DARC 기반에서의 실시간 인증서 유효성 검증에 관한 연구

장 홍 종[†] · 이 성 은[††] · 이 정 현[†††]

요 약

공개키 기반 인증시스템에서 사용자의 실수로 비밀키가 노출되었거나 자격의 박탈, 유효기간 만료 등의 이유로 인증서를 폐지해야 할 경우가 있다. 이에 따라서 각 사용자는 수신한 인증서가 유효한 것인지를 확인해야만 한다. 이 인증서 폐지 여부를 확인하는 방법으로는 CRL, Delta-CRL, OCSP 등의 방식이 개발되었다. 하지만 이 모든 방식에서의 인증서 유효성 검증은 실시간으로 처리해야 하므로 많은 통신량을 발생시키는 문제점을 가지고 있다. 본 논문에서는 CRL관리의 문제점인 전송시점 차이에 따른 무결성 문제와 실시간 처리로 인한 서버와 네트웍의 과도한 트래픽 발생을 해결한 DARC(DAta Radio Channel)를 이용한 효율적인 CRL 구축 방안을 제안하였다.

A Study on the Realtime Cert-Validation of Certification based on DARC

Hong-Jong Chang[†] · Seong-Eun Lee[††] · Jung-Hyun Lee[†††]

ABSTRACT

There are cases that revoke the certification because of disclosure of private key, deprivation of qualification and the expiration of a term of validity based on PKI. So, a user have to confirm the public key whether valid or invalid in the certification. There are many method such as CRL, Delta-CRL, OCSP for the cert-validation of certification. But these method many problems which are overload traffic on network and the CRL server because of processing for cert-validation of certification. In this paper we proposed the realtime cert-validation of certification method which solved problems that are data integrity by different time between transmission and receiving for CRL, and overload traffic on network and the CRL server based on DARC.

키워드 : 공개키 기반구조(PKI), 유효성 검증(Cert-Validation), FM 부가 방송(DARC), 폐인증서(CRL)

1. 서 론

지식 정보화 사회에서 각 분야의 비즈니스처리 환경은 종이문서위주, 대면위주의 처리방식에서 비대면 온라인 전자문서기반으로 전환되어 하나의 정보기술 공유기반 위에서 각종 정보와 서비스를 신속하게 제공하게 될 것이다.

그러나 네트웍을 통한 주요 문서 및 정보의 유통이 급격히 증가하게 됨에 따라 온라인 상에 노출되는 정보들에 대한 불법적인 도청, 위·변조 및 신분위장 등 각종 역기능에 의한 위협이 예상되고 있다.

이에 각국에서는 유통정보의 안전성·신뢰성 확보를 위해 각종 분야에 공개키 암호기술을 적용하여 당사자의 신원확인, 전자문서의 정보보호 및 무결성 보장, 전자행위에 대한 부인봉쇄 등을 제공하는 PKI(공개키 기반구조 : Public Key Infrastructure)를 구축하고 있다[1].

공개키 암호시스템은 공개된 사용자의 공개키가 그 소유자와 대응되는 지를 확신할 수 있어야 하며 그렇지 못할 경우 자신의 공개키를 다른 사람의 공개키로 위조할 수 있다. 이를 해결하기 위해 신뢰할 수 있는 제3자인 인증기관에서 각 사용자의 신분과 공개키를 확인한 후 공개키 확인서를 발급하고 사용자는 이를 검증하여 공개키 인증 문제를 해결한다. 그러나 사용자의 실수로 비밀키가 노출되었거나 자격의 박탈, 유효기간 만료 등의 이유로 인증서를 폐지해야 할 경우가 있다. 따라서 각 사용자는 수신한 공개키가 유효한 것인지를 확인해야 하며 이는 인증기관이 폐지된 인증서에 대한 정보를 공개하거나 사용자가 원하는 인증서의 상태를 인증기관에 직접 의뢰를 함으로써 알 수 있다[2]. 이 폐지 여부를 알 수 있는 가장 일반적인 방법으로 인증서 폐지 목록(CRL : Certification Revocation List) 방식이 있다. 이 방법은 간

† 정 회 원 : 행정자치부 전문위원
†† 정 회 원 : 행정자치부
††† 종신회원 : 인하대학교 전자전기컴퓨터공학부 교수
논문접수 : 2001년 8월 1일, 심사완료 : 2001년 10월 18일

단한 반면 확인서 폐지목록을 다운로드 해야하며, 파일의 크기가 커지는 단점이 있으며 목록에서 대상이 되는 인증서가 존재하는지 확인해야 하므로 많은 부하가 걸린다. 이를 개선하기 위해 전체 CRL을 다루지 않고 CRL이 발행된 시점에서 새로운 CRL이 발행된 시점까지의 목록을 모아둔 delta-CRL 방식이 있으나 이 또한 이전 목록은 저장하고 있어야 한다. 또한 인증기반의 확산으로 CRL, delta-CRL 모두 전송량이 늘어나고 있으며 전송시간 역시 일정시간의 간격을 두고 이루어지고 있어 많은 문제점이 발생되고 있다. 최근 이들의 단점을 보안하여 실시간으로 전송하도록 개선한 OCSP (Online Certification Status Protocol)라는 새로운 방식이 개발되었다. 하지만 이 방식은 인증서의 유효성 검증을 실시간으로 처리해야 하므로 많은 통신량을 발생시키는 또 다른 문제점을 가지고 있다. 본 논문에서는 이와 같은 CRL 관리의 문제점인 전송시점 차이에 따른 무결성 문제와 실시간 처리로 인한 서버와 네트워의 과도한 트래픽 발생을 해결한 DARC(DAta Radio Channel)을 이용한 효율적인 CRL 구축 방안을 제안하였다.

