EAP-MD5 AAAv6 운영을 위한 인증처리 최적화 모델

정 윤 수[†] · 우 성 희[††] · 이 상 호[†††]

요 약

이동 인터넷 환경에서 보안성과 급증하는 서비스 요구를 효율적으로 제어하기 위해 AAAv6기반 Diameter 기술이 사용자 인증에 사용되고 있다. 그러나 Diameter에서 제공하는 기본적인 인증기법은 로밍 서비스나 인터넷 전송 과정에서 보안성이 떨어지는 단점을 가지고 있어 EAP-MD5와 같은 암호알고리즘과 결합하여 사용자 인증처리를 수행한다. 이러한 사용자 인증처리를 효율적으로 수행하기 위해서는 AAAv6 환경을 구성하고 있는 AAA attendent, AAAv, AAAb, AAAh, HA 서버들의 성능 충족 방안이 필요하다. 따라서, 이 논문에서는 도메인간의 이동성을 가지는 AAAv6 인증 모델중의 하나인 EAP-MD5기반의 운영 모델을 설계하고 실험을 통하여 사용자 인증 기능을 수행하는 각 서버의 최적 성능지표를 산출하고 이를 이용하여 AAAv6의 사용자 인증 처리를 최적화 시킬 수 있는 지표들을 제시한다.

키워드 : EAP-MD5, AAAv6, 성능 예측, 사용자 인증처리

Authentication Processing Optimization Model for the EAP-MD5 AAAv6 Operation

Jeong Yoon Su[†] · Woo Sung Hee[††] · Lee Sang Ho[†††]

ABSTRACT

With the increasing service quality and security in the Mobile Internet, Diameter technology based on the AAAv6 is being used in the user authentication. But there are some problems on the authentication procedures of the Diameter in which the security falls down from a loaming service or Internet transmission course. We combine it with the cipher algorithm like EAP-MD5 and accomplish a user authentication processing. If we want to supply the user authentication with the mobility among domains by AAAv6-based Diameter, we need the efficient capacity allocation among AAA attendent, AAAv, AAAb, AAAh, HA servers in the AAAv6. Therefore in this paper, we propose to make the authentication capacity index to carry out user authentication ability by analyzing an EAP-MD5 server capacity model of AAAv6 authentication models for users with mobility among domains, and to find the optimized condition for the AAAv6 capacity by the index.

Key Words : EAP-MD5, AAAv6, Performance Estimation, User Authentication

1. 서 론

이동전화와 Wireless LAN을 통한 무선 인터넷의 확산에 따라 이동중의 인터넷 서비스뿐만 아니라 서비스의 안정성과 신뢰성, 보안성 등을 위한 여러 가지 도메인 간 응용 서비스가 등장하게 되었다. 이들 서비스들은 기본 서비스에 비해 보다 신뢰적이고 안전한 관리를 요구하게 되었고, 이들의 요구사항을 IETF(The Internet Engineering Task Force)에서는 각 분야에 적합한 AAA(Authentication, Authorization, Accounting) 프로토콜을 연구하게 되었다[9, 15, 16].

현재 PPP(Point-to-Point)나 터미널 서버 액세스와 같은 서비스를 위한 AAA 프로토콜로 RADIUS(Remote Authenticationn Dial-In User Service)프로토콜이 사용되는 AAA기술은 업체간에 연동 가능한 망 개수가 겨우 4개에 불과한 데다, 로밍 서비스나 인터넷 전송 과정에서 보안성이 크게 떨어져, 다양한 유·무선 통신망의 융합, 급증하는 로밍 서비스 수요 충족에 부적한 것으로 평가 되고 있다[1, 7, 12, 17]. 이러한 문제들을 해결하기 위해 AAA 환경을 구성하고 있는 다양한 서버들은 CMS(Cryptographic Message Syntax) 확장을 통해 보안을 강화하고 NASREQ-EQP 응용 기술을 사용하여 신뢰적이고 효율적인 사용자 인증을 추구하고 있다[2-6].

AAAv6 환경 구축을 위한 서버로는 AAA attendent, AAAv, AAAb, AAAh, HA등 5개의 엔터티를 정의하고 있다. AAA attendent는 이동 노드가 외부 링크에서 가장 먼저 접속하게

† 준 회 원 : 충북대학교 이공대학 전자계산학과 재학
†† 정 회 원 : 청주과학대학 컴퓨터과학과 부교수
††† 종신회원 : 충북대학교 전기전자컴퓨터공학부 컴퓨터정보통신연구소 교수
논문접수 : 2005년 4월 6일, 심사완료 : 2005년 7월 29일

되는 외부 엔티티로서 이동 노드가 전송하는 패킷에대한 통과, 폐기, 보류 등의 정책을 수행할 수 있으며, AAA 서버를 통한 인증 성공시 패킷을 통과 시킬 수 있다. AAAv는 외부 링크의 AAA 인증 서버로서 이동 노드로부터 인증 요청을 수신하면 먼저 AAA attendent를 인증하고 메시지의 NAI나 홈 주소를 통해 이동 노드의 홈 도메인에 존재하는 AAA 인증 서버로 전송한다. AAAh는 홈 도메인의 AAA 인증 서버로서, 이동 노드의 인증에 필요한 인증 정보들로 구성된 프로파일을 관리하고 있다. 각 도메인별 AAAv6기반 서버들의 효율적인 운영을 위해서는 각 서버의 성능 보장을 통한 유기적 연계가 필수적 요소이다[18].

