타원 곡선 암호 기반의 프라이버시와 완전한 전방향 안전성을 제공하는 UMTS-AKA 프로토콜

김대영*, 최용강*, 김상진**, 오희국*

*한양대학교 컴퓨터공학과, **한국기술교육대학교 인터넷미디어공학부

ECC-based UMTS-AKA Protocol Providing Privacy and Perfect Forward Secrecy

Daeyoung Kim*, Yonggang Cui*, Sangjin Kim**, Heekuck Oh*

*Department of Computer Science and Engineering , Hanyang University
**School of Internet Media Engineering Korea University of Technology and Education.

요 약

3G 이동통신기술중 하나인 UMTS(Universal Mobile Telecommunications System)에서는 무선 구간의 안전한 통신을 위해 UMTS-AKA(Authentication and Key Agreement) 프로토콜이 사용된다. 그러나 SN(Serving Network)과 HN(Home Network)의 통신량 소비 문제, SQN(SeQuence Number) 동기화 문제 등 여러 가지 문제점이 제기되었다. 본 논문에서는 기존 프로토콜의 문제점과 IMSI(International Mobile Subscriber Identity)의 노출로 인한 프라이버시 문제점을 해결하고, ECDH(Elliptic Curve Diffie Hellman) 기법으로 완전한 전방향 안전성을 제공하는 프로토콜을 제안한다.

I. 서론

유럽을 비롯한 많은 나라에서 3세대 이동통신인 UMTS를 사용하고 있다. 이동통신 사용이 활발해지면서 무선구간에서의 보안이 중요시되고 있으며, 이로 인해 UMTS의 표준화 기구인 3GPP(The 3rd Generation Partnership Project)에서는 무선구간에서의 안전한 통신을 위한 UMTS-AKA프로토콜을 개발하였다[1].

그러나 UMTS-AKA 프로토콜의 SN과 HN의 통신량 소비 문제, SQN 동기화 문제 등의 여러 가지 문제점들이 제기되고 있다.

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터(ITRC) 지원사업의 결과로 수행되었음.

이 연구에 참여한 연구자는 '2단계 BK21 사업'의 지원을 받았음.

이를 해결하기 위해 개선된 UMTS-AKA 프로토콜이 제안되었는데 이와 관련된 연구로는 AP-AKA, Harn&Hsin, X-AKA 프로토콜 등이 있다[2][3][4]. 그러나 이 프로토콜들은 보안 프로토콜의 요구사항 중 하나인 전방향 안전성과 프라이버시 보호를 만족하지 못한다.

본 논문에서는 프라이버시 보호와 완전한 전방향 안전성을 제공하는 UMTS-AKA 프로토콜을 제안한다.

II. 연구배경

1. 수학적 배경

정의 1 (Elliptic Curve Discrete Logarithm Problem (ECDLP)). $Q = xP$인 유한체 Z_p에서의 타원곡선 위의 두 점 Q와 P가 주어졌을 때, $1 \leq x < P$를 찾는 것을 타원 곡선 이산대수 문제라 한다.

정의 2 (Elliptic Curve Diffie-Hellman Problem (ECDHP)). P와 $Q_1 = aP, Q_2 = bP$인 유한체 위의 타원 곡선의 두 점 Q_1과 Q_2가 주어졌을 때, $Q_3 = abP$를 찾는 것은 타원 곡선 Diffie-Hellman 문제라 한다.

현재까지 ECDLP, ECDHP를 해결하는 것은 계산적으로 어렵다고 알려져 있다. 본 논문에서 제안하는 프로토콜에서는 ECDH 기법을 사용함으로써 기존 알고리즘보다 상대적으로 작은 길이의 키를 사용하여 같은 안전성을 제공한다.

2. 전방향 안전성

1) 완전한 전방향 안전성(Perfect Forward Secrecy): 모든 참여자의 장기간 키가 노출되어도 이전 세션에 교환된 기밀성이 요구되는 메시지의 내용이 노출되지 않아야 한다.

2) 부분 전방향 안전성(Partial Forward Secrecy): 일부 참여자들의 장기간 키가 노출되어도 이전 세션에 교환된 기밀성이 요구되는 메일의 내용이 노출되지 않아야 한다.

