능동 네트워크에서의 향상된 AAA 구조방안

이효성[O], 김기천, 김인수
건국대학교 컴퓨터공학
{angelkis[O], kckim, insu}@cse.konkuk.ac.kr

An Enhanced AAA Mechanism in Active Netwok

Hyosoung Lee[O], Keecheon Kim, Insu Kim
Dept. of Computer Science, Kon-Kuk University

요 약

본 논문에서는 액티브 라우터를 이용 Enhanced Mobility Management(EMM) 알고리즘을 사용하는 이동성관리 구조에서, 이동노드의 신뢰성 확보를 위한 AAA프레임워크와의 연동모형을 전제로 한다. 액티브 라우터로 구성된 능동망내에서 액티브 캡슐에 의한 EMM모듈의 운용시 발생할 수 있는 노드의 망 접속인증과 이동노드로의 인증모형을 기존의 AAA구조와 연계하여 해결하는 방안을 제시한다. 지역등록시 발생하는 통신지연 문제를 해결하기위한 강화된 AAA구조와의 연동기법을 설계하여 보다 더 부드럽고 안전한 핸드오프 과정을 제안한다

1. 서 론

네트워크 기술이 발전함에 따라 네트워크를 기반으로 하는 다양한 어플리케이션과 서비스들이 증가하고 있다. 그러나, 현재 네트워크의 기반구조는 증가하는 네트워크 서비스들을 발빠르게 수용하기에 한계를 가지고 있다. 이러한 문제를 해결하기 위해 제안된 개념이 액티브 네트워크이며, 현재 액티브 네트워크에 대한 다양한 연구가 진행 중이다[1,3].

Mobile IP 망에서는 방문 망에서의 지역등록이 일어날 때 마다 이동 노드 재인증 절차와 방문 망에서 홈 망까지의 트랜잭션으로 인한 통신 지연의 문제가 발생한다.

이러한 지연을 줄이기 위한 방안으로, 본 논문에서는 액티브 네트워크를 이용한 이동성관리와 홈망의 AAA서버를 관여 시키지 않고, 방문망의 AAA서버에게 전달되는 AEM(Authenticator Extension Message)를 이용하여 홈망의 AAA서버의 역할을 방문망의 AAA서버가 대행하여 인증문제의 해결 개선방안을 제안하고자 한다.

2장에서는 액티브 네트워크 개념과 EMM 알고리즘을 이용한 경로설정 과정을 알아보고 3장에서는 본 논문에서 제안하는 MN의 인증등록처리 절차와 처리 과정에 대해 기술 후 마지막 4장에서 결론을 내린다.

2. 관련 연구

2.1 Active Network

현재 네트워크의 기반구조는 고정된 프로토콜 스택이나 표준 제정의 시간 지연등으로 인하여 다양한 형태의 네트워크 서비스들을 신속하게 수용하기에 한계를 가지고 있다[1,2,3].

액티브 네트웍은 중간 노드에서 사용자 프로그램을 실행할 수 있도록 함으로써 기존 네트웍의 문제점을 보완한 네트웍을 말한다. 즉, 현재 중간 노드가 "축적-전송"의 기능을 한다면 액티브 네트웍 기반구조에서는 "축적-처리-전송"의 기능을 담당한다[1].

이러한 기능으로 인해 액티브 네트웍은 유연하고 동적인 네트웍 구조를 제공할 수 있다. 액티브 노드는 들어오는 패킷을 수신한 뒤 실행 여부를 결정하며, 실행 시에는 실행 환경으로 액티브 코드를 전달한다. 액티브 노드는 실행 결과에 따라 수신한 코드를 그대로 보내거나 또는 새로운 코드를 가진 패킷을 생성하여 다음 노드로 전달한다. 중간 노드의 실행은 노드 운영체계와 실행 환경을 구축함으로써 가능하게 된다.