따라서, 이 논문에서는 AAAv6 환경의 서버들이 도메인간의 이동성을 가지는 사용자들에 대해서 안정적으로 서비스할 수 있도록 EAP-MD5의 암호 알고리즘을 DSA와 RSA로 구분하여 사용자들의 평균도착시간 간격에 따른 각 서버의 최적 성능지표를 구하고자 한다.

이 논문의 구성은 다음과 같다. 2장에서는 EAP를 확장한 EAP-MD5 인증 메커니즘에 대해서 기술한다. 3장에서는 실험을 위한 모델과 실험 수치를 산출하고, 4장에서 실험 및 결과을 분석한다. 마지막으로 5장에서는 결론 및 향후연구에 대해 기술한다.

2. EAP-MD5

EAP는 무선과 유선 모두에서 사용될 수 있다. 하지만 EAP-MD5는 단방향 해시(one-way hash) 기능과 수하(challenge)를 사용해서 요구자의 신원증명서를 확인하며, 이것은 802.1x에서 가장 간단하게 사용할 수 있다. 하지만 무선쪽에서는 보통 선택이 잘 안되고 있는데, 그 이유는 이것이 클라이언트 인증만 지원해서 불량 무선 AP(Access Point)에는 취약성을 남겨두기 때문이다. EAP-MD5 수하는 가장 초기의 EAP 인증 유형이고, 유일한 필수 구현 방식이다. 이 프로토콜은 802.1x 프레임워크에서 기본 수준의 EAP를 지원하는 대표적인 EAP 인증유형이다. EAP 인증 유형의 표준이 하나로 결정되기 전까지, 앞으로 많은 사업자들이 무선랜 보안 시장에 뛰어들수록 더 많은 EAP 인증 유형들이 생겨날 것이다.

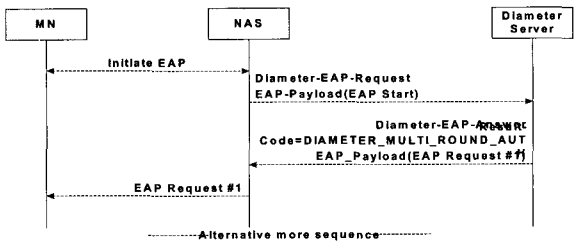
초기 드래프트에서 Diameter NASREQ 애플리케이션의 일부분이었던 Diameter EAP는 NASREQ에 많이 의존한다[14]. 가장 초기의 EAP 인증 유형이고 유일한 필수(mandatory) 구현 방식인 EAP-MD5를 AAAv6에서 사용하기 위해서는 새로운 Diameter Command Code가 필요하다. <표 1>은 Diameter에서 EAP를 사용하기 위한 Command이다[8, 13].

〈표 1〉 Diameter EAP Command Code

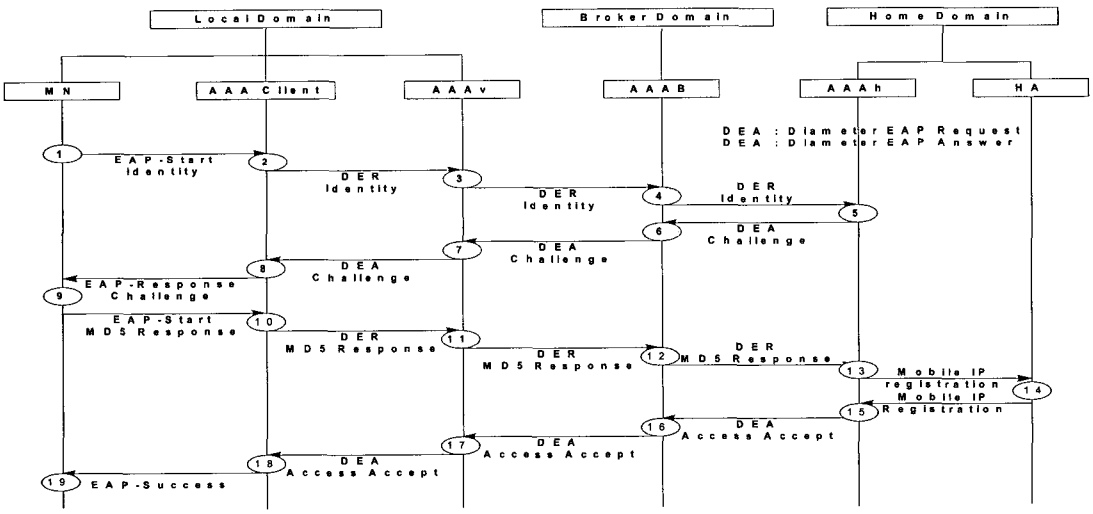
Command-Name	Abbrev	Code
Diameter-EAP-Request	DER	268
Diameter-EAP-Answer	DEA	268

EAP Conversation은 User와 NAS(AAA attendent)간에 PPP와 IEEE 802.1X와 같은 Link Layer에서 시작된다. EAP Conversation이 시작되면 NAS는 Diameter 서버에게 Diameter-EAP-Request를 보낸다. 만약 Diameter Home Server가 EAP 인증을 수행하게 되면, 암호화된 EAP 패킷에 EAP-Payload AVP를 담아 Diameter-EAP-Answer 메시지를 보내게 된다.

