通信情報保護學會論文誌
第 6 卷 第 1 號, 1996. 3

보안 서비스를 적용한 LAN의 성능 평가*

김 회 림**, 채 기 준***

Performance Evaluation of LAN with Security Services*

Hoe Rim Kim**, Ki Joon Chae***

요 약

LAN의 사용이 증가하면서 정보의 정확성과 전달 속도뿐만 아니라 신뢰성이 점점 더 중요해짐에 따라 보안 서비스를 LAN에 적용하는 것이 필요하게 되었다. 그러나, 정보 보호를 위해 보안 서비스를 적용하여 정보를 LAN을 통해 교환할 경우 메시지 전달 지연 시간이 길어지고, LAN의 처리량에도 영향을 미치게 된다. 따라서 적용되는 암호 시스템과 전체 정보량에서의 암호화 정보량이 LAN의 성능에 미치는 영향을 미리 예측하는 것이 중요하다.

본 논문에서는 이와 같은 필요성에 의해 보안 서비스를 LAN 상에 적용할 수 있는 방법을 제시하기 위해서 Ethernet, Token Ring, FDDI를 사용하였고, DES, Knapsack, RSA와 같은 암호 시스템을 적용하였다. 이와 같은 다양한 LAN 환경과 그에 적용할 암호 시스템을 선택하여 교체 적용함으로써 여러 가지 다른 조건의 환경에서의 성능을 평가할 수 있는 보안 서비스가 적용된 LAN의 시뮬레이션 모델을 개발하였다. 또한 이러한 시뮬레이션 모델을 이용하여 보안 서비스를 LAN에 적용했을 때의 성능을 평가하였다.

Abstract

As local area networks have been proliferated at increasing pace, reliability of information has been important as well as accuracy and speed. As a result, providing security service to LAN is required. However, since message transfer delay is getting longer and throughput of LAN is affected when secure encryption systems are applied to LAN to provide security services, it is desirable to apply them after considering their effects for performance of LAN.

---

* 이 논문은 1994년도 이화여자대학교 교내 연구비의 지원에 의하여 이루어졌음

** LG 전자 미디어 통신 연구소

*** 이화여자대학교 전자계산학과

In this paper, the method to apply security services to LAN is proposed and simulation model is developed to evaluate performances of LANs with security services. In the model, Ethernet, Token Ring and FDDI are used for LAN and encryption systems such as DES, Knapsack and RSA are appiled to the LANs. Using this simulation model, performances of the LANs are analyzed for the various parameters such as the degree of the encryption, message interarrival time, message length, the type of encryption system, etc.

1. 서 론

급변하고 있는 정보화 사회에서 컴퓨터 사용이 증가하면서 필연적으로 네트워크를 이용한 정보 교환이 증가하고 정보가 다양해짐에 따라 정보전달의 속도뿐만 아니라 신뢰성이 점점 더 중요해 지고 있다. 모든 분야에서 상호 전달되어야 하는 정보 중에는 비밀성을 유지해야 하는 정보가 있을 수 밖에 없다. 이러한 정보를 네트워크를 통하여 전달하기 위해서 정보의 보호를 위하여 정보를 암호화하고 암호화된 정보를 인정된 사용자만이 해독하여 정보를 안전하게 활용하는 보안 서비스가 네트워크에 적용되어져야 한다.

특히, 1970년대 후반 Ethernet이라는 근거리 통신망(Local Area Network: LAN)이 처음 소개된 후 LAN의 사용자는 전세계적으로 급속한 속도로 증가하였고, 국내에서도 1980 년대 중반 이후 LAN의 보급이 급격히 증가하는 추세이다. 현재 상호간의 빈번한 정보 교환이 LAN을 통해 이루어지고 있기 때문에 전달되는 정보의 보호가 LAN에 적용되는 것이 우선적으로 요구된다. 그러나, 정보 보호를 위해 보안 서비스를 적용하여 정보를 LAN을 통해 교환할 경우 정보가 발생해서 전송된 후 모든 처리가 끝날 때까지의 시간인 메시지 전달 지연 시간이 길어지고, LAN의 처리량에도 영향을 미치게 된다. 그러므로, 각 사용자의 환경에 맞는 암호 시스템을 선택하고, LAN 성능의 적정 수준을 유지하기 위해 전송되어야 하는 전체 정보 중에서 보안이 필요한 정보의 양을 조절하려면, 적용되는 암호 시스템과 전체 정보량에서의 암호화 정보량이 LAN의 성능에 미치는 영향을 미리 예측하는 것이 중요하다.

그러나, 이러한 예측을 할 수 있는 기존의 연구 결과가 없었고 기존의 단순한 LAN 만의 성능 평가를 이용해 원하는 결과를 얻을 수는 없다. 기존의 연구된 LAN에 대한 분석적 모델들은 분석을 위한 가정에 있어서 너무 제한적이어서 다양한 네크워크 환경에 적용할 수 없다.[1] 또한 기존의 LAN에 대한 시뮬레이션 모델을 이용한 성능 평가도 LAN 상에서의 단순한 정보 교환시의 성능 평가만을 고려한 것이기 때문에 보안 서비스를 적용했을 때의 성능을 평가할 수 없다.

이러한 필요에 의해 본 논문에서는 IEEE 802.10에서 제안하고 있는 보안 서비스를 LAN 상에 적용하기 위한 방법을 제시하였고, 다양한 LAN 환경과 그에 적용할 암호 시스템을 선택하여 교체 적용함으로써 여러 가지 다른 조건을 갖는 환경 하에서의 성능을 평가할 수 있는 보안 서비스가 적용된 LAN의 시뮬레이션 모델을 개발하였다. 또한 이러한 시뮬레이션 모델을 이용하여 보안 서비스를 LAN에 적용했을 때의 성능을 평가하여 보았다.

