通信情報保護學會誌
第3卷 第4號, 1993. 12

DES를 적용한 ETHERNET의 성능 평가

김회림* · 안옥정* · 채기준**

요 약 (Abstract)

LAN을 이용한 정보 교환이 증가함에 따라 LAN을 이용한 정보교환 시에도 중요한 정보의 보호를 위한 보안체제가 필요하다. 이 보안 서비스를 위한 암호화 알고리즘을 LAN상에 적용할 때 그 알고리즘이 LAN의 성능에 미치는 영향을 고려한 후 실제 LAN상에 적용하는 것이 바람직하다. 따라서 본 논문에서는 다양한 암호 알고리즘 중 대표적인 단일키 암호 시스템인 DES 알고리즘을 오늘날 전세계적으로 가장 많이 사용되어지고 있는 LAN인 Ethernet에 적용시 현재 표준화가 진행중에 있는 IEEE 802.10 SILS에서 제안한 SDE 프로토콜을 사용하여 보안 서비스의 제공 정도가 Ethernet상의 정보 전달속도에 미치는 영향을 시뮬레이션을 통하여 성능 분석하여 살펴 보았다.

1. 서 론

급변하고 있는 정보화 사회에서 컴퓨터 사용이 증가하면서 네트워크를 이용한 정보 교환이 증가함에 따라 그 정보전달 속도와 신뢰성이 점점 더 중요해지고 있다. 특히 중요한 정보의 보호를 위하여 정보를 암호화하고 암호화된 정보를 인정된 사용자만이 해독하여 정보를 안정하게 활용하는 암호화 기술을 네트워크에 어떻게 적용하는 가는 매우 중요한 문제이다.

특히, 1970년대 후반 Xerox사에서 Ethernet이라는 근거리 통신망(Local Area Network : LAN)을 처음 소개한 후 LAN의 사용자는 전세계적으로 급속한 속도로 증가하였고, 국내에서도 1980년대 이후 LAN의 보급이 급격히 증가하는 추세이다. 이와 같은 추세로 LAN의 사용량이 증가할 때 LAN 상에서 주고받는 정보의 보호는 필수적인 것이 될 것이다. 그러나, LAN상에 암호화 알고리즘을 적용하는 것은 그 알고리즘을 적용하지 않을 때보다 정보가 전달되어지는 시간이 더 걸리기 때문에 적용되는 암호화 알고리즘이 그 알고리즘을 적용하고자 하는 사용자의 LAN 환경에서 LAN의 성능에 미치는 영향을 미리 예측한 후 암호화 알고리즘을 적용하는 것이 중요하다. 또한 메시지 도착 간격과 같은 사용자의 LAN 환경의 변화가 있을 때마다 원하는 LAN의 성능에 부합되는 정보의 암호화 정도를 결정하여 암호화 알고리즘을 적용하는 것이 필요하다.

이 논문에서는 현재 표준화가 진행중에 있는 IEEE 802.10 SILS[1, 2](Standard for Interoperable LAN Security)에 의해서 제안된 SDE(Secure Data Exchange) 계층을 LLC(Logical Link Control) 계층과 MAC(Medium Access Control) 계층 사이에 두고 SDE 프로토콜에 따라 대표적인 단일키 암호

* 이화여자대학교 전자계산학과 대학원
** 이화여자대학교 전자계산학과 조교수

시스템인 DES(Data Encryption Standard) 알고리즘을 현재 국내외적으로 가장 널리 사용되어지고 있는 LAN인 Ethernet에 적용하였다. NETWORK II.5라는 시뮬레이션 패키지를 사용하여 성능평가를 하기 위한 시뮬레이션을 하였다.

본 논문에서는 먼저 Ethernet, IEEE 802.10 SILS와 DES 알고리즘에 대하여 살펴보고, NETWORK II.5를 사용한 실제 모델과 성능평가 결과를 분석하였다.

