VSAT 위성통신 보호를 위한 키 분배 방식의 적용

박 정 현† · 임 선 배††

요 약

본 논문에서는 VSAT 위성통신의 안전성을 위해 변형 Yacobi 방식과 변형 Diffie-Hellman 키분배 방식을 제안 한다. 제안된 변형 DH 방식은 세션키로 키센터에서 발급한 비밀키를 사용하지 않으며 수시로 변경할 수 있다. 또한 변형 Yacobi 방식도 세션키가 키센터에서 발급한 비밀키에 독립적이며 안전성을 이산대수 문제와 큰 소수의 인수분해의 어려움에 바탕을 두고 있다. 제안된 방식은 VSAT 위성통신의 특성상 키센터를 중심국의 망관리 및 운영부로 두고 가입자를 VSAT 단말로 하여 시뮬레이션 했으며 여기서 모듈러 연산을 위해 몽고메리 알고리즘을, 해쉬 함수로 MD5를 각각 이용했다.

Adaptation of a Key Distribution Scheme for VSAT Satellite Communications

Jeong-Hyun Park† · Sun-Bae Lim††

ABSTRACT

This paper presents a key distribution scheme based on the Yacobi scheme that does not use the secret key provided by key distribution center, but uses instead a random number generated by the user. The scheme is independent of the exposure of the secret key. This paper also presented the key distribution schemes based on the Diffie-Hellman (DH) and ID (identity). The schemes based on the solving of the discrete logarithm and prime resolution into factors are better on the expose of secret key. The proposed scheme based on the DH was applied to VSAT satellite communications and simulated on PC using Montgomery algorithm for modular and MD5 (Message Digest) for hashing function.

1. 서 론

대부분의 VSAT 위성망은 단일 중심국인 HUB와 지역적으로 분산되어 있는 많은 VSAT(Very Small Aperture Terminal) 단말국과 성형망(Star Topology)을 채택하고 있으며 중앙에 있는 고출력의 HUB국이 위성망의 관리 및 운영을 관장하도록 하고, 단말국은 HUB국에 비해 소형화 및 저렴화 되도록 하고 있다. VSAT망을 통한 통신 형태는 VSAT과 HUB, HUB와 VSAT, VSAT과 VSAT사이의 통신이 가능하며, VSAT과 VSAT사이의 통신은 HUB의 중계에 의한 간접 통신만이 가능하다. 위성 링크는 VSAT에서 HUB로 연결되는 inbound 채널과 HUB에서 VSAT으로 연결되는 outbound 채널로 구성되어 있다[3, 4, 5, 6]. 일반적으로 inbound채널에 대한 다원접속은 TDMA

† 정 회 원 : 한국전자통신연구원 이동관리연구실 선임연구원
†† 정 회 원 : 한국전자통신연구원 이동관리연구실 책임연구원
논문접수 : 1998년 4월 23일, 심사완료 : 1998년 10월 14일