본 논문에서는 ISO, IEEE, ANSI 등에 의해 표준화가 되어 있고, 현재 국내외적으로 가장 널리 사용되어지고 있는 LAN인 Ethernet[2], Token Ring[3], FDDI (Fiber Distributed Data Interface)[4]에 보안 서비스를 적용하기 위해 LAN의 LLC (Logical Link Control)[5] 계층과 MAC(Medium Access Control) 계층 사이에 IEEE 802.10 SILS[6][7](Standard for Interoperable

LAN Security)의 제안에 따라 SDE(Secure Data Exchange) 계층을 둔 프로토콜을 사용하는 프레임 구조를 채택했다. 암호 시스템으로는 대표적인 단일키 암호 시스템인 DES (Data Encryption Standard)[8] 시스템과 공개키 암호 시스템인 Knapsack[9]과 RSA[10] 시스템을 적용하였다. 암호 시스템 적용시 필요한 키를 얻는 방식으로는 LAN이 WAN에 비해 접속된 스테이션의 수가 적고 LAN을 사용하는 접속자가 이미 일정 목적을 공유하며 그룹화되어 있다는 특성을 고려하여 LAN에 적합한 중앙 집중식 키분배 방식을 선택했다. 또한 각 암호 시스템을 적용하기 위해서 각 시스템을 수행하는데 드는 수행 명령어의 수를 구하였다. 이 수행 명령어의 수를 구하기 위해 암호 시스템을 C 언어로 프로그래밍하여 어셈블리어로 된 프로그램으로 번역하였다. 기계 독립적인 C 언어로 작성했기 때문에 모든 기계에서 쉽게 어셈블리 코드의 명령어로 변환하여 수행 시간을 계산할 수 있다. 암호 시스템을 적용하여 수행하고자 하는 기계의 하나의 명령어를 수행하는 데 드는 시간인 1 basic cycle time을 알면 실제 수행 시간을 구할 수 있어 시뮬레이션 모델에 적용된다. 위와 같은 보안 서비스를 적용한 LAN에서의 정보의 교환을 시뮬레이션할 수 있는 모델을 개발하기 위해서 시뮬레이션 언어인 SLAM II를 사용하였다. 이러한 시뮬레이션 모델에서 메시지 전달 지연 시간과 처리량에 영향을 주는 파라미터를 변화시키면서 보안 서비스를 LAN에 적용하였을 때의 결과를 분석하였다.

본 논문의 구성은 2장에서 보안 서비스를 적용하는데 있어 이론적 바탕이 되는 SDE, 키 분배 방식, 암호 시스템 구현을 위한 Multiple-precision 연산에 대하여 간단히 살펴보고, 3장에서는 시뮬레이션 모델의 설계와 구현에 대하여 설명한 다음 4장에서 시뮬레이션 결과를 분석하고 마지막으로 결론을 맺고자 한다.

2. 이론적 고찰

2.1 SDE

IEEE 802.10 SILS에서는 LAN 상에 보안 서비스를 제공하기 위하여 IEEE 802.2에서 정의된 LLC 계층과 LAN의 종류에 따라 IEEE 802.3, 802.4, 802.5 등에 의해서 정의된 MAC 계층 사이에 SDE라는 새로운 계층을 첨가하였다.

SILS에서 정의하고 있는 SDE PDU 구조는 그림 1에서 보는 바와 같으며, SDE PDU에 대한 기능과 각 필드의 길이는 다음과 같다.

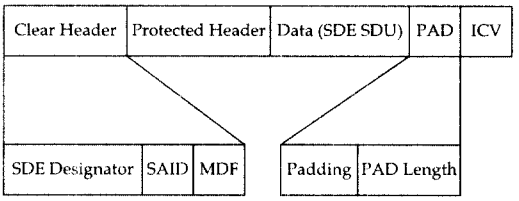


그림 1. SDE PDU의 구조

- Clear Header
  SDE PDU를 식별하고 PDU에 있는 정보의 처리를 도와주며 선택적으로 사용되어질 수 있다.
  - SDE Designator : LLC 개체를 포함하지만 SDE가 아닌 개체는 SDE PDU를 처리할 수 없도록 한다. Clear Header가 사용되면 필수적으로 있어야 하며, 길이는 3 옥텟이다.
  - SAID (Security Association Identifier) : Clear Header가 사용되면 필수적으로 있어야 하며, 길이는 4 옥텟이다.
  - MDF (Management-Defined Field) : 선택적으로 사용되어질 수 있으며, 최대 길이는 20 옥텟이다.
- Protected Header
  선택적으로 사용되어질 수 있고, 보안

서비스가 제공되는 부분으로 전송을 시작하는 스테이션을 나타내는 Station ID 필드로만 구성되며, 길이는 8 옥텟이다.

- Data
  LLC 계층으로부터 SDE 계층으로 보내진 정보로 보안 서비스가 제공되어지지 않을 때에는 이 데이타가 MAC 계층으로 보내진다.
- PAD
  암호화 알고리즘이나 특정 비밀유지나 데이타 무결성 알고리즘 적용시 어떤수의 정수배의 옥텟이 필요하다. 이러한 목적을 위하여 최대 255 옥텟까지의 Padding 필드를 사용할 수 있고, 그 길이는 1 옥텟의 PAD length 필드에 의해서 명시된다.
- ICV (Integrity Check Value)
  데이타 무결성 서비스가 제공되어질 때에 데이타 수정을 감지하기 위하여 선택적으로 사용되어지는 필드이며, Protected Header, Data 필드, PAD 필드에 대해 계산되어진다.

2.2 키분배 방식

공개키 방식에서 암호화 알고리즘과 공개키는 공개되지만 단일키 암호화 방식의 공통키와 공개키 방식에서 복호화 키는 비밀을 유지해야 한다. 따라서 비밀을 유지해야 하는 암호키의 관리가 매우 중요한 과제이다. 암호키 관리는 키 생성, 키분배, 키유지의 분야로 나누어질 수 있는데 암호 통신망 가입자가 아닌 제삼자에게 노출되지 않도록 어떻게 안전하게 키를 분배할 것인가가 네트워크를 통해 정보를 전달할 때 가장 큰 문제이다[11].

전통적으로는 중앙의 키 생성 센터에서 키를 생성하여 사람이 직접 키를 전달하는 방법을 사용하여 왔다. 그러나, 이러한 키분배 방법은 암호 통신망 가입자 증가에 따른 보조를 맞출 수 없고 보안의 안전성을 위해 키 변경이 빈번히 요구되어지는 경우에는 더욱 부적합할 뿐만 아니라 시간 지연이 가장 큰문제이다. 따라서, 암호화에 사용될 키도 네트워크를 이용해서 분배되어지는 것이 더욱 편리하다. 물론 교환되어질 키 자체도 보안이 유지되어져야 한다.