2. Ethernet

Ethernet은 1979년 제록스사에서 처음 개발한 후 급속한 속도로 보급이 되어 현재는 전 세계적으로 가장 많이 사용되어지고 있는 LAN으로서 전송속도는 10 Mbits/sec이며 전송매체로는 동축 케이블이나 트위스티드 패어를 사용한다. 전송 방식기에 따라 베이스 밴드(디지탈 신호)와 브로드 밴드(아날로그 신호)의 두 가지로 나누어 진다. 동축 케이블을 사용하는 베이스 밴드 Ethernet에는 10BASE5(Thick Ethernet : 최대 세그멘트 길이 500m)와 10BASE2 (Thin Ethernet : 최대 세그멘트 길이 200m)의 두 종류가 있으며 버스 토폴로지를 갖는다. 트위스티드패어를 사용하는 것에는 10BASET가 있고 Hub를 통하여 스테이션들을 연결하는 성형 토폴로지를 갖는다. 본 논문에서는 10BASE5 Ethernet을 사용하였다.

Ethernet은 IEEE 802.3[3]에 의해서 표준화된 CSMA/CD(Carrier Sense Multiple Access with Collision Detection)라는 프로토콜을 사용하는데, 그 작동 원리는 다음과 같다. 네트워크 안의 어떤 스테이션이 패켓을 보내고 싶으면 다른 스테이션이 패켓을 현재 전송하고 있는지를 조사한다. 아무도 패켓 전송을 하지 않는 않는 것이 확인되면 패켓의 전송을 시작한다. 그러나 다른 스테이션이 패켓 전송을 하고 있으면 전송이 끝날 때까지 기다렸다 전송을 시작한다. 그러나 두 개 이상의 스테이션이 동시에 패켓 전송을 시작하면 충돌(Collision)이 발생한다. 전송 전 다른 스테이션의 패켓 전송여부를 조사하였음에도 불구하고 패켓 전파 시간(propagation delay)이 0이 아니기 때문에 충돌이 발생한다. 충돌이 발생하면 전송을 하던 스테이션들은 전송을 중지하고 네트워크 내의 모든 스테이션들에게 충돌이 발생했음을 알리기 위하여 잼 신호를 보낸다. 잼 신호를 보낸 후 임의의 시간(Backoff delay)을 기다린 후에 다시 전송을 시도한다. 동일 패켓에 대한 반복적인 충돌은 네트워크의 사용량이 매우 높다는 것을 나타내기 때문에 각 스테이션들은 재 전송의 시기를 지연시킴으로 네트워크의 부하를 조절할 수 있다. 이러한 지연시간은 Truncated Binary Exponential Backoff라고 하는 무작위 과정을 통하여 이루어지며 스롯 시간의 정수배이다. 스롯 시간은 최대 왕복 전파시간보다 크거나 같아야 한다. 표준안에서는 10Mbits/second의 전송속도를 갖는 CSMA/CD 네트워크에 대하여 스롯 시간을 51.2μseconds로 정하고 있다. n번째 재 전송에 대한 스롯 시간의 숫자는 0과 2^k 사이의 임의의 정수가 된다. (단, $k=min(n, 10)$)재 전송의 숫자가 16번이 되면 그 스테이션은 전송을 포기하고 에러를 그 위 계층인 Logical Link Control 계층에게 알려준다. 이 과정을 알고리즘으로 기술하면 다음과 같다.

```
while(number-of-attempts<16)do
  begin
    k : =min(number-of-attempts, 10) ;
    r : =Random(0, 2^k) ;
    delay : =r* slot-time
  end
```

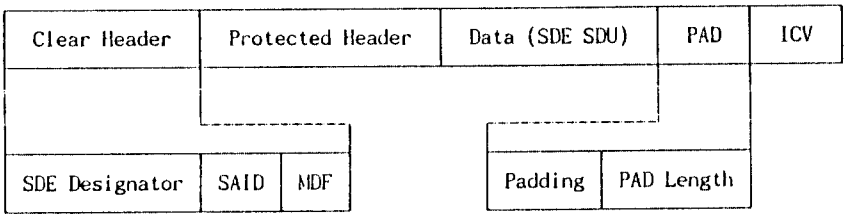
CSMA/CD 프로토콜은 512 비트의 최소 패켓 길이를 지정하고 있다. 패켓의 길이가 512비트 보다 작으면 그 차이 만큼의 패드 비트를 데이타 뒤에 붙여준다.

