Smooth Handoff 지원을 위한 빠른 인증 알고리즘

김 인 수[†]·김 기 천[††]·김 현 곤[†††]

요 약

IMT-2000망 핵심기술은 mobile IP를 이용하는 북미의 3G packet data system과 GSM망과 연계를 하는 유럽의 GPRS로 구분할 수 있다. 이러한 IMT-2000망 핵심기술은 글로벌한 로밍을 위해 Mobile IP 도입을 추진하고 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 기법에서 효과적인 AAA프로토콜의 적용에 관하여 논한다.

A Fast Authentication Algorithm For Smooth Handoff

In-Su Kim[†] · Kee-Cheon Kim[††] · Hyun-Gon Kim[†††]

ABSTRACT

IMT-2000 technologies are divided 3G packet data system that using mobile IP and GPRS that based on the GSM networks. These technologies push introduce mobile IP to support seamless roaming. In mobile IP environments, use AAA server such as RADIUS or DIAMETER to provide authentication service for dial-up computers. This factor is important for mobile nodes. Mobile IP require strong authentication between mobile nodes and home agents. We propose application of AAA protocols for smooth handoff mechanism in IMT-2000 environments.

키워드 : 모바일 IP(Mobile IP), AAA, 핸드오프(Handoff)

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 표준화가 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 위

※ 본 논문은 2001년도 한국전자통신연구원 정보보호연구본부의 연구비 지원에 의해서 수행되었습니다.
† 준 회 원 : 건국대학교 대학원 컴퓨터공학과
†† 종신회원 : 건국대학교 컴퓨터공학과 교수
††† 정 회 원 : 한국전자통신연구원 AAA정보보호연구팀장
논문접수 : 2001년 12월 31일, 심사완료 : 2002년 1월 16일

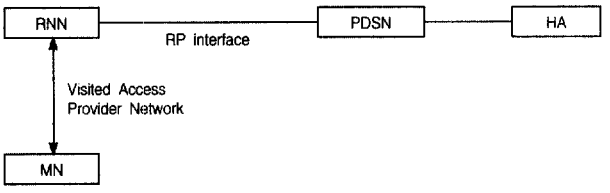
해 사용되고 있는데, 이것은 MN에게 매우 중요하다. Mobile IP는 MN과 HA간에 강력한 인증을 요구하기 때문이다.

2. Micro Mobility 기술을 이용한 Smooth handoff 지원

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 Micro Mobility를 이용한 계층적인 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 인터페이스에서의 핸드오프 처리가 이에 해당한다. 유-무선 인터페이스에서의 Mobile IP적용은 Mobile IP의 지역적 등록과 연계될 수 있다.



(그림 1) R-P Interface

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

3. Mobile IP의 인증확장

AAA서버들은 MN를 식별하기 위해 NAI를 사용하고, 이 때 항상 홈 주소가 필요하지는 않다. 그래서 MN들은 홈 주소 없이 자신을 인증하고 Foreign Domain에 접속허가를 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 키들을 확장 안에서 확인할 수 있고, HA나 FA와의 보안협력을 생성하는 일을 신뢰할 수 있게 한다.

AAA 서버의 인증과정을 살펴보면 다음과 같다.

- MN가 홈 네트워크에서 떠나면 홈 주소를 가지지 않기 때문에 HA와의 보안협력을 가지지 않게 된다.
- MN가 처음으로 HA에 등록할 때 등록요청에 MN-AAA 인증확장을 포함한다.
- MN-AAA 인증확장내의 정보가 AAA서버에 의해 확인되면 AAA서버는 MN를 위해 키를 생성하고 MN과의 보안협력에 따라 키를 인코딩한 후 등록응답에 삽입한다.
- 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.
- 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. 인증을 고려한 Mobile IP의 등록절차

Mobile IP의 등록전에는 MN-HA, MN-FA, FA-HA간의 인증확장(Authentication Extension)들이 준비되어야 한다. Mobile IP의 기본 인증 알고리즘은 prefix+suffix 모드의 keyed-MD5 알고리즘이다.