2. 주요 기반기술

2.1 PKI 인증기반

공개키 암호방식은 암호화 할 때 사용하는 암호화키와 복호화 할 때 사용하는 복호화 키가 서로 다른 암호방식으로서 암호화키를 공개하더라도 복호화 키를 찾아낼 수 없는 방식이다.

즉, 암호화 키(Public Key)는 전화번호부 또는 게시판과 같은 곳에 공개하여 누구나 쉽게 사용할 수 있게 하고 복호화키(Private Key)만을 자신이 비밀로 간직함으로써 복호화 키를 모르는 사람은 아무도 암호문을 평문화 시킬 수 없도록 하는 암호시스템 이다. 따라서 공개키 암호는 비대칭키 암호(Asymmetric Cryptosystem)라고도 불리며 통상 암호화키를 공개키로 복호화 키를 비밀키라 부른다.

공개키 암호방식의 개념은 1976년 미국 Stanford 대학의 Diffie와 Hellman이 발표한 논문 "New Direction in Cryptography"에서 처음으로 제시되었으며[3], 실질적인 공개키 암호방식은 Merkle과 Hellman이 제안한 Knapsack 암호시스템과 미국 MIT 대학의 Rivest, Shamir, Adleman에 의해서 제안된 RSA System이 초기에 나온 대표적인 공개키 암호라고 할 수 있다.

공개키 암호방식은 사용자가 아무리 증가하더라도 개인의 공개키와 비밀키 한 쌍만을 관리하면 되기 때문에 키 관리가 용이하며 상대방에게 최초의 공개키를 분배하는 것도 일반 통신수단을 사용하여 손쉽게 할 수 있다. 또한 공개키 암호방식의 중요한 장점은 전자문서의 무결성과 부인봉쇄기능을 갖고 있는 전자서명을 구현하는데 활용될 수 있으며 다양한 암호프로토콜에 사용될 수 있다는 것이다. 물론 모든 공개키 암호가 전자서명에 활용될 수 있는 것은 아니지만 메시지에 서명자의 비밀키를 사용하여 전자서명을 하고 수신자는 상대방의 공개키를 이용하여 서명자를 확인할 수 있도록 할 수 있다.

PKI는 <표 1>과 같은 5가지 기본 보안 서비스를 제공한다.

〈표 1〉 PKI 보안 기본 서비스

1. 위조불가 (Unforgeable) : 합법적인 서명자만이 전자서명을 생성할 수 있음
2. 서명자 인증 (User Authentication) : 전자서명의 서명자를 불특정 다수가 검증할 수 있어야 함
3. 부인방지 (Non-Repudiation) : 서명자는 서명행위 이후에 서명한 사실에 대해 부인할 수 없음
4. 변경불가 (Unalterable) : 서명한 문서의 내용을 변경할 수 없음
5. 재사용불가 (Not Reusable) : 전자문서의 서명을 다른 전자문서의 서명으로 사용할 수 없음

2.2 CRL 및 delta-CRL

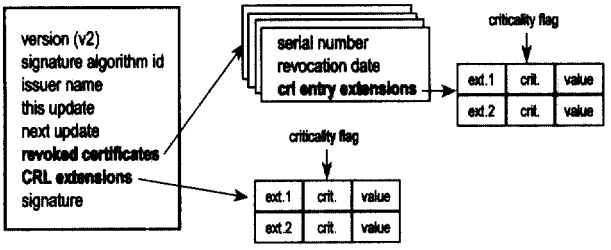
인증서 소유자가 단체를 떠나거나 개인키의 신뢰가 손상이 되었을 때 인증서를 폐지할 필요가 있다. 본 논문에서는 (그림 1)과 같은 X.509 V2 인증서 폐지목록이 인증서 폐지를 기준으로 제안한다[4].

인증서 폐지목록은 만료되지 않은 폐지된 인증서들의 목록을 포함한다. 인증서 폐지목록에는 갱신시간, 다음 갱신시간을 모두 포함하므로 사용자는 현재 갖고 있는 인증서 폐지목록이 가장 최근 것인가를 알 수 있다. 인증기관들은 발급된 인증서들에 대한 인증서 폐지목록을 주기적으로 갱신해야 한다. 인증서 폐지목록 분배를 위한 통신비용이 매우 높으므로 본 논문에서는 필요에 따라 클라이언트들이 인증서 폐지목록을 요청하는 PULL 분배 모델을 따르도록 한 방식을 기준으로 하였다. 클라이언트는 인증서 폐지목록을 조회하면 통신비용을 줄이기 위해 다음 변경시간까지 그 인증서 폐지목록을 캐쉬 하여 메모리에 갖고 있도록 한다.

주기적 폐지 방법은 인증기관이 정기적인 시간이내에서는 안전하게 인증서 폐지를 알릴 수가 없다.

