X.25 프로토콜 기반의 새로운 키 분배 및 인증 방식

손 기 욱† · 박 응 기† · 이 진 석†† · 신 기 수†

요 약

컴퓨터 통신망을 통한 정보전송에 있어 정보보호의 문제는 매우 중요하며 이를 제공하기 위한 정보보호 시스템 개발이 여러 방면에서 이루어지고 있다. 이러한 정보보호 시스템 개발시 비밀키의 분배 및 상호 인증은 정보보호의 필수 불가결한 요소이며, 이에 대한 많은 방법들이 제시되어 왔다. 그러나 이러한 많은 방법들은 통신 프로토콜을 고려하지 않은 경우가 많아 실제 통신 환경에 적용하기가 쉽지 않았다. 본 논문에서는 패킷 통신의 하나인 X.25 프로토콜을 중심으로 프로토콜이 갖는 특성을 유지하면서 키 분배 및 인증을 수행하는 방법을 제안하였으며, 선택적으로 비밀 통신을 할 수 있는 방법을 함께 제안함으로써 정보보호 시스템이 범용성을 갖도록 하였다.

A Key Distribution and Authentication Scheme based on X.25 Protocol

Ki-Wook Sohn† · Eung-Ki Park† · Jin-Seok Lee†† · Ki-Soo Shin†

ABSTRACT

The information security is very important in computer communication network, and the security system has been developed in many aspects to provide secure communication. The secret key distribution and mutual user authentication are essential element in designing security system, then many algorithms and implementation schemes have been proposed. But they don't consider communication protocol, so they are not easy to adapt a real communication networks.

In this paper, we propose a key distriburion and mutual user authentication scheme based on X.25 protocol which is the most popular in packet communication, and the proposed scheme maintains a protocol transparency and can select communication mode, so the security system is more capable.

1. 서 론

컴퓨터 통신망이 발전함에 따라 사용자들은 많은 양의 정보를 컴퓨터 통신망을 통해 주고 받고 있다. 효율적인 전송과 신뢰성이 높은 통신은 컴퓨터 통신망의 사용을 증가시킬 것이며, 전송되는 정보의 증가는 물론 그 내용 면에서도 중요성을 더해갈 것이다.

† 정 회 원:한국전자통신연구원
†† 종신회원:한국전자통신연구원
논문접수:1997년 3월 13일, 심사완료:1997년 10월 18일

이러한 통신망의 비약적인 발전 속에서 전송되는 정보에 대한 보호 문제가 대두되었고, 정보보호 문제는 컴퓨터 통신망의 한 분야로서 많은 연구가 진행되고 있다. 특히 키 분배 및 통신 상대자에 대한 인증은 안전한 비밀 통신을 위해 반드시 필요한 요소가 된다.[1][2]

본 논문에서는 키 분배 및 상호 인증 알고리즘을 실제 패킷망 환경에 적용시켜 안전한 통신을 제공할 수 있는 방안을 제시하였는데, 패킷망을 구성하는 프로토콜은 X.25를 모델로 하였다. X.25 프로토콜은 패킷 통신을 대표하는 프로토콜로서 일반 데이터 통신

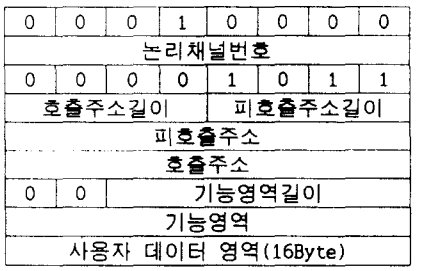
은 물론, 통신망 사이의 연동 프로토콜로도 많이 사용되고 있다.[3][4][5] 또한, 일반 기업체나 기관에서는 X.25 사설망을 구축하여 기업 내부의 통신에 사용하고 있으며, 현재 추진중인 협대역 ISDN이나 광대역 ISDN이 완전히 자리잡기 전까지는 앞으로도 상당 기간 사용되리라 생각된다. 본 논문에서는 X.25 프로토콜의 호 설정 과정 및 제공되는 선택사항(option)을 이용하여 키 분배 및 인증 알고리즘을 적용했다. 또한, 일반적으로 정보보호 시스템을 사용하는 사용자와 그렇지 못한 사용자들 사이에서는 정보보호 시스템이 선택적으로 암호화를 수행하여 융통성을 부여할 수 있어야 한다. 이는 통신 선로의 가용성을 높임과 동시에 정보보호 시스템의 설치로 인한 통신 두절 현상은 바람직하지 못한 것이기 때문에 정보보호 시스템이 갖는 요구사항의 하나로 정의될 수 있다. 따라서, 본 논문에서는 이와 같은 문제를 해결할 수 있도록 정보보호 시스템이 선택적으로 비밀 통신을 할 수 있는 방법을 제안하였다.

