안전한 데이터 통신에서의 지연분석

신 상 욱 , 이 경 현

부경대학교 전자계산학과

Delay Analysis on Secure Data Communications

Sang Uk Shin , Kyung Hyune Rhee

Dept. of Computer Science , Pukyong National University

Abstract

In this paper, we quantify the tradeoff between security and performance in secure data communication systems based on the queueing theory, and propose the optimization methods, such as the preprocessing, a message segmentation, compression, integration of compression and encryption and integration of user authentication and access control, which are able to reduce the delay induced by the security mechanisms and protocols. Moreover, we analyze the average delay for the secure data communication systems through the computer simulations, which are modeled by $M/M/1$, $M/E_2/1$ and $M/H_2/1$ queueing systems, respectively. We consider the DES, RSA digital signature and the combination of IDEA and RSA as security mechanisms for applying security services.

1. 서론

급변하는 정보화 사회에서 컴퓨터의 사용이 증가하면서 필연적으로 컴퓨터 네트워크의 급속한 보급이 이루어지고 이에 따라 정보 통신 서비스의 역할이 중요시되어 통신 기능의 고도화가 요구되고 있으며, 또한 안전하고 효율적인 통신 시스템을 구축하기 위한 요구가 증대되고 있다. 이런 환경에서 시큐리티는 네트워크의 필수적인 요구 사항이 되어 왔으며 특히 강한 시큐리티 기술이 통신 네트워크에서 정보를 보호하기 위해 요구되어진다. 하지만 점점 더 고속화되어 가는 네트워크 환경에서 이러한 시큐리티 요구 사항은 필연적으로 네트워크의 성능 저하를 유발한다. 즉, 기밀 통신을 위해 시큐리티 서비스를 적용하여 통신할 경우 정보가 발생하여 전송된 후 모든 시큐리티 서비스를 받아 처리가 끝날 때까지의 시간인 메시지 전달 지연 시간이 증가하고, 네트워크의 성능에도 영향을 미친다. 따라서, 네트워크 성능을 적정 수준으로 유지하기 위해 어느 정도의 시큐리티 서비스를 제공할 것인지를 결정하기 위해서는 시큐리티 서비스가 네트워크의 성능에 얼마만한 영향을 미치는 지를 알아야한다.

그러나, 지금까지 시큐리티 기법과 네트워크의 성능 각각에 대해 독립적으로는 많은 연구가 있었지만, 컴퓨터 네트워크에서 시큐리티와 성능 요구 사항 사이의 tradeoff에 대한 연구는 적었다. Zorkadis[1]는 기밀 네트워크에서의 시큐리티와 성능 사이의 tradeoff를 대기 이론의 M/D/1 시스템을 이용하여 분석하였고, 성능 향상을 위한 최적화 기법으로 암호화 과정에 대한 전처리를 제시하고 분석하였다. 김희림, 채기준[2]은 LAN(Local Area Network) 상에 시큐리티 서비스를 적용하기 위해, Ethernet, Token Ring, FDDI(Fiber Distributed Data Interface)를 사용하여 DES (Data Encryption Standard), Knapsack, RSA와 같은 암호 시스템을 적용하여, 시큐리티 서비스를 적용했을 때의 시큐리티와 성능 사이의 tradeoff를

분석하였다. 본 논문에서는 데이터 통신 시스템에 시큐리티 서비스가 제공되어졌을 때, 시큐리티와 성능 사이의 tradeoff를 정량화하여 보이고, 기밀 통신 시스템의 성능을 향상시키기 위한 최적화 기법으로 Zorkadis가 제안한 암호화 과정에 대한 전처리 기법에 다른 서비스가 추가되어졌을 때의 성능을 분석한다. 또한 메시지의 분할과 압축 기법을 제시하고 암호화와 압축의 결합 기법, 사용자 인증과 액세스 제어의 통합도 제시한다. 그리고, 시큐리티 서비스를 제공하기 위해 DES, RSA를 이용한 디지털 서명, IDEA (International Data Encryption Algorithm)와 RSA를 결합한 기법을 사용한 각각의 경우에 대해 이들을 대기 체계의 $M/E_2/1$, $M/M/1$ 와 $M/H_2/1$ 시스템으로 모델링한 후 네트워크에서 평균 지연을 분석한다.

먼저 2장에서는 중요한 시큐리티 서비스 계층들과 시큐리티 메커니즘을 살펴보고, 3장에서는 시큐리티와 성능 사이의 tradeoff를 살펴보고, 4장에서는 최적화 기법을 기술하고 분석한다. 그리고, 5장에서는 각 시큐리티 메커니즘을 적용한 기밀 통신망에서의 지연을 대기 체계의 $M/E_2/1$, $M/M/1$ 와 $M/H_2/1$ 시스템으로 모델링한 후 비교, 분석한다.

2. 시큐리티 서비스와 시큐리티 메커니즘

2.1 시큐리티 서비스

기밀 통신 시스템에는 OSI(Open Systems Interconnection) 시큐리티 구조 7498-2에 규정된 5가지 시큐리티 서비스가 있다.

1) 인증(Authetication) 서비스[3]는 메시지 인증뿐만 아니라 통신 개체의 일방 또는 쌍방 인증을 뜻한다. 통신 개체 인증은 메시지를 교환하기 전에 일어나고, 메시지 인증은 데이터 전송 단계 동안 일어난다. 인증은 메시지 교환 전에 그리고 데이터 전송 단계 동안 성능에 영향을 미친다.

2) 액세스 제어(Access Control) 서비스[3]은 연결 지향 통신에서는 연결 설정 단계에, 무연결 통신에서는 각 메시지에 대해 발생한다. 성능 관점에서 이는 분명한 계산 비용을 발생시킨다.