이 제한을 극복하기 위해 즉시적 폐지 방법이 사용될 수 있다. 폐지 정보를 인증서 폐지목록 게시 시간주기에 제한받지 않고 사용자에게 바로 알릴 수 있으며 이를 위해 사용자는 인증서를 발급한 인증기관과 온라인 거래를 해서 인증서의 유효성을 검증해야 한다. 요청된 정보가 비인가된 사용자에 의해 변경될 수 없어야 하며 거래가 안전하게 이루어져야 한다. 이 방식으로 구현에서의 매우 큰 기반구조로 하는 것은 매우 어렵고 비용이 많이 든다. 신뢰된 서버나 보안 프로토콜 없이 인증기관이 결정하는 인증서 폐지목록 발급주기를 충분히 작게 하여 폐지 통지를 가능한 한 적절한 시기에 할 수 있도록 하여야 한다. 폐지목록이 많은 경우에 키 신뢰 손상을 인증기관에게 보고하는데 수시간 또는 수일의 지연

이 발생하며, 인증서 폐지목록 발급간격은 폐지목록 분배의 지연과 빈번한 갱신의 통신비용 사이의 균형을 이루도록 설정되어야 한다.



(그림 1) X.509 V2 인증서 폐지목록 구조

인증서 폐지목록이 도달할 수 있는 크기는 매우 중요하다. 만약 인증서 폐지목록이 매우 커지면 통신 및 처리 성능 면에서 큰 부담이 된다. 부담을 줄이기 위해 인증서 폐지목록에 있는 엔트리는 인증서가 만료되면 인증서 폐지목록으로부터 삭제된다.

일반적인 표준을 준용하는 인증기관은 두 종류의 인증서 폐지목록을 생성하여야 한다. 한 개는 사용자들을 위한 것이고 또 하나는 인증기관들을 위한 것이다. 인증기관을 위한 인증서 폐지목록은 매우 짧아 인증 경로를 처리하는데 매우 효율적이며 사용자 인증서 폐지목록은 받아들이기 힘들 정도의 크기로 커질 수 있다. 이 경우에 (그림 2)와 같은 X.509 확장을 이용하여 한 인증기관의 인증서들을 여러 개의 집단으로 나누고 각 집단을 1개의 인증서 폐지목록 분배점에 연관시킬 수 있다. 인증서 폐지목록 분배점은 자신의 인증서 폐지목록을 배포하는 디렉토리 엔트리를 갖고 있으며 X.509 확장을 이용하면 폐지 사유(이름변경, 키손상 등)에 따라 다른 인증서 폐지목록 분배점을 가질 수 있도록 할 수 있다. 인증서 폐지목록 확장영역 프로파일은 (그림 3)과 같다.

항 목		인 증 서					
		최상위 인증기관		인증기관		사용자	
		사용여부	C	사용여부	C	사용여부	C
Key Information	Authority Key Identifier			Y	F	Y	F
	Subject Key Identifier	Y	F	Y	F	Y	F
	Key Usage			Y	T	Y	T
	Extended Key Usage						
	Private Key Usage Period						
Policy Information	Certificate Policies			Y	O	O	O
	Policy Mappings			O	F		
Subject and Issuer Attributes	Subject Alternative Name			O	F	O	F
	Issuer Alternative Name			O	F	O	F
	Subject Directory Attributes						
Certification Path Constraints	Basic Constraints	Y	F	Y	T		
	Name Constraints			O	T		
	Policy Constraints			O	T		
CRL Identification	CRL Distribution Points			Y	O	Y	O

• 사용여부
Y - YES, 빈칸 - 사용하지 않음, O - 인증정책에 따라서 사용여부를 결정
• C(Criticality)
T - TRUE, F - FALSE, O - 인증정책에 따라 critical의 여부를 결정

(그림 2) 인증서 확장영역 프로파일

항 목		인증서 폐지 목록	
		사용여부	C
CRL Entry Extensions	Reason Code	Y	F
	Hold Instruction Code		
	Invalidity Date		
	Certificate Issuer	O	T
CRL Extensions	Authority Key Identifier	O	F
	Issuer Alternative Name	O	F
	CRL Number	Y	F
	Issuing Distribution Point	O	O
	Delta CRL Indicator	O	F

• 사용여부
Y - YES, 빈칸 - 사용하지 않음, O - 인증정책에 따라서 사용여부를 결정
• C (Criticality)
T - TRUE, F - FALSE, O - 인증정책에 따라 critical의 여부를 결정

(그림 3) 인증서 폐지목록 확장영역 프로파일

delta-CRL은 가장 최근 폐지된 인증서만을 포함하는 인증서 폐지목록이다. 즉, 가장 최근에 발급된 인증서 폐지목록에 포함된 폐지 인증서와 그 바로 직전에 발급한 인증서 폐지목록에 포함된 폐지 인증서와의 차이만큼을 포함하는 인증서 폐지목록이다. delta-CRL을 사용함으로써 클라이언트들의 인증서 상태 처리 시간과 CRL의 크기를 작게 개선할 수 있다. 이를 통해 이미 로컬 데이터베이스에 존재하는 기존 폐지 정보는 그대로 두고 추가로 폐지된 정보만 데이터베이스에 더하면 된다.

delta-CRL을 발급할 때에도 인증기관은 전체 인증서 폐지목록은 발급되어야 한다. 즉, delta-CRL은 전체 인증서 폐지목록 없이는 발급될 수 없다. delta-CRL과 전체 인증서 폐지목록의 인증서 폐지목록 번호 값은 동일해야 한다.

2.3 OCSP

2.2절에서 설명한 CRL과 delta-CRL 모두 인증서 폐지 목록의 갱신 주기성의 문제점을 갖고 있다. 최근 이와 같은 문제를 해결한 OCSP(Online Certificate Status Protocol)가 개발되었다.

또한 IETF의 PKIX 워킹 그룹(RFC2560)[5]에서 정의 중이며 효율적인 인증 처리 방법을 제공하는 것을 목적하고 있으며 기존의 CRL과 같은 정적 리스트 모델보다 다이나믹하게 처리한다. 즉, OCSP는 폐지 및 효력정지 상태의 파악이 정확하고 실시간으로 인증서를 검증하도록 개발되었다.