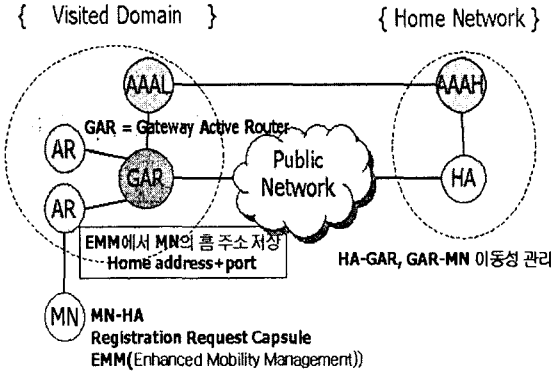

그림1. 액티브 네트워크에서의 Mobile IP

액티브 노드는 그림1과 같이 방문망에서의 효과적인 MN(mobile Node)의 이동성지원방법을 제안은 액티브 노드로 구성된 방문망의 최외곽에는 GAR(Gateway Active Router)라는 노드를 두어 이동성관리의 핵심요소로 사용한다. Mobile IP는 HA(Home Agent)-GAR, GAR-MN간의 두 단계를 구분하여 이동성관리를 하게 된다. 이 방법은Mobile IP서비스를 이용하는 MN은 대부분 지역망내서의 국지적인 위치이동을 자주하는 것을 전제로 한다.[4]

2.2 액티브 네트워크에서 EMM을 이용한 경로설정

액티브노드는 액티브 캡슐내에 있는 프로그램 코드를 실행할 수 있다. 본 논문에서는 액티브노드의 특성을 이용하여 터널링을 하지 않고 경로를 설정하는 방법을 제안한다. MN이 HA에게 전달하도록 요청하는 등록요청캡슐(Registration Request Capsule)은 Mobile IP의 등록메시지와 Enhanced Mobility Manageme(EMM) 알고리즘을 이용한 프로그램 코드로 구성된다.[4]

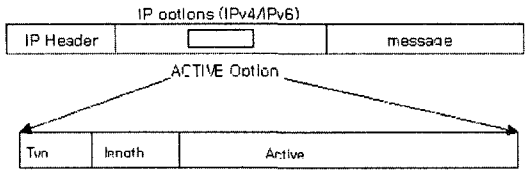

그림2. EMM 알고리즘(Registration Request Capsule)

각 액티브 노드의 패킷분석모듈(packet parser)은 캡슐을 분해하여 필요한 정보를 추출해낸다. 분리된 프로그램 코드는 액티브 노드의 실행환경(execution environment)의 code loader module로 보내지고, 프로그램을 실행시킨다. 그림 2에서와 같이 실행된 EMM프로그램은 등록요청캡슐에서 추출한 MN의 홈주소를 액티브 노드의 기억장소에 저장시킨다. 액티브 노드의 forwarder는 수신된 캡슐 전체를 다음 노드로 전송한다.[4]

액티브 노드가 등록응답메시지(registration reply message)를 받으면 자신의 라우팅 테이블에 MN의 홈주소와 출력포트를 매핑하여 저장한다. 이후에 목적지가 MN으로 수신되는 메시지는 'longest prefix matching rule'에 의해 라우팅 테이블의 MN의 주소를 참조하여 전달되게 된다. MN의 홈주소 엔트리를 관리할때는 타이머를 두어서, 일정시간동안 타이머갱신이 이루어지지 않으면 라우팅 테이블내의 엔트리를 삭제한다. MN으로의 설정경로는 일시적이므로 이 과정을 무시하면 MN의 이동성을 효율적으로 관리할 수 없게된다. 액티브 노드가 새로운 등록요청 캡슐을 수신하게 되면, 노드는 캡슐을 처리하는 대신에 다음노드로 그대로 전달한다. 이 때, 자신의 라우팅 테이블에 등록되어있는 MN의 등록요청 캡슐이 수신되면, 라우팅 테이블을 갱신하고, Mobile IP의 등록응답 메시지를 생성하여 MN에게 전송한다. 이 캡슐은 다음 노드로 전송되지 않는다. 이러한 방법으로 방문망 내에서의 MN까지의 경로를 설정하여 운영하게 된다. MN의 지역적인 이동시에 등록요청메시지를 HA까지 전달하지 않고 중간에 처리하게 되므로 MN의 핸드오프(handoff)시간이 빨라지고, 패킷손실을 극소화할 수 있게된다.[4]