3. UMTS 네트워크 구조

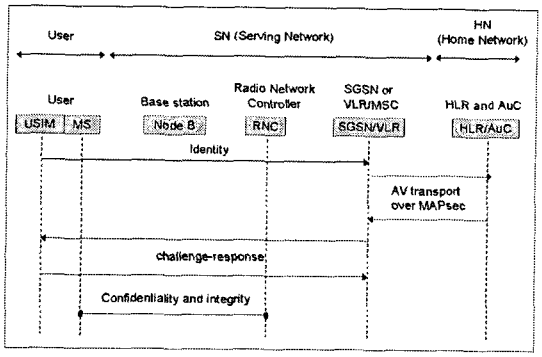

그림 1: UMTS 네트워크 구조와 액세스 보안

그림1은 UMTS 네트워크 구조와 액세스 보안에 대해 나타내고 있다.

• USIM(Universal Subscriber Identity Module): UMTS-AKA 프로토콜을 수행하기 위해 필요한 가입자의 비밀키 K와 IMSI 등의 사용자 정보와 암호 알고리즘 등을 저장하는 모듈이다.

• MS(Mobile Station): USIM이 삽입될 단말기로써, 무선구간에서 암·복호화와 무결성을 검증하는 기능을 가지고 있다.

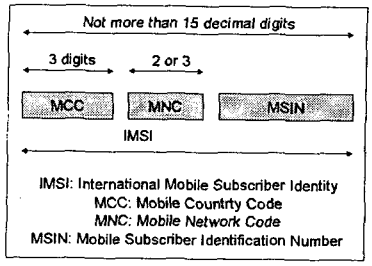

그림 2: IMSI 구조

• Node B(or Base station): MS와 RNC사이에 연결을 담당하는 역할을 한다.

• RNC(Radio Network Controller): Node B를 제어하고, SGSN이나 VLR/MSC와 연결되며 암·복호화와 무결성을 검증을 수행한다.

• SGSN(Serving GPRS Support Node): GPRS(General Packet Radio Service) 서비스 지역 내에서 MS와의 데이터 패킷 전달을 담당하는 노드이다.

• MSC/VLR(Mobile Switching Center/Visitor Location Register): MSC는 CS(Circuit Switched) 서비스를 제공하고 VLR은 방문 가입자에 대한 정보를 저장하는 역할을 한다.

• HLR(Home Location Register): 가입자에 대한 정보가 저장되며, SGSN이나 MSC/VLR에게 전달하게 된다.

• AuC(Authentication Center): 가입자의 인증과 무선구간에서 암호화를 지원하는 시스템으로 가입자의 IMSI와 비밀키 K를 저장하고 있다.

• IMSI(International Mobile Subscriber Identity): IMSI는 가입자 식별값으로 USIM과 AuC에 저장되어 있다. IMSI는 초기에 가입자를 식별할 때 사용되어 진다. 그림 2는 IMSI의 구조를 나타낸다.

III. 관련연구

1. 표기법

표 1은 본 논문에서 사용된 프로토콜 표기법이다.

표 2: 표기법

표기	의미
RAND	난수

K	MS와 HN간의 공유키
CK(*Cipher* Key)	f_K^3 함수에 의해 만들어지는 암호화 키
IK(*Integrity* Key)	f_K^4 함수에 의해 만들어지는 무결성 키
AK(*Anonimity* Key)	f_K^5함수에 의해 익명성 키
$RES, XRES$	f_K^2 사용자 인증함수로 만든 값
$MAC, XMAC$	f_K^1 함수에 의해 생성되는 메시지 인증 코드
AMF (*Authentication Management Field*)	다중 인증 알고리즘과 키를 지원하거나 암호화키와 무결성키의 수명을 관리하는 인증관리필드
TID_O, TID_N	IMSI의 보호를 위해 사용되는 임시 ID
$H(M)$	메시지 M을 해쉬한 값
T	타임스탬프
SK	세션키

2. UMTS-AKA 프로토콜

1) *MS*는 *SN*에게 인증을 요청하기 위해 *IMSI*를 보낸다.