OCSP는 주로 데이터 트랜잭션 중요성이 매우 높아 실시간 인증서의 유효성 검증이 필요한 경우 사용될 수 있다. 예를 들어 고가의 증권정보, 고액의 현금거래 등이 이 경우에 해당된다. 하지만 이와 같은 방식이 있어서도 인증서의 유효성 검증을 실시간으로 처리해야 하므로 많은 트랜잭션과 서버에 대한 과부하를 발생시키는 문제점은 여전히 가지고 있다. 본 논문에서는 이와 같은 CRL 관리의 문제점인 전송시점 차이에 따른 무결성 문제와 실시간 처리로 인한 서버와 네트워크간의 과도한 트래픽 발생을 해결하고자 한다.

2.4 DARC

FM 부가방송은 하나의 FM 방송채널에 할당된 대역폭중 미 사용중인 53~100KHz의 대역에 음성 또는 디지털 데이터를 다중화하여 방송함으로써 FM 방송 수신자에게 부가적인 서비스 즉, 자동공조, 프로그램 자동선국, 시간정보, 교통정보, 날씨정보, 주식동향 등의 실시간 사회정보, 무선호출, 비상경보, 그리고 자동주행 시스템의 교통 데이터 제공등의 높은 부가가치의 서비스를 제공하는 부가적인 방송서비스를 지칭한다[6, 7, 8].

이러한 FM 부가방송은 80년대 초부터 유럽의 여러 국가가 산악과 같은 지리적인 장애로 인한 방송 전파송신의 어려움을 극복하고 집약구조의 방송망 활용도를 높이기 위해 개발되었다. FM 부가방송의 종류는 <표 2>와 같다[9].

〈표 2〉 부가방송의 종류

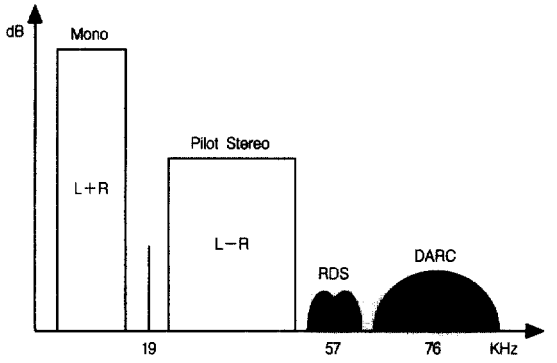
1. RDS(Radio Data System) : 유럽 및 대부분의 미국에서 상용화된 시스템
2. DARC(DAta Radio Channel) : 일본, 스위스, 프랑스, 독일 등에서 상용화된 시스템
3. HSDS(High Speed Subcarrier Data System) : 미국 일부 지역에서 상용화된 시스템

RDS는 전송속도가 1.187Kbps이므로 영상과 같은 많은 양의 데이터를 전송할 수 없다는 단점을 가지고 있다. 이를 극복하기 위해 개발된 방식이 DARC와 HSDS 이다. 국내에서는 DARC에 대한 연구가 진행되고 있으며 현재 문화방송에서 DARC에 대한 방송을 실시하고 있다[10].

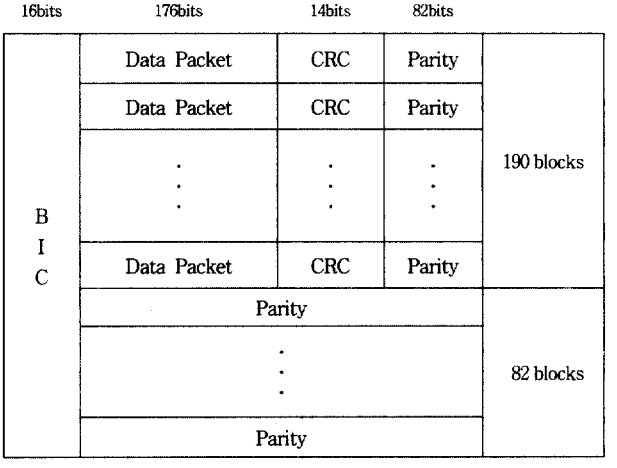
세계적으로도 DARC가 이미 1996년 세계표준인 ITU-R BS.1194로 채택되었다. DARC의 데이터 전송속도는 16Kbps로 전송 중 전송오류를 개선하기 위한 Parity를 제외한 정보전송속도는 9.78Kbps(C Frame, 데이터를 압축하지 않은 상태)를 유지한다.

DARC 시스템은 7계층의 OSI(Open System Interconnection) 참조 모델을 기본으로 한다. 이러한 OSI 참조모델을 기본으로 하여 DARC 시스템의 계층 구조는 시스템과 시스템간의 물리적인 접속을 제어하기 위한 기능을 제공하는 물리계층(layer 1), 물리적인 특성을 이용하여 데이터 전송에서의 오류검출과 복원 등을 수행하는 프레임 구조 계층(layer 2), 시스템간의 데이터 교환 기능을 제공하는 것을 목적으로 하는 데이터 패킷 계층(layer 3), 종단 시스템간의 데이터 전송에 관한 오류 검출, 복원 및 다중화 등을 제공하는 데이터 그룹 계층(layer 4), 데이터의 제어 및 동기를 수행하는 세그먼트 계층(layer 5), 데이터의 형식 처리를 수행하는 표시계층(layer 6), 응용 프로세서간의 정보교환 기능을 위한 응용계층(layer 7) 등으로 구성된다[11]. 물리계층은 (그림 4)과 같다.

