축약 서명 기반의 실시간 인증서 상태 검증 기법

김 현 철[†] · 안 재 명[††] · 이 용 준[†††] · 오 해 석[††††]

요 약

최근 온라인을 이용한 금융거래가 매우 빠른 속도로 증가함에 따라 해당 거래에 대한 유효성 보장은 더욱 중요한 의미를 가지게 되었다. 해당 거래에 대한 유효성 보장을 효과적으로 제공하기 위해서는 거래 당사자의 신원확인, 거래 데이터의 무결성 및 기밀성 보장, 거래의 대한 부인방지 기능 등을 실시간으로 제공할 수 있는 인증서 상태 검증 시스템이 요구된다. 기존의 실시간 인증서 상태 검증 시스템은 모든 트랜잭션에 대해 하나의 노드에서 처리해야하는 구조적인 집중화 현상이 발생한다. 또한 상태 검증을 요청할 때마다 불필요한 정보까지 모두 전송하기 때문에 네트워크 과부하와 통신 병목현상이 발생한다. 이와 같은 문제점으로 인해 실시간 응답시간이 중요시 되는 금융거래에는 적합하지 않다. 본 논문에서는 기존의 실시간 인증서 상태 검증 요청시 불필요한 정보와 구조적인 집중화 현상으로 인한 문제점을 개선하기 위하여 검증서버를 도메인별로 분산시켜 상태 검증을 처리한다. 또한 인증서 상태 검증에 반드시 필요한 축약정보만을 이용하여 검증을 요청함으로써 네트워크 과부하와 통신 병목현상을 해결 할 수 있는 실시간 인증서 상태 검증 기법을 제안한다. 또한, 실험을 통하여 기존 OCSP(Online Certificate Status Protocol) 기법에 비해 약 15%정도 인증서 상태 검증 속도가 향상됨을 확인하였다.

A Real-Time Certificate Status Verification Method based on Reduction Signature

Hyun Chul Kim[†] · Jae Myoung Ahn[††] · Yong Jun Lee[†††] · Hae Seok Oh[††††]

ABSTRACT

According to banking online transaction grows very rapidly, guarantee validity about business transaction has more meaning. To offer guarantee validity about banking online transaction efficiently, certificate status verification system is required that can an real-time offer identity certification, data integrity, guarantee confidentiality, non-repudiation. Existing real-time certificate status verification system is structural concentration problem generated that one node handling all transactions. And every time status verification is requested, network overload and communication bottleneck are occurred because all useless informations are transmitted. it does not fit to banking transaction which make much account of real response time because of these problem. To improve problem by unnecessary information and structural concentration when existing real-time certificate status protocol requested , this paper handle status verification that break up inspection server by domain. This paper propose the method of real-time certificate status verification that solves network overload and communication bottleneck by requesting certification using really necessary Reduction information to certification status verification. And we confirm speed of certificate status verification 15% faster than existing OCSP(Online Certificate Status Protocol) method by test.

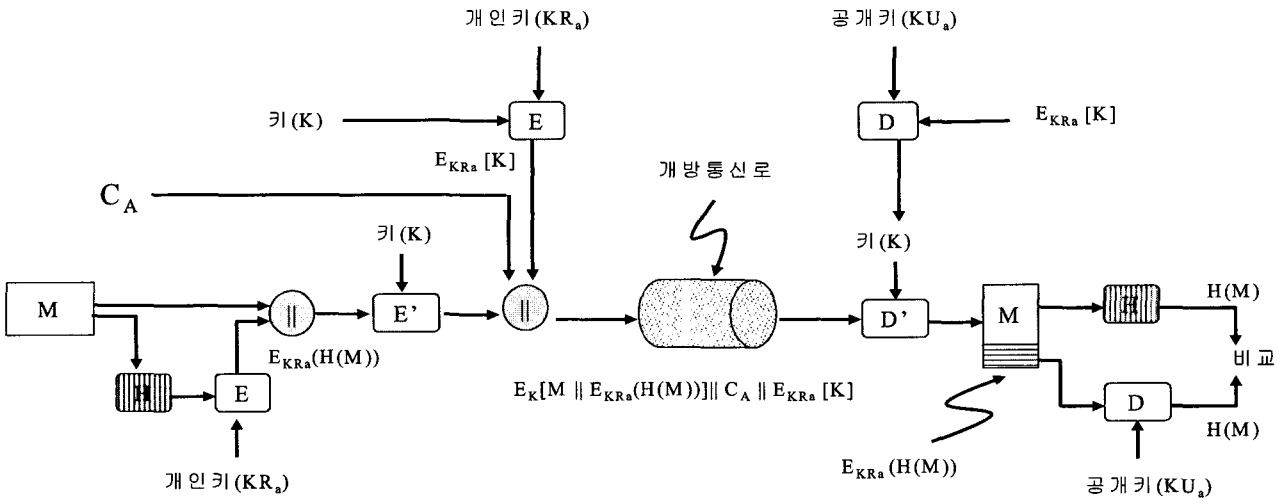
키워드 : 축약 서명(Reduction Signature), 실시간 인증서 상태검증(Real-time Certificate Status Verification), OCSP(Online Certificate Status Protocol)

1. 서 론

최근 인터넷의 발달 및 보급 확대에 따라 전자상거래를 통한 경제활동 비중이 높아지고 있다. 이에 따라, 전송되는 정보의 위·변조 등과 같은 외부 위협요소로부터 사용자 피해 발생 가능성도 증가하고 있다. 이러한 소비자 피해를 줄이기 위해서는 해당 거래에 대한 유효성 보장이 반드시 선행되어져야 한다. 이를 위해 해당 거래에 대해 인증서를 이용하는 인증 시스템이 요구된다.

