응답시간 단축을 위한 분산 OCSP 인증서 검증 모델

정회원 최 승 권*, 장 윤 식**, 지 홍 일*, 신 승 수***, 조 용 환*

Distributed OCSP Certificate Verification Model for Reducing Response Time

Seung kwon Choi*, Yoon sik Jang**, Hong il Ji*,
Seung soo Shin***, Yong hwan Cho* ***Regular Members***

요 약

무선 PKI에서 OCSP기법은 인증서 폐지·효력 정지 상태 파악을 실시간으로 정확하게 할 수 있는 특성이 있다. 그러나 많은 클라이언트들이 OCSP서버에 인증에 대한 서비스를 요청할 경우 OCSP서버의 부하는 증가하게 되고, 많은 갱신 정보들이 집중화될 때도 OCSP서버는 많은 부하를 갖게 된다. 이에 분산 OCSP서버 기법을 무선 PKI에 적용함으로서 빠른 인증서 검증과 OCSP서버로의 트래픽 집중을 막고, 중앙 집중적인 구조의 많은 제약들을 분산된 OCSP서버로 해결하고자 한다. 시뮬레이션 실험 결과 분산 OCSP를 사용한 경우, OCSP 서버의 수가 늘어날 수록 서버의 부하감소와 인증서 검증 요청 평균 응답시간이 단축됨을 확인할 수 있었다. 또한 복수의 OCSP 서버를 제공하여 자원의 분산화가 가능하며 부수적인 효과로 장애에 대한 대비로 이중화 효과를 얻을 수 있었다.

Key Words : OCSP, PKI, WPKI, certificate, verification.

ABSTRACT

OCSP has specific characters which can suspend, close, and correct in real time. But, as more clients use the OCSP server verification, more updated information is needed, which can lead to jamming in the OCSP server. To apply this technique of Distributed OCSP server so as to reduce the certificate verification OCSP from jamming. Also, the Distributed OCSP server will solve the problems of the intensive central structure. Simulation results show that the average reply time of certificate verification request and server load are reduced in the case using distributed OCSP. In addition to this advantage, resource distribution and fault tolerance are acquired because of multiple OCSP.

Ⅰ. 서 론

무선 PKI(WPKI: Wireless Public Key Infra-structure)는 기존의 PKI(Public Key Infra-structure) [3]에 근간을 두면서, 무선 단말기에 탑재되는 인증서와 관련 프로토콜 등을 간결하고 단순한 형태의 규격으로 제공함으로써 무선 인터넷 구간에서도 전자서명 및 암호화를 수행할 수 있는 기반이 된다 [1]. PKI 구축을 위하여 사용되는 기술 중 인증서 검증 기법은 실제 전자상거래에서 그 거래의 유효성에 관한 것이므로 가장 신중하게 처리되어야 한다. 이를 위하여 X.509에서는 인증서 효력정지 및

* 충북대학교 전기전자컴퓨터공학부 (skchoi1972@hotmail.com), ** SK 텔레콤
*** 동명정보대학교 정보보호학과
논문번호 : KICS2004-07-099, 접수일자 : 2004년 7월 15일

폐지목록(CRL:Certificate Revocation List)과 CRL 분배점 사용을 제시하고 있다[2].

그리고 IETF(Internet Engineering Task Force)는 온라인상에서 즉시 인증서 검증이 가능하도록 하는 온라인 상태 검증 프로토콜(OCSP:Online Certificate Status Protocol)을 제안하였다. 이 방식은 중앙 집중적인 서버를 이용한다. OCSP는 인증서 폐지·효력정지 상태 파악을 실시간으로 정확하게 할 수 있다는 특성이 있지만, 많은 클라이언트들이 OCSP서버에 인증 서비스를 요청할 경우 OCSP서버의 부하는 증가하게 되고, 많은 CRL정보들이 갱신될 때도 OCSP서버는 많은 부하를 갖게 된다.

이에 본 논문에서는 무선 PKI 기반에 적합한 인증서 검증 기법에 대해서 고찰하고 OCSP서버 부하의 증가와 응답시간 지연 문제를 해결하기 위해 분산 OCSP 기법에서의 CRL정보 획득 방법과 장애 발생 시의 해결 방법 및 클라이언트의 OCSP 인증서 검증 요청 및 응답에 대해 알아본다. 그리고 네트워크 시뮬레이션 프로그램인 NSII를 이용하여 사용자가 1,000대일 때로 가정하여 분산된 OCSP서버의 대수에 따라 변하는 서버 부하율의 변화와 인증서 상태 검증 요청에 대한 응답시간의 변화를 측정하고 분석하고자 한다.

