# OCSP서버의 지속적인 서비스를 위한 시스템 연구*

신재훈, 최해랑, 신동휘, 원동호, 김승주†
성균관대학교 정보통신공학부 정보보호연구소
e-mail:zmsin@skku.edu

# A Study on System of OCSP server for Services*

Jaehoon Shin, Haelahng Choi, Donghwi Shin, Dongho Won, Seungjoo Kim†
Information Security Group, School of Information Communication Engineering, Sungkyunkwan University

요 약

최근 인터넷의 급속한 발달은 온라인 뱅킹, 인터넷 쇼핑몰 등에서의 실물 경제행위를 온라인상으로 처리할 수 있는 환경을 제공하지만 온라인상의 업무처리는 개인정보유출, 개인정보의 위조 및 변조 등의 문제를 가지고 있다. 사용자가 CA에게서 받은 인증서의 공개키로 전자서명 함으로써 개인정보유출, 정보의 위조 및 변조 등의 문제를 해결한 PKI(Public Key Infrastructure)기반의 인증서 검증시스템이 제안되어 사용되고 있다. 인증서 상태검증 방법에는 CRL(Certificate Revocation List)기반의 검증방식, OCSP(Online Certificate Status Protocol)기반의 검증방식 등이 있다. CRL기반의 인증서 검증방식은 인증서 취소목록을 검색해서 인증서의 유효성 여부를 응답하는 방식으로 시간이 지남에 따라 크기 증가와 오프라인 방식으로 인해서 목록을 다운받는 시간의 부담으로 인해서 OCSP방식이 제안되었다. 하지만 OCSP 방식 역시 서비스의 요청이 집중될 경우 문제가 발생될 수 있다. 그래서 분산된 OCSP를 구축하고 각 서버의 부하의 균형을 유지하기 위해 로드밸런싱 기법을 사용하고 있지만 그 방법 역시 지속적인 서비스 제공이 불가한 문제를 가지고 있다. 본 논문에서는 서비스 요청의 집중으로 인한 시스템 마비나 각 응답서버의 부하가 불균형적임으로써 생길 수 있는 문제를 해결할 수 있는 방법을 제안한다.

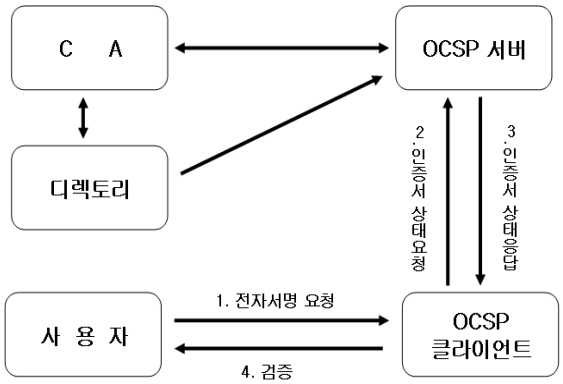
## 1. 서론

인터넷이 보편화되고 누구나 온라인을 통해 오프라인과 동일한 전자적 거래를 할 수 있는 정보사회에서는 안전성과 신뢰성의 확보가 중요하다. 공개키 암호 시스템(Public Key Cryptography)은 전자 상거래 등의 정보 보호를 위한 분야에서 대표적으로 쓰이고 있으며 이를 효율적으로 사용하기 위해 등장한 개념이 공개키 기반구조(PKI : Public Key Infrastructure)이다. 공개키 기반 구조에서 인증서의 유효성 검증 방식에는 CRL(Certificate Revocation List), OCSP(Online Certificate Status Protocol) 등의 방법이 있다.[1] CRL기반의 인증서 검증방식은 인증서 취소목록을 검색해서 인증서의 유효성 여부를 응답하는 방식으로 시간이 지남에 따라 CRL의 크기 증가와 오프라인 방식으로 인해서 목록을 다운받는 시간의 부담, 그리고 실시간 인증이 불가능하다는 단점이 있다. 그런 문제를 해결하고자 제안된 방식이 OCSP방식이다. OCSP방식은 CRL방식의 인증서 검증상태에서 발생하는 문제를 해결하였지만 서비스의 요청이 집중될 경우 서버의 과부하문제가 발생될 수 있다. 그래서 분산된 OCSP를 구축하고 서버부하의 균형을 유지하기 위해 로드밸런싱(Load Balancing) 기법을 사용하고 있지만 시스템의 동작이 마비된다거나 각 응답서버의 부하가 불균형으로 배분될 수 있는 문제가 있다.

