Diameter 프로토콜에서의 Credit-Control

박건영*, 김기천*
*건국대학교 컴퓨터공학과

e-mail : gunzero@kkucc.konkuk.ac.kr

Credit-Control scheme of AAA protocol

Gunyoung Park*, Keecheon Kim*
*Dept. of Computer Science& Engineering Konkuk University

요 약

유무선의 다양한 환경에서 신뢰할 수 있는 Accounting 을 할 수 있도록 AAA 프로토콜중에 하나인 DIAMETER 의 기능과 특성에 대해서 알아보고 기존의 Accounting 의 문제점을 보완한 Credit-Control 모델에 대해 알아 보도록 한다.

1. 서론

네트워크 환경이 유선에서 무선으로 변화해 가면서 네트워크 환경이 점점 다양화되어 가고 있다. 그에 따라 기존에는 사용할 수 없었던 서비스에 대한 요구가 점차 높아져 가고 있는 상황이다. 이러한 사용자들의 요구를 충족 시키기 위해서는 여러 가지 문제점을 해결해야 하는데, 기존의 환경보다 사용자의 수가 증가함으로써 사용자 요구에 대한 서비스를 효율적으로 관리해야 할 필요성이 증가 하였고, 무선 환경을 지원하게 됨으로써 다양한 Access 기술에 따른 고려를 해야 한다. 또한 유선에 비해서 무선의 보안이 아직 부족하기 때문에 보안에 대한 문제점과 과금에 대해서 해결해 주지않고서는 서비스 사용자와 제공자간의 신뢰할 수 있는 서비스 환경이 이루어 지지 않기 때문에 서비스 제공시에 사용자와 서비스 제공자간의 인증과 서비스에 대한 과금과 같은 사항을 처리할 AAA 기술에 대한 필요성이 점차 증가 하고 있다.

AAA 프로토콜은 Authentication, Authorization, Authority 를 지원 하는 것으로서 네트웍을 이용하는 사용자와 서비스 제공자에게 서로 믿을 수 있는 보안 서비스를 제공하고 사용자의 권한 레벨에 따른 차별화된 서비스를 제공할 수 있게 해준다. 서비스 제공자의 입장에서는 사용자의 이동이나 네트워크에 문제가 발생했을 지라도 제공된 서비스에 대한 정확한 과금 처리를 할 수 있도록 고안된 프로토콜이다. 기존에 나와 있는 AAA 프로토콜로는 RADIUS 가 있는데 RADIUS 의 경우에는 유선환경을 바탕으로 만들어진 것으로 NAS(Network Access Server) 와 Authentication 서버 사이에서 AAA 정보를 전달하기 위하여 사용되는 프로토콜이다. 그러나 기존 유선 LAN 에서 사용되어 지던 AAA 프레임워크인 RADIUS 나 TACACS+는 소수의 사용자를 위해 설계되어져 확장성이 떨어지고 이동성의 지원과 End-to-End 보안이 되지 않는 문제점들이 있다. 따라서 이러한 문제점들을 해결해줄 필요성이 생기게 되었다 Diameter 는 이러한 요구에 가장 적합하도록 설계된 프레임워크로써 PPP, 로밍, Mobile IP 와 같은 기존 기술과 새롭게 요구되는 기술에 대한 AAA 서비스를 제공하기 위한 가볍고 확장성 있는 peer 기반의 AAA 프로토콜이다. 이 글에서는 이러한 기존 AAA 프로토콜의 대안으로 생긴 Diameter 에 대해 알아보고 Accounting 기법중의 하나인 Credit-Control 에 대해 알아봄으로써 Accounting 기법의 발전 방향에 대해 알아보도록 한다.

2. Diameter

Diameter 프로토콜은 그 자체로는 AAA 서비스를 제공하지 않고 그림 1 과 같이 특정한 프레임워크에 확장된 형태로 사용된다. PPP dial-in 등의 access protocol 과 확장을 위한 protocol extension 으로 구성 되어 Accounting, End-to-End security 그리고 Mobile IP[1]를

지원한다. Roaming 및 Mobile IP 등은 모두 데이터망에서 이동을 전제로 다양한 Access 망에 접속하여 일관된 서비스를 제공받는 것을 요구하므로 AAA 프레임워크를 필요로 한다.

