韓國 컴퓨터情報學會 論文誌
第13卷 第3號, 2008. 5.

2008-13-3-1-10

분산 OCSP에서 인증서 상태 검증을 위한 효율적인 CRI 운영에 관한 연구

김 경 자*, 장 태 무**

A Study on Efficient CRI managing for Certificate Status Validate in Distributed OCSP

Kim Young Ja *, Chang Tae Mu **

요 약

기존 CA(Certificate Authority)에서 인증서의 유효기간 및 클라이언트에서 폐지한 CRI (Certificate Revocation Information)를 관리하는데 있어서 많은 문제점이 있었다. 이를 해결하기 위한 여러 연구들이 행하여졌으나, 클라이언트 측면에서 인증서의 상태 정보를 실시간으로 검증할 수 있기에는 미흡하였다.

본 논문은 이러한 한계를 극복하기 위하여 분산 OCSP(On-line Certificate Status Protocol) 환경에서 새로운 CRI 운영 모델을 제안한다. CRL(Certificate Revocation Lists)을 분할하여 여러 OCSP 서버에게 최신의 CRL을 중복시키고, 그 외 CRL은 각 서버들에게 중복하여 분산시킨다. 이로써 기존의 CA의 병목현상을 줄이고, 전송되는 CRL의 크기도 효과적으로 줄임으로써 클라이언트가 인증서 상태를 실시간으로 검증할 수 있다.

Abstract

The conventional CA(Certificate Authority) has problems in dealing with certificates whose valid time is expired and in managing CRI(Certificate Revocation Information) produced by clients. Many researches are conducted to solve them, but they have limitations in providing real-time verifications of certificates' status for clients.

In this paper, we propose a new CRI management model to address these limitations in distributed OCSP(On-line Certificate Status Protocol) environments. CRL(Certificate Revocation List) is divided into two parts: one part that is recent is replicated over several OCSP servers, the other part is replicated and distributed over servers. Our methods can help to break the bottleneck of CA, and effectively reduce the size of CRL transferred. Therefore, with our methods, clients can verify the state of certificates in real time.

▸ Keyword : 인증기관(Certificate Authority), 인증서(Certificate), 인증서 취소 목록(Certificate Revocated Lists), OCSP(Online Certificate Status Protocol),

---

• 제1저자 : 김경자
• 접수일 : 2008. 4. 4, 심사일 : 2008. 5. 6, 심사완료일 : 2008. 5. 24.
*세종대학교 컴퓨터공학과 시간강사 **동국대학교 컴퓨터공학과 교수

Ⅰ. 서 론

인터넷이 대중화됨에 따라 온라인상에서 정보 노출로 인해 불법적인 위조, 변조 및 신분위장 등의 각종 위협이 많아지고 있다. 이에 인터넷상에서 사용자와 정보 제공자간의 정보보호를 위해 상호간의 인증이 각종 위협을 막을 수 있는 가장 근원적인 요소가 되었다[1].

공개키 기반 구조에서 인증을 위한 기본 절차는 인증 기관에서 인증서를 발행하고, 인증서를 교부 받은 사용자는 정보를 제공 받기 위하여 사용자가 보유하고 있는 인증서의 유효성을 검증 받은 후, 해당 정보를 제공받게 된다. 많은 사용자들이 인증서 검증을 위하여 해당 인증 기관에 요청을 하게 됨으로 인증서 검증을 위한 과정들이 많은 오버헤드가 되고 있다. 이러한 오버헤드를 해결하기 위하여 많은 방법들이 제시되어 왔으나, CRL의 크기가 점점 증가함에 따라 사용자측면에서 빠른 검증 결과를 받아볼 수가 없고, 실시간으로 발생하는 CRI를 갱신하는데 많은 비용이 소모되고 있다. 이에 인증서 검증을 위한 문제점 중에서도 CRL을 좀더 효율적으로 관리할 수 있는 방안들이 제시되고 있다[2][7].

이에 본 논문에서는 인증 기관이 관리해야 하는 CRL을 여러 개로 분산된 OCSP Server에게 중첩되게 분배함으로 CA의 인증서 상태 정보 검증을 위한 작업을 여러 OCSP Server에게 할당하여 인증서 상태 정보의 검증을 위한 병목 현상을 줄이고자 한다. 또한, 여러 대의 분산 OCSP Server를 Front Server가 관리함으로 인증서 상태를 검증하는 데 있어서 CA를 거치지 않고도 빠른 시간 안에 응답을 받아 볼 수 있게 한다. 또한, 여러 분산 OCSP Server에게 CRL을 분산시켜 관리함으로써 단일한 CA의 관리보다는 보안 측면에서의 손상 정도를 줄일 수 있다고 본다.