본 논문에서는 OCSP방식의 인증서 유효성 검증방식과 분산된 OCSP방식의 인증서 유효성 검증방식, 로드밸런싱 기법과 문제점을 2장에서 기술하고, 과도한 검증 요청으로 서비스 불능 상태가 되거나 응답서버에 부하가 불균형적으로 분배됨으로써 생길 수 있는 문제를 해결할 수 있는 시스템을 3장에서 제안한다. 4장에서는 제안한 시스템의 장점과 단점을 분석하여 결론을 맺는다.

## 2. 관련 연구

### 2.1 OCSP방식의 인증서 유효성 검증방법




(그림 1) OCSP방식의 인증서 검증과정

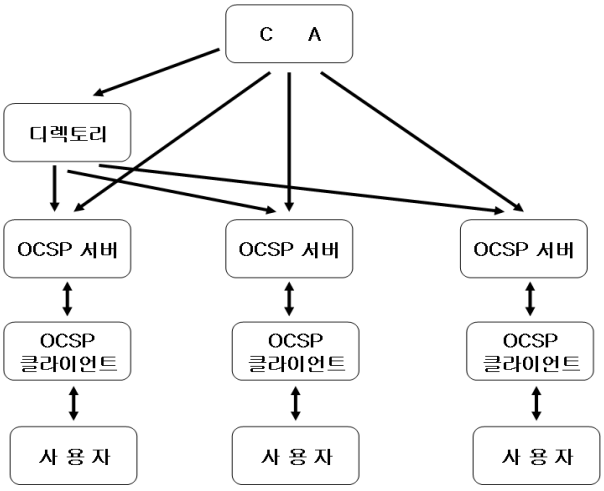
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(IITA-2007-C1090-0701-0028)

† 교신저자, skim@security.re.kr

OCSP는 실시간으로 인증서 상태를 요청하는 OCSP클라이언트와 응답을 하는 OCSP서버로 구성된다.[2] (그림 1)은 OCSP방식의 인증서 상태검증 과정을 나타낸다.

### 2.3 분산된 OCSP서버의 구조

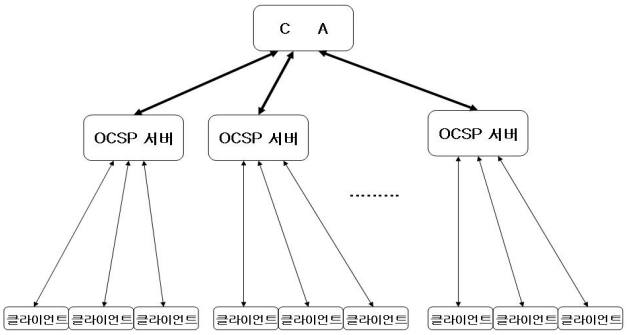
OCSP방법은 기존의 CRL방법에 비해서 CRL의 다운 및 점점 커져가는 CRL의 크기, 그리고 실시간 처리라는 관점에서 보았을 경우에 굉장히 효과적인 방법이다. 그러나 에모든 클라이언트들이 OCSP서버 한곳에 서비스를 요청한다면 OCSP서버는 부담을 가지게 되고 서버 과부하로 인한 OCSP서버의 불능 가능성 역시 커지게 된다. 게다가 최근에는 전자상거래를 이용하는 사용자가 급격히 증가하고 있는 상태에서 단일 OCSP서버의 사용으로 인한 과부하 현상은 더욱 증가될 것이고 이에 따른 OCSP서버의 불능 가능성 역시 더욱 증가될 것이다. 이러한 단일 OCSP서버 방식의 문제점을 해결하기 위해서 분산된 OCSP서버 방식이 제안되었다. (그림 2)[3][4]