3. AEM(Authentication Extension Message)를 이용한 인증 등록처리 절차

3.1 홈 등록

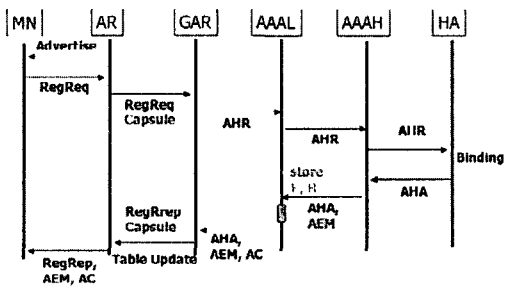

그림3. Home Registration

AgentAd : Agent Advertisement
RegReq : Registration Request
RegRep : Registration Reply
AHR : Home AAA Authentication Request
AHA : Home AAA Authentication Answer
AEM = Authenticator Extension Message
R = Authenticator Algorithm
E = Authenticator computes (R * AA)
AC = Authentication Challenge

MN은 AR(active rout)에게서 받은 Advertise를 통하여 자신의 이동을 감지하고 홈 네트워크로 등록을 시도한다. Advertisement 안에 포함된 C-COA를 사용하여 자신의 IP주소를 갱신하고, Advertisement에 포함된 GAR의 주소로 로 등록메시지를 보내게 된다. 이때 MN-HA(AAAH)간의 인증을 위해 authentication extension을 첨부하고, authenticator로 등록요청 메시지를 MN-AAAH간의 shared scret을 사용하여 암호화한 값을 설정한다.

GAR는 MN으로부터 등록 메시지를 받으면 임시 바인딩 리스트에 MN의 정보(home_address, COA, lifetime, identifier)를 저장한 후, AAAL에 메시지를 건네준다. 이 때, COA필드값을 자신의 주소로 대치하여, HA가 GAR를 MN의 access point로 등록되게끔 한다.

AAAL은 Local AAA서버로 작동하며, 등록메시지를 홈 네트워크로 전달해주는 역할을 한다.

AAAH는 Home AAA서버로 작동한다. AAAH는 등록메시지를 받으면 Authentication Extension내에 있는 authenticator를 복호화하여 MN을 인증하고, 인증이 확인되면 HA로 authentication extension이 제거된 등록요청 메시지를 전달한다.이 때, MN의 인증여부를 Extension을 통하여 전달한다.

HA는 AAAH로부터 등록요청 메시지를 받으면 Extension에 있는 인증여부에 따라서 바인딩 갱신을 한다. 바인딩 갱신이 완료되면 등록응답 메시지를 작성하여 AAAH에 돌려준다.

AAAH는 HA로부터 받은 등록응답 메시지의 Code가 등록성공일 경우, Session Key를 생성하여, MN-AAAH간 Shared Security와 AAAH-AAAL간 Shared Security를 사용하여 각각 암호화한 후, Authentication Extension인 형태로 메시지에 삽입한다. 완성된 메시지는 지역이동간에 MN와 AAAL간의 인증에 필요한 AEM에세지를 포함하여 AAA프로토콜을 통하여 AAAL에 전달하게 된다.

AAAL은 AAAH로부터 받은 등록응답 메시지에서 코드가 등록성공일 경우 AAAH-AAAL간의 Shared Security를 사용하여 암호화된 Session Key를 취득하고, MN의 지역내 이동에 따른 재인증 필요한 Authentication Extension 형태의 AEM(Authentication Extension Message)와 함께 replay proection에 대비해 AC (Authentication Challenge)값을 저장 후, Authentication Extension 하나를 제거하여 GAR로 전송한다. 등록실패 메시지일 경우 그대로 GAR로 전송한다.