CSMA/CD 프로토콜에 대한 대표적인 논문들은 다음과 같다. [4]에서 Bux는 CSMA/CD를 포함한 여러 LAN들의 성능을 비교 분석하였다. LAM [5]은 CSMA/CD의 개발에 기본이 되었고 패켓 라디오 네트워크에 대하여 개발된 CSMA 프로토콜에 대하여 서술하고 있다. [6]에서 Tobagi와 Hunt는 CSMA/CD 프로토콜에 대한 성능을 분석하였다.

3. Secure Data Exchange(SDE)

IEEE 802.10 SILS(Standard for Interoperable LAN Security)에서는 LAN상에 보안 서비스를 제공하기 위하여 IEEE 802.2 [7]에서 정의된 Logical Link Control(LLC) 계층과 다른 종류의 LAN에 따라 IEEE 802.3, 802.4 [8], 802.5 [9] 등에 의해서 정의된 Medium Access control(MAC) 계층 사이에 Secure Data Exchange(SDE)라는 새로운 계층을 첨가하였다.

SILS에서 정의하고 있는 SDE PDU(secure Data Exchange Protocol Data Unit)의 구조와 각 field의 길이는 다음과 같다.



1) Clear Header : SDE PDU를 식별하고 PDU에 있는 정보의 처리를 도와주며 선택적으로 사용되어질 수 있다.
   a. SDE Designator : Clear Header가 사용되면 필수적으로 있어야하며, 길이는 3octets이다.
   b. SAID(Security Association IDentifier) : Clear Header가 사용되면 필수적으로 있어야하며, 길이는 4 octets이다.
   c. MDF(Management-Defined Field) : 선택적으로 사용되어질 수 있으며, 최대길이는 20 octets이다.
2) Protected Header : 선택적으로 사용되어질 수 있고, 보안 서비스가 제공되는 부분으로 전송을 시작하는 스테이션을 나타내는 Staion ID field로만 구성되며, 길이는 8 octets이다.
3) Data : LLC 계층으로부터 SDE 계층으로 보내진 정보로 보안 서비스가 제공되어 지지 않을 때에는 이 데이타가 MAC 계층으로 보내진다.
4) PAD : 특정 비밀유지나 데이타 무결성 알고리즘은 적용시 어떤 수의 정수배의 Octet이 필요하다. 이러한 목적을 위하여 최대 255 Octets까지의 Padding field를 사용할 수 있고, 그 길이는 1 octet의 PAD length field에 의해서 명시된다.
5) ICV(Integrity Check Value) : 데이타 무결성 서비스가 제공되어질 때에 데이타 수정을 감지하기 위하여 선택적으로 사용되어지는 field이며, Protected Header, Data field, PAD field에 대해 계산되어진다.

본 논문에서는 보안 서비스를 제공하기 위한 SDE PDU의 각 field의 길이를 다음과 같이 지정했다.

Clear Header : 13 octets
(SDE Designator : 3, SAID : 4, MDF(SMIB의 한 항목의 길이) : 6)

Protected Header(Station ID) : 8 octets

PAD :8 octets(비밀유지 알고리즘으로 DES를 사용하기 때문에 최대 63 bits가 필요하기 때문에 8 octets로 지정)

4. DES ALGORITHM

DES(Data Encryption Standard) [10]는 IBM에서 Lucifer 시스템을 개선하여 개발한 암호시스템으로, 1977년 미국 상무성의 국립 표준국(National Bureau of Standard, NBS)에서 미국 표준암호 알고리즘으로 채택한 64비트 블럭 암호 시스템이다. 64비트의 키블럭 중 56비트가 암호화 및 복호화에 사용되고 나머지 8비트는 키 블럭의 패리티 검사용으로 사용된다.

DES는 기본적으로 16라운드로 구성되며, 암호화는 동일한 동작과정의 반복으로 이뤄진다. 복호화

는 암호화과정과 동일하나 사용되는 키만 역순으로 작용하면 된다.