네트워크를 통해 암호키를 분배하기 위해 여러 암호키분배 방식이 제안되어 왔다. 단일키 암호 방식에서는 암호 통신망 가입자 증가에 따른 암호키 증가 문제를 해소하면서 키분배의 동시성을 갖는 암호키분배 방식으로 키분배소(KDC : Key Distribution Center)를 이용한 방식과 이산 대수 문제를 이용한 공개키 분배 방식이 제안되었다. 또한 공개키 암호화 방식에서 암호키를 등록한 공개 화일의 관리 문제를 해결하기 위한 방안으로 ID 정보에 의한 키분배 방식이 제안되었다. 키분배소를 두는 방식은 단일키 암호 방식과 공개키 암호 방식 모두에 적용 가능한데 통신망 내의 모든 대화키 생성과 분배의 기능을 수행하는 키분배소를 전체 통신망에 하나만 두는 중앙 집중식 키 관리 센터 방식과 키분배와 관리의 역할을 계층적으로 구성된 키분배소에게 분산시키는 계층적 키 관리 센터 방식, 각 사용자가 키분배소의 역할을 수행하는 완전 분산식 키 관리 방식이 있다.[12][13]

본 논문에서는 LAN에 보안 서비스를 적용하는데 있어 중앙 집중식 키 관리 센터 방식을 다음과 같은 이유에서 채택하였다. 키 관리 센터를 이용하는 방식은 널리 사용되고 있는 일반적인 방법이고, 키 변경시 키 관리 센터에 등록만 되면 되므로 키 변경이 편리하여 보안 유지에 더욱 효율적이고 키분배를 여러 스테이션에 한 번에 할 수 있다. 특히, 본 논문에서 보안 서비스를 적용하는 LAN은 특성상 공통된 목적을 공유하고 있는 가입자가 접속되어 있어 이미 그룹을 형성하고 있고, WAN

(Wide Area Network)에 비해 가입자 수가 적어 하나의 키분배소만으로도 관리가 가능하므로 키분배소를 두어 키 관리, 생성, 분배를 담당하게 하는 것이 효율적이다.

2.3 Multiple-precision 연산

공개키 암호 시스템 적용시 일반적으로 사용되는 컴퓨터에서 제공하는 정수의 범위를 넘는 큰 정수의 연산을 해야 한다. 이러한 경우 일반적인 정수의 배열을 사용하여 연산을 하게 되는데 본 논문에서는 이미 연구되어져 있는 Multiple-precision 연산을 위한 알고리즘들을 사용하였다.[14]

큰 수를 표현하기 위해 n 개의 배열을 사용한 경우 n 자리(n-place) 정수는 b^n 보다 작은 임의의 정수를 의미한다. 매우 큰 수를 n 개의 배열로 표현할 때 배열의 한 원소에서 나타낼 수 있는 수의 범위가 0 부터 b-1 까지라면 n 개의 배열로 표현된 수는 베이스가 b인 n 자리 수이다.

multiple-precision 연산을 하기 위해서 single-precision 연산을 이용하기 때문에 효율적인 multiple-precision 연산을 하려면 베이스의 선택이 중요하다. 곱셈 연산시 한 자리수의 곱은 두 자리수의 결과를 만들어 내기 때문에 다음에 살펴 볼 곱셈 연산 알고리즘과 같이 덧셈과 곱셈을 동시에 하기 위해서는 배열의 한 원소가 0 부터 $(b-1)^2$ 까지 표현할 수 있어야 한다.

또한, RSA 암호 시스템 수행 시의 지수 계산에 있어서 일반적인 지수 계산 방법을 사용하면 엄청난 수행 시간이 들기 때문에 수행 시간을 줄이기 위해 고속 지수 계산법을 사용하였다.

3. 시뮬레이션 모델의 설계와 구현

여기에서는 2장에서 살펴 본 바와 같은 이론적 배경을 바탕으로 하여 보안 서비스가 적용된 LAN의 시뮬레이션 모델을 설계 및 구현하였다.

3.1 LAN 모델링

각 LAN의 프로토콜을 수행할 수 있는 SLAM 네트워크 모델을 다음과 같이 설계, 구현하였다. Ethernet, Token Ring, FDDI의 SLAM 모델에서 공통되는 개체의 어트리뷰트는 다음과 같다.

- SOURCE - 메시지가 발생한 스테이션의 번호, 일양 분포로 발생
- DEST - 메시지의 목적지 스테이션의 번호, 일양 분포로 발생
- LENGTH - 메시지의 길이, 지수 분포로 발생
- ARRIVAL - 메시지의 도착 시간, 지수 분포로 발생, CREATE 노드에서 기록

통계치로 메시지가 발생하여 완전히 전송이 끝나 목적지 스테이션까지 도착하는데 걸리는 시간과 네트워크 상에서 전송된 모든 메시지의 합을 COLCT 노드에 의해 구한다. 그림 2는 Ethernet의 기본 시뮬레이션 모델, 그림 3은 Token Ring과 FDDI의 공통되는 기본 시뮬레이션 모델의 SLAM 네트워크 모델을 나타내는데 여기에서는 상세한 내용은 생략하고 주기능만 표현하였다.

3.1.1 Ethernet 모델링

그림 2는 Ethernet의 프로토콜을 수행하는 기본 SLAM 모델이다. 개체의 어트리뷰트 ATTEMPT는 메시지 생성 후 전송을 시도했던 회수로서 충돌이 발생할 때마다 전송 회수가 증가한다. 어트리뷰트 ORDER는 전송을 시

작한 BUS 내의 메시지 중 그 메시지의 전송 시작 순서이다. ORDER가 1인 메시지는 전송을 시작한 첫번째 메시지로서 전송을 시작했음이 모든 스테이션에 전파될 때까지 전송을 시작한 다른 스테이션이 없으면 전송이 성공적으로 이루어지고, 전송을 시작한 스테이션이 있으면 충돌이 발생한 것이므로 전송을 시작한 메시지들은 신호 발생, backoff 지연 시간 처리를 거쳐 다시 전송을 시도하게 된다. backoff 지연 시간은 FORTRAN 서브루틴을 연결하여 계산하였다. 그림 2에서 DUR1은 전송을 시작한 메시지의 존재가 BUS에 연결되어 있는 모든 스테이션에 전파되는 시간, DUR2는 근원 스테이션에서 목적 스테이션까지의 전파 시간을 나타내고, 9.6 micro sec는 메시지의 전송이 끝나고 다음 메시지의 전송을 시작할 수 있을 때까지의 시간으로 표준을 따랐다.

3.1.2 Token Ring 모델링

Token Ring에서는 토큰이 돌다가 메시지를 전송하고자 하는 스테이션이 있으면 전송을 하고, 전송이 끝나고 비지 토큰이 전송한 스테이션에 돌아 왔을 때 다시 토큰을 생성시킨다. 따라서, SLAM 모델 설계에 있어서 전송을 하고자 하는 스테이션 중에서 하나의 스테이션을 선택할 때 스테이션의 순차적 순서를 고려해야 한다. 큐에서 대기하고 있는 개체 중에서 하나를 선택할 때 대기열 선택 규칙에서 이와 같은 선택 규칙을 제공해 주지 않아서 전송을 하고자 하는 스테이션은 그 개체를 RING이라는 화일에 넣고 선택하도록 FORTRAN 서브루틴을 작성하여 연결하였다. 그림 3의 EVENT,1에서는 대기 메시지인 개체를 화일 RING에 넣고 EVENT,2에서는 현재 토큰이 있는 위치의 스테이션의 개체를 화일 RING에서 선택한다. DUR1은 다음 메시지를 전송할 때까지 토큰이 돌고 있는 시간이고, DUR2는 근원 스테이션에서 목적 스테이션까지의 전파 시간이다.

