cdma2000 패킷 데이터 서비스를 위한 효율적인 상호 인증과 키 분배 프로토콜

신상욱*, 류희수*

*한국전자통신연구원 정보보호연구본부

Efficient mutual authentication and key distribution protocol for cdma2000 packet data service

Sang Uk Shin*, Heuisu Ryu*

*Information Security Research Division, ETRI

요 약

본 논문에서는 DIAMETER AAA(Authentication, Authorization and Accounting) 하부 구조를 가지고 Mobile IP 액세스 기법을 사용하는 cdma2000 패킷 데이터 서비스에서 MN(mobile node)와 AAAH(home AAA server)간의 상호 인증과 Mobile IP 개체들간에 안전한 세션키 분배를 위한 방법을 제안한다. 제안된 프로토콜은 DIAMETER AAA 하부 구조를 가정하며 DIAMETER AAA의 비효율성을 개선하고, 인증과 키 분배 프로토콜의 시큐리티 요구 사항들을 모두 만족한다.

I. 서론

현재 3GPP2(3rd Generation Project Partnership 2)에서 표준화 진행 중인 cdma2000 패킷 데이터 서비스에서 IP(Internet Protocol) 요소들은 P.S0001-A[3]와 P.R0001[2] 표준에 명시된 Mobile IP[11], RADIUS AAA(Authentication, Authorization and Accounting)[12], IPSec(IP Security)[4]에 기반한다.

cdma2000 패킷 데이터를 위한 3GPP2 시큐리티 요구 사항은 Mobile IP Authentication Extension, IPSec, 1xEV-DO Radio Access 계층 시큐리티[1]에 기반한다. 현재 RADIUS AAA 하부 구조가 실제 많이 구현되어 사용 중에 있으며, DIAMETER AAA[8]는 Mobile IP 개체의 키들이 무선 인터페이스를 통해 전달되어야 하고 AAAH(home AAA server)가 각 Mobile IP 개체들의 키들을 두 번씩 암호화하여 전달하므로 RADIUS AAA에 비해 비효율적이기 때문에, 3GPP2는 패킷 데이터 서비스를 위한 하부 구조로 현재 IETF에서 개발 중인 DIAMETER AAA 하부 구조 대신 RADIUS AAA 하부 구조를 선택하였다.

본 논문에서는 cdma2000 패킷 데이터 서비스에서 MN(mobile node)와 AAAH간의 상호 인증과 Mobile IP 개체들간에 안전한 세션키 분배를 위한 방법을 제안한다. 현재의 3GPP2 표준 문서는 Mobile IP 개체들간의 키 분배를 정의하고 있지 않으며, RADIUS AAA 하부 구조를 가정한다. 제안된 프로토콜은 DIAMETER AAA 하부 구조를 가정하고, 위에서 언급한 DIAMETER AAA의 비효율성을 개선한 Mobile IP 개체들간의 안전한 키 분배를 제안한다. 제안된 기법은 2장에 기술한 시큐리티 요구 사항을 모두 만족하며, 초기 셋업 시간에 최소한의 영향을 준다.

II. cdma2000 Mobile IP 참조 모델과 시큐리티 요구 사항

1. cdma2000 Mobile IP 참조 모델

cdma2000 패킷 데이터 구조는 RADIUS AAA 하부 구조와 IPSec 하부 구조를 포함하는 두 개의 핵심 IP 액세스 메커니즘으로 분리된다. RADIUS AAA와 IPSec은 Mobile IP 구조에 결합된다. cdma2000 패킷 데이터를 위해 정의된 두 가지 핵심 액세스 기법은 Simple IP와 Mobile IP이다[3].

- Simple IP : MN이 local Packet Data Service Node(PDSN)로부터 동적으로 할당된 IP 주소를 가지고 local service provider 네트워크에 의해 라우팅 서비스가 제공되는 서비스이다. local PDSN 이상의 IP 주소 이동성(mobility)을 제공하지 않는다. 따라서 MN은 새로운 (PDSN) 네트워크로 로밍(roaming)하면 새로운 Transport Layer 연결을 설정해야 한다.