이때 결과 코드(Result-Code) AVP는DIAMETER_MULTI_ROUND_AUTH로 설정된다. 그 과정은 아래 (그림 1)과 같으며 선택적으로 여러 라운드로 이루어 질 수 있다.



(그림 1) Diameter EAP 인증 협상



(그림 2) Diameter EAP-MD5 인증 메커니즘

EAP-MD5는 (그림 2)와 같은 인증 과정을 거치게 된다. MN(Mobile Node)은 AAA attendent와 인증을 위하여 사용하게 될 EAP에 관한 negotiation(initiate EAP MD5)을 하게 되고, 그 결과에 따라 Diameter-EAP-Request 메시지를 AAA attendent가 AAA server에게 전송하게 된다. MN의 인증 유형은 크게 Intra 도메인와 Inter 도메인으로 나뉜다. Intra 도메인의 경우는 MN이 Local 사용자이기 때문에 인증 시퀀스는 ①→②와 ⑱→⑲로 마치게 된다. Inter 도메인은 ①→⑲의 모든 시퀀스를 거친다[8].

3. AAA 서버 성능평가를 위한 Diameter 기반의 EAP-MD5 인증 모델

각 서버의 효율적인 서비스를 위해 HA에서 등록 메시지를 처리하는 전/후과정을 등록 요구처리/등록 응답처리라고 정의하고, 암호처리 프로세스와 등록 프로세스 수치값들을 구하기 위한 실험 가정을 각 서버 환경에 맞게 설정한다. 설정된 수치값들은 암호 연산 시간과 등록 연산 시간을 합한 평균 처리속도를 이용하여 AAAv6 시스템 환경에서의 사용자 인증 수행을 최적화 할 수 있는 각 서버 성능 지표를 구한다.

3.1 가정

Diameter 기반의 EAP-MD5 환경에서의 각종 서버들의 최적 요구성능을 얻기 위한 실험 모델의 가정은 아래와 같다.

① 각 서버의 안정적 운영을 위하여 서버의 이용율은 70% 수준으로 설정한다.

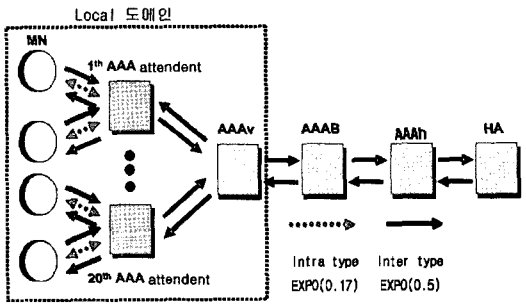
② 하나의 local 도메인에는 20개의 AAA attendent가 있고, 각 AAA attendent의 처리능력은 동일하다.

③ Diameter EAP-MD5 인증 메시지는 한개의 AAA 브로커(Broker)을 경유한다.

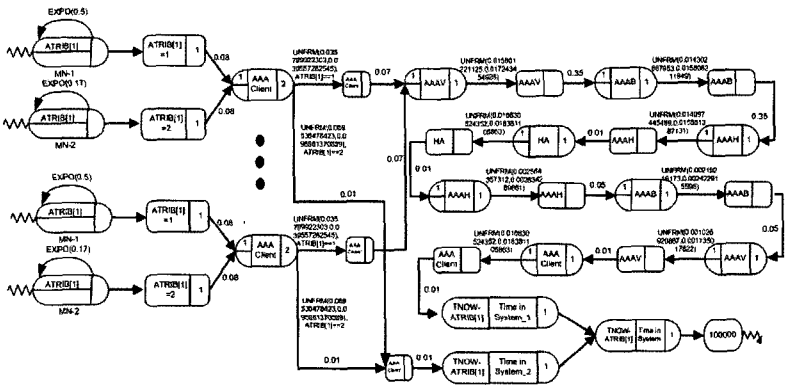
④ Registration Message Request 처리는 Mobile IP 등록 이전 단계로 하고 Registration Message Response 처리는 Mobile IP 등록 이후 단계로 한다.

3.2 모델설계

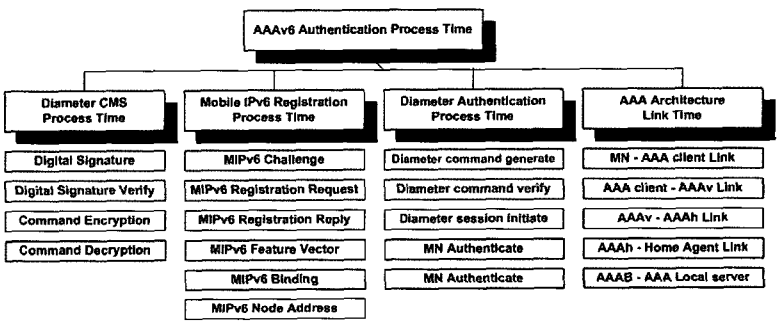
시뮬레이션을 위한 Diameter기반의 EAP-MD5 인증모델은 (그림 3)과 같으며, EAP-MD5의 환경을 구성하고 있는 MN들의 입력 패턴은 크게 Intra 도메인과 Inter 도메인으로 구분하고, 각 도메인별 입력에 대한 평균 도착시간 간격은 0.17와 0.5의 지수분포로 정의한다.



