효율을 개선한 메시지 인증방식

°이 정 숙*, 이 임 영**

* 한국항공대학교 항공통신정보공학과, ** 순천향대학교 전산학과

Efficient Message Authentication Methods

°Jeong Sook Yi*, Im Yeong Lee**

* Dept. of Telecomm. and Inform. Eng., Hankuk Aviation University

** Dept. of Computer Science, Soon chun hyang University

요 약 문

통신로에서 메시지 수정 등을 검출하는 수단인 메시지 인증법에 관해 살펴보고, 기존의 방식과 새로 제안하는 방식을 메시지 에러율과 효율성면에서 고찰하여, 제안된 방식이 기존의 방식보다 통신로 비트 에러율이 10^{-2}~10^{-5}일 때 효율이 크게 좋아지고 메시지 에러율이 개선됨을 보인다.

1. 서론

컴퓨터의 보급이 늘어나고 전기통신기술이 발달함에 따라 종합 정보 시스템이 구축되고 있으며 이러한 정보시스템의 확대로 우리 사회는 정보화 사회로 진입되고 있다. 정보화 사회에서는 정보의 가치가 산업사회에서의 물질이나 에너지 이상으로 중요해지는 사회이다. 이와 함께 정보의 도청, 수정, 시스템에 대한 부정 access 등의 부정행위 (공격) 가 사회적으로 문제화되어가고, 이러한 문제에 대한 대응책, 즉 정보 Security의 기술이 큰 주목을 받고 있다. 특히 전자 송금이나 문서 통신 등에 있어서 안전성 문제가 시급하게 대두되고 있다.

정보 Security 기술은 암호화 기술과 인증·서명 기술로 크게 나뉜다. 암호화 기술로서의 암호는 오래전부터 제3자에게 알리고 싶지 않은 정보를 전송할 때에 이용되어진 방법이었으나, 최근에는 이러한 암호를 이용한 인증, 서명 기술이 Security 문제의 강력한 해결책으로 큰 기대를 모으고 있다.

본 논문에서는 부정행위에 대한 여러가지 정보 Security 기술에 관해서 설명한 다음에 기존에 연구된 메시지 인증법에 대해 살펴보고 마지막으로 효율과 메시지 에러율을 개선시킬 수 있는 새로운 메시지 방식을 제안한다.[1],[2]

2. 부정행위와 해결책

비밀이 보장되지 않는 통신로에서 발생 할 수 있는 부정행위는 제3자에 의한 통신 내용의 도청과 제3자에 의한 메시지 내용의 변경, 송신 부정 및 수신문의 위조, 신분 위장 등이 있다.[2],[3],[4]

이와같은 부정행위와 이에 대한 대비책이나 해결방안을 좀 더 자세히 살펴보면 다음과 같다.

2.1 메시지 도청과 암호화

메시지를 전송하는 통신로가 안전한 것이 아니므로 메시지를 전송하는 경우 제3자가 도청할 가능성이 있다. 이를 해결하기 위해서 메시지를 암호화하는 방법이 있다. 메시지를 암호화하여 제3자가 도청을 하더라도 그 내용을 알 수 없도록 하는 방법이다. 하지만 도청을 해서 그 내용을 복호하는 것은 막을 수가 없다. 특히 메시지를 도청당했는지 여부를 알 수 없는 것이 더욱 문제이다.

2.2 메시지 내용 변경과 인증

메시지 내용 변경을 알기 위해서는 단순히 암호하는 방법과 인증하는 방법이 있다. 메시지를 암호화를 해서 전송할 경우 제3자가 암호문에 수정을 하면 복호했을 때 의미가 통하지 않는 문장이 되므로 수정이 가해졌다는 것을 알 수 있다. 하지만 제3자가 메시지를 복호해서 수정을 한 후에 암호화한 후에 전송하는 것은 막을 수 없다.

인증은 인증자를 작성하여 메시지에 부가하여 보내는 방법이다. 수신측에서는 수신한 메시지를 바탕으로 인증자를 작성해서 작성된 인증자와 수신한 인증자가 같은지 비교해 본다. 인증자가 서로 같으면 메시지가 변경되지 않은 것으로 생각해서 메시지를 받아들이고, 인증을 해서 메시지 내용이 변경된 것을 알게 되면 수신된 메시지를 버리고 메시지의 재전송을 요구한다.