본 논문의 구성은 효율적인 인증서 상태 검증의 필요성을 1장에서 제시하고, 2장에서는 인증서 상태 검증을 위한 기존 모델들을 비교하였다. 3장은 본 논문의 기본 환경이 되는 OCSP Server를 분산하여 관리하는 분산 OCSP Server 구조와 인증서 상태 검증 과정을 보이고 있다. 4장에서는 CRL을 분할하여 분배하는 제안 모델을 제시하고 있다. 5장은 기존의 OCSP Server들과 제안 모델을 CRL에 관련된 작업량을 비교한다. 마지막으로 6장에서는 결론을 제시하고 향후 분산 OCSP Server가 고려해야 할 방향들을 제시하며 끝을 맺는다.

Ⅱ. 관련 연구

인터넷상의 인증서 사용 증가로 인해 인증서 상태 정보의 검증을 위한 효율적인 여러 방법들이 제시되어왔다[4]. 〈표 1〉는 CRL을 효율적으로 관리하는 기존 여러 기법들을 CRL의 분할 및 분배 여부와 갱신 기간에 대해서 비교하였다.

CRL DP는 CRL의 크기를 줄이기 위한 방법으로 인증서의 일련번호들을 기준으로 다수의 CRL들을 생성하여 여러 공개 저장소에 게시하는 방식으로 Directory Server의 부하를 감소시키고자 하는 기법이다. 즉, 인증서의 폐지 여부를 확인하기 위하여 분배점(DP: Distribution Point)을 두어 해당 폐지 목록 위치를 확인하는 기법이다. Delta CRL기법은 Base CRL에는 CRL 생성 시에 폐지 상태에 있는 인증서 정보를 게시하고, Delta CRL에는 Base CRL 생성 이후에 폐지된 인증서의 정보를 게시한다. Indirect CRL은 CRL 관

표 1. 기존 CRL 관리 기법들
Table 1. a schemes for managing CRL

	CRL DP	Delta CRL	Indirect CRL	Dynamic CRL DP	OCSP	SCVP
발행 기관	CA	CA	CRL 기관	CA	CA	CA
검증 기관	CA	CA	CRL 기관	CA	OCSP Server	SCVP Server
분할 여부	○	○	×	○	×	×
분배 여부	×	×	×	×	×	×
갱신 기간	Periodic	Periodic	Periodic	Dynamic	Periodic	Periodic

리를 위한 인증기관의 부담을 줄이기 위해서 제안된 방식으로 CRL 전문 발행기관이 다수의 인증기관을 대행하여 CRL을 발행하는 방식이다. Dynamic CRL DP는 CRL을 분할하기 위한 초기 기준과의 간격을 설정 후 서비스 운영과정에서 인증서 발행 및 폐지의 추이에 따라 동적 으로 분할 간격을 조정하는 방식이다. 이 기법은 인증서 발행 및 폐지의 추이를 분석해야 하는 부담이 있다. OCSP모델은 사용자수가 증가함에 따라 CRL 사용의 부담을 줄이기 위한 모델로 OCSP Server는 검증 대행 요청에 의해 온라인으로 인증서의 상태를 확인한 후 그 결과를 전자 서명하여 사용자에게 전송하는 방식으로 현재의 인증서 관리에서 가장 널리 사용되는 방식이다[6]. 그러나, 검증 요청이 들어올 때마다 CRL을 새롭게 다운 받아야 하는 부담이 발생한다. SCVP(Simple Certificate Validation Protocol)는 OCSP Server의 기능과 유사하며 인증서의 경로 생성, 경로 검증, 인증서 검증을 대행해 주는 서버를 두어 사용한다.

사용자 인증 기반의 환경에서는 사용자수가 증가하므로 많은 인증서 관련 문제들이 발생되고 있다. 이에 잦은 인증서 폐지로 인해 CRL의 크기를 관리하는 모델과 실시간으로 인증서의 상태 정보를 검증할 수 있도록 보완하는 여러 방법들이 있었다. 그러나, 기하급수적으로 증가하는 CRL의 크기와 더욱 빠른 서비스를 받고자 하는 사용자들의 요구를 맞추기에는 많은 문제들을 가진다. 따라서, 본 논문에서는 사용자들의 빠른 서비스 제공을 위해 실시간으로 인증서의 상태 검증을 해주고, 기존의 CA에서 CRL관리에 필요한 작업량을 여러 OCSP Server에게 분산시키는 모델을 제안한다.