3) 기밀(Confidentiality) 서비스[3]은 메시지의 전체 또는 일부뿐만 아니라 트래픽에 관련된 정보에 대해 사용될 수 있다. 이 서비스는 암호 알고리즘에 기초한다. 성능 관점에서는 항상 종국 시스템에서 처리 비용을 초래한다. 키 교환과 암호 알고리즘 파라메터에 관련된 추가 비용도 발생한다.

4) 무결성(Integrity) 서비스[3]은 허가 없이 데이터를 변경, 삭제, 대치하는 것을 방지한다. 메시지에 sequence number 와 check sums 등을 추가하고, replay attack에 대해 time stamp를 사용한다. 이로 인한메시지의 확장과 check sum 계산 등이 성능에 영향을 끼친다.

5) 부인 방지(Non-Repudiation) 서비스[3]은 통신 당사자가 메시지 교환이 일어났다는 것을 나중에 부인하는 것을 방지하기 위한 서비스이다. 이는 항상 인증, 무결성 서비스를 포함하고, 이로 인해 추가적인 비용이 발생한다.

위에서 시큐리티 서비스에 따라 발생하는 성능 비용을 살펴보았다. 연결 지향 통신에서는 연결 설정 단계와 데이터 전송 단계가 중요하다. 고려해야 할 성능 척도로는 효율과 지연이 있다. 연결 설정 단계에서는 지연이 중요한 고려 사항이고, 데이터 전송 단계에서는 무연결 통신과 마찬가지로 두 가지 모두를 고려해야 한다. 본 논문에서는 데이터 전송 단계에서의 성능만을 고려한다.

2.2 시큐리티 메커니즘

본 논문에서는 시큐리티 메커니즘으로 다음 3가지의 경우를 고려한다. 즉, DES를 이용한 경우, RSA의 디지털 서명을 이용한 경우와 IDEA와 RSA의 결합시켜 적용한 경우이다.

1) DES[4,5,6,7,8]를 이용한 경우는 기밀 서비스로 DES를 적용하고, MD5(Message Digest 5) 메시지 digest 알고리즘[8]을 사용하여 인증 서비스를, 여기에 타임스탬프를 추가하여 무결성 서비스를 제공한다. 이 경우에는 인증 서비스를 제공하기 위해 사전에 교환된 전송측과 수신측만이 알고 있는 비밀키 값을 이용하여 메시지 digest를 계산한다.

2) RSA를 사용한 디지털 서명[4,5,6,7,8]을 적용한 경우로, 먼저 MD5를 사용하여 메시지 digest를 계

산한 후, 이를 자신의 비밀키를 이용하여 서명을 한다. 서명이 된 메시지 digest와 원래의 메시지에 상대방의 공개키를 이용하여 암호화하여 이를 전송한다. 이 경우에는 위에서 기술한 시큐리티 서비스 중에서 액세스 제어를 제외한 나머지 서비스를 하나의 서비스 메커니즘으로 모두 제공해 줄 수 있게 된다. 본 논문에서 사용된 RSA의 키 크기는 512 비트이다.

3) IDEA[4,5,6,7,8]와 RSA를 결합한 경우는 먼저 MD5를 이용하여 메시지 digest를 계산한 후, 이를 자신의 비밀키를 이용하여 서명한다. 서명한 메시지 digest와 원래 메시지에 대해 기밀 서비스로는 IDEA를 사용한다. 이 경우 RSA는 전체 메시지가 아닌 128 비트의 메시지 digest에만 적용된다. 이때 키의 크기는 512비트이다.

2.3 다정도(Multiple-precision) 연산

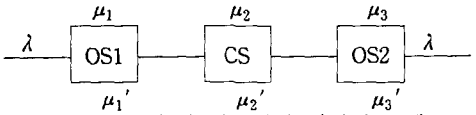
공개키 암호화 방식에서는 일반적으로 사용되는 컴퓨터의 정수 범위를 넘는 큰 정수의 연산을 필요로 한다. 이런 경우 정수의 배열을 사용하여 연산을 하게 되는데 본 논문에서는 기존에 이미 알려져 있는 다정도 연산 알고리즘[11,12]을 이용하였다. 그리고, 다정도 연산을 하기 위해서는 단정도 연산을 이용하기 때문에 효율적인 다정도 연산을 위해서는 베이스의 선택이 중요하다. 본 논문에서는 베이스를 2^{16}으로 선택하였다.

또한, RSA 암호 방식의 경우 지수 연산을 필요로 하므로 고속 지수 계산법을 적용하여 수행 시간을 줄였다. 본 논문에서는 Russian peasant combined exponentiation/modulo 알고리즘[12]을 이용하였다. 그리고, 두 개의 서로 소인 p 와 q를 알고 있는 경우에는 Chinese Remainder Theorem을 이용한 모듈러 지수 연산[12]을 사용하여 수행 시간을 줄였다. 이것은 모듈러 n 이나 지수 e 를 요구하지 않고 미리 계산된 값을 사용한다.

3. 통신 시스템 모델링 및 지연 분석

이 절에서는 시큐리티 서비스를 제공해 주는 시스템과 제공하지 않는 시스템을 모델링하여 분석한다. 모델은 3가지 요소로 구성된다. <그림 2>는 두개의 개방형 통신 시스템 (OS1, OS2)과 하나의 통신 서브시스템(CS)을 가진 모델을 나타낸다. 모델의 예로 T1회선을 사용하는 Interlock 시스템[13]을 고려한다. Interlock 시스템은 500Kbps의 암호화와 1.2Mbps의 데이터 무결성과 데이터 origin 인증을 제공한다. 도착과정에서는 평균도착률 λ의 포아송 분포를 따르고, 서비스 시간은 각각 서비스율 μ_i $(i=1,2,3)$의 상수 값을 갖는 것으로 가정한다.