(그림 2) 분산 OCSP서버 구조

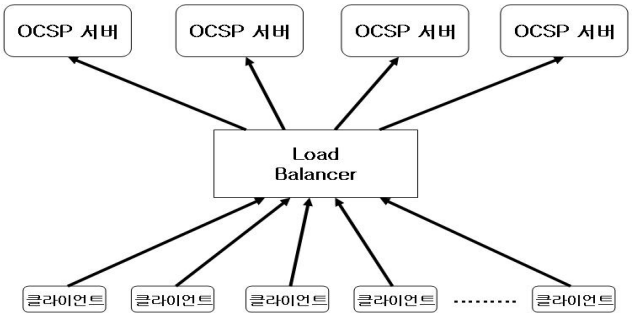
### 2.4 로드밸런싱(Load Balancing) 기법

OCSP서버의 부하를 줄이기 위해 여러 개의 OCSP서버를 두지만 하나의 OCSP서버로 인증이 집중되는 현상을 제어하지 못한다면 분산 OCSP방식은 의미가 없다. 이런 문제를 해결하기 위해 클라이언트와 OCSP서버 간의 연결을 제어하는 로드 밸런싱 기법을 적용한다. 로드 밸런싱 기법은 정적 기법과 적응형 기법으로 나눌 수 있으며 적응형 기법은 다시 집중형 정책과 분산형 정책으로 분류할 수 있다. 집중형 정책은 로드 밸런싱을 위한 정보를 하나의 서버가 모아서 부하의 분배를 결정하는 방식이고, 분산형 정책은 모든 서버가 서로의 부하에 관한 정보를 감시하여, 로드 밸런싱 알고리즘에 따라 높은 부하를 가진 서버의 작업을 낮은 부하의 서버에게 전송시켜 부하를 분배하는 방식이다. 현재 분산 OCSP에 주로 적용되고 있는 로드 밸런싱 기법은 정적 로드 밸런싱 정책(그림 3)와 적응형 기법 중 분산형 정책(그림 4)이다.




(그림 3) 정적 로드 밸런싱 정책을 사용한 분산 OCSP

정적 로드 밸런싱 정책을 사용한 분산 OCSP서버는 클라이언트의 물리적인 위치에 따라 응답서버를 할당하는 방법으로 각 응답서버에게 가해지는 부하가 불균형 적이고 불균형이 심할 경우 OCSP서버가 응답불능의 상황까지 이르는 문제점이 있다.




(그림 4) 집중형 로드 밸런싱 정책을 사용한 분산 OCSP

집중형 로드 밸런싱 정책을 사용한 분산 OCSP서버는 인증요청 메시지가 하나의 로드 밸런서에게 몰리기 때문에 네트워크에 병목현상이 발생하여 전체 시스템의 효율을 저하시키고, 로드 밸런서에 결함이 생길 경우 시스템 전체의 동작이 마비되는 문제점이 있다.

## 3. 제안하는 시스템

제안하는 시스템은 OCSP클라이언트와 서버사이에 서버의 부하를 측정하는 장치를 두고 서버의 부하를 실시간으로 감시하게 한 후 OCSP서버의 부하가 임계치 이상이 되거나 불능상태가 되었을 때 다른 OCSP서버로 연결 시켜 인증서비스를 지속적으로 제공할 수 있는 방법이다. 서버의 부하는 서버에 연결되어 인증서비스를 받고 있는 사용자의 수를 말하며 불능상태란 서버에 요청을 하였을 때 그에 대한 응답이 평소 응답시간의 5배가 걸릴 때를 말한다. 서버부하감지장치는 OCSP서버의 부하를 감지하고 서버의 부하가 정해진 임계치 이상이 되거나 평소의 응답시간보다 확연히 오래 걸림에도 불구하고 서버가 클라이언트에게 응답기능을 수행하지 못할 경우 서버의 상태를 불능이라 판단하며 각 OCSP서버의 수치를 서버부하감지장

