Diameter Base Protocol 의 향상된 경로 권한검증 기법

유희종*, 김현곤*
*한국전자통신연구원 AAA 정보보호연구팀
e-mail : anny5@etri.re.kr

Improved Path Authorization of Diameter Base Protocol

Hui-Jong Yu*, Hyun-Gon Kim*
AAA System team, ETRI

요 약

Diameter Base 프로토콜은 Diameter 노드라면 반드시 지원해야 하는 기본 프로토콜이다. 현재 Diameter Base 프로토콜은 IETF RFC 3588 로 표준화되었으나 여전히 논의되어야 할 문제점이 존재하며 IETF WG Mailing List 에서 이에 관한 논의가 진행되고 있다. 경로 권한 검증 문제는 이미 IETF WG Mailing List 에서 일부 언급되었으나 충분한 논의가 이루어지지 못한 상태이다. 따라서 RFC 3588 내에서 정의한 내용들에 서로 모순되고 비효율적인 기능들이 존재한다. 본 논문에서는 RFC 에 새롭게 추가된 기능인 경로 권한 검증 기능의 문제점에 대해 분석하여 표준에 벗어나지 않으며 보다 효율적으로 개선된 방안을 제시한다.

1. 서론

랩탑, 노트북, 이동전화와 같은 장비들이 사무실 밖에서 이동 중에도 사용할 수 있도록 소형화 되었다. 그러나 크기와 이동성 뿐 아니라 안전성도 제공되어야 한다. 또한 사용자의 수가 급격히 늘어나면서 발생하는 문제점들을 해결해야 한다. 불법적으로 서비스를 사용하는 것을 방지해야 하고, 가입자의 권한 레벨을 부여하고 검증해야 하며, 과금 및 자원 계획을 수립하기 위해 네트웍 사용에 대한 측정이 필요하다.

AAA(Authentication, Authorization, Accounting) 프로토콜은 다중 네트워크와 플랫폼 상에서 인증(Authentication), 권한검증(Authorization), 과금(Accounting) 등의 기능들을 조정하는 프레임웍으로서 위의 여러 문제점들을 해결할 수 있는 방법이다. AAA 프로토콜의 기능은 다음과 같다.

○· 인증(Authentication)
망 접근을 허용하기 전 사용자의 신원을 검증하는 것이다. AAA 서버는 사용자가 제공한 인증 데이터와 자신의 데이베이스 안의 사용자 관련 데이터를 비교하여 인증서가 일치하면 망에 대한 접근을 허락한다. 만일 일치하지 않으면 인증실패로 인해 망 자원 사용을 허용하지 않는다.

○· 권한검증(Authorization)
망 사용이 허락된 사용자에 대해 어떤 권한과 서비스를 허용할 것인지를 정하는 것이다. 여기에는 IP 주소, 제공될 응용 및 프로토콜을 결정하기 위한 필터 등이 포함된다. 인증과 권한검증은 AAA 동작 환경에서 일반적으로 함께 수행된다.

○· 과금(Accounting)
사용자의 자원 사용에 관한 정보를 모으는 방법을 제공한다. 그리고 이 정보는 사용요금, 회계 그리고 용량 증설에 사용된다.

일반적으로 PPP(Point-to-Point Protocol)나 터미널 서버 액세스와 같은 서비스를 위한 AAA 프로토콜로 RADIUS(Remote Authentication Dial-In User Service)

프로토콜이 사용되어 왔다. 그러나, 급격하게 증가하는 네트웍 환경 하에서 RADIUS 는 Scalability 와 Security, 프로토콜의 기술적인 한계 등에서 AAA 서비스를 위한 프로토콜로 부적합한 것으로 밝혀지고 있다.

Diameter 는 이러한 환경에서 RADIUS 를 대체할 수 있는 AAA 서비스 프로토콜로서 RADIUS 가 가지는 많은 단점을 개선하여 이동인터넷 환경에서 AAA 서비스에 적합한 프로토콜로 현재 규격 정의 작업이 일부 완료되었으며 다른 일부는 진행 중이다.

이러한 Diameter 프로토콜은 다음과 같이 기본 프로토콜 이외에 여러 Application 들을 통하여 다양한 서비스를 제공할 수 있다.

○Diameter Base Protocol[1]
○Diameter Credit Control Application[2]
○Diameter NASREQ(Network Access Server REQiurement) Application[3]
○Diameter Mobile IP Application[4]
○Diameter EAP Application[5]

Diameter Base 프로토콜은 기본적으로 하부 전송 계층과 연동하여, 각 Diameter 노드간의 전송 계층 연결을 설정, 해지 및 관리하여 상위 응용 계층 블록들이 안전하게 메시지를 송수신할 수 있는 환경을 제공한다. 또한 이를 통해서 수신한 Diameter 메시지를 처리하기도 하며, 필요시 상위 응용 블록으로 전달하기도 한다. 그리고 상위 응용 블록에서 생성한 Diameter 메시지를 하부로 전송하는 기능도 제공한다. 본 논문에서는 이러한 기본 프로토콜 기능의 하나인 경로 권한검증 기능에 대하여 논의한다.