그림 1의 a)와 같이 64비트의 블럭 평문이 입력되면 19단계를 거쳐 64비트의 암호문을 만들게 된다. 초기 단계는 64비트 평문상의 키와는 독립적인 치환이 이루어 진다. 마지막 단계는 이 초기치환의 역치환이다. 그림 1의 b)는 단계를 세분화 해서 살펴본 것인데 왼쪽출력은 오른쪽 입력의 복사본이고 오른쪽 출력은 왼쪽 입력과 각 단계별 키와 오른쪽 입력의 함수 f 값과의 exclusive-or 연산결과이다.

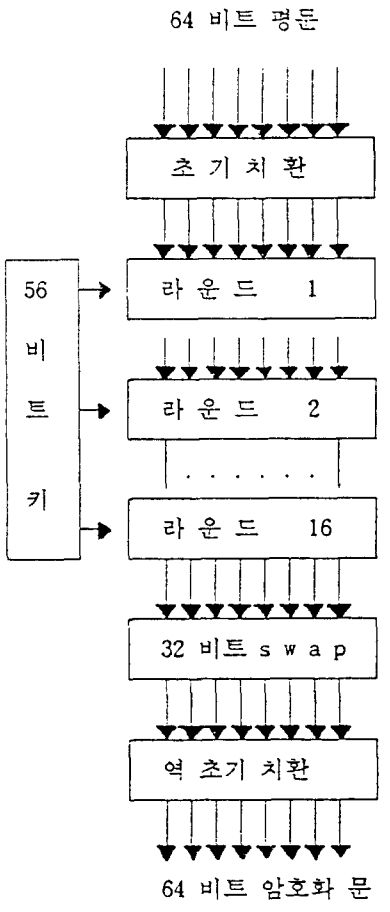
키 생성은 64비트에서 패리티 비트 8비트가 제거된 56비트가 다시 48비트로 압축된 후 28비트씩 나눠져 일정한 규칙에 의해 이동한 후 선택 치환에 의해 48비트의 라운드키를 생성한다. 복호화 시는 이동 방향만 바뀐다.

본 논문에서는 LLC 계층에서의 DES적용은 한 명령어를 1 Basic Cycle Time으로 두어 DES 모듈에서 처리되는 시간을 중심으로 시뮬레이션 하였다.

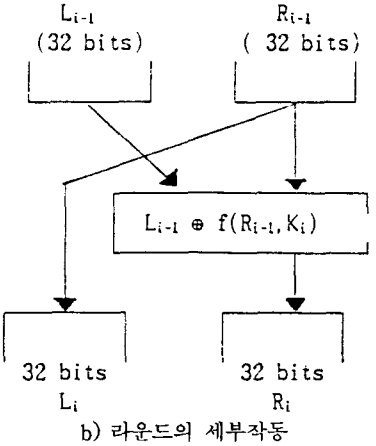
5. 시뮬레이션 모델

본 논문에 필요한 시뮬레이션을 위해 각 스테이션에 다음과 같은 Module을 작성하였다. Module과 Module 사이의 이탤릭체로 쓰여진 이름은 관련 메시지이고, 다음 Module과 연결 시 그 메시지를 전달한다.

그림 2는 한 스테이션에서 정보 전송시 작업을 처리하기 위한 Module의 순서와 그러한 작업을 스케쥴하기 위해 사용되는 메시지를 나타내고 있다. 각 스테이션 당 MODULE LLC에서는 사용자가 정의한 Inter-arrival time에 따라 전송될 정보가 발생되는데, 암호화 서비스가 적용된 정보는 그림 2의 오른쪽 경로에 해당되는 Module들을 거쳐 암호화되고, 일반적인 정보는 그림 2의 왼쪽 Module을 통과한 후 두 종류의 정보 모두 MAC Header를 붙인 뒤 목적지의 스테이션으로 전송된다. 암호화될 정보와 일반적인 정보의 비율은 사용자가 Network II.5를 사용하여 프로그램할 때 지정해 줄 수 있다. MODULE LLC에서 발생된 정보들 중 암호화되어야 할 정보는 LLC 계층에서 MAC 계층으로 가기 전에



