 이동했을 때 이동망에서 독립적으로 인증을 수행하는 것보다 제안 프로토콜을 수행했을 때 효율성이 증대되었음을 보이고자 한다. 효율성은 통신량과 계산량에 대하여 HLR/AuC, UAGS 및 사용자의 측면에서 분석하였다.

(1) HLR/AuC 측면

제안 프로토콜이 기반하고 있는 연동 시스템에서는, 통합된 인증을 지원하기 위하여 하나의 HLR/AuC가 인증 정보를 생성하는 중앙 집중형 구조를 가지고 있다. 따라서 HLR/AuC의 계산량 및 통신량 증가는 연동 시스템의 성능 저하를 가져올 뿐 아니라, 이를 이용한 서비스 거부 공격에 취약해질 수 있다. HLR/AuC는 효율성을 위하여 한 번에 최대 5개의 인증 벡터를 생성하여 VLR/SGSN(혹은 AAA 서버)으로 전송하고, VLR/SGSN(혹은 AAA 서버)는 인증이 이루어질 때마다 HLR/AuC로의 통신없이 저장하고 있는 인증 벡터를 하나씩 사용한다[8,12,13]. 최악의 경우로서, 이전망의 VLR/SGSN(혹은 AAA 서버)에 저장된 5개의 인증 벡터가 다 사용되었고 최근 인증에 사용된 키들의 사용기간 만료된 경우라면, HLR/AuC가 새로 인증 벡터를 생성하고 이를 이동한 망의 VLR/SGSN(혹은 AAA 서버)로 전송하여 인증 프로토콜을 수행해야 할 것이다. 이것은 제안한 프로토콜을 사용하지 않고 기존의 프로토콜들을 별도로 수행하는 것과 동일하다. 그러나 이전망의 VLR/SGSN(혹은 AAA 서버)에 미사용된 인증 벡터들이 남아 있다면, 이전망의 VLR/SGSN(혹은 AAA 서버)은 제안 프로토콜을 이용하여 UAGS를 거쳐 이동한 망의 VLR/SGSN(혹은 AAA 서버)로 전송하게 된다. 이 경우 HLR/AuC는 추가의 인증 벡터 생성을 하지 않게 되며, 이동한 망의 VLR/SGSN(혹은 AAA 서버)이 HLR/AuC로부터 인증벡터를 가져오지 않아도 되기 때문에 HLR/AuC로의 통신도 발생하지 않는다. 따라서 제안 프로토콜에서 HLR/AuC의 계산량 및 통신량은, 최악의 경우에는 제안 프로토콜을 사용하지 않았을 때와 동일하며 그 외의 경우에는 효율성이 높아진다.

(2) UAGS 측면

만약, 이동한 망이 3G망이라면 기존의 인증 프로토콜을 이용하더라도 UAGS의 개입은 없을 수 있다. 그러나, 이 경우에는 새로운 인증 벡터의 생성을 위한 HLR/AuC의 계산량 및 통신량을 증가시킨다. 이동한 망이 WLAN이나 WiBro라면 기존의 인증 프로토콜을 이용하더라도 AAA 서버가 반드시 UAGS를 경유하여 인증 벡터를 수신해야 한다. 따라서 제안 프로토콜을 이용하여 UAGS가 이전망에서 이동한 망으로 인증 벡터 전송을 중계함으로써 발생하는 부가의 통신량과 계산량은 없다. 단, 이전망의 VLR/SGSN(혹은 AAA 서버)이 새로운 VLR/SGSN(혹은 AAA 서버)로 인증 벡터들을 전송해야 하는 부가의 작업이 필요하게 된다. 그러나 VLR/SGSN(혹은 AAA 서버)은 HLR/AuC의 작업량을 줄이기 위한 개체들로서, 제안 프로토콜에서도 HLR/AuC의 통신량을 분담하는 역할을 하게 된다.

(3) 사용자 측면

제안 프로토콜에서 사용자는 CK와 IK를 새로 계산하지 않고, 정당한 키를 소유하고 있음을 확인시키기 위해 MAC 값을 계산하고 검증하는 과정만 수행하게 된다. MAC의 계산 및 검증은 기존 프로토콜에서도 필요한 과정이기 때문에, 기존 프로토콜을 이용할 경우보다 통신량은 증가하지 않으면서 계산량이 감소하는 것으로 분석된다. 뿐만 아니라, 기지국과 VLR/SGSN(혹은 AAA 서버)과의 통신량도 감소한다.