2. X.25 프로토콜

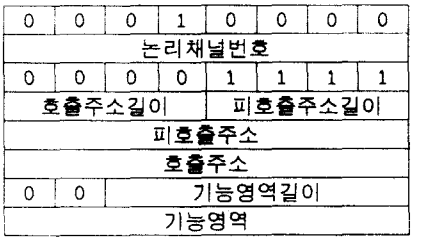
2.1 호 설정 과정

X.25 프로토콜에서는 가상호(virtual circuit)라는 개념을 도입하여, 하나의 실회선(physical line)에 다수의 가입자들이 동시에 사용할 수 있도록 하였다. 가상 회선은 패킷망에 접속된 DTE(Data Terminal Equipment)들 사이에 이루어진 양방향 회선을 의미하며 이는 실제 회선을 나타내는 것이 아니라 논리적 통신 선로를 의미한다. 따라서 하나의 실회선을 통해 다수의 DTE는 원격의 DTE들과 통신이 가능하며 이때 가상회선에 존재하는 논리 채널 번호는 접속된 DTE의 수만큼 존재하며 그 값은 채널마다 다르게 할당된다. 이렇게 패킷망에 접속된 DTE들이 서로 통신을 위해서는 가상 회선을 설정해야 하는데 이를 위한 과정을 호 설정 단계라 한다. 가상 회선에는 교환 가상 회선(SVC: Switched Virtual Circuit)와 영구 가상 회선(PVC: Permanent Virtual Circuit)의 두 가지 종류가 있다. 교환 가상 회선은 두 DTE 사이에 설정되는 임시 경로를 의미하며, 호출(calling) DTE가 호 요구 패킷을 패킷망으로 송신함으로써 시작되며 피호출(called) DTE가 이에 대한 응답으로 호 수락 패킷을 송신함으로써 호가 이루어지게 된다. 교환 가상 회선은 일단 호가 설정된 이후에 어느 DTE든지 해제 요구를 할 경우, 이미 설정된 호는 끊어지게 되며 논리 채널 번호는 반납된다. 이에 반해 영구 가상 회선은 영구적인 경로를 말하며 이는 X.25를 이용하는 가입자가 최초로 패킷망에 가입할 때 영구 가상 호로 등록함으로써 가능하며 가입 기간이 끝나기 전에는 통신을 위한 호 설정 단계가 필요 없이 통신이 가능하게 된다. 본 논문에서는 교환 가상 호의 호 설정 단계를 이용, 정보보호 서비스를 제안하였다.

패킷망에 접속된 두 DTE 사이의 호 설정단계는 통신을 원하는 DTE가 호 요구 패킷을 전송함으로써 시작된다. 호 요구 패킷 및 착신 호 패킷은 (그림 1)과 같이 송신 DTE의 주소, 수신 DTE의 주소, X.25 프로토콜이 제공하는 기능을 나타내는 기능 영역(facility field) 및 사용자 데이터 영역으로 구성되어 있다. 호의 설정은 호출 DTE가 호 요구 패킷을 패킷망으로 전송함으로써 시작된다. 이를 수신한 패킷망은 피호출 DTE에게 착신 호 패킷을 송신하고, 피호출 DTE로 부터 호 수락 패킷을 수신한다. 이후 호출 DTE에