시큐리티 서비스를 고려하면, 도착율 λ는 같게 유지되지만 서비스율은 추가적인 처리 비용과 메시지 확장으로 인해 μ'_i $(i=1,2,3)$로 바뀐다. 최대 효율은 파라메터 $\mu'_b = \min(u_i')$, $i \in \{1,2,3\}$를 가진 병목 큐에 의해 결정된다.



<그림 2> 통신 시스템의 간단한 모델

Utilization $\rho_i = \frac{\lambda}{\mu_i}$ 로, $s_i = \frac{\mu_i}{\mu'_i}$ 라 두면, $\rho'_i = \frac{\lambda}{\mu'_i} = s_i(\frac{\lambda}{\mu_i}) = s_i\rho_i$ (1)

시스템에서 평균 지연은 시스템의 각 큐에서 소비한 시간의 합과 같다. 이 모델은 M/D/1 대기 체계[14,15]로 병목 요소를 결정하여 다른 요소에서 소비한 서비스 시간을 더함으로써 지연을 계산할 수 있다. 안전성이 보장되지 않는 시스템에서 평균시간을 T로, 안전한 시스템에서 평균시간을 T'라 두면 다음과 같이 T와 T'를 구할 수 있다.

$$T = \frac{1}{\mu_b} + \frac{1}{\mu_b}\frac{\rho_b}{2(1-\rho_b)} + \sum_{i=1, i\neq b}^{3}\frac{1}{\mu_i} \quad (2)$$

$$= \frac{1}{\mu_b}\frac{\rho_b}{2(1-\rho_b)} + \sum_{i=1}^{3}\frac{1}{\mu_i}$$

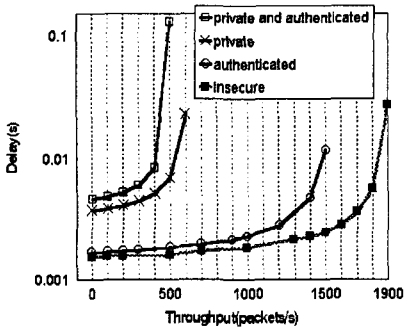
$$T' = \frac{1}{\mu'_b} + \frac{1}{\mu'_b}\frac{\rho'_b}{2(1-\rho'_b)} + \sum_{i=1, i\neq b}^{3}\frac{1}{\mu'_i} \quad (3)$$

$$= \frac{1}{\mu'_b}\frac{\rho'_b}{2(1-\rho'_b)} + \sum_{i=1}^{3}\frac{s_i}{\mu_i}$$

S_i는 시큐리티 기능뿐만 아니라 메시지 길이에도 의존하고, 통신 프로토콜에도 의존한다. 시큐리티로 인한 메시지 확장은 CRC와 같은 기능에 대해 더 많은 서비스 시간을 초래하지만, routing과 같은 기능에 대해서는 그렇지 않다. <그림 3>은 다음의 4가지 예에 대한 지연을 비교한 그래프이다.

1) $u_1 = u_2 = u_3 = 1920$ packets/s , 100bytes 길이 packet에 대한 insecure 통신
2) $u'_1 = u'_3 = 1920$ packets/s , $u'_2 = 1548$ packets/s, 데이터 무결성과 origin 인증
3) $u'_1 = u'_3 = 625$ packets/s , $u'_2 = 1920$ packets/s, 100bytes 길이 packet에 대한 암호화
4) $u'_1 = u'_3 = 504$ packets/s , $u'_2 = 1548$ packets/s, 100+24 bytes 길이 packet에 대한 인증과 암호화 (OS1과 OS2에서 암호화 서비스 시간은 500Kbps이다)

<그림 3>에서 시큐리티 서비스 추가와 지연 증가 사이에 tradeoff가 있음을 명확히 알 수 있다.



<그림 3> Throughput에 대한 case 1), 2), 3), 4)의 Average Delay

4. 최적화

이 장에서는 성능 향상을 위해 더 빠른 하드웨어나 소프트웨어의 사용은 물론 분산 처리 시스템에서와 같이 병렬 처리의 수행을 배제한 최적화 개념[1]을 고려한다. 느린 요소를 더 빠른 요소로 대치하지 않고 최대 효율을 증가시킬 수는 없다. 그렇지만, 같은 효율에 대해 지연은 개선할 수가 있다. 최적화 기법으로는 먼저 암호화 서비스에 대해 전처리 기법을 사용하여 처리 시간을 줄일 수가 있음을 보인다. 그리고, 기밀 서비스이외의 다른 서비스가 추가되었을 때의 지연을 분석한다. 메시지 분할과 메시지 압축에 의해서도 성능의 향상을 이룰 수 있다

4.1 전처리

이 절에서는 암호화에 대한 전처리만을 고려한다. 암호화를 위해 DES의 OFB (Output Feedback) mode [5,6,7]를 사용한다. OFB mode는 CFB(Cipher Feedback)나 CBC(Cipher Block Chaining) mode와 달리 에러 전파가 일어나지 않는다. 그렇지만, 좀더 복잡한 동기화 과정이 요구되고, 비트 오류에 민감하다. OFB mode를 사용하면, 실제 암호화 기능은 이진 난수 발생기(pseudo-random bit string generator)처럼 사용된다. 여기서는 연결 지향 통신의 경우만을 고려한다. 시스템은 idle 과 busy 상태가 교대로 일어나기 때문에, OFB mode를 사용했을 때 이진 난수 발생기를 전처리하여 지연을 줄일 수가 있다.