2) *SN*은 *MS*에게 받은 *IMSI*를 *HN*에게 전달한다.

3) *HN*은 *MS*와 공유하고 있는 *K*와 *HN*이 생성한 *RAND*를 이용해 *SN*에게 전달할 AV를 n개 생성한다.

4) *HN*은 생성한 $AV[1...n]$를 *SN*에게 전달한다.

5) *SN*은 AVs를 보관하고 i번째 AV를 선택한다.

6) *SN*은 선택한 $RAND[i], AUTN[i]$를 *MS*에게 보낸다.

7) *MS*는 *RAND*와 *K*로 $AUTN$을 검증한다. 이 때, *SQN*을 확인하고 *RES*를 생성한다.

8) *MS*는 생성한 *RES*를 *SN*에게 보내 인증을 하게 되고, *MS*는 *CK,IK*를 생성한다.

9) *SN*은 *MS*에게 받은 *RES*를 *XRES*와 비교해 검증하고 *CK,IK*를 생성한다.

IV. 제안하는 프로토콜

1. 프로토콜의 가정

- MS는 자신의 HN과 비밀키와 임시ID인 TID와 암호화 알고리즘을 공유하고 있다.
- SN과 HN은 MAPsec(Mobile Application Part Security)과 같은 Network Domain Security 메커니즘을 통해 안전하다고 가정한다.

2. 프로토콜

1) *MS*는 인증과 키 동의를 수행하기 위해 *SN*에게 $ID_{HN} = MCC||MSIN$, 임시ID로 생성한 $ID_{MS} = H(IMSI||TID_O), aP$, T, MAC_{MS}를 *SN*에게 보낸다.

2) *SN*은 ID_{HN}을 확인한 뒤, *MS*로부터 받은 메시지를 *HN*에게 전달한다. 이 때, aP를 보관한다.

3) *HN*은 ID_{MS}와 MAC_{MS}를 확인한다. 그리고 새로운 TID_N를 생성하고 $ID_{MS} = H(IMSI||TID_N), TID_N$를 저장한다. 마지막으로, *MS*가 검증하기 위한 MAC_{HN}을 계산한다.

4) *HN*은 *TK*를 생성해 TID_N과 XOR한 값을 포함한 $AUTN_{HN}$을 *SN*에게 보낸다. 이 때, *SN*에게 *IMSI* 정보도 같이 보내게 된다.

5) *SN*은 *HN*과 안전한 채널을 가지기 때문에 aP를 비교해 이전에 저장했던 값과 같으면 bP를 생성해 $SK = abP$를 생성한다. 그리고 $RAND_{SN}$를 생성하고 MAC_{SN}을 생성한다.

6) *SN*은 *MS*에게 $AUTN_{SN}$을 보낸다.

7) *MS*는 SK를 생성해 MAC_{SN}, MAC_{HN}을 검증하고 $TK \oplus TID_N$에서 *TK*를 이용해 TID_N을 구하고 새로운 ID_{MS}를 생성해 저장한다. 그리고 $RAND_{SN}$와 SK로 *RES*를 생성하고 *CK,IK*를 생성한다.

8) *MS*는 생성한 *RES*를 *SN*에게 보낸다.

9) *SN*은 *RES*와 *XRES*를 비교해 검증하고 *CK,IK*를 생성한다.