3.1.3 FDDI 모델링

FDDI는 Token Ring에서와 같이 비지 토큰이 돌아 오기를 기다려서 토큰을 발생시키는

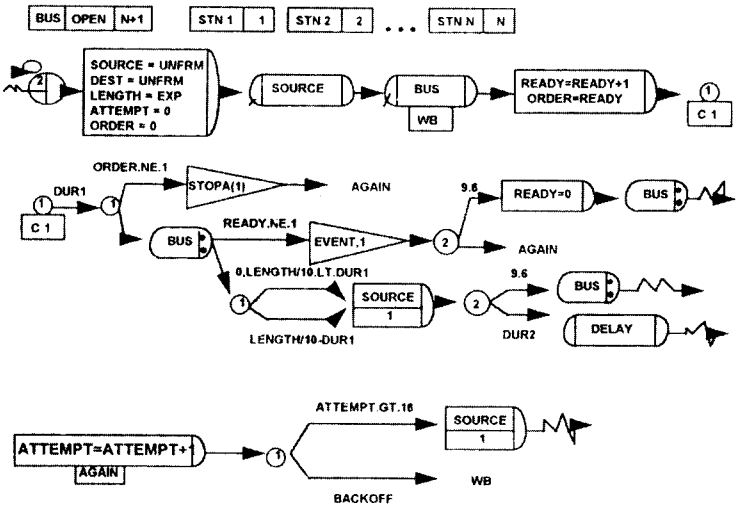


그림 2. Ethernet의 기본 시뮬레이션 모델

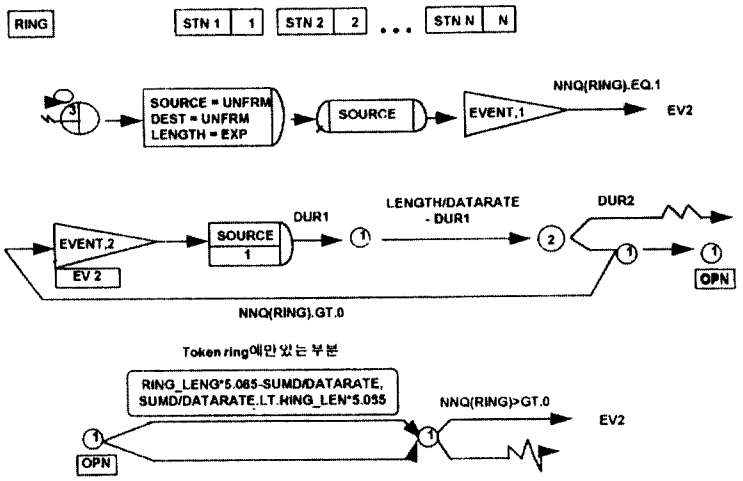


그림 3. Token Ring과 FDDI의 공통되는 기본 시뮬레이션 모델

것이 아니라 전송을 끝낸 후 바로 토큰을 발생시킨다는 점을 제외하고는 프로토콜에 있어서 Token Ring과 유사하다. 동기식 데이타는 실시간 처리를 요구하는 데이타, 화상, 음성을 포함하는데 이러한 데이타는 일반적으로 보안의 필요성이 크지 않고 암호화를 적용하기 위해서는 시간 지연이 있기 때문에 보안 서비스를 제공하는데 있어서 실용성이 적다. 따라서 본 논문에서는 비동기식 데이타만 있는 경우를 가정하여 시뮬레이션하였다.

3.2 SDE의 적용

본 논문의 시뮬레이션 모델은 OSI(Open System Interconnection) 7 Layer 중 데이타 연결 계층에서의 작동을 모델링하였다. 데이타 연결 계층은 다시 LLC 계층과 MAC 계층의 두 개의 부계층으로 구성되어 있다. 여기에 본 논문에서는 보안서비스를 적용하기 위해 새로운 계층인 SILS에서 제안한 SDE 계층을 LLC와 MAC 계층 사이에 첨가하여 모델링하였다.

LLC 계층에서 전송되는 메시지는 평균 메시지 도착 시간 간격에 따라 발생되고 사용자가 정하는 비율에 의해 암호화 서비스를 요구하지 않는 일반 정보와 암호화를 요구하는 정보로 분류된다. 일반 정보는 SDE 계층을 거치지 않고 바로 MAC 계층으로 전송되어 MAC Header를 첨가한 후 LAN을 통해 목적지 스테이션으로 전송되도록 하였다. 암호화를 요구하는 메시지는 키분배소와 수신자 스테이션 간의 키분배 과정을 거친 후 암호 서비스를 받기 위해 SDE 계층으로 넘어간다. SDE 계층에서는 필요한 필드들이 부가되고 지정된 암호 시스템에 의해 암호문으로 암호화된 후 MAC 계층으로 전송되는데 암호 적용 순서와 필드의 크기는 다음과 같다. 우선 스테이션 ID로 구성되는 8 옥텟의 Protected Header를 붙인 후 암호화시 데이타를 블럭 단위로 만들기 위해 필요한 PAD를 붙이고 지정된 암호 시스템을 적용하여 암호화하고 SDE 계층에서 전송된 정보임을 알리는 Clear Header를 첨가한 후 MAC 계층으로 전송한다. 이 때 Clear Header는 3 옥텟의 SDE Designator, 4 옥텟의 SAID로 구성되어 7 옥텟의 길이를 갖는다. MAC 계층에서는 일반 메시지와 마찬가지로 MAC Header를 첨가하여 LAN을 통해 목적지 스테이션으로 전송한다.

목적지 스테이션에서는 송신 과정의 역순으로 모델링하였다. 암호 서비스를 받지 않은 일

반 메시지는 MAC 계층에서 MAC Header를 제거한 후 바로 LLC 계층으로 전송된다. 그러나 암호 서비스를 받는 메시지는 MAC 계층에서 MAC Header를 제거한 후 SDE 계층으로 넘어간다. SDE 계층에서는 송신 과정의 역순으로 먼저 Clear Header를 제거한 후 암호화에 사용된 암호 시스템과 같은 방식으로 복호화된다. 여기서 암호화 시 사용된 암호 시스템에 따라 복호화 시 사용되는 키가 달라진다. 단일키 암호 시스템이 사용되었다면 암호화 시와 같은 키로 복호화되고 공개키 암호 시스템이 사용되었다면 자신의 비밀키로 복호화한다. 복호화 과정이 끝나면 SDE 계층에서 첨가된 필드들이 제거된 후 LLC 계층으로 보내진다.