2.3 송신부정 및 수신문의 위조와 디지탈 서명 기술

송신 부정 및 수신문의 위조는 통신 내용의 도청이나 메시지 내용의 변경, 신분 위장과 같은 공격과는 다르게, 송수신을 행하는 당사자간에의 분쟁을 야기시킨다. 그 대응책은 대단히 중요한 과제로서 디지탈 서명이 있으며 현재 많은 연구가 행하여 지고 있다. 디지탈 서명은 송신자이외의 어느 누구도 만들 수 없으며, 그 서명은 누구라도 그 송신자 자신에 의해 작성된 것이라는 것을 확인할 수 있으며, 이것은 공개키 암호를 이용하면 실현이 가능하다. 따라서 디지탈 서명을 적용하면 수신자에 의한 수신문의 위조뿐만 아니라 제3자에 의한 메시지의 수정도 검출할 수 있다.

2.4 위장과 신원 확인 기술

신분 위장중에서 제3자에 의한 위장의 경우에는 송수신자간의 신원을 확인함으로서 방지할 수 있다. 구체적인 방법으로는 패스워드 (password) 의 사용, ID에 의한 신원확인 등이 있다. 또 다른 관용암호를 이용한 암호통신에 있어서는 비밀키의 공유를 확인함으로서 실현이 가능하다. 이러한 문제와 관련하여 최근에는 개인의 특징(지문, 성문, 망막 등)을 이용한 개인 식별 기술의 연구가 활발히 행해지고 있다.

3. 메시지 인증법

메시지 인증은, 앞에서 설명한 바와 같이 통신로에 있어서 메시지의 수정을 검출하는 기능으로 이를 위하여 메시지에 미리 Redundancy를 부가하여, 그 Redundancy를 이용하여 메시지의 정당성을 인식하는 수단이다. 이하에서는 메시지의 비익화를 필요로하는지 않는지를 나누어 논하기로 한다[5],[6],[7],[8].

3.1 메시지의 비익성을 필요로 하지 않는 경우

여기서는 먼저 메시지를 그냥 보낼 경우를 생각한다. 이때 어떻게 메시지에 Redundancy를 부가할 것인가를 생각하기 전에 이러한 것과 유사한 기술인 에러 정정 검출 부호에 대하여 생각하기로 한다.

에러 정정·검출 부호는 통신로에 있어서의 자연 잡음 등에 의한 메시지의 에러를 검출 혹은 정정할 수 있다. 그러나 이러한 에러 정정 검출 부호를 능동적 에러도 고려해야만 하는 통신로에서 메시지 인증용으로 사용할 수 없다. 왜냐하면 사용하고 있는 부호를 특징지을 수 있는 파라메터 (parameter) 인 생성 행렬, 부호길이, 최소거리 등이 일반적으로 알려져, 제3자는 임의로 부호어를 변경시켜 메시지의 수정을 행할 수가 있다. 이러한 파라메터를 비밀로 하는 것도 생각할 수 있으나, 그때는 그것들을 쉽게 추정

할 수 없도록 해야한다. 그러므로 수정을 막기 위하여 메시지 인증용의 Redundancy 부분으로부터 그것을 작성한 알고리즘을 추정할 수 없도록 해야만 한다. 이를 위해 인증자를 작성하는 알고리즘으로 송수신자만이 그 비밀을 보유하는 관용암호 등을 이용하는 방법이 제안되고 있다.

