위성통신환경에서의 단말간 기밀통신 방안에 대한 성능 분석

손태식*, 임진수*, 이상하**, 김동규*

*아주대학교 정보통신공학과, **동서울대학교 정보통신공학과

A Performance Analysis of Secure Communicaton Method between Terminals in Satellite Communication Environments

Tae-Shik Sohn*, Jin-Su Lim, Sang-Ha Yi, Dong-Kyoo Kim

*Department of Information Communicaton Engineering, Ajou Univ
**Department of Information Communicaton Engineering, Dong Seoul College

요 약

늘어가는 정보통신 서비스에 대한 수요를 만족시키기 위하여 현재 유·무선망을 통합하며 지상망과 위성통신망을 연동하는 방안이 사용되고 있다. 위성통신망은 여러 단말들로 구성되어 있으며, 무선 환경에 노출되어 있어 위성통신망 단말들 사이의 보안이 필수적인 요구된다. 따라서 본 논문에서는 Pull과 Push 형태의 두 가지 키 분배 모델과 대칭키, 비대칭키 암호화 알고리즘을 사용하여 위성통신망에서 적합한 단말간 키 분배 모델을 제안하며 그 성능을 분석함으로써 위성통신환경에서의 적합성을 검증하였다

I. 서론

현재 정보통신망은 유·무선 통신의 결합, 지상망과 위성망의 결합 그리고 전송되는 데이터 또한 음성, 화상, 동영상을 포함하는 광대역 통합망 형태로 발전해 가고 있다. 이러한 추세에 있어 위성통신망의 구축은 필수적이며 위성통신망을 구성하는 여러 단말들 사이의 정보보호 필요성 역시 점점 커지고 있다[6][7].

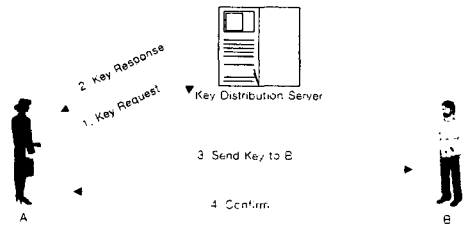
본 논문에서는 위성통신망의 여러 단말 사이에서의 기밀 통신을 지원하기 위한 키 분배 모델과 키 분배과정에서 사용되는 암호화 기법에 대하여 연구한다. 제2장에서는 위성통신망에서 사용될 수 있는 키 분배 모델과 암호화 기법을 제시한다. 제3장에서는 2장에서 연구된 키 분배 모델과 암호화 기법으로 구성된 위성통신망의 기밀통신방안을 제안한다. 4장에서는 제안된 방안에 대한 성능 평가를 수행한다. 마지막으로 5장에서는 본 논문의 연구 결과를 서술한다

II. 키 분배 모델과 암호화 기법

본 장에서는 위성통신망에 적용 가능한 두 가지 키 분배 모델과 암호화 기법에 대한 연구가 수행되었다.

1. 키 분배 모델

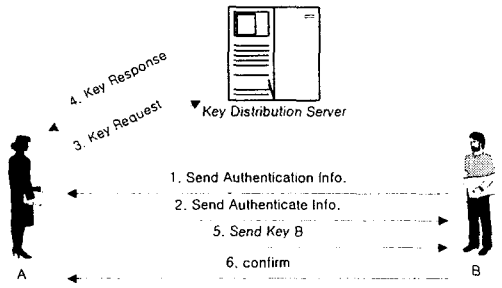
본 논문에서는 위성통신망에 적용하기 위한 키 분배 모델로서 Pull과 Push 형태의 두 가지 방안을 제안한다. 이 두 가지 키 분배 모델의 두 단말은 기본적으로 단말 자체의 기본적인 인증 과정을 성공하였다고 가정한다. Pull 형태의 키 분배 모델은 그림 1과 같이 두 단말 사이에서 어느 한 단말이 키 분배 서버에게 키를 얻어와 상대 단말에게 분배하는 방식이다. 이 모델은 인증된 두 단말 사이에서 기본적인 키 분배 기능만을 수행하며 두 단말간 통신 절차가 간단한 특성을 가지고 있다.