0~53KHz는 기존의 FM 스테레오 신호에 할당되며 그 밖의 미사용 대역폭인 53~100KHz는 다중 데이터 신호를 배치한다. 프레임 구조 계층은 데이터 전송에 관계된 프레임 동기, 데이터 포맷, 오류에 대한 보호 그리고 스크램블링을 제공한다. (그림 5)는 프레임 계층의 구조이다.



(그림 4) 기저대역의 DARC 부반송파 스펙트럼



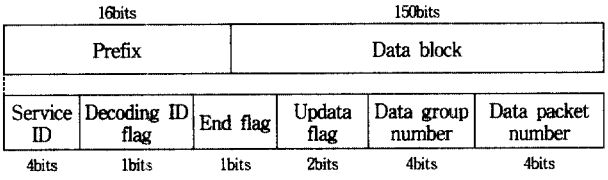
(그림 5) 프레임 계층 구조

데이터 패킷 계층은 서로 다른 3개의 채널로 구성된 데이터 패킷과 논리채널로 구성된다. 이 3가지 형태는 서비스 ID에 의해 구별되며 서비스 채널, 단(short) 메시지 채널, 장(long) 메시지 채널로 나누어지며 각 채널의 데이터 패킷은 176비트로 구성된다. 이에 대한 구조는 (그림 6)와 같다.

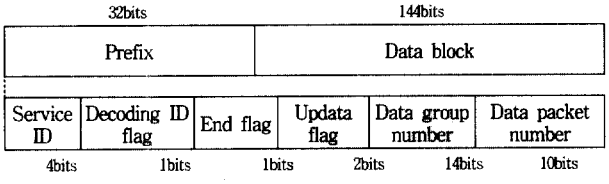
데이터 그룹 계층은 서비스 메시지, 단 메시지, 장 메시지의 서로 다른 3개의 메시지에 의해서 구분되는데 각 데이터 그룹은 하나 혹은 여러 개의 데이터 블록으로 구성된다. 데이터 그룹 계층의 구조는 (그림 7)과 같다. 일반 문자와 그래픽 정보는 데이터로서 전송되며 수신기를 위한 부가정보는 세그먼트로서 전송된다. 이는 부가정보의 길이가 1비트 혹은 10비트 정도로 짧기 때문이다.

프로그램은 복수개의 페이지들로 구성되며 프로그램 제어 데이터와 페이지 데이터들로 구성된다. 세그먼트 정보가 담겨 있는 세그먼트 데이터부와 정보를 지칭하고 그 길이를 표시해주는 세그먼트헤더부로 구성된다. 표시 계층은 표시 스크린 포맷과 문자형태, 사진표현법, 지리명령형식 및 다른 항

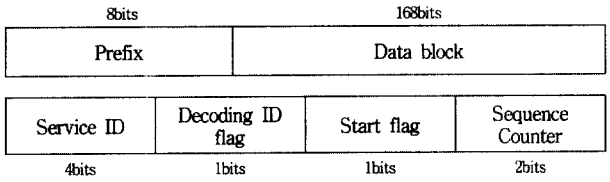
목 등을 규정한다. 응용 계층은 뉴스, 일기예보, 주식정보 등의 부가정보를 전송한다.



(a) Service Channel

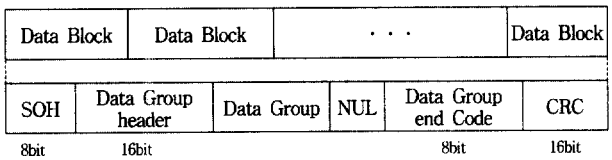


(b) Service Message Channel

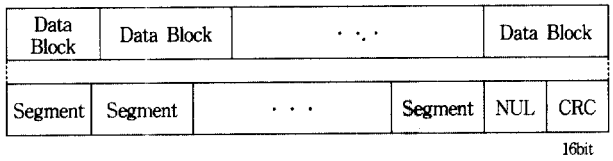


(c) Long message Channel

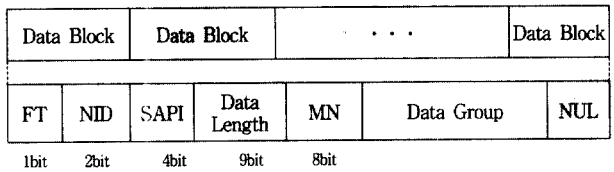
(그림 6) 테이터 패킷 구조



(a) Service message



(b) Short message



(c) Long message

(그림 7) 데이터 그룹 구조

3. 제안 시스템

3.1 CRL전송 및 수신

DARC을 이용한 CRL 전송 시스템에서 전송될 CRL의 유무를 체크하고 발생시 CRL을 DARC 서버에 송신한다.

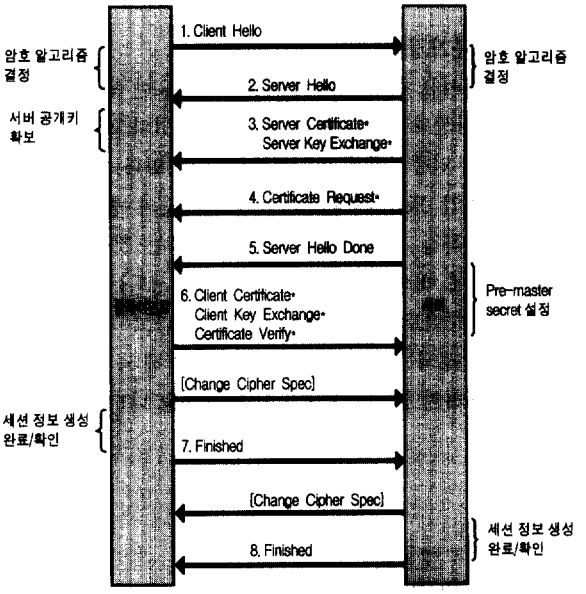
인터넷상에서 제공되는 데이터 중에서도 상호보안이 유지되는 상태에서 전송되어야만 하는 경우가 존재한다.