2. 경로 권한검증 기능

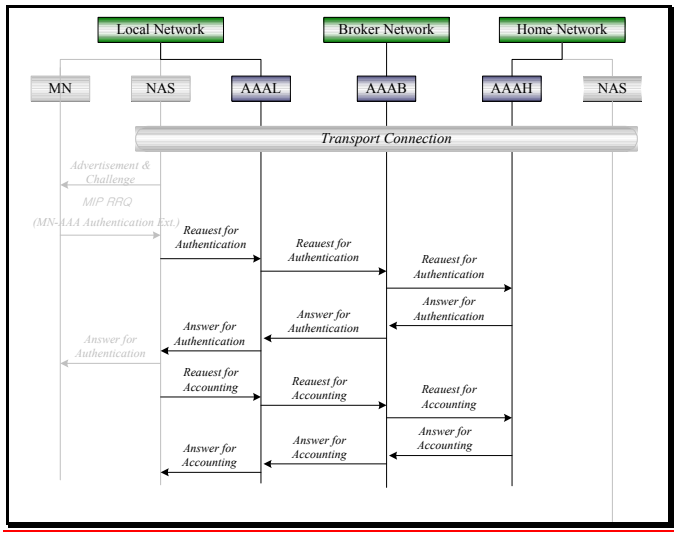

그림 1 Diameter 사용자 인증, 권한검증 및 과금 과정

그림 1 은 외부망으로 이동한 사용자(MN : Mobile Node)에 대한 인증 및 과금 과정을 나타낸다. MN 은 Diameter Mobile IP 응용 혹은 Diameter EAP 등의 응용 모두에 적용될 수 있으며 본 논문에서는 이러한 과정을 기본 환경으로 설정한다.

MN 은 외부망에서 홈 망의 AAA 서버(AAAH)에게 인증받기 위해 로컬의 NAS(Network Access Server)에게 접근하며 Diameter 클라이언트 기능을 제공하는 NAS 는 로컬의 AAA 서버(AAAL)에게 인증 요청 메시지를 전송한다. 이 인증 요청 메시지는 브로커 망을 통해 AAAH 에게 전송되며 성공적인 인증 응답 메시지를 수신한 NAS 는 해당 과금 세션을 열고 과금 메시지를 AAAH 와 주고받아 과금을 수행한다.

경로 권한검증 기능은 이러한 Diameter 노드들 사이에 전송되는 메시지 모두에 적용 가능하다. 경로 권한검증 과정은 AAAL 과 AAAH 에서 수행되며 다음과 같이 진행된다.

• AAAH 에서 진행될 경우

인증 요청 메시지를 수신한 AAAH 는 Route-Record AVP 를 검사한다. Route-Record AVP 에는 해당 메시지가 거쳐온 경로 노드에 대한 정보가 포함되어 있다. AAAH 에서 acceptable 하지 않은 경로가 포함되어 있다면 AAAH 는 인증 실패 처리 후 인증 응답 메시지를 DIAMETER_AUTHORIZATION_REJECTED 로 설정하여 전송한다.

• AAAL 에서 진행될 경우

이 경우는 AAAH 에서는 인증이 성공하여 인증 응답 메시지를 전송하였으나 이를 수신한 AAAL 이 인증 응답 메시지의 Route-Record AVP 를 검사하여 메시지의 송수신 경로가 acceptable 하지 않다고 판단하게 되는 경우이다. 인증 응답 메시지가 성공적으로 수신되었을 경우 보통 AAAL 에서는 이를 NAS 에게 알리고 과금 요청 메시지를 수신하여 AAAH 에게 전송하게 되어 있다. 따라서 표준 문서에 따르면 경로 권한검증의 실패 결과는 과금 요청 메시지에 포함되어 전송된다. 즉, 과금 요청 메시지의 Result-Code AVP 에 DIAMETER_UNABLE_TO_COMPLY 에러 코드가 삽입되어 AAAH 에게 경로 권한 검증 실패의 결과를 알린다.

3. 경로 권한검증의 문제점 및 개선 방안

3.1 경로 권한 검증의 문제점

• AAAH 에서 진행될 경우

경로 권한 검증이 수행되어 사용자의 인증이 실패하였으나 다시 시도할 경우 AAAL 에서는 정확한 원인을 알 수 없어 동일한 경로로 메시지를 전송할 수 있다. 즉, 이는 경로 권한검증의 실패 결과 값이 다른 인증 실패의 경우와 같기 때문에 발생한다.