GAR는 AAAL로부터 받은 등록응답메시지가 등록성공일 경우 자신의 임시 바인딩 리스트의 정보를 사용하여 바인딩 리스트를 갱신한다. 리스트 갱신 후 등록응답 메시지를 MN에게 전달한다.

MN은 등록응답 메시지에 첨부된 AEM에 있는 Authenticator를 이용하여 지역등록시 인증에 사용한다.

3.2 지역적 이동성관리

MN이 AR간 이동은 하였지만, 같은 GAR 하부망일 경우 등록은 HA대신 GAR에 등록을 하여 지역적인 바인딩 갱신이 이루어진다. 이때, MN-AAAL Authentication Extension 간의 재인증을 통해 MN-GAR의 경로 설정을 한다.

MN은 AR에게서 받은 Advertise를 통하여 자신의 이동을 감지하고 홈 네트워크로 등록을 시도한다. Advertisement 안에 포함된 C-COA를 사용하여 자신의 IP주소를 갱신하고, Advertisement에 포함된 GAR의 주소로 로 등록메시지를 보내게 된다. 이 때,

Advertisement내의 GAR주소가 변하지 않았으면 지역등록을 실행한다. MN-GAR(AAAL) 간의 인증을 위해 AEM authentication extension을 첨부하고, AAAL로부터 받은 AC로 authenticator를 해쉬하여 등록요청 메시지와 함께 보내진다.

AR는 MN으로부터 등록 메시지를 받으면 임시 바인딩 리스트에 MN의 정보(home_address, COA, lifetime, identifier)를 저장한 후, AAAL에 메시지를 그대로 건네준다.

AAAL은 등록메시지의 AEM authenticator를 자신이 가진 AEM메시지의 E값을 비교 후 인증 결과를 AR에게 통보한다.

AR는 AAAL로부터 받은 인증여부를 바탕으로 바인딩 갱신을 한 후, 등록응답 메시지를 만들어서 MN에 전달한다.

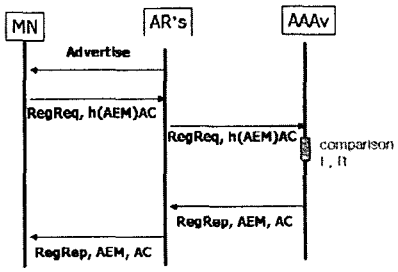

그림4. Regional Registration

1) AR→MN : AgentAd
2) MN(AEM)→AR : Rreq Msg, h(authenticator)AC
3) AR(AEM)→AAA : Rreq Msg, h(authenticator)AC
4) AAA(AEM, AC)→AR : Rrep Msg, AC
5) AR(AEM, AC)→MN : Rrep Msg, AC

3.3 제안된 인증절차 방안

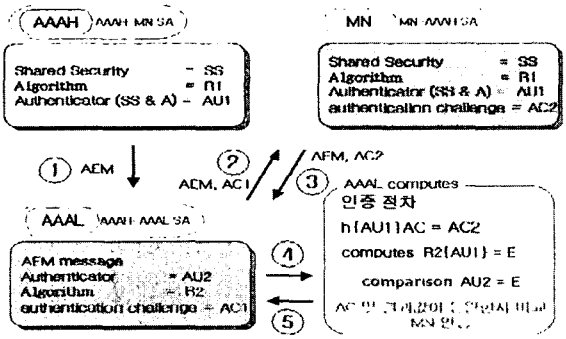

그림5. AAAL의 AEM 인증절차

AR은 세션키가 없으므로 키 획득을 위해 홈 망의 AAAH를 거쳐 정상적인 Mobile IP 등록 절차를 수행해야 한다. 이경우 EMM의 EMM모듈을 실행시킬 수 있고, 이 모듈은 액티브노드를 일시적인 Mobile Agent로 작동하게 하여 보다 빠른 핸드오프를 실행할 수 있도록 해 준다.

