AAA 성능향상을 위한 분석과 시뮬레이션

김지선, 차은철, 최형기
성균관대학교 정보통신공학부
e-mail: {jskim, iris1212, hkchoi}@ece.skku.ac.kr

Study and Simulation of Enhancements for AAA Performance

JI-Sun Kim, Eun-Chul Cha, Hyung-Kee Choi
School of Information and Communication Engineering,
Sungkyunkwan University

요 약

네트워크 서비스를 제공함에 있어서 사용자 인증, 접근 권한 및 요금 처리는 필수적인 기능이다. 이러한 기능을 제공하기 위해 AAA 기술이 정의되었다. AAA의 성능은 네트워크 서비스 전체의 성능에 큰 영향을 줄 수 있다. 현재 AAA 성능에 관련된 이슈와 그 해결책은 알려져 있으나, 이를 통한 성능 향상의 정도는 분석되지 않았다. 본 논문은 AAA 이슈에 대한 분석과 해결책을 설명하고 시뮬레이션을 통해 각 이슈에 대한 성능 향상의 정도를 가시적으로 보여주고 있다. 시뮬레이션 결과에 따르면 AAA의 해결책을 적용한 경우 평균 33%의 성능 향상을 기대할 수 있다.

1. 서론

최근 인터넷이 제공하는 서비스의 종류가 늘어나면서 다루어지는 사용자 정보의 양도 급격히 증가했다. 사용자 식별 정보를 비롯한 서비스 이용 권한에 대한 정보, 사용 요금에 대한 정보 등 사용자 정보의 종류 역시 다양해졌다. 개별 사용자를 비롯한 서비스 사업자는 그러한 정보들의 교환 및 처리가 안정된 환경에서 다뤄지길 원한다. 분산되어 저장되고 다뤄지는 정보들의 보안 역시 중요하다 [1].

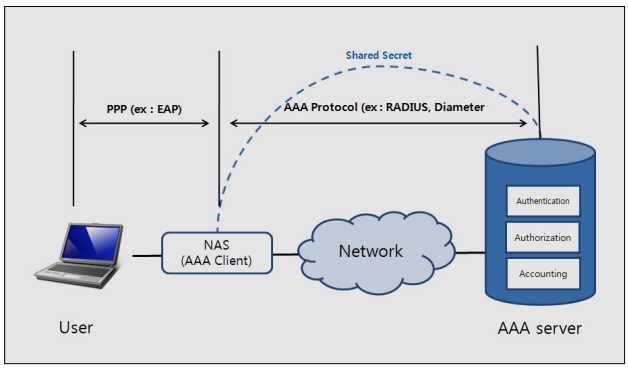
현재 대부분의 유, 무선 환경에서 AAA을 적용하여 서비스 관련 정보를 보호하고 있다. AAA(Authentication, Authorization, Accounting) 는 서비스 사업자를 대신하여 사용자를 인증(Authentication)하고 서비스 이용 권한을 관리(Authorization)하며 사용자가 이용한 서비스에 대한 사용 요금을 정산(Accounting)하는 과정을 체계적으로 지원하는 기술이다 [2]. 사용자 인증과 권한 관리, 과금 처리와 같은 서비스 공급 과정에 직접 관여하기 때문에 AAA의 구조와 체계, 사용하는 프로토콜의 성능 개선은 전체 서비스 향상을 유도 할 수 있다. AAA 성능 개선에 대해 다양한 AAA 자체 이슈들이 제시 되었음에도 불구하고, 현재 대부분의 AAA 성능 개선 연구는 다른 기술과의 연동 및 응용을 통한 개선에 중점을 두는 것이 일반적이다 [3][4][5][6]. AAA 자체 성능 개선 이슈들에 대한 검증 작업 역시 이루어 지지 않았다. 본 논문은 AAA 자체 성능 개선 이슈들과 해결책을 분석하고, 시뮬레이션을 통해 실제 성능 향상의 효과를 확인한다. 이와 같은 연구는 AAA 성능 개선에 대한 의미 있는 접근이 될 것이다.