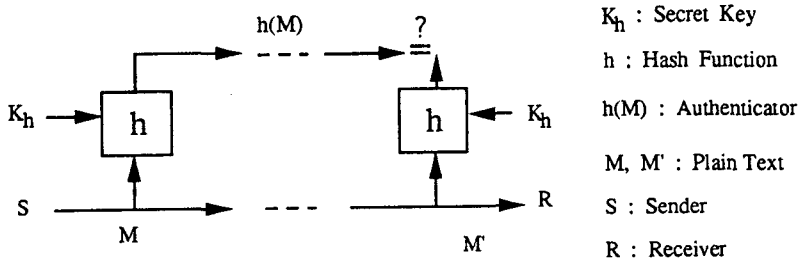


그림1. 메시지의 비익성을 필요로 하지 않을 경우

3.2 메시지의 비익성을 필요로 할 경우

인증자를 포함한 메시지 전체를 암호화해서 보낼 경우는 인증자 작성 알고리즘을 송수신자의 비밀로 할 필요가 없기 때문에 주로 관용 암호를 이용하지 않고 인증자를 생성한다. 인증자를 생성하는데 암호화 방법을 이용하지 않고 해쉬함수를 이용하면 암호화 키와 인증용 키를 따로 갖출 필요가 없어 키이 관리가 편리하다.

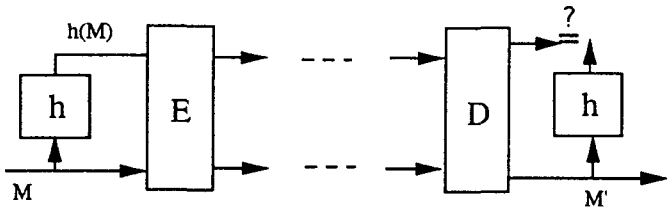


그림2. 메시지의 비익성을 필요로 할 경우

3.3 디지탈 서명과의 관계

디지탈 서명을 이용하여 메시지 인증이 실현 가능하다는 것은 앞에서 설명하였다. 디지탈 서명은 그림 3에서와 같이 공개키 암호를 서명 알고리즘으로 이용하면 간단히 실현할 수 있다.

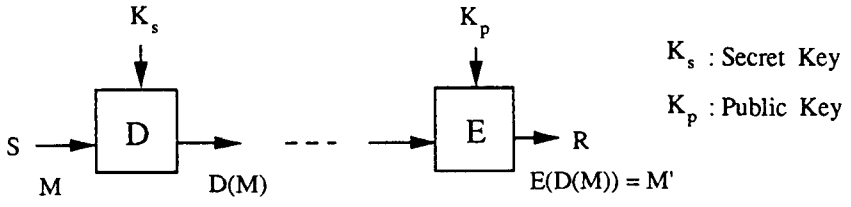


그림3-a. 디지탈 서명

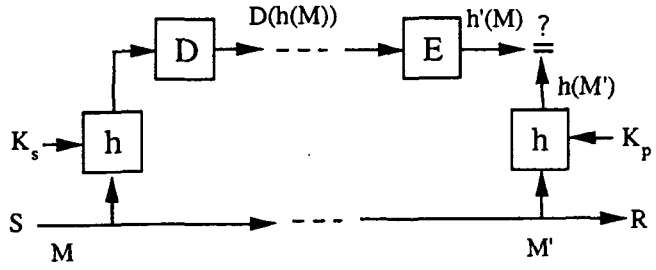


그림3-b. 인증자 조회법에 의한 디지탈 서명

그림3-a는 메시지 자신의 Redundancy성을 이용하여 메시지 인증을 행하는 방식으로, 효율과 의미 처리에 있어서 문제가 있다. 그림3-b에서는 메시지에 있어서 인증자를 작성하고 그곳에 서명을 부여하는 방식이다.

3.4 기존의 메시지 인증법 (방식 I) 의 특성

통신에서 일어난 메시지 내용 변경을 알기 위한 메시지 인증법 중에서 인증자를 생성하여 메시지에 부가하여 전송하는 방법을 그림4에 나타낸다.