Ⅱ. 무선 PKI 기반의 인증서 검증

유선 인터넷 환경과 마찬가지로 무선 인터넷이 안전한 서비스를 제공하기 위해서는 인증, 접근 통제, 기밀성, 무결성, 부인봉쇄와 같은 보안 서비스를 제공해야 한다. 이를 위한 인증 서비스의 기반기술로서 무선 PKI 가 현재 가장 주목받고 있다. 무선 PKI란 기존의 유선 PKI의 구성요소를 그대로 이용한다. 무선환경에 적합하도록 기능을 최소한 변화시킨 것이 무선 PKI이다.

2.1 무선 PKI 구성요소

무선 PKI를 구성하는 요소는 그림 1과 같으며, 그 구성요소들은 다음과 같다.

- 인증기관(CA:Certification Authority)[3]
- 등록기관(RA:Registration Authority)
- 디렉토리(Directory)[4] · 사용자(End Entity)
- 인증서(Certificate)[5]
- 인증서 효력정지 및 폐지목록[6]

위에서 설명한 중추적인 구성 요소 외에 무선 인터넷 사용자를 대신하여 인증서 상태 정보와 함께 인증 경로에 대한 검증 정보들을 제공하는 OCSP (Online Certificate Status Protocol)나, 무선 단말기의 계산 능력 저하로 인한 단점을 보완하기 위하여 사용되는 보안 모듈 등이 무선 인터넷상에서 PKI를 구성하기 위한 부수적인 구성 요소이다. 더불어 무선 PKI는 무선 인터넷상에서 구성되어야 하므로, WAP 방식이나 ME 방식과 같은 무선 인터넷 접속 기술 또한 중요한 구성 요소이다. 각 접속 기술에 따라 PKI를 구성하는 인증서의 형식, 전송 포맷, 서명 알고리즘, 키분배 알고리즘 등이 각 방식에 적합하게 변형되어 사용된다.

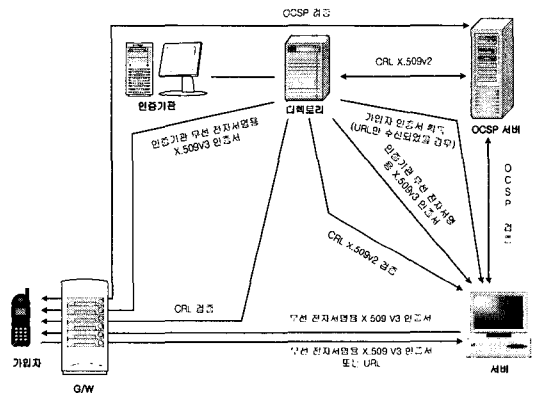


그림 1. 무선 PKI 구성도

2.2 무선 PKI 기반의 인증서 검증

무선 PKI 모델에서 기본적으로 무선용 X.509인증서를 사용하지만, 무선 CA 서버는 단말기의 검증 능력을 고려하여 WTLS인증서를 사용하며, 무선 단말기의 저장 공간 문제를 해소하기 위해 인증서를 발급 받을 경우 인증서의 URL을 이용하기도 한다. 단말기에서 무선용 X.509 서버 인증서의 검증 기법으로는 CRL이나 OCSP를 사용하도록 한다. 또한 무선에서는 최신의 CRL만을 모아놓은 Delta CRL을 옵션으로 사용한다. 단말기에서 RSA를 사용하여 키 생성이 용이하지 않을 경우를 고려하여 ECDSA를 사용하여 키를 생성할 수 있는 기능이 추가로 제공되며, 서명 알고리즘으로는 RSA, ECDSA가 사용되고 키분배용 알고리즘으로는 RSA, ECDH 등이 있다.

2.2.1 CRL을 이용한 인증서 검증

무선 인터넷 단말기는 제한된 컴퓨팅 파워와 메모리 용량을 가지고 있으므로 인증서 검증에 대한

부하를 줄이기 위한 여러 가지 방법을 적용하고 있다. CRL은 FRC2459에서 정의되었으며 인증서의 사용 취소 행위 발생 시 취소된 인증서에 대한 정보를 관리함으로써 PKI의 안정성 및 효율성을 고취시킨다. 일반적으로 CRL은 유효기간이 지나지 않았으나 취소된 인증서들의 리스트를 포함하며 X.509v2 CRL 양식 및 내용은 표 1과 같다[7].

표 1에서와 같이 CRL은 발행시간과 그 다음 발행시간 사이에서만 유효하다. 이러한 설정은 온라인 뿐 아니라 오프라인 상태에서도 CRL을 다운로드받아 사용하기 위해 도입되었으며 이로 인해 해당 유효기간 동안에 폐지된 인증서 역시, 유효한 인증서로 검증될 수밖에 없다. 현재 국내의 공인 인증기관 4사 역시 CRL을 기본적인 인증서 검증 방식으로 사용하고 있으며, CRL의 크기를 줄이기 위해 CRL 분배점(Distribution Points)라는 분할된 CRL을 사용하고 있다. 하지만 여전히 인증서 상태의 즉시성을 보장하기는 어렵다.