• AAAL 에서 진행될 경우

이 경우는 더욱 복잡하며 Diameter 프로토콜에 모순을 가져온다. 첫째, 과금 요청 메시지에 Result-Code AVP 가 포함된다. 이는 요청 메시지에는 Result-Code AVP 가 포함되지 않는다는 Diameter 프로토콜을 따르

지 않는 것이다. 현재 RFC 3588 에는 모든 요청 메시지에는 Result-Code AVP 가 포함되지 않는 것으로 정의되어 있다. 둘째, AAAH 에서는 인증이 성공한 것으로 알고 있으나 AAAL 에서 실패함으로써 무의미한 과금 요청 메시지가 전송된다는 것이다. 인증이 실패하였는데 과금 메시지가 생성되는 것 또한 표준과 상이한 결과를 발생시킨다. 셋째, AAAL 에서 경로 권한검증이 실패한 경우 NAS 에게 이를 알릴 방법이 정의되어 있지 않다. 과금 요청 메시지의 생성은 NAS 에서 수행하므로 성공한 인증 응답 메시지를 수신한 AAAL 은 이를 변경한 후 NAS 에게 전송해야 한다. 그러나 표준의 어떤 부분에도 이에 관한 언급도 존재하지 않는다. 넷째, AAAL 에서의 경로 권한검증 기능을 수행하기 위해서는 모든 Diameter 응답 메시지에 Route-Record AVP 가 포함되어야 한다. 그러나 현재의 Diameter 문서들에는 이에 관한 내용을 찾을 수 없다.

다음 절에서는 이러한 문제점들을 해결할 수 있는 개선된 방법을 제안한다.

3.2 개선된 경로 권한검증

• AAAH 에서 진행될 경우

AAAH 에서 경로 권한검증 문제점을 해결하기 위하여 새로운 Result-Code AVP 의 값을 정의한다. 경로 권한 검증 실패 문제는 현 시점에서는 해결이 불가능하나 추후 다른 경로를 통한다면 해결 가능하므로 Transient Failures 로 분류할 수 있으며 따라서 4000 번대의 에러 코드로 정의할 수 있다[1]. 또한 현재 4000 번대의 에러 코드는 4003 번까지 정의되어 있으므로 다음과 같이 정의할 수 있다.

PATH_AUTHORIZATION_FAILURE 4004

AAAH 는 수신한 인증 요청 메시지의 Route-Record AVP 를 검사하여 acceptable 하지 않은 경로라고 판단되면 에러코드 4004 를 포함한 인증 응답 메시지를 생성하여 AAAL 에게 전송한다. 이러한 에러 코드를 수신한 AAAL 은 NAS 에게 별도로 알리지 않고 다른 경로를 통하여 인증 요청 메시지를 송신한다.

• AAAL 에서 진행될 경우

AAAL 에서의 경로 권한검증 문제점을 해결하기 위해서는 다음과 같은 사항이 고려되어야 한다.

° 요청 메시지에 Result-Code AVP 가 추가되지 않는 것이 바람직하다.

° 무의미한 과금 요청 메시지는 생성 및 전송되지 않는 것이 바람직하다.

° NAS 는 경로 권한 검증의 결과에 상관없이 동작하는 것이 바람직하다.

° 모든 Diameter 응답 메시지에 Route-Record AVP 가 포함되어야 한다.

최근 IETF AAA WG 에서는 4 번째 문제에 대한 논의가 이루어 졌다. Mailing List 논의 결과를 통하여 AAAL 의 경로 권한검증 수행을 가능하도록 하기 위해서 모든 응답 메시지에 Route-Record AVP 를 포함시키는 것으로 결정되었다.

본 논문에서는 위와 같은 사항들을 고려하여 개선된 방법을 제안한다.

다음과 같은 AVP 를 정의한다. GROUP 타입으로 AAAL 에서 acceptable 하지 않은 DiameterIdentity 타입의 HOST 혹은 REALM 들을 포함한다.

Unvalid_Path AVP (AVP Code – Application 별 정의)

이 AVP 코드는 Diameter 가 구현되는 시스템에서 별도로 정의한다.

