UMTS를 위한 인증과 키 동의 프로토콜 설계

오가경, 김현성, 부기동
경일대학교 컴퓨터공학부
e-mail: kim@kiu.ac.kr

Design of Authentication and Key Agreement Protocol for UMTS

Ka-Kyung Oh, Hyun-Sung Kim, Ki-Dong Bu
School of Computer Engineering, Kyungil University

요 약

UMTS(Universal Mobile Telecommunications System)의 인증 및 키 교환 프로토콜은 기본적으로 3GPP(3 Generation Partnership Project)에서 제안한 UMTS AKA(Authentication and Key Agreement) 프로토콜을 표준으로 사용한다. 하지만 UMTS AKA 프로토콜은 네트워크 대역폭 소모, 저장 공간의 오버헤드, *SQN* 동기화 문제 등이 제기되고 있다. 본 논문에서는 UMTS AKA 관련 프로토콜들의 문제점을 분석하고 이를 해결하기 위한 전방향 안전성을 제공하는 F-AKA 프로토콜을 제안한다. 제안하는 프로토콜은 상호인증을 제공하고, 프라이버시를 강화하였으며 전방향 안전성을 보장한다.

1. 서론

3세대 이동 통신 기술 중의 하나인 UMTS (Universal Mobile Telecommunications System)는 3GPP에 의해 표준화되고 있다[1]. 이러한 무선 이동통신 서비스를 안전하게 제공하기 위해 보안 기술은 매우 중요하다[2]. UMTS는 크게 무선 구간에서의 엑세스 보안, 핵심 망에서의 보안, 사용자 영역에서의 보안 등으로 분류할 수 있다. 그 중 특히 보안에 취약한 무선구간에서의 엑세스 보안이 중요시 되고 있고 이를 위한 인증과 키 동의 과정이 필수적이다[3].

이로 인해 3GPP에서는 무선 구간에서의 안전한 통신을 위한 UMTS AKA 프로토콜을 개발하였다[3]. UMTS AKA 프로토콜은 사용자와 네트워크 사이의 상호 인증을 제공하고, 통신을 위한 암호화키와 무결성키를 확립시켜주는 인증 및 키 동의 프로토콜이다. 하지만 UMTS AKA는 대역폭 소모와 저장 공간의 오버헤드 문제, SQN 동기화 문제 등의 문제점들이 있다. 이 문제점들을 해결하기 위하여 UMTS X-AKA등이 제안되었다[4-5]. 하지만 Huang 등이 제안한 티켓기반의 UMTS X-AKA 역시 비밀키 k의 노출 시 통신의 안전성에 대한 문제가 제기되었다.

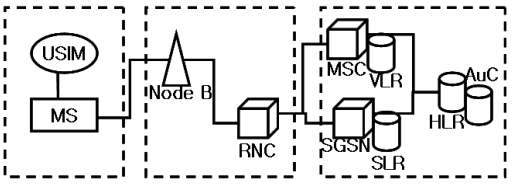
본 논문에서는 UMTS AKA와 UMTS X-AKA의 문제점들을 해결하고 두 프로토콜들의 장점만을 가지는 전방향 안전성을 제공하는 F-AKA 프로토콜을 제안한다.

2. 관련연구

본 장에서는 UMTS 네트워크 구조를 살펴보고, 3GPP에서 제안한 UMTS AKA[3] 프로토콜과 Huang 등이 제안한 UMTS X-AKA[4] 프로토콜에 대해 살펴본다.

2.1. UMTS 네트워크 구조

(그림 1)은 본 논문의 기반이 되는 UMTS 네트워크 구조를 보여준다[1].



(그림 1) UMTS 네트워크 구조

네트워크를 구성하는 각 요소는 다음과 같다.