(그림 3) Diameter EAP-MD5 사용자 인증 실험 모델



(그림 4) Awesim 모델



(그림 5) AAAv6 인증과정의 수행 시간

(그림 3)의 실험 모델을 Awesim 모델로 표현하면 (그림 4)와 같다.

3.3 성능 평가를 위한 파라미터 설정

성능평가 실험을 위해 필요한 AAA 서버들의 수치값은 Diameter CMS(Cryptographic Message Syntax) process time, Mobile IPv6 Registration process time, Diameter Authentication process time, AAA Architectural Link Delay time 등이 있고, 이들 프로세스 수치값들의 합은 각 서버의 평균 처리 시간으로 구한다. (그림 5)는 Mobile IPv6를 지원하는 AAAv6 인증과정에서 소요되는 각종 처리시간을 나타낸다[9-10, 11, 19-22].

3.3.1 MN으로부터의 인증요청 유형

AAAv6 인증 모델중의 하나인 EAP-MD5의 환경을 구성하고 있는 서버들의 서비스 입력 유형은 크게 Intra 도메인과 Inter 도메인으로 분류할 수 있다. Intra 도메인의 경우 local 도메인내에서 평균 도착시간 간격을 0.17의 지수분포로 서비스하는 유형을 말하고, Inter 도메인의 경우는 local 도메인간의 평균 도착시간 간격을 0.5의 지수분포로 서비스하는 유형을 말한다[11]. 그리고 각 서버가 사용자 인증을 처리하는데 소용되는 시간의 오차 범위는 서비스 환경에 영향을 줄 수 있는 여러 가지 요소들을 감안하여 ±5%의 이항분포로 설정한다.

3.3.2 Diameter 암/복호 처리시간

Hop-by-Hop Security를 위하여 이 논문에서 사용되고 있는 Diameter CMS 프로세스 시간은 DSA와 RSA를 이용한 Digital Signature와 3DES를 통한 암호화 처리시간를 사용하고 있으며, 암호 알고리즘에 사용되는 속도는 속도 Benchmarks를 참조하여 유추하였다[9].

Diameter CMS 프로세스를 위해 사용하는 각 암호화 알고리즘의 Signature와 Verification 수치는 암호화 알고리즘을 평가한 연구를 참조하여 Diameter EAP command의 길이와 처리시간을 구하였다[4]. <표 2>는 CMS 프로세스 처리과정에 의해 DSA와 RSA의 평균 처리시간을 계산한 최종 결과값이다.

〈표 2〉 Diameter 암/복호 처리시간

(단위 : μs)

서 버 / 처리시간	AAA Attendent	AAAv	AAAb	AAAh	HA
DSA 평균처리시간	9,135.6644	18,275.2041	18,271.328550	13,703.496413	4,567.832138
RSA 평균처리시간	9,775.66428	19,551.32856	19,551.328550	14,663.496413	4,887.832138

3.3.3 MIPv6 등록/인증 수행 시간

등록메시지에 대한 각 노드별 평균 처리시간을 토대로 각 노드별 프로세싱 시간을 가정하여 MN이 등록을 요청하면, AAAh와 AAAv는 HA와 AAA attendent의 메시지를 Relay하는 역할의 비중이 가장 크므로, AAAh와 AAAv는 AAAb와 동일한 수행시간을 갖는다고 가정한다. Diameter infrastructure를 구성하고 있는 각 노드의 인증 메시지 등록 관련 처리속도는 AAA 관련 보고서의 결과를 참조하여 P-2.1GHz에서의 연산 속도 가정치를 구하면 <표 3>과 같다[10].

〈표 3〉 P-2.1GH에서의 연산 속도 가정치

(단위 : μs)

처리시간 \ 서 버		AAA attendent		AAAv	AAAB	AAAh	HA
		Inter	Intra				
평균 처리 시간	등록 요구처리	49,700	697	49,700	697	249,900	49,700
	등록 응답처리		697	697	697	49,030	

3.3.4 EAP-MD5 수행 시간

EAP-MD5의 수행시간은 AAA key와 128bit의 challenge 그리고, 홈 주소를 키 해싱(keyed hashing)하는 과정으로 이루어져 있다. 사용되는 56bit의 키를 secret key로 가정하면 hashing하는 총 길이는 216bit가 되고, HMAC-MD5 연산 시간은 215.761 MByte/Second(1,809.9344 bit/μs)이 된다. 216bit를 hashing하는 총 시간은 0.11μs가 되고, EAP-MD5의 수행되는 노드는 MN과 AAA attendent, AAAh 모두 3곳에서 이루어진다.

3.3.5 AAAv6 링크 통신시간

실험평가를 위한 AAA Infrastructure의 링크는 A.Hess의 AAA 성능평가 실험 연구를 통해 얻은 링크 수치를 이용한다[11]. 통신 실험을 위하여 링크 처리를 (그림 2)의 메커니즘처럼 변경하면, <표 4>처럼 처리절차에 따른 링크 처리시간이 구해진다.

〈표 4〉 링크 통신시간

(단위 : μs)

Delay 시간 \ 서 버		MN -AAA attendent	AAA attendent - AAAv	AAAv-AAAB	AAAB-AAAh	AAAH-HA
Delay	등록 요구처리	30,000	30,000	15,000	15,000	10,000
	등록 응답처리	10,000	10,000	50,000	50,000	10,000

4. 성능평가 및 분석

4.1 실험환경

EAP-MD5기반의 AAAv6 모델을 실험하기 위해 사용되는 시뮬레이터는 Awesim3.0으로 하고, 실험에 사용되는 MN의 사용자 인증요청 메시지는 Intra/Inter 도메인에서 총 10만건이 AAA Attendent에 인증을 요청하는 것으로 한다. 또한 실험 환경에서 인증 요청메세지가 모두 처리되는데 소용되는 시간은 총 6시간이며 실험 환경은 <표 5>와 같다.