인증서를 이용한 인증 시스템은 합법적인 서명자만이 전자서명을 생성할 수 있는 위조불가, 전자서명의 서명자를 불특정 다수가 검증 할 수 있는 서명자인증, 서명자가 서명한 사실을 부인할 수 없는 부인방지, 서명한 전자 문서의 내용을 변경할 수 없는 변경불가, 전자문서의 서명을 다른

† 준 회 원 : 경원대학교 박사과정
†† 종신회원 : (주)리테일테크 대표이사
††† 준 회 원 : 숭실대학교 컴퓨터학과 박사
†††† 종신회원 : 경원대학교 소프트웨어대학 교수
논문접수 : 2004년 6월 3일, 심사완료 : 2004년 8월 17일



(그림 1) 전자서명 검증

전자문서의 서명으로 사용할 수 없는 재사용불가등의 기능을 제공함으로써 해당 거래에 대한 유효성 보장을 제공한다[1].

인증기관에 의해 발급된 인증서는 개인키분실, 자격상실, 키변경 등의 여러 가지 이유로 폐지될 수 있다. 이러한 이유로 검증자는 수신한 인증서에 대해 유효한 인증서인지 아닌지 확인해야 한다. 이를 인증서 상태 검증이라 한다[2].

인증서 상태 검증 기술은 인증서의 현재 상태와 인증서의 소유자 및 발행자의 신원확인을 확인하는 과정으로 전자거래에 있어 가장 중요한 부분이다. 이러한 인증서 상태 검증 기법은 주기적 기법과 실시간 기법으로 구분할 수 있다[3].

주기적 기법은 인증서 폐지 목록(Certificate Revocation List : CRL)[4]을 이용한다. 그러나 CRL의 주기적 배포 특성으로 인해 인증서 상태에 대한 실시간성을 반영할 수 없다. 이러한 CRL을 이용한 주기적 기법의 문제를 개선하기 위하여 온라인 인증서 상태 프로토콜 (Online Certificate Status Protocal : OCSP)[5]과 같은 실시간 기법이 제기 되었다. 이 기법은 CRL을 이용한 주기적 기법에 문제점인 비실시간성을 해결한다. 그러나 모든 검증 트랜잭션에 대해 하나의 노드에서 응답해야하는 구조적인 집중화 문제가 있다. 또한 상태 검증을 요청할 때마다 인증서의 모든 정보를 전송해야 하기에 네트워크 과부하와 통신 병목현상이 발생한다. 이와 같은 원인으로 인해 인증서 상태 검증 속도가 다소 느리다는 단점이 있다. 따라서 기존의 실시간 기법은 금융거래와 같이 실시간 응답시간이 중요한 경우에 적합하지 않다[6-8].

본 논문은 실시간 인증서 상태 검증 기법의 구조적인 집중화 현상으로 인한 문제점을 개선하기 위해 검증서버를 도메인별로 분산시켜 상태 검증을 처리한다. 또한 검증 요청 시 불필요한 정보 전송으로 인해 발생하는 문제를 해결하기 위해 인증서 상태 검증 과정에서 반드시 필요한 축약정보(인증서 일련번호, 인증서 식별명)만을 전송하고 인증서 상태 검증을 요청한다. 이에 대한 결과로 인증서 상태 검증 수행 속도를 향상시킴으로써 금융거래에 적합한 인증서 상태 검증 기법을 제안하고자 한다.

2. 관련 연구

2.1 전자서명 검증

전자서명 검증은 개인키와 공개키로 구성된 하나의 키쌍을 이용하여 문서를 전자서명하고 검증하는 기술이다. 즉 서명자는 자신만이 아는 개인키를 이용하여 문서를 전자서명하고 검증자에게 검증을 요청한다. 검증자는 서명자의 공개키를 이용하여 수신한 전자서명 문서에 대해 검증하는 행위를 전자서명 검증이라 한다. 전자서명 검증은 서명한 내용에 대한 무결성과 인증을 제공한다. 이는 적절한 암호화 알고리즘을 이용하며 수행되며, 오프라인 상에서도 검증이 가능하다[9]. 전자서명 검증 전자서명 검증 과정은 (그림 1)과 같다.

2.2 CRL을 이용한 주기적 인증서 상태 검증 기법

CRL은 RFC2459에서 정의되어 있다. CRL은 여러 가지 이유로 폐지된 인증서를 모아놓은 목록으로 인증기관이 폐지된 모든 인증서의 일련번호, 폐지시간, 폐지이유를 주기적으로 생성하여 서명한 후 디렉토리에 게시한다. 게시된 CRL을 검증자가 검증시점에 디렉토리로부터 검색하고 다운로드 한 후 인증서 상태 검증시 다운 받은 CRL을 이용하여 인증서 상태 검증을 수행하는 기법이다[10].

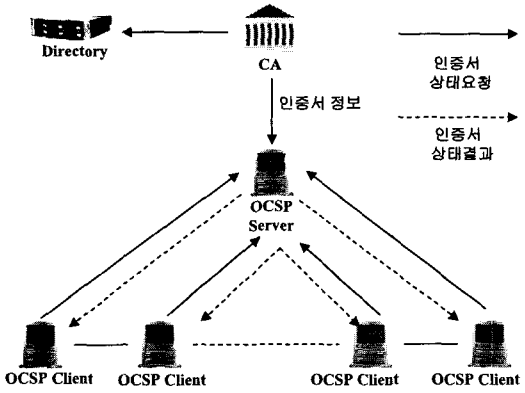
2.3 OCSP 기반의 실시간 인증서 상태 검증 기법

1999년 6월 'X.509 Public Key Infrastructure Online Certificate Status Protocol' OCSP 버전 1.0이 발표되었다. 이후 2001년 3월 현재 사용되고 있는 OCSPv2가 드래프트 형태로 발표 되었다[11].