- USIM(Universal Subscriber Identity Module) : 가입자의 비밀키 k와 가입자 식별값인 *IMSI*(International Mobile Station Identity) 등의 가입자 정보와 암/복호화 알고리즘 등을 저장하는 모듈이다.
- MS(Mobile Station) : USIM이 삽입되는 단말기이다.
- Node B(or Base station) : MS와 RNC 사이에 통신 연결을 담당하는 기지국이다.
- RNC(Radio Network Controller) : Node B와 SGSN (Serving GPRS Supporting Node) 또는 MSC/VLR (Mobile Switching Center/Visitor Location Register) 사이에서 서비스를 제어하는 서비스 엑세스 포인트이다.
- MSC/VLR : MSC는 회선 교환 서비스를 제공하고 VLR은 방문 가입자의 서비스 프로파일을 저장한다.
- SGSN : GPRS(General Packet Radio Service) 서비스 지역 내에서 패킷 교환 서비스를 제공한다.
- HLR(Home Location Register) : 가입자의 정보가 저

장되는 데이터베이스이며 가입자의 정보는 사용자가 가입할 때 저장된다.

- AuC(Authentication Center) : 가입자의 비밀키 k와 $IMSI$가 저장되어 있고 무선 통화 구간에 대한 암호화를 지원한다.

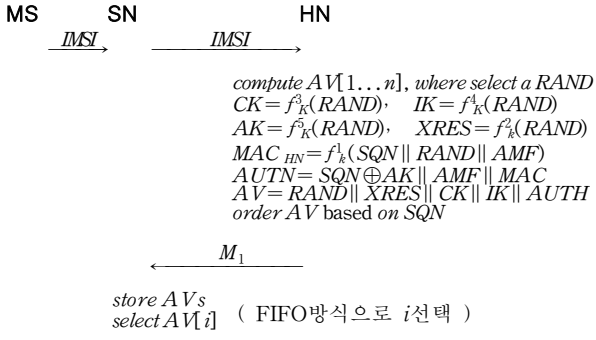
UMTS 네트워크의 모든 프로토콜에서는 MS의 USIM과 HN의 AuC가 서로 비밀키를 공유하고 있고, SN과 HN의 통신구간은 MAPsec(Mobile Application Part Security)이나 IPsec(IP Security)과 같은 네트워크 도메인 보안을 통해 서로 안전한 통신을 수행한다고 가정한다.

2.2. UMTS AKA 와 UMTS X-AKA 프로토콜

본 소절에서는 3GPP에서 제안된 UMTS AKA 프로토콜[3]과 Huang등이 제안한 UMTS X-AKA 프로토콜[4]에 대해 설명한다.

UMTS AKA : UMTS AKA 프로토콜은 MS가 SN에 서비스를 요청했을 때 HN을 통해 인증을 수행하고, MS와 SN사이에 안전한 통신을 위한 암호화키와 무결성키를 확립시켜주는 키 동의 프로토콜이다[3]. (그림 2)는 UMTS AKA 프로토콜의 인증 요청단계를 보여주고, (그림 3)은 UMTS AKA프로토콜의 인증 및 키 동의 단계를 보여준다.

인증요청을 받은 HN은 n개의 AV(Authentication Vector)를 생성하여 SN에게 보내고 SN은 AVs를 저장한다. SN은 i번째 AV를 선택하여 MS에게 M_2를 보낸다. MS는 SQN을 구한 다음 SQN의 유효성에 대해 검증하여 동기화를 수행한다. SQN이 유효하다면 MS는 M_3을 SN에게 보내고 SN은 RES와 $XRES$값을 비교하여 MS를 확인하고 서로 확립된 CK와 IK를 이용하여 안전하게 통신을 하게 된다.



(그림 2) UMTS AKA프로토콜 - 인증요청

UMTS X-AKA : UMTS X-AKA 프로토콜은 임시 키인 티켓키를 발급함으로써 대역폭 소비문제를 해결하고 저장 공간 오버헤드를 줄였다[4]. 먼저 MS는 $MAC_{MS}=f1_K(T_{MS})$을 계산하고 SN을 거쳐 HN에게 M_1을 전송한다. HN은 MAC_{MS}를 검증하고 TK와 MAC_{HN}을 생성한 다음 $AUTH_{HN}$을 만든다. HN은 SN에게 M_2를 전송한다.

$$M_1=\{IMSI, T_{MS}, MAC_{MS}\}$$
$$MAC_{HN}=f1_K(RAND_{HN} \| AMF)$$
$$TK=f^x_K(T_{MS})$$
$$AUTH_{HN}=MAC_{HN} \| RAND_{HN} \| AMF$$
$$M_2=\{AUTH_{HN}\}$$

SN은 N_{SN}을 생성하고 MAC_{SN}을 계산한 다음 $AUTH_{SN}$을 만든다. 그 후 SN은 MS에게 M_3을 전송한다.