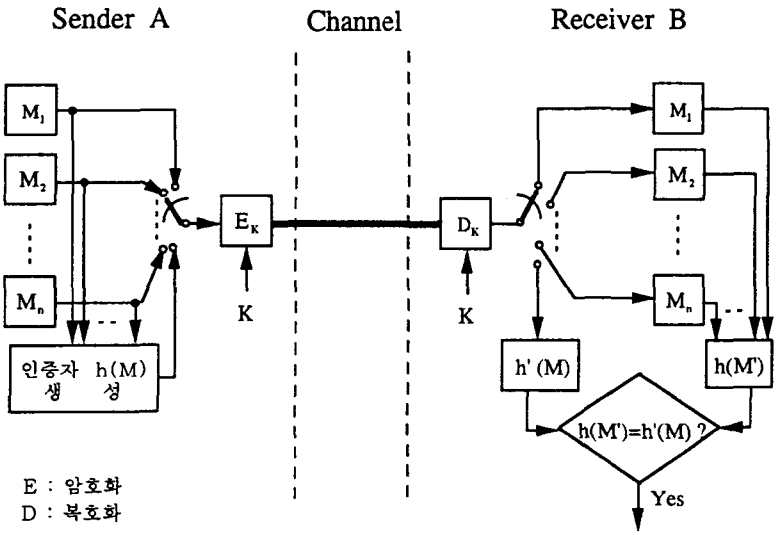


그림4. 인증자 생성

통신로 에러 및 메시지 수정 등을 고려해야 하는 통신로에 대하여 예전부터 이용되고 있는 메시지 인증법을 적용했을 경우의 특성에 대하여 논한다. 즉 메시지가 수정 등으로 변화하였음에도 불구하고 정당하다고 인식하는 확률 (이하 메시지 에러율이라고 함) 과 메시지를 받아 들일 때까지 몇회의 통신이 필요한가 (효율) 에 대하여 생각한다. 종래에 제안된 메시지 인증방식 (이하 방식 I 이라고 함) 은 그림5와

같다.

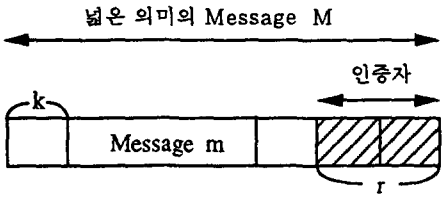


그림5. 메시지 전체를 인증하는 방식 (방식 I)

이 방식은 먼저 메시지 m을 k 비트씩 n개의 블럭 m_i (길이 k bit, i=1, 2, ··· n) 로 분할하여, 이것에 대한 Hash Function h에 의해 r 비트의 인증자 h(m)을 구한다. 그리고 넓은 의미의 메시지 M=(m||h(m))을 만들어 k 비트씩 암호화하여 송신하는 방식이다. 이때 수신측에서는 수신한 인증자 h'(m)과 수신문 m'로부터 생성한 인증자 h(m')이 일치하는가의 여부를 판정하여, 일치하면 통신로에서의 수정 등이 일어나지 않았다고 판단하여 그것을 받아들이고, 일치하지 않으면 수정이 일어났다고 판단하여 재전송을 요구한다. 재전송 요구가 있으면 다시 똑같은 통신을 행한다. 그리고 메시지를 받아들이면 그 통신은 완료된 것으로 한다.

이때, 통신로에 있어서

1) 에러가 발생하지 않고, 모든 메시지 블럭이 올바르게 받아들여진다.
2) 에러가 발생한 것이 검출되어, 모든 메시지를 버리고 재전송을 요구한다.
3) 에러가 발생함에도 불구하고, 올바르다고 인식하여 받아들인다.

의 3가지의 경우가 있다. 이때의 확률을 각각 $P_c(q)$, $P_d(q)$, $P_u(q)$라고 하면

$$P_c(q) = q^{n+\alpha} \tag{1}$$

$$P_d(q) = (1-q^n)(1-2^{-k\alpha}) + (q^n - q^{n+\alpha}) \tag{2}$$

$$P_u(q) = (1-q^n)\cdot 2^{-k\alpha} \tag{3}$$

가 된다. 여기서 q는 메시지 1 블럭에 있어서 올바르게 받아들일 확률이고, p를 2원 대칭 통신로에 있어서의 비트 에러율이라고 하면

$$q = (1-p)^k \tag{4}$$

로 나타내진다. 여기서 $\alpha = r/k$이고, $P_c + P_d + P_u = 1$이다. Hash Function h에 의해 구해진 인증자는 메시지의 모든 비트에 의존하고, 메시지 1 비트의 변화에 의해 랜덤하게 변화한다고 가정한다. 이때 받아들여진 메시지가 에러를 포함할 확률 P_e는

$$P_e = \frac{P_u}{P_c + P_u} = \frac{(1-q^n)2^{-k\alpha}}{q^{n+\alpha} + (1-q^n)2^{-k\alpha}} \tag{5}$$

