LAN의 보안서비스에 대한 성능평가

안옥정　　김회림　　채기준
이화여자대학교 전자계산학과
서울 서대문구 대현동 11-1
Tel) 360-2370, 3231　　Fax) 313-2633

급변하고있는 정보화 사회에서 컴퓨터 사용이 증가하면서 네트워크를 이용한 정보 교환이 증가함에 따라 그 정보전달 속도와 신뢰성이 점점 더 중요해 지고 있다. 특히 중요한 정보의 보호를 위하여 정보를 암호화하고 암호화된 정보를 인정된 사용자만이 해독하여 정보를 안전하게 활용하는 암호화 기술을 네트워크에 어떻게 적용하는 가는 매우 중요한 문제이다. 1970년대 후반 Xerox사에서 Ethernet이라는 근거리 통신망 (Local Area Network: LAN)을 처음 소개한 후 LAN의 사용자는 전세계적으로 급속한 속도로 증가하였고, 국내에서도 1980년대 중반 이후 LAN의 보급이 급격히 증가하는 추세이다. 이와 같은 추세로 볼 때 LAN의 사용량이 증가함에 따라 LAN 상에서 주고 받는 정보의 보호는 필연적인 것이 될 것이다. 그러나, LAN 상에 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.

본 논문에서는 현재 국내외적으로 가장 널리 사용되어지고 있는 LAN인 Ethernet을 중심으로 현재 표준화가 진행중에 있는 IEEE 802.10 SILS (Standard for Interoperable LAN Security)에 의해서 제안된 SDE (Secure Data Exchange) 프로토콜에, IBM에서 Lucifer 시스템을 개선하여 개발한 암호 시스템으로 1977년 미국 상무성의 국립 표준국 (National Bureau of Standard: NBS)에서 미국 표준암호 알고리즘으로 채택한 대표적인 단일키 암호 시스템인 DES (Data Encryption Standard) 알고리즘을 적용 하였다. 성능평가를 위하여 시뮬레이션 패키지인 NETWORK II.5를 사용하여 Ethernet에 여러 개의 스테이션들이 접속되어 있는 상황에서 보안 서비스를 적용한 시스템을 실제 모델링하고 성능평가 결과를 분석하였다.

시뮬레이션 모델을 통한 결과를 분석해 보면 교통량이 적은 상황에서는 암호화의 정도가 평균 메시지 전달시간에 큰 영향을 주지 않는데 비해, 교통량이 많은 상황에서는 암호화의 정도가 평균 메시지 전달시간에 극심한 영향을 미침을 알 수 있었다. 즉, 교통량이 적은 LAN 환경에서는 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. 다른 해결 방안으로는 성능이 우수한 프로세서를 사용하여 평균 메시지 처리시간을 줄일 수 있다. 또한 보안 서비스가 적용되는 메시지가 일반 메시지보다 훨씬 더 평균 메시지 전달시간에 큰 영향을 끼침을 알 수 있었다. 특히 교통량이 많은 상황에서 암호화 서비스가 적용되는 메시지의 전달시간이 일반 메시지의 전달시간이 증가하는 것보다 급격히 증가한다는 사실을 확인했다.