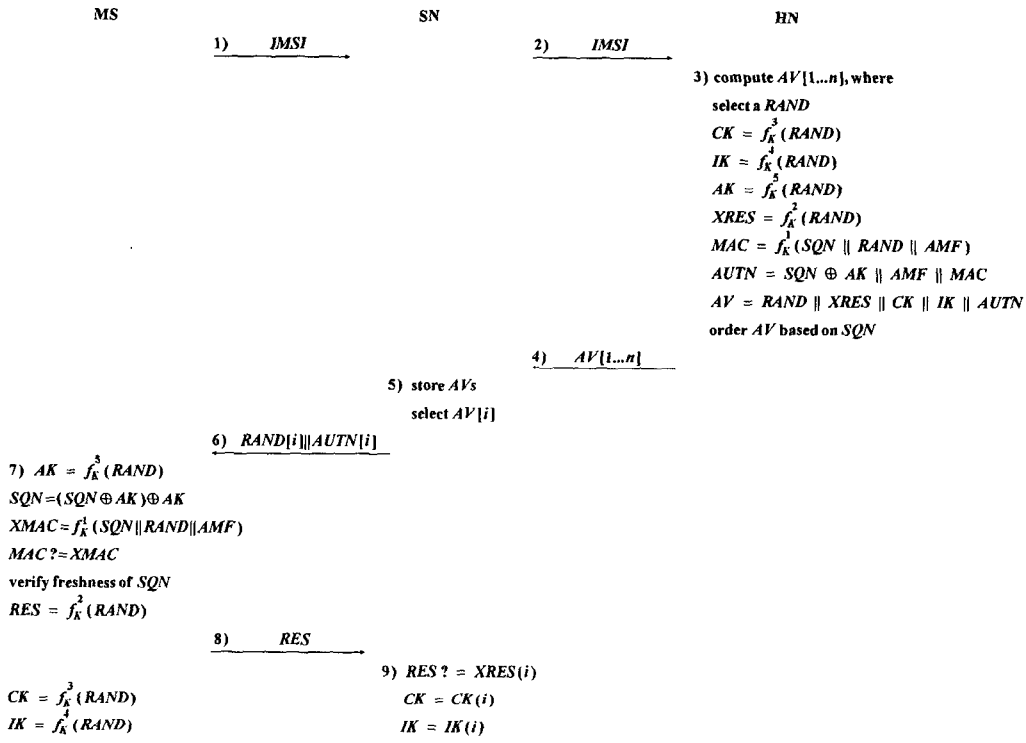

그림 3: UMTS-AKA 프로토콜

V. 프로토콜 분석

1. 안전성 분석

- MS와 HN의 상호 인증: MS는 MS과 HN가 미리 공유하고 있는 키로 생성한 MAC값을 보내기 때문에 HN이 MS를 인증하게 된다. 마찬가지로 MS도 HN이 보낸 MAC값으로 인증하게 된다. MS는 HN을 인증함으로써 SN도 인증한다.
- 무선구간에서 데이터의 기밀성, 무결성 보장: 제안하는 프로토콜이 수행됐을 경우, CK와 IK로 통신을 하기 때문에 기밀성과 무결성을 보장하게 된다.
- 완전한 전방향 안전성 만족: ECDH 기법을 이용해 MS와 SN간에 키를 생성하기 때문에 장기간 비밀키인 K가 노출되어도 완전한 전방향 안전성을 만족하게 된다.
- 프라이버시 보호: 초기 프로토콜을 진행할 때 프라이버시를 위해 IMSI와 TID를 해쉬한 값으로 보내고 추적을 방지하기 위해 매번 TID가 바뀌기 때문에 프라이버시가 보호된다.

2. 효율성 분석

- SN과 HN의 통신량 감소: 기존의 프로토콜처럼 인증벡터를 n개 생성하는 것이 아니라 SN에서 생성하기 때문에 SN과 HN사이에 통신량이 감소된다.
- SN의 저장 공간 오버헤드 감소: 기존 프로토콜에서는 AV를 n개 사용하기 때문에 m개의 MS만큼 필요해서 오버헤드가 발생했다. 그러나 제안하는 프로토콜은 티켓키 생성방식으로 불필요한 저장 공간 오버헤드를 감소시켰다.
- MS와 HN간의 동기화 불필요: SQN을 제거해 MS와 HN간의 동기화가 불필요해짐으로써 통신량 소비 면에서 더 효율적이다.