(Time Division Multiple Access) 방식을 사용하며, outbound 채널을 통한 데이터 전송은 TDM(Time Division Multiplex)방식을 사용한다. Inbound 채널의 TDMA 프레임의 타임 슬롯은 트래픽의 특성 및 서비스 요구 사항에 따라 고정할당(PA/TDMA), 예약할당(DA/TDMA) 혹은 랜덤 억세스(RA/TDMA)를 통한 이용이 가능하다. 일반적으로 길이가 짧은 데이터는 랜덤 억세스를 통한 전송이 유리한데 비해 긴 데이터는 예약할당 방식을 사용하는 것이 유리하다. VSAT망에서 트래픽의 특성 및 부하 정도에 따라 이러한 두 가지 방식을 선택적으로 택할 수 있는 적응할당(AA/TDMA) 방식도 채택한다. Inbound 채널의 TDMA 프레임의 슬롯 억세스에 관한 정보는 HUB가 슬롯 맵(Slot Map) 정보를 outbound 채널을 통하여 방송하므로 써 VSAT들에게 알린다. Inbound 채널의 경우 64-128 Kbps, outbound 채널의 경우 64-512 Kbps의 전송 속도를 가지며 안테나의 크기는 HUB가 5-8 m, VSAT 단말국이 1.2-1.8 m 정도이다[3, 4, 5, 6]. 이와 같은 VSAT망은 위성통신의 고유 장점을 그대로 갖게 되어 높은 전송 신뢰도, 낮은 전송 비용을 갖는 망 구축이 가능하고, 망 사용 비용을 안정화 시킬 수 있으며, 망이 추가 및 삭제가 간편하며 망 운영 및 관리가 용이하다. 이러한 VSAT망은 공공분야, 일반 서비스업 및 산업체 등에서 널리 이용하리라 기대된다. 그러나 VSAT을 이용한 데이터 통신도 위성통신의 취약성을 그대로 갖고 있기에 프라이버시 보호, 국가 및 산업 기밀 정보 보호, 기타 비권한 지구국의 통신 내용 해독 방지를 위해 보호 기술이 필요하다. 이에 본 연구에서는 기존의 보호 기술 중 암호 기술 구현에 있어 매우 중요한 키분배 방식을 제시한다. 이를 위해 먼저 기존의 키분배 방식을 살펴보고 VSAT망에서 필요한 변형된 키분배 방식을 제안한다. 이를 바탕으로 VSAT 위성통신에서 안전성을 위한 키분배 프로토콜을 제시하고 제시된 키분배 프로토콜을 시뮬레이션하여 가능성을 확인한다.

2. 키 분배 방식 제안

키분배는 키센터에서 가입자의 비밀 정보 및 공개 정보를 IC 혹은 스마트 카드에 담아 분배하는 과정과 분배 받은 카드를 이용해 각 가입자가 상대방과 비밀 통신을 위해 공통키를 생성하는 과정으로 볼 수 있다. 본 소절에서는 앞에서 검토된 Diffie-Hellman(DH) 방식과 Yacobi 방식을 변형한 키분배 공유 방식을 제안한다. 다음은 제안된 키 분배 및 공유 과정이다.

2.1 시스템 준비 및 카드 발행 단계

과정 1 : 키센터는 두개의 큰 소수 p와 q를 선택하고 이들의 곱으로 n을 생성한다. 또 e,d{mod (p-1).(q-1)} = 1인 조건을 만족하며 n보다 적은 e(Encryption Key)와 d(Decryption Key)를 결정하고, GF(p)상의 원시 원소이면서 GF(q)상의 원시 원소인 g를 생성한다.

과정 2 : 카드 발행 단계에서 키센터는 가입자 I의 개인정보인 ID_i를 이용해 $S_i = ID_i^{-d} \bmod n$인 S_i를 생성한다. 여기서 $S_i^e \cdot ID_i \bmod n = 1$의 식이 성립된다.

과정 3 : 키센터는 가입자 I의 스마트 카드에 시스템 전체의 공개 정보인 e, n, g와 가입자I의 비밀 정보S_i, d를 저장하여 카드를 발급한다.

다음은 통신 단계에서 제안된 방식별 공통키 생성 과정이다.

2.2 Yacobi 방식의 변형

변형 Yacobi 방식에서 통신 상대자간의 키공유 과정은 다음과 같다.

과정 1 : 가입자 I는 랜덤 수 R_i를 생성하고 $X_i = g^{S_i} \bmod n$와 $Y_i = (R_i.e + S_i)$를 계산하여 가입자 J에게 보낸다.

과정 2 : 가입자 J는 랜덤 수 R_j를 생성하고 $X_j = g^{S_j} \bmod n$와 $Y_j = (R_j.e + S_j)$를 계산하여 가입자 I에게 보낸다.

과정 3 : 가입자 I와 J는 상대에서 받은 X와 Y, 그리고 자신이 생성한 랜덤 수를 이용해 공통키 $WK_{ij} = WK_i = WK_j = (g^{Y_i}.X_j^{-1})^{R_i} = (g^{Y_j}.X_i^{-1}) = g^{R_i R_j e} \bmod n$를 계산 한다.

이렇게 하므로 두 통신자는 서로간의 공통키(세션키)를 공유한다. 그리고 모듈러를 큰 소수로 하는 대신 큰 수의 합성수로 하므로 안전성을 이산 대수 문제와 합성수 인수분해의 어려움에 기초를 둔다. 그러나 이 방식도 DH방식에서의 세션키 변경 문제는 개선할 수 있으나 키센터로 인해 발생 가능한 문제는 여전히 존재 한다.