3.3 암호 시스템의 적용

LAN의 보안 서비스 적용시 암호 시스템 수행의 시간을 계산하기 위해서 기계 독립적인 C 언어로 프로그램을 작성한 뒤 어셈블리어로 번역하여 명령어의 수를 계산하고 암호 시스템을 적용하고자 하는 기계에서 하나의 명령어를 수행하는데 드는 시간을 1 basic cycle time이라 할 때 명령어의 수와 1 basic cycle time을 곱하여 실제 수행 시간을 계산하였다. 어셈블리어로 번역시 본 논문이 수행된 기계에 기본을 두었지만 일반적인 기계에서의 수행과 큰 차이는 없으므로 대략적인 성능을 평가하고자 하는 본 논문의 시뮬레이션의 목적에 위배되지 않고 만약 정확성을 기하고자 하는 경우는 일반적인 프로그래밍 언어인 C로 작성했기 때문에 쉽게 그 기종의 어셈블리 코드의 명령어로 변환하여 수행 시간을 계산할 수 있다. 암호 시스템 수행 명령어 수를 계산함에 있어서 최대 수행을 가정하였다.

C의 int 형은 보통 컴퓨터가 사용하는 표준 워드의 크기가 주어지는데, 일반적으로 32 비트이다. 따라서 효율적인 multiple-precision 연산을 위해 베이스 b를 2^{16}으로 선택하였다. multiple-precision 연산을 위한 각 알고리즘들은 C 함수로 작성하였다.

시뮬레이션 모델을 구현하기 위해 사용한 각 암호 시스템의 1 블럭의 길이와 하나의 명령어를 수행하는데 드는 시간을 1 basic cycle time이라 할 때 1 블럭 당 처리 시간을 basic cycle time 단위로 살펴 보면 다음과 같다.

단일키 알고리즘인 DES에 대하여는 다음과 같은 값들을 적용하였다. DES 암호 시스템의 한 블럭의 길이는 64 비트이다. DES 암호 시스템을 적용할 경우에는 평문과 암호문의 길이가 변하지 않으므로 보내고자 하는 정보의 길이와 그 정보를 암호화하여 실제로 보낼 때의 정보의 길이는 같다. DES 암호 시스템을 C 언어로 작성할 때는 이미 알려져 있는 프로그램을 사용하였고 결과로 107081 basic cycle time을 얻었다. 암호 시스템은 64 비트의 블럭 단위로 적용되므로 암호화되어져야 하는 정보의 길이와 Pad의 길이를 합한 정보의 길이에 비례한다.

RSA 암호 시스템 적용에 기본이 되는 값들은 다음과 같다. 키 생성은 모델이 초기화될 때 이뤄진다는 가정하에 RSA 암호 시스템을 암호화 부분과 복호화 부분에 적용시켰다. 시뮬레이션시 적용한 키의 크기 즉 한 블럭의 크기는 일반적으로 사용되는 512 비트를 사용하였다. 한 블럭은 베이스가 2^{16}이므로 multiple-precision 연산시 32 개의 일반 정수 원소로 이루어진 배열로 나타낼 수 있다. 512 비트의 크기를 갖는 평문 P를 e 번 곱하는데 있어서 최대 $2 * \log_2(e)$ 번의 곱셈과 $2 * \log_2(e)$ 번의 나눗셈이 필요하다. 이런 암호 시스템 적용시 수행되는 암호화 또는 복호화에 걸리는 시간으로는 한 블럭당 72590854 basic cycle time을 얻었다.

마지막으로 Knapsack 암호 시스템에 적용되어진 자료에 대해 언급하자면 아래와 같다. Knapsack 암호 시스템을 적용시키기 위한 한 블럭을 200 비트로 하였다. 블럭의 한 비트에

해당하는 정수(term)는 1과 2^{402} - 1 사이의 수이다. 따라서 Knapsack 암호화 알고리즘을 1 블럭에 적용하여 얻어지는 결과값은 200 개의 최대 402 비트인 정수들의 합이므로 410 비트로 표현 가능하다. 200 비트의 정수를 32 비트 컴퓨터에서 표현하기 위해서는 베이스 2^{16} 일 때 13 개의 정수 원소를 가진 배열이 필요하다. 앞의 Knapsack 알고리즘을 이용한 암호화 과정의 설명에서 본 바와 같이 1 블럭의 암호화 시에 최대 200 개의 정수를 더하는데 120004 basic cycle time이 필요하고 복호화시에는 최대 200 번의 빨셈과 1 번의 mod 연산이 필요하며 280035 basic cycle time이 계산된다.

3.4 키분배 방식의 적용

보안이 필요한 정보를 암호화하여 전송하기 전에 암호화하는데 필요한 키를 얻기 위해서 키분배가 먼저 이루어져야 한다. 키분배 시에도 암호화되어져야 하는 정보들은 앞에서 살펴본 바와 같이 SDE 계층을 거쳐 암호화하여 전송되고 암호화되어질 필요가 없는 정보들은 LLC 계층에서 MAC 계층으로 바로 보내진다.

키분배 과정을 시뮬레이션 모델링하기 위해 키분배 시 필요한 키의 길이와 키분배 시의 메시지 길이 연산과 처리 시간의 연산에 대해 살펴 보자. 우선, 모든 암호 시스템에 관련되는 사항은 다음과 같다. 보내는 정보에 상대 스테이션을 명시해야 할 경우 그 정보의 길이는 8 바이트로 추정하였다. 두 스테이션 간에 확인을 위해 핸드쉐이킹할 때 보내는 작은 정보의 길이는 최소 길이 1 바이트로 추정하였다. 보내야 할 정보를 암호화하여 보낼 때 SDE 계층을 거치므로 암호 시스템을 적용하기 전에 Pad와 Protected Header를 붙인 후 암호 시스템을 적용하여 평문을 암호화한 후 Clear Header를 붙여 보낸다. 키분배 시에 보내려고 하는 정보를 블럭으로 나눌 때 1 블럭이 되지 않으면 Pad 비트를 붙여서 1 블럭을 만든다.

키분배에 DES를 적용할 때 전달되어지는 키의 길이는 56 비트이고 Pad를 붙여 한 블럭 단위가 되게 만들어 키분배시에도 한 블럭당 107081 basic cycle time의 시간으로 암호화 복호화하여 정보가 전달된다.