3장에서와 같이 도착은 파라메터 λ의 포아송 분포를 따르고, d 결정적 서비스 시간을 가진 M/D/1 시스템을 가정한다. 큐에 메시지가 없고 서비스 중인 마지막 메시지가 서버를 떠나면, 즉 시스템이 idle 상태가 되면, 서버는 다음에 도착할 메시지를 위해 이진 난수 발생을 전처리한다. 분석을 단순화시키기 위해, 서버는 idle 상태 동안 다른 메시지에 대한 적절한 이진 난수 발생을 전처리하고, 다음 메시지 도착 전에 이진 난수 발생이 다 처리되면, 시스템은 idle 상태가 된다. 그리고, XOR 연산의 처리 시간은 무시한다.

메시지가 도착할 때 시스템의 상태는 다음 중의 하나이다.

1) 확률 p로, 시스템은 새로운 메시지보다 이전에 도착한 메시지들을 가진 busy 상태이다. 이 경우 메

시지는 자기앞에 도착한 메시지가 처리되기까지 대기해야 한다. 서버의 서비스 시간은 d이다.

2) 확률 (1-p)로, 시스템은 새로 도착할 메시지를 위해 필요한 처리의 전부 또는 일부를 전처리한다. 그래서, 새로운 서비스 시간은 마지막 메시지가 시스템을 떠난 이후 경과한 시간에 의존한다. 0 에서 d 사이의 값을 가진다.

포아송 도착을 가정했기 때문에 idle period는 M/G/1 시스템처럼 지수 분포를 따른다[14,15,16]. g(y)를 새로운 서비스 시간에 대한 확률밀도함수(probability density function)로 두고, $G^*(s)$을 Laplace transform이라 하자.

$$g(y) = pu(y-d)+(1-p)f(y) \quad (4) \qquad f(y) = \begin{cases} \lambda e^{-\lambda(d-y)} + e^{-\lambda d}u(y) & ,0 \le y \le d \\ 0 & ,otherwise \end{cases} \quad (5)$$

$u(y-d)$는 unit impluse 함수이다.

p는 시스템이 전처리 부분 없이 메시지를 처리하는 시간 비율이다. 새로운 서비스 시간을 d'라 두자. 그러면, p와 d'는 다음과 같이 얻어진다.

$$p = d'\lambda = \lambda\left[pd + (1-p)\int_0^d yf(y)dy\right] \quad (6) \qquad d' = \begin{cases} d - \frac{1}{\lambda}(1-e^{-\lambda d}) & ,0 < \lambda \le \frac{1}{d} \\ 0 & ,\lambda = 0 \end{cases} \quad (7)$$

새로운 서비스 시간의 second moment를 $\overline{Y^2}$라 두면, 다음과 같이 구해진다.

$$\overline{Y^2} = \int_0^d y^2 g(y)dy \quad or \quad \frac{d^2G^*(s)}{ds^2}|_{s=0} = (-1)^2\overline{Y^2} \qquad \overline{Y^2} = \lambda d' d^2 + (1-\lambda d')\left\{d^2 - \frac{2}{\lambda^2}(d\lambda - 1 + e^{-\lambda d})\right\} \quad (9)$$

메시지가 시스템에 도착했을 때, 큐에서 대기하는 메시지 수와 그들의 서비스 시간은 독립적이다. 연속적인 메시지 사이에서는 전처리을 위한 idle period가 없기 때문에 모든 메시지에 대해 d의 서비스 시간이 요구된다. 그래서, 다음의 식이 유도된다[14,15,16].

$$E[W_i] = E[R_i] + E[\sum_{j=i-N_i}^{i-1} E[X_j = d | N_i \neq 0]] = E[R_i] + dE[N_i] \quad (10)$$

W_i : i번째 메시지의 큐에서 대기 시간

R_i : i번째 메시지에 의한 residual service time

X_j : j번째 메시지의 서비스 시간

N_i : i번째 메시지가 도착했을 때 큐에 대기하고 있는 메시지의 수

이 식에서, $i \to \infty$ 를 취하면, $W = R + dN_Q = R + \lambda dW = \frac{R}{(1-d\lambda)}$ (11)

R은 M/G/1 시스템에서처럼 $R = \frac{\lambda\overline{Y^2}}{2}$로 얻어진다[14,15,16].

전처리가 없을 때와 있을 때의 지연을 각각 T 와 T'라 두면, 이것은 Pollaczek-Khinchin formula [14,15,16]를 사용하여 다음과 같이 얻을 수 있다.

$$T = d + \frac{\lambda d^2}{2(1-d\lambda)} \quad , \quad T' = d' + \frac{\lambda\overline{Y^2}}{2(1-d\lambda)} \quad (12)$$

<그림 4>는 시스템 효율 ρ의 변화에 따른 T와 T'의 값을 비교한 그래프이다. ρ=0.4일 때 전처리를 하므로서 약 75%의 지연 감소율을 보이고, ρ=0.6일 때 60%, ρ=0.8일 때 35%의 감소율을 보인다.

다음은 암호화에 대한 전처리에 다른 시큐리티 서비스를 추가한 경우에 지연을 분석한다. 이 경우의 결정적인 서비스 시간을 d라 두면,

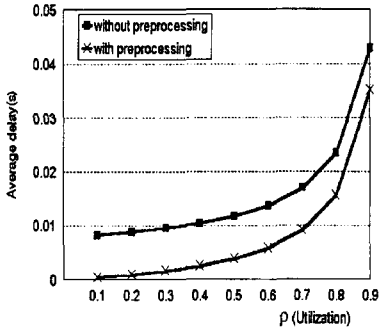
$d = d_e + d_{ai}$ (d_e : 암호화 서비스 시간 , d_{ai} : 인증과 무결성 서비스 시간)

이때의 새로운 서비스 시간 d'와 지연 T는 다음과 같다.