치가 받아서 연결 테이블을 만든 후 사용자의 요청이 들어왔을 시 보다 원활한 인증작업이 이루어 질 수 있도록 한다. OCSP서버가 불능상태가 되었을 시 클라이언트의 요청이 불능상태의 OCSP서버로 연결되어 서버의 부하가 지속적으로 가중되는 것을 막는 기능을 할 뿐만 아니라 서버부하감지장치 사이의 부하상태 전달을 통한 연결 테이블을 토대로 클라이언트의 인증요청을 다른 OCSP서버로 연결하게 하는 인증경로에 대한 정보제공을 통해 클라이언트로 하여금 다음에 연결할 OCSP 서버로 인증요청을 할 수 있도록 한다.

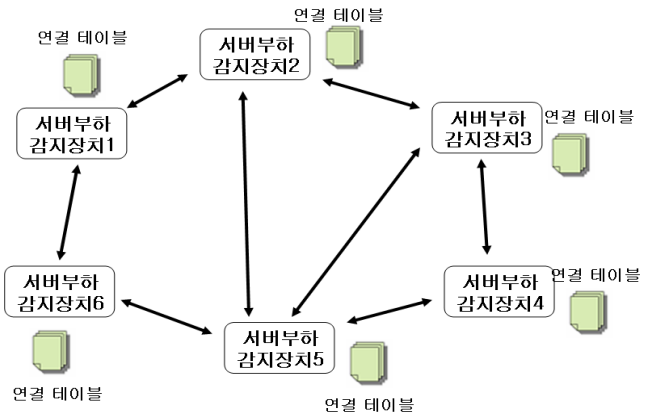
### 3. 1 연결 테이블의 작성

제안하는 시스템에서 연결 테이블은 OCSP이름과 부하수치(OCSP에 연결된 사용자의 수)로 구성된다. OCSP이름은 분산 OCSP서버 환경에서 각각의 서버를 구별하기 위한 서버의 이름이고 부하수치는 특정 OCSP서버에 연결된 사용자 수로 사용자가 많을수록 부하수치는 높다. 초기의 연결테이블은 표 1과 같이 자신의 OCSP서버에 관한 부하수치만 알고 있다.

| OCSP서버 | 부 하 수 치 (사용자 수) |
|---|---|
| OCSP 1 | 15 |
| | |
| | |
| | |

(표 1) 초기 서버부하감지장치 1의 연결 테이블

연결 테이블의 작성은 인접한 서버부하감지장치끼리의 연결 테이블 교환으로 이루어진다. 그림 5와 같이 서버부하감지장치가 인접해 있다. 서버부하감지장치 2는 장치 3, 5와 연결 테이블을 교환했고 장치 1은 장치 6과 연결테이블을 교환했다면 장치 1과 장치 2의 연결 테이블 교환 후 서버부하감지장치1은 직접적으로 인접하지 않아서 알지 못했던 3과 5의 부하수치를 알 수 있다. 이와 같은 과정으로 모든 OCSP서버의 부하수치를 기록한 연결 테이블을 얻을 수 있다.




(그림 5) 서버부하감지장치의 연결 테이블 생성

서버부하감지장치는 연결테이블을 받을 때마다 부하수치를 기준으로 정렬을 한다. 정렬은 합병정렬을 사용하며 서버부하감지장치 1이 장치 2로부터 연결테이블을 받았을 때 정렬되는 과정의 예는 다음과 같다.

| OCSP서버 이 름 | 부하수치 (사용자 수) |
|---|---|
| OCSP서버1 | 15 |
| OCSP서버6 | 43 |
| | |
| | |
| | |