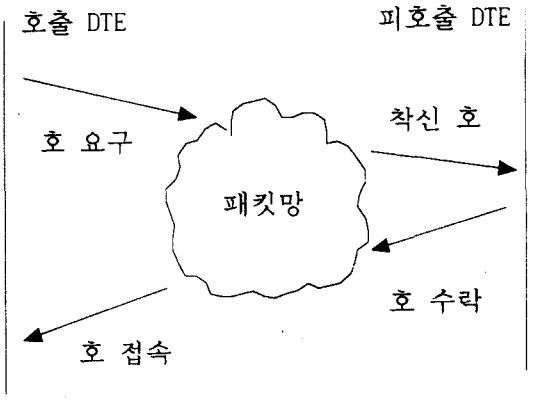
(그림 1) 호 요구 및 착신 호 패킷
(Fig. 1) Call request/incoming call packet



(그림 2) 호 수락 및 호 접속 패킷
(Fig. 2) Call accept/call connect packet

게 호 접속 패킷을 전송함으로써 호 설정을 마치게 된다. (그림 2)에서는 호 접속 및 호 수락 패킷을 나타내고 있는데, 구성은 호출 DTE의 주소와 착신자의 주소 영역 및 X.25의 기능 영역으로 구성되며 호 요구 패킷 및 착신 호 패킷과는 달리 사용자 영역이 존재하지 않는다.

(그림 3)에서는 호출 DTE와 피호출 DTE 사이의 호 설정 과정을 나타내고 있다.



(그림 3) 호 설정 과정
(Fig. 3) Call setup phase

2.2 Fast Select Option 및 응용

Fast Select는 X.25가 제공하는 여러 가지 기능 가운데 하나로, 호 설정 및 해제에 관련된 패킷의 사용자 데이터 영역을 128 옥텟으로 확장하여 이 영역을 사용할 수 있도록 한 가능이다. 이 기능의 대표적인 응용으로는 POS(point of sale) 이나 신용카드 조회 등이 있다. 128 옥텟의 사용자 영역을 이용하여 구매자를 확인할 수 있는 정보들(예를 들면, 구매자의 신용카드 번호 및 파기일자, 구매일자, 구매액 등)을 호 요구 패킷의 사용자 영역에 기입하여 송신하게 된다. 수신 측에서는 호 수락 패킷을 이용하여 송신측에서 문의한 구매자에 대한 확인 결과를 사용자 영역을 이용하여 송신한다. 이러한 Fast Select Option은 호 설정 과정만을 통해 필요한 정보를 교환함으로써, X.25 프로토콜이 구조적으로 갖고 있는 흐름 제어 및 오류 제어의 과부하를 줄이는 방안으로 사용될 수 있다. Fast Select Option 기능은 통신량이 적은 트랜잭션 단위의 환경에서 많이 사용 될 수 있다. 각각의 DTE들이 Fast Select Option을 사용하게 될 경우, 호 설정 단계는 두 가지 경우로 나누어 질 수 있는데 첫째는, 일반적인 호 설정 단계를 그대로 유지하면서 호를 설정한 뒤, 데이터의 송,수신이 있게 되고 이후 호 해제 과정을 통해 종료하는 방법이다. 이 경우는 호 설정 패킷의 사용자 데이터 영역을 16 옥텟에서 128 옥텟으로 확장해서 사용한다는 점만 다를 뿐 앞에서 기술한 호 설정 단계와 다를 것이 없다. 두 번째 경우는 호 설정과 동시에 호 해제가 이루어지는데, 이 경우는 짧은 데이터를 갖는 트랜잭션 단위의 통신에 많이 사용된다. 먼저 호출 DTE는 호 요구 패킷의 사용자 데이터 영역을 이용하여 피호출 DTE에게 데이터를 전송하게 되고, 이는 패킷망을 경유하여 피호출 DTE에게 전송된다. 착신 호 패킷을 수신한 피호출 DTE는 해제 요구 패킷의 사용자 영역에 호출 DTE가 원하는 내용을 작성하여 전송하고 이는 패킷망을 통해 발신자에게 해제 확인 패킷으로 전송된다. 이 경우 호 요구 및 호 해제 패킷의 전송만으로 데이터의 전송이 완료되므로 불필요한 패킷의 전송이 없어진다. 이러한 Fast Select Option을 이용한 호 설정이 이루어지기 위해서는 모든 DTE들이 Fast Select Option을 가지고 있어야 한다. 만일 어느 한 쪽이 이러한 기능을 갖고 있지 않다면 호는 설정되지 않는다.