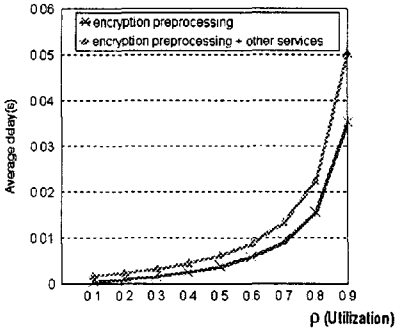
$$d' = \frac{d + d_{ai} - \frac{i}{\lambda}(1-e^{-\lambda d_e})}{e^{-\lambda d_e} - \lambda d_{ai}} \quad (13) \qquad \overline{Y^2} = \lambda d' d^2 + (1-\lambda d')\left\{d_e^2 + d_{ai}^2 - \frac{2}{\lambda^2}[\lambda d_e - 1 + e^{-\lambda d_e}]\right\} \quad (14)$$

$$T = d' + \frac{\lambda \overline{Y^2}}{2(1-\lambda d)} \qquad (15)$$

<그림 5>에서 전처리를 가진 기밀성 서비스에 다른 서비스를 추가함으로서 지연이 증가되는 것을 알 수 있다. 그러므로, 시큐리티 서비스의 추가와 지연의 증가 사이에 tradeoff가 존재함을 알 수 있다. 따라서, 트래픽의 양에 따라 필요한 서비스만을 제공해서 시스템의 성능을 적정 상태로 유지해 주어야 한다.



<그림 4> Utilization에 대한 전처리가 있을 때와 없을 때의 Average Delay



<그림 5> 암호화에 대한 전처리와 암호화에 대한 전처리에 다른 서비스를 추가했을 경우에 대한 Average Delay의 비교

4.2 메시지의 분할과 압축

긴 메시지에 시큐리티 서비스를 제공하여 통신할 때, 작은 데이터 unit으로 메시지를 분할함으로써 성능 향상을 이룰 수가 있다. 이는 packet 대 메시지 switching의 경우와 같다. 분할로 인한 추가적인 overhead가 데이터 unit의 길이를 결정하기 위해 고려되어져야 한다. 메시지의 일부가 병목 요소에서 서비스될 동안 다른 부분은 다음의 시스템 요소에서 서비스를 받을 수 있다는 것에 의해 성능에서의 향상을 이룰 수가 있다. RSA를 사용할 경우 메시지의 분할이 필요하고 이에 의해 처리 시간의 향상을 이룰 수 있다.

압축은 긴 메시지를 통신할 때 성능 척도에서 더 많은 향상을 얻기 위해 메시지 분할과 결합되어 사용될 수 있다. 압축에 의한 성능의 향상은 명확하다. 또다른 최적화의 방법으로 메시지 압축과 암호화를 결합하는 방법도 있다[17]. 산술 부호화에 비밀 키 기능을 부가하여 정보원 부호화와 동시에 정보 보안의 효과를 얻는다. 산술 부호화에 있어 부분 구간은 일반적으로 정보원 알파벳의 순서대로 위치시키게 되나, 그 순서를 변경함에 따라 같은 입력 계열에 대해 전혀 다른 부호 계열이 얻어지게 된다. 이 성질을 이용하여 산술 부호화 과정에서 정보 보안의 기능을 부여한다. 이와 같이 산술 부호화의 분할 구간을 랜덤 치환에 의해 변경시킴으로서 평균 부호의 길이를 약 5%정도 증가하는 정도에서 DES 출력에 대응하는 효과를 얻을 수 있다.

4.3 사용자 인증과 액세스 제어의 통합

외부 사용자가 시스템의 자원을 액세스 하기 위해서는 먼저 사용자 인증 단계를 거쳐야 한다. 사용자 인증을 위해 패스워드 검증 기법이 널리 쓰인다. 그리고, 사용자 인증을 거친후, 시스템은 사용자가 액세스하려는 자원에 대해 액세스 권한이 있는지를 판단해야 하는데, 이러한 액세스 권한의 검증을 액세스 제어라 한다. 액세스 제어의 안전성은 그 자체뿐만 아니라 사용자 인증 메카니즘에 의존하다. 따라서, 이 두가지 서비스를 나누어 처리하는 것보다는 하나의 모듈로 통합시키는 것을 고려해 볼 수 있다. Harn과 Lin[18]은 사용자 인증과 액세스 제어를 동시에 제공하면서, 시간 복잡도가 공개 키에 기초한 패스워드 인증 기법과 거의 같은 통합 기법을 제시했다. 이 기법은 3개의 단계로 나누어진다.

1) 등록 단계 : 각 사용자가 호스트 시스템으로부터 패스워드를 얻어 등록하는 단계

step 1. 시스템은 두 개의 큰 소수 p, q를 선택. N=p·q

그리고, $\gcd(a, N) = 1$이 되는 $a \in [2, N-1]$를 선택

step 2. 각 파일 F_j에 소수 ef_j를 할당, 그리고, $ef_j \cdot df_j \bmod \Phi(N)=1$이 되는 df_j 계산

파일 F_j의 권한 r에 관계되는 토큰 KF_j 계산, $KF_{j,r}=\alpha^{df_j} \bmod N$

시스템의 마스터 키 $K_{master}=(\alpha)^{\prod df_j^{-}} \bmod N$ 을 계산.

$T=\prod ef_j$ 를 계산하여 K_{master}는 비밀로 유지하고 T는 공개한다.

step 3. ID_i를 각 사용자에게 소수 eu_i를 할당, 그리고, $eu_i \cdot du_i \bmod \Phi(N)=1$이 되는 du_i 계산

파일 F_j에 액세스 권한 $r_{i,j}$를 가진 각 사용자 ID_i의 패스워드를 계산

$$PW_i=\alpha^{du_i \prod df_j^{r_{i,j}}} \bmod N$$

ID_i에게 비밀 패스워드 PW_i 를 할당하고, $t_i=\prod df_j^{r_{i,j}}$를 공개한다.