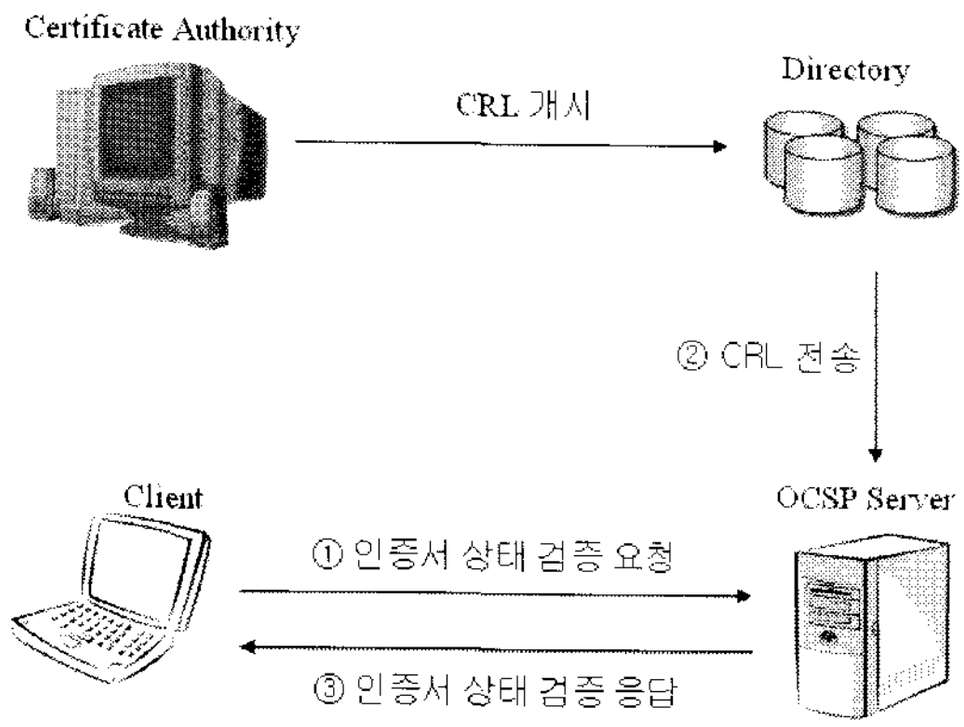


그림 1. OCSP Server를 통한 인증서 검증 과정
Fig 1. A certificate validate step by OCSP server

III. Front Server를 가지는 분산 OCSP

본 장에서는 OCSP Server를 통한 인증서 상태 검증 과정과 여러 OCSP Server를 두어 온라인으로 분산하는 모델의 구조와 인증서 상태를 검증하는 과정을 보인다. 〈그림 1〉은 Client가 OCSP Server를 통해 인증서 상태 검증을 받는 과정이다. CA는 CRL을 생성하여 Directory에 보관하게 된다. Client가 인증서 상태 검증을 OCSP Server에 요청을 하게 되면 OCSP Server는 최신의 CRL을 Directory Server로부터 전송 받아 인증서의 상태를 검증한 후 Client에게 검증 결과를 Good/Revoked/Unknown의 응답 메시지 형태로 전자 서명하여 전달하게 된다. 이 구조는 인증서 상태 요구가 폭주하여 서비스가 불가하게 될 수도 있다. 또한, 응답 메시지 중에서 에러 메시지는 전자 서명을 하지 않기 때문에 보안에 대해 취약점이 될 수 있다.

기존의 OCSP Server 구조의 인증서 상태 요구의 폭주로 인해 서비스 불능 상태가 되는 경우를 보완하기 여러 대의 OCSP Server를 분산시켜 인증서 상태 검증 요구에 대한 병목 현상을 줄이고자 하였다. 그러나, 이는 모든 OCSP Server가 동일한 CRL을 전송 받아 사용하므로 CRL의 전송 횟수를 근원적으로는 줄일 수가 없었다.