OCSP 상태 검증 시스템의 전체 구성은 다수의 클라이언트가 중앙에 위치한 서버를 이용하는 형태로 구성되어 있다. 따라서 서버 부하가 집중되며, 서버 부하가 고도화됨에 따라 처리비용이 지수적으로 증가한다. 또한 각각의 클라이언

트에서 검증 요청을 할 때마다 인증서의 모든 정보를 서버로 전송해야 하기 때문에 네트워크 과부하 및 통신 병목현상이 발생할 수 있다.

결과적으로 위에서 지적한 문제점으로 인해 인증서 상태 검증에 소요되는 시간이 오래 걸린다. OCSP 기반의 인증서 상태 검증 시스템의 전체 구성은 (그림 2)와 같다.



(그림 2) OCSP 인증서 상태 검증 시스템 전체 구조

OCSP클라이언트는 해당 거래에 사용되는 인증서에 대해 상태 검증을 OCSP서버에게 요청한다. 또한 서버로부터 수신한 처리결과를 서명자에게 전송하는 기능을 담당한다. 서버는 클라이언트 요청에 대해 상태 검증을 수행하고 수행결과를 클라이언트에게 전송하는 기능을 담당한다. OCSP 인증서 상태 검증 기법의 시스템 구조는 (그림 3)과 같다.

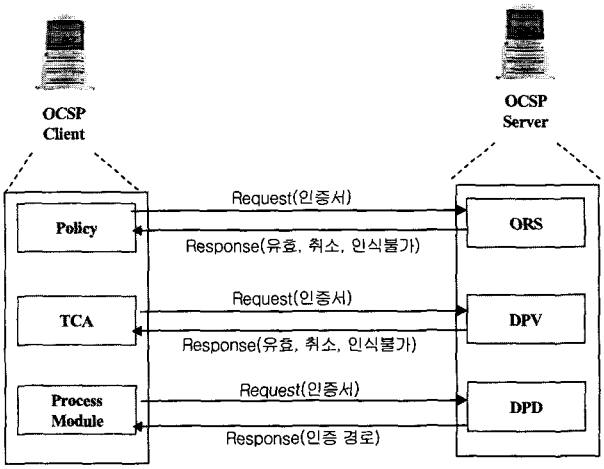
OCSP 서버는 온라인 취소 유효 확인, 대리 인증 경로 탐색, 대리 인증 경로 검증 등과 같은 기능을 제공한다[12].

온라인 취소 유효 확인 서비스(Online Revocation Status : ORS)는 클라이언트가 서버에게 특정 인증서의 정보를 제공하고 서버는 클라이언트에게 특정 인증서의 취소 상태를 알려준다[13].

대리 인증 경로 검증 서비스(Delegated Path Validation : DPV)는 클라이언트의 검증 요청을 받은 서버는 인증서의 정책에 따라 최근의 인증서 상태정보를 이용하여 인증서 검증을 수행한다[14].

대리 인증 경로 탐색 서비스(Delegated Path Discovery : DPD)는 서버가 인증서 경로 구축 정책에 따라 클라이언트 대신 신뢰정점까지의 인증서 경로를 구축한다[13-14].

OCSP 인증서 상태 검증 기법의 내부 처리 과정은 (그림 4)와 같다.