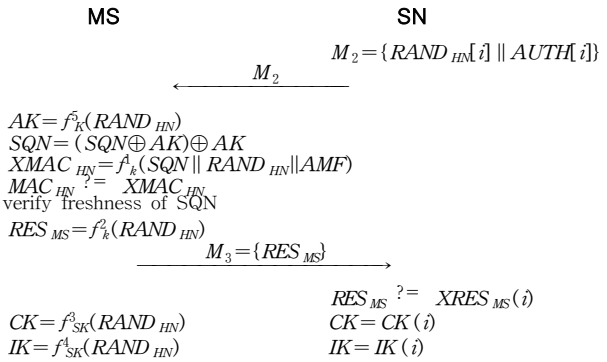
$$MAC_{SN}=f1_{TK}(MAC_{HN} \| RAND_{SN} + j \times RAND_{HN})$$
$$AUTH_{SN}=MAC_{SN} \| RAND_{SN} \| RAND_{HN} \| AMF \| j$$
$$M_3=\{AUTH_{SN}\}$$

MS는 MAC_{HN}과 MAC_{SN}을 검증하고 j번째가 맞는지 확인한다. MS는 SN에게 RES를 계산하여 M_4를 전송하고, SN은 $XERS$와 비교하여 RES를 검증한다.

$$RES=f2_{TK}(RAND_{SN})$$
$$M_4=\{RES\}$$

마지막으로 MS와 SN은 CK와 IK를 생성해 안전한 통신을 수행할 수 있게 된다.

$$CK=f3_{TK}(RAND_{SN})$$
$$IK=f4_{TK}(RAND_{SN})$$



(그림 3) UMTS AKA프로토콜 - 인증 및 키 동의 단계

2.3. 프로토콜의 분석

먼저 UMTS AKA는 AV들을 사용함으로 인해 SN과 HN 간의 대역폭 소모를 야기 시키고, SN의 저장 공간 오버헤드를 발생시키는 문제점이 있다. X-AKA는 AV들 대신에 티켓 키를 사용함으로써 이런 문제점을 해결 하였다.

그리고 UMTS AKA에서는 HN은 MS를 인증하지 못하고 MS만 HN을 인증하는 단방향 인증만을 제공한다. 하지만 X-AKA에서는 HN이 MAC_{MS}를 검증과, MS는 MAC_{HN}과 MAC_{SN}을 검증함으로써 MS와 HN, MS와 SN간의 상호 인증을 제공한다.

하지만 UMTS AKA와 UMTS X-AKA는 장기간 비밀키(long-term key)인 k가 노출되면 이전의 통신의 내용이 모두 유출될 수 있는 문제점을 가지고 있다. 특히, X-AKA에서는 단기간 비밀키(short-term key)인 TK가 노출 될 경우, TK를 이용한 이전의 통신 내용이 모두 노출지만, UMTS AKA에서는 AV들에 포함된 단기간 비밀키가 노출되더라도 다른 AV들에게 영향을 미치지 않는다.

또한 두 프로토콜 모두 프로토콜 수행의 초기 단계에서 $IMSI$값을 적어도 한번은 평문 형태로 전송하기 때문에 프라이버시에 대한 문제점도 있다.

3. 전방향 안정성을 제공하는 F-AKA 프로토콜

본 장에서는 기존에 제안된 UMTS AKA 관련 프로토콜들의 문제점을 해결하고 이들의 장점을 취할 수 있는, 전방향 안정성을 제공하는 F-AKA 프로토콜을 제안한다. 제안된 프로토콜은 티켓 기반 인증을 수행하고 MS와 HN 간의 쌍방향 인증을 제공한다.