a) 전체적 작동 구조



b) 라운드의 세부작동

그림 1. DES 암호화 알고리즘

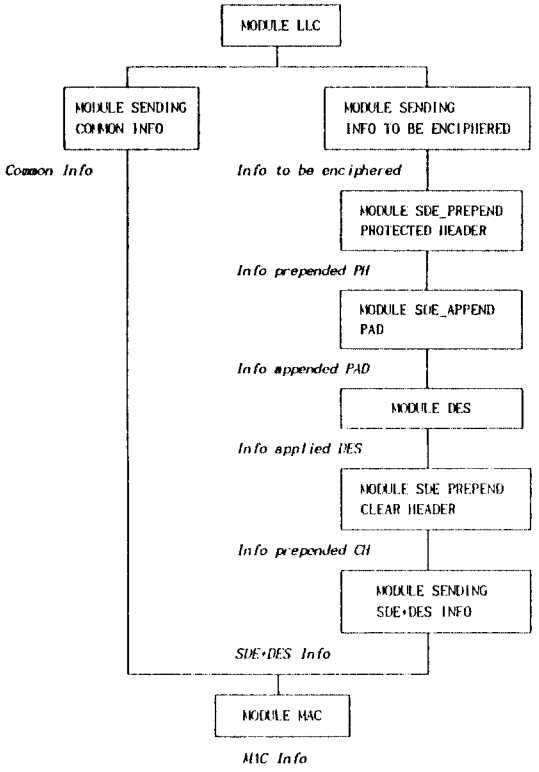


그림 2. 송신을 위한 작업처리 과정

SDE 계층이 첨가된다. MODULE SENDING INFO TO BE ENCIPHERED에서 암호화가 요구되는 정보를 받은 후 SDE PDU를 구성하기 위해서 MODULE SDE_PREPEND PROTECTED HEADER, MODULE SDE_APPEND PAD에서 Protected Header와 Pad를 붙인 뒤 MODULE DES에서 암호화를 위해 DES Algorithm을 적용한다. Clear Header는 암호화될 필요가 없기 때문에 DES 적용 후 MODULE SDE PREPEND CLEAR HEADER에서 붙여 주었다. MODULE LLC에서 발생된 일반적인 정보와 함께 위와 같은 과정을 거쳐 암호화된 정보는 MODULE MAC에서 MAC Header를 붙여 Ethernet을 통해 보내진다.

그림 3은 한 스테이션에서 수신 시 처리해야 할 작업을 위한 Module을 각 단계에서 필요한 메시지와 함께 순서대로 나타내었다. 정보를 받아 MODULE REMOVE MAC에서 MAC Header를 제거한 후 일반적인 정보는 그대로 LLC 계층으로 보내고 암호화된 정보는 SDE 계층에서 복호화 한 후 LLC 계층으로 보내어져야 하므로 송신시와 반대가 되는 작업을 수행하게 된다. MODULE SDE_REMOVE CLEAR HEADER에서 Clear Header를 제거한 후 MODULE DECIPHERING DES에서 DES 적용을 복호화하고 MODULE SDE_REMOVE PAD, MODULESDE_REMOVE PROTECTED HEADER에서 Pad와 Protected Header를 제거한 후 LLC계층으로 보내진다.

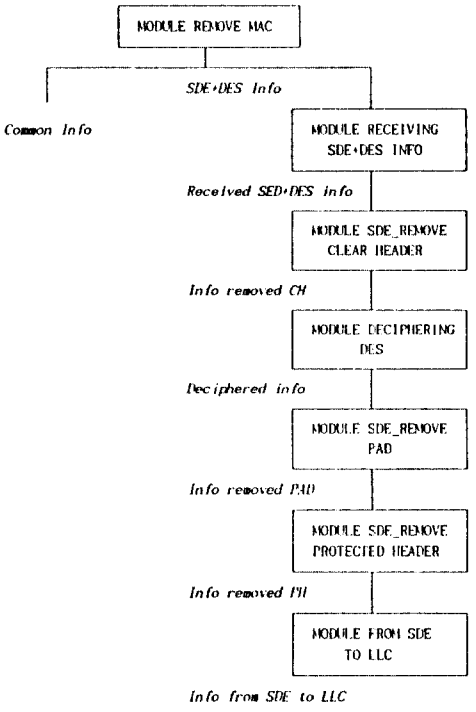


그림 3. 수신을 위한 작업처리 과정

6. 결과 분석

본 논문에서 암호화 서비스를 적용한 결과를 얻기 위해서 다음과 같은 자료를 사용하였다.