표 1. 인증서 폐지 목록 구성

필 드 명	설 명
Version	현재 버전은 2이다.
Signature	CRL의 무결성과 인증을 위해 서명된다.
Issuer	CRL 발행자의 이름이 기입된다.
This Update	CRL의 발행 시간
Next Update	CRL의 다음 발행시간
Revoked Certificates User Certificates Revocation Date CRL Entry Extensions	폐지된 인증서 목록과 함께 폐지일시, 폐지 사유가 포함된다.
Extensions	CRL 확장필드가 포함된다.

2.2.2 OCSP를 이용한 인증서 검증

주기적으로 CRL을 체크하는 것을 보완함으로써 인증서의 폐지 상태에 관하여 적시의 정보를 얻어내는 요구가 점차 증가하고 있다. 예를 들면, 높은 가치의 자금거래나 금융거래에서는 실시간으로 인증서 폐기상태 정보를 검증해 볼 수 있어야 한다. 따라서 OCSP는 가능한 한 CRL보다 적시의 폐기 정보를 제공할 수 있도록 한다.

기본적인 OCSP 인증 구조는 그림 2와 같이 서버·클라이언트 구조로 구성되며, OCSP클라이언트는 OCSP응답자에게 인증서에 대한 상태요구를 한다. 그리고 OCSP클라이언트는 OCSP응답자로부터 응답이 올 때까지 요청한 인증서의 승인을 대기 시킨다. OCSP서버는 요청된 인증서의 상태를 유효·폐지·알 수 없음의 3가지 형태로 응답한다. OCSP에 관련된 표준에서는 인증서의 상태를 체크하는 어플리케이션과 상태정보를 제공하는 서버와의 주고받는 데이터에 한해서만 명시되어있다. 따라서 현재의 인증서 상태를 CA에서 OCSP 서버로 전달하기 위한 적절한 표준이 시급한 형편이다.

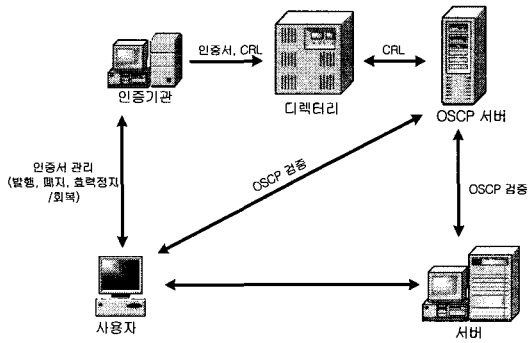


그림 2. OCSP를 이용한 인증서 검증 모델

OCSP(PKIX Online Certificate Status Protocol)는 응용 프로그램이 검증하고자 하는 하나 또는 그 이상의 인증서의 상태를 조회할 수 있도록 한다. CRL보다 인증서의 상태 정보를 보다 실시간으로 얻을 수 있다. 사용자가 OCSP서버에게 인증서 상태를 요구하면 서버는 인증서의 상태를 응답하는 구조로 되어 있다. IETF의 RFC 2560은 인증서 상태를 체크하는 응용 프로그램과 상태 정보를 제공하는 서버 상에서 오가는 데이터의 구조를 정의하였다[7].

OCSP를 이용한 온라인 상태 검증에 관한 연구가 활발히 진행되고 있다. 현재 활발하게 추진 중인 무선 PKI에서는 OCSP 인증서 검증 방식을 CRL 검증 방식과 함께 선택적으로 사용하도록 하고 있으며, 각 공인 인증기관에서는 이미 OCSP를 도입하였거나 추진 중에 있다. 하지만, OCSP는 그 특성상 중앙 집중적인 관리가 되어야 하며, 상용화된 S/W가 적어 도입하기가 어렵다. 또한 국내의 경우 공인 증기관간의 기술적, 정책적인 이해관계에 의해 중앙 집중적으로 통합하여 관리되기가 어려운 단점을 지닌다. 이러한 점은 인증기관의 수가 늘어나면서 더욱 심화될 것이며, 특히 국제적인 상호연동을 위해

서는 표준화된 인증서 검증방식이 꼭 선결되어야 한다.