2.3 Diffie-Hellman (DH) 방식의 변형

변형 DH 방식에서 통신 상대자간의 키공유 과정은 다음과 같다.

과정 1 : 가입자 I와 J는 각각 비밀키 S_i와 S_j를 이용해 공개키 P_i와 P_j를 다음과 같이 계산하여 공개한다.
$P_i = g^{Si} \bmod n$이고 $P_j = g^{Sj} \bmod n$이다.
여기서 $n = p \times q$이다.

과정 2 : 가입자 I와 J는 각각 랜덤 수 R_i와 R_j를 발생시켜 다음과 같이 X_i와 X_j를 구하고 Y_i와 Y_j를 계산하여 서로 교환 한다.
$X_i = g^{Ri} \bmod n$ 이고 $X_j = g^{Rj} \bmod n$ 이다.
$Y_i = X_i.Z_{ij} \bmod n$ 이고 $Y_j = X_j.Z_{ij} \bmod n$ 이다.
여기서 $Z_{ij} = (P_j)^{Si} \bmod n = (P_i)^{Sj} \bmod n$ 이다.

과정 3 : 가입자 I와J는 상대에서 받은 X와 Y, 그리고 자신이 생성한 랜덤 수를 이용해 공통키 Wij $= (Y_j.Z_{ij}^{-1})^{Ri} = (Y_i.Z_{ij}^{-1})^{Rj} = g^{Ri.Rj} \bmod n$을 얻는다.

위 방식은 각각 R_i와 R_j만 같지 않으면 생성되는 세션키는 항상 다르며 또한 S_i와 S_j가 노출되어도 랜덤 수를 멱승하여 전송하기 때문에 세션키는 분석되지 않는다. 그리고 모듈러를 큰 소수 p 대신 합성수 n을 사용하므로 앞의 변형 Yacobi 방식 처럼 안전성을 이산대수 문제와 합성수 인수분해의 어려움에 기초를 둔다.

2.4 Diffie-Hellman (DH) 방식에 ID개념 도입

다음은 변형 DH 방식에 ID 개념이 도입되어 통신 상대자간에 직접 인증이 가능한 방식으로 통신 상대자간의 키공유 과정은 다음과 같다.

과정 1 : 가입자 I와 J는 자신이 생성한 랜덤 수 R_i와 R_j, 키센터에서 받은 비밀키 S_i와 S_j, 그리고 상대방의 ID를 이용해 $X_i = g^{(R_i \cdot S_i + ID_j)} \bmod n$ 와 $X_j = g^{(R_j \cdot S_j + ID_i)} \bmod n$를 계산하여 교환한다.

과정 2 : 가입자 I와 J는 각각 교환한 X_i와 X_j를 이용해 가지고 있는 해쉬 함수로 C_i와 C_j를 계산하고 이를 이용해 Y_i와 Y_j를 계산해 서로 교환한다.
여기서, C_i = hash(X_i, ID_i, ID_j, t) 이고 C_j = hash (X_j, ID_i, ID_j, t) 이며 t는 time stamp이다. 또 $Y_i = g^{(R_i \cdot S_i \cdot C_i)} \bmod n$ 이고 $Y_j = g^{(R_j \cdot S_j \cdot C_j)} \bmod n$ 이다.

과정 3 : 가입자 I와J는 각각 자신의 랜덤 수와 비밀키를 이용해 공통키 $W_{ij} = (g^{-IDj}.\ X_j)^{Ri.Si} = (g^{-IDi}.\ X_i)^{Rj.Sj} = g^{Ri.Rj.Si.Sj} \bmod n$ 를 얻는다.

과정 4 : 그리고 $S_j = X_i^{Ci'}/(Y_i.g^{IDj.Ci}.\ ID_j^d) \bmod n$인지를 통해 가입자 J는 가입자 I를 인증하고 가입자 I도 똑 같은 방식으로 인증 한다. 즉 가입자 J는 Y_i를 통해 받은 C_i'가 이전에 받은 C_i와 같은지를 확인하며 이때 C_i의 함수인 X_i가 다르면 C_i'와 C_i는 달라 인증식이 다르게 되어 서로간에 인증이 가능하다.