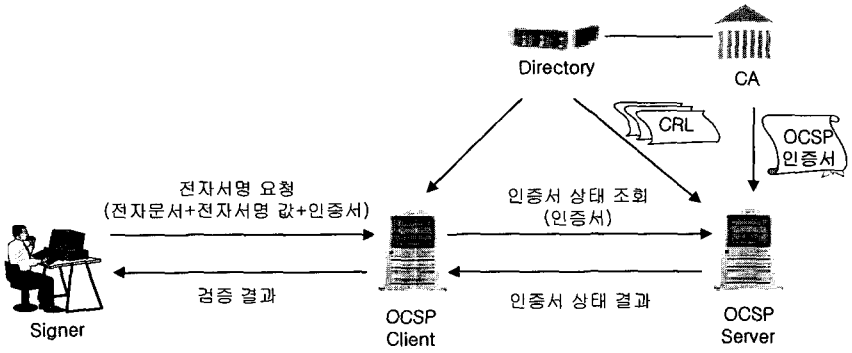
(그림 4) OCSP 기반 인증서 상태 검증 기법 내부 처리 과정

3. 제안하는 인증서 상태 기법

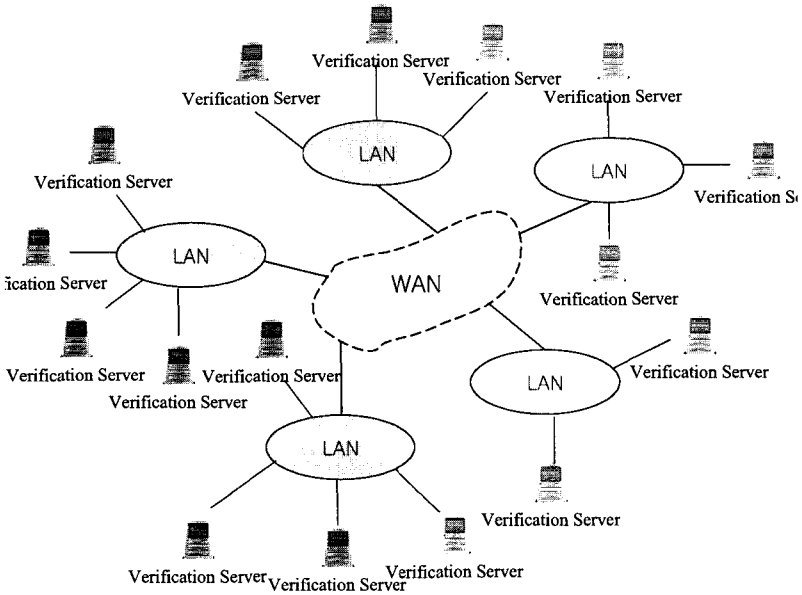
3.1 분산된 검증서버 구조

CRL기반의 인증서 상태 검증 기법과 비교했을 때 OCSP 기반의 인증서 상태 검증 기법은 실시간성을 제공한다는 점에서 매우 유용하다. 하지만 앞절에서 제시한 문제점으로 인해 상태 검증 수행 시간이 오래 소요된다. 특히 현재 PKI 기반의 인증 시스템의 80%이상이 금융거래와 같은 실시간 응답시간을 중요시 하는 분야에 사용된다는 점에 비추어 볼 때 OCSP 기법은 적절하지 않은 방법이다.

도메인은 이미 엄청난 수가 존재하며, 그 사용량 역시 매우 빈번하다. 또한 분산된 도메인은 동시에 같은 정보를 응답함으로써 확장성이 매우 뛰어나다. 그리고 기존의 도메인을 그대로 사용함으로써 추가 시스템 도입에 따른 추가적인 비용이 소요되지 않으며 구조적인 특성상 네트워크 부하의 효과적인 분산이 가능하다. 따라서 본 논문에서는 검증 서버를 각각의 지역 도메인 내에 분산시킴으로서 OCSP구조적



(그림 3) OCSP 인증서 상태 검증 기법 시스템 구조



(그림 5) 분산된 검증 서버 구조

으로 발생할 수 있는 문제를 해결한다. 제한하는 기법의 분산 검증 서버 구조는 (그림 5)와 같다.

3.2 축약서명

축약서명은 기존의 전자서명을 간소화한 서명 방법이다. 기존의 서명자는 검증을 요청할 때 전자서명문서, 전자서명값, 인증서를 검증자에게 전송하고 검증을 요청한다. 이때 전송되는 정보는 전자문서 크기에 따라 차이는 있지만 대략 1500byte정도이다. 그 중 인증서 정보는 1300byte를 차지한다. 제안하는 축약서명 방식은 인증서 대신 인증서 상태 검증에 꼭 필요한 정보(시리얼번호, 식별명)와 전자서명문서, 전자서명 값만을 검증자에게 전송하고 검증 요청을 한다. 이때 시리얼번호와 식별명은 서명자 인증서 자체에서 축출하고 해당 정보를 보호하기 위해 암호화되어 전송한다. 이때 전송되는 정보의 최대 크기는 전자문서에 크기에 따라 차이는 있지만 300byte를 넘지 않는다.

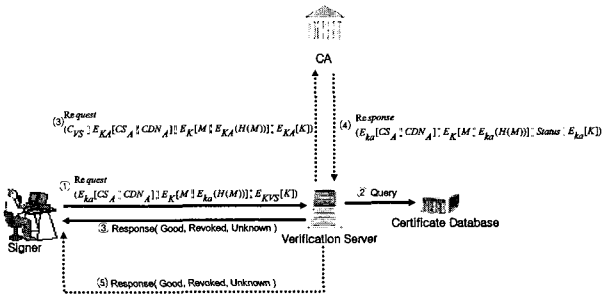
본 논문에서 제안하는 상태 검증 기법 시스템 구조는 OCSP 기법과 달리 클라이언트가 없이 검증서버와 인증서 정보를 저장하고 있는 데이터베이스로 구성된다. 제안하는 상태 검증 시스템 구조는 (그림 6)과 같으며 사용되는 프로토콜의 정의는 <표 1>과 같다.

〈표 1〉 프로토콜 정의

- Signer ==> Verification Server
  $E_{ka}[CS_A \| CDN_A] \| E_K[M \| E_{ka}(H(M))] \| E_{KVS}[K]$
- Verification Server ==> CA
  $C_{VS} \| E_{KA}[CS_A \| CDN_A] \| E_K[M \| E_{KA}(H(M))] \| E_{KA}[K]$
- CA ==>Verification Server
  $E_{ka}[CS_A \| CDN_A] \| E_K[M \| E_{ka}(H(M))] \| Status \| E_{ka}[K]$
- Response Message
  Good, Revoked, Unknown

A	:	사용자 A, K : 대칭키, E : 암호화
ka	:	사용자 A의 개인키
KA	:	사용자 A의 공개키
KVS	:	검증서버의 공개키
CS_A	:	사용자 A의 인증서 시리얼번호
CDN_A	:	사용자 A의 인증서 DN
M	:	메시지
H( )	:	해쉬함수
C_{VS}	:	검증서버의 인증서
Good	:	유효
Revoked	:	폐지
Unknown	:	알 수 없음

(그림 6)의 시스템의 구조에서 ①, ②, ③은 검증 서버 데이터베이스에 검증을 요청한 인증서 정보가 존재 할 경우에 처리과정이다. 또한 ①, ②, (3), (4), (5)는 검증 서버 데이터베이스에 검증을 요청한 인증서 정보가 존재 하지 않을 경우에 처리 과정이다.