서버부하감지장치1의 연결 테이블

+

| OCSP서버 이 름 | 부하수치 (사용자 수) |
|---|---|
| OCSP서버2 | 12 |
| OCSP서버5 | 26 |
| OCSP서버3 | 56 |
| | |
| | |

서버부하감지장치2로부터 받은 연결테이블

↓

| OCSP서버 이 름 | 부하수치 (사용자 수) |
|---|---|
| OCSP서버2 | 12 |
| OCSP서버1 | 15 |
| OCSP서버5 | 26 |
| OCSP서버6 | 43 |
| OCSP서버3 | 56 |
| | |

정렬 후 서버부하감지장치 1의 연결 테이블

① 서버1과 서버2의 수치 비교 후 낮은 것 선택(서버1)
② 서버2와 서버6의 수치 비교 후 낮은 것 선택(서버2)
③ 서버6과 서버5의 수치 비교 후 낮은 것 선택(서버6)
④ 과정 반복...

위와 같은 과정으로 (표 2)와 같이 모든 OCSP서버의 부하수치에 관한 연결 테이블을 작성한다.

| OCSP서버 | 부 하 수 치 (사용자 수) |
|---|---|
| OCSP 2 | 12 |
| OCSP 1 | 15 |
| OCSP 5 | 26 |
| OCSP 6 | 43 |
| OCSP 3 | 56 |
| OCSP 4 | 69 |
| OCSP 10 | 88 |
| ⋮ | ⋮ |

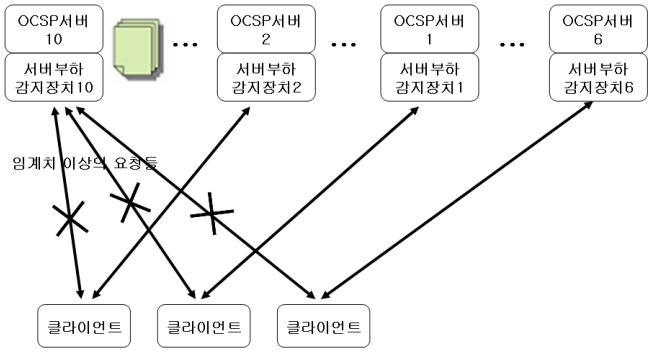
(표 2) 완성된 연결 테이블의 구성

이러한 테이블의 작성은 30초마다 이루어져 서버부하의 변화를 반영한다. 단, 유의할 점은 서버 과부하 상태인 서버부하감지장치는 연결테이블을 사용하고 있기 때문에 테

이블의 갱신에서 제외한다. 나머지 서버부하감지장치사이에서는 처음과 마찬가지로 연결테이블을 초기화 한 후 인접 서버부하감지장치끼리 전달하는 방법을 사용한다.

### 3. 2 제안 시스템의 작동과정

서버부하감지장치의 연결 테이블 작성이 완료되면 임계치 이상의 사용자 요청을 연결 테이블에 따라 다른 OCSP 서버로 연결한다. 연결방법은 부하수치가 낮은 상위 10개의 OCSP서버에게로 돌아가며 연결하는 방법을 통해 서버의 부하가 고루 분배될 수 있도록 한다. 예를 들어 임계치 이상의 부하로 서버부하감지장치가 표 2 같이 연결 테이블을 작성했다면 임계치 이상의 요청 순서대로 첫 번째 요청은 OCSP서버 2로, 두 번째 요청은 OCSP서버 1로, 세 번째 요청은 OCSP서버 6으로 보낸다. 이런 식으로 부하수치가 적은 상위 10개의 서버로 돌아가면서 연결함으로써 부하가 어느 한곳으로 집중되는 것을 방지한다.




(그림 6) 제안 시스템의 작동 과정

서버의 부하가 임계치 이상이 되거나 불능이 되는 서버는 여러 개 있을 수 있고 그 상황에서는 각각의 서버부하감지장치가 가지고 있는 연결테이블을 바탕으로 사용자의 요청을 다른 OCSP서버로 연결한다.