로 나타낼 수 있다. 이 확률 P_e는 받아들여진 N(=n+α)개의 메시지 블럭중 적어도 1 블럭이 잘못되었을 확률을 나타내고 있다. 다음은 N개의 메시지 블럭이 받아들여질 때까지 필요한 송신 블럭 수 r_A를 구하기로 한다. 각회의 통신에서 받아들여지는 확률 P_a는 $P_a = P_c + P_u$로서 나타내지고, 1회에 있어서 송신 블럭 수는 n+α이므로 r_A는

$$r_A = (n+\alpha)P_a + 2(n+\alpha)P_a(1-P_a) + 3(n+\alpha)P_a(1-P_a)^2 + \cdots$$
$$\cdots + r(n+\alpha)P_a(1-P_a)^{r-1} + \cdots$$
$$= \frac{(n+\alpha)}{P_a} \qquad (6)$$

가 된다. 구체적인 수치 예를 대입해보면 이 방식의 메시지 에러율은 아주 낮지만, 통신로의 비트 에러율 p가 10^{-3}보다 클 경우에는 효율이 대단히 나쁘다.

4. 새로운 메시지 인증 방식

4.1 블럭별로 메시지 인증을 행하는 방식 (방식Ⅱ)

방식Ⅰ의 결점을 개량한 방식 (이후 방식Ⅱ라고 함) 을 그림6에 나타낸다.

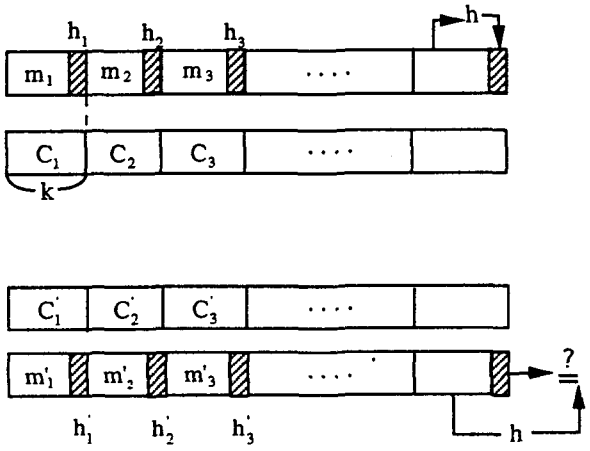


그림6. 블럭별로 메시지 인증을 행하는 방식 (방식Ⅱ)

이 방식은 메시지 블럭 ((1-β)k bit)에 대하여 각각의 인증자 (βk bit)를 부가하기 때문에 수신시의 메시지 인증은 메시지 블럭 단위로 행하여 진다. 이때 각 블럭 단위로 올바르게 받아 들여질 확률을 $P_{bc}(q)$, 에러를 검출할 확률을 $P_{bd}(q)$, 에러가 발생되었음에도 불구하고 올바르게 인식할 확률을 $P_{bu}(q)$라고하면 이것들은 각각

$$P_{bc}(q) = q \tag{7}$$

$$P_{bd}(q) = (1-q)(1-2^{-k\beta}) \tag{8}$$

$$P_{bu}(q) = (1-q)\cdot 2^{-k\beta} \tag{9}$$

가 된다. 또 1 블럭에 있어서의 에러율은

$$\begin{aligned} P_{be} &= \frac{P_{bu}}{P_{bc}+P_{bu}} \\ &= \frac{(1-q)2^{-k\beta}}{q+(1-q)2^{-k\beta}} \end{aligned} \tag{10}$$

가 된다. 따라서 받아들여진 N개의 메시지 블럭 중 적어도 1 블럭에 에러가 있을 확률, 즉 에러율 P_e는

$$\begin{aligned} P_e(q) &= 1-(1-P_{be})^N \\ &= 1-\left\{\frac{q}{q+(1-q)2^{-k\beta}}\right\}^N \end{aligned} \tag{11}$$