(그림 6) 축약 서명 기반의 인증서 상태 검증 시스템 구조

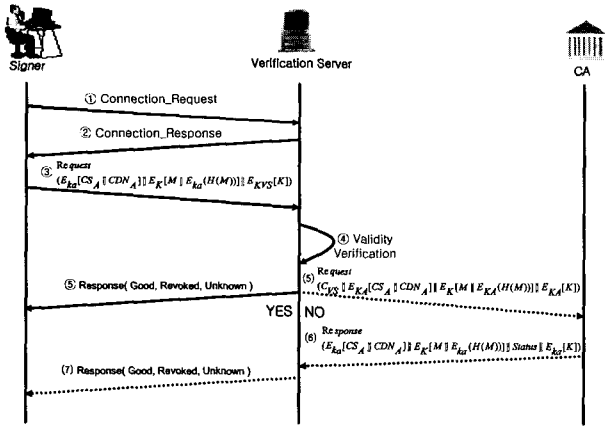
3.3 인증서 상태 검증 처리 과정

본 논문에서 제안하는 인증서 상태 검증 기법은 검증을

요청한 인증서 정보가 검증서버 데이터베이스에 존재 할 경우와 검증서버 데이터베이스에 해당 정보가 존재하지 않을 경우로 구분하여 처리한다. 검증서버는 다음과 같은 기능을 수행한다.

- 전자서명문서, 전자서명값에 대한 전자서명 검증을 수행한다.
- 검증서버는 전송받은 축약정보를 복호화하고 시리얼 번호와 식별명을 획득한다.
- 데이터베이스에서 시리얼번호, 식별명이 일치하는 인증서 정보를 찾는다.
- 일치하는 정보가 있을 경우 해당 인증서에 대한 상태 검증을 수행한다. 그러나 일치하는 정보가 없을 경우 CA에게 해당 인증서에 대한 상태 검증을 요청한다.
- 처리결과를 사용자에게 전송한다.

서명자와 서버사이에 정보 전송 과정에서 전송 메시지 손실과 같은 예외 상황에 대한 고려가 필요하다. 서명자는 검증서버에게 정보를 전송하고 해당 정보에 대한 응답 정보가 도착할 때까지 기다린다. 하지만 서버로부터의 응답 메시지가 여러 가지 이유로 전송 도중 손실될 수 있다. 이러한 예외사항에 대비하기 위하여 타임 기능을 이용한다. 서명자는 검증서버에 정보를 전송하고 일정시간동안 응답이 도착하지 않으면 해당 연결을 끊고 새로운 연결을 다시 시도한다. 제안하는 상태 검증 방식의 전체 처리 과정은 (그림 7)과 같다.



(그림 7) 전체 처리 과정

3.2.1 인증서 정보가 존재 할 경우

이 경우 검증서버는 서명자, 유효기간, 정책, 인증서상태 등과 같은 항목에 대하여 검증을 수행하고 처리결과를 데이터베이스에 반영하고 서명자에게 전송한다. 처리절차를 다음과 같다.

① 서명자는 검증서버에 접속 요청을 한다.
② 검증서버는 서명자에게 접속 여부를 알려준다.
③ 접속이 이루어지면 상태 검증을 요청한다. 요청 정보는 다음과 같다.

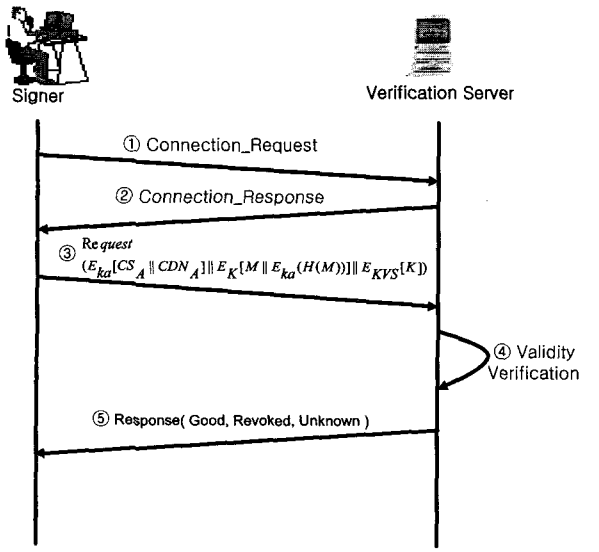
$$E_{ka}[CS_A \| CDN_A] \| E_K[M \| E_{ka}(H(M))] \| E_{KVS}[K] \quad (1)$$

A는 사용자 A를, $E_{ka}[CS_A \| CDN_A]$는 사용자 A에 인증서 시리얼번호와 식별명을 A의 개인키로 암호화한 값 즉 축약정보이며 M은 전자문서이다. 또한 $E_{ka}(H(M))$는 전자문서 M을 해쉬하고 얻은 값을 A의 개인키로 암호화 한 전자서명값이다. $E_{KVS}[K]$ 는 대칭키 K를 검증서버의 공개키로 암호화 한 값이다.