위 방식은 기본적으로 키센터의 기능을 강조하면서 한편으로는 두 통신간에 사용되는 세션키를 항상 다르게 하는 방식이다. 이는 위성 중심국, 위성관제센터, 혹은 위성 송신국을 키관리 센터로 두어 센터의 기능을 강조하면서 두 통신자간의 비밀성을 인정해 주는 위성통신 환경에 적합한 형태로 본다. 또한 DH방식의 세션키 고정 문제점을 개선하면서 통신 상대자간의 직접 인증이 가능한 특징을 갖고 있다.

2.5 변형 DH 방식의 확장

변형 Diffie-Hellman 방식에 ID개념을 도입한 방식을 확장하여 다수의 가입자 그룹이 형성되어 동시에 공통키를 생성하려 할 때 그 과정은 다음과 같다. 이를 위해 가입자 K 명이 구성된 통신망이라 가정 한다.

과정 1 : 가입자 I와 J는 자신이 생성한 랜덤 수 R_i와 R_j, 키센터에서 받은 비밀키 S_i와 S_j, 그리고 상대방의 ID를 이용해 $X_i = g^{(R_i \cdot S_i + ID_j)} \bmod n$, $X_j = g^{(R_j \cdot S_j + ID_i)} \bmod n$를 계산하여 교환 한다.

과정 2 : 가입자 I와 J는 각각 교환한 X_i와 X_j를 이용해 C_i와 C_j를 계산하고 이를 이용해 Y_i와 Y_j를 계산해 서로 교환한다.
C_i = hash(X_i, ID_i, ID_j, t) 이고 C_j = hash(X_j, ID_i, ID_j, t) 이며 여기서 t는 time stamp다.
또 $Y_i = g^{(R_i \cdot S_i \cdot C_i)} \bmod n$ 이고 $Y_j = g^{(R_j \cdot S_j \cdot C_j)} \bmod n$ 이다.

과정 3 : 그리고 $S_j = X_i^{Ci'}/(Y_i\ .\ g^{IDj.Ci}.\ ID_j^d) \bmod n$인지를 통해 가입자 J는 가입자 I를 인증하고 가입자 I도 똑 같은 방식으로 인증 한다.

과정 4 : 가입자 J는 가입자 I와 진행한 X, Y, C를 두

가입자간의 X, Y, C로 계산해 다음 가입자와 또 같은 형태로 진행한다.

과정 5 : 이렇게 하여 마지막 가입자는 처음 진행한 가입자I와 똑 같은 과정을 거쳐 그룹의 X, Y, C를 계산하고 인증을 하게 된다.

과정 6 : 최종적으로 생성된 그룹간의 공통키 W_k와 X_{i-k}, Y_{i-k}, C_{i-k} 다음과 같이 표현 된다.

$X_{i-k} = g^{(R_{i-k} \cdot S_{i-k} + ID_{i-k})} \bmod n$

$Y_{i-k} = g^{(R_{i-k} \cdot S_{i-k} \cdot C_{i-k})} \bmod n$

$C_{i-k} = \text{hash}(X_{i-k}, ID_{i-k}, ID_{i-k}, t)$

$W_k = g^{(R_{i-k} \cdot S_{i-k})} \bmod n$

위 방식은 일정 그룹간의 통신 혹은 회의용 키분배 개념으로 적용해 볼 수 있으며 위성 통신을 이용한 데이터 통신에도 적용이 가능하리라 생각된다.

3. VSAT 위성통신의 안전성을 위한 키 분배 프로토콜의 적용

VSAT 위성통신에서 링크 보호를 위한 보호 구조가 정의되어 구현되었을 때 안전성에 가장 결정적으로 영향을 주는 부분이 암호 알고리즘을 위한 공통키 공유 과정이다. 이를 위해 본 연구에서는 VSAT 위성통신에서 안전성을 위한 키분배 프로토콜로 앞에서 제안된 변형 DH 방식을 적용 한다. 이는 VSAT 위성통신의 특성상 중심국 망 운영 및 관리부의 키관리센터 기능을 높이면서 높은 안전성을 기대할 수 있는 방안으로 고려된다.