시스템은 p, q, K_{master}를 비밀로 유지하고 T를 공개한다. 각 사용자는 PW_i를 비밀로 유지하고, t_i를 공개한다.

2) 검증 단계 : ID_i를 가진 사용자가 파일 F_j에 권한 r을 가지고 액세스할 경우, 사용자는 5개의 정보 (ID_i , PW_i , t_i , F_j , r)을 시스템에 제출해야한다. 시스템은 먼저 ID_i가 정당한지 검사한 후, $A=t_i/ef_j^r$이 정수인지 확인한다. 만약 정수라면, 시스템의 K_{master}와 사용자 패스워드 PW_i로부터 권한 r에 관련된 두 개의 토큰을 계산하여 같은지를 검사한다.

$$V=(K_{master})^{T^{r}/ef_j} \bmod N=(\alpha)^{(\prod df_k^{r})*(\prod ef^{r})/(ef)} =(\alpha)^{1/ef_j}=(\alpha)^{df_j}=KF_{j,r}$$

$$V'=(PW_i)^{eu_i*t_i/ef_j} \bmod N=(\alpha)^{(du_i*\prod df_k^{r_{i,k}})(eu_i*\prod ef_k^{r_{i,k}})/ef_j} \bmod N =(\alpha)^{1/ef_j} \bmod N=KF_{j,r} \bmod N$$

만일 $V=V'$이면 사용자는 인증되어지고, 액세스 권한도 부여된다. 그렇지 않으면, 요구는 거부된다.

(3) 운영 단계 : 동적인 액세스 제어 메카니즘으로 사용자의 패스워드를 변경함으로서 모든 동작이 구현된다. 새로운 사용자의 삽입은 사용자의 권한에 해당하는 새 패스워드를 만들어 부여함으로서 수행되고, 사용자 삭제는 시스템에서 사용자 ID_i 항목을 삭제함으로서 수행된다. 새로운 파일의 삽입은 새로운 파일에 대한 액세스 권한을 가지는 사용자들의 패스워드를 갱신하여 배포함으로서 구현되고, 파일의 삭제는 시스템에서 대응하는 파일 항목을 삭제함으로서 수행된다. 액세스 권한을 부여하는 동작은 두 개의 단계를 거친다. 먼저, 권한 부여 요구를 한 사용자가 권한을 부여할 권리를 가졌는지 검증하는 권한 검증 단계를 거친후 새로운 권한을 받는 사용자의 패스워드를 발생시킨다. 액세스 권한의 취소 역시 두 개의 단계를 거치는데 먼저, 권한 검증 단계를 거친 후, 이 액세스 권한에 관련된 파일을 삭제하고, 앞의 새로운 파일 삽입 동작과 같이 시스템에 파일을 다시 삽입한다.

이와 같이 패스워드 인증과 액세스 제어를 하나의 모듈에 통합함으로서, 사용자는 자신의 패스워드만을 비밀로 유지하고, 시스템은 그것의 마스터 키만을 비밀로 유지하면 되므로 시스템에서 유지해야 할 비밀 정보의 양이 줄어들고, RSA와 거의 같은 정도의 안전성을 얻을 수 있다. 그리고, 기존의 공개 키에 기초한 패스워드 인증 기법과 같은 계산량을 가지면서 동시에 두 개의 서비스를 제공해 줄 수 있게 된다.

5. 대기 이론을 이용한 기밀 통신 네트워크의 성능 분석

이 장에서는 2장에서 논의한 3가지 시큐리티 메커니즘을 적용한 경우에 기밀 통신 네트워크의 성능을 대기 이론을 이용하여 분석한다. 각 시큐리티 메커니즘에 3가지의 대기 체계를 적용한다. 75MHz 펜티움 PC에서 Turbo-C++를 이용하여 시뮬레이션 하였다.

5.1 시뮬레이션 모델

대기 체계 중에서 3가지 모델을 시뮬레이션에 적용한다. 3가지 모델 모두에 대해 도착하는 메세지는 파라메터 λ의 포아송 분포를 따르고, T1 회선 (1.5Mbps)을 통해 통신을 한다고 가정한다. 본 논문에서는 키 발생과 키 분배는 고려하지 않는다. 그리고, 시스템이 항상 안정 상태를 유지하기 위해서는

$\rho = \frac{\lambda}{\mu} < 1$ 이 되어야 한다. 시큐리티 서비스를 제공할 경우 서비스율은 $\rho < 1$ 이 되도록 3장에서 와 같이 $\rho = s \times \frac{\lambda}{\mu}$, $s = \frac{\mu}{\mu'}$ 로 조정된다.

1) M/M/1 시스템[14,15,16]

서비스 시간은 확률밀도함수(probability density function)가

$$b(x) = \mu e^{-\mu x} \qquad (16)$$

인 파라메터 μ 를 가지는 지수 분포를 따른다.

2) M/ E_2/1 시스템[14,15,16]

서비스 시간은 확률밀도함수가

$$b(x) = 2\mu e^{-2\mu x} \qquad (17)$$

인 파라메터 μ 를 가지는 차수 2의 Erlang 분포를 따른다.

3) M/ H_2/1 시스템[14,15,16]

서비스 시간은 확률밀도함수가

$$b(x) = \frac{1}{3}\frac{\mu}{2}e^{-\frac{\mu x}{2}} + \frac{2}{3}2\mu e^{-2\mu x} \qquad (18)$$

인 파라메터 μ 를 가지는 차수 2의 Hyperexponential 분포를 따른다.