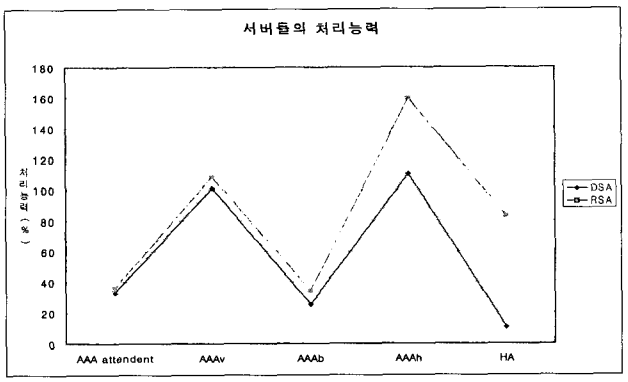
〈표 5〉 실험 환경

구 분	내 용
시뮬레이션 툴	AWESIM 3.0
메모리	256 MB
컴퓨터사양	Pentium4 2.4GHz Processor
OS	Windows XP SP1

4.2 실험 및 결과

3.3절에서 설정한 수치를 기반으로 AAAv6 모델에서의 암호처리는 AAA attendent에서 처리하고, 실험을 통하여 서버의 CPU 요구처리능력, 인증 처리시간, 인증요청 메시지 대기시간등의 지표를 구하고자 한다.

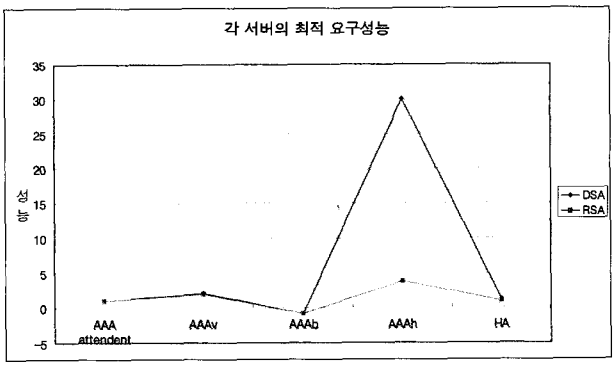
서버의 CPU 요구처리능력 지표를 구하기 전에 EAP-MD5을 적용한 AAAv6기반 서버들의 처리능력을 DSA와 RSA로 나누어 살펴보면 (그림 6)과 같다. (그림 6)에서 보는것과 같이 AAAv6기반 서버들이 처리할 수 있는 최대 처리능력을 100%라고 할 때 RSA를 사용하고 있는 서버들이 DSA를 사용하고 있는 서버보다 서버간의 처리능력이 비효율적이다. RSA를 사용하고 있는 AAAv와 AAAh는 DSA를 사용하고 있는 AAAv와 AAAh의 최대 처리능력보다 각각 8%와 49% 이상의 일을 더 처리하고 있다. 특히 AAAv의 경우 AAA attendent수를 20개로하여 실험하였기 때문에 Local Domain의 AAA attendent에서 보내오는 인증 메시지가 AAAv로 집중되기 때문에 AAAv에서 병목현상이 일어난다. 이런 결과는 각 서버간의 처리능력이 비효율적으로 동작되는 것을 알 수 있다.



(그림 6) AAAv6기반 서버들의 처리능력

(그림 7)은 사용자들에게 신뢰적이고 효율적인 사용자 인증을 제공하기 위한 각 서버의 최적 요구성능지표를 시간적 측면에서 DSA와 RSA로 구분하여 나타내고 있다. DSA의 경우 4.3절에서 설정한 수치를 기반으로 AAA attendent 서버의 성능을 펜티엄 4 2GHz의 성능을 가지는 서버라고 할때 AAAv, AAAh, HA 서버들의 성능은 각각 2.03배, 29.98배, 1.09배 빠른 서버가 필요하고 AAAb 서버는 0.82배 느린 서버가 필요하다. 특히 AAAh의 경우 AAAv6기반 서버들의 암호처리 작업을 수행하기 때문에 AAA attendent보다 28.98배 빠른 서버가 필요하고, AAAb의 경우 Diameter EAP-MD5 인증 메시지가 AAAb를 경유만하기 때문에 다른 서버보다 낮은 성능의 서버가 필요하다.

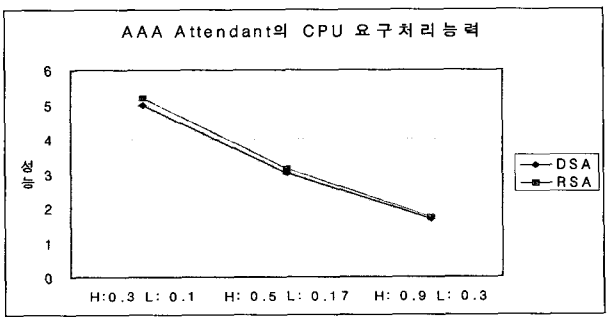
RSA의 경우 AAA attendent 서버의 성능이 DSA와 동일한 펜티엄 4 2GHz의 서버라고 할때 AAAv, AAAh, HA 서버들의 성능은 각각 1.95배, 3.817배, 0.98배 빠른 서버가 필요하고 AAAb의 경우는 0.88배 느린 서버가 필요하다. AAAb는 DSA와 마찬가지로 EAP-MD5 인증 메시지가 AAAb를 경우만하기 때문에 다른 서버보다 낮은 성능의 서버가 필요하다.