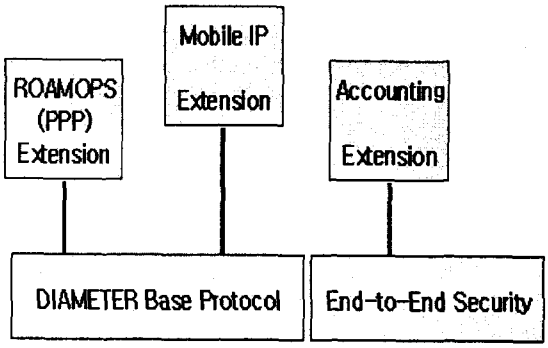

그림 1 Diameter Protocol

2.1 Diameter Protocol 특징

Diameter base protocol 은 Attribute/Value Pair(AVP)를 전달하고 에러가 생겼을 경우에 통지해주는 기능과 Diameter extension application 에서 필요한 기본적인 기능들을 처리해 준다.

Diameter 는 AVP 와 Proxy 를 지원하는 면에서는 기존 AAA 프로토콜과 유사하나 AVP 의 사용 범위에 있어서 차이를 보인다. RADIUS 의 경우 Attribute Value 가 255 바이트를 넘지 못하고 AVP 주소 공간이 확인 메시지를 받기 전에 255 쌍만을 유지할 수 있지만 Diameter 는 32bits 의 AVP 주소 공간을 가지고 있어 수백만 쌍 이상을 지원 가능하기 때문에 RADIUS 에 비해 많은 유무선 사용자들을 지원해줄 수 있고, Diameter Server 가 NAS 의 메시지 처리량에 따라 메시지를 조절하여 송신하기 때문에 장애에 대한 대비를 할 수 있다. 또한 RADIUS 서버는 클라이언트가 요구하지 않으면 메시지를 보낼 수 없지만 Diameter 는 NAS 에서 Diameter 서버가 과금이나 연결 종료를 알려주어야 할 경우 메시지를 보낼 수도 있다. Diameter 는 재전송과 장애 복구 기능을 개선하여 RADIUS 보다도 망 회복력 기술에 대한 AAA 서비스를 제공한다. 그리고 Diameter 는 RADIUS 가 지원하지 않는 종단간 보안(End-to-End Security)기법을 제공함으로써 신뢰할 수 있는 통신 환경을 만들어 준다.[3]

2.2 Diameter Protocol 응용 기술

Diameter Protocol 응용의 예를 보면 Diameter CMS(Cryptographic Message Syntax)[2] 보안 Application 의 경우에는 기존의 AAA 기술은 메시지 전송을 부인하는 부인 봉쇄와 메시지 전송시에 거치는 중간 노드들에 의해 생길 수 있는 메시지 변조의 가능성으로 인해 무결성에 대한 문제점등 보안에 취약점을 가지고 있었다. 이러한 문제로 Diameter 노드간의 인증이 필요하게 되어 공개키 암호방식(PKI)을 사용하여 메시지의 암호/복호화 및 서명/검증 기능을 통하여 End-to-End 간 Diameter 메시지의 인증, 무결성, 기밀성, 부인봉쇄 등의 강한 인증과 암호화 기능을 제공하는 Diameter CMS 가 나오게 되었다. 두개의 Diameter peer 간의 security association 은 X.509 인증서를 이용하여 Diameter AVP 안에 data 를 CMS 로 encapsulation 하여 동기, 비동기 혼합방식의 변환을 통하여 이루어 진다.

3. Accounting

Diameter Accounting 프로토콜은 서비스 제공자가 제공한 서비스에 대해 사용자에게 신뢰성 있고 안전하게 과금을 할 수 있도록 해주고, 사용자들의 네트워크 자원 사용량을 측정하여 네트워크의 확장을 하는데 설계자료 등으로 활용하기위해 사용 한다.[4] 그러나 기존의 Diameter base accounting protocol 은 실시간으로 다양한 사용자 디바이스와 환경에 따라서 생길 수 있는 Accounting 정보의 손실을 최소화 할 수 있도록 하는 방안이 고려 되어야 하는데 부족한 부분들이 있었다. IETF 의 "draft-ietf-aaa-diameter-cc-00" [5]에서는 이 부분에 대해 보완할 수 있는 방안들이 나오고 있다. 이 드래프트에서는 다양한 서비스 환경에서의 Accounting 에 대해 언급하고 있다. 예를 들면 SIP service, Messaging service, 무선환경에서의 과금등 사용자의 서비스가 다양화되어감에 따라 실시간 비용과 Credit-Control 을 Diameter 에서 지원하는 방안을 설명하고 있다.