그림 5에서 처럼 MN의 홈등록시 AAAH는 AAAL에게 MN을 인증하기 위한 Authenticator(AU2)와 Algorithm(R3)를 포함한 AEM메세지를 보내게 된다.

AAAL은 MN의 지역등록시 재인증을 확인하기 위해 AEM메세지에는 AC1(인증 챌린지)를 포함하여 보내어지게 되며, MN은 전달받은 AEM의 AC1를 이용하여 지역등록시 AU1과 AC1로 AU1을 해쉬한 값인 AC2를 AEM에제지에 포함하여 보내게 된다.

AAAL은 MN의 AEM을 검증하기 위해 AU1을 AC1으로 해쉬해서 얻은 값과 AC2를 비교하여 MN의 AEM 메시지를 검증하고 인증계산을 위해 AU1을 R2방식으로 계산되어진 E값과 AAAH로 부터의 AU2값을 통해하여 MN을 인증받게된다.

AAAL는 새로운 AC를 MN의 지역 등록 응답 메시지와 함께 보내어지게되고 재인증 절차를 마치게 된다.

그러므로 그림6과 같이 MN은 지역 등록을 수행하며 AR은 AAAH까지 재 등록 절차가 생략되므로 지연을 최소화 할 수 있게된다.

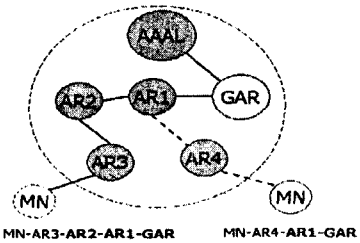

그림6.MN의 새로운 경로 수립

4.결론

홈등록시 AAAH-AAAL에게 AEM인증 확장 메시지를 전달받는다. AAAL는 AAAH에로 부터 AEM메시지에 MN의 인증에 필요한 Authenticator와 Algorithm을 저장 후 AC를 포함하여 MN에게 전달된다.

MN은 지역등록시 AEM메세지에 AU값을 AC값으로 해쉬한 값을 첨부하여 보내어지게 되고, MN의 지역등록 요청 메시지를 받은 AR은 순간 Mobility Agent로 작동하여 지역등록시 발생하게 되고 AAAL는 AAAH의 역할을 수행하여 MN의 등록메세지와 AEM를 저장되어진 AC로 Authenticator의 해쉬값과 비교 replay protected를 방지하기 위한 AEM 메시지 인증절차를 가진다.

따라서, 액티브노드를 이용하게되는 이점을 유지하면서, 안전한 노드의 이동성확보를 제공할 수 있다..

본 논문에서는 액티브노드를 일시적인 Mobile Agent로 작동하게 하여 EMM모듈 실행환경의 능동네트워크 망에서 빠른 핸드오프와 MN의 안정적 인증절차를 간소화 하는 방안을 제시하였다

참고문헌

[1] D. L. Tennenhouse, et al., "A Survey of Active Network Research," IEEE communications magazine, Jan. 1997.

[2] D. L. Tennenhouse, et al., "Towards an active network architecture," In Multimedia Computing and Networking '96, Jan. 1996.

[3] D. Raz, et al., "An Active Network Approach to Efficient Network Management," IWAN '99, 1999.

[4] Insu Kim., "Secure Mobility Management for Active Access Networks" EALPIIT 2003.

[5] K. Psounis, "Active Networks: Applications, Security, Safety, and Architectures", IEEE Communications Surveys, First Quarter, 1999.

[6] Young-Ju Han, Jin-Seok Yang, Hee-Seung Kim, Hyoun-Ku Kim, Beom-Hwan Chang, Tai-Myoung Chung, "A Study on the Distrubuted Vulneability Analysis Model based on Active Networks", Proc. of the 20th KIPS Fall Conference, Korea, Nov. 2003. (in Korean).