키분배에 있어서도 공개키 암호화 방식에서는 정보를 전송하고자 하는 스테이션과 상대 스테이션의 핸드쉐이킹에 있어서 Knapsack 암호 시스템과 RSA 암호 시스템을 적용하였다. 키분배 방식과 암호화하여 보내고자 하는 데이타에 적용되는 알고리즘이 RSA인 경우에 RSA의 한 블럭의 크기는 512 비트이고 공개키와 비밀키의 길이 모두 512 비트이다. RSA 알고리즘을 적용할 경우에도 평문과 암호문의 길이가 같으므로 보내고자 하는 정보의 길이와 그 정보를 암호화하여 실제로 보낼 때의 정보의 길이는 같다. 암호화 시간은 앞에서의 설명과 같다.

적용 알고리즘이 Knapsack 알고리즘인 경우에는 한 블럭의 크기는 200 비트이고 각 한 비트에 해당하는 정수(term)의 크기는 최대 402 비트이므로 키의 길이는 402 * 200 = 80,400 바이트가 된다. 또한 Knapsack 암호 시스템의 특징은 200 비트의 한 블럭을 암호화하면 최대로 402 비트 짜리 정수 200 개가 더해지기 때문에 410 비트의 길이가 된다는 데 있다. 암호화와 복호화 시간은 앞에서의 설명과 같다.

3.5 시뮬레이션 모델 파라미터

본 논문에서 구현한 시뮬레이션 모델은 평균 메시지 도착 시각 간격, 평균 메시지의 길이, 전체 메시지에 대한 암호화되어져야 하는 보안이 필요한 메시지가 차지하는 비율, 전송 매체의 길이, 스테이션의 수 등의 파라미터 값을 변화시켜 가면서 시뮬레이션하였다.

시뮬레이션 결과로서 메시지가 발생하여 전송을 포함한 모든 처리가 끝날 때까지의 시간과 처리가 끝난 메시지의 양이 보안이 요구되었던 메시지와 필요하지 않았던 일반 메시지

각각에 대해 구해진다. 또한, 모든 처리가 끝난 뒤 모아지는 통계량과는 달리 초당 전송되는 데이타의 양인 네트워크만의 처리량을 구할 수 있다.

4. 결과 분석

본 논문의 보안 서비스를 적용한 LAN의 시뮬레이션 모델은 다양한 LAN 환경하에서의 시뮬레이션을 가능하게 한다. 다음은 그 중 일부로 보안 서비스를 적용한 LAN의 시뮬레이션의 결과이다. 각 LAN에 10 개의 스테이션이 접속되어 있는 네트워크 환경에서 1 basic cycle time을 1 micro sec로 가정하고 메시지 도착 시간 간격, 전체 메시지에 대한 암호화 메시지의 비율 등을 변화시키면서 시뮬레이션하였다.

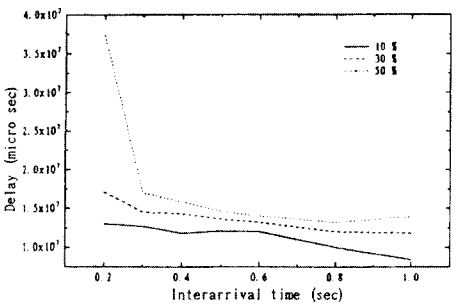


그림 4. DES 적용시 암호화 정도에 대한 전달 지연 시간의 비교

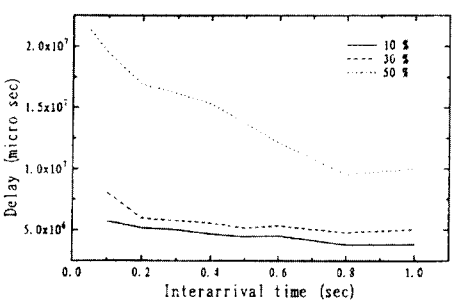


그림 5. Knapsack 적용시 암호화 정도에 대한 전달 지연 시간의 비교

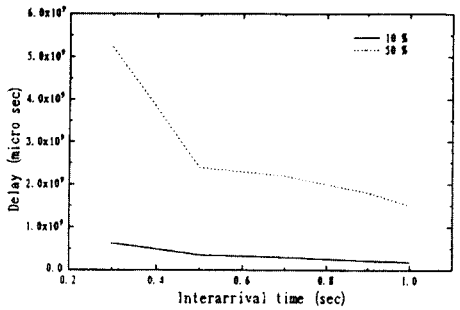


그림 6. RSA 적용시 암호화 정도에 대한 전달 지연 시간의 비교

그림 4, 5, 6은 Token Ring에 각각 DES, Knapsack, RSA 암호 시스템을 적용한 경우로 평균 메시지의 길이는 1000 비트, Token Ring의 길이는 10 km, 전체 메시지에 대한 암호화 요구 메시지의 양이 10 %, 30 %, 50 % 일 때 한 스테이션의 평균 메시지 도착 간격을 0.1 초에서 1.0 초까지 변화시키며 구한 암호화된 정보의 메시지 전달 지연 시간 결과이다. 메시지 전달 지연 시간은 메시지가 발생해서 모든 처리가 끝나서 사라질 때까지의 암호화 시간, 복호화 시간, 전송 시간, 대기 시간 등이 모두 포함된 시간을 의미한다. 단, RSA 암호 시스템 적용시는 1 basic cycle time을 0.1 micro sec로 가정하였다. 그림에서 보는 바와 같이 암호화 메시지가 차지하는 비율이 10 % 정도로 크지 않은 경우에는 LAN 상의 교통량이 많아져도 메시지 전달 지연 시간의 급격한 증가를 보이지 않지만 암호 메시지의 비율이 높아질수록 교통량이 많은 경우 전달 시간의 증가폭이 커진다. 이것은 세 가지 암호 시스템 적용시 모두 공통적이다. 이와 같은 결과를 볼 때 교통량이 적은 LAN 환경에서는 암호화 정도가 성능을 저하시키는 정도가 적으므로 보안이 필요한 많은 정보에 보안 서비스를 제공할 수 있다. 그러나, 교통량이 많은 경우 중요한 정보를 선별하여 암호 서비스를 제공받도록 하는 것이 LAN의 성능을 고려할 때 합리적이다.

이처럼 보안 서비스를 적용한 LAN 모델의 파라미터 값을 변화시키면서 시뮬레이션해 보면 서로 다른 각 환경에서 전달 시간의 급격한 변화를 가져오는 교통량 부분을 알 수 있다. 그러면 원하는 메시지 전달 지연 시간과 처리량을 얻기 위해 메시지 발생량과 암호 메시지의 비율을 조절할 수 있다.