3. X.25의 Security Service

X.25 프로토콜을 이용한 데이터 통신에 정보보호 서비스를 제공하기 위해서는 X.25 프로토콜의 투명성(transparency)을 유지해야 한다. 발신자가 전송한 패킷은 여러 경로를 통해 착신자에게 전송되는데, 이러한 경로를 설정할 때 이를 위한 정보가 포함되어 있는 패킷 헤더를 참조하게 된다. 따라서 정보보호를 위해 패킷에 대한 암호화 및 복호화 시에는 패킷 헤더가 변형되지 않도록 선별적으로 이루어져야 한다. 또한 X.25가 사용하는 패킷중 암호화 대상은 데이터 패킷에 국한 되야 하며 이외의 패킷은 프로토콜의 투명성을 위해 원래의 형태 및 값을 유지해야 한다. 본 장에서는 X.25 프로토콜을 유지하면서 정보보호 서비스를 제공할 수 있는 방안을 제시하고자 한다. 본 논문에서의 키 분배 및 인증은 두 단계로 나누어 지는데, 첫번째 단계는 인증과 키 교환을 위한 시스템

준비 단계이고, 두번째 단계는 키 분배 및 인증을 수행하는 통신 단계이다. 통신 단계에서는 X.25 프로토콜에서 사용되는 패킷의 시퀀스 번호를 제어하는 방법과 Fast Select Option을 이용하는 방법으로 나누어 제안하였다.

3.1 시스템 준비 단계

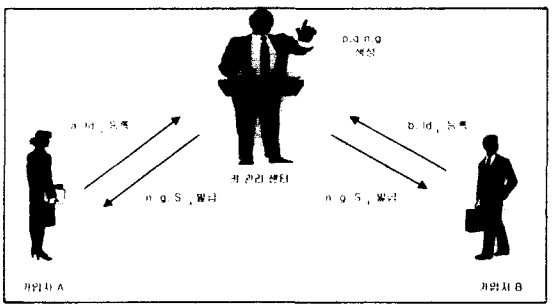
시스템 준비 단계에서 키 관리 센터(Key Management Center)는 자신의 비밀 정보 및 공개 정보를 생성하고, 가입자의 ID 정보를 이용해서 각 가입자에 대한 비밀 정보를 생성하여 스마트 카드와 같은 안전한 채널을 이용해 가입자에게 분배한다.

[단계 1] 키 관리 센터는 두 개의 큰 소수 p와 q를 이용하여 이들의 곱인 n을 생성한다. 이 때 p, q 및 n 등은 안전성을 고려하여 선택이 되어야 하고, 일반적으로 RSA 암호 방식에서 선택하는 것과 동일한 조건으로 생성된다.[6][7][8][9] 또한 키 관리 센터는 $GF(p)$와 $GF(q)$의 원시 원소인 g를 생성한다.

[단계 2] 카드 발행 단계에서 키 관리 센터는 각 가입자에게 분배할 비밀 정보 생성을 위해 각 가입자가 제출한 자신의 정보에 대해 정당성을 확인한 후, 가입자 a의 개인 정보인 id_a를 이용해서 비밀 정보인 S_a를 다음과 같이 생성한다.

$$S_a = ID_a^{-1} \bmod \phi(n),\ ID_a = (id_a \,||\, 1),\ [||\text{ = Concatenation}]$$
$$ID_a^{-1} ID_a = 1 \bmod \phi(n),\ \phi(n) = (p-1)(q-1)$$

키 관리 센터는 가입자 a에 대해 시스템의 공개 정보인 n, g 및 가입자의 비밀 정보인 S_A를 스마트 카드에 저장하여 발급한다. (그림 4)에서는 시스템 준비 단계를 나타내고 있다.