5 결 론

3G 이동통신 서비스는 높은 이동성을 제공하고, WLAN은 전송속도와 저렴한 요금이라는 장점을 가지고 있다. 그러나 3G 서비스는 높은 요금과 낮은 속도라는 문제점을 가지고 있으며, WLAN은 이동성이 낮다는 단점을 가지고 있다. 이에 높은 전송속도와 이동성을 제공하기 위한 노력의 결과로 WiBro가 탄생되었으며, 이들 서비스를 일관된 방법으로 사용자가 제공받을 수 있도록 하기 위한 연동 시스템이 제안되었다. 각 서비스는 보안 및 과금을 위해 인증과정이 필수적으로 수행되어야 하며, 이종 망을 연동하기 위해서는 서로 다른 인증체계나 프로토콜을 통합 관리할 수 있는 방법이 필요하다. 본 논문에서는 3G-WLAN-WiBro 연동 네트워크상에서 사용자가 이종 망으로 이동했을 때 로밍 및 인증을 위한 키 관리 프로토콜을 제안하였다. 제안한 프로토콜은 사용자가 동일한 사업자의 이종망으로 이동하는 경우에 효율적이고 안전하게 인증이 이루어지도록 하였으며, 기존 인증 프로토콜의 안정성을 저하시키지 않고 HLR/AuC의 부가적 작업이나 통신이 발생하지 않도록 하면서 인증정보를 관리하는 키관리 프로토콜을 설계하였다.

참 고 문 헌

[1] 김종필, 한진희, 전성익, "무선 네트워크 연동에 다른 보안 취약성 및 그 대응 방안", NCS 2005, pp.13-16, 2005. 12.

[2] 3GPP TR 22.934, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on 3GPP System to Wireless Local Area Network(WLAN) Interworking," 3GPP, Sep., 2003.

[3] 3GPP TS 23.934, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System to Wireless Local Area Network (WLAN) Interworking; Functional and Architectural Definition," 3GPP, Jan., 2004.

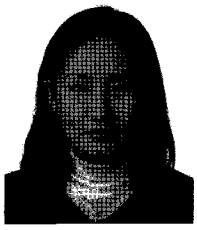
[4] 3GPP TS 23.234, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System to Wireless Local Area Network (WLAN) Interworking; System Description," 3GPP, Oct., 2006.

[5] 3GPP TS 33.234, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Wireless Local Area Network (WLAN) Interworking Security," 3GPP, Jun., 2006.

[6] 이정우, 전성익, "USIM 기반 통합 인증을 위한 USIM Access Gateway System 설계", NCS 2005, pp.17-21, 2005. 12.
[7] 3GPP TR 31.900, "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; SIM/USIM Internal and External Interworking Aspects," 3GPP, Mar., 2006.
[8] 3GPP TS 33.102, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture," Dec., 2005.
[9] J. Arkko and H. Hayerinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," IETF RFC 4187, Jan., 2006.
[10] P. Calhoun, J. Loughney, E. guttman, G. Zorn and J. Arkko, "Diameter Base Protocol," IETF RFC3588, Sep., 2003.
[11] 3GPP TS 23.003, "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering Addressing and Identification," 3GPP, Jun., 2006.
[12] 3GPP TS 23.008, "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Organization of subscriber data," 3GPP, Jun., 2006.
[13] 3GPP TS 29.002, "3rd Generation Partnership Project; Technical Specification Group Core etwork and Terminals; Mobile Application Part (MAP) Specification," Jun., 2006.
[14] 3GPP TS 24.008, "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile Radio Interface Layer 3 Specification; Core Network Protocols; Stage 3," 3GPP, Jun., 2006.
[15] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz, "Extensible Authentication Protocol (EAP)," IETF RFC3748, 2006. 6.
[16] National Institute of Standards and Technology, "Federal Information Processing Standard (FIPS) Publication 180-1, Secure Hash Standard," NIST Apr., 1995.
[17] National Institute of Standards and Technology, "Federal Information Processing Standards (FIPS) Publication 186-2 (with change notice); Digital Signature Standard (DSS)," NIST, Jan., 2000.

조 태 남

e-mail : tncho@ws.ac.kr
1986년 이화여자대학교 전자계산학과(이학사)
1988년 이화여자대학교 대학원 전자계산학과(이학석사)
1988년~1996년 한국전자통신연구원 선임연구원
2004년 이화여자대학교 과학기술대학원 컴퓨터학과(공학박사)
2004년~2005년 이화여자대학교 컴퓨터학과 전임강사
2005년~현재 우석대학교 정보보안학과 조교수
2006년~현재 한국전자통신연구원 무선보안응용연구팀 초빙연구원
관심분야 : 키 관리, 알고리즘 설계, 네트워크 보안 등



한 진 희

e-mail : hanjh@etri.re.kr
1997년 숭실대학교 정보통신공학과 (공학사)
1999년 광주과기원 정보통신과 (공학석사)
1999년~현재 한국전자통신연구원 무선보안응용연구팀 선임연구원
관심분야 : 스마트 카드, USIM, 무선 보안 기술 등

전 성 익

e-mail : sijun@etri.re.kr
1985년 중앙대학교 전자계산학과(공학사)
1987년 중앙대학교 전자계산학과(이학석사)
1997년~현재 한국전자통신연구원 책임연구원
2003년~현재 한국전자통신연구원 무선보안응용연구 팀장
관심분야 : 정보보호, 무선 보안, 실시간 운영체제, 스마트 카드 기술 등