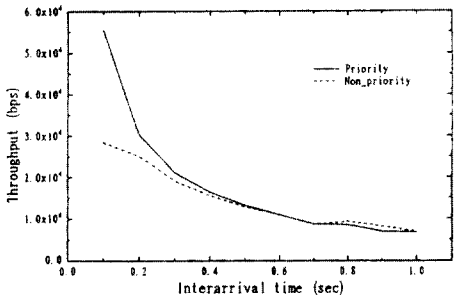


그림 7. 우선 순위 적용에 대한 처리량의 비교

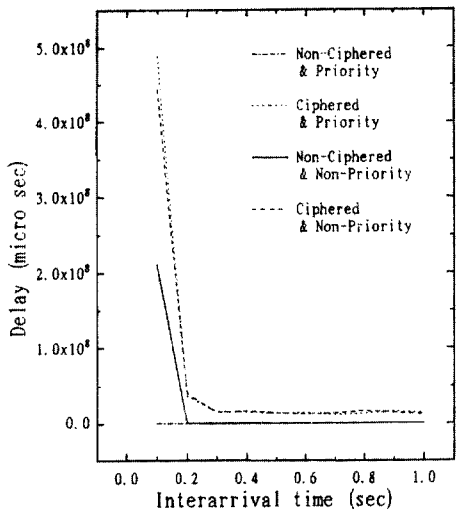


그림 8. 우선 순위 적용에 대한 전달 지연 시간의 비교

그림 7과 그림 8은 Token Ring에서 DES 암호 시스템을 적용한 환경으로 평균 메시지 길이는 1000 비트, Token Ring의 길이는 10 km, 암호 메시지의 확률이 50 % 일 때 한 스테이션에서의 평균 메시지 도착 간격을 0.1 초에서 1.0 초까지 변화시키며 얻은 처리량과 메시지 전달 지연 시간 그래프이다. 여기에서 메시지의 성격에 관계없이 도착 순서로 처리를 하게 되는 경우와 일반 정보에 우선 순위를 주는 경우를 비교한 결과를 보여 준다. 일반 정보에 우선 순위를 주는 것은 보안 서비스가 필요없는 일반 정보가 암호 처리를 해야 하는 정보로 인해 지연 시간이 길어지는 경우를 피하기 위함이다. 그림 8은 스테이션에서의 평균 메시지 도착 간격에 대한 암호 메시지와 일반 메시지의 전달 시간의 비교 결과를 보여 주는데, 우선 순위를 적용한 경우가 우선 순위를 적용하지 않은 경우보다 암호화되지 않는 일반 정보가 빨리 전달된다는 예견된 사실과 함께 암호화 메시지의 메시지 전달 지연 시간에 우선 순위의 적용이 거의 영향을 끼치지 않음을 보여 준다. 발생되는 메시지의 대부분이 일반 메시지인 경우가 아니라면 일반 메시지에 우선 순위를 주어 처리를 하면 암호화 메시지에 영향을 거의 주지 않으면서 일반 메시지의 처리량이 많아져 그림 7에서 보는 바와 같이 LAN의 교통량이 많을 때 성능의 향상을 보임을 알 수 있다.

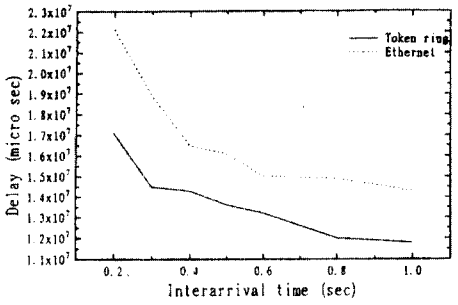


그림 9. Ethernet과 Token Ring의 전달 지연 시간의 비교

그림 9는 전체 메시지에 대한 암호 메시지의 비율이 30 %이고, 평균 메시지 길이 1000 비트, 전송 매체의 길이 10 km 일 때 DES 암호 시스

템을 Token Ring과 Ethernet에 각각 적용했을 때, 한 스테이션에서의 메시지의 평균 메시지 도착 시각 간격을 0.1 초에서 1.0 초로 변화시키며 얻은 암호 메시지의 메시지 전달 지연 시간의 비교 결과를 보여 준다. Token Ring과 Ethernet은 전송 속도가 각각 4 Mbps, 10 Mbps로 비슷하지만 서로 다른 프로토콜을 갖고 있다. 전체적으로 Token Ring에서의 메시지 전달 지연 시간이 짧아 대부분의 경우에 있어 Token Ring이 Ethernet 보다 성능이 좋음을 보여 준다.

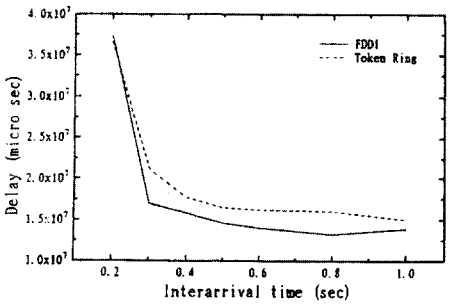


그림 10. Token Ring과 FDDI의 전달 지연 시간의 비교

그림 10은 그림 9와 같은 조건으로 각각 프로토콜이 거의 같은 Token Ring과 FDDI에 적용했을 때의 암호 메시지의 메시지 전달 지연 시간을 비교하여 보여준다. 기울기의 변화와 같은 증가 양상은 비슷하지만, FDDI 의 전송 속도가 훨씬 빠르기 때문에 교통량이 적은 상황에서는 FDDI에서의 메시지 전달 지연 시간이 짧지만 교통량이 많은 상황에서는 전체 메시지 전달 지연 시간에서 네트워크를 통해 전달되는 시간이 미치는 영향이 상대적으로 적어지고 암호 처리를 위한 대기 시간이 길어지기 때문에 거의 같은 수준이 된다.

5. 결 론

본 논문에서는 보안 서비스를 LAN 상에 적용할 수 있는 방법을 제시하였고, 다양한 LAN 환경과 그에 적용할 암호 시스템을 선택하여 교체 적용함으로써 여러가지 다른 조건을 갖는 환경에서의 성능을 평가할 수 있는 보안 서비스가 적용된 LAN의 시뮬레이션 모델을 개발하였다. 또한 이러한 시뮬레이션 모델을 이용하여 보안 서비스를 LAN에 적용했을 때의 성능을 평가하였다.