5개의 스테이션을 갖는 Ethernet 환경에서 DES 알고리즘이 적용된 시스템을 시뮬레이션하였다. 각 스테이션은 시뮬레이션 시 모든 조건이 동일하므로 메시지의 도착 간격의 감소는 스테이션의 증가를

의미할 수 있다. 따라서 본 논문과 같이 스테이션의 수가 고정되어 있다 하더라도 스테이션의 수가 다양한 Ethernet 환경에 본 논문의 결과가 적용될 수 있다.

각 스테이션의 MODULE LLC에서 발생되는 하나의 메시지의 길이는 1280bits, 암호화가 적용되는 메시지의 경우 더해지는 길이는 앞의 SDE 부분에서 설명된 바와 같이 232bits(29 octets)이다. MODULE DES와 MODULE DECIPHERING DES의 수행시간은, 64 bits 당 DES 알고리즘을 적용하고 한 명령어 수행시간을 1 Basic Cycle Time(Micro Second)으로 할 때 약 6000 Basic Cycle Time이 걸린다. 그리고 Ethernet으로 전송하기 전 붙여져야 하는 MAC Header의 길이는 208bits를 사용하였다. 또한 메시지는 지수 분포(Exponential Distribution)로 도착한다.

그림 4와 그림 5는 위와 같은 자료를 적용하여 여러번의 시뮬레이션을 행한 결과를 보여 준다.

그림 4는 각 스테이션의 LLC계층을 거쳐 오는 메시지의 도착 간격을 0.1, 0.2, 0.3, 0.4, 0.5, 0.6초로 지정했을 때 메시지의 평균 전달시간을 나타내는 그래프로서 전체 메시지중 보안이 필요한 메시지와 일반 메시지의 비율이 2 : 8, 3 : 7, 4 : 6, 5 : 5, 6 : 4인 경우를 비교하여 암호화의 정도가 시스템에 미치는 영향을 보여준다. 각 스테이션의 메시지 도착 간격이 0.4, 0.5, 0.6초 일 때와 같이 교통량이 적은 상황에서는 암호화의 정도가 평균 메시지 전달시간에 큰 영향을 주지 않는데 비해, 각 스테이션의 메시지 도착 간격이 감소함에 따라 암호화 정도가 클 수록 메시지의 평균 전달시간이 급격히 증가한다. 그러므로, 0.1, 0.2초 일 때와 같이 교통량이 많은 상황에서는 암호화의 정도가 평균 메시지 전달시간에 극심한 영향을 미침을 알 수 있다.

위의 결과를 볼 때 교통량이 적은 LAN환경에서는 암호화 정도가 성능을 저하시키는 정도가 적으므로 보안이 필요한 많은 정보를 암호화 할 수 있다. 그러나, 교통량이 많은 경우 아주 중요한 정보를 선별하여 암호화하는 것이 LAN의 성능을 고려할 때 합리적이다. 보안 서비스를 제공하기 위해 DES를 적용하고자 하는 Ethernet 환경의 사용자는 본 논문의 결과를 통해 사용자 LAN 환경에 따라 원하는 시스템의 성능과 부합되는 정보의 암호화의 정도를 결정할 수 있다. 메시지 도착 간격과 같은 사용자의 LAN 환경의 변화가 있을 때마다 정보의 암호화 정도도 변화시켜 사용자가 원하는 LAN의 성능을 유지할 수 있다. 정보의 암호화 정도가 정해지면 정보의 중요도에 의한 우선 순위에 따라 메시지에 DES를 적용하여 전송한다.

