AAA 인증을 고려한 Smooth handoff

° 김인수 ° 김기천 김현곤
° 건국대학교 컴퓨터공학과 한국전자통신연구원
darkguy@konkuk.ac.kr kckim@konkuk.ac.kr hyungon@etri.re.kr

Smooth handoff for AAA protocol

° In-Su Kim ° Kee-Cheon Kim Hyun-Gon Kom
° Dept. of Computer Engineering Science, Kon-kuk University / ETRI

요 약

*IMT-2000*망 핵심기술은 *mobile IP*를 이용하는 북미의 *3G packet data system*과 GSM망과 연계를 하는 유럽의 GPRS로 구분할 수 있다. Mobile IP상에서는 RADIUS나 DIAMETER같은 AAA 서버가 다이얼 업 컴퓨터의 인증, 허가 서비스를 제공하기 위해 사용되고 있는데, 이것은 MN에게 매우 중요하다. Mobile IP는 MN과 HA간에 강력한 인증을 요구하기 때문이다. 본 논문에서는 이러한 IMT-2000 환경에서 고려되고 있는 Smooth Handoff 지원 방안에 관하여 논한다.

1. 서 론

IMT-2000 핵심 망 기술은 mobile IP를 이용하는 북미의 3G packet data system과 GSM망과 연계를 하는 유럽의 GPRS로 구분할 수 있다.

3G packet data system은 제3세대 ANSI-41 네트워크 및 이를 기초로 한 cdma2000 무선접속 기술 및 단말기 등 세부 규격 작성을 위해 1999년 1월 결성된 3GPP2에서 표 준화가 진행중이다. 3G packet data system은 IMT-2000의 핵심망 구조로써 회선 교환망과 패킷 교환망이 분리된 형태를 가지며 패킷 교환망은 기본적으로 이동 에이전트 (Mobile Agent)를 이용하여 패킷의 이동성을 지원하고 보안, 인증 서비스를 강화하여 사용자로 하여금 인터넷과 사설망의 서비스까지도 이용 가능하도록 표준화가 진행 중에 있다.

GPRS는 GSM네트워크와 이를 기초로 한 W-CDMA 접속기술과 단말기등의 세부규격을 작성하기 위한 표준화 기구인 3GPP에서 표준화가 진행 중이다. GPRS도 역시 회선 교환망과 패킷 교환망이 분리된 형태를 가지며 2세대의 GSM(Group Special Mobile)망에서 UMTS로의 진화를 위한 과도기적인 2.5세대 패킷 교환망이다. 유럽은 이미 현재 GPRS망을 서비스 중인 곳도 있다. 그러나 GSM/GPRS기반의 핵심망을 벗어나면 로밍이 되지 않는 단점이 있으므로 이를 해결하기 위해 GPRS망에서 Mobile IP를 수용하는 'Mobile IP in UMTS', 'All IP' 형태를 단계적으로 정의하고 있다.

IMT-2000 환경에서는 단말기의 이동성에 초점을 두어서 Handoff 기술이 필연적으로 필요하게 된다. 따라서, Handoff를 얼마나 유연하게 구현하는가, 또한 얼마나 안전한 메커니즘을 통해서 이루어지는가가 주요 관심사가 될 수밖에 없다. 현재 Smooth Handoff를 위해 나와있는 기술에는 계층적 에이전트를 사용한 지역적 등록이 있다.

MN는 인터넷 링크계층의 접속 점을 바꾼 후에도 다른 노드와 계속적인 통신이 필요하게 된다. 이 때 HA가 MN으로부터 멀리 떨어져 있을 경우 HA로의 잦은 등록은 많은 오버헤드 야기하게 된다. FA들을 계층적으로 구성하여 각 계층에서 하부 이동만을 관리하게 되는 지역적 등록(Regional Registration)이 필요하게 된다.

Mobile IP상에서는 RADIUS나 DIAMETER같은 AAA 서버가 다이얼 업 컴퓨터의 인증, 허가 서비스를 제공하기 위해 사용되고 있는데, 이것은 MN에게 매우 중요하다. Mobile IP는 MN과 HA간에 강력한 인증을 요구하기 때문이다.

2. Smooth handoff 지원방안

IMT-2000 환경에서는 단말기의 이동성에 초점을 두어서 Handoff 기술이 필연적으로 필요하게 된다. 따라서, Handoff를 얼마나 유연하게 구현하는가, 또한 얼마나 안전한 메커니즘을 통해서 이루어지는가가 주요 관심사가 될 수밖에 없다. 현재 Smooth Handoff를 위해 나와있는 기술에는 계층적 에이전트를 사용한 지역적 등록이 있다.