[그림 1] Pull 형태의 키 분배 모델

Push 형태의 키 분배 모델은 그림 2와 같이 두

단말 사이의 부가적 인증 정보 교환 과정을 수행한다. 그 후 한 단말이 키 분배 서버에서 키를 얻어와 상대에게 분배한다. 이 방식은 우선 부가적인 인증을 통한 안전성 확보가 필요한 경우와 또한 특정 단말이 키 분배 서버와 직접적인 통신이 불가능한 경우 등에 상대 단말을 통해 키를 얻고 기밀 통신을 수행할 수 있는 특징을 가지고 있다.[7]



[그림 2] Push 형태의 키 분배 모델

2.2 암호화 기법

위성통신망의 단말 사이에 키 분배 모델에서는 암호화 알고리즘의 연산 속도가 상대적으로 빠른 대칭키 기법과 MAC과 키 패딩 기법을 함께 사용하여 메시지 크기를 줄이는 방안과 상대적으로 높은 비도를 가지며 PKI 기반의 인증 체계와 연동이 가능한 비대칭키 기반의 암호화 알고리즘을 사용하는 방안이 고려 될 수 있다.[7]

3. 위성통신환경에 적합한 단말간 정보보호 방안

위성통신환경을 구성하는 단말은 해상 이동 단말, 공중 이동 단말, 육상 이동 단말 그리고 지상 고정 단말 등 여러 종류가 있다. 이러한 단말들은 무선환경에 노출되어 있기 때문에 단말간 사전 인증을 수행하고 기밀 통신 채널을 확립하는 것이 필수적이다. 이러한 사전 인증 과정으로는 위성통신망의 Bearer 프로토콜로 사용되는 CDMA 등에 의한 단말 식별과정과 단말을 사용하는 사용자가 미리 발급 받은 스마트 카드 등을 사용하여 단말 자체의 인증을 통해 스마트 카드를 지닌 사용자가 정당함을 확인하는 인증 과정이 있다. 이러한 인증 외에 부가적인 인증과정이 필요한 경우에는 키 분배에 사용되는 프로토콜에 인증 과정을 포함하는 방안과 응용 서비스 수행 전에 인증 과정을 수행하는 방안 등이 있다.

위성통신환경은 다른 통신 환경과 달리 환경 특성에 의한 전파 지연이 큰 변수로 작용하기 때문에 제안하는 단말간 인증 및 키 분배 모델은 우선 위성망 환경의 높은 지연(250ms)을 고려해야 한다. 그래서 제안하는 단말간 기밀통신 방안은 단말간 통신 절차의 최소화, 단말간에 전달되는 메시지 크기의 최소화 그리고 단말간 인증 및 키 분배 과정에 사용되는 암호화 알고리즘의 연산 속도 등의 요구 사항을 충족시켜야한다.

따라서 본 논문에서는 앞서 열거한 요구 사항을 충족시키기 위한 방안으로 Pull 형태의 키 분배 모델과 비대칭키 암호화 알고리즘을 사용하는 방안과 Push 형태의 키 분배 모델과 대칭키 암호화 알고리즘을 사용하는 방안을 제안한다.

3.1 Pull 형태의 비대칭키 기반 키 분배 모델

키 분배를 통해 기밀 통신을 수행하는 두 단말 중 어느 한 단말이 키 분배 서버에 키를 요청하고 얻어 온 키를 상호간에 분배하게 된다. 초기 단말간의 상호 인증 과정이 생략되므로 키 분배에 필요한 절차를 최소한으로 유지할 수는 장점과 함께 또한 비대칭키 암호화 기법은 대칭키 기법에 비해 관리해야 할 키의 수가 줄어 키 관리 용이성은 물론이고 향후 무선 환경을 고려하여 구축되고 있는 무선 공개키 기반 구조(WPKI : Wireless Public Key Infrastructure) 환경과의 연동도 고려 할 수 있다. 하지만 비대칭키 기법은 대칭키 기법에 비해 알고리즘의 연산 속도가 비교적 느리고 공개키/개인키 쌍에 대한 유효성 검증 문제 등을 가지고 있다.

가정 : 단말 자체의 사용자 인증 과정과 위성통신망 자체의 단말 인증 과정은 성공으로 가정한다.