논문의 구성은 다음과 같다. 2장에서 AAA에 대한 정의와 성능 개선을 위한 이슈들을 살펴보고 3장에서 이슈들을 분석하여 해결책을 제시한다. 그리고 4장에서 제시된 해결책을 적용했을 때 프로세스의 향상을 시뮬레이션을 통해 보여준 후 5장에서 결론을 맺는다.

2. AAA

2.1 AAA 개요

AAA를 적용한 네트워크 환경에서 서비스 사업자는 사용자의 식별 정보를 판단하여 사용자를 인증한 후 해당 서비스에 대한 접근을 승인하거나 거부한다. 이를 AAA의 사용자 인증과 권한 부여 과정이라고 한다.



(그림 1) AAA의 구조

본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-C1090-0801-0028)

부여받은 권한에 따라 사용자는 서비스에 접근하여 이용하게 되고, 발생되는 요금에 대한 정보를 AAA가 관리하는 것이 AAA의 과금 처리 과정이다. AAA의 통신환경은 보통 server-client 구조로 구현한다. (그림 1)은 AAA server-client 구조를 도식화 한 것이다.

(그림 1)에서 보듯이 AAA의 기능을 수행하는 핵심적인 역할은 AAA server가 담당하고, 사용자 단말과 AAA server 사이에 AAA client, NAS(Network Access Server)을 배치한다. 단말과 NAS는 Point-to-Point 로 연결되어 EAP [7]와 같은 Point-to-point protocol [8]을 이용한다. NAS와 AAA server는 멀티 홉 환경에 용이한 AAA 프로토콜을 사용한다. 대표적인 AAA 프로토콜로 RAIDUS [9]와 Diameter [10]를 들 수 있다. NAS는 단말로부터 전송 되어 온 PPP 프레임을 해당 AAA 프로토콜 프레임에 다시 수납하여 전송함으로 AAA server와 사용자 단말 사이에 프로토콜 차이로 인한 문제를 해결 해준다.

대표적인 AAA 프로토콜 중 하나인 RADIUS는 AAA 프로토콜의 초기 형태로 전형적인 server-client protocol 성격을 지니고 있다. 전송 방식으로 비 연결형, 비 신뢰형의 UDP(User Datagram Protocol)을 사용한다. Diameter는 1998년 결성된 IETF의 AAA Task Group이 제시한 AAA 표준 프로토콜이다. Diameter는 차세대 통신환경에 적합한 로밍 기술을 지원한다. RADIUS에 비해 Peer-to-Peer protocol 성격을 지니고 있고, 신뢰성 있는 스트림 전달 형태인 SCTP(Stream Control Transmission protocol)와 TCP(Transmission Control Protocol)을 전송 방식으로 사용 한다 [3].

2.2 AAA 이슈

개방된 네트워크 환경에서 AAA의 역할이 점점 부각되며, AAA 성능 개선을 위한 이슈들이 주목 받고 있다. AAA의 모든 기능은 사용자와 서비스 네트워크 간의 통신으로 시작이 된다. 이 때문에 AAA 프로토콜 및 전송 방식에 관련된 이슈들은 다양한 AAA 자체 이슈들 중에서도 특히 중요하다. 대부분 사용자 단말과의 통신에서 NAS 와의 PPP인 EAP를 사용한다는 사실에 착안하여, EAP의 효율에 영향을 주는 AAA 프로토콜 이슈인 HOL (Head-of-Line) 차단과 SWS (Silly Window Syndrome)에 초점을 맞추었다.

3. AAA 이슈 및 해결책 설명

3장에서는 EAP 효율에 영향을 주는 AAA 이슈들인 HOL 차단과 SWS를 살펴보고 각 이슈들의 해결책을 설명한다.