- Mobile IP : Mobile IP는 RFC2002에 기반한 서비스로 MN이 다른 PDSN에 연결된 radio 네트

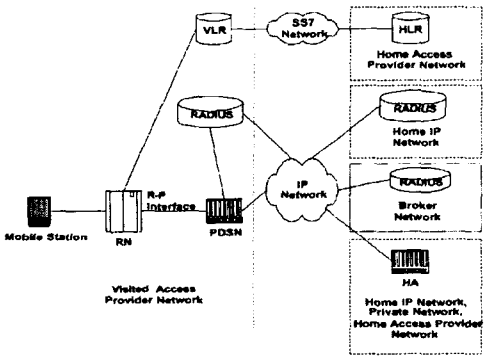

그림 1: Mobile IP 액세스를 위한 참조 모델

워크간 핸드 오프가 발생할 때에도 영구 IP 주소를 유지할 수 있는 서비스이다. 즉 Transport Layer 연결이 영향을 받지 않는다. MN은 static IP 주소 또는 MN의 home IP 네트워크로부터 동적으로 할당된 IP 주소를 사용할 수 있다.

본 논문에서는 Mobile IP를 고려한다. 3GPP2 P.S0001-A에 정의된 Mobile IP 참조 모델은 그림 1과 같다. cdma2000 패킷 데이터의 상황에서 PDSN은 MN이 홈 또는 방문 망에 있는지에 무관하게 항상 FA(foreign agent)로 동작한다. PPP가 MN과 PDSN간의 데이터 링크 프로토콜로 사용된다. PPP는 MN과 PDSN간에 IP 데이터그램이 교환되기 이전에 설정된다. MN과 PDSN간에 하나의 PPP 세션만이 지원된다.

현재의 표준 문서는 Mobile IP에 대해 CHAP 또는 PAP가 수행되지 말아야 한다는 것을 명시한다[2][3]. CHAP 또는 PAP가 수행되면 추가적인 RADIUS 과정으로 인해 초기 셋업 시간과 재설정 시간이 더 길어진다. RADIUS AAA를 사용한 초기 등록 과정은 그림 2와 같다. 2001년 12월 3GPP2 회의에서 Verizon Wireless 사는 패킷 데이터 서비스를 위한 Simple IP와 Mobile IP 시큐리티를 분석한 후 키 계층을 제안하였으며[7], 2002년 6월 3GPP2 회의에서는 Lucent 사가 RADIUS 하부 구조를 가진 Mobile IP 환경을 위한 키 분배 기법을 제안하였다[10].

2. 시큐리티 요구 사항

인증과 키 분배 프로토콜의 주요 목적은 사용자와 네트워크가 서로를 상호 인증하고 의도된 개체들만이 키를 알고 키가 새롭고 랜덤하다는 것을 보장하는 것이다. 로밍과 같은 상황에서의 추가적인 요구 사항은 네트워크 경로의 확인이다. 본 논문에서는 기본적으로 다음의 요구 사항들을 모두 만족하는 기법을 제안한다.

(1) 상호 인증 : AAAH가 MN이 SA(security association)를 설정할 권한을 가졌다는 것을 인증하고 외부 도메인에서 FA로부터 서비스 받는 것은 인가할 수 있어야 한다. 동시에 MN은 AAAH

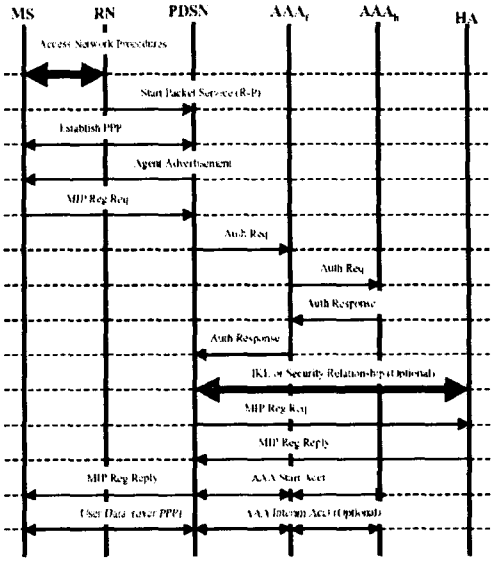

그림 2: RADIUS AAA를 사용한 초기 등록 과정

를 인증할 수 있어야 한다.

(2) 세션키 설정 : 개체들간에 임시 세션키를 설정할 수 있도록 세션 마스터 키(MSK)를 생성해야 한다. MN과 AAAH에게 MSK가 새롭고 랜덤하다는 것을 보장해야 한다.