Ⅲ. 분산 OCSP 모델

3.1 분산 OCSP서버

OCSP 기법은 기존의 CRL 기법과 비교해서 실시간 온라인 처리라는 점에서 상당히 효과가 있는 방법이다. 그러나 OCSP서버에 한꺼번에 많은 OCSP클라이언트들이 OCSP서버에 부담을 줄만큼의 많은 량의 인증서 검증을 요청한다면 OCSP서버는 엄청난 트래픽 부하를 가지게 될 것이다. 그것은 최근에 무선 인터넷 사용자가 급격히 증가하고 있고, 무선 환경에서의 인증서 검증 요구가 빈번해짐에 따라 OCSP서버의 부담이 가중되고 있다. 이는 OCSP서버의 트래픽 증가로 인한 인증서 상태 확인 요청 및 응답시간의 지연을 초래한다.

그림 3은 OCSP서버의 집중화 현상을 나타내고 있다. 하나의 OCSP서버에 n개의 OCSP클라이언트들이 접속해 OCSP서버에 인증서 상태 확인을 요청할 때 OCSP서버에 트래픽 집중이 일어나는 것을 보여주고 있다. 많은 양의 서비스 요청에 의해서 OCSP서버에 부담을 가하게 되고 그로 인해 OCSP서버의 성능이 저하된다.

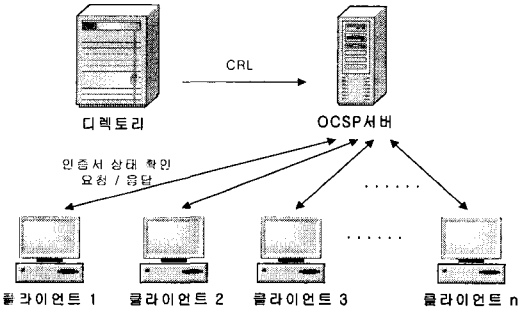


그림 3. OCSP서버 집중화 현상

이에 하나의 중앙 집중적인 OCSP서버의 부담을 줄이고, 동시에 인증서 상태 확인 요청이 쇄도할 경우 효과적으로 대처하기 위해 분산 OCSP서버 기법을 사용하고자 한다. 이 분산 OCSP서버는 CA에서 관리를 하게되고, 각 OCSP서버에 전달되어지는 CRL정보는 동일한 디렉토리를 이용하여 각각의 OCSP서버에 있는 CRL정보가 하나의 정보를 항상 유지할 수 있도록 해야 한다. 즉 각각의 OCSP서버의 CRL정보는 모두 같아야 한다.

그림 4는 분산 OCSP서버에 대해서 설명하고 있다. OCSP서버를 여러 대 설치함으로써 한 대일 때의 OCSP서버의 트래픽 부하를 여러 대의 OCSP서버로 분산시킨다.

OCSP서버는 사용자가 원하는 공인인증서 상태 조회 요청이 있을 경우 해당 공인인증서의 상태 정보를 사용자에게 응답하여 준다. OCSP서버는 해당 공인인증서의 상태 정보를 조회하기 위해 CA에서 제공되는 최신의 효력정지 및 폐지 정보를 획득·관리하여야 한다.

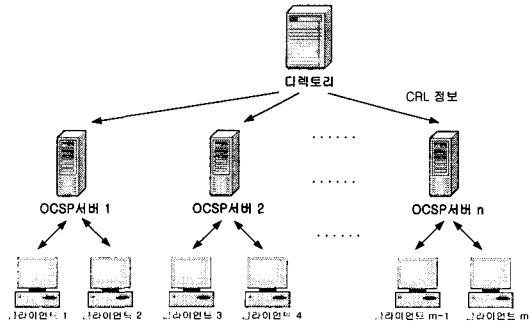


그림 4. 분산 OCSP서버 구성도

3.1.1 분산 OCSP 모델 고려사항

분산 OCSP서버를 구축하기 위해서 몇 가지 고려사항이 있다. 첫 번째, 모든 OCSP서버는 인증서 저장소로부터 사용자의 인증서 검증을 위한 CRL을 일정시간 주기적으로 배포 받는다. 두 번째, 모든 OCSP서버가 클라이언트에게 제공하는 CRL정보는 CA가 제공하는 최신 공인인증서 상태 정보가 모두 반영되어 있어야 한다. 세 번째, 모든 OCSP서버의 인증서 및 CRL정보는 같아야 한다. 네 번째, 디렉토리서버와 OCSP서버간 핸드쉐이크(Handshake) 과정 중에 인증서는 X.509v2 CRL 인증서를 사용한다. 다섯 번째, 모든 OCSP서버에 최신정보를 전달할 때 속도적인 측면을 고려해야 한다. 여섯 번째 디렉토리에서 각 OCSP서버로 최신 CRL정보를 전달할 때 정보의 보안을 유지해야 한다. 일곱 번째, 디렉토리와 각 OCSP서버 사이에 전달되는 신호는 단순해야 한다. 여덟 번째, OCSP서버가 CA서버에 접근하는 경우 CA서버는 OCSP서버에 대한 접근통제 기능을 가져야 한다.