이 된다. N개의 메시지 블럭이 완전히 받아들여질때까지 평균 몇회의 통신이 필요한가를 생각하기로 하자. 어떤 블럭에 대하여, 단위 블럭에 있어서의 평균 통신 회수 r_{Bb}를 구하면

$$\begin{aligned} r_{Bb} &= 1p_{ba}+2p_{bd}p_{ba}+\cdots+rp_{bd}^{r-1}p_{ba}+\cdots \\ &= \frac{1}{p_{ba}} \end{aligned} \tag{12}$$

이 된다. 따라서 N 블럭에 있어서의 평균 송신 블럭 수는

$$r_B = Nr_{Bb} = \frac{N}{P_{ba}} \tag{13}$$

이 된다.

구체적인 수치 예를 적용해 보면 방식Ⅱ에서의 메시지 에러율은 방식Ⅰ보다 나쁘나 효율은 매우 좋아짐을 알 수 있다.

4.2 연속하는 2 블럭을 연쇄시켜서 메시지 인증을 행하는 방식 (방식Ⅲ)

이 방식은 그림7과 같다.

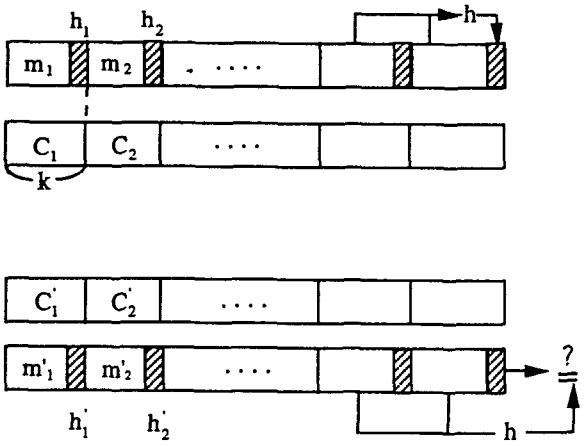


그림7. 2 블럭을 연쇄시켜서 인증하는 방식 (방식Ⅲ)

그림7에 나타낸 바와 같이 인증자를 블럭마다 붙이는 점에서는 방식Ⅱ와 같으나, 그 붙이는 법을 직전 블럭에도 의존하게끔 하고 있다. 이와 같이 하면, 그 블럭의 인증은 자신의 인증자와 다음의 블럭의 인증자에 의해 이루어진다. 이 방식에 있어서의 에러율와 효율을 앞절에서와 마찬가지로 구한다. 어떤 블럭에 있어서, 그 블럭이 올바르게 받아들여질 확률을 $P_{cc}(q)$, 에러가 검출할 확률될 $P_{cd}(q)$, 에러가 발생함에도 불구하고 올바르게 인식할 확률을 $P_{cu}(q)$라고 하면 이것들도 각각

$$P_{cc}(q) = q \tag{14}$$

$$P_{cd}(q) = (1-q)(1-2^{-2k\beta}) \tag{15}$$

$$P_{cu}(q) = (1-q)\cdot 2^{-2k\beta} \tag{16}$$

가 된다. 또 블럭에 있어서의 에러율은

$$P_{ce} = \frac{P_{cu}}{P_{cc}+P_{cu}} = \frac{(1-q)2^{-2k\beta}}{q+(1-q)2^{-2k\beta}} \tag{17}$$

가 된다. 이때 어떤 블럭에 있어서 이것들의 확률은 전후 2 블럭에서의 에러 발생에 의존하고 있음에 주의해야 한다. 받아들여진 N개의 메시지 블럭 중 적어도 1개에 에러가 있을 확률, 즉 에러율 P_e와 N 블럭에 있어서의 평균 송신 블럭 수 r_c 를 방식Ⅱ에서와 마찬가지로 구해보면 에러율 P_e는

$$P_e(q) = 1-(1-P_{ce})^N = 1-\left\{\frac{q}{q+(1-q)2^{-2k\beta}}\right\}^N \tag{18}$$