3.1 변형 Diffie-Hellman 방식을 이용한 키분배

다음은 변형 DH 방식을 VSAT 위성통신에 적용했을 때 HUB와 VSAT간의 키공유 과정이다. 기본적인 파라메터는 키센터의 기능을 갖는 HUB에서 미리 준비했고 VSAT 단말도 이미 필요한 파라메터를 키센터로 부터 받은 것으로 간주한다.

과정 1 : HUB와 VSAT은 각각 비밀키 S_h와 S_v를 발생하고 공개키 P_h와 P_v를 다음과 같이 계산하여 공개 한다.

$P_h = g^{Sh} \bmod n$이고 $P_v = g^{Sv} \bmod n$이다.

여기서 $n = p \times q$이다.

과정 2 : HUB와 VSAT은 각각 랜덤 수 R_h와 R_v를 발생시켜 다음과 같이 X_h와 X_v를 구하고 Y_h와 Y_v를 계산하여 서로 교환 한다.

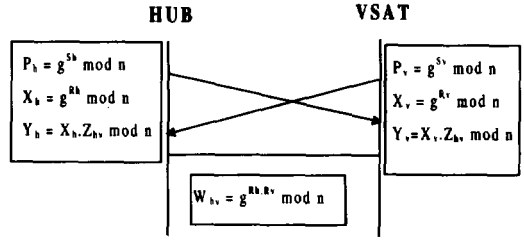
$X_h = g^{Rh} \bmod n$ 이고 $X_v = g^{Rv} \bmod n$ 이다.

$Y_h = X_h.Z_{hv} \bmod n$ 이고 $Y_v = X_v.Z_{hv} \bmod n$ 이다.

여기서 $Z_{hv} = (P_v)^{Sh} \bmod n = (P_h)^{Sv} \bmod n$ 이다.

과정 3 : HUB와 VSAT은 각각 자신이 생성한 랜덤 수를 이용해 공통키 $W_{hv} = (Y_v.Z_{hv}^{-1})^{Rh} = (Y_h.Z_{hv}^{-1})^{Rv} = g^{Rh.Rv} \bmod n$를 얻는다.

위의 프로토콜에서는 각각 R_h와 R_v만 같지 않으면 생성되는 모든 키들이 서로 다르다. 또한 S_h와 S_v가 노출되어도 랜덤 수를 멱승하여 전송하기 때문에 세션키는 분석되지 않는다. 따라서 공개키의 사용 기간은 세션키보다 훨씬 길며 특히 비밀키의 보관은 안전해야 한다. 그리고 위 과정에서 생성되는 랜덤 수와 X, Y는 주기적으로 자주 변경되어야 할 것이다. 다음 그림은 위 과정을 도식화한 것이다.



(그림 1) 변형 DH 방식을 이용한 HUB와 VSAT간의 키공유
(Fig. 1) Key Sharing between HUB and VSAT based on the modified Diffie-Hellman

3.2 변형 Diffie-Hellman 방식에 ID개념이 도입한 방식을 이용한 키분배

ID 개념이 도입된 변형 DH 방식을 VSAT 위성통신에 적용 했을 때 HUB와 VSAT간에 키공유 과정은 다음과 같다. 기본적인 파라메터는 키센터의 기능을 갖는 HUB에서 미리 준비했고 VSAT 단말도 이미 필요한 파라메터를 키센터로부터 받은 것으로 간주한다.

과정 1 : HUB와 VSAT은 자신이 생성한 랜덤 수 R_h와 R_v, 센터에서 받은 비밀키 S_h와 S_v, 그리고 상대방의 ID를 이용해 $X_h = g^{(R_h \cdot S_h + ID_v)} \bmod n$와 $X_v = g^{(R_v \cdot S_v + ID_h)} \bmod n$를 계산하여 교환한다.

과정 2 : HUB와 VSAT은 각각 교환한 X_h와 X_v를 이용해 C_h와 C_v를 계산하고 이를 이용해 Y_h와

Y_v를 계산해 서로 교환한다.