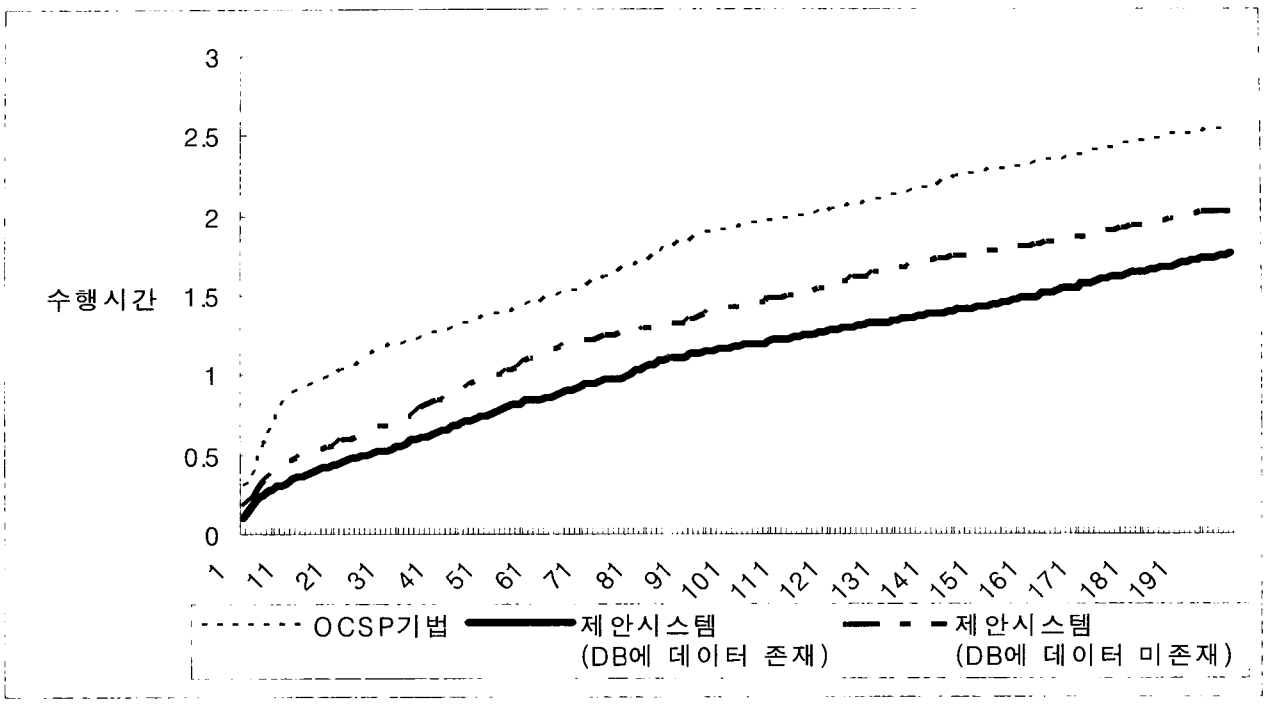
이때 검증서버의 공개키로 대칭키를 암호화하는 것은 만약 사용자의 개인키로 암호화 하였을 경우 그 개인에 대한 공개키를 알고 있는 사람으로 인해 대칭키가 노출될 수 있다는 문제가 발생할 수 있다. 따라서 사용자가 검증을 요청하는 서버의 공개키를 이용하여 키를 암호화함으로써 안정성을 보장할 수 있다.

④ 검증서버는 전송받은 정보를 복호화를 수행한 후 인증서 일련번호와 식별명을 획득한다. 획득한 정보를 이용하여 자신의 데이터베이스에서 일치하는 인증서 정보를 찾고 상태 검증을 수행한다.
⑤ ④번 과정의 처리결과를 데이터베이스내에 Status 필드에 저장하고 처리 결과를 서명자에게 전송한다. 처리 결과에 대한 응답 형태는 OCSP와 동일하며 Good, Revoked, Unknown 세가지 값을 가진다. Good은 유효한 인증서, Revoked 폐지된 인증서, Unknown 인증서 상태를 알 수 없음을 의미한다.

인증서 정보가 데이터베이스에 존재하는 경우에 대한 인증서 상태검증 처리 과정은 (그림 8)과 같다.



(그림 8) 인증서 상태 정보가 DB에 존재 할 경우 인증서 상태검증 처리 과정



(그림 10) 인증서 상태 검증 실험 결과

3.2.2 인증서 정보가 존재 하지 않을 경우

검증서버 데이터베이스에 인증서 정보가 존재하지 않을 경우 검증서버는 인증기관에게 인증서 상태 검증을 요청한다. 처리절차는 다음과 같다.

(1) 서명자는 검증서버에 접속 요청을 한다.
(2) 검증서버는 서명자에게 접속 여부를 알려준다.
(3) 접속이 이루어지면 전자서명문서, 전자서명값, 축약정보를 전송하고 상태 검증을 요청한다.
(4) 검증서버는 전송받은 정보를 복호화를 수행한 후 인증서 일련번호와 식별명을 획득한다. 획득한 정보를 이용하여 자신의 데이터베이스에서 일치하는 인증서 정보를 찾고 상태 검증을 수행한다.
(5) (4)번 과정 결과 일치하는 인증서 정보가 존재하지 않기 때문에 CA에게 해당 인증서에 대한 상태 검증을 요청한다. 전송되는 정보는 다음과 같다.

$$C_{VS} \| E_{KA}[CS_A \| CDN_A] \| E_K[M \| E_{KA}(H(M))] \| E_{KA}[K] \quad (2)$$

C_{VS}는 검증서버의 인증서, E_{KA}는 사용자 A의 공개키를 의미한다. 이때 검증서버의 인증서는 CA에게 상태검증을 수행하는 검증서버가 유효한 검증서버 임을 증명하기 위해 사용된다.

