情報保護學會論文誌
第13券 第2號, 2003. 4

cdma2000 패킷 데이터 서비스를 위한 효율적인 상호 인증과 키 분배 프로토콜

신 상 욱*, 류 희 수*

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

Sang Uk Shin*, Heuisu Ryu*

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 안전성 요구 사항들을 모두 만족한다. 또한 1xEV-DO에 대한 패킷 데이터 세션 하이재킹 공격을 방지하기 위해 제안된 기법에 의해 분배된 키를 1xEV-DO 무선 인터페이스 패킷 데이터 보안을 위한 키 생성에 적용한다.

ABSTRACT

In this paper, we propose an efficient mutual authentication and key distribution protocol for cdma2000 packet data service which uses Mobile IP access method with DIAMETER AAA(Authentication, Authorization and Accounting) infrastructure. The proposed scheme provides an efficient mutual authentication between MN(Mobile Node) and AAAH(home AAA server), and a secure session-key distribution among Mobile IP entities. The proposed protocol improves the efficiency of DIAMETER AAA and satisfies the security requirements for authentication and key distribution protocol. Also, the key distributed by the proposed scheme can be used to generate keys for packet data security over 1xEV-DO wireless interface, in order to avoid a session hijacking attack for 1xEV-DO packet data service.

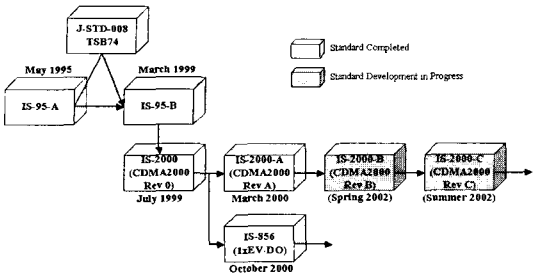
Keyword : *cdma2000, mutual authentication, key distribution, Mobile IP, AAA*

Ⅰ. 서 론

동기식 CDMA 이동통신 방식은 3GPP2(3rd Generation Project Partnership 2)에서 표준화 진행 중이며, 크게 2G인 IS-95 계열과 3G인 IS-2000 계열로 구분된다. IS-95는 무선 구간의 접속 방식을 CDMA로 최초로 정의한 무선 구간 프로토콜이다. IS-2000은 cdma2000 방식의 무선 구간 프로토콜로 IMT-2000을 지향하고 있다. [그림 1]은 CDMA 무선 인터페이스 표준의 진화 과정을 보여준다.

IS-2000은 1x 또는 3x라고 불리며, Rev(Revision). 0~Rev.B는 일반적인 음성과 데이터 서비스에 대해 최대 307kbps(1x), 1.04Mbps (3x)의 전송 속도를 지원한다. HDR(High Data Rate), HRPD(High Rate Packet Data), 1xEV(Evolution)-DO(Data Only)라고 불리는 IS-856[6]은 기존의 IS-2000 무선 프로토콜과는 다른 패킷 데이터 서비스를 위한 전용 프로토콜로, 최대 2.4Mbps의 전송 속도를 제공한다. IS-2000 Rev.C

* 한국전자통신연구원 정보보호연구본부({shinsu, hsryu}@etri.re.kr)



〔그림 1〕 CDMA 무선 인터페이스 표준

이후의 기술은 1xEV-DV(Data and Voice)라고 불리며 현재 표준화가 진행 중이며, 3Mbps~5Mbps의 데이터 전송 속도를 제공할 예정이다. cdma2000 1xEV-DO는 이전의 프로토콜과 달리 무선 인터페이스 계층 구조에 따로 분리된 시큐리티 계층(security layer)을 가진다. 이 시큐리티 계층에서 패킷 데이터 서비스를 위한 인증과 암호화 서비스를 제공한다. 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 안전성 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. DIAMETER는 dial-up PPP(point-to-point protocol)만을 지원하는 기존의 RADIUS 프로토콜의 여러 문제들을 개선하고, 새로운 액세스 기법들(무선, Mobile IP 등)을 지원하는 새로운 AAA 프로토콜로 현재 IETF에서 표준 개발 중이다. 패킷 데이터 서비스 제공을 위한 3GPP2의 현재 표준들[2][3]은 기존의 RADIUS AAA 하부 구조를 지원하지만, 최근 3GPP2 회의에서는 DIAMETER AAA 하부 구조를 지원하는 것에 관해 계속 논의하고 있는 상황이다.