3.1 Credit-Control

차세대 무선 네트워크 환경에서는 Diameter 의 기본적인 Accounting protocol 보다 무선 환경을 고려한 향상된 Accounting 기술을 요구하는데 예를 들면 3GPP 환경에서는 실시간으로 사용에 따른 요금 부과와 billing 이 이루어져야 한다. 이렇게 하려면 사용자가 요청한 서비스에 대해서 서비스를 제공하기 전에 사용자에 대해서 Accounting 을 할 수 있는 영역에 있는지 확인하고 서비스를 제공해야 하고 사용자 입장에서는 중간에 네트워크가 끊기는 등의 네트워크의 문제로 인해 서비스를 제공받지 못했거나 광고 같은 패킷의 경우에는 그에 대한 요금 부과를 받지 않도록 하여야 한다. 이와 같이 하기위해서 기존의 Diameter 프레임워크에 새로운 Credit-Control 서버를 추가 하는 방안이 나왔다. Diameter Credit-Control Server 는 선불 가입자들을 인증하는 역할을 하고, 네트워크 자원에 대한 사용자 Authenticate 와 Authorize 는 Diameter base protocol 을 사용하여 하게 된다

3.2 Credit-Control Model

기존의 Accounting 과정은 서비스가 초기화된 후에 Diameter Base Accounting protocol 을 이용하여 Accounting 정보를 받고, 서비스가 완료될 때 까지 중간 합산한 결과를 받아서 처리하게 되는데 실시간 Credit-Control 을 하기에는 이 방법으로는 부족한 점이 있다.

실시간 Credit-Control 에서는 정당한 사용자인지 검증하고, Account balance 가 서비스 수행비용을 충분히

커버할 수 있는지 확인하기 위해서 Credit-Control Client 와 Credit-Control Server 의 연결이 서비스가 사용자에게 제공되기 전에 이루어진다. NAS, MobileIP 환경을 생각해 보면 프로토콜의 효율성을 위해서 Authorization, Authentication 을 먼저 호출하여 실행하고, 추가적인 credit authorization 은 Credit-Control command 를 이용하여 하게 된다. Credit-Control Client 는 이 방법들을 NAS, MobileIP 환경에서 지원해야 하고 이 경우에 Credit-Control Server 와 AAA Server 는 물리적으로 분리되어 실행 된다. Credit-Control Server 와 AAA Server 간의 동작하는 과정은 서비스에 대한 request message 를 AAA Server 가 수신하면 다시 Credit-Control Server 에게 전달해주는 방식으로 동작한다. 또 다른 서비스 환경으로 3GPP Network 이나 SIP 환경을 보면 네트워크의 특성상 access 와 registration 서비스 요청 간의 연결과 해제가 자유로워야 한다는 특성을 반영해야 한다. 여기서 Credit-Control Server 와 Credit-Control Client 의 역할을 보면 Credit-Control Server 는 사용자가 요청한 서비스에 대한 정보를 파라미터로 받아서 비용을 산출, 평가하고, Credit-Control Client 의 경우에는 Credit-Control Server 로부터 지시를 받아 제공되는 서비스에 대한 모니터링을 하게 된다. 이러한 Credit-Control Server 와 Credit-Control Client 모델은 2 가지가 있다

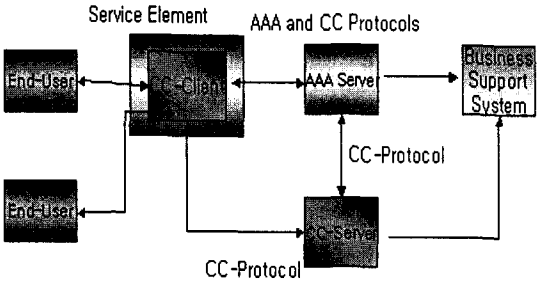

그림 2 Credit-Control Model1

그림 2 는 일반적인 Credit-Control 구조로서 Credit-Control protocol 은 Diameter base protocol 과 Diameter Credit-Control application 간에 사용되어 진다.

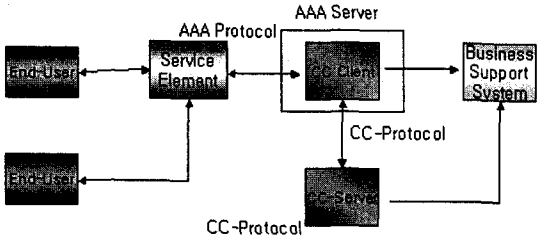

그림 3 Credit-Control Model2

그림 3 은 Service Element 에서 Credit-Control 프로토콜을 지원하지 않는 구조 이다.