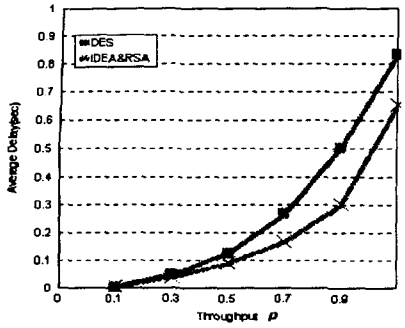
5.2 시뮬레이션 결과 및 분석

<그림 6>에서 <그림 8>의 그래프들로부터 각 시큐리티 메커니즘에 대해 3가지 대기 체계에서 거의 유사한 경향을 보임을 알 수 있다. RSA의 디지털 서명이 다른 2가지 메커니즘에 비해 평균 지연이 매우 크게 나타나는 것은 DES나 IDEA의 관용 암호 방식에 비해 RSA의 공개키 암호 방식의 처리속도가 거의 200배 정도 느리기 때문에 이러한 결과를 보이는 것이다. 하지만, 시큐리티 서비스의 추가와 지연의 증가 사이에 tradeoff가 존재하므로 하나의 시큐리티 메커니즘에 의한 서비스의 통합은 그렇지 않은 경우보다 이점이 있음을 알 수 있다. 이 경우에는 $\rho < 0.5$ 일 때는 (즉, low와 medium 트래픽인 경우) 트래픽이 증가해도 지연이 완만한 증가를 보이지만, heavy 트래픽인 경우, 지연이 급격하게 증가함을 알 수 있다. 그리고, DES를 이용한 경우와 IDEA와 RSA의 결합을 적용한 경우를 비교해 보면, 후자의 경우가 더 짧은 지연을 보이는 것을 알 수 있는데, 이것은 RSA의 사용은 128 비트의 메시지 digest에만 국한되어 수행 시간에 거의 영향을 주지 않고 IDEA의 처리 속도가 DES에 비해 빠르기 때문이다.
이 경우 트래픽이 적은 경우에는 비슷한 지연을 보이지만, 중간 정도의 트래픽에서 DES를 이용한 경우에 지연의 증가가 더 큰 것을 알 수 있다. ρ = 0.5 일때 DES를 사용한 것보다 IDEA와 RSA의 결합 기법을 사용하므로서 약 35%의 지연 감소를 보이고, ρ = 0.7 일 때는 약 47%의 향상을 얻을 수 있다. 트래픽이 증가할수록 IDEA와 RSA를 결합한 기법이 서비스 시간에서 얻는 이점은 많아짐을 알 수 있다.

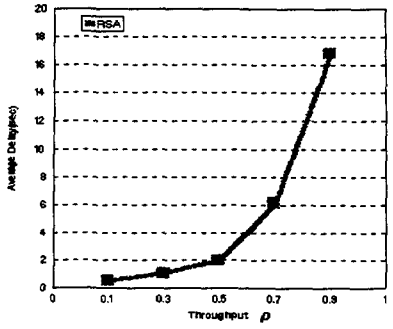
3가지 시큐리티 메커니즘에 거의 비슷하게 low 트래픽인 경우는 시큐리티 서비스에 의한 지연의 증가 정도가 적으나, heavy 트래픽인 경우, 지연이 급격하게 증가함을 알 수 있다. 그러므로, 트래픽이 많은 경우는 정보를 선별하여 시큐리티 서비스를 제공함으로서 네트워크의 성능을 적절한 상태로 유지해 줄 수 있다. 그리고, 급격한 지연 증가를 보이는 부분을 알면, 시스템의 성능을 적정 상태로 유지하기 위해 전체 메시지에 대한 시큐리티 서비스의 제공 비율을 조절할 수 있다.

6. 결론

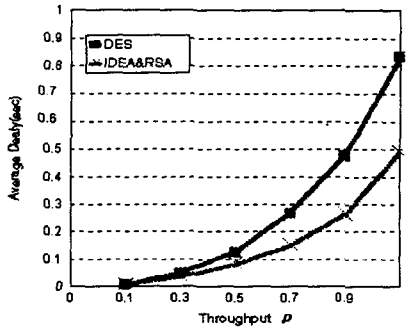
본 논문에서는 데이터 네트워크에서 시큐리티 서비스를 부가할 경우 대기 이론을 이용하여 이를 M/M/1 , M/ E_2/1 와 M/ H_2/1 시스템으로 모델링한 후 시스템의 지연 시간을 분석하였다. 부가적인 시큐리티 서비스는 OSI 시큐리티 서비스에 근간하였으며 시큐리티 서비스의 추가와 지연 사이의 tradeoff



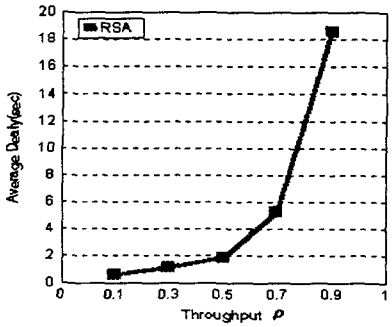
<그림 6-1> DES를 사용한 경우와 IDEA와 RSA를 결합하여 사용한 경우를 M/M/1 시스템을 적용했을 때 평균 지연



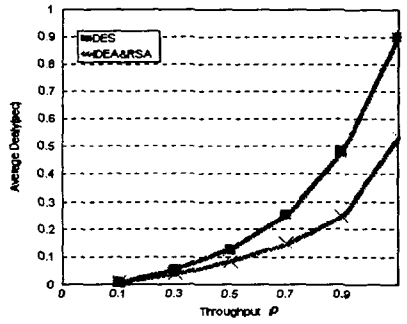
<그림 6-2> RSA의 디지털 서명을 사용한 경우에 M/M/1 시스템을 적용했을 때의 평균 지연