본 논문에서는 cdma2000 패킷 데이터 서비스에서 MN(mobile node)과 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[2][3]. 제안된 프로토콜은 DIAMETER AAA 하부 구조를 가정하고, 위에서 언급한 DIAMETER AAA의 비효율성을 개선한 Mobile IP 개체들간의 안전한 키 분배를 제안한다. 제안된 기법은 2장에 기술한 안전성 요구 사항을 모두 만족하며, 초기 셋업 시간에 최소한의 영향을 준다. 또한 Carroll[7]에 의해 지적된 1xEV-DO에 대한 패킷 데이터 세션 하이재킹 공격을 방지하기 위해, 제안된 상호 인증과 키 분배 프로토콜을 통해 분배된 MN과 FA 사이의 키(MN_FA_Key)를 무선 인터페이스 상의 패킷 데이터 암호화와 인증을 위한 키를 생성하는데 적용할 수 있다.

먼저 2장에서는 cdma2000 Mobile IP 참조 모델과 안전성 요구 사항을 기술하고, 3장에서 cdma2000 패킷 데이터 서비스를 위한 효율적인 상호 인증과 키 분배 프로토콜을 제안하고 분석한 후, 1xEV-DO 무선 인터페이스 패킷 데이터 보안을 위한 키 생성에 적용한다. 마지막 4장은 결론이다.

II. cdma2000 Mobile IP 참조 모델과 안전성 요구 사항

2.1 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].

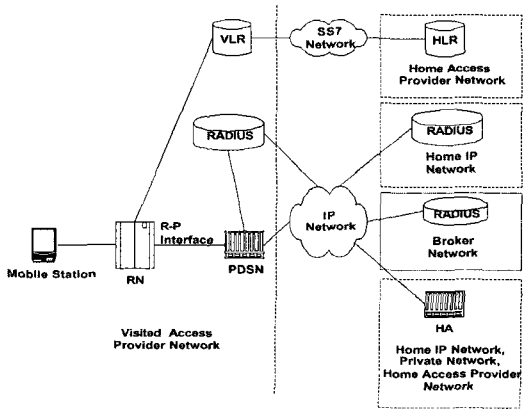
- Simple IP : Simple IP는 MN이 local Packet Data Service Node(PDSN)로부터 동적으로 할당된 IP 주소를 가지고 local service provider 네트워크에 의해 라우팅 서비스가 제공되는 서비스이며, local PDSN 이상의 IP 주소 이동성(mobility)을 제공하지 않는다. 따라서 MN은 새로운 (PDSN) 네트워크로 로밍(roaming)하면 새로운 Transport Layer 연결을 설정해야 한다.
- Mobile IP : Mobile IP는 RFC2002에 기반한 서비스로 MN이 다른 PDSN에 연결된 radio 네트워크간 핸드 오프가 발생할 때에도 영구 IP 주소를 유지할 수 있는 서비스이다. 즉 Transport Layer 연결이 영

향을 받지 않는다. MN은 static IP 주소 또는 MN의 home IP 네트워크로부터 동적으로 할당된 IP 주소를 사용할 수 있다.

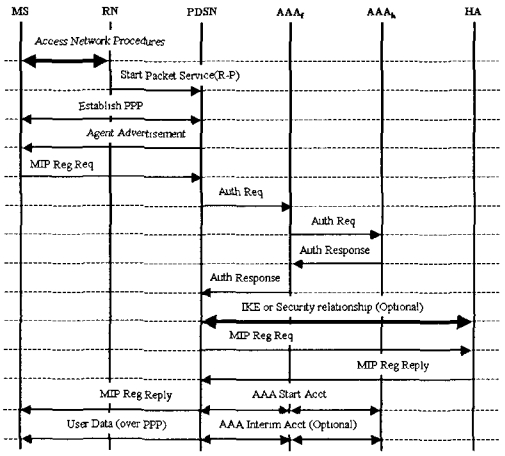
또한 패킷 데이터 서비스가 가능한 MS(mobile station)은 독립 모드와 중계 모드로 동작할 수 있다, 중계 모드에서 MS는 액세스 계층 부분만을 지원하는 cdma2000 패킷 데이터 모뎀으로만 동작하고 MN은 데이터 포트로 MS에 연결되고 상위 계층인 PPP, IP(Internet Protocol), Mobile IP 계층을 제공한다. 즉 MN은 랩탑 PC의 형태이다. 반면에 독립 모드에서 MS는 MN과 AT(access terminal)로 동작한다. 즉 액세스 계층으로부터 Mobile IP 계층의 완전한 프로토콜 스택이 같은 장비에 존재한다.