C_h = hash(X_h, ID_h, ID_v, t) 이고 C_v = hash(X_v, ID_v, ID_h, t) 이며 여기서 t는 time stamp다. 또 $Y_h = g^{Rh.Sh.Ch} \bmod n$ 이고 $Y_v = g^{Rv.Sv.Cv} \bmod n$ 이다.

과정 3 : HUB와VSAT은 각각 자신의 랜덤 수와 비밀키를 이용해 공통키 $W_{hv} = (g^{-IDv}. X_h)^{Rh.Sh} = (g^{-IDh}. X_v)^{Rv.Sv} = g^{Rh.Rv.Sh.Sv} \bmod n$를 얻는다.

과정 4 : $S_v = X_h^{Ch'}/(Y_h.g^{IDv.Ch}. ID_v^d) \bmod n$인지를 통해 VSAT은 HUB를 인증하고 HUB도 똑 같은 방식으로 인증 한다. 즉 VSAT은 Y_h를 통해 받은 C_h'가 이전에 받은C_h와 같은지 확인하며 이때 C_h의 함수인 X_h가 다르면 C_h'와 C_h는 달라 인증식이 다르게 되어 서로간에 인증이 가능하다.

4. 시뮬레이션

앞에서 제안된 변형 DH 방식에 ID 개념이 도입된 키분배 프로토콜에 대해 시뮬레이션 결과를 제시 한다. 키 분배에 적용한 알고리즘은 보통 공개키 알고리즘을 사용하고 실제 데이터를 암호화 하는데는 비밀키 암호 알고리즘을 사용하는 것이 구현이나 효율성면에서 효과적이다. 본 연구에서는 제안된 키분배 및 공유 과정에서 필요한 모듈러 연산을 위하여 Montgomery 알고리즘을 이용하였으며 계산에 사용된 해쉬 함수는 MD5(Message Digest 5)를 이용하였다. 이들 연산은 PC 486상에서 시뮬레이션 되었으며 ID 개념이 도입된 변형 DH 방식에 대한 시뮬레이션 결과는 다음과 같다.

① GF(p)와 GF(q)에서 동시에 원시원인 g와 모든 가입자에게 공통으로 알려진 공개 인수이며 합성수인 n 값은 각각 다음과 같다.

g = 17ed a2d6 f551 6389 c514 5639 096f dd5c
c928 2097 ad21 1a5b ea56 4bab 28c0 6bba
0a00 81f7 a58b 42cf d959 2d72 e001 0c34
bb17 35e6 72cf bf47 d247 ca13 6297 6549

n = 9505 e383 51fc 6769 8fcb e0a8 da98 95b2
c74f c59e ce12 6073 8e49 b2da 49b2 32cc
0f8f dc9e 9769 21da 2947 f4ef f5b4 ba61
33d7 34d7 6689 3bd0 801b 1643 4df4 2465

② HUB와 VSAT은 랜덤수를 생성하고 X와 Y를 구한 후 서로 교환 한다.

(HUB)

S_h = time

ID_h = chul-su

R_h (Random Number) =
bea8 abaa a3aa e2ae 3546 abc5 42ae aa2a
b555 5445 957b 1575 2bc5 70d4 2aea 0ae5
474c 84bd 622b 945d 4578 ae2a 2a1a f52d
4aa2 e2b5 15d4 2aaf 42b5 01ea 8aba 8aeb

X_h = f509 3f56 e7aa 4633 bf61 f221 acae a548
2575 48a0 7a18 e92b 580e 15c3 2af1 bf98
7781 3687 0757 eb76 d539 779a 1661 56a0
a148 8cb5 c399 560b fc80 ed28 25ba 984e

C_h = 094c ff3d 6645 cfdf b5da 22d1 99e3 e7e3
c725 dbf8

Y_h = 0017 8255 f2b9 7f3b a46b a508 0844 9ef7
d131 49d9 b06c a225 0c01 18af 3d80 9683
131b f203 10a5 3183 b0e0 38dd fb26 8d25
6d7a 9673 0478 e89b 4c9b 0e07 364c 76e4

(VSAT)

ID_v = sun-hee

S_v = gold

R_v (Random Number) =
d454 0aae 7312 6547 515d 43af 51cc cad4
3eae a28d a2ea 51cd 475d 15d4 751a ea35
d42b ab51 5d59 95aa 1d1e 2f95 1455 5217
4213 0ebb d457 54af 52af 5157 d50a a556