(3) forward secrecy : forward secrecy의 개념은 세션키의 손상이 그 키에 의해 보호된 데이터에만 영향을 준다는 개념을 말한다. 즉 공격자가 한 세션을 위한 키를 구성할 수 있는 세션 마스터 키를 유도할 수 있더라도, 과거와 미래의 세션 키들은 손상되지 않는다는 것을 보장한다.

(4) AAAH에 의한 경로 인증 : AAAH가 MN에서 AAAH로의 경로에 있는 개체들의 신분을 검증할 수 있어야 한다.

(5) MN에 의한 경로 인증 : MN이 MN에서 AAAH로의 경로에 있는 개체들의 신분을 검증할 수 있어야 한다.

III. cdma2000 패킷 데이터 서비스 구조를 위한 효율적인 상호 인증과 키 분배 기법

이 장에서는 DIAMETER AAA 하부 구조를 가지고 Mobile IP 액세스 기법을 사용하는 cdma2000 패킷 데이터 서비스 구조를 위한 효율적인 상호 인증과 세션키 분배 기법을 제안한다.

제안된 기법에서는 MN과 AAAH가 128비트 비밀키 RK를 공유하고 있다고 가정한다. 또한 AAAH와 HA, AAAF와 FA, AAAH와 AAAF 사이에 SA가 설정되어 있는 것을 가정한다. 제안된 프로토콜의 결과로 Mobile IP 개체(MN, FA, HA)들간에 세션키들이 생성된다.

1. 용어

- AAA : Authentication, Authorization and Accounting DIAMETER 서버
- AAAH : home AAA 서버
- AAAF : foreign AAA 서버
- AUTH_HA : MN의 challenge에 대한 HA의 응답
- AUTH_MN : MN의 FA challenge에 대한 응답
- FA : foreign agent
- FA_HA_Key : FA와 HA 사이의 128비트 세션키
- HA : home agent
- MAC : 메시지 인증 코드(message authentication code)
- MN : mobile node
- MN_FA_Key : MN과 FA 사이의 128비트 세션키
- MN_HA_Key : MN과 HA 사이의 128비트 세션키
- NAI : network access identifier
- NF : FA의 challenge(nonce)
- NH : AAAH의 challenge(nonce)
- NM : MN의 challenge(nonce)
- PRF : 의사 랜덤 함수(pseudo-random function)
- RK : MN과 AAAH 사이에 공유된 128비트 루트 키
- MSK : 128비트 세션 마스터 키로 MN_FA_Key, MN_HA_Key, FA_HA_Key 유도를 위해 사용된다.

2. 제안된 프로토콜

제안된 프로토콜은 그림 3과 같이 동작한다.

(1) FA는 challenge nonce NF를 생성하여 자신의 속한 AAAF의 ID와 함께 FA Advertisement 메시지를 MN에게 브로드캐스트 한다.

(2) MN은 challenge nonce NM을 생성하고, 루트 키 RK를 사용하여 다음처럼 MN Authentication Response AUTH_MN을 계산한다.

AUTH_MN = MAC(RK, FA_ID||AAAF_ID||NF||NM||NAI)

MN은 NAI, NF, NM, AUTH_MN을 포함한 Registration Request 메시지를 PDSN에게 전달한다.

(3) PDSN은 NF를 검증한 후 NF, NM, NAI, AUTH_MN을 포함한 DIAMETER AMR(AA-Mobile-Node-Registration-Request) 메시지를 AAAF에게 전송한다.

(4) AAAF는 FA의 ID를 추가한 AMR 메시지를 AAAH에게 전달한다.

(5) AAAH는 먼저 AUTH_MN을 검증한다. 검증이 성공하면, MN의 challenge인 NM에 대한 AAAH Authentication Response AUTH_HA를 다음처럼 계산한다.

AUTH_HA = MAC(RK, NM||NF||NAI||AAAF_ID||FA_ID)

AAAH는 NH를 생성하고, 세션 마스터 키 MSK를 계산한다.

MSK = PRF(RK, NM||AUTH_HA||NH)

생성된 MSK를 사용하여 Mobile IP 세션키들을 계산한다.

MN_FA_Key = PRF(MSK, NF||NM||NAI||FA_ID)

MN_HA_Key = PRF(MSK, NM||NH||NAI||HA_ID)

FA_HA_Key = PRF(MSK, NH||NF||FA_ID||HA_ID)

AAAH는 MN_HA_Key와 FA_HA_Key를 포함한 DIAMETER HAR (Home-Agent-MIP-Request) 메시지를 HA에게 전송한다.