본 논문에서는 패킷 데이터 서비스를 위해 Mobile IP 액세스 기법을 사용하는 경우만을 고려한다. 3GPP2 P.S0001-A에 정의된 Mobile IP 참조 모델은 [그림 2]와 같다. cdma2000 패킷 데이터의 상황에서 PDSN은 MN이 홈 또는 방문 망에 있는지에 무관하게 항상 FA(foreign agent)로 동작한다. MN과 PDSN간의 데이터 링크 프로토콜로 PPP가 사용된다. PPP는 MN과 PDSN간에 IP 데이터그램이 교환되기 이전에 설정되며, MN과 PDSN간에 하나의 PPP 세션만이 지원된다.

현재의 표준 문서는 Mobile IP에 대해 CHAP (challenge-handshake authentication protocol) 또는 PAP(password authentication protocol)가 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 3]과 같다. 2001년 12월 3GPP2 회의에서 Verizon Wireless 사는 패킷 데이



〔그림 2〕 Mobile IP 액세스를 위한 참조 모델



〔그림 3〕 RADIUS AAA를 사용한 초기 등록 과정

터 서비스를 위한 Simple IP와 Mobile IP의 안전성을 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].

2.2 안전성 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 것을 인가할 수 있어야 한다. 동시에 MN은 AAAH를 인증할 수 있어야 한다.

(2) 세션키 설정 : 개체들간에 임시 세션키를 설정할 수 있도록 세션 마스터 키(MSK)를 생성해야 한다. MSK는 MN과 AAAH만 알 수 있어야 하고, MSK가 새롭고 랜덤하다는 것이 보장되어야 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 세션키들은 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.

추가적으로 불법적인 사용자가 방문 망으로부터 서비스를 제공받는 것을 방지해야 하고, 공격자가 다른 사용자에 의해 설정된 통신 세션에 대한 제어를 강탈하는 것(세션 하이재킹)을 방지해야 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. 그리고 제안된 기법에서 AAAH와 HA, AAAH와 AAAF, AAAF와 FA 사이의 중요 데이터(세션 키 등) 교환은 DIAMETER AAA의 시큐리티 서비스에 의해 보호된다고 가정한다.

3.1 용어

- AAA : Authentication, Authorization and Accounting DIAMETER 서버
- AAAH : home AAA 서버
- AAAF : foreign AAA 서버
- $AUTH_{HA}$: MN의 challenge에 대한 HA의 응답
- $AUTH_{MN}$: FA challenge에 대한 MN의 응답
- FA : foreign agent. PDSN이 FA의 기능을 수행한다.
- 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
- N_F : FA의 challenge(nonce)
- N_H : AAAH의 challenge(nonce)
- N_M : 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.

3.2 제안된 프로토콜

제안된 프로토콜은 [그림 4]와 같이 동작한다.

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

(2) MN은 challenge nonce N_M을 생성하고, 루트 키 RK를 사용하여 다음처럼 MN Authentication Response $AUTH_{MN}$을 계산한다.

AUTH_MN = MAC(RK, FA_ID||AAAF_ID||N_F||N_M||NAI)

MN은 NAI, N_F, N_M, $AUTH_{MN}$을 포함한 Registration Request 메시지를 PDSN에게 전달한다.

(3) PDSN은 N_F를 검증한 후 N_F, N_M, NAI, $AUTH_{MN}$을 포함한 DIAMETER AMR(AA-Mobile-Node-Registration-Request) 메시지를 AAAF에게 전송한다.

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

(5) AAAH는 먼저 $AUTH_{MN}$을 검증한다. 검증이 성공하면, MN의 challenge인 N_M에 대한 AAAH Authentication Response $AUTH_{HA}$를 다음처럼 계산한다.

$AUTH_{HA}$ =MAC(RK, N_M || N_F ||NAI|| AAAF_ID||FA_ID)

AAAH는 N_H를 생성하고, 세션 마스터 키 MSK를 계산한다.