3.1 HOL 차단

Diameter와 같이 신뢰성 있는 전송 프로토콜을 사용하는 AAA 프로토콜에서 모든 인증 요청에 대해 연결을 설정하는 것은 비효율적이다. 예를 들어 48-port NAS를 사용하고 TCP 상에서 Diameter를 사용할 경우 최대 48개의 TCP 연결을 동시에 유지해야 한다. 그러므로 자원의 효율적 관리를 위해 하나의 지속적 연결(persistent connection)을 만들고 이 연결을 통해 단말들의 요청들을 파이프 라이닝(pipelining)하는 것이 합리적이다. 그러나 이 경우에 하나의 패킷의 유실이 여러 단말의 인증 세션에 걸쳐 영향을 미치는 HOL 차단현상이 발생할 수 있다. HOL 차단현상은 TCP에서 패킷이 유실 되면 그 패킷의 재전송을 마치기 전까지 그 후에 도착한 모든 패킷의 전송이 지연되기 때문에 발생한다. HOL 차단현상은 SCTP의 멀티스트림을 사용하여 해결 할 수 있다. 멀티스트림은 하나의 연결을 여러 개의 독립적인 메시지의 스트림으로 전송하는 SCTP의 기능을 가리킨다. 이 기능을 사용하면 다른 사용자의 인증 세션을 다른 스트림을 통해 전송하는 것이 가능하다. 이 경우 어떤 인증 세션의 스트림에서 패킷이 유실되어도 다른 스트림에는 영향을 미치지 않으므로 HOL 차단현상을 방지할 수 있다.

3.2 SWS

SWS는 TCP에서 보내는 쪽의 어플리케이션이 데이터를 느리게 발생시키거나 받는 쪽에서 받은 데이터를 느리게 소비할 때 발생한다. 두 경우 모두 작은 세그멘트를 전송하게 하여 네트워크의 효율을 떨어뜨린다. 극단적인 예로 보내는 어플리케이션이 계속적으로 1 바이트의 데이터를 발생시킬 경우 실제로 전송되는 데이터는 41 바이트로 유용한 정보에 비해 부하가 커지게 된다. TCP에는 네트워크에서 MSS(Maximum Segment Size) 보다 작은 패킷의 불필요한 전송을 제한하기 위한 목적으로 만들어진 메커니즘(SWS avoidance)들이 있다. 그 대표적인 메커니즘은 Nagle 알고리즘과 Delayed ACK 메커니즘이다.

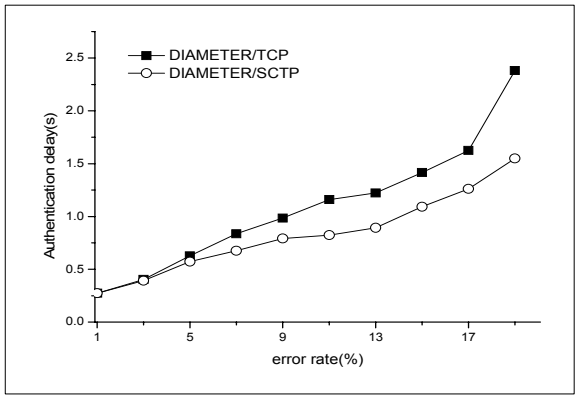
Nagle 알고리즘은 SWS를 송신 측에서 해결하고자 하며 전송측 버퍼내의 데이터가 MSS보다 커지거나 ACK가 도착할 때까지 데이터의 전송을 보류하는 메커니즘이다. Delayed ACK은 반대로 수신 측 측면의 해결책이다. Delayed ACK는 데이터를 받은 후에 즉시 ACK를 보내지 않고 버퍼에 데이터가 존재하거나 타이머가 만료된 후에 ACK를 보낸다. 일반적으로 인증 프로토콜의 메시지의 크기는 MSS보다 작다. 그러므로 SWS avoidance를 위한 메커니즘들을 사용하여 여러 AAA 메시지를 하나의 패킷에 결합하는 것은 네트워크의 부담을 줄이는데 도움이 된다.

4. 시뮬레이션을 통한 해결책 효과 분석

4장에서는 앞서 3장에서 설명한 이슈의 해결책들이 네트워크 환경에 미치는 영향을 시뮬레이션을 통해 분석한다. 사용된 시뮬레이터 NS-2 [11]이고 시뮬레이션을 위해 IEEE 802.16 네트워크 환경이 선택되었다. 서비스를 요구하는 사용자의 최대 단말 수는 100개로 한정하고 단말과 NAS 간 통신에 사용될 프로토콜은 PPP EAP, NAS와 AAA server 간 통신에 사용될 프로토콜은 AAA 표준 프로토콜인 Diameter으로 선택 하였다.