### 3. 3 제안 시스템의 장점

집중형 로드 밸런싱 정책을 사용한 분산 OCSP방식은 모든 클라이언트들의 요청을 하나의 로드 밸런서가 서버에 분배함으로써 역시 인증요청이 집중될 경우 로드 밸런서에 이상이 생기면 시스템 전체의 동작이 마비될 수 있다. 로드 밸런서에 이상이 생기면 로드 밸러서를 복구하는 시간만큼 서비스를 이용할 수 없게 되며 로드 밸런서를 거쳐 가는 모든 사용자가 서비스를 받지 못하게 된다. 정적 로드 밸런싱 정책을 사용한 분산 OCSP방식은 클라이언트들이 요청할 수 있는 서버를 정적으로 고정해 놓았기 때문에 순간적으로 인증요청이 집중될 경우 서버의 부하가 집중되고 심할 경우 특정 OCSP서버에 인증요청을 하도록 고정되어 있는 클라이언트는 인증이 불가능하다. 즉 특정 OCSP서버가 문제가 생기게 되면 그 OCSP서버를 복구하는 시간만큼 서비스를 이용할 수 없게 되며 OCSP에 인증요청을 하도록 고정되어 있는 모든 사용자는 모두 서비스를 받지 못하게 된다.

제안한 시스템은 OCSP서버가 불능이 되어도 서버부하감지장치가 작성하는 연결 테이블을 바탕으로 지속적인 서비스를 가능하게 한다. 연결 테이블은 30초마다 갱신하여 서버부하감지장치가 가지고 있으므로 OCSP서버가 불능이 되어 인증요청이 불가할 때 불필요한 시간소모 없이 바로 클라이언트의 요청을 부하가 적은 OCSP서버로 연결함으로써 지속적인 서비스는 물론 부하의 분배 역시 이루어지도록 하였다. 특정 OCSP서버에 문제가 생기더라도 부하가 적은 다른 OCSP서버로 연결하기 때문에 서비스의 지연은 다른 OCSP서버로 연결하는 시간밖에 걸리지 않으며 서비스를 이용하지 못하는 사람 역시 모든 OCSP서버가 과부하 상태일 때를 제외하고는 발생하지 않는다.

## 4. 결론

본 논문에서는 로드 밸런싱 기법을 적용한 분산 OCSP 서버 환경에서 발생할 수 있는 서비스 불능의 문제를 서버부하감지장치를 이용한 시스템으로 해결하였다.

서버부하감지장치는 OCSP서버의 부하와 응답시간을 실시간으로 감지하여 서버의 불능여부를 판단하고 연결 테이블을 작성하며 임계치 이상의 사용자 요청으로 불능이 된 OCSP서버의 추가적인 요청을 연결 테이블에 따라서 다른 OCSP서버들로 연결하는 기능을 한다. 제안하는 시스템은 기존의 OCSP환경을 그대로 유지, 활용할 수 있으며 서버부하감지장치만 추가함으로써 정적 로드 밸런싱 정책을 사용한 분산 OCSP서버나 집중형 로드 밸런싱 정책을 사용한 분산 OCSP서버에서 발생할 수 있는 인증요청 집중시의 서비스 불능문제를 해결하여 클라이언트가 지속적인 서비스를 받을 수 있도록 고안하였다. 향후에는 서버부하감지장치가 제공할 수 있는 다른 기능들에 대해 연구하여 더욱 활용도를 높일 수 있도록 연구하겠다.

## 참고문헌

[1] R.Housley, W.Ford, T.Polk, D.Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC2459, Jan. 1999

[2] M.Myers et al, "Draft, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol", version 2, IETF, 2002

[3] C.Popescu, B.Crispo, S.Tanenbaum, "A Certificate Revocation Scheme for a Large-Scale Highly Revocation Distributed System", IEEE, 2003

[4] 고훈, 장의진, 신용태, "PKI환경의 OCSP 서버 부하 감소를 위한 OCSP 분산 기법", 정보보호학회 논문지, 제13권 6호, 2003. 12