1. A -> KDS : m1
2. A <- KDS : $E_{KU_a}[m2||Sign_{KRkds}(m2)]$ ||
   $E_{KU_b}[m3||Sign_{KRkds}(m3)]$
3. A -> B : $E_{KU_b}[m3||Sign_{KRkds}(m3)]$, $E_{Ks1}[N_1]$
4. A <- B : $E_{Ks1}[f(N_1)]$

*m1 = (ID_A||ID_B), *m2 = (K_{S1}||ID_B||T)
*m3 = (K_{S1}||ID_A||T)

1.단말 A는 위성을 통해 KDS에 단말 B와의 통신을 요청한다. 이때 단말 A는 자신의 식별자와 통신을 원하는 상대의 식별자를 전송한다.

2.KDS는 단말 A가 보낸 인증 요청 메시지를 검증한 후에 단말 A와 단말 B 사이의 기밀 통신에 필요한 비밀키를 전송한다.

3.단말 A는 단말 B에게 통신에 필요한 비밀키를 전송한다.

4.단말 A, B 사이에 분배된 비밀키의 정당성을 확인하기 위해 두 단말은 특정 랜덤 값을 상호 간의 비밀키를 통해 상호 검증하여, 검증이 완료되면 기밀 통신을 확립한다.

[표-1] Pull 형태의 비대칭키 기반 키 분배 모델 기호

기호	설명
IDx	단말 X의 식별 인자.
KDS	키 분배 서버
E_{KUx}	단말 X의 공개키
E_{KRx}	단말 X의 개인키
E_{KUkds}	KDS의 공개키
E_{KRkds}	KDS의 개인키
$Sign_{KRx}()$	x의 개인키를 사용한 서명값
K_{S1}	단말 A와 단말 B가 공유하는 비밀키
T	타임스탬프
N_1	Nonce(Random Number)

3.2 Push 형태의 대칭키 기반 키 분배 모델

본 모델은 대칭키를 기반으로 키 분배 서버에서 기밀 통신을 원하는 단말 수만큼의 대칭키를 관리해야되는 문제를 가지고 있다. 하지만 다양한 다이제스트 값을 생성할 수 있는 MAC(Message Authentication Code) 함수를 사용하여 상호 간에 전달되는 메시지의 크기를 조절할 수 있고, 단말간 비밀키 분배에 있어 단말간의 비밀키를 암호화된 MAC 값과의 XOR 연산을 이용하여 패딩 하는 기법을 사용한다. 또한 메시지 암호화 및 다이제스트 생성에 쓰이는 알고리즘은 공개키 암호화 및 서명 알고리즘에 비하여 연산 속도가 빠른 특징을 가지고 있다. 그러므로 MAC과 관용 암호화 알고리즘을 사용하는 비밀키 기반의 키 분배 모델은 위성통신망 단말의 낮은 성능과 무선 링크 환경을 고려하는 경우에 있어 최소한의 연산, 메시지 크기의 감소 그리고 메시지 크기 조절 가능이라는 장점을 가질 수 있다. 또한 단말이 만약 키 분배 서버와 통신이 어려와 기밀 통신을 위한 키 분배를 요청할 수 없는 긴급 상황의 경우에도 본 대칭키를 기반의 키 분배 모델은 Push 모델을 기본으로 구성되어 상대 단말에게 대신 키 분배를 요청하는 과정을 통하여 사용이 가능한 특성을 가지고 있다.

가정 : 단말 자체의 사용자 인증 과정과 군 위성통신망 자체의 단말들에 대한 인증 과정은 성공으로 가정한다. 그리고 단말 B는 단말 A에게 기밀 통신에 필요한 키를 대신 요청한다.

1.A <- B : N_b
2.A -> B : N_a
3.A -> KDS : N_a || N_b || ID_b
4.A <- KDS : $MAC_a(m1)$ || $E_a[MAC_a(m1)]\oplus K_{ab}$, $MAC_b(m2)$ || $E_b[MAC_b(m2)]\oplus K_{ab}$
5. A -> B : $MAC_{ab}(m3)$ || $MAC_b(m2)$ || $E_b[MAC_b(m2)]\oplus K_{ab}$
6. A <- B : $MAC_{ab}(N_a, N_b)$

*m1 = $(N_a||K_{ab}||ID_b)$, *m2 = $(N_b||K_{ab}||ID_a)$
*m3 = $(N_a||N_b||ID_a)$