보안 서비스를 적용하기 위해 LAN의 LLC 계층과 MAC 계층 사이에 IEEE 802.10 SILS에서 제안한 SDE 계층을 둔 프로토콜을 사용하고 프레임 구조를 채택했다. 암호 시스템으로는 대표적인 단일키 암호 시스템인 DES 시스템과 공개키 암호 시스템인 Knapsack과 RSA 시스템을 적용하였다. LAN에 적합한 암호키분배 방식으로 중앙 집중식 키분배 방식을 선택했다. 특히 공개키 암호 시스템의 키분배 방식에서는 LAN의 성능을 향상시키기 위해서 LAN의 그룹화된 특성을 이용하여 키분배소와 스테이션 사이의 데이타의 교환 시의 암호화는 하지 않고 정보를 전송하고자 하는 스테이션과 상대 스테이션 간의 정보 교환시에는 암호 시스템을 적용하는 방법을 사용하였다. 암호 시스템을 C 언어로 프로그래밍하여 어셈블리어로 된 프로그램으로 번역하여 각 암호 시스템을 적용하기 위해서 각 시스템을 수행하는데 드는 수행 명령어의 수를 구하였다. 이 수행 명령어 수는 암호 시스템을 적용하여 수행하고자 하는 기계의 1 basic cycle time과 결합되어 실제 수행 시간을 구할 수 있어 시뮬레이션 모델에 적용된다.

시뮬레이션 모델에서 메시지 전달 지연 시간와 처리량에 영향을 주는 파라미터를 변화시키면서 시뮬레이션을 수행하여 보안 서비스를 LAN에 적용하였을 때의 결과 분석을 통해 다음과 같은 결과를 얻었다.

교통량이 적은 LAN 환경에서는 암호화 정도가 성능을 저하시키는 정도가 적으므로 보안

이 필요한 많은 정보에 보안 서비스를 제공할 수 있다. 그러나, 교통량이 많은 경우 중요한 정보를 선별하여 암호 서비스를 제공받도록 하는 것이 LAN의 성능을 고려할 때 합리적이다.

발생되는 메시지의 대부분이 일반 메시지인 경우가 아니라면 일반 메시지에 우선 순위를 주어 처리를 해도 암호화 메시지에 영향을 거의 주지 않으면서 일반 메시지의 처리량이 많아져 LAN의 교통량이 많을 때 성능의 향상을 보인다.

전송 속도가 비슷하지만 서로 다른 프로토콜을 갖는 Token Ring 과 Ethernet을 비교한 결과, 전체적으로 Token Ring에서의 메시지 전달 지연 시간이 짧아 대부분의 경우에 있어 Token Ring이 Ethernet 보다 성능이 좋음을 알 수 있었다.

프로토콜이 거의 같은 Token Ring과 FDDI에 적용했을 때, FDDI의 전송 속도가 훨씬 빠르기 때문에 교통량이 적은 상황에서는 FDDI에서의 메시지 전달 지연 시간이 짧지만 교통량이 많은 상황에서는 전체 메시지 전달 지연 시간에서 네트워크를 통해 전달되는 시간이 미치는 영향이 적어지기 때문에 거의 같은 수준이 된다.

LAN과 암호 시스템의 종류에 관계없이 대부분의 결과에서 교통량이 적은 상황에서 교통량이 많은 상황이 될 때, 메시지 전달 지연 시간의 증가에 있어서 교통량이 적을 때는 완만한 증가를 하지만 어떤 부분에 이르면 급격한 증가를 보임을 알 수 있었다. 이처럼 보안 서비스를 적용한 LAN의 시뮬레이션 모델의 파라미터 값을 변화시키면서 시뮬레이션해 보면 서로 다른 각 환경에서 메시지 전달 지연 시간의 급격한 변화를 가져오는 교통량 증가 부분을 발견할 수 있다. 이러한 성능 저하 부분을 알게 되면 원하는 메시지 전달 지연 시간와 처리량을 얻기 위해 메시지 발생량과 암호 메시지의 비율을 조절할 수 있다.

참 고 문 헌

[1] V. S. Frost, W. W. LaRue, A. G. McKee, A. j. Ernstein, P. Kishore, and M. J. Gormish, "A tool for local area network modeling and analysis," Simulation, pp.283-297, Nov. 1990.

[2] IEEE 802.3, "Local Area Networks: Carrier Sense Multiple Access with Collision Detection (CAMA / CD) access method and physical layer specifications," 1992.

[3] IEEE Standard 802.5, "Local Area Networks: Token Ring access method and physical layer specifications," 1989.

[4] ANSI Standard X3.139, " Fiber Distributed Data Interface (FDDI) - Token Ring media access control," 1987.

[5] IEEE Standard 802.2, "Logical Link Control," 1985.

[6] IEEE P802.10A / D1, "Standard for Interoperable Local Area Network (LAN) Security (SILS): Part A - The Model", Dec. 1989.

[7] IEEE P802.10B / D2, "Standard for Interoperable Local Area Network (LAN) Security (SILS): Part B - Secure Data Exchange", May 1991.

[8] National Bureau of Standards, "The Data Encryption Standards," Federal Information Processing Standard (FIPS) Publication 46, Jan. 1977.

[9] R. C. Merkle and M. E. Hellman, "Hiding Information and Signatures in Trapdoor Knapsacks," IEEE. Trans. Inform. Theory, Vol. IT-24, No.5, pp.525-530, Sep. 1978.

[10] R. L. Rivest, A. Shamir and L. Adelman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystem," Comm. ACM, Vol.21, No.2, pp.120-126, Feb. 1978.

[11] 원동호, "암호방식과 키분배", 한국통신정보보호학회지, 제 1권, 제 1호, 1991. 4.

[12] R. M. Needham and M. D. Schroeder, "Using Encryption for Authentication in Large Networks of Computer," Comm. ACM, Vol.21, No.12, pp.993-999, Dec. 1979.

[13] D. E. Denning and G. M. Sacco, "Time stamps in Key Distribution Protocols," Comm. ACM, Vol.24, No.8, pp.533-536, Aug. 1981.

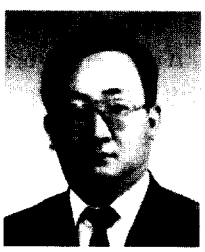
[14] D. E. Knuth, The Art of Computer Programming, Vol.2, Seminumerical Algorithms, 2nd Edition, Addison-Wesley, Reading, Mass.,1981.

□ 著者紹介

김 회 림

1989년 ~ 1993년 이화여자대학교 전자계산학과 학사
1993년 ~ 1995년 이화여자대학교 전자계산학과 석사
1995년 ~ 현재 LG 전자 미디어 통신 연구원

※ 주관심분야 : 개인휴대통신, 보안이론



채 기 준

1976년 ~ 1982년 연세대학교 수학과 학사
1982년 ~ 1984년 미국 Syracuse University, 전자계산학과 석사
1984년 ~ 1990년 미국 North Carolina State University, 컴퓨터공학과 박사
1990년 ~ 1992년 미국 해군사관학교 전자계산학과 조교수
1992년 ~ 현재 이화여자대학교 전자계산학과 부교수

※ 주관심분야 : 고속통신망, LAN, 망관리, 성능평가, 암호학 응용