X_v = 9b3b 19a4 69b1 333b b33c d9be cbe8 9ffb
29d1 006c a9c8 2c0f 8e6f 8479 3024 52ca
c126 1aa0 7abe 4b40 b621 3e04 6ac4 2731
fc75 e8df 00bd e1e1 3767 90b5 35b7 ad39

C_v = 4dc0 74a6 a15b adbe fc19 4452 c84d c3f1
a4b7 dcad

Y_v = 8358 a083 9b26 1f51 d11e 121b a200 f536
016e f1e9 c0e9 826b 29c2 3870 0fc1 abf3
bba5 98bc 983a 5a53 dd2c bb13 9ee6 dd7f
d8be 0fc7 8602 3e7d e796 04de fb28 e577

③ HUB와 VSAT은 보내온 X와 Y를 이용해 인증하고 서로간 공통키를 계산한다.

W_{hv} (Working Key) =

2d2c	f512	1437	88b5	34b0	8d27	193c	7e87
184d	220e	9584	454c	9e6b	12fe	251c	6d79
b3f9	4f51	0eb9	40bc	92ee	77d0	538b	fb31
8eb5	4aed	7727	4549	9d0d	ba42	64a4	6162

제안된 키분배 프로토콜을 시뮬레이션하는 과정에서 사용했던 해쉬 함수는 MD5[12]였고, 모듈러 연산을 위해 Montgomery 알고리즘[11]을 적용했다. 이들 프로그램을 PC 486에서 수행한 시간은 대략 MD5 가 512 비트 입력에 대해 3 ms 정도, Montgomery 알고리즘의 경우 4 ms 정도가 소요되었다. 전체는 제안된 두 방식 각각에 대해 약 3-6 ms 정도를 소요 했다. 이는 VSAT 위성통신의 환경상 위성의 시간 지연 약 200-600 ms를 감안하고 중심국과 단말국의 idle time을 이용해 Precomputation and Lookup Table[13] 기법을 이용한다면 효과적이라 고려된다.

5. 결 론

1대 1 통신 혹은 1대 N 통신 형태로 이루어지는 VSAT위성통신은 정보의 노출이 쉬운 전송로를 가지며, 또한 다자간의 통신이 이루어지는 통신망이다. VSAT 위성통신에서 보호는 위성을 이용한 데이터 통신 측면에서 먼저 중심국과 단말국간의 송수신되는 데이터가 보호되어져야 한다. 이에 본 연구에서는 VSAT 위성통신의 안전성을 위한 키 분배 방식을 제안 했다. 제안된 키 분배 방식은 기존의 방식은 단점을 보완하면서 안전성 측면에서 강화되고 VSAT 위성통신의 특성을 맞는 특징을 갖고 있다. 먼저 비밀 정보S_i는 mod n 에서 ID_i의 d멱승으로 ID_i나 n, g를 이용하여 계산하기는 매우 어렵다는 것이 이산 대수 문제로 이미 입증되었다. 또한 n을 통해 p, q를 찾는 것도 합성수의 소인수 분해의 문제로 이미 안전성이 입증 되었다. 그리고 X_i 혹은 Y_i를 통해 세션키 (WK)를 찾는 것도 이산 대수 문제와 합성수 소인수 분해의 어려움을 바탕으로 하고 있어 그 안전성은 매우 높다 할 수 있다. 기타 변형 DH 방식에 ID 개념을 도입한 방식은 두 통신자간에 직접 인증이 가능하며 RSA[13] 방식에서 처럼 모든 가입자가 서로 다른 n을 갖지 않아도 되고 세션키의 변경을 수시로 할 수 있다. 그밖에 가입자는 처음 네트워크 가입시 센터로부터 파라메터를 받고 이후부터는 센터의 지원 기능이 필요치 않으며 새로운 가입자가 추가되어도 기존 가입자의 키 수정이 필요 없다는 것이 특징이다. 제안 방식의 실제 구현에 있어서는 스마트 카드와 Precomputation and Lookup Table [13] 개념 도입으로 효율성을 유도할 수 있으며 VSAT 위성통신의 특성상 키센터를 VSAT위성 중심국의 운영 및 관리부로 두어 센터의 기능을 강조한다면 VSAT 위성통신 환경에 적합한 모델로 기대된다. 아울러 ID 개념이 도입된 변형 DH 방식은 통신 상대자간의 직접 인증이 가능하며 안전성을 큰 소수의 합성수 문제와 이산 대수의 문제 해결에 바탕을 두고 있다. 이 방식은 위성의 여러 사용자간의 비밀 통신을 위한 공유키 생성으로 확대 적용 가능하다.