예를 들어 전자상거래나 온라인 뱅킹, 인증기관에 이르기까지 정보가 누출되어서는 안 되는 경우가 있다. 이러한 경우에는 일반적으로 사용되어지는 HTTP protocol이 아닌 특별한 종류의 protocol을 필요로 하며, 가장 널리 사용되어지는 방법이 SSL을 이용한 HTTP protocol이다. SSL 서버에서 제한된 클라이언트에게만 접근을 허용하는 경우에도 사용되어진다.

예를 들어 서버는 클라이언트에게 인증서를 요구할 수 있으며, 클라이언트의 인증서를 바탕으로 하여 접근여부를 판단할 수 있다.

이에 따라 본 논문에서도 DARC서버에 CRL 전송에는 CA의 CRL전송서버와 DARC서버간에 SSL을 이용하여 안전하게 전송한다.

CRL서버를 클라이언트, DARC서버를 서버라 하면 SSL을 이용한 클라이언트와 서버간의 전송 Operation은 크게 (그림 8)과 같은 순서로 이루어진다.



(그림 8) CA CRL 송신 서버와 DARC 서버와의 핸드쉐이크

첫째, 클라이언트는 서버에게 Client Hello message를 전송한다.

둘째, 서버는 클라이언트에게 Server Hello message와 서버인증서를 전송하고. 만약 클라이언트인증서가 필요한 경우에 인증서 요청도 함께 전송한다.

셋째, 클라이언트는 암호화에 사용되는 세션키와 함께 클라이언트에서 지원하는Cipher Suite를 서버로 전송. 서버가 인증서를 요청한 경우에는 클라이언트의 인증서도 함께 전송한다.

넷째, 클라이언트는 Finished message를 서버로 전송하고 데이터 전송단계로 이동한다.

다섯째, 서버는 Cipher Suite를 받아들이고(또는 거부하고) Finished message를 클라이언트로 전송한 후 데이터 전송단

계로 이동하고 상호 합의한 Cipher Suite에 의해서 암호화된 메시지를 교환한다.

이러한 절차에 따라 DARC서버에 수신된 CRL은 DARC 송신 시스템에 의해 브로드 캐스팅 된다. CRL 전송은 1시간 간격으로 전체 CRL을 브로드캐스팅하고 발생하는 CRL은 발생 즉시 브로드캐스팅 한다.

DARC에 의해 브로드캐스팅된 CRL은 DARC 수신기에 의해 수신되고 세션키로 복호화된 후 데이터베이스에 저장된다.

3.2 인증서 유효성 검증

데이터베이스화된 CRL은 수신된 인증서의 확인을 위해 사용된다. 전송된 인증서의 유효성을 검증하기 위해서는 현재상태의 CRL을 필요로 한다. 인증서발급번호로 로컬 데이터베이스에 저장된 CRL을 확인하고 인증서의 유효성 여부를 확인한다. 본 논문에서 제안하는 시스템의 구성도는 (그림 9)와 같다

3.3 실험 및 평가

3.3.1 기본가정

본 논문에서는 통신량을 분석할 때 필요한 인증기관의 구성은 하나 이상의 인증기관이 존재할 수 있다고 가정하며 디렉토리는 각 인증기관에 속해 있을 수도 있다. 즉, 인증기관과 디렉토리간 또는 사용자와 디렉토리간의 통신량을 생각할 때 어느 특정 디렉토리를 대상으로 하는 것이 아니고 전체 디렉토리에 대해서 네트워크 상에서 발생되는 통신량을 고려한다. 즉, 디렉토리가 전체에 하나가 있다고 가정하는 것과 동일하다. 발생되는 통신량을 분석하기 위해 <표 3>과 같은 표기를 사용하며 1일을 기준으로 통신량을 나타낸다. 일반적으로 인증서가 폐지되는 비율은 10% 정도로 한다[12].