4.1 HOL 차단 해결 효과 분석

HOL 차단 이슈의 해결책으로 제시된 SCTP 멀티스트림의 사용의 효과를 확인하기 위해 시뮬레이션을 수행하였다.

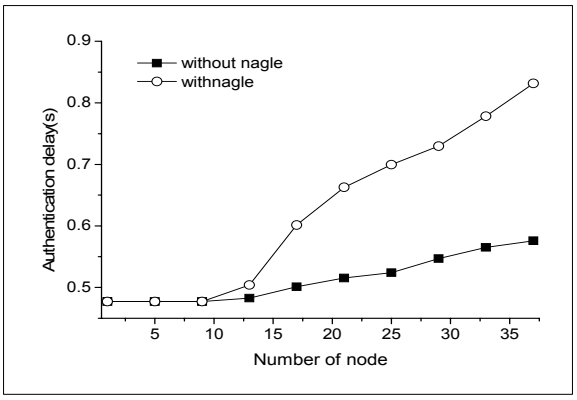


(그림 2) Diameter에서 SCTP 멀티스트림의 효과

시뮬레이션을 위해 의도적으로 에러를 포함한 패킷을 발생시키며 EAP 인증을 수행하도록 하였다. (그림 2)에서 볼 수 있듯이 링크의 에러율이 높아짐에 따라 TCP와 멀티스트림을 사용하는 SCTP 사이의 차이가 확연하게 나타난다. SCTP를 사용 했을 경우, TCP를 사용했을 때보다 인증 지연 시간에서 최대 37.5% 향상이 있다. 에러율이 5%이었을 때 TCP를 사용한 AAA 프로토콜과 SCTP를 사용한 AAA 프로토콜의 인증 지연 시간의 차이는 0.5초 정도 이지만, 이후 에러율이 19%에 달했을 때 인증 지연 시간 차이는 약 1.25초로 벌어진다. 그 이유는 앞에서 언급한 것과 같이 SCTP의 멀티스트림이 HOL 차단현상을 방지하기 때문이다. 하나의 패킷 유실이 여러 인증 세션에 걸쳐 영향을 미치는 TCP와 달리 멀티스트림을 사용하는 SCTP는 하나의 패킷 유실은 하나의 인증 세션에만 영향을 미친다.

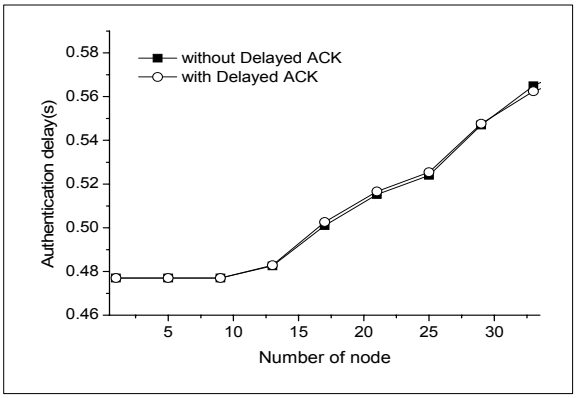
4.2 SWS 해결 효과 분석

Nagle 알고리즘과 Delayed ACK이 성능에 미치는 영향을 시뮬레이션을 통해 확인하였다.