참 고 문 헌

[1] Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. of Crypto'84, 1984.

[2] M. Fiat and A. Shamir, "How to prove yourself : practical solution to identification and signature problems," Proc. Crypto 86, Santa Babara, Springer-Verlag, LNCS Vol.263, pp.186-199, 1986.

[3] K. M. Sundara Murthy, "VSAT User Network Examples," IEEE Communication Magazine, pp. 50-57, May 1989.

[4] Jim Stratigos and Rakesh Mahindru, "Packet Switch Architecture and User Protocol Interfaces for VSAT networks," IEEE Communication Magazine, Vol.26, No.7, pp.39-47, July 1988.

[5] Dattackumar M. Chitre and John S. McCoskey, "VSAT Networks : Architectures, Protocol, and Management," IEEE Communication Magazine, Vol.26, No.7, pp.28-38, July 1988.

[6] Chakraborty, "VSAT Communications Networks - An Overview," IEEE Communication Magazine, Vol.26, No.5, pp.10-24, May 1988.

[7] Eiji Okamoto and Kazue Tanaka, "Key Distribution System based on Identification Information," IEEE Journal on Selected Areas in Communications, Vol.7, No.4, pp.481-485, May 1989.

[8] Y. Yacobi and Z. Shmuely, "On Key Distribution," Proc. Crypto '89, pp.335-346, 1989.

[9] K. Koyama and K. Ohta, "Identity-Based Con-

ference Key Distribution Systems," Proc. Crypto 87, pp.175-184, 1984.

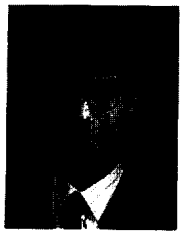
[10] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. Inform. Theory, Vol.IT-22, No.6, pp.644-654, 1976.

[11] P.L. Montgomery, "Modular Multiplication Algorithm using Lookahead Determination," IEICE Trans., Vol.E76-A, No.1, pp.70-77, January 1993.

[12] R. Rivest, "The MD5 Message Digest Algorithm," Requests for Comments (RFC) 1321, 1992.

[13] A. Fujioka, T. Okamoto, and S. Miyaguchi, "ESIGN : An Efficient Digital Signature Implementation for Smart Cards," Proc. of the Eurocrypt 91, pp.446-457, May 1991.

[14] 박정현, 이상호, "Applied to Satellite Communications of the Modified Diffie-Hellman Scheme," 한국통신정보보호학회 논문지, 9월호, 1996.



박 정 현

e-mail : jhpark@amadeus.etri.re.kr

1982년 2월 숭실대학교 전자공학과 졸업(공학사)

1985년 2월 숭실대학교 대학원 전자공학과 졸업(공학석사)

1997년 2월 충북대학교 대학원 전자계산학과 졸업(이학박사)

1982년 3월~현재 한국전자통신연구원 이동관리연구실 선임연구원

관심분야 : 네트워크 시큐리티, 시큐리티 프로토콜, 이동 및 위성 통신 보안

임 선 배

e-mail : sblim@amadeus.etri.re.kr

1978년 2월 고려대학교 전자공학과 졸업(공학사)

1989년 2월 한국과학기술원 전자계산학과 졸업(이학석사)

1993년 2월 고려대학교 대학원 전자공학과 졸업(공학박사)

1979년~1984년 금성사/금성반도체 선임연구원

1984년 3월~현재 한국전자통신연구원 이동관리연구실장, 책임연구원

1997년 3월~현재 TTA SC7 IMT-2000 망 연구위원회 의장

관심분야 : IMT-2000 Network/Security/Protocol/UPT