(1) FA→MN : AgentAd
(2) MN→FA : RegReq, h(RegReq)k FM, h(RegReq)k HM
(3) FA→HA : RegReq, h(RegReq)k FH, h(RegReq)k HM

kFM, kHM, kFH : FA-MN, HA-MN, FA-HA 간의 약속된 키

h(m)k : 키 k에 의해 암호화되는 해싱 값
AgentAd : 에이전트 광고 메시지
RegReq : 등록요청 메시지

이 방법은 모든 노드에 해당하는 키를 가지고 있어야 하는 문제점 때문에 확장성문제가 지적되었다. 그래서 이 문제를 해결할 수 있는 인증서기반의 알고리즘이 제시된다. 이 방법은 우선 키의 분배문제가 효율적이다. 인증서기반의 방법에서는 인증서들을 인증해 줄 수 있는 CA(Certificate Authority)가 존재한다. CA는 신뢰성있는 에이전트이며, 자신의 공개키를 노드들에 배포한다. CA는 다른 노드의 공개키를 자신의 비밀키로 암호화하며, 다른 노드들은 CA의 공개키로 복호화할 수 있다.

(1) FA→MN : AgentAd, h(AgentAd)kFA, CertFA
(2) MN→FA : RegReq, h(RegReq)kMN, CertMN
(3) FA→HA : RegReq, h(RegReq)kMN, h(RegReq)kFA, CertFA

(4) HA→FA : RegRep, h(RegRep)kHA, CertHA
(5) FA→MN : RegRep, h(RegRep)kHA

CertA : A의 인증서
kA : A의 비밀키

5. Micro Mobility환경의 Smooth Handoff를 위한 인증 알고리즘

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.

위의 두 경우 모두 홈 네트워크의 AAA 서버(Radius)와 지역 네트워크의 AAA서버가 CA로 동작을 하게된다.

최초 등록시 MN-FA-GFA-HA를 거치는 과정에서는 앞절에 나타낸 인증서기반의 등록절차를 따른다.

(1) FA→MN : AgentAd, h(AgentAd)kFA, CertFA
(2) MN→FA : RegReq, h(RegReq)kMN, CertMN
(3) FA→GFA : RegReq, h(RegReq)kMN, h(RegReq)kFA, CertFA
(4) GFA→HA : RegReq, h(RegReq)kMN, h(RegReq)kGFA, CertGFA
(5) HA→GFA : RegRep, h(RegRep)kHA, CertHA
(6) GFA→FA : RegRep, h(RegRep)kHA, CertHA
(7) FA→MN : RegRep, h(RegRep)kHA, CertHA

CertA : A의 인증서
kA : A의 비밀키

각 인증서에는 공개키, 인증서의 ID, 인증서의 시간값이 포함된다. 그리고, 홈 네트워크의 AAA서버에는 MN의 공개키가 있다고 가정된다. 여기에서 메시지의 암호화에 사용된 각 키는 인증확장의 SPI필드, 인증서는 Authenticator 필드에 첨가된다.

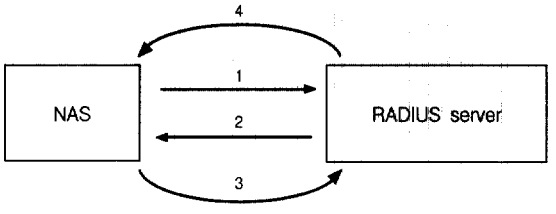
상기된 절차중, 한 군데에서라도 인증과정을 통과하지 못하면 등록 실패 메시지가 돌아오게 된다.

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 있게 된다. 이때, GFA는 HA의 인증서를 등록응답 메시지에 삽입시켜서, MN으로 하여금 등록이 성공적으로 끝났음을 확인하게 한다. 이 때, MN의 인증서는 최초 등록시에 GFA에게로 전달된다.