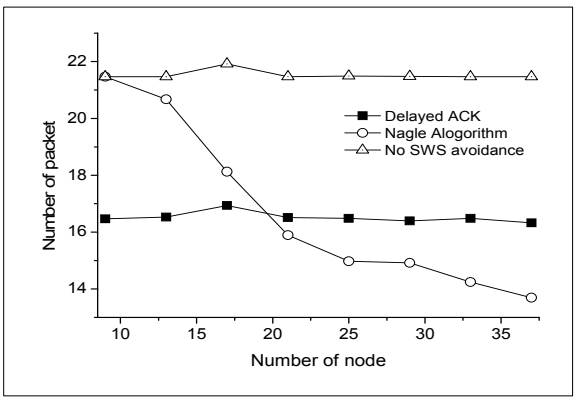
(그림 3) Nagle 알고리즘 사용 시 Diameter 성능의 변화

(그림 3)에서 보는 것과 같이 Nagle 알고리즘을 사용한 경우 사용하지 않았을 때에 비해 인증에 걸리는 시간이 긴 것을 확인할 수 있다. 일반적으로 인증 메시지는 대부분 MSS 보다 작다. 그렇기 때문에 데이터를 전송하기 위해서 버퍼에 MSS 이상으로 데이터가 들어오기까지 기다리는 시간이 필요하다. 이 시간 때문에 전체 인증 시간에 영향을 미치게 되는 것이다.



(그림 4) Delayed ACK 사용 시 Diameter의 성능 변화

Nagle 알고리즘과 달리 Delayed ACK은 인증 시간에 크게 영향을 미치지 않는 것을 (그림 4)를 통해 확인할 수 있다. Delayed ACK은 데이터를 수신 했을 때 송신 측에 보낼 데이터를 가지고 있으면 지연 없이 데이터를 ACK에 피기백 해서 보낸다. Nagle 알고리즘을 적용 했을 때보다 성능향상의 효과가 또렷하지 않다. 그 이유는 인증 프로토콜을 사용하는 수신자들은 대부분 메시지를 받으면 바로 응답 메시지를 전송하기 때문에 Delayed ACK의 영향을 거의 받지 않기 때문이다.

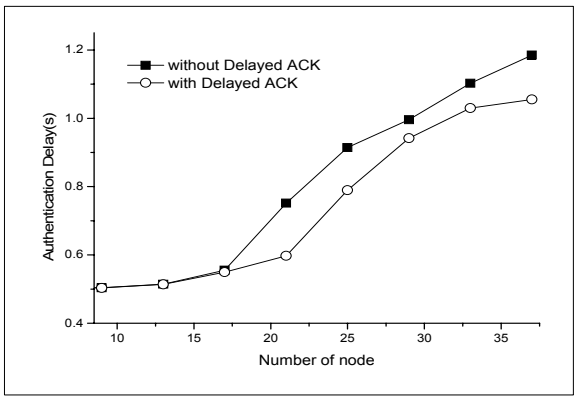


(그림 5) SWS avoidance에 의한 네트워크 부하 감소

(그림 5)은 Nagle 알고리즘과 Delayed ACK가 인증 시간에는 악영향을 줄 수 있지만 네트워크 부담을 줄이는 데 도움을 줄 수 있음을 보여준다. 그림에서 볼 수 있듯이 Delayed ACK을 사용했을 때는 전체적으로 전송되는 패킷의 개수가 SWS avoidance를 적용하지 않은 경우의 30% 정도인 것을 볼 수 있다. 이는 데이터가 ACK에 피기백 되면서 ACK 메시지의 수가 감소하기 때문이다.

Nagle 알고리즘의 경우 인증을 요청하는 노드의 수가 증가함에 따라 점차적으로 패킷의 개수가 줄어든다. 9개의 노드가 있을 때 21개에 달하던 패킷은 노드가 37개로 늘어나자 13개로 줄어든다. 이는 노드의 수가 증가함에 따라 전송되는 인증 메시지의 수가 증가하며 그에 따라 메시지들이 하나의 패킷으로 결합되는 확률이 증가하기 때문이다. 패킷의 갯수을 기준으로, SWS avoidance 매커니즘을 사용하지 않은 경우와 대비하여 Nagle 알고리즘은 38%, Delayed ACK은 23% 의 성능 향상을 보여준다.