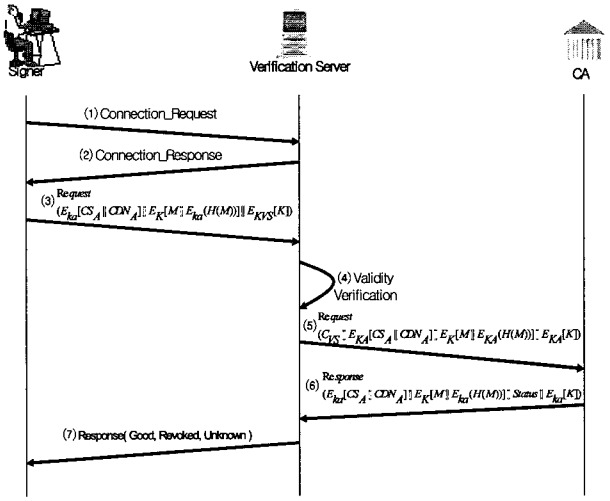
(6) CA는 처리결과를 검증서버에게 전송한다. 처리결과에 포함되는 정보는 다음과 같다.

$$E_{kz}[CS_A \| CDN_A] \| E_K[M \| E_{kz}(H(M))] \| Status \| E_{kz}[K] \quad (3)$$

Status는 인증서 상태 결과를 가지고 있다.

(7) 검증 결과를 서명자에게 전송한다. 이때 사용자에게 전송되는 응답 메시지는 인증서 상태 정보가 DB에 존재할 경우 인증서 상태검증 처리 과정과 동일한 Good, Revoked, Unknown 세 가지 값을 가진다.

인증서 정보가 데이터베이스에 존재하지 않을 경우에 상태 검증 처리 과정은 (그림 9)와 같다.



(그림 9) 인증서 상태 정보가 DB에 존재하지 않는 경우 인증서 상태 검증 처리 과정

4. 성능평과

4.1 실험

본 논문에서는 기존의 OCSP 기반의 인증서 상태 검증

방법과 제안하는 축약서명 기반의 인증서 상태 검증 기법 사이에 검증자수에 따른 검증속도에 대한 실험을 수행하였다. 또한 축약 서명 기법의 실험은 검증서버 데이터베이스에 인증서 상태 정보가 있을 경우와 없을 경우로 구분하여 실험을 하였다. 실험에 있어서 주요 요소는 검증을 요청하는 수에 따라 어떻게 처리속도가 차이가 있는가에 중점을 두고 실험을 하였다. 또한 실험범위는 각각의 기법에 대해 검증자수를 최대 200명으로 하였으며, 인증서 상태 검증을 총 600회를 수행하였다.

4.2 실험결과

<표 2>와 (그림 10)은 기존의 OCSP 기반의 인증서 상태 검증 기법과 제안하는 실시간 축약서명 기반의 인증서 상태 검증 기법의 수행 시간에 대한 실험 결과를 보여주고 있다.

(그림 10)에서 상단의 추세선은 기존의 OCSP 기반의 인증서 상태 검증 처리 결과를 보여주고 있다. 가장 하단에 있는 추세선은 제안하는 기법으로 검증서버 데이터베이스에 검증 요청한 인증서에 대한 상태 정보가 존재하는 경우이다. 이 경우는 검증서버 자체에서 상태 검증을 수행하고 바로 서명자에게 응답을 하기 때문에 다른 기법에 비해 속도가 빠른 것을 확인할 수 있다. 가운데 있는 추세선은 제안하는 기법으로 검증서버 데이터베이스에 인증서 상태 정보가 없는 경우이다. 하지만 클라이언트와 서버간의 검증요청 단계와 서버와 CA간에 검증요청 단계로 이루어지는 OCSP와 달리 제안하는 기법은 클라이언트가 존재하지 않기 때문에 클라이언트와 검증서버간의 노드가 줄어든다.

〈표 2〉 인증서 상태 검증 실험 결과

(단위 : 초)

실험기법 / 검증자수	OCSP	제안 기법 (DB에 데이터 존재)	제안 기법 (DB에 데이터 미존재)
1	0.3	0.10	0.18
10	0.87	0.32	0.45
20	1.01	0.44	0.57
30	1.18	0.53	0.69
40	1.26	0.64	0.84
50	1.37	0.75	0.97
60	1.45	0.85	1.11
70	1.55	0.94	1.22
80	1.69	1.03	1.27
90	1.84	1.11	1.33
100	1.92	1.18	1.42
110	1.98	1.23	1.49
120	2.04	1.28	1.58
130	2.10	1.33	1.66
140	2.19	1.39	1.72
150	2.27	1.42	1.76
160	2.32	1.49	1.81
170	2.38	1.57	1.87
180	2.45	1.64	1.93
190	2.50	1.70	1.98
200	2.54	1.75	2.03

즉 검증서버에서 직접 CA에게 인증서 상태 검증을 요청하고 수행 결과를 사용자에게 전송하기 때문에 OCSP에 비해 한번의 노드가 줄어들기 때문에 OCSP보다 빠르다는 것을 확인할 수 있다.

5. 결 론

기존의 OCSP 기반의 인증서 상태 검증 기법은 구조적인 집중화 문제와 불필요한 정보 전송 등으로 인한 네트워크과부하 병목현상이 발생한다. 그 결과로 인증서 상태 검증 수행시간이 오래 걸린다는 문제점이 있다. 따라서 기존의 OCSP 기반의 인증서 상태 검증 기법은 인증 시스템이 은행, 증권등과 같은 주로 실시간 응답시간을 중요시 하는 분야에 사용된다는 점에서 유효하지 않다.