(1) FA→MN : AgentAd, h(AgentAd)kFA, CertFA
(2) MN→FA : RegReq, h(RegReq)kMN, CertMN
(3) FA→GFA : RegReq, h(RegReq)kMN, h(RegReq)kFA, CertFA
(4) GFA→FA : RegRep, h(RegRep)kGFA, CertGFA
(5) FA→MN : RegRep, h(RegRep)kGFA, CertGFA

CA의 역할을 하게 되는 RADIUS서버는 Challenge/Response 인증방법을 통해서 인증서를 발급한다. 서버는 인증서를 요청하는 클라이언트에 특정한 Challenge값을 전송하고, 클라이언트는 Challenge에 해당하는 응답을 Server에 전송한다. Challenge값에는 클라이언트가 응답할 메시지의 암호화 방법이 명시된다. 이 응답에는 각 노드가 Radius에 등록할 때 사용한 자신의 홈주소/홈네트워크의 RADIUS 서버주소 등이 포함된다. 이 때, RADIUS에 해당하는 엔트리가 없을 시에는 홈네트워크의 RADIUS서버와의 연동으로 노드의 공개키를 가져와서 인증서를 작성하고, 해당 노드에 access-accept메시지와 인증서를 전달한다.



(그림 2) RADIUS 동작모형

1) Access Request
2) Access Challenge
3) New Access Request
4) Access-accept, Access-reject, Access-challenge

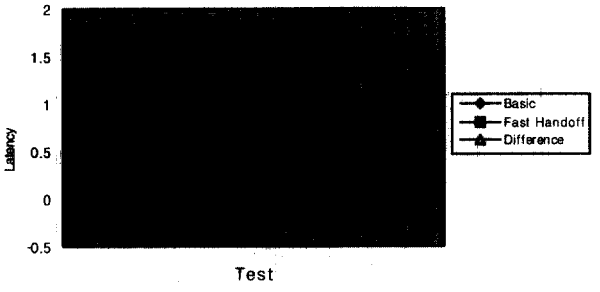
6. 성능평가

6.1 성능 평가를 위한 모델링

본 제안 기법에 대한 성능 평가를 위한 모델링은 MN이 FA1에서 현재 등록과정을 마치고 서비스를 받으려고 하는 상태를 시뮬레이션 이벤트의 시작점으로 두었다. MN이 FA1에서 등록 과정을 마친 후 FA2로 이동할 수 있도록 하였다. 그리고, MN의 FA2에서 등록 과정을 마치는 기점을 시뮬레이

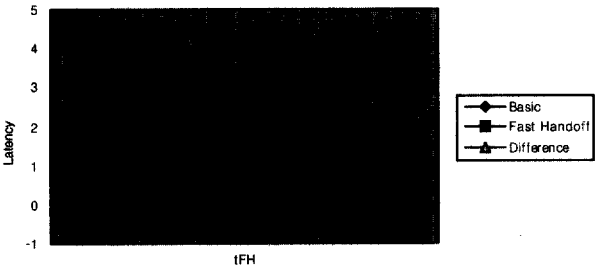
션 이벤트의 끝점으로 두었다. FA1과 FA2가 같은 GFA하의 지역 도메인내에 있을 가능성은 30%로 설정한다.

본 제안 기법과 기존 기법에 대한 성능평가를 위해서 몇 가지 가정을 두었다. 먼저, 두 기법 모두 동일하게 이동 노드가 서비스를 받기 위해서 셀에 들어오는 평균 시간을 0.6초, 나가는 평균 시간을 0.8초로 하였다. 시뮬레이션상에서 횟수는 10회로 제한하였다. 또한 MN-FA 간의 메시지 전달시간을 tMF, FA-GFA 간의 메시지 전달시간을 tFG, GFA-HA또는 FA-HA간 전달시간을 tFH로 가정하였다. 또한, AAA서버로부터 인증서를 받기까지의 평균응답시간을 tNA초, AAA서버간 연동시간을 tAA로 가정한다. 각 t값을 임의로 선택하고 시뮬레이션한 결과는 다음과 같다.



(그림 3) 평균 Handoff Latency

tFH의 변화를 주어 HA-(G)FA 간의 시간(tFH)을 변경시켜 측정해 본 결과는 다음과 같다.