SWS avoidance에 의한 패킷 수 감소의 효과는 일반적이 상황에서 보다 네트워크 혼잡이 발생할 때 더 유효하다. 네트워크 혼잡은 여러 개의 NAS가 하나의 AAA server에 연결되어 있을 때 발생할 수 있다. 또한 발생 빈도가 높지는 않지만 AAA server가 전원 문제 등으로 정상적인 동작을 하지 않다가 복구되었을 때 동시에 많은 양의 인증 요청이 발생하면서 네트워크 혼잡이 발생할 수 있다. SWS avoidance 메커니즘들은 패킷의 수를 감소시킴으로써 네트워크 혼잡시 라우터 등에서 발생하는 큐잉 지연이나 재전송 지연을 줄일 수 있다.



(그림 6) 네트워크 혼잡시 Delayed ACK의 효과

네트워크 혼잡 시 SWS avoidance의 효과를 보기 위해 NAS와 AAA server 사이에 링크 용량의 85%에 해당하는 UDP 트래픽을 생성시키며 시뮬레이션을 수행하였다. (그림 6)은 네트워크 혼잡이 발생할 때 Delayed ACK의 효과를 보여준다. 그림에서 볼 수 있듯이 Delayed ACK을 사용할 경우 Delayed ACK을 사용하지 않을 때보다 인증 시간이 감소하였다. (그림 5)에서 Delayed ACK의 사용으로 전송되는 패킷 수가 감소하는 것을 확인 하였다. 패킷 수의 감소로 인해 큐잉 지연이나 재전송 지연이 역시 감소했기 때문이다.

5. 결론

인터넷이 확장되며 다양한 형태의 네트워크가 공존하기 시작했다. 복잡해진 네트워크 환경에서 사용자 인증과 서비스 공급을 관리하는 AAA의 역할은 중요하다.

AAA의 성능 개선은 전반적인 서비스 공급 과정의 향상을 유도 할 수 있다. 성능 개선에 대한 AAA 자체 이슈들과 해결책은 이미 알려져 있었지만, 실제 얼마만큼의 성능 개선이 이루어지는지, 그 영향에 대한 직접적인 분석은 없었다. 특별히 정보교환 과정에 연관 있는 AAA 이슈들을 선택하여 각 이슈들의 해결책이 실제 네트워크 향상에 기여하는 정도를 분석 하였다. NS-2를 사용하여 IEEE 802.16 네트워크 환경에서 수행된 시뮬레이션은 알려진 AAA 이슈의 해결책들이 평균 33%의 향상 효과가 있는 것으로 나타났다.

참고문헌

[1] C. Rensing *et al.,* "AAA: a survey and a policy-based architecture and framework", *IEEE Network*, Vol.16, No.6, Nov. 2002

[2] H.G Kim, B.G. Lee *et al.*, "On the International Standardization of AAA Technology" , *ETRI* korea, 2003.

[3] R Ekstein *et al.*, "AAA Protocols: Comparison between RADIUS, Diameter, and COPS", *IETF NASREQ WG INTERNET-DRAFT,* draft-ekstein-nasreq-protcomp-00.txt, Oct. 2000.

[4] Pat R. Calhoun *et al.*, "Diameter Mobile IPv4 Application," *IETF AAA WG, INTERNET-DRAFT*, draft-ietf-aaa-diameter-mobileip-20.txt, Aug. 2004.

[5] A. Yegin *et al,*, "AAA Mobile IPv6 Application Framework," *IETF MIP6 WG, INTERNET-DRAFT*, draftyegin-mip6-aaa-fwk-00.txt, Aug. 2004.

[6] B. Aboba *et al.*, "Authentication, Authorization and Accounting (AAA) Transport Profile", RFC 3539, June. 2003.

[7] B. Aboba *et al.*, "Extensible Authentication Protocol(EAP)", RFC 3748, June. 2004.

[8] W. Simpson, "Point-to-Point Protocol(PPP)" RFC 1661, July. 1994.

[9] C. Rigney *et al.*, "Remote Authentication Dial In User Service(RADIUS)", RFC 2058, June. 2000

[10] P. Calhoun *et al.*, "Diameter base prtocol", RFC 3588, Sep. 2003

[11] Network Simulator NS-2. http:// www.isi.edu/nsnam/ns/