1.단말 B는 A에게 임시 랜덤 값 전송하며, A에게 자신과 기밀 통신을 위한 비밀키를 키 분배 서버에 요청할 것을 요구한다.
2.단말 A는 B에게 임시 랜덤 값 전송하여 추후의 상호 인증 과정의 확인에 사용한다..
3.단말 A는 EKDM에게 단말 B와 교환한 임시 랜덤 값과 단말 B의 ID를 함께 보냄으로써 단말 B의 키 분배 대행 요청을 수행하게 된다.
4.EKDM은 단말 A에게 단말 A와 B사이의 비밀키를 포함하는 두 개의 메시지를 전송. 각 메시지는 처음 상호간에 교환했던 자신의 임시 랜덤 값, A, B사이의 공유키 그리고 상대방 식별자들을 자신과 EKDM 사이의 비밀키로 MAC 값을 생성하고, 생성된 MAC 값을 다시 비밀키로 암호화한 후 두 단말 사이의 비밀키와 XOR 연산을 한 값을 생성해낸다.
5.단말 A는 EKDM으로부터 받은 메시지에서 자신과의 비밀키로 생성된 MAC 값을 암호화하여 XOR 연산으로 패딩된 단말간 비밀키를 알아낸다. 그 후 단말간 비밀키로 자신의 식별자와 임시 랜덤 값들에 대한 MAC을 생성하여 전에 EKDM으로 받은 단말 B에 대한 메시지들을 함께 보낸다.
6.단말 A로부터 해당 정보를 받은 B는 A, B 간의 공유키로 처음에 교환했던 임시 랜덤 값의 MAC을 생성하여 다시 보낸다. 단말 A는 단말 B로부터의 임시 랜덤 값들의 MAC 값을 검증함으로써 상호 인증 및 키 분배 과정의 정당성을 확인한다.

[표-2] Pull 형태의 비대칭키 기반 키 분배 모델 기호

기호	설명
ID_x	단말 x의 식별 인자
KDS	키 분배 서버
N_x	단말 x의 임시 랜덤값
MAC_x	단말 x와 KDS의 비밀키를 사용한 MAC값
MAC_{xy}	단말 x와 단말 y의 비밀키를 사용한 MAC값
E_a	단말 x와 EKDM의 비밀키
E_{xy}	단말 x와 y의 비밀키

4. 성능 분석

본 논문에서 앞서 제안한 키 분배 방안의 성능 분석을 이해 위성통신망의 구성 시스템들을 그림 3과 같이 간단히 모델링 한다. 그림 3의 위성통신망 모델은 위성 단말, 위성체 그리고 지상망의 키 분배 서버 시스템으로 구성된다.

[그림 3] 위성통신망 모델링

위성통신망 모델링에서 각 파라미터들은 표-3과 같으며 도착하는 패킷들은 평균 도착률 λ의 포아송 분포를 따르고 서비스 시간은 각각 μ_1, μ_2, μ_3의 상수 값을 가지는 것으로 가정한다. 하지만 각 시스템에서 인증 및 키 분배를 위한 암호화 및 복호화와 같은 부가적인 정보보호 서비스를 고려하면 시스템에 도착하는 데이터에 대한 평균 도착율은 같게 유지되지만 각 시스템에서의 서비스율은 각각 μ'_1, μ'_2, μ'_3로 추가된다. 그리고 이 시스템의 최대 효율은 $\mu'_b = \max(1/\mu'_i)$, i=1,2,3, 즉 가장 긴 서비스 시간을 가지는 시스템에 의해서 결정되며 시스템에서의 평균 지연시간은 각 시스템 큐에서 소비한 시간의 합과 같다.

[표-3] 위성통신망 모델링 기호

기호	설명
ρ_i	일반 시스템의 효율
ρ'_i	정보보호 시스템의 효율
μ_i	일반 시스템의 서비스 율
μ'_i	정보보호 시스템의 서비스 율
d_i	일반 시스템의 서비스 율과 정보보호 시스템의 서비스 율의 차이
T	전체 시스템의 지연 시간
ld	위성 링크 상의 지연 시간(단말~위성)

위성통신 환경 시스템 모델에서는 일반적인 위성통신 환경에서의 정보보호 서비스를 추가로 가정함으로써 각 시스템마다의 가변적인 서비스 시간에 추가로 결정적인 서비스 시간(정보보호 서비스)을 가진다. 결국 정보보호 서비스의 추가에 따라 각 시스템마다의 서비스시간도 결정적으로 증가함을 알 수 있다. 따라서 큐잉모델 중 M/D/1 대기 체계로 정보보호 서비스를 제공하는 위성통신 환경 시스템을 모델링하여 아래의 표 5와 같이 지연 시간을 분석한다.[2][4]