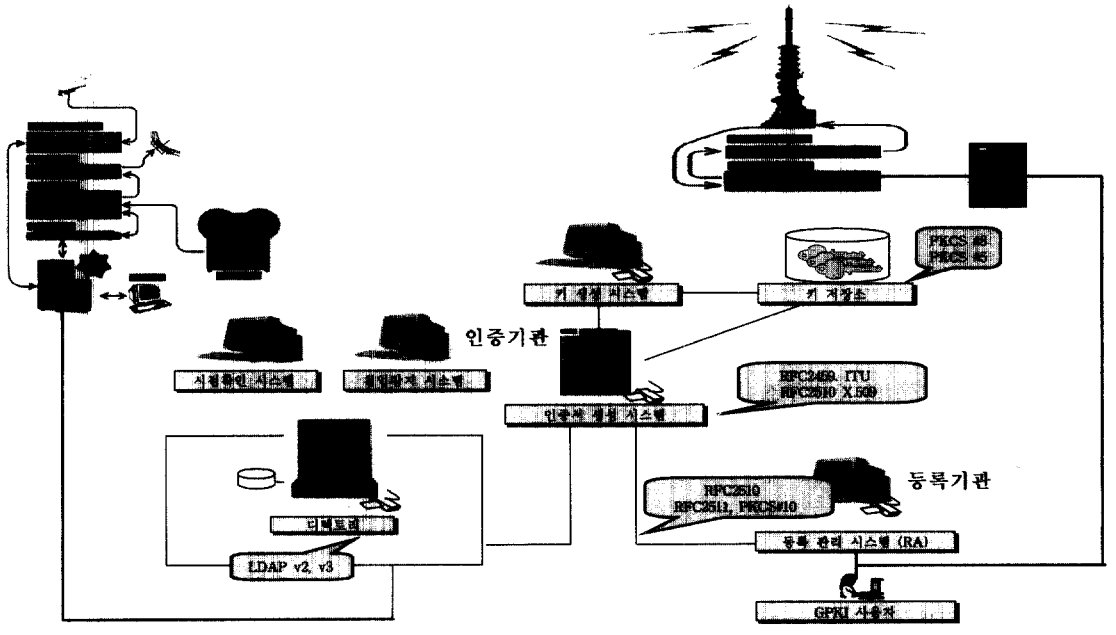
3.3.2 실험 및 평가

요구되는 통신량을 계산해보면 인증기관과 디렉토리사이에는 하루에 폐지된 인증서에 대해서 갱신 횟수만큼 목록을 전송해야 하므로 <표 3>과 같은 표기 방법으로 도식화하면 $T \times r \times l = T \times n \times p \times l$ 만큼의 비트를 전송해야 하며 디렉토리가 1일 동안 사용자들에게 전송해야 하는 양은 $q \times p \times k \times l$ 비트이다.

〈표 3〉 표 기

n	전체 총 인증서의 수
k	한 인증기관에 속한 평균 인증서 수
p	폐지되는 인증서의 비율
r	폐지된 인증서의 수($r = n \times p$)
T	폐지리스트의 1일 갱신 횟수
l	인증서의 일련번호를 나타내는 비트 수
q	사용자들이 인증기관에 인증서의 유효 여부를 질의하는 횟수(일)

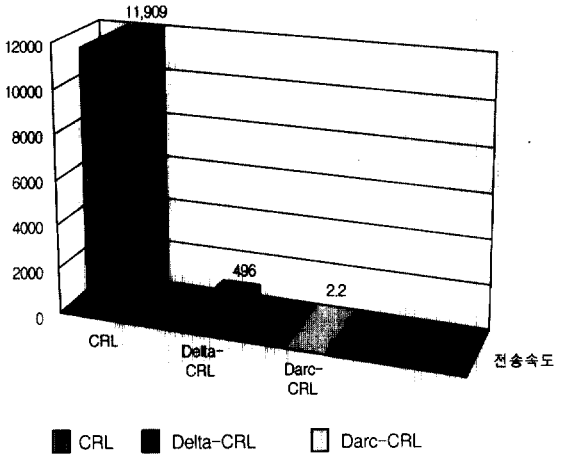
한 인증기관에 속한 평균 인증서 수가 3,500만건 취소되는 인증서의 비율을 10%라고 하면 폐지되는 인증서의 수는 350만건, 폐지리스트의 1일 갱신 횟수를 12회, CRL의 크기를 35byte, 사용자들이 인증기관에 인증서의 유효여부를 질의하는 횟수를 350만회라 하면 기존의 CRL 방식의 전체 전송량은 350만 $\times 0.1 \times 3{,}500$만 $\times$ 35byte = 428.75 Tbyte이다. 10Mbps로 전송한다면 전체전송시간은 11,909시간이다. 또한 delta-CRL 방법으로 전송 시에도 전체 전송량 중 시간당 145,833건 발생하고 이를 다시 24시간을 기준으로 계산하면 18Tbyte가 되며, 만약에 10Mbps로 전송한다면 전체 전송시간은 496시간



(그림 9) 제안시스템 구성도

이다. 실제의 전송속도는 네트워크 부하나 시스템의 부하에 의해 더욱더 나쁜 결과를 도출한다.

본 논문에서 제안한 방법은 인증서가 폐지될 때마다 실시간으로 전송되고 한번의 전송으로 가정한 350만의 사용자에게 브로드캐스팅되므로 실제 전송량은 350만건×35byte = 122.5Mbyte 이다. 16Kbps로 전송시 2시간 13분이면 전송을 완료할 수 있다. 이것은 시간당 145,833건의 CRL이 발생한 것과 같으며 이것의 전송은 약 5.4분만에 전송이 가능하다. 이 들의 전송시간을 비교하면 (그림 8)과 같다. 또한 검증을 위해 폐지목록을 다운 받기 위한 대기시간 없이 즉시 검증도 가능하다.



(그림 10) 전송시간 비교도

CRL과 delta-CRL은 전송주기에 따른 자료의 무결성이 발생하나 본 논문에서 제안한 방법은 실시간으로 인증서의 유효성을 검증할 수 있다. 또한 CRL의 확장 필드를 이용하여 그룹을 분리하여 이용자가 필요한 그룹을 선택적으로 수신할 수 있어 이용자에게 더욱 더 효율적인 방법을 제공할 수 있다.

이를 위한 프로파일은 <표 4>와 같이 구성하였다.

〈표 4〉 Darc-CRL 프로 파일 추가 부분

Field	C	CRL	비고
darcCRLGroup	O		추가
CRLGroupIdentifier			추가
FrequencyIdentifier			추가
CRLClassification			추가

(1) darc 사용 확인 필드(Darc CRL Group)
darc의 사용 유무를 확인한다. 이 필드는 시스템 구성에 따라 사용여부를 결정한다.