본 논문에서 사용하는 프로토콜의 표기법은 (표 1)과 같다. 제안하는 프로토콜을 위해 다음을 가정한다. MS와 HN은 비밀키 k와 프라이버시 보호를 위해 사용하는 임시 ID인 TID_{MS}와 암호알고리즘을 공유하고 있고, SN과 HN은 IPsec이나 MACsec과 같은 네트워크 도메인 보안 메커니즘을 통해 안전한 통신을 한다고 가정한다. 또한 MS는 현재 자신이 속해 있는 SN의 ID인 ID_{SN}을 알 수 있다고 가정한다.

(표 1) 프로토콜 표기법

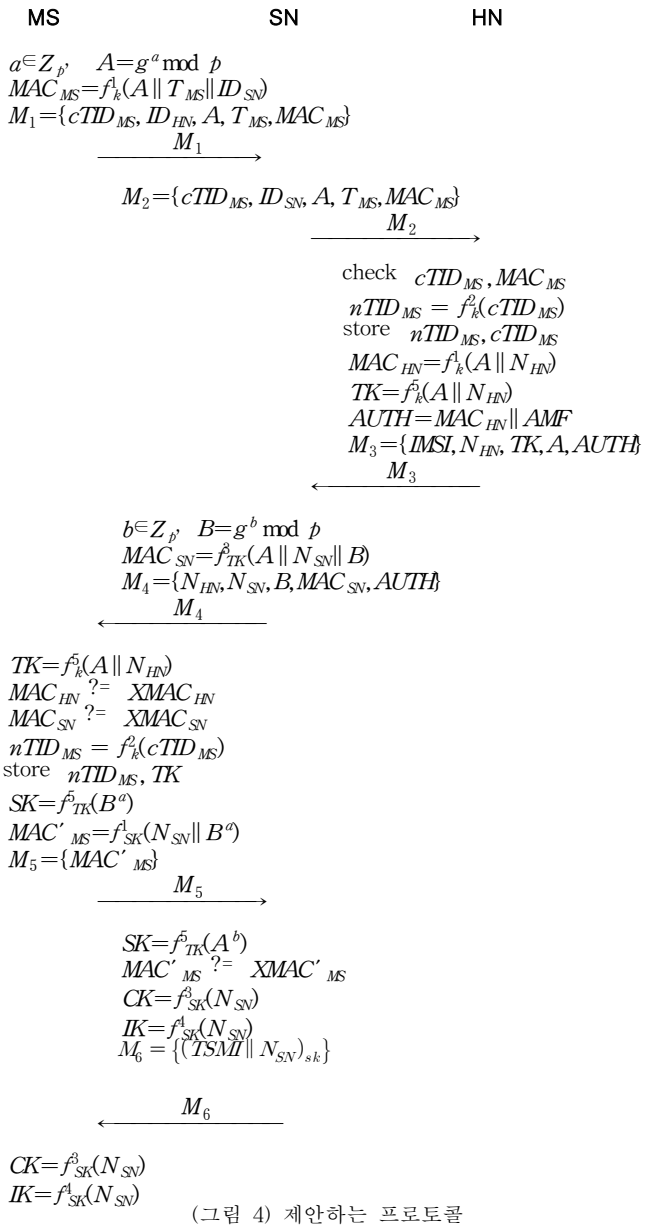
표기	의미
N_R	R에서 생성한 난수
ID_R	R의 식별자
f_K^1	MAC(Message Authentication Code)값과 그에 대응하는 검증 값인 XMAC 값을 계산하는 메시지 인증 함수
f_K^2	사용자 인증(RES/XRES)을 위한 메시지 인증 함수
f_K^3	암호화 키(CK)를 생성하는 함수
f_K^4	무결성 키(IK)를 생성하는 함수
f_K^5	익명성 키(AK)를 생성하는 함수
AMF	암호화키와 무결성키의 수명을 관리하는 Authentication Management Field
T_R	R이 생성한 타임스탬프
$cTID_{MS}$ or $pTID_{MS}$	프라이버시 보호를 위해 IMSI 대신 사용되는 임시 ID. $cTID_{MS}=f_k^2(pTID_{MS})$:현재 사용되는 임시ID $pTID_{MS}$:이전에 사용된 임시ID
g	$g<p$이고, p와 서로소인 원시근
p	매우 큰 소수
TK	HN에서 발급하는 티켓 키
SK	Diffie-Hellman 기법으로 생성한 세션키