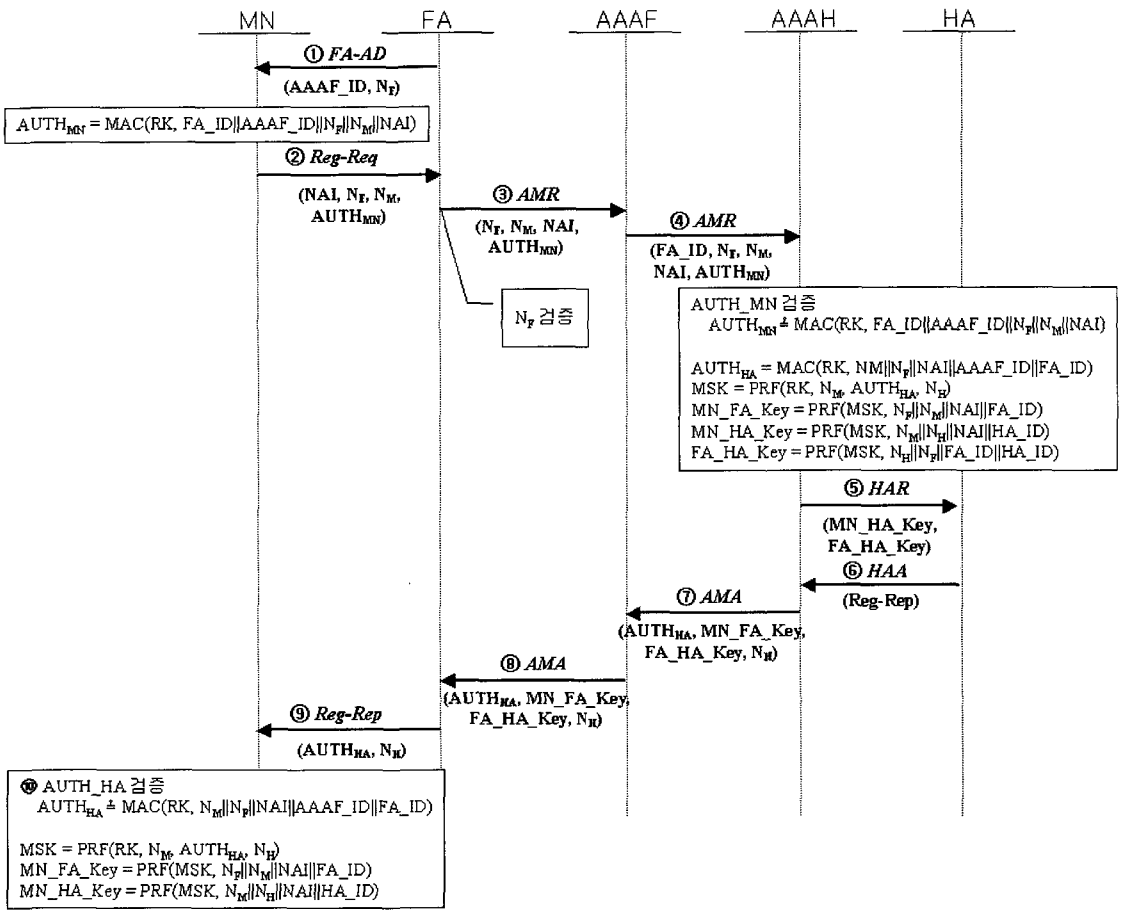
MSK = PRF(RK, N_M || $AUTH_{HA}$ || N_H)

생성된 MSK를 사용하여 Mobile IP 세션키들을 계산한다.

MN_FA_Key = PRF(MSK, N_F || N_M ||NAI||FA_ID)

MN_HA_Key = PRF(MSK, N_M || N_H ||NAI||HA_ID)

FA_HA_Key = PRF(MSK, N_H || N_F ||FA_ID||HA_ID)



〔그림 4〕 제안된 상호 인증과 키 분배 프로토콜

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, N_H를 포함한 AMA(AA-Mobile-Node-Registration-Answer) 메시지를 AAAF에게 전송한다.

(8) AAAF는 AMA를 PDSN에게 전달한다.

(9) PDSN은 $AUTH_{HA}$, N_H를 포함한 Registration Reply 메시지를 MN에게 전달한다.