[표-4] M/D/1 큐의 파라미터

L=the time average number of customers in the system
$= \lambda/\mu + \lambda^2/2\mu(\mu-\lambda) = \rho + \rho^2/2(1-\rho)$
w=the average time an arrival spends in the system
$= 1/\mu + \lambda/2\mu(\mu-\lambda) = \mu^{-1} + \rho\mu^{-1}/2(1-\rho)$
w_q=the average time the customer spends in the queue
$= \lambda/2\mu(\mu-\lambda) = \rho\mu^{-1}/2(1-\rho)$
L_q=the time average number in the queue
$= \lambda^2/2\mu(\mu-\lambda) = \rho^2/2(1-\rho)$

[표-5] 위성통신망 지연 시간 측정

$\rho_i = \lambda/\mu_i$

$d_i = \mu_i/\mu'_i$ ($\cong \mu'_i = \mu_i/d_i$)

$\rho'_i = \lambda/\mu'_i = \lambda * d_i/\mu_i = d_i * \lambda/\mu_i = d_i * \rho_i$

$$T = w + \sum_{i=0, i\neq b}^{3} 1/\mu'_i + (ld*2)$$

$$= (1/\mu'_b + \rho'_b\mu^{-1}_b/2(1-\rho'_b)) + \sum_{i=0, i\neq b}^{3} 1/\mu'_i + (ld*2)$$

$$= \rho'_b\mu^{-1}_b/2(1-\rho'_b) + \sum_{i=0}^{3} 1/\mu'_i + (ld*2)$$

$$= \lambda/2\mu'_b(\mu'_b-\lambda) + \sum_{i=0}^{3} 1/\mu'_i + (ld*2),$$

$(\mu'_b = \max[1/\mu'_i],\ i=1,2,3)$

성능 분석에 사용되는 표 6, 표 7의 암호화 알고리즘의 연산 속도는 셀러론 850Mhz에서 동작하는 윈도우 운영체제상에서 측정된 결과이며 암호화 알고리즘들은 C++로 구현되었다. 또한 위성 시스템 및 각 시스템의 기본 지연은 0.01msec, 단말과 위성사이의 왕복 지연은 250msec(즉, ld=125msec) 그리고 arrival rate은 10 packets/slot으로 가정하였다.[1][5]

[표-6] 대칭키 알고리즘의 연산 속도

Algorithm	Bytes Processed	Time Taken	Mbps
DES	134217728	9.945	102.968
DES-EDE3	33554432	6.740	37.984
RC5	536870912	12.988	315.368
Blowfish	134217728	7.091	144.408
MD5-MAC	1073741824	12.078	678.256

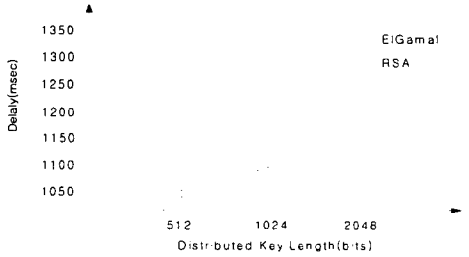
[표-7] 비대칭키 알고리즘의 연산 속도

Algorithm	Encrypt	Decrypt	Sign	Verify
RSA 512bits	0.14	1.93	1.92	0.13
RSA 1024bits	0.32	10.23	10.29	0.30
RSA 2048bits	0.89	64.13	64.13	0.85
ElGamal512bits	2.62	1.37	-	-
ElGamal1024bits	11.03	5.77	-	-
ElGamal2048bits	49.19	25.35	-	-

다음은 실제 제안된 두 가지 단말간 인증 및 키 분배 모델에서의 암호화 알고리즘과 분배되는 키 길이 따른 지연시간을 분석하였다. Pull 모델을 사용하는 단말간 키 분배 모델은 단말간에 4번의 통신 과정이 필요하므로 위성통신 환경에서 기본적

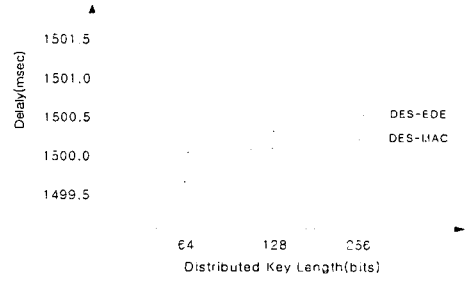
으로 걸리는 왕복 지연 시간이 1000msec(250*4)이고 Push 모델을 사용하는 단말간 키 분배 모델은 단말간에 6번의 통신 과정이 필요하므로 1500msec(250*6)이다.