이 된다. 또 어떤 블럭이든 단위 블럭에 있어서의 평균 통신 회수 r_{cb}는

$$r_{cb} = 1p_{ca} + 2p_{cd}p_{ca} + \cdots + rp_{cd}^{r-1}p_{ca} + \cdots = \frac{1}{p_{ca}} \quad (19)$$

이 된다. 따라서 N 블럭에 있어서의 평균 송신 블럭 수는

$$r_c = Nr_{cb} = \frac{N}{P_{ca}} \quad (20)$$

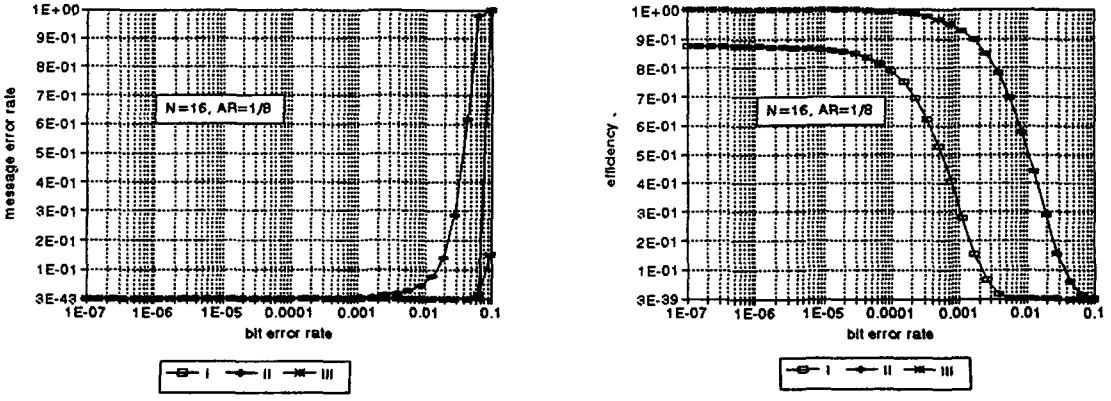
이 된다.

4.3 수치계산 결과 및 검토

앞에서 유도한 방식 I, II, III의 메시지 에러율과 효율성을 인증자율 ($= \frac{\text{인증자 길이}}{\text{전체 메시지 길이}}$, Authenticator Rate, AR) 과 전체 메시지 블럭 수 N을 파라메터로하여 수치계산한 결과를 그림8과 그림9에 나타내었다. 단, 한 블럭의 길이는 K=64, 인증자 블럭 수는 2, 통신로의 비트 에러율 p는 10^{-1}~10^{-7}을 고려하였다.

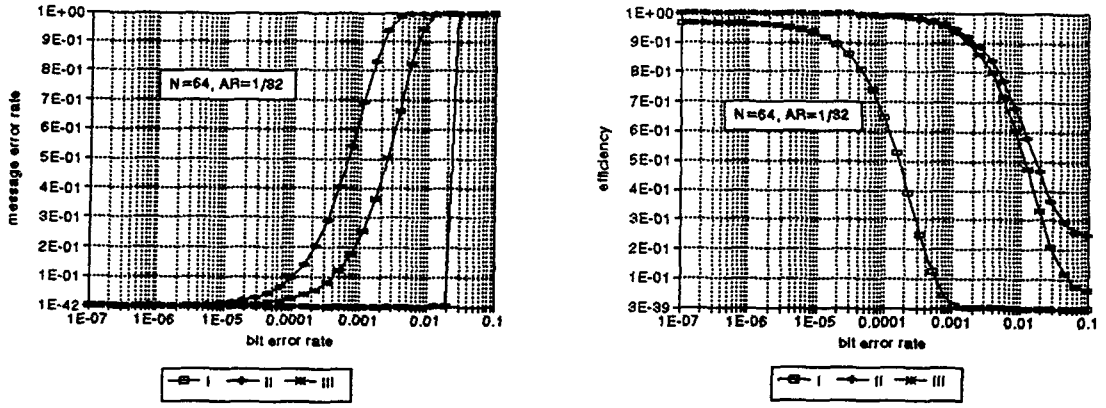
그림8은 인증자의 블럭 수가 2개이고 전체 메시지 블럭 수가 16개일 때, 방식 I, II, III의 메시지 에러율 (그림8-a) 과 효율성 (그림8-b) 을 나타내는 그래프이다. 그림8-a에서 방식 I과 III은 통신로 비트 에러율 0.1이하에서 급격히 감소되고 방식II는 0.01 즉 10^{-2} 이하가 되어야 한다. 그림 8-b에서 방식 I은 통신로 비트 에러율이 아주 낮을 때도 효율성이 떨어지고 방식 II와 III은 10^{-3}정도만 보장되면 아주 양호한 특성을 나타낸다.