3.3 Credit-Control 과정

Credit-Control 의 과정의 예를 살펴보면 다음과 같다. 사용자가 SIP 서비스를 요청 하면 Service Element(ex. Sip proxy)는 그 요청을 사용자 Home domain 의 서버에게 요청을 하게 된다. Visited domain 에 있을 경우에는 Home domain 과 사전에 계약이 있어야 한다. Credit-Control 하는 동안 session 이 생성되는데 각 Credit-Control session 은 고유한 session id 를 가지고 실행되며 Credit-Control session 의 lifetime 동안에는 변경이 될 수 없다. Session based Credit-Control 은 두 가지 방법이 있는데 하나는 Authorization, Authentication 후에 사용 하는 것이고, 다른 하나는 Authorization , Authentication 중간에 실행 하는 것이다. 두 가지 방법 중에 첫번째 방법에 대해서 알아보면 그림 4 와 같다. Diameter CC Client 는 Service Element 에 존재하고, 필요한 정보는 Authorization Server 에게서 얻게 된다. Credit-Control 은 CC Server 가 서비스를 제공하기 전에 사용하고 Accounting protocol 과 parallel 하게 사용된다. Credit Control 초기화 과정이 끝나면 Diameter Server 에 의한 Accounting 이 시작 되고, 서비스를 사용 중에 Authorization life time 이 만료 되었을 경우에는 re-authorization 메시지를 보내 갱신하게 된다. 사용자가 서비스를 종료 하기를 원하면 CC Client 와 Server 간의 Credit-Control 종료 과정을 거치고 Service Element 와 Diameter 서버간의 Accounting 종료 과정을 거쳐 서비스를 끝마치고 과금을 하게 된다.

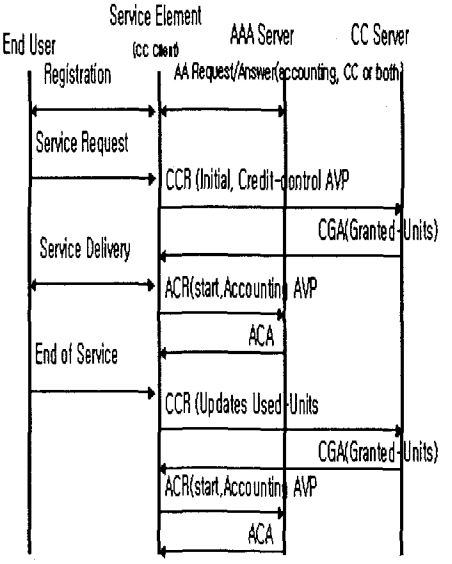

그림 4 Accounting & Credit-Control

4. 결론.

AAA 프로토콜은 차세대 네트워크 환경에서 그 중요성이 증가되고 있는 프로토콜이다. Diameter 의 경우 앞으로 AAA 프로토콜의 주된 기술이 될 것으로 보여지는 기술로서 기존의 AAA 프로토콜인 RADIUS 에 비해 확장성, 보안, 로밍 등의 부분에서 많은 보완을 하였다. 그러나 Accounting 의 경우 다양한 네트워크 환경에서의 실시간 Accounting 에 대한 부분에서는 부족한 점들이 있었다. 이 글에서는 이러한 문제점에 대한 방안으로 Diameter Credit-Control Application 을 살펴봄으로써 사용자와 서비스 제공자에게 다양한 서비스를 제공하고 그에 대한 Accounting 에 대해 신뢰를 제공해 줄 수 있는 기술의 발전 방향을 알아 볼 수 있었다

참고문헌

[1] Pat R Calhoun, T. Johansson, C. Perkins "draft-ietf-aaa-diameter-mobileip-14.txt", IETF work in progress

[2] Pat R. Calhoun , Stephen Farrell, William Bulley "draft-ietf-aaa-diameter-cms-sec-04.txt", IETF work in progress

[3] Pat R. Calhoun, Erik Guttman, Glen Zorn, Jari Arkko, "draft-ietf-aaa-diameter-17.txt", IETF work in progress

[4] B.Aboba, J.Arkko, D.Harrington. "Introduction to Accounting Management", RFC 2975, October 2000.

[5]Harri Hakala, Leena Mattila,"draft-ietf-aaa-diameter-cc-00.txt", IETF work in progress