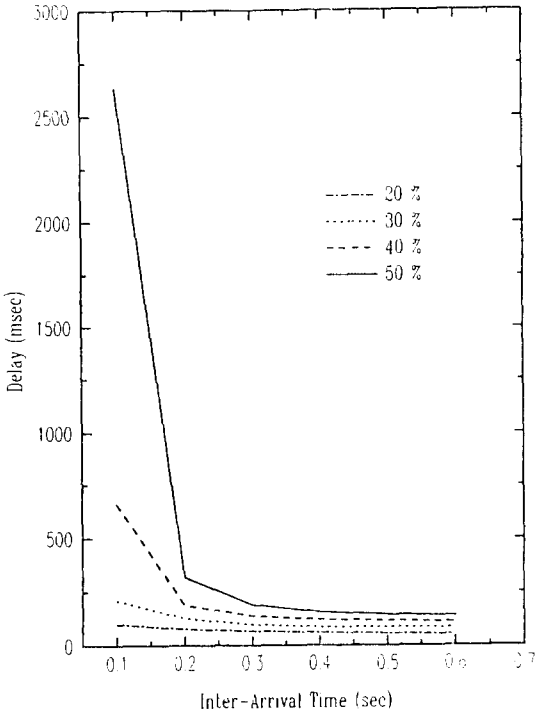


그림 4. 암호화 정도에 대한 전달시간의 비교

그림 5는 각 스테이션의 LLC 계층을 거쳐 오는 메시지의 도착 간격을 0.1, 0.2, 0.3, 0.4, 0.5, 0.6초로 지정 했을 때 메시지의 평균 메시지 전달시간을 나타내는 그래프로서 전체 메시지중 보안이 필요한 메시지와 일반 메시지의 비율이 4 : 6인 경우에 보안 서비스를 적용할 메시지와 일반 메시지 각각이 시스템에 미치는 영향을 보여 준다. 이 그림을 통하여 보안 서비스가 적용되는 메시지가 일반 메시지보다 훨씬 더 평균 메시지 전달시간에 큰 영향을 끼침을 알 수 있다. 특히 교통량이 많은 상황에서

암호화 서비스가 적용되는 메시지의 전달시간이 일반 메시지의 전달시간이 증가하는 것 보다 급격히 증가한다는 사실은 그림 4에서 얻은 암호화 정도가 평균 메시지 전달시간에 미치는 영향에 관한 결론을 뒷받침한다.

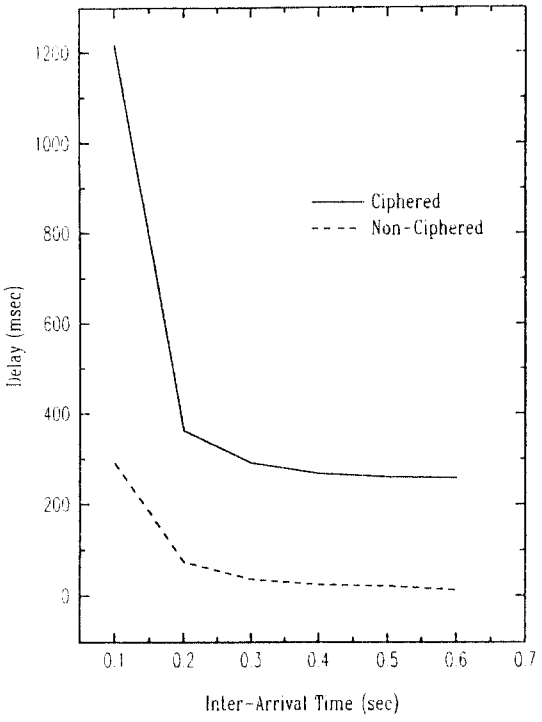


그림 5.암호화 메시지와 일반 메시지에 대한 전달시간의 비교

7. 결 론

LAN의 사용량이 증가할 때에 LAN상에서 주고받는 정보의 보호는 필연적인 것이 될 것이다. 그러나, LAN상에 암호화 알고리즘을 적용하는 것은 그 알고리즘을 적용하지 않을 때보다 정보가 전달되어지는 시간이 더 걸리기 때문에 적용되어지는 암호화 알고리즘이 LAN의 성능에 미치는 영향을 미리 예측한 후 실제 LAN에 암호화 알고리즘을 적용하는 것이 중요하다. 또한 메시지 도착 간격과 같은 사용자의 LAN 환경의 변화가 있을 때마다 원하는 LAN의 성능에 부합되는 정보의 암호화 정도를 결정하여 암호화 알고리즘을 적용하는 것이 필요하다.