3.1. 프로토콜

본 소절에서는 제안하는 프로토콜에 대해 설명한다. 제안하는 프로토콜은 티켓 기반의 인증을 수행하여 AVs 사용의 문제점을 해결하고 Diffie-Hellman 기반의 세션키를 생성함으로써 전방향 안전성을 제공한다. 또한 임시 ID를 사용하여 프라이버시를 강화시키고 MS와 HN간의 상호인증을 제공한다. (그림 4)는 제안하는 프로토콜의 전체적인 수행 과정을 보여준다.

제안하는 프로토콜은 다음과 같이 수행된다.

① MS는 랜덤값 $a \in Z_q$를 선택하고, A와 MAC_{MS}를 계산하여 M_1을 SN에게 보낸다. 이때 HN과 미리 공유되어 있는 임시 ID인 $cTID_{MS}$를 포함시켜서 보내게 된다.



(그림 4) 제안하는 프로토콜

$cTID_{MS}$는 각 세션마다 새롭게 계산되어진다. 이렇게 각 세션 마다 새로운 ID를 발급하여 사용함으로써 프라이버시를 강화할 수 있을 것이다.

② SN은 ID_{HN}을 확인하고 HN에게 ID_{HN}대신 ID_{SN}을 포함한 M_2를 보낸다. 이렇게 함으로써 HN은 MS와 SN이 보낸 ID_{SN}이 서로 일치하는지 확인할 수 있다.

③ HN은 데이터베이스에서 수신한 $cTID_{MS}$를 검색한다. 데이터베이스에는 가입자의 $IMSI$, $cTID_{MS}$, $pTID_{MS}$가 저장되어 있다. 만약 TID_{MS}동기화 문제가 발생하면, $pTID_{MS}$를 검색해 봄으로써 문제를 해결할 수 있다. HN은 MAC_{MS} 검증 시에 SN으로부터 받은 ID_{SN}이 MAC_{MS}에 포함된 ID_{SN}이 맞는지 확인하고, T_{MS}의 유효성을 확인한다.

④ HN은 새로운 $nTID_{MS}$와 N_{HN}을 생성한다. $nTID_{MS}$는 데이터베이스의 현재 임시 ID 필드에 저장되고, $cTID_{MS}$

는 이전 임시 ID 필드에 저장된다. HN은 MAC_{HN}과 TK를 생성하고 SN에게 M_3을 전송한다.

⑤ SN은 랜덤값 $b \in Z_p$를 선택하고, B와 MAC_{SN}을 계산하여 MS에게 M_4를 전송한다.

⑥ SN으로부터 M_4를 받은 MS는 TK를 생성하고 MAC_{HN}과 MAC_{SN}을 검증한다. 검증이 끝나면 다음에 사용할 임시 ID인 $nTID_{MS}$를 계산하고 TK와 함께 저장한다. MS는 SK를 계산하고 M_5를 SN에게 전송한다.

⑦ SN은 SK를 계산한 후 MAC'_{MS}를 검증하고 CK와 IK를 생성한다. 그 후 실제 통신에 사용될 ID인 $TMSI$를 생성해 N_{SN}과 함께 SK로 암호화시킨 메시지 M_6를 MS로 전송한다.

⑧ MS는 SN으로부터 받은 M_6를 복호화하고, CK와 IK를 계산한다. 그리고 MS와 SN은 확립된 이 키들을 이용하여 안전한 통신을 할 수 있다.

4. 안전성 및 효율성 분석

4.1. 안전성 분석

본 절에서는 제안하는 프로토콜의 안전성을 분석한다.