(6) HA는 Registration Reply를 포함한 HAA (Home-Agent-MIP-Answer) 메시지를 AAAH에게 전송한다.

(7) AAAH는 AUTH_HA, MN_FA_Key, FA_HA_Key, NH를 포함한 AMA(AA-Mobile-Node- Registration-Answer) 메시지를 AAAF에게 전송한다.

(8) AAAF는 AMA를 PDSN에게 전달한다.

(9) PDSN은 AUTH_HA, NH를 포함한 Registration Reply 메시지를 MN에게 전달한다.

(10) MN은 AUTH_HA를 검증한다. 검증이 성공하면, 세션 마스터 키 MSK를 계산한 후, Mobile IP 세션키들을 유도한다.

MSK = PRF(RK, NM||AUTH_HA||NH)

MN_FA_Key = PRF(MSK, NF||NM||NAI||FA_ID)

MN_HA_Key = PRF(MSK, NM||NH||NAI||HA_ID)

FA_HA_Key = PRF(MSK, NH||NF||FA_ID||HA_ID)

3. 프로토콜 분석

제안된 프로토콜은 MN과 AAAH 사이의 메시지 교환을 최소화하여 인증 과정에서의 지연을

최소화한다. 또한 3GPP2의 RADIUS AAA 등록 과정에서는 상대적으로 멀리 떨어진 위치에 있는 외부 망과 홈 망간에 총 4번의 메시지 교환이 발생하지만 제안된 프로토콜에서는 2번의 메시지 교환만 발생하여 통신 지연을 최소화한다. 그리고 제안된 기법은 기존의 DIAMETER AAA의 메시지 흐름을 그대로 사용하므로 추가적인 메시지 교환이 발생하지 않는다.

제안된 프로토콜은 2장에서 기술한 시큐리티 요구 사항을 모두 만족한다.

(1) 상호 인증 : 단계 5에서 AAAH는 AUTH_MN 검증을 통해 MN을 인증할 수 있다. AUTH_MN의 계산에 NF가 포함됨으로써 매 세션마다 freshness가 보장된다. 또한 NAI가 포함됨으로써 공유 비밀키 RK와 사용자 신분간의 정확한 binding이 보장된다.

MN은 단계 9에서 challenge NM에 대한 AAAH의 응답인 AUTH_HA 검증을 통해 AAAH를 인증한다. AUTH_HA의 freshness는 NM에 의해 보장된다.

(2) 세션키 설정 : MN과 AAAH는 세션 마스터 키 MSK를 생성한다. 이 키를 사용하여 Mobile IP 개체들간에 세션키를 설정한다. MSK의 freshness와 랜덤성은 NM, NH, AUTH_HA의 freshness와 PRF의 성질로부터 보장된다.

(3) forward secrecy : forward secrecy는 PRF의 성질과 프로토콜이 공격자에게 RK에 관한 어떠한 정보도 노출하지 않는다는 것으로부터 보장된다.

(4) AAAH에 의한 경로 인증 : AAAH는 AAAF를 그들 사이에 직접적인 SA를 통해 AAAF를 인증한다. AAAF는 FA와 설정된 SA에 의해 FA를 인증한다. AAAF에 의해 전달된 FA_ID가 AUTH_MN 계산에 사용되기 때문에, AUTH_MN의 유효성은 FA의 유효성을 함축한다.

(5) MN에 의한 경로 인증 : MN은 FA를 암호학적으로 인증하지 않지만, 위에서 기술한 것처럼 AAAF_ID와 FA_ID가 포함된 AUTH_HA의 성공적인 검증은 MN에게 경로의 확실성을 보장한다.

부정한 네트워크 개체에 의한 재연 공격(replay attack)은 MN, FA, AAAH에 의해 매 세션마다 새롭게 생성되는 nonce에 의해 방지된다.

제안된 프로토콜의 안전성은 사용된 MAC 함수와 PRF의 성질에 의존한다. 이들 함수들은 인증, 세션의 freshness, 세션키의 freshness와 랜덤성을 보장하도록 적용되어야 한다. MAC과 PRF 함수로 HMAC-SHA1[9]을 고려할 수 있다.