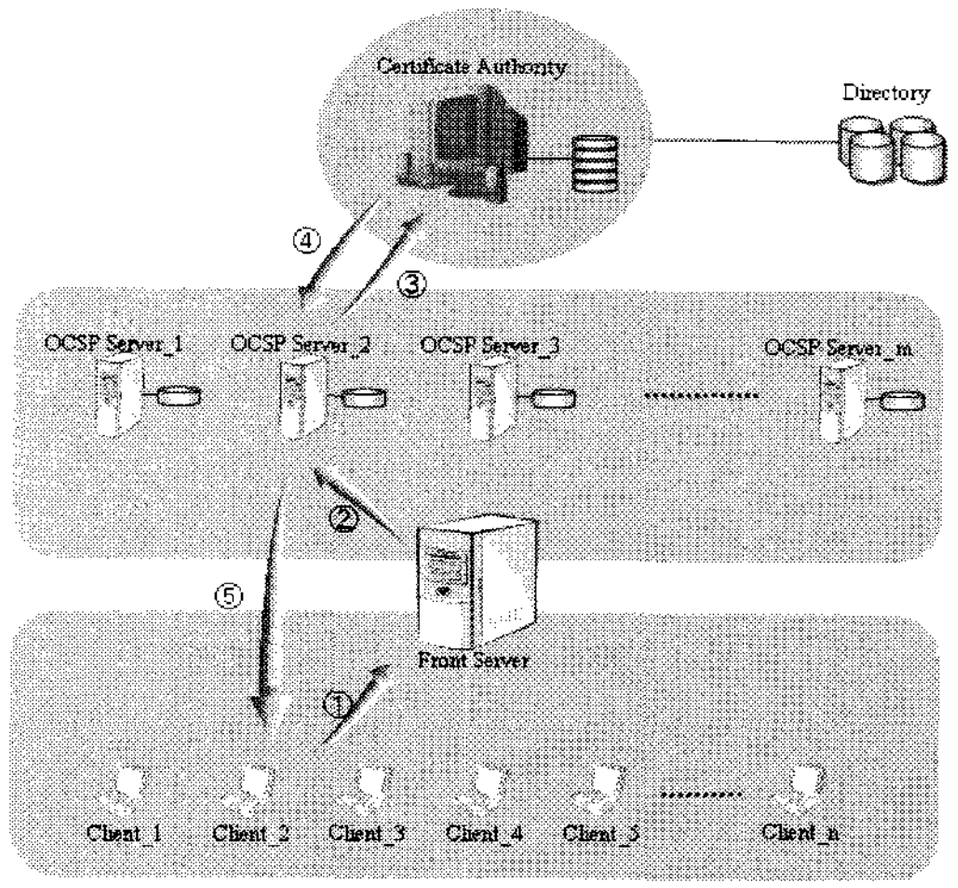


그림 2. Front Server를 가지는 분산 OCSP Server 구조
Fig 2. A framewark of distributed OCSP server using front server

이에 본 논문에서는 각 분산 OCSP Server가 동일하게 사용했던 CRL을 Base/Delta CRL에서 사용했던 방식과 유

사하게 CRL을 Cool_CRL/Hot_CRL로 분류하고, Cool_CRL에 대해서는 인증서의 일련번호를 바탕으로 분할하게 된다. 여러 개로 분할된 CRL은 여러 대의 OCSP Server에게 중첩해서 분산시키는 구조로 기존의 OCSP Server에서의 병목 현상을 줄일 수 있게 되고 각 OCSP Server가 On-line으로 전송 받아야 하는 CRL의 크기를 대폭 줄일 수 있는 구조를 제안한다.

〈그림 2〉는 본 논문의 바탕이 되는 Front Server를 가지는 분산 OCSP Server를 두는 구조에서 인증서 상태 검증 과정을 보이고 있다. 각 Client는 Front Server에게 인증서 상태 검증 요청 메시지를 보내고, Front Server는 OCSP Server들 중에서 가장 idle한 OCSP Server에게 인증서 상태 검증 요청 메시지를 전달한다. OCSP Server는 CA로부터 최신의 CRL을 다운받아 인증서의 상태 검증을 한 후, 해당 응답 메시지를 전자 서명하여 Client에게 보내게 된다.

기존의 T-OCSP(Traditional OCSP)는 CA의 인증서 상태 검증을 대신하는 Server를 둠으로써 CA의 작업량을 줄일 수 있는 모델이다. 반면에 본 논문의 기반이 되는 분산 OCSP 모델은 많은 사용자에 따라 인증서 상태 검증 요청도 증가함으로 이를 분산시키기 위하여 여러 OCSP Server를 두고 인증서 상태 검증 요청이 들어오면 Front Server가 적절한 OCSP Server에게 요청을 전달하게 되는 모델이다. 또한, 각 OCSP Server가 실시간으로 CA에게서 최신의 CRL을 다운 받아 사용함으로써 Client는 빠른 서비스를 제공받을 수 있게 된다. 그러나, 인증서 상태 검증 요청을 받을 때마다 실시간으로 CA에게서 CRL을 다운 받아 사용하는 것은 여러 분산 OCSP Server에게는 여전히 부담이 된다. 따라서, 본 논문에서는 분산 OCSP Server가 다운 받아야 하는 CRL을 Cool_CRL과 Hot_CRL로 구분하여 Cool_CRL은 주기적으로 전송하고 Hot CRL은 요청이 발생할 때마다 실시간으로 전송 받아 사용하게 된다. 따라서, CRL을 전송 받는 부담을 줄일 수가 있고, Client에게 더욱 빠르게 응답할 수가 있게 된다.