그림9는 인증자의 블럭 수가 2개이고 전체 메시지 블럭 수가 64개일 때, 방식 I, II, III의 메시지 에러율 (그림9-a) 과 효율성 (그림9-b) 을 나타내는 그래프이다. 그림9-a를 보면 방식I은 통신로 비트 에러율이 0.01 즉 10^{-2}이하에서 급격하게 감소되며 방식II와 III은 0.0001 즉 10^{-4} 정도가 되어야만 한다. 그림9-b에서는 방식I은 10^{-5}이하가 되어야만 양호한 반면 방식 II, III은 10^{-3}이하만 되면 된다.



(a) 메시지 에러율 (b) 효율성

그림8. N=16, AR=1/8 일 때 방식 I, II, III 비교



(a) 메시지 에러율 (b) 효율성

그림9. N=64, AR=1/32 일 때 방식 Ⅰ, Ⅱ, Ⅲ 비교

방식Ⅰ은 통신로의 비트 에러율이 10^{-2} (0.01) 이하에서 높은 신뢰성 (꽤 낮은 메시지 에러율) 을 얻을 수 있으나 효율면에서는 비트 에러율이 10^{-4}~10^{-6} 정도되는 통신로를 확보하여야만 한다. 이에 비해 방식Ⅱ는 효율면에서 볼 때 비트 에러율이 10^{-3} 이하에서 양호한 특성을 얻을 수 있다. 방식Ⅲ에서는 N이 클 경우 방식 Ⅱ와 비교하여 현저한 에러율의 개선이 보여진다.

5. 결론

본 논문에서는 통신로에서 생길 수도 있는 메시지 수정 등을 검출하는 수단인 메시지 인증법을 메시지 에러율면과 효율면에서 고찰하였다.

메시지 전체를 한번에 인증하는 방식은 효율이 크게 떨어지는 결점이 있는데, 그 결점은 본논문에서 제안한 블럭별로 인증을 행하는 방식을 사용하면 효율이 크게 개선된다. 하지만 제안하는 방식은 효율이 개선되는 반면에 신뢰성은 떨어지나 블럭을 연쇄하여 인증을 행하면, 통신로 비트 에러율 10^{-3}정도이하에서 효율을 떨어뜨리지 않고도 에러율를 낮출 수가 있다.

참 고 문 헌

[1] 오영인, 이인환, "인증과 네트워크의 보안성," 주간기술동향 통권 642호, pp. 16~33. 1994. 4. 11.

[2] 컴퓨터범죄와 암호화 대책, 한국전자통신연구소 편저, pp. 64~98, 1990.

[3] W. Diffe & M. E. Hellman, "New Direction in Cryptography," IEEE Trans. on Information Theory, vol. IT-22, no. 6, pp.135-145, Nov. 1976.

[4] 현대암호학, 한국전자통신연구소 편저, pp. 157~170, 1991.

[5] D. W. Davies and W. L. Price, Security for Computer Networks, John Wiley & Sons Ltd., pp. 119~144, 1983.

[6] R. R. Jueneman, S. M. Matyas, & C. H. Meyer, "Message Authentication," IEEE Communications Magazine, vol. 23, no. 9, pp. 29~40, Sep. 1985.

[7] Jennifer Seberry & Josef Pieprayk, Cryptography, Prentice Hall, pp. 131-180, 1989.

[8] Carl H. Meyer & Stepen M. Matyas, Cryptography : A New Dimension in Computer Data Security, John Wiley & Sons Ltd., pp. 350~385, 1982