(그림 4) FA-HA 거리에따른 Handoff Latency

6.2 성능 분석

본 논문의 제안 기법과 기존 기법의 핸드오프 시간을 비교한 결과로 기존 기법의 핸드오프 시간을 보면 기존 기법보다 줄어들었다는 것을 알 수 있다. 제안 기법이 최악의 경우(계속 HA의 바인딩이 갱신)되는 경우를 제외하고는 평균 핸드오프 시간의 우위를 보였다. 또한, FA-HA간 레이턴시가 커질수록 제안된 방법의 우월성이 커졌다. 그러므로 제안 기법의 핸드오프 시간이 기존 기법보다 성능이 나음을 알 수 있다.

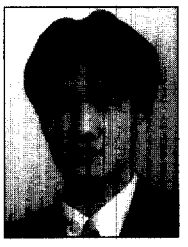
7. 결 론

IMT-2000 망의 실현이 다가오면서 이동 컴퓨팅 환경에 대한 사용자의 요구가 확대되어 가고 있다. 이러한 환경을 위해 IMT-2000에서 도입될 Mobile-IP상에서 기본적인 라우팅 기법을 그대로 사용하기보다는 보다 빠르고 손실이 적은 최적화 기법들을 적용하기 위한 연구가 필요할 것이다.

본 논문에서는 Micro Mobility 기반의 빠른 Handoff 적용 모형에서 AAA의 활용방법을 제안하고 테스트하였다. 이러한 시도의 결과로, Handoff시 발생될 수 있는 데이터의 지연과 손실을 줄이는 방법을 제안하였다. 향후 연구과제는 보다 최적화된 AAA프로토콜을 설계하여 보다 더 부드러운 핸드오프 과정을 제안할 것이다.

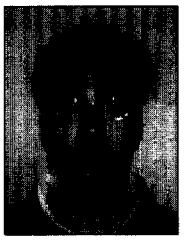
참 고 문 헌

[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 1998.
[4] C. Perkins, "Mobile IP support," Internet RFC 2002, Oct. 1996.
[5] Thomas Wu. "The Secure Remote Password Protocol," 1999, Internet Society NDSS, Mar. 1998.
[6] David Jablon, "Public Key Methods for Shared Secret Authentication," RSA'98, January 14, 1998.
[7] Bellovin & Merritt, "Encrypted Key Exchange," I.E.E.E on Security and Privacy, May, 1992.
[8] Halevi, "public-key cryptography & password protocols," ACM Trans. on ISS, Vol.2, Aug. 1999.
[9] Taekyoung Kwon, "Authentication and key agreement via memorable password," IEEE, P1363, Aug. 20, 2000.



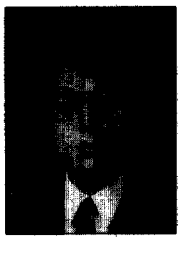
김 인 수

e-mail : darkguy@konkuk.ac.kr
2000년 건국대학교 컴퓨터공학과 학사
2000년~현재 건국대학교 일반대학원 컴퓨터공학과 석사과정
관심분야 : 이동 인터넷, 모바일 미들웨어, IMT-2000



김 기 천

e-mail : kckim@konkuk.ac.kr
1988년 서울대학교 계산통계학과 학사
1992년 미 Northwestern University 전산학 박사
1992년~1996년 한국통신기술(주) 연구소 선임연구원
1996년~1998년 신세기통신(주) 기술연구소 책임연구원/차장
1998년~현재 건국대학교 컴퓨터공학과 조교수
관심분야 : 차세대 인터넷, 이동 컴퓨팅, IMT-2000



김 현 곤

e-mail : hyungon@etri.re.kr
1992년 금오공과대학교 전자공학과 학사
1994년 금오공과대학교 전자공학과 석사
1998~현재 충남대학교 전자공학과 박사과정
1994~현재 한국전자통신연구원 정보보호연구본부 AAA정보보호연구팀장
관심분야 : 차세대 이동통신, 이동통신 정보보호, 무선 인터넷 정보보호