Ⅳ. CRL 분할 및 분배 기법

본 장에서는 분산 OCSP들에게 분배할 CRL을 어떠한 규칙으로 분할할 것이며, 분할된 CRL을 어떤 OCSP서버에게 분배할 것인지를 기술하고 있다. 기존의 분산 OCSP Server 구조가 가지고 있는 분배 규칙을 기반으로 하여 24시간을 주기로 하여 Cool_CRL을 분할 및 분배 하도록 하고, 주기적인 재구성 이후에 작성된 Hot_CRL은 인증서 상태 검증 요청을 받게 되면 모든 OCSP서버가 실시간으로 최신의 Hot_CRL을 전송 받아 검증을 해줄 수 있도록 한다. 〈그림 3〉은 CRL의 분할(Step-1), 분배(Step-2) 및 검증(Step-3) 과정을 개략적으로 보이고 있다.

4.1 CRL 분할

본 논문의 CRL 갱신 주기는 기존 분산 OCSP Server의 CRL갱신 주기와 동일하게 24시간을 주기로 가정하였다. 해당 주기마다 CRL을 갱신하게 되고, 갱신 이후에 폐지된 인증서 목록은 Hot_CRL로 관리하게 된다. Cool_CRL은 갱신 주기인 24시간을 기준으로 하여 하루에 한번씩 정해진 시간에 CRL을 갱신하게 된다. CRL DP에서 사용되었던 기법과 유사하게 일정량의 인증서 일련번호(#1~#3000)로 CRL을 분할하게 된다. 반면에, Hot_CRL은 CRL의 갱신이 이루어진 이후부터 다음 주기 내에 발생한 CRL을 저장하게 된다.

4.2 CRL 분배

주기적인 CRL 갱신에 의해 분할된 Cool_CRL들은 여러 OCSP Server에게 중복해서 분배하게 된다. 분배 정보 내역을 가지는 OCSP State Table은 각 갱신 주기마다 Front Server에게 전달하게 된다. OCSP State Table을 전달받은 Front Server는 Client로부터의 인증서 상태 검증 요청이 들어오면 해당 정보를 가지고 있는 OCSP Server를 OCSP State Table로부터 찾아서 인증서 상태 검증 요청 메시지를 전달하게 된다. 반면에, Hot_CRL의 분배는 인증서 상태 검증 요청을 받은 OCSP Server는 기존의 OCSP의 방식과 동일하게 실시간으로 전송 받아 사용하게 된다. 갱신 주기 내에 한번 전송 받은 Cool_CRL은 주기가 변경될 때까지 OCSP Server은 재전송 받지 않는다. Hot_CRL의 경우는 인증서 상태 검증 요청을 받을 때마다 CA로부터 새롭게 재전송 받게 된다. 따라서, 기존의 분산 OCSP에서는 검증 요청을 받을 때마다 모든 CRL을 대부분 재전송 받아야 했으나, 본 논문에서 제안하는 모델은 CRL의 일부인 Hot_CRL만을 실시간 재전송을 받게 된다.

CA에서 CRL의 갱신 주기에 Cool_CRL을 재구성한 후에 각 OCSP Server가 관리해야 하는 CRL의 크기를 고려하여 분할된 Cool_CRL을 중첩하여 OCSP State Table을 구성하여 Front Server에게 전송하게 된다.