3.1.2 분산 OCSP서버의 CRL정보 획득

서버가 공인인증서의 상태를 제공하기 위해서 CRL정보를 획득·관리하여야 한다. 이를 위해서

OCSP서버는 최신의 공인인증서 효력정지 및 폐지 정보를 획득해야 한다. 디렉토리는 각 분산된 OCSP서버들에게 최신의 갱신 정보들을 주기적으로 전송한다. 이때 디렉토리는 OCSP서버에 정보를 전달할 때 정보의 비밀성을 유지하기 위해서 디렉토리와 각 OCSP서버간에 세션키를 이용해서 암호화한 후에 각 OCSP서버에 전달하게 된다.

Handshake과정은 크게 Full Handshake, Abbreviated Handshake 등으로 구분할 수 있다. 이 가운데 Full Handshake는 새로운 세션을 시작할 때 사용되며, Abbreviated Handshake는 기존의 세션을 재개해서 다시 이용할 경우에 사용된다. Full Handshake 과정은 그림 5와 같다.

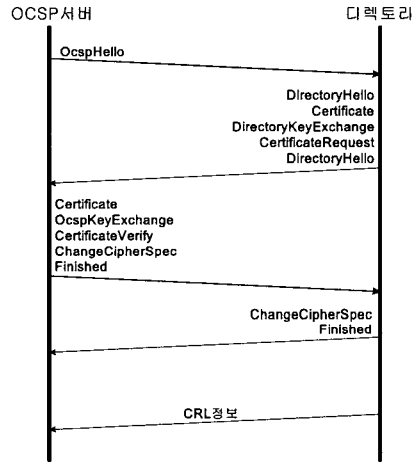


그림 5. Full Handshake

OCSP서버는 OcspHello 메시지를 전송함으로써 서버에게 연결을 요청한다. 이 때 OCSP서버가 사용할 수 있는 관용 알고리즘의 목록, 공개키 알고리즘의 목록, 압축 방법들의 목록들을 전송한다. OcspHello 메시지를 수신한 디렉토리는 이에 대한 응답으로 DirectoryHello 메시지를 전송한다. 이 때 디렉토리는 OCSP서버가 전송한 암호 매개변수들의 목록에서 세션에서 사용할 것을 결정하여 전송하며, 디렉토리 인증을 위해서 디렉토리의 인증서를 전송하고 OCSP서버 인증을 위해서 OCSP서버 인증서를 요청한다. 이 과정을 통해서 서로를 인증하고 필요한 암호 매개변수들을 생성한 OCSP서버와 디렉토리는 Finished 메시지를 보내서 Handshake 과정을 종료하고 실제 CRL정보를 교환한다. Change cipher spec은 하나의 메시지로 구성되며, 이 메시지가 전송된 이후의 메시지는 새로운 보안 파라미터에 의해서 암호화되어 전송됨을 알리는 역할을 한다. Handshake 과정에서 교환되는 정보는 표 3과 같다.

표 3. Handshake 과정에서 교환되는 정보

정 보	설 명
Session Identifier	서버가 세션을 식별하는데 사용하는 임의의 수
Protocol Version	프로토콜 버전
Peer Certificate	서버 및 클라이언트 인증서
Compression Method	데이터 암호화에 앞서 사용되는 압축 방법
Cipher Spec	사용되는 관용 암호 알고리즘 및 MAC 알고리즘
Master Secret	클라이언트와 서버에 의해서 공유되는 20바이트의 비밀 정보
Sequence Number Mode	현재 세션에 사용되는 일련번호 사용 방법(off, implicit, explicit)
Key Refresh	보안 서비스 제공에 사용되는 정보(암호키, MAC 정보, IV)등의 교체 주기
Is Resumable	현재 세션이 새로운 세션을 시작하는데 사용될 수 있는지 여부를 나타내는 표시자

Abbreviated Handshake에서는 이전 세션 정보를 이용하여 세션을 시작하기 때문에 인증서 교환과 같은 서버와 클라이언트 인증을 위한 정보는 교환되지 않으며 이전 세션에서 사용한 암호 매개변수로부터 새로운 세션에서 사용될 매개변수들을 생성한다.

디렉토리는 CRL정보를 압축하고 해쉬 및 암호화를 수행하여 전송하고, OCSP서버는 수신한 CRL정보를 복호화 및 검사하는 역할을 한다. 이 때 데이터 압축, 해쉬 계산, 암호화 등에 사용되는 매개변수들은 Handshake 과정에서 결정된다.