따라서 본 논문에서는 정보 보안을 위한 암호 알고리즘을 기존의 LAN 프로토콜에 적용하여 LAN의 성능을 평가하였다. 이 논문에서는 현재 국내외적으로 가장 널리 사용되어지고 있는 LAN인 Ethernet을 중심으로 현재 표준화가 진행중에 있는 IEEE 802.10 SILS에 의해서 제안된 SDE 프로토콜에 대표적인 단일키 암호 시스템인 DES 알고리즘을 적용하여 보안 서비스의 제공 정도가 Ethernet상의 정보 전달속도에 미치는 영향을 시뮬레이션을 통하여 성능 분석하여 살펴 보았다.

시뮬레이션 모델을 통한 성능분석 결과, 교통량이 많은 상황에서는 교통량이 적은 상황에 비해 암호화의 정도가 평균 메시지 전달시간에 큰 영향을 미침을 알수 있었다. 그래서 교통량이 적은 LAN 환경에서는 암호화 정도가 성능을 저하시키는 정도가 적으므로 보안이 필요한 많은 정보를 암호화 할 수 있으나, 교통량이 많은 경우 아주 중요한 정보를 선별하여 암호화하는 것이 LAN의 성능을 고려할 때 합리적이다. 보안 서비스를 제공하기 위해 DES를 적용하고자 하는 Ethernet 환경의 사용자는 본 논문의 결과를 통해 사용자 LAN 환경에 따라 원하는 시스템의 성능과 부합되는 정보의 암호화의 정도를 결정할 수 있다. 메시지 도착 간격과 같은 사용자의 LAN 환경의 변화가 있을 때마다 정보의 암호화 정도도 변화시켜 사용자가 원하는 LAN의 성능을 유지할 수 있다. 정보의 암호화 정도가 정해지면 정보의 중요도에 의해 메시지에 DES를 적용하여 전송하기 위해 정보의 중요도에 따라 정보에 우선 순위를 주는 것이 필요하다.

이 논문에서 제시된 Ethernet상의 성능 평가 모델링 방법을 Token Ring이나 FDDI(Fiber Distributed Data Interface)와 같은 다른 LAN의 성능 평가에 적용할 수 있고, 또한 DES이외의 RSA나 Knapsack과 같은 공개키 암호화 알고리즘 등의 성능 평가 모델 개발에 적용할 수 있다.

8. 참고 문헌

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

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

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

[4] W.Bux, "Local-Area Subnetworks : A performance comparison", IEEE Trans. Commun., Vol. COM-29, no.10, pp. 1465-1473, Oct. 1981.

[5] S.S.Lam, "A Carrier Sense Multiple Access Protocol for Local Networks", Comput. Networks, Vol. 4, pp. 21-32, 1980.

[6] F.A.Tobali and V.B. Hunt, "Performance Analysis of Carrier Sense Multiple Access with Collision Detection", Computer Networks, Vol.4, pp.245-259, 1980.

[7] IEEE Standard 802.2, "Logical Link control", 1985.

[8] IEEE Standard 802.4, "Local Area Networks : Token-Passing Bus access method and physical layer specifications", 1985.

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

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

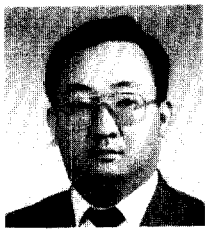
□ 著者紹介

김 희 림

1983년 2월 이화여자대학교 전자계산학과 학사 졸업
1993년 3월~현재 이화여자대학교 전자계산학과 대학원

안 옥 정

1993년 2월 이화여자대학교 전자계산학과 학사
1993년 3월~현재 이화여자대학교 전자계산학과 대학원



채 기 준

1982년연세대학교 수학과(학사)
1984년 미국 시라큐즈 대학교 전자계산학(석사)
1990년 미국 노스캐롤라이나 주립대학 컴퓨터 공학(박사)
1990년 8월~1992년 2월 미국 해군사관학교 전자계산학과 조교수
1992년 3월~현재 이화여자대학교 전자계산학과 조교수