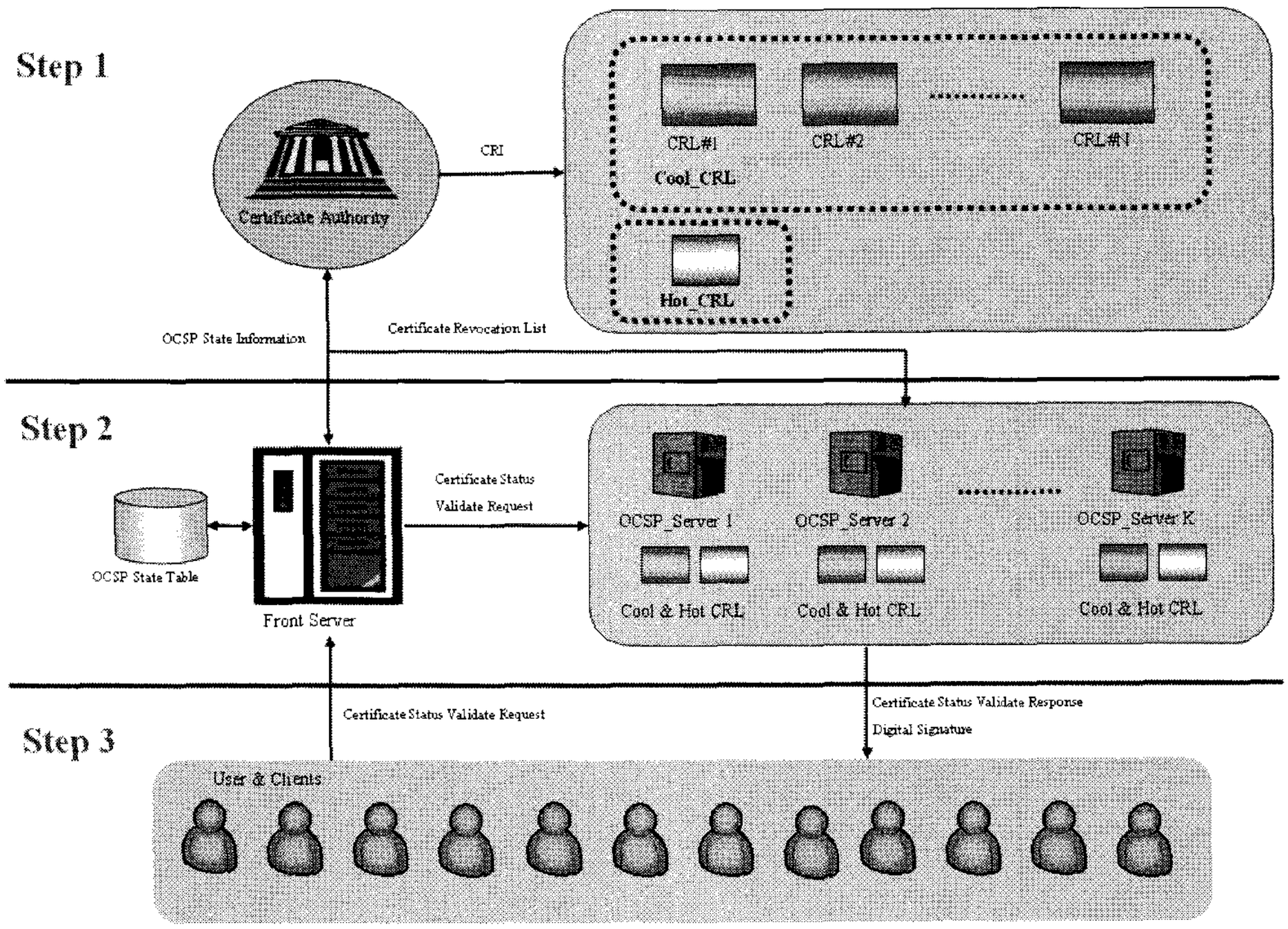


그림 3. 제안하는 CRL 분할 및 분배 기법을 적용한 전체 구조도
Fig 3. A proposed structure for CRL partitioning and distributing

4.3 인증서 상태 검증

기존의 T-OCSP는 Client가 OCSP Server에게 인증서 상태 검증을 요청하면 실시간으로 CA로부터 최신의 CRL을 다운받아 검증을 하게 된다. 또한 분산 OCSP은 계층적으로 여러 OCSP Server마다 관리하는 Client들을 두어 기존 T-OCSP와 동일하게 검증 절차를 진행한다. 본 논문에서의 검증 절차는 기존의 OCSP Server 방식과는 달리 Client가 Front Server에게 인증서 검증 요청 메시지를 보냄으로 검증 절차가 시작된다.

제안 모델의 인증서 상태 검증 절차는 〈그림 3〉에서 보는 바와 같이 Client가 Front Server에게 인증서 상태 검증 요청 메시지를 보내고, 요청 메시지를 받은 Front Server는 OCSP State Table을 바탕으로 해당 인증서를 관리하는 OCSP Server에게 인증서 검증 요청 메시지를 전달하게 된다. 메시지를 전달받은 OCSP Server는 기존에 보유하고 있는 Cool_CRL의 유효기간을 확인하여 사용 불가능한 경우에만 CA로부터 최신의 Hot_CRL과 Cool_CRL을 전송받는다. 만약 OCSP Server에서 보유하고 있는 Cool_CRL의 유효기간이 아직 유효하다면 최신의 Hot_CRL만 재전송받아 인증서 상태 검증을 확인하게 된다. OCSP Server는 인증서 상태를 확인한 후 Good/Revoked/Unknown의 응답 형식으로 검증을 요청한 Client에게 전자 서명하여 응답 메시지를 보내게 된다.