그림 6은 분산 OCSP서버의 CRL정보 송수신 과정을 나타낸 것이다. 하나의 디렉토리 서버를 이용해서 각각의 OCSP서버는 CRL정보를 수신함으로서 동일한 CRL정보를 유지하게 된다. 일정 시간 간격으로 디렉토리에서 CRL정보를 전송하게 되면 OCSP서버는 CRL정보를 획득하고 관리하게 된다. OCSP서버에서 디렉토리로부터 받은 CRL에 대한 응답 메시지를 보내지 않으므로 OCSP서버의 부담을 약간이나마 줄여줄 수 있다. 즉 디렉토리는 각 OCSP서버가 CRL정보를 잘 받았는지에 대해서는 책임을 지지 않는다.

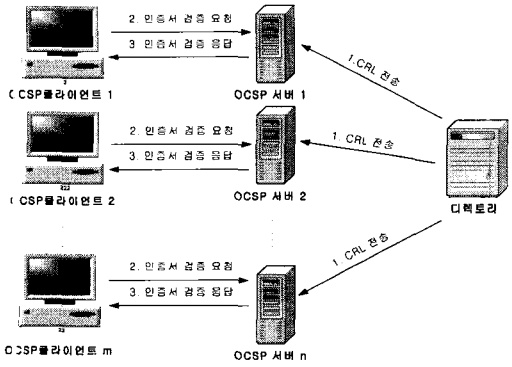


그림 6. 분산 OCSP서버 CRL정보 송수신 과정

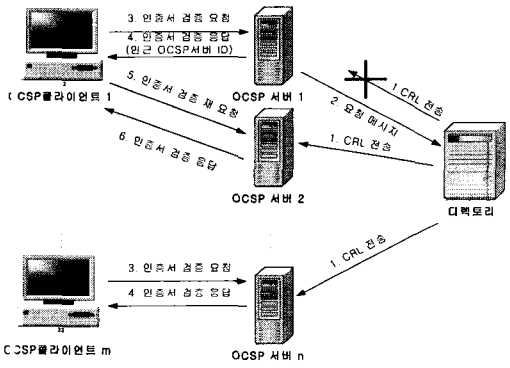


그림 7. 디렉토리로부터 CRL 전송이 없을 때

그림 7과 같이 디렉토리로부터 일정 시간이 지났음에도 CRL 전송이 없을 때에는 OCSP서버가 CRL 요청 메시지를 보낸다. CRL 요청 메시지를 보냈음에도 디렉토리로부터 일정 시간동안 CRL이 전송되지 않을 때는 OCSP서버는 자기 자신을 불능의 상태로 만들고 인근에 있는 다른 분산 OCSP서버의 ID를 OCSP클라이언트에게 보내서 재 인증서 검증을 요청하도록 한다. 이렇게 한 이후에 OCSP 서버는 계속하여 디렉토리에 CRL정보 요청 메시지를 보내서 정상상태가 되도록 한다.

3.2 분산 OCSP 모델의 인증서 검증 서비스

분산 OCSP서버 기법은 IETF PKIXWG에서 2000년 11월 드래프트 형태로 발표한 OCSPv2가 제공하는 서비스를 따르고 있다. OCSPv2는 클라이언트가 온라인 상에서 특정 인증서의 상태를 OCSP서버에게 문의하거나 그에 대한 인증 경로를 획득 가능하게 하고 획득한 인증경로의 유효성에 대해 검증할 수 있는 프로토콜로 제안되었다. OCSPv2가 포함하고 있는 서비스로는 온라인 취소 상태 확인 서비스(ORS), 대리 인증 경로 검증 서비스(DPV), 대리 인증 경로 발견 서비스(DPD)등이 있다.

그림 8은 인증서 상태확인 모듈을 OCSP서버가 대행하는 것을 나타낸다. OCSP는 위임받은 서버에게 인증서 상태확인을 의뢰한다. 클라이언트는 실시간에 가까운 인증서 폐지 상태 정보를 OCSP 서버를 통해서 실시간으로 얻을 수 있다. 인증서 검증은 인증 경로상의 모든 인증서에 대하여 수행되며, 인증서 내에 존재하는 서명 검증, 폐지 상태, 유효기간 검증, 정책 처리 · 검증 등으로 구성된다. 이를 3부분으로 나누면 인증서 경로 구축, 인증서 경로 검증, 인증서 상태 확인 등으로 구분된다.