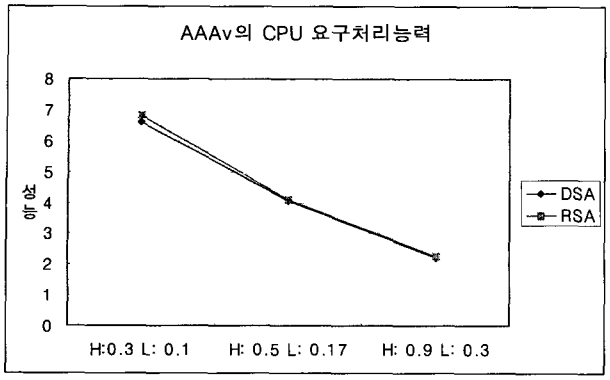
(그림 7) 각 서버 최적성능 결과

DSA와 RSA를 사용하는 AAAv6기반 각 서버들의 CPU 요구처리능력을 살펴보기 위해 MN들의 평균 도착시간 간격에 따라 크게 0.1와 0.3, 0.17와 0.5, 0.3와 0.9의 3가지 지수분포로 구분하여 AAAv6기반의 각 서버들의 성능을 분석한 결과 (그림 8), (그림 9), (그림 10), (그림 11), (그림 12)과 같다. AAAh를 제외한 나머지 서버들은 DSA보다 RSA에서 MN의 평균 도착시간 간격이 빠를수록 각 서버에서의 CPU 요구처리 능력이 높다. 그러나 암호처리가 이루어지는 AAAh 서버의 경우에는 MN의 평균 도착시간 간격이 빠를수록 각 서버에서의 CPU 요구처리능력이 RSA보다 DSA를 사용할 경우에 26.163배 더 높다.

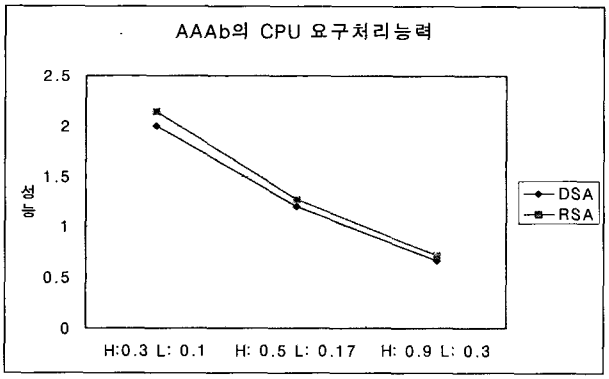
MN들의 평균 도착시간 간격에 따라 서버의 인증처리시간을 살펴보면 (그림 13)과 같으며, 인증처리 시간을 DSA와 RSA로 나누어 비교분석한 결과 DSA와 RSA 모두 MN에서의 평균 도착시간 간격이 짧을수록 서버의 인증처리시간은 적게들고 평균 도착시간 간격이 길수록 서버의 인증처리시간은 높게 나타나고 있다.