V. 제안 모델 분석

본 장에서는 기존의 T-OCSP와 분산 OCSP를 제안하는 모델과 비교한다. 〈표 2〉에서 보여주는 비교 항목들은 [3]에서 사용되었던 비교 항목들을 사용하였다.

OCSP Server의 수는 분산 OCSP 모델에서 여러 대를 두어 사용하게 되었다. OCSP Sever의 증가는 많아질수록 응답 시간이 짧아지는 것은 당연하나, Client수에 비례해서 적절하게 OCSP Server 수를 증가해야 할 것이다.

CSV(Certificate Status Validate)의 병행성 측면에서는 제안하는 분산 OCSP는 기존의 분산 OCSP보다는 덜 제약적이다. 또한 CSV의 부하는 Front Server에 의해서 가장 부하가 적은 OCSP Server에게 요청 메시지를 전달하게 되므로 각 OCSP Server들의 부하 균형이 기존의 분산 OCSP 모델에 비해 가능하다. 또한, CRL의 분배에 있어서는 모든 모델들이 CRL을 분배할 때 CA의 전자서명을 한 파일을 받기 때문에 분배 받은 CRL에 대해서는 무결성을 지닌다고 볼 수 있다. 제안 분산 OCSP 모델은 작업의 부하 균형을 위하여 Front Server를 두어 각 OCSP Server들의 작업량 균형을 이루도록 하였다.

〈표 3〉은 CRL을 분할하고 분배하는데 필요한 작업량을 비교하였다. k는 OCSP Server 수를 나타내고, d는 동일한 CRL의 중복 비율이다. 제안 모델은 각 주기마다 CRL을 분할하는 작업을 시행하고 Front Server에게 분할에 관련된 OCSP State 정보를 전달하게 된다. CA에서 CRL을 OCSP Server에게 전달하는 횟수는 기존의 T-OCSP와 분산 OCSP의 경우에는 요청이 들어오면 CRL전체를 전달하기 때문에 전체적으로 검증요청 시마다 CRL를 전송 받게 된다. 반면에 제안모델은 Cool_CRL의 경우는 각 주기에 한 번 각 OCSP Server에게 전달하고, Hot_CRL의 경우는 요청이 발생할 때마다 최신의 CRL을 전송 받게 되므로 기존 기법에 비해 CRL의 갱신 횟수가 적고, 전체 CRL을 전송해야 하는 기존 기법에 비해 네트워크 작업량이 적다.

〈표 3〉의 전달 횟수만을 본다면 제안하는 모델이 최대 횟수를 가지나 전송하는 CRL의 크기는 제안하는 분산 OCSP 모델이 적은 값을 보인다. 전송 크기는 기존의 T-OCSP나 분산 OCSP의 경우에는 전체 CRL을 모두 전송해야 하나, 제안하는 분산 OCSP에서는 CRL의 일부만을 전송하게 되므로 전달하는 횟수가 많아도 전체적으로 전송하는 크기가 최소한 1/d로 줄게 된다.

표 2. 제안 모델과 기존 모델들과 비교
Table 2. A comparison of proposed model and the legacy model

	T-OCSP	분산 OCSP	제안 분산 OCSP
OCSP Server 수	Single	Multitude	Multitude
CSV Concurrency	-	Difficult	Possible
CSV Capacity	Low	High	High
CSV Load Balancing	-	Difficult	Possible
Integrity of CRL in Distribution	O	O	O
Confidentiality of CRL in Distribution	X	X	X
Server for Load Balancing	X	X	O

표 3. CRL에 관련된 작업량 비교
Fig 3. A comparision of workload for CRL

		T-OCSP	분산 OCSP	제안 분산 OCSP
CA	분할 횟수	-	-	주기
	분배 횟수	-	-	주기
	전달 횟수	주기x검증요청	주기x검증요청	Cool_CRL: 주기x k Hot_CRL: 주기x검증요청
	전송 크기	Full CRL	Full CRL	Partial CRL
OCSP Server	요청 횟수	주기x검증요청	(주기x검증요청)/k	주기x검증요청
	응답 횟수	주기x검증요청	(주기x검증요청)/k	(주기x검증요청)/(dxk)

Ⅵ. 결론 및 향후 연구 과제

인증서 상태 검증을 위하여 일반적으로 CRL을 사용하게 된다. 그러나, 사용자수가 많아짐에 따라 CRL의 크기가 기하급수적으로 증가되어 관리 측면에서 CA의 부담이 되고 있다. 따라서, OCSP을 사용하여 CA의 인증서 상태 검증 절차를 실시간으로 OCSP Server가 진행하도록 하여 CA의 부담을 줄이려는 방안들이 제시되어왔으나, 기존 OCSP에서는 최신의 CRL을 전송 받아 사용함에 있어서 네트워크 부하가 크게 발생되고, 기존 CA가 가졌던 병목현상은 여전히 OCSP Server가 가지게 되는 단점이 있다.