본 논문에서는 기존의 중앙 집중형 서버 클라이언트 인증 시스템 구조를 도메인별로 분산된 단일 서버 형태로 구조를 변경함으로써 구조적인 집중화 현상을 해결했다. 또한 인증서 검증 요청시 불필요한 정보를 모두 전송하는 OCSP와 달리 인증서 상태 검증에 반드시 필요한 정보인 축약정보만을 이용하여 인증서 상태 검증을 요청함으로써 불필요한 정보 전송으로 발생하는 네트워크 과부하 통신 병목현상을 해결했다. 그 결과 기존 OCSP 기법보다 인증서 상태 검증에 소요되는 시간이 15% 가량 향상됨을 실험을 통해 확인할 수 있었다. 따라서 금융거래와 같이 실시간 응답시간이 중요시 되는 분야에 적용할 경우 기존의 시스템보다 인증서 상태 검증을 처리하는데 있어서 효과적으로 이용될 수 있다.

본 연구를 기반으로 향후 대규모 사용자가 동시에 검증요청을 하는 실제 시스템 즉 온라인 처리를 에 적용할 수 있도록 계속적인 연구의 필요성이 요구된다.

참 고 문 헌

[1] 김현철, 이용준, 백주호, 오해석, "서명자 정보를 이용한 인증서 상태 검증 기법," 2004년 정보과학회 춘계학술발표 논문집, Vol.31, No.1, 2004.

[2] Ray Hunt, "PKI and Digital Certification Infrastructure," Proceeding of the 9th IEEE International Conference on Networks, 2001.

[3] 칼리슬 아담스, 스티브 로이드 공저 | 장기식 역, "보안을 위한 효율적인 기법 PKI," 인포북, pp.51-67, 2003.

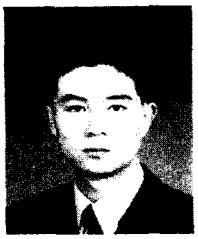
[4] RFC2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, 1999.

[5] RFC2560, Internet X.509 Public Key Infrastructure Online Certificate Status Protocol(OCSP), 2001.

[6] 정재동, 오해석, "실시간 인증서 상태검증의 성능개선," 정보처리학회논문지C, 제10-C권 제4호, pp.433-440, 2003.

[7] Barbara Fox & Brian LaMacchia, "Online Certificate Status Checking in Financial Transaction : The Case for Re-

issuance," Financial Cryptography, 1999. 02.
[8] 정재동, "CSMP 기반의 실시간 인증서 상태검증의 성능개선," 숭실대학교 박사학위 논문, pp.30-55, 2003.
[9] 심희원, 심영철, 임찬순, 이만희, 변옥환, "안전한 DNS에서의 효율적인 동적갱신과 존 전송 기능의 설계," 정보처리학회논문지A, 제7권 제1호, pp.99-114, 2000.
[10] RFC 3080, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile," 2002.
[11] 곽 진, 이승우, 조석향, 원동호, "온라인 인증서 상태 검증 프로토콜(OCSP)의 최근 연구 동향에 관한 분석," 정보보호학회 학회지, pp.50-61, 2002
[12] 이승우, 곽 진, 조석향, 주미리, 원동호, "실시간 인증서 검증 시스템 모델에 관한 연구," 2002년 정보처리학회춘계학술발표 논문집, 제9권 제1호, pp.833-836, 2002. 05.
[13] 고 훈, 장의진, 신용태, "PKI 환경의 OCSP 서버 부하 감소를 위한 OCSP 분산 기법," 정보보호학회 논문지, 제13권, 6호, pp.97-106, 2003. 12.
[14] draft-ietf-pkix-ocspv2-ext-01, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol, version2, 2002.

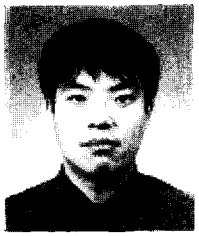


김 현 철

e-mail : dmzpolice78@korea.com
2003년 인제대학교 학사
2005년 경원대학교 석사
2005년~현재 경원대학교 박사과정
관심분야 : PKI, Home-Networking

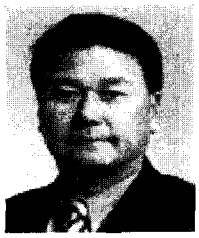
안 재 명

e-mail : retail@retailtech.co.kr
1988년 강원대학교 통계학과(학사)
1995년 성균관대학교 경영학과(석사)
2003년 숭실대학교 컴퓨터학과(박사수료)
2004년~현재 (주)리테일테크 대표이사
관심분야 : 통신보안, RFID, Ubiquitous Computing



이 용 준

e-mail : bigman2u@hotmail.com
1999년 강남대학교 전자계산학과(학사)
2001년 숭실대학교 컴퓨터학과 (석사)
2005년 숭실대학교 컴퓨터학과(박사)
관심분야 : 정보보호, 암호학, PKI



오 해 석

e-mail : oh@kyungwon.ac.kr
1975년 서울대학교 응용수학과(학사)
1981년 서울대학교 계산통계학과(석사)
1989년 서울대학교 계산통계학과(박사)
1982년~2003년 숭실대학교 컴퓨터학부 교수/부총장(역임)
2003년~현재 경원대학교 소프트웨어대학 교수/부총장
관심분야 : Multimedia, Database, 지식경영