(2) 그룹 분류를 위한 필드(CRL Group Identifier)
이 필드는 CRL이 필요한 그룹을 분리 서비스가 가능하도록 한다.

(3) 주파수 구분필드 (Frequency Identifier)
주파수 대역의 확인용 필드이다.

(4) CRL 구분 필드(CRL Classification)
이 필드는 CRL 과 Delta-CRL을 구분 하는 필드이다.

각각의 CRL에 대한 비교는 <표 5>와 같다.

〈표 5〉 기존의 CRL과 DARC-CRL의 비교표

구 분	CRL	Delta-CRL	OSCP	Darc-CRL
전송방식	유선 네트워크	유선 네트워크	유선 네트워크	FM
전송주기	클라이언트 요청시	일정주기	실시간	실시간
자료의 무결성	보장못함	보장못함	보 장	보 장
네트워크 부하	과 도	과 도	보 통	없 음
응답지연	과 도	과 도	보 통	없 음
최종 CRL 보관 장소	클라이언트	클라이언트	CRL서버	클라이언트
전송방법	요구시 CRL 전송	일점시점 전송	요청시 전송	즉 시
전송내용	전체 데이터필드	전체 데이터필드	데이터 프래그	전체데이터 or 프래그

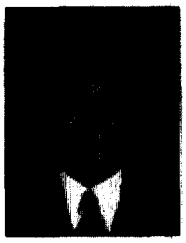
4. 결 론

본 논문에서는 CRL관리의 문제점인 전송시점 차이에 따른 무결성 문제와 실시간 처리로 인한 서버와 네트웍의 과도한 트래픽 발생을 해결하기 위하여 DARC를 이용한 인증서 유효성 검증방안을 제안하였다. 또한 현재 제안되어진 인증서 유효성 검증방법의 장단점을 분석하여 각각의 단점을 배제하고 장점을 수용한 방법을 제안함으로써 효율적인 인증서 유효성 검증 체계를 제안하였다.

참 고 문 헌

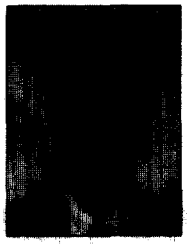
[1] ITU-T Recommandation X.509 (1997) ISO/IEC 9594-8. 1997, Information Technology-Open Systems Interconnection The Directory : Authentiation Framework, 1997.
[2] IETF, Online Certification State Protocol.
[3] W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory, IT-22* (6) : 644-654, November 1976.
[4] R. Housley, W. Ford, W. Polk, and D. Solo, RFC2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999.
[5] RFC2560 , Internet X.509 Public Key Infrastructure Online Certificate Status Protocol(OCSP)-Version 2.0L. Draft-ietf-pkix-ocspv2-02.txt, March 2001.
[6] Linda Zeger, "Analysis and simulation of Multipath Interference of FM Subcarrier Digital Signal," *Proc. of the third IEEE Symposium on Computer and Communication*, pp. 35-41, June 1998.
[7] Irving S. Reed, Xuemin Chen, "Error-Control coding for Data Networks," *KAP*, 1999.

[8] P, Scomazzon, R. Andersson, "SWIFT EU 1197-A multi-applicative services using a high rate data system implemented in the Terrestrial FM Radio Network," *Proc. of the 5th IEEE International Symposium on the Personal Indoor and Mobile Radio Communication*, Vol.1, September, 1995.
[9] "United States RBDS Standard," *National Radio System Committee*, 1998.
[10] "FM 다중방송 연구보고서", MBC, 1996.
[11] 강창언, 김산령, "데이터통신이론", 대영사, 1998.
[12] S. Micali, Efficient Certificate Revocation Technical Memo MIT/ LCS/TM-524b, 1996.



장 홍 종

e-mail : realking@gcc.go.kr
1992년 한양대학교 전자계산공학과(공학석사)
2000년 인하대학교 전자계산공학과(박사수료)
1983년~1998년 (재)건설기술교육원 전산실장
1993년~2000년 인천전문대학교 강사
1995년~1998년 수원과학대학 겸임교수
1998년~1999년 썬버드 전산부장
1999년~2000년 인하대학교 강사
1999년~2000년 경인여자대학 겸임교수
2000년~현재 성결대학교 겸임교수
2000년~현재 행정자치부 전문위원
관심분야 : 정보보안, 정보보호시스템 평가, 음성인식, 암호학, 스마트카드, HCI



이 성 은

e-mail : pinetree@gcc.go.kr
1987년 한양대학교 졸업(공학사)
1992년 한양대학교 산업대학원 전자계산학(공학석사)
2001년 건국대학교 대학원 컴퓨터정보통신공학과(박사과정)
1990년~1996년 (주)대상, 아주대학교의료원, 중앙일보
1996년~현재 행정자치부
관심분야 : 정보보안, 암호학, 스마트카드, 지불시스템, 뉴럴네트웍

이 정 현

e-mail : jhlee@dragon.inha.ac.kr
1977년 인하대학교 전자공학과 졸업
1980년 인하대학교 대학원 전자공학과(공학석사)
1988년 인하대학교 대학원 전자공학과(공학박사)
1979년~1981년 한국전자기술연구소 시스템 연구원
1984년~1989년 경기대학교 전자계산학과 교수
1989년~현재 인하대학교 전자전기컴퓨터공학부 교수
관심분야 : 자연어처리, HCI, 정보검색, 음성인식, 음성합성, 컴퓨터구조, 정보보안