(10) MN은 $AUTH_{HA}$를 검증한다. 검증이 성공하면, 세션 마스터 키 MSK를 계산한 후, Mobile IP 세션키들을 유도한다.

$$MSK = PRF(RK, N_M \,||\, AUTH_{HA} \,||\, N_H)$$

$$MN\_FA\_Key = PRF(MSK, N_F \,||\, N_M \,||\, NAI||FA\_ID)$$

$$MN\_HA\_Key = PRF(MSK, N_M \,||\, N_H \,||\, NAI||HA\_ID)$$

$$FA\_HA\_Key = PRF(MSK, N_H \,||\, N_F \,||\, FA\_ID||HA\_ID)$$

3.3 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([그림 3]에서 Auth Req, Auth Response, MIP Reg Req, MIP Reg Reply 메시지) 교환이 발생하지만 제안된 프로토콜에서는 2번의 메시지([그림 4]에서 4번과 7번 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 안전성 요구 사항을 모두 만족한다.

(1) 상호 인증 : 단계 5에서 AAAH는 $AUTH_{MN}$ 검증을 통해 MN을 인증할 수 있다. $AUTH_{MN}$의 계산에 N_F가 포함됨으로써 매 세션마다 freshness가 보장된다. 또한 NAI가 포함됨으로써 공유 비밀키 RK와 사용자 신분간의 정확한 binding이 보장된다. MN은 단계 9에서 challenge N_M에 대한 AAAH의 응답인 $AUTH_{HA}$ 검증을 통해 AAA H를 인증한다. $AUTH_{HA}$의 freshness는 N_M에 의해 보장된다.

(2) 세션키 설정 : MN과 AAAH는 세션 마스터 키 MSK를 생성한다. 이 키를 사용하여 Mobile IP 개체들간에 세션키를 설정한다. MSK는 무선 구간으로 전달되지 않고, MN과 AAAH에 의해 공유된 비밀키 RK와 nonce에 기반하여 유도된다. 따라서 RK를 알지 못하는 공격자가 MSK를 획득하기 위한 최선의 방법은 랜덤한 추측 공격이다. MSK의 freshness와 랜덤성은 N_M, N_H, $AUTH_{HA}$의 freshness와 PRF의 성질로부터 보장된다. 그리고 추가적으로 AAAH와 HA, AAAH와 AAAF, AAAF와 FA 사이의 세션 키 교환은 DIAMETER AAA의 시큐리티 서비스에 의해 보호된다.

(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, $AUTH_{MN}$의 유효성은 FA의 유효성을 함축한다.

(5) MN에 의한 경로 인증 : MN은 FA를 암호학적으로 인증하지 않지만, 위에서 기술한 것처럼 AAA F_ID와 FA_ID가 포함된 $AUTH_{HA}$의 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. 위장 방지는 위의 안전성 요구 사항으로부터 쉽게 유도된다. 네트워크 개체에 대한 honesty 가정이 성립하면, MN의 인증은 서비스 제공업자에게 정당한 사용자가 서비스를 제공받는다는 것을 보장한다. 또한 세션 마스터 키 MSK의 비밀성은 불법적인 사용자가 기존의 세션을 하이재킹할 수 없다는 것을 보장한다.

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.

3.4 cdma2000 1xEV-DO 무선 인터페이스 패킷 데이터 보안을 위한 키 생성

cdma2000 1xEV-DO는 무선 인터페이스 상에서 패킷 데이터 암호화와 인증을 제공할 수 있는 Access Security 계층을 정의하며, 트래픽 채널에 인증과 암호화를 적용할 수 있다. 또한 두 개체간에 공유 비밀키를 분배하기 위해 Diffie-Hellman(DH) 키 교환 기법을 이용한다. 하지만 DH 키 교환은 수동적 도청자에 대해서만 안전하고, 키 교환 개체들을 인증하지 않기 때문에 능동적 공격자(Man-in-the-Middle (MIM) 공격자)에 대해 취약하다. 또한 DH 키 교환은 무선 단말기에서 계산량적으로 복잡한 모듈러 지수승 연산을 수반한다.