MN는 인터넷 링크계층의 접속 점을 바꾼 후에도 다른 노드와 계속적인 통신이 필요하게 된다. 이 때 HA가 MN으로부터 멀리 떨어져 있을 경우 HA로의 잦은 등록은 많은 오버헤드 야기하게 된다. FA들을 계층적으로 구성하여 각 계층에서 하부 이동만을 관리하게 되는 지역적 등록(Regional Registration)이 필요하게 된다.

Mobile IP는 MN과 FA간에 링크계층에서의 연결을 요구한다. IMT-2000망에서는 RNN(Radio Network Node), PSDN(Packet Data Serving Node)사이의 RP 인터페이스 에서의 핸드오프 처리가 이에 해당한다. 유-무선 인터페이스에서의 Mobile IP적용은 Mobile IP의 지역적 등록과 연계될 수 있다.

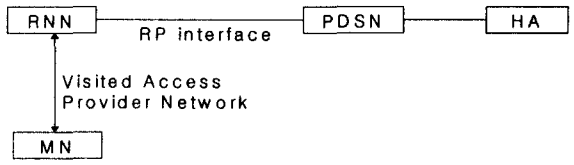

그림 1 . 무선환경에서의 이동성관리

IMT-2000망에서의 MN등록은 MN-PDSN간의 등록과 PDSN-HA간의 등록 2단계로 나누어 생각할 수 있다. 이 때 PDSN-GFA, RNN-RFA로 대응관계가 성립된다.

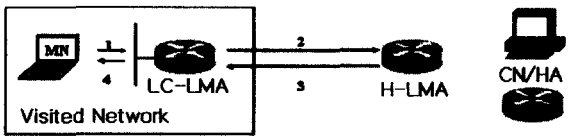

그림 2 . Smooth handoff를 위한 Agents

위의 그림은 이동성있는 노드에 대하여 smooth handoff를 지원해 주기 위한 agent들을 나타낸 모양이다. LC-LMA는 Link Connected Local Mobility Agents로써 MobileIP상의 Foreign Agent와 유사한 기능을 한다. H-LMA는 Higher Local Mobility Agents로써, handoff 시 발생되는 등록정보를 중간에서 조정해준다. 즉 동일한 H-LMA하에서의 MN의 이동에 대해서는 최상위 HA에 등록하는 대신에 H-LMA에 대한 등록을 실시하므로써, handoff시에 발생되는 네트워크의 부하를 줄일 수 있다.

3. AAA 인증과정

Mobile IP상에서는 RADIUS나 DIAMETER같은 AAA 서버가 다이얼 업 컴퓨터의 인증, 허가 서비스를 제공하기 위해 사용되고 있는데, 이것은 MN에게 매우 중요하다. Mobile IP는 MN과 HA간에 강력한 인증을 요구하기 때문이다.

AAA서버들은 MN를 식별하기 위해 NAI를 사용하고, 이 때 항상 홈 주소가 필요하지는 않다. 그래서 MN들은 홈 주소 없이 자신을 인증하고 Foreign Domain에 접속 허가를 받는 것이 가능하다. Mobile IP가 동작하려면 MN는 HA와의 보안협력(Security Association)을 가져야만 한다. Mobile IP 등록응답이 MN-AAA 인증확장(MN-AAA Authentication Extension)에 의해 인증되면 MN는 AAA서버가 만든 키 들을 확장 안에서 확인할 수 있고, HA나 FA와의 보안협력을 생성하는 일을 신뢰할 수 있게 한다.

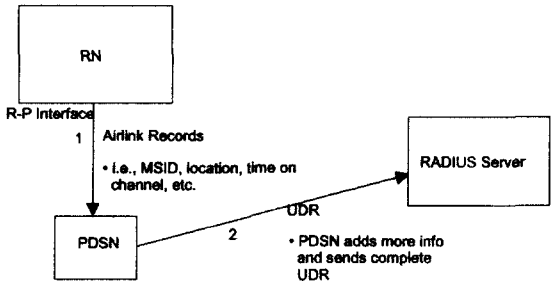

그림 3 . AAA 인증과정

AAA 서버의 인증과정을 살펴보면 다음과 같다.