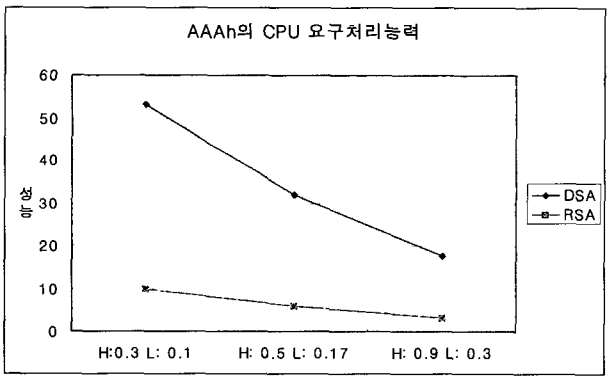
(그림 8) AAA Attendent CPU 요구처리능력



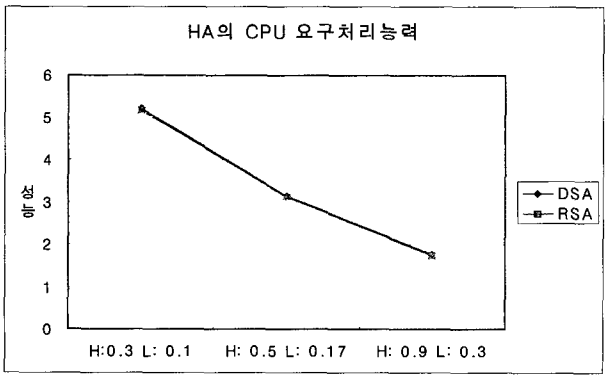
(그림 9) AAAv CPU 요구처리능력



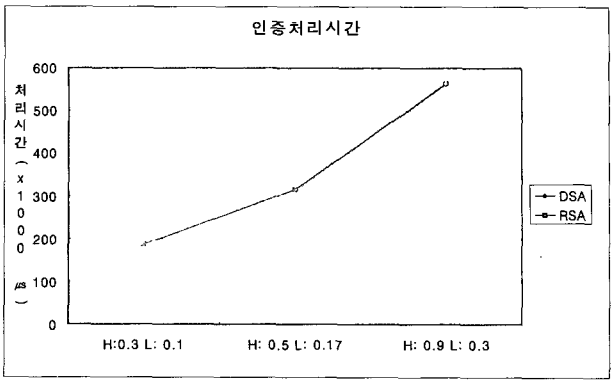
(그림 10) AAAb CPU 요구처리능력



(그림 11) AAAh CPU 요구처리능력

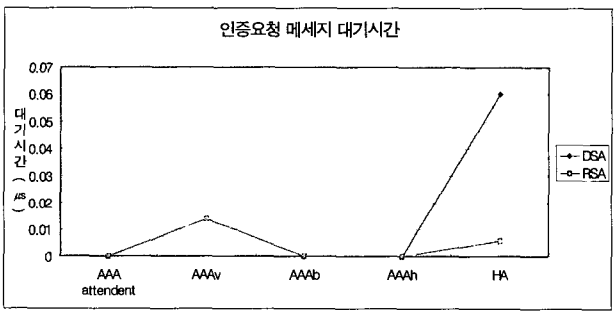


(그림 12) HA CPU 요구처리능력



(그림 13) 서버의 인증처리시간

각 서버에서의 인증요청 메시지의 대기 시간은 (그림 14)와 같으며, EAP-MD5 환경을 구성하고 있는 AAA attendent수를 20개로하여 실험하였기 때문에 Local Domain의 AAA attendent에서 보내오는 인증 메시지가 AAAv로 집중되어 병목 현상이 일어난다. DSA 알고리즘을 이용하는 AAAh의 경우 AAAv6기반 서버들의 암호처리 작업을 수행하기 때문에 전체 평균 대기시간 측면에서 보면 DSA보다 RSA가 약 0.383% 빠른 것으로 나타나고 있다. 이런 결과는 인증 메시지의 서버 대기 시간이 서버의 CPU 요구처리능력에 많은 영향을 미치는 것으로 나타났다.



(그림 14) 서버에서의 인증요청 메시지 대기시간

4.3 평가

DSA의 서버 이용률 중에서 AAAh의 CPU 요구처리 능력이 RSA보다 약 26.163배 높게 실험결과가 나타나고 있어 서버의 CPU 요구처리능력이 최적성능 수치에 많은 영향을 미치고 있다. 각 서버에서의 인증 메시지의 대기 시간은 Local Domain의 AAA attendent에서 보내오는 인증 메시지가 AAAv로 집중되기 때문에 AAAv에서 병목 현상이 일어난다. DSA의 AAAh의 경우 RSA보다 많은 암호처리 수행이 일어나지만 전체 평균 대기시간 측면에서 보면 DSA보다 RSA가 빠르게 처리되고, 인증 메시지의 서버 대기 시간의 실험 결과수치는 서버의 이용도등에 많은 영향을 미치는 것으로 나타났다. 결과적으로 각 서버 성능을 최적의 상태로 유지하기 전과 후의 전체 시스템 평균 처리시간을 현재의 Draft에 따라 시간적 측면에서 살펴보면 각 서버가 최적의 서비스를 제공하였을 때는 DSA보다 RSA가 0.383% 빠르게 처리된다.

5. 결 론

이동통신 기술을 이용한 서비스들은 기본 서비스에 비해 보다 신뢰할 수 있고 안전한 관리를 요구하게 되었고, 공개키 전자서명 및 검증, 서버간 노드 인증, 부인봉쇄, 기밀성 등의 기존 기술에서 문제되었던 보안 취약점을 해결해야 한다.

이의 해결을 위해, IETF AAA 워킹 그룹에서는 기존 RADIUS나 TACACS+를 보완 및 확장하여 새로운 프로토콜인 Diameter의 표준화를 진행중이고, Mobile IP 접속 서비스를 지원하도록 설계하고 있다. 이 논문에서는 AAAv6 환경을 구성하고 있는 AAA attendent, AAAv, AAAb, AAAh, HA 서버들이 도메인간의 이동성을 가지는 사용자들에 대해서 안정적으로 서비스 할 수 있도록 Diameter AAAv6을 확장한 EAP-MD5기반의 사용자 인증을 사용하였고, 사용자 인증에 필요한 암호 알고리즘은 DSA와 RSA로 구분하여 MN들의 평균도착시간 간격에 따라 AAAv6 서버들이 원활하게 서비스를 할 수 있도록 서버성능을 ±1% 미만의 오차범위를 갖는 최적 성능지표를 구하였다.

AAAv6기반 각 서버들의 CPU 요구처리능력은 암호처리가 이루어지는 AAAh서버를 제외한 나머지 서버들의 MN 평균도착시간 간격이 빠를수록 각 서버들의 CPU 요구처리 능력이 높지만 서버의 인증처리시간에서는 DSA와 RSA 모두 MN에서의 평균도착시간 간격이 짧을수록 서버의 인증처리시간은 적게 든다. 또한 각 서버의 최적 성능지표를 DSA와 RSA로 구분하여 각 서버가 원활하게 서비스 할 수 있는 실험을 하였을 경우 EAP-MD5의 최적성능 지표는 DSA보다 RSA가 약 0.383% 빠른 것을 알 수 있다. 이런 결과는 3DES 암호알고리즘에 RSA를 EAP-MD5에 적용한 것이 DSA를 적용하였을 때보다 각 서버의 서비스가 원활하게 동작되는 결과를 얻을 수 있다.