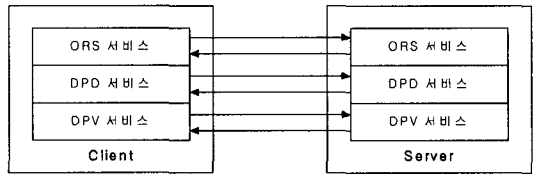


그림 8. OCSP 서버 · 클라이언트 구조

Ⅳ. 실험 및 결과분석

본 장에서는 무선 PKI에서의 분산 OCSP서버 모델에 대해 실험을 통해 본 모델에 대한 실험 결과와 가능성을 알아본다. 네트워크 시뮬레이션 프로그램인 NSⅡ를 이용하여 OCSP서버의 대수에 따라 변하는 서버의 부하율과 인증서 상태 검증 요청에 대한 응답시간의 변화를 알아본다.

4.1 실험 환경

앞서 분산된 OCSP서버들에게 디렉토리의 CRL 정보를 안전하게 전달하는 모델을 설명하였다. 분산 OCSP 기법에 대한 실험을 하기 위해 표 4와 같은 실험환경과 조건들을 설정하였다.

네트워크의 기본 환경은 기존의 기본 환경을 그대로 적용하였다. 한국전산인증에서는 1,000개당 하나의 CRL파일을 할당하고 있다. 그리고 빈 CRL은 55kb의 크기를 가지고 있으며, 인증서 크기가 일반적으로 1~3kb인데 본 논문에서는 한 개당 3kb의 크기를 할당하였다. 그리고 공개키 암호/복호 처리 속도를 1.6Mbyte/sec로 하였고, 인증서 검증 시간을 32ms로 하였다. 이를 기반으로 OCSP서버가 1대일 경우와 2대일 경우 또 그 이상 5대까지의 경우들을 실험하여 각각의 성능을 측정하였다.

표 4. 실험 환경

Host (User)	1,000대
OCSP 서버	1 ~ 5대
암호화 알고리즘	DES
해쉬 알고리즘	SHA1
서명 알고리즘	ECDSA
무선 대역폭	2Mbps
유선 대역폭	10Mbps
Empty CRL 크기	55kb
인증서 크기	3kb
인증서갱신요청시간	30sec
평균서비스요청시간	10sec

4.2 실험 결과 및 분석

그림 9는 OCSP서버가 클라이언트의 인증서 상태 검증 요청에 대하여 1대일 때와 2대일 때 그 이상일 때 각각의 경우에 OCSP서버 CPU의 평균 부하율을 측정하여 그래프로 나타낸 것이다. 그림 19는 OCSP서버의 대수에 따라 인증서 상태 검증 서비스를 요청했을 때 서버의 성능을 나타낸 것이다. OCSP서버가 한 대일 경우는 1000대의 사용자가 요청하기 때문에 많은 부하가 있음을 보여주고 있다. 평균 부하율은 약 89.12%의 높은 부하율을 보이고 있다. 그러나 2대일 경우와 3대일 경우는 각각 35.4%와 28.6%로 나타나고 있다. 5대일 경우에는 평균 부하율은 23.74%을 보인다.

그림 10은 인증서 상태 검증 서비스 요청에 대한 응답시간을 보여주고 있다. 이 응답시간에 관한 결과 또한 서버를 분산했을 경우가 한 대일 경우보다 빠른 응답시간을 보여준다. 한 대일 때의 응답시간은 평균 1.22초이다. 그러나 2대일 경우와 3대일 경우는 0.845초와 0.824초로 거의 차이를 보이지 않고 있다. 4대일 때와 5대일 때도 비슷한 결과가 나타났다. 1대일 때와 2대일 대를 비교하면 응답시간의 차이가 어느 정도 보여지나 2대 이상에서의 응답시간의 비교는 무의미할 정도로 미미한 차이를 가진다.

V. 결 론

본 논문은 무선 PKI에서 기존의 하나의 OCSP서버에서 인증서 상태 검증 서비스를 할 때 많은 클라이언트들이 OCSP서버에 서비스를 요청할 때의 OCSP서버에 가해지는 부하율의 증가와 응답시간의 지연에 대해서 분석을 하고 이에 대한 해결 방안으로 분산 OCSP서버를 활용하였다. 하나의 OCSP서버가 담당하던 인증서 유효성 검사를 몇 대의 OCSP서버로 분산시키는 방법을 통해서 OCSP서버의 대수가 1대일 때, 2대일 때, 그 이상일 때에 대해서 실험하였다. OCSP서버의 수가 늘어날수록 서버의 부하 감소와 인증서 검증 요청 평균 응답시간이 단축됨을 증명하였다. 그리고 OCSP서버의 수가 2대일 때 비용효율 면에서 가장 경제적인 것을 알 수 있었다. 따라서 무선 인터넷에서 전자상거래의 수요에 따라 OCSP서버의 대수를 적절히 유지해나가는 것이 효율적일 것이다. 또한 복수의 OCSP서버를 제공하여 자원의 분산화가 가능하며, 부수적인 효과로 장애에 대한 대비로 이중화 효과를 얻을 수 있다.