최근 Carroll은 1xEV-DO가 패킷 데이터 세션 하이재킹에 대해 취약하며 DH 키 교환에 대해 다음과 같이 간단히 MIM 공격이 수행될 수 있다는 것을 지적하였다[7]. MIM 장치는 액세스 터미널에게 cdma2000 네트워크로 위장하고 동시에 cdma2000 네트워크에 대해서는 액세스 터미널로 위장한다. 모든 액세스 계층 시큐리티 키들이 DH 키 교환으로부터 유도되기 때문에 액세스 계층 트래픽 채널 인증 또는 암호화가 적용되더라도 능동적 MIM 공격자는 정당한 사용자의 NAI에 기반하여 세션에 패킷을 주입할 수 있다.

이러한 문제는 Carroll에 의해 지적된 것처럼 무선 액세스 계층이 아닌 상위 프로토콜 계층에서 분배된 키를 이용하여 무선 인터페이스 상의 패킷 데이터에 대한 암호화와 인증을 위한 키를 생성함으로써 해결될 수 있다[7]. 이를 위해 3.2절에서 제안된 AAA와 Mobile IP 하부 구조에서 상호 인증과 키 분배 과정에서 MN과 PDSN에게 분배된 MN_FA_Key로부터 1xEV-DO 무선 인터페이스 패킷 데이터 암호화

와 인증을 위한 키를 생성한다. 이것은 패킷 데이터 서비스 사용을 위해 AAA/Mobile IP 등록 과정을 거친 후 액세스 계층 시큐리티 키 교환(DH 키 교환) 과정을 독립적으로 수행하는 것보다 효율적이며, 또한 낮은 계산 처리 능력을 가진 MN에서 복잡한 모듈러 지수승 연산을 없앨 수 있다.

MN은 MN_FA_Key가 악의적인 MS에게 노출되는 것을 방지하기 위해 다음과 같이 MN_FA_Key와 PDSN으로부터 동적으로 할당된 Unicast Address(UATI)에 기반하여 다음처럼 액세스 터미널 키 AT_Key를 생성할 수 있다.

$$AT\_Key = PRF(MN\_FA\_Key, UATI)$$

여기서 UATI는 PDSN으로부터 액세스 터미널(AT)에게 동적으로 할당된 값으로 각 액세스 계층 세션 동안 유일한 값이다. AT는 동적으로 UATI를 할당받아 MN에게 전달한다.

AT은 MN으로부터 수신한 AT_Key를 이용하여 1xEV-DO 액세스 계층에서 메시지 인증과 암호화를 위한 키들을 다음과 같은 형태로 생성할 수 있다.

$$Auth\_Key = PRF(AT\_Key, "1")$$
$$Enc\_Key = PRF(AT\_Key, "2")$$

PDSN 역시 Mobile IP 등록 과정에서 홈 AAA 서버로부터 전송된 MN_FA_Key와 자신이 AT에게 할당한 UATI로부터 AT_Key를 유도한 후 액세스 계층 시큐리티를 위한 인증과 암호화 키를 유도한다.

Ⅳ. 결 론

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 안전성 요구 사항을 모두 만족하며, 초기 셋업 시간에 최소한의 영향을 준다. 또한 제안된 프로토콜을 통해 분배된 키를 이용하여 무선 인터페이스 상의 패킷 데이터 암호화와 인증을 위한 키를 생성함으로써 1xEV-DO에 대한 패킷 데이터 세션 하이재킹 공격을 방지할 수 있다.

제안된 상호 인증과 키 분배 프로토콜에 대한 증명 가능한 안전성은 [5]과 [6]에 적용된 것들과 유사한 기법에 의해 증명될 수 있을 것으로 보이지만, 이것에 대한 엄밀한 증명은 향후 연구 과제이다.

참 고 문 헌

[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.

〈著者紹介〉

신 상 욱 (Sang Uk Shin) 정회원

1995년 2월 : 부산수산대학교(현 부경대학교) 전자계산학과(학사)
1997년 2월 : 부경대학교 전자계산학과(석사)
2000년 2월 : 부경대학교 전자계산학과(박사)
2000년 4월~현재 : 한국전자통신연구원 선임연구원
<관심분야> 암호학, 이동통신 보안

류 희 수 (Heuisu Ryu) 정회원

1990년 2월 : 고려대학교 수학과(학사)
1992년 2월 : 고려대학교 수학과(석사)
1999년 5월 : Johns Hopkins University 수학과(박사)
2000년 7월~현재 : 한국전자통신연구원 선임연구원
<관심분야> 정보보호이론, 타원곡선암호