이에 본 논문에서는 CRL을 전송 받는데 드는 전체적인 네트워크 부하를 줄이기 위하여 CRL을 주기마다 생성되는 Cool_CRL과 주기 사이에 발생되는 CRI를 가지는 Hot_CRL로 분류하였다. 또한 Cool_CRL은 여러 OCSP Server들에게 중복되어 분배되고, Hot_CRL의 경우는 인증서 상태 검증 요청 메시지가 있을 때마다 실시간으로 전송받아 검증절차를 진행하게 된다. 이는 기존의 분산 OCSP보다는 OCSP Server의 작업량을 줄였고, OCSP Server에서 전송 받는 CRL의 전송 크기를 최소한으로 줄임으로써 네트워크 전반의 전송되는 데이터 크기를 줄이고자 하였다. 전체적인 작업량을 골고루 분산시키기 위해서 Front Server에서는 각 OCSP Server의 작업 부하 정도를 모니터링 하게 된다. Front Server의 작업 균등화에 관련된 부분의 기술은 향후에 진행할 것이다.

본 논문에서 제안하는 모델은 기존의 모델들과 비교해서 전체적인 네트워크의 부하를 줄일 수는 있으나, Front Server를 경유해서 메시지가 전달되는 과정으로 인해 교환되는 메시지의 수는 기존의 모델에 비해 더욱 증가되는 단점을 가진다[5]. 이러한 교환 메시지를 줄이고 CRL의 접근 횟수를 근원적으로 줄일 수 있는 방안을 모색하여 인증서 상태 검증에 대한 응답을 더욱 빠르고 정확하게 받을 수 있는 연구가 진행되어야 할 것이다.

참고문헌

[1] 이상렬, "실시간 상호인증 지원을 위한 무선랜 보안시스템에 관한 연구", 한국컴퓨터정보학회, 제 10권 제5호, 2005년 11월, pp.161-179.

[2] 이영교, 남정현, 김지연, 김승주, 원동호, "D-OCSP-KIS에서 OCSP Responder의 세션 개인키의 노출을 검출하는 방법", 정보보호학회 논문지, 제15권 제4호, 2005년 8월, pp.83-92.

[3] 이호, 강현중, 박준홍, "D-OCSP에서의 그룹키를 이용한 CRL 배포 방법에 관한 연구", 한국컴퓨터정보학회 논문지, 제11권, 제1호, 2006년 3월, pp.35-44.

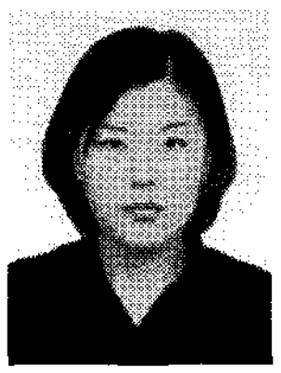
[4] Bogdan C. Popescu, Bruno Crispo, Andrew S. Tanenbaum: A Certificate Revocation Scheme for a Large-Scale Highly Replicated Distributed System. ISCC 2003: 225-231.

[5] K. Papapanagiotou, G. F. Marias, P. Georgiadis, and S. Gritzalis, "Performance evaluation of a distributed OCSP protocol over MANETs," in Proceedings of 3rd IEEE Consumer Communications and Networking Conference (CCNC'06), vol.1, pp.1-5, LasVegas, Nev, USA, January 2006.

[6] Iliadis J., Gritzalis S., Spinellis D., De Cock D., Preneel B., Gritzalis D. (2003), "Towards a framework for evaluating certificate status information mechanisms", Computer Communications, Vol. 26 No.16, pp.1839-1850.

[7] R. Housley , W. Polk , W. Ford , D. Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC Editor, 2002.

저 자 소 개



김 경 자

2004년 8월 : 동국대학교 컴퓨터공학박사

2005년 3월 ~ 2008년.2월 : 세종대학교 컴퓨터공학과 초빙교수

관심분야 : MANET, 라우팅 프로토콜, MAC 프로토콜

장 태 무

1995년2월:서울대학교 전산기공학박사

1981년3월 ~ 현재: 동국대학교 컴퓨터공학과 교수

관심분야:컴퓨터구조, 병렬/분산처리, Power-aware computing