다음 그림 4에서는 제안된 비대칭키를 사용하는 단말간 키 분배 모델의 기본 왕복 지연을 고려하여 암호화 알고리즘과 분배되는 키 길이를 인자로 하여 지연 시간을 분석하였다. 그림 4를 통해 비대칭키를 사용하는 Pull 모델의 키 분배에서는 2048bits 크기 이상의 키를 분배한다면 약 1350msec 정도의 지연 시간을 가지는 것을 알 수 있다.



[그림 4] Pull 형태의 비대칭키 키분배 모델 성능 분석

다음 그림 5에서는 제안된 대칭키를 사용하는 단말간 키 분배 모델의 기본 왕복 지연을 고려하여 암호화 알고리즘과 분배되는 키 길이를 변수로 하여 지연 시간을 분석하였다. 그림 5를 통해 대칭키를 사용하는 Push 모델의 키 분배에서는 약 1500msec 정도의 지연 시간을 가지는 것을 알 수 있다.



[그림 5] Push 형태의 대칭키 키 분배 모델 성능 분석

본 논문에서 제안된 Push 모델을 사용하는 단말간 키 분배 모델과 Pull 모델을 사용하는 단말간 키 분배 모델은 기본적으로 500msec의 왕복 지연 시간 차이가 있었으나 Pull 모델을 사용하는 키 분배 과정에서 비대칭키 암호화 알고리즘을 사용하여 2048bits 크기 이상의 키를 분배하고 Push 모델을 사용하는 키 분배 과정에서 비밀키 암호화 알고리즘을 사용하는 경우에는 두 모델사이의 지연 시간 차이는 최소 150msec 정도로 줄어들었다.

5. Conclusion

본 논문에서는 위성통신망의 단말간 정보보호를 위한 기밀통신 방안으로서 키 분배 모델과 암호화 알고리즘을 적용하여 두 가지 모델을 제안하였다. 제안된 방안은 Pull 형태의 비대칭키 기반의 암호화 알고리즘을 사용하는 키 분배 모델과 Push 형태의 대칭키 기반 암호화 알고리즘을 사용하는 키 분배 모델이다. 두 제안된 모델의 성능 분석을 통하여 비 대칭키 알고리즘을 사용하는 Pull 형태의 키 분배 모델에서 2048bits 크기 이상의 키를 분배하는 경우에 대칭키 알고리즘을 사용하는 단말간 키 분배 모델과의 지연 시간의 차이가 최소 150msec 이하까지 줄어듦을 알 수 있다.

그러므로 본 논문에서 제안한 두 가지 단말간 키 분배 모델들의 성능 분석을 통하여 제안한 두 가지 모델들이 비록 상이한 암호화 알고리즘과 인증 및 키 분배 방식을 사용하지만 비슷한 지연 시간을 가지며 위성통신환경에 적용 가능함을 알 수 있었다.

참고문헌

[1] S.W.Kim, "Frequency-Hopped Spread-Spectrum Random Access with Retransmission Cutoff and Code Rate Adjustment", IEEE, Vol.10, No.2, Feb 1992

[2] Kyung Hyune Rhee, "Delay Analysis on Secure Data Communication", KIISC, Vol.7, No.12, Dec 1997

[4] Jerry Banks, "Discrete-Event System Simulation",Prentice-Hall, pp264-265, 1996

[5] William Stallings, "Cryptography and Network Security", Prentice-Hall, pp 292-293, 1999

[6] National Institute of Standards Technology,"Framework for National Information Infrastructure Services," N*ISTR 5478* (Gaithersburg, MD: NIST, July 1994).

[7] Tae-Shik Shon, Kyoo-Dong Kim, "A Study on Security Threat Elements Analysis and Security Architecture in Satellite Communication Network", KIISC, Vol.11, No. 4, Aug 2001