앞으로 사용자의 증가에 따른 OCSP서버의 최적 대수를 구하는 연구를 계속 해나가야 하며, 최신 CRL정보를 전송하기 위해 사용되는 Handshake과정이 CRL 송수신간 큰 오버헤드로서 작용하지 않도록 더욱 간소화하고 경량화하여 디렉토리와 OCSP 서버 간 정보전송 속도를 높여야 한다.

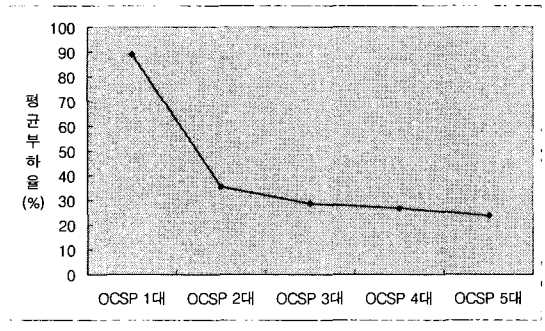


그림 9. OCSP서버 평균 부하율 비교

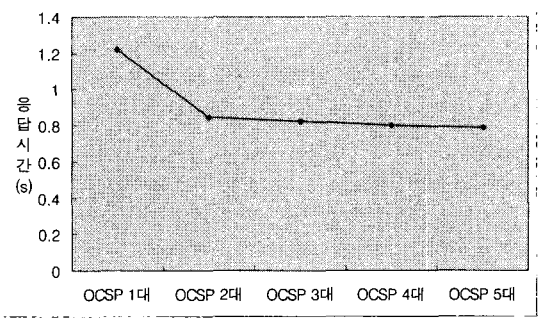


그림 10. 인증서 상태 검증 서비스 요청에 대한 응답시간

참 고 문 헌

[1] 김현회, "WPKI 기반의 무선 공인인증 서비스 개요", 지급결제와 정보기술, 금융결제원, 2003.

[2] 이석래, "무선보안기술동향", 전자서명인증관리센터, 한국정보보호진흥원, 2002.

[3] "전자상거래를 위한 보안 기술 체계 및 요소 기술에 대한 이해", 한국전산원 차세대 서비스부, 1999. 6.

[4] R.L Rivest, A. Shamir and L. Adleman, "A Method for obtaining digital signatures and public-key cryptosystems", ACM, Vol.21. no.2, pp.644-654 Feb. 1978.

[5] Jalal Feghhi, Jalil Feghhi, Peter Williams, "Digital Certificates-Applied Internet Security", Addison Wesley, 1998.

[6] Schneier. B, "Applied Cryptography : Protocols, Algorithms, and Source Code in C", Jone Wiley & Sons, New York, 1996.

[7] 채송화, "CRL 분배 및 온라인 인증서 상태 확인 비교", 전자서명 인증관리 센터, 한국정보보호진흥원, 1999.

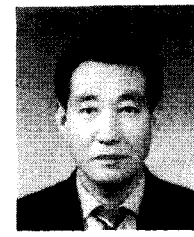
최 승 권 (Seung kwon Choi) 정회원

2001년 8월 충북대학교 컴퓨터공학과 대학원(공학박사)

현재 충북대학교 초빙교수

<관심분야> 멀티미디어 통신, 멀티미디어 콘텐츠

장 윤 식 (Yoon sik Jang) 정회원



1998년 2월 광운대학교 전자공학과 대학원(공학석사)

현재 SK 텔레콤 상무이사

<관심분야> 이동 통신, 모바일 콘텐츠

지 홍 일 (Hong il Ji) 정회원

2002년 2월 충북대학교 컴퓨터공학과 대학원(공학석사)

현재 충북대학교 컴퓨터공학과 대학원(박사과정)

<관심분야> 멀티미디어통신, 네트워크

신 승 수 (Seung soo Shin) 정회원

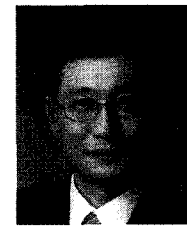
한국통신학회 논문지 제 26권 제 4A호 참조

2004년 8월 충북대학교 컴퓨터공학과 대학원(공학박사)

현재 동명정보대학교 정보보호학과 교수

<관심분야> 무선 PKI, 암호화

조 용 환 (Yong hwan Cho) 정회원



한국통신학회 논문지 제 23권 9호 참조

현재 충북대학교 전기전자컴퓨터공학부 교수

<관심분야> .Net Framework, 멀티미디어통신, 트래픽공학, Mobile PKI, 정보통신정책