AAAL 은 인증 요청 메시지에 Unvalid_Path AVP 를 포함시켜 전송한다. Diameter 메시지를 전송하는 과정의 중간 노드들은 보통 Route-Record AVP 를 검사하여 라우팅 경로를 결정한다. 인증 요청 메시지가 전송되는 경로의 Diameter 노드들은(브로커 등) Route-Record AVP 뿐 아니라 Unvalid_Path AVP 또한 검색하여 해당 HOST 혹은 REALM 을 거치지 않도록 라우팅한다. 응답 메시지는 요청 메시지가 전송된 경로를 거꾸로 따라서 전송되므로 AAAH 로부터 수신된 인증 응답 메시지는 AAAL 에서 충분이 acceptable 한 경로이다. 따라서 경로 권한검증 기능에 따른 과금 요청 메시지는 생성되지 않는다.

제안하는 방법은 과금 요청 메시지가 경로 권한검증 기능에 의해 생성되지 않으므로 요청 메시지에 Result-Code AVP 가 포함되지 않으며 송수신되는 메시지 수를 감소시켜 보다 효율적으로 동작하도록 한다. 또한 NAS 는 경로 권한검증에 대해 독립적으로 동작할 수 있다.

그림 2 에 개선된 경로 권한검증 기능 수행 과정을 나타내었다.

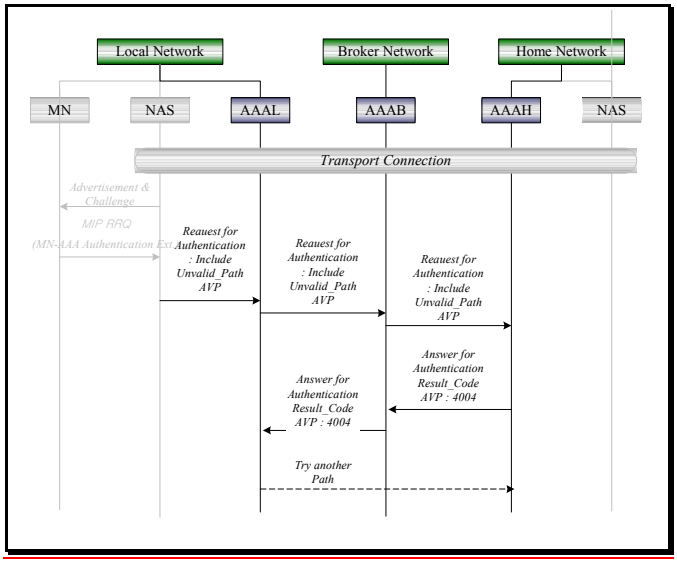

그림 2 제안하는 경로 권한검증

또한 이 AVP 를 AAAH 에서 생성되는 인증 응답 메시지에 포함시킬 수도 있다. 이는 AAAH 에서 경로 권한검증시 유효하지 않은 경로를 통해 전송된 인증 요청 메시지인 경우 AAAH 가 인증 응답 메시지에 AAAH 에서 acceptable 하지 않은 경로 정보를 알리는 방법으로 사용될 수 있다. 이 메시지를 수신한 AAAL 은 추후의 인증 요청 메시지 전달 경로를 결정하는데 참고할 수 있으며 따라서 불필요한 메시지들의 송수신을 감소시킴으로써 보다 효율적인 프로토콜의 설계가 가능하다.

4. 결론

Diameter 프로토콜은 다양한 응용에서 사용자의 인증, 권한 검증, 과금등의 서비스를 지원할 수 있다. Diameter Base 프로토콜은 이러한 서비스를 가능하도록 하기 위하여 기본적으로 하부 전송 계층과 연동하며, 각 Diameter 노드간의 전송 계층 연결을 설정, 해지 및 관리하여 상위 응용 계층 블록들이 안전하게 메시지를 송수신할 수 있는 환경을 제공한다. 2003 년 9 월 Diameter Base 프로토콜이 RFC 로 정해졌으나 아직 논의가 필요한 부분이 남아있다. 경로 권한검증 기능도 그러한 부분으로 다소 논의가 되기는 하였으나 이전의 기능과 충돌하거나 프로토콜의 불필요한 추가 기능이 요구되는 문제점이 존재한다. 본 논문에서는 이 문제점들을 분석하고 개선된 방안을 제시한다. 실제 Diameter Base 프로토콜의 구현에 있어서도 개선된 방안이 유용하게 사용되리라 사료된다.

참고문헌

[1] Diameter Base Protocol, RFC 3588, September 2003
[2] Diameter Credit-Control Application, draft-ietf-aaa-diameter-cc-03.txt, February 2004
[3] Diameter Network Access Server Application, draft-ietf-aaa-diameter-nasreq-14.txt, February 2004
[4] Diameter Mobile IPv6 Application, draft-le-aaa-diameter-mobileipv6-03.txt, April 2003
[5] Diameter Extensible Authentication Protocol Application, draft-ietf-aaa-eap-02.txt, June 2003