IV. 결론

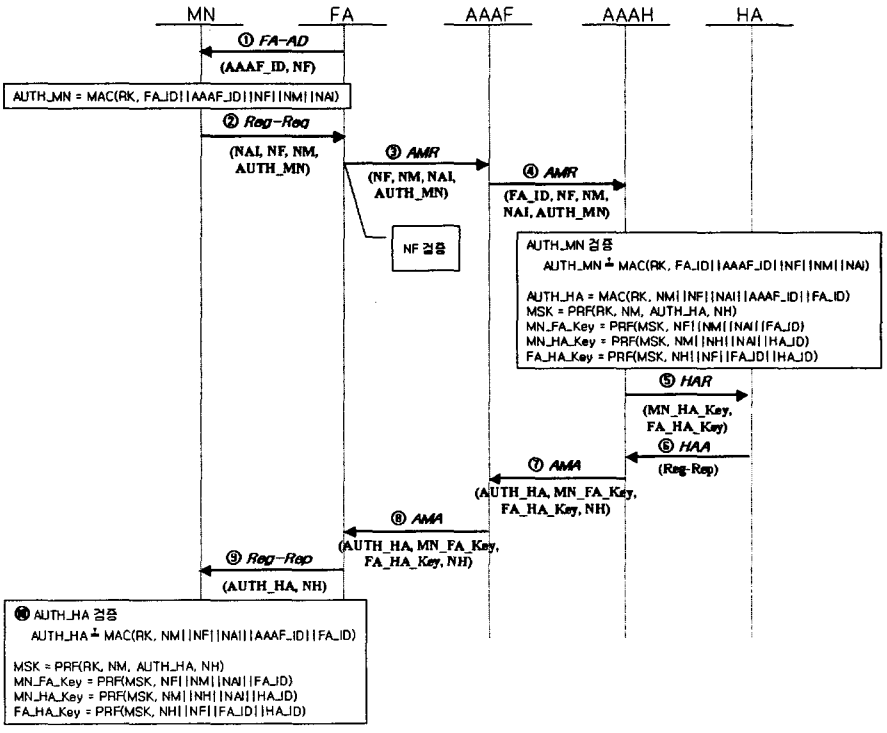

그림 3: 제안된 상호 인증과 키 분배 프로토콜

본 논문에서는 DIAMETER AAA 하부 구조를 가지고 Mobile IP 액세스 기법을 사용하는 cdma2000 패킷 데이터 서비스 구조를 위한 효율적인 상호 인증과 세션키 분배 기법을 제안하였다. 제안된 기법은 2장에 기술한 시큐리티 요구사항을 모두 만족하며, 초기 셋업 시간에 최소한의 영향을 준다.

제안된 프로토콜에 대한 증명가능한 안전성은 [5]과 [6]에 적용된 것들과 유사한 기법에 의해 증명될 수 있을 것으로 보이지만, 이것에 대한 정확한 증명은 향후 연구 과제이다.

참고문헌

[1] 3GPP2 C.S00024 "cdma2000 High Rate Packet Data Air Interface Specification", 2001.12.

[2] 3GPP2 P.R0001 "Wireless IP Architecture Based on IETF Protocols", 2000.7.14.

[3] 3GPP2 P.S0001-A "Wireless IP Network Standards", 2001.7.16.

[4] R. Atkinson, "Security Architecture for the Internet Protocol", *RFC 1825, IETF*, August 1995.

[5] M. Bellare, R. Canetti, H. Krawczyk, "A modular approach to the design and analysis of authentication and key exchange protocols", *STOC'98*, pp.419-428, 1998.

[6] M. Bellare, P. Rogaway, "Entity authentication and key distribution", *CRYPTO'93*, LNCS. vol. 773, pp.232-249, 1993.

[7] C. Carroll, "cdma2000 Packet Data Security Assessment", *3GPP2 TSG-S WG4 S40-20011203-003*, December 2001.

[8] Pat R. Calhoun, Haseeb Akhtar, Jari Arkko, Erik Guttman, Allan C. Rubens, Glez Zorn, "Diameter Base Protocol", *Work in progress - Internet Draft, IETF*, July 2002. draft-ietf-aaa-diameter-12.txt

[9] C. Madson, "The Use of HMAC-SHA-1-96 within ESP and AH", *RFC 2404, IETF*, November 1998.

[10] M. Marcovici, S. Mizikovsky, "Enhanced Mobile IP Authentication and Shared Key Exchange protocol", *3GPP2 TSG-S WG4 S40-20020610-011*, June 2002.

[11] C. Perkins, Ed, "IP Mobility Support for IPv4", *RFC 3220, IETF*, January 2002.

[12] C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote Authentication Dian In User Service(RADIUS)", *RFC 2865, IETF*, June 2000.