① MN가 홈 네트워크에서 떠나면 홈 주소를 가지지 않기 때문에 HA와의 보안협력을 가지지 않게 된다.
② MN가 처음으로 HA에 등록할 때 등록요청에 MN-AAA 인증확장을 포함한다.
③ MN-AAA 인증확장내의 정보가 AAA서버에 의해 확인되면 AAA서버는 MN를 위해 키를 생성하고 MN과의 보안협력에 따라 키를 인코딩한 후 등록응답에 삽입한다.
④ 만약 응답이 인증을 통과하고, AAA 확장안에 MN-HA 키가 포함되어 있으면 MN는 AAA와의 보안협력에 따라 키를 디코딩한다. 키는 HA와의 보안협력을 생성하고, MN-HA 인증확장을 인증하는데에 사용된다.
⑤ 유사하게 만약 응답이 인증을 통과하고, AAA 확장안에 MN-FA 키가 포함되어 있으면 MN는 AAA와의 보안협력에 따라 키를 디코딩한다. 키는 FA와의 보안협력을 생성하고, MN-FA 인증확장을 인증하는데에 사용된다.

등록응답이 AAA 확장내에 MN-HA 키를 포함하고 있으면, 등록응답은 MN-HA 키에 의해 생성된 Mobile Home 인증확장을 포함해야 한다. 마찬가지로 등록응답이 AAA 확장내에 MN-FA 키를 포함하고 있으면, 등록응답은 MN-FA 키에 의해 생성된 Mobile Foreign 인증확장을 포함해야 한다.

4. AAA 인증을 고려한 Smooth handoff

기존의 AAA인증과정은 MN은 반드시 직접 홈 네트워크의 AAA 서버로부터 인증을 받아야 한다. 이 과정에서 국지적인 이동이 발생시에, MN은 HA와의 연결을 위해

다시 홈 네트워크의 AAA서버와의 인증과정을 거쳐야 하고, 이것은 홈네트워크와의 거리가 멀거나 이동이 빈번할시에 지연을 발생시키는 문제점을 나타낸다. 또한 Smooth handoff 알고리즘의 이동성관리의 장점을 소실시키게 된다. 따라서, 본 연구에서는 에이전트의 계층화와 마찬가지로, AAA서버의 계층화를 제안한다.

방문 도메인에는 홈 네트워크의 AAA서버와는 별개의 지역적인 AAA서버를 두어서, 방문한 MN을 인증하고, 자신은 홈 네트워크의 AAA서버로부터 인증을 받는다.

방문 도메인에 있는 AAA서버는 기존의 인증과정을 활용하여 접속된 MN을 인증하게되고, 그 도메인 내에서의 이동은 홈 네트워크의 재 인증을 받지 않도록 한다.

홈 네트워크의 AAA서버는 MN의 인증이 필요할 시에는 해당하는 방문 도메인의 AAA서버와 연동되어 처리한다.

만약, MN이 도메인간의 이동을 하여 새로운 도메인에 방문했을시는, 등록과정과 함께 지역내 AAA서버와의 인증과정, 지역내 AAA서버와 홈 네트워크의 AAA서버와의 공조가 발생하게 된다. 홈 네트워크의 AAA서버는 각각의 MN들의 인증을 담당하는 대신, 해당하는 방문 도메인들의 에이전트와 AAA서버만의 인증을 관리하게 되어. 인증과정시에 생기는 지연을 감소시키고, 보다 유연한 handoff과정을 이끌어낼 수 있게된다.

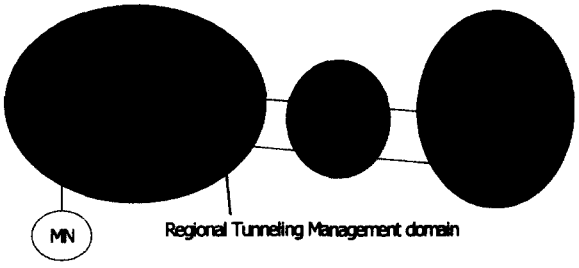

그림 4 . 계층적 인증모형

5. 참고문헌

[1] Charles E. Perkins, Mobile IP, Addison Wesley, 1998.

[2] A. Bakre and B.R. Badrinath, "I-TCP : Indirect TCP for Mobile Hosts", Proceedings of the 15th international conference on distributed computing systems, June, 1995.

[3] K.I.Kim, et al, "Locality-based Internet Mobile Protocol," APCC/ICCS 98.

[4] C. Perkins, "Mobile IP support", Internet RFC 2002, Oct 1996

[5] 3GPP2, "Wireless IP Network Standard based on IETF protocol", 3GPP2 Document, Dec 1999

[6] R. Ramjee / T. La Porta/S. Thuel / K. Varadhan / L. Salgarelli, "IP micro-mobility support using HAWAII", Internet Draft, Jun 1999