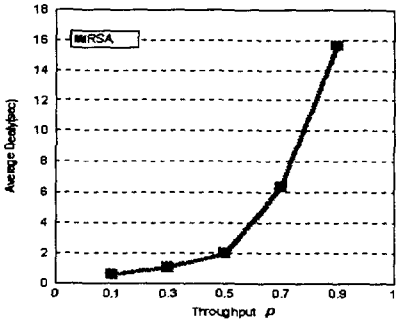
<그림 7-1> DES를 사용한 경우와 IDEA와 RSA를 결합하여 사용한 경우를 M/ E_2/1 시스템을 적용했을 때 평균 지연



<그림 7-2> RSA의 디지털 서명을 사용한 경우에 M/ E_2/1 시스템을 적용했을 때의 평균 지연



<그림 8-1> DES를 사용한 경우와 IDEA와 RSA를 결합하여 사용한 경우를 M/ H_2/1 시스템을 적용했을 때 평균 지연



<그림 8-2> RSA의 디지털 서명을 사용한 경우에 M/ H_2/1 시스템을 적용했을 때의 평균 지연

를 정량화하여 보였다. 지연을 줄이기 위해 최적화 개념을 도입하였는데 Zorkadis [1]는 DES의 OFB 모드를 이용한 기밀성 서비스에 대한 전처리를 고려하였는데, 본 논문에서는 이에 다른 서비스를 추가하므로서 발생하는 지연을 분석하였다. 그리고, RSA 디지털 서명을 이용한 시큐리티 서비스의 통합 기법을 소개하므로서 다양한 시큐리티 서비스를 제공할 수 있었다. RSA를 사용할 경우 서비스 시간(지연)의 증가는 필연적이지만(실제 RSA의 사용시 작은 e의 값을 사용함으로써 처리 시간을 줄일 수 있다)

시큐리티 서비스의 추가와 지연의 증가 사이에 tradeoff가 있음으로 하나의 시큐리티 메커니즘에 의한 서비스의 통합은 그렇지 않은 경우보다 이점이 있음을 알 수 있었다. 또한 IDEA와 RSA의 결합을 이용한 시큐리티 메커니즘을 사용하므로서 DES를 이용한 경우보다 서비스 시간에서 좀 더 향상된 결과를 보임을 알 수 있었다. 또한 압축과 암호화 과정을 결합하여 처리하는 방법과 사용자 인증과 액세스 제어의 통합 기법을 고려하므로서 또다른 통신 요구 서비스에 대한 성능 향상을 이룰 수 있었다.

시큐리티 서비스를 제공하는 네트워크에서 low 트래픽인 경우엔 시큐리티 서비스에 의한 지연의 증가가 완만하지만, heavy 트래픽인 경우엔 지연의 증가가 급격해진다. 그러므로, 네트워크의 성능을 적정 상태로 유지하기 위해서는 정보를 선별하여 시큐리티 서비스를 제공해줄 필요가 있고, 필요한 시큐리티 서비스만을 제공해줄 필요가 있다. 시큐리티 메커니즘에 관계없이 트래픽의 증가에 따라 어떤 부분에 이르면 지연이 급격하게 증가하는 것을 알 수 있으므로, 이러한 성능 저하 부분을 알게되면 적정 네트워크 성능을 얻기 위해 시큐리티 서비스를 제공할 메시지의 양을 조절할 수 있다.

또한 추후 연구 과제로 컴퓨터 네트워크 상에서 서버의 수가 다수인 경우에 대해 시큐리티 서비스의 수행에 따른 성능 평가를 위한 M/G/c 시스템으로의 모델링과 시큐리티 서비스에 필연적으로 발생하는 키 발생, 분배 등에 의한 서비스 등급에 따른 대기 이론 모델링에 대한 연구를 고려할 수 있다.

< 참 고 문 헌 >

[1] Vasilios Zorkadis, Security versus Performance Requirements in Data Communication Systems, ESORISC'94 Computer Security Lecture Notes in computer science, vol. 875, p.19~30, 1994

[2] 김 희림, 채 기준, 보안 서비스를 적용한 LAN의 성능 평가, 통신정보보호학회논문지, 6권, 1호, p.25~38, 1996, 3

[3] ISO 7498-2 : Security Architecture

[4] Warwick Ford, "Computer Communication Security", Prentice-Hall, 1994

[5] Gustavus J. Simmons, "Contemporary Cryptology", IEEE Press, 1992

[6] D.W. Davies, W.L. Price, "Security for Computer Networks", 2nd, John Wiley & Sons, 1989

[7] 한국전자통신연구소, 현대암호학, 1991

[8] B. Schneier, "Applied Cryptography", 2nd, John Wiley & Sons, 1996

[9] W. Stallings, "SNMP, SNMPv2 and CMIP : The practical guide to network management standards", Addison-Wesley, 1993

[10] W. Stallings, "Data and Computer Communications", 4nd, Macmillan, 1994

[11] D.E. Knuth, " The Art of Computer Programming, Vol.2, Seminumerical Algorithms ", 2nd, Addison-Wesley, 1981

[12] Philip Zimmermann, PGP source code, PGP 인터내셔널 홈페이지 (http://www.ifi.uio.no/pgp/)

[13] ANS CO+RE Systems, Interlock 2.1 and ANSKeyRing,(18.08.1993)

[14] L. Kleinrock, "Queueing Systems Volumn I : Theory", John Wiley & Sons, 1975

[15] D. Gross, C. M. Harris, "Fundamentals of Queueing Theory", John Wiley & Sons, 1985

[16] D. Bertsekas, R. Gallager, "Data Networks", Prentice-Hall, 2nd, 1989

[17] 박 지환, 이 경현, 오류 검출 및 정보보안 기능을 갖는 데이터 압축 방식에 관한 연구, 한국전자통신연구소, 1993

[18] L. Harn, H.Y. Lin, "Integration of user authentication and access control", IEE Proceedings, Vol.139, No.2, p. 139-143, March 1992