VI. 결론

본 논문에서는 프라이버시를 보호하고 완전한 전방향 안전성을 제공하는 UMTS-AKA 프로토콜

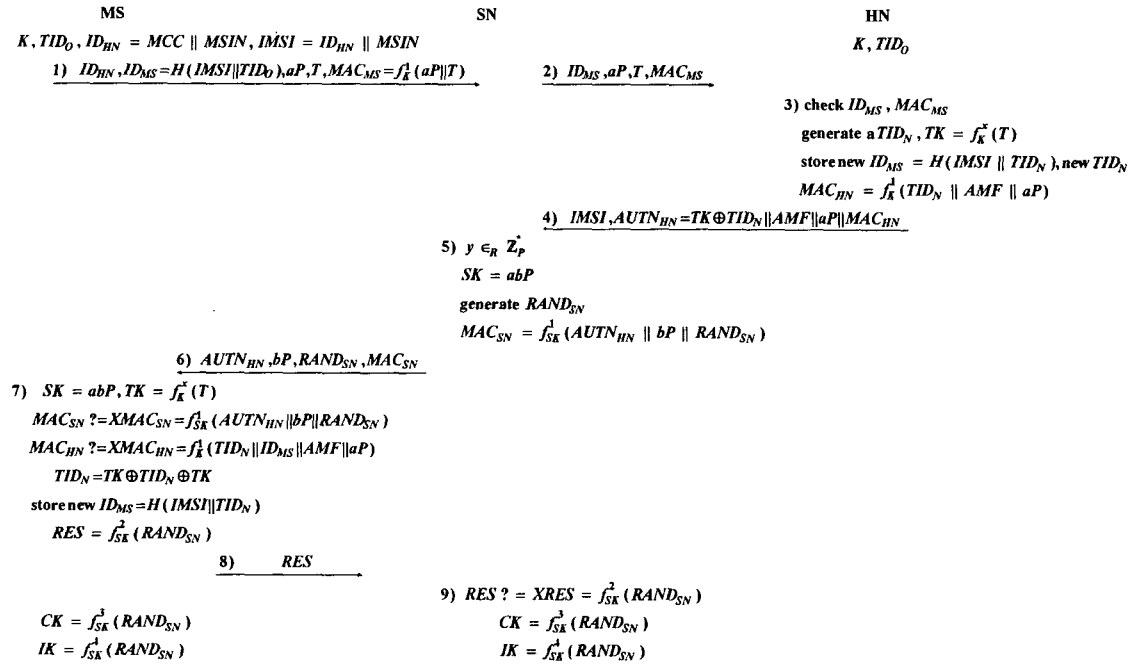

그림 4: 제안하는 프로토콜

을 제안하였다. 제안하는 프로토콜은 기존의 UMTS-AKA 프로토콜의 문제점을 보완한 프로토콜로써, IMSI를 무선 구간에서 평문상태로 보내지 않음으로써 프라이버시를 보호할 수 있다. 그리고 ECDH 기법을 적용해 보안 프로토콜의 중요한 요구사항 중 하나인 완전한 전방향 안전성을 제공하였다.

참고문헌

[1] 3GPP TS 33.102 (v7.0.0), Security architecture, Release 7, 2005.

[2] M. ZHang, Y.Fang, "Security Analysis and Enhancement of 3GPP Authentication and Key Agreement Protocol," Wireless Communications IEEE Transactions in 2005.

[3] L. Harn and W.J. HSin, "On the Security of Wireless Network Access with Enhancements," In Proc. ACM workshop on Wireless Security, pp.88-95, 2003.

[4] C. Huang, J. Li, "Authentication and Key Agreement Protocol for UMTS with Low Bandwidth," Advanced Information Networking and Applications, 2005.

[5] M. Zhang. Provably-Secure Enhancement on 3GPP Authentication and Key Agreement Protocol. Cryptology ePrint Archive, Report, 2003.

[6] G.M. Koien, "An Introduction to Access Security in UMTS", IEEE Wireless Communications, 2004.

[7] 3GPP TS 23.003 (v6.9.0), Numbering, addressing and identification, Release 6, 2006.

[8] 3GPP TS 23.060 (v7.0.0), General Packet Radio Service (GPRS) Stage2, Release 7, 2006.

[9] 3GPP TS 23.002 (v7.1.0), Network architecture, Release 7, 2006.

[10] 3GPP TS 23.008 (v7.1.0), Organization of subscriber data, Release 7, 2006.

[11] 3GPP TS 33.801 (v1.0.0), Access Security Review, Release 7, 2005.

[12] 3GPP TS 43.020 (v6.3.0), Security related network functions, Release 6, 2006.