향후연구에서는 EAP-MD5이외의 EAP-TTLS, EAP-AKA, LEAP등의 효율성 향상 및 실험등의 연구를 통해 실세계에 적용 가능한 시스템 개발이 필요할 것이다.

참 고 문 헌

[1] D. Mitton, M. St.Johns, S. Barkley, D. Nelson, B. Patil, M. Stevens, B. Wolff, "Authentication, Authorization, and Accounting : Protocol Evaluation," RFC 3127 June, 2001.

[2] P. Calhoun, H. Akhtar, J. Arkko, E. Guttman,A. Rubens, "Diameter Base Protocol," RFC3588 September, 2003.

[3] Pat R. Calhoun, Tony Johansson, Charles E. Perkins, draft-ietf-aaa-diameter-mobileip-14.txt "Diameter Mobile IP Application," April, 2003.

[4] P. Calhoun, W. Bulley, S. Farrel, "Diameter CMS Security Application," draft-ietf-aaa-diameter-cms-sec-04.txt, IETF work in progress, March, 2002.

[5] P. Calhoun, W. Bulley, A. Rubens, J. Haag, "Diameter NASREQ Application," draft-ietf-aaa-diameter-nasreq-12.txt IETF work in progress June, 2003.

[6] C. Perkins et al. "AAA for IPv6 Network Access," draft-perkins-aaav6-06.txt May, 2003.

[7] L. Blunk, "PPP Extensible Authentication Protocol," IETF RFC 2284, Mar,. 1998.

[8] P. Eronen, Ed, T. Hiller, G. Zorn "Diameter Extensible Authentication Protocol (EAP) Application," draft-ietf-aaa-eap-02.txt June, 30, 2003.

[9] Wei Dei, Crypto++ 5.1 Benchmark http://www.eskimo.com/~weidai/benchmarks.html

[10] 김현곤, "안전한 이동 인터넷을 위한 AAA 서버 기술 개발 및 IMT-2000 시스템 적용을 위한 정보보호 알고리즘 연구," *한국전자통신연구원 보고서*, 정보통신부, 2002

[11] A, Hess; G.Schafer, "Performance Evaluation of AAA," In Proc of 2ND Polish-German Teletraffic Symposium Poland September, 2002.

[12] C. Rigney, A. Rubens, W. Simpson, S. Willens, "Remote Authentication Dial in User Service (RADIUS)," RFC 2865, June, 2000.

[13] P. Calhoun, C. Perkins, "Diameter Mobile IPv4 Application," IETF work in progress, 2002.

[14] P. R. Calhoun, "Diameter Base Protocol," IETF Internet-Draft, draft-ietf-aaa-diameter-08.txt, work in progress, Nov., 2001.

[15] D. Nessett, "Serial Authentication Using EAP-TLS and EAP-MD5," IEEE, 802.11-01/400r22, July, 2001.

[16] Diameter, http://www.linkionary.com/d/diameter.html

[17] Christopher Metz, "AAA PROTOCOLS : Authentication, Authorization, and Accounting for the Internet," Cisco Systems, http://www.computer.org/internet/v3n6/w6onwire.htm

[18] Diameter extends remote authentication, http://www.nwfusion.com/news/tech/0131tech.html#diagram

[19] Eva Gustafsson, Annika Jonsson, Charles E. Perkins, "Mobile IPv4 Reg. Reg," draft-ietf-Mobileip-reg-tunnel-06.txt, March, 2002.

[20] D.B Johnson "Mobility Support in IPv6" Internet Draft, draft-ietf-mobileip-ipv6-I6.txt, in http://www.letf.org.march, 2002.

[21] C.E. Perkins and David B.Johnson. "mobility support in IPv6," in ACM Mobicom '96, November, 1996.

[22] 정윤수, 이지인, 김한섭, 백승호, 조영복, 김형도, 이상호, "AAAv6에서의 사용자 인증 성능 분석," *한국전자통신연구원 보고서*, 정보통신부, 2004.

정 윤 수

e-mail : bukmunro@netsec.cbnu.ac.kr
1998년 청주대학교(이학사)
2000년 충북대학교 대학원 전자계산학과 (이학석사)
2003년~현재 충북대학교 이공대학 전자계산학과 재학
관심분야 : 암호이론, 정보보호, Network Security, 이동통신보안, 전자상거래보안

우 성 희

e-mail : shwoo@cjnc.ac.kr
1990년 청주대학교 공학사
1993년 충북대학교 이학석사 전자계산학 전공
1999년 충북대학교 이학박사 전자계산학 전공
1995년 청주과학대학 컴퓨터과학과 부교수
관심분야 : Protocol Engineering, Data Communication, Computer network, Network Security

이 상 호

e-mail : shlee@chungbuk.ac.kr
1976년 숭실대학교 전자계산학과
1981년 숭실대학교 전자계산학과(MS)
1989년 숭실대학교 전자계산학과(PHD)
1976년~1979년 한국전력 전자계산소
1981년~현재 충북대학교 전기전자컴퓨터 공학부 교수
관심분야 : Protocol Engineering, Network Security, Network Management, Network Architecture