- 상호인증 : MS와 SN, MS와 HN의 상호 인증이 가능하다. HN은 MS가 서로 공유하고 있는 비밀키 k로 생성한 MAC_{MS}를 검증함으로써 MS를 인증할 수 있다. MS는 HN이 생성한 MAC_{HN}을 검증함으로써 HN을 인증할 수 있다.
- 재전송 공격 : MAC값에 타임스탬프와 난수를 포함함으로써 메시지의 최신성을 검증할 수 있기 때문에 공격자의 재전송 공격에 강하다.
- TID_{MS}동기화 공격 : 만약 MS가 SN을 통해 HN으로 전송하는 M_1을 차단한다고 가정한다면, MS는 일정 시간 동안 M_4를 받지 못하면 세션을 종료하고 새로운 세션을 시작하므로 문제가 없다. HN이 SN을 통해 MS에게 보내는 M_3을 공격자가 차단한다고 가정한다. 이때 HN은 MS의 새로운 $nTID_{MS}$를 갱신하게 되는데, MS는 HN으로부터 M_4를 받지 못했으므로 이전의 $cTID_{MS}$를 유지하고 있게 된다. 하지만 HN은 이전에 사용한 $cTID_{MS}$를 $nTID_{MS}$와 함께 저장하고 있으므로 MS가 세션을 다시 시작하더라도 동기화를 할 수 있기 때문에 TID_{MS} 동기화 공격에 안전하다.
- 전방향 안전성 : 이전에 제안된 프로토콜들은 장기간 비밀키 k가 노출되면 전체 통신에 영향을 끼친다. 제안한 프로토콜은 Diffie-Hellman 기법을 사용하여 MS와 SN간에 세션키를 생성함으로써 전방향 안전성을 제공한다.

4.2. 효율성 분석

본 절에서는 제안하는 프로토콜의 효율성을 UMTS AKA와 UMTS X-AKA와의 비교 분석을 통해 제시한다.

제안하는 프로토콜은 AV들을 사용하지 않고 하나의 인증 데이터를 생성하기 때문에 SN과 HN의 네트워크 대역폭 소모를 감소시켰으며 SN의 저장 공간 면에 있어서 효율적이다. MS와 HN, MS와 SN간의 상호 인증이 가능하며 Diffie-Hellman 기법으로 생성한 세션키를 사용하므로 장기간 비밀키나 단기간 비밀키가 노출이 되더라도 통신에 영향을 미치지 않는다. 또한 세션키를 생성하는데 계산상의 부담이 적다.

(표 2) 프로토콜 비교

속성 \ 프로토콜	UMTS AKA	UMTS X-AKA	제안하는 프로토콜
AVs 사용 여부	○	ticket key	ticket key
MS와 SN의 동기화	SQN	time stamp	time stamp
SN과 HN 간의 네트워크 대역폭 소모	○	×	×
SN의 저장공간 오버헤드 여부	○	×	×
MS와 HN의 상호 인증	×*	○	○
MS와 SN의 상호 인증	○	○	○
장기간 비밀키 노출의 영향	○	○	×
단기간 비밀키 노출의 영향	×	○	×

* : MS만 HN을 인증 할 수 있음

5. 결론

본 논문에서는 전방향 안전성을 제공하는 F-AKA 프로토콜을 제안하였다. MS와 HN 사이와, MS와 SN 사이의 상호 인증을 제공하고 임시 ID를 사용함으로써 프라이버시를 강화하였다. 또한 티켓 키 사용으로 SN과 HN사이의 네트워크 대역폭 소모를 감소시키고, SN의 저장 공간 오버헤드를 감소시켰다. Diffie-Hellman 기반의 키 동의 프로토콜을 사용하여 비밀키가 노출이 되더라도 통신에 영향을 끼치지 않는다.

참고문헌

[1] 3GPP TS 23. 101 v7.0.0 (2007-06)

[2] G. Horn, K. M. Martin and C. J. Mitchell, "Authentication protocols for mobil network environment value-added services", *IEEE Trans. on Vchi. Tech.,* 51, pp. 383-392, 2002.

[3] 3GPP TS 33. 102 (v7.0.0), Security architecture, Release 7, 2005.

[4] C. Huang and J. Li, "Authentication and Key Agreement Protocol for UMTS whit Low Bandwidth", *Proc. of the 19th IEEE Conf. on AINA*, pp. 392-397, 2005.

[5] M. Zhang and Y. Fang, "Security Analysis and Enhancement of 3GPP Authentication and Key Agreement Protocol," *IEEE Trans. on Wireless Communications*, Vol. 4, No. 2, pp. 734-742, 2005.