(그림 4) 시스템 준비 단계
(Fig. 4) System setup phase

키 관리 센터가 각 가입자의 비밀 정보를 위와 같이 선택한 후 해당 가입자에게 스마트 카드를 통해 분배하게 되는데 이 때, 다른 가입자들의 비밀 정보를 계산 할 수 있거나 유추해서는 안된다. 이에 대한 안전성은 센터가 생성하는 n의 소인수 분해 문제에 의존하게 되며 이 경우 n의 구성 인자수를 적게 하는 것이 안전성이 우수한 n을 생성할 수 있다. 합성수 n은 다음과 같은 식이 만족하는 수로 구성한다.[7][10]

$p = 2p' + 1$, p'은 소수
$q = 2q' + 1$, q'은 소수

이 경우의 $\phi(n)$을 살펴보면,

$$\begin{aligned}\phi(n) &= (p-1)(q-1)\\ &= (2p'-1)(2q'-1)\\ &= 4p'q'\end{aligned}$$

가 된다. 즉, ϕ(n)은 p′, q′ 및 4를 인수로 갖게 되므로 위에서 언급한 n의 생성 조건에 만족한다고 볼 수 있다. 각 개인의 비밀 정보 S_i가 ϕ(n) 상에서 생성되므로 S_i가 존재하기 위해서는 각 개인의 비밀 정보 id_i와 ϕ(n)이 서로소의 관계를 가져야 한다.

$$gcd(id_i, \phi(n)) = 1$$

이 때, 각 id_i가 홀수이면서 p′ 또는 q′를 인수로 갖지 않으면 위의 조건을 만족하게 된다.

각 개인의 id 정보는 주민등록번호, 이름, 전화번호, 주소 등을 사용할 수 있으며, 이 정보들이 짝수일 확률은 1/2이 된다. 어떤 가입자의 개인 정보가 짝수인 경우 ϕ(n)과의 서로소 관계를 만족할 수 없으므로 해당 가입자에 대해 비밀 정보를 생성할 수 없는 문제가 발생한다. 이러한 문제는 각 가입자들이 키 관리 센터에 제출한 개인 정보 id에 대해 1을 연접(concatenation)시켜 ID로 사용하면, 문제점을 해결할 수 있다.

본 논문에서 사용한 키 분배 및 인증 방식에 대한 안전성에 대하여 고찰하면 다음과 같다. 먼저 가입자 i가 전송하는 정보는 아래와 같다.

$Y_i = ID_i^{Si} \cdot g^{CiRiIDj} \bmod n$

$Z_i = g^{IDiIDjRi} \bmod n$

$C_i = HASH(Z_i, ID_i, ID_j, T_i)$,

[T_i = time stamp, R_i = 가입자 i가 선택한 난수]

비밀 정보 s_i는 mod ϕ(n)에서 ID_i에 대한 곱셈 역원이므로 공개 정보인 ID_i, n, g를 이용하여 계산하기는 어렵다. 왜냐하면, ϕ(n)은 센터만이 아는 비밀 정보이며 공개 정보 n을 통해서 ϕ(n)의 값을 얻어내는 것은 합성수의 소인수 분해 문제에 해당하게 되며 이에 대한 안전성은 이미 계산적으로 안전함이 입증되어 있다. 또한 Z_i를 통해서 R_i의 값을 알아내는 것은 이산 대수 문제에 해당되며 이에 대한 안전성 역시 입증되어 있다. 따라서 본 노문에서 제안한 키 분배 방식은 이산 대수 문제 및 합성수의 소인수 분해 문제의 어려움에 기반을 둔 안전한 키 분배 방식이라 할 수 있다. 또한, 송신 및 수신 정보에 대한 직접 인증이 가능하므로 가입자들이 정보 전송 후 송, 수신 정보의 부인을 봉쇄할 수 있는 방식이라 생각된다.[11]

3.2 시퀀스 번호를 제어하는 방안

본 절에서는 패킷 단말기와 패킷망 사이에 정보보호 시스템을 접속하여 정보보호 시스템에서 패킷의 시퀀스 번호를 제어하는 방법을 통해 통신 DTE들 사이의 인증 및 키 교환이 이루어지는 과정을 설명하고자 한다.

일단 통신을 하고자하는 DTE들은 호 설정 단계를 통해 정보 전송을 할 수 있는 상태로 들어간다. 이 때 호출 DTE와 접속된 정보보호 시스템(이하, "호출 정보보호 시스템")에서는 데이터 패킷을 다음과 같이 생성하여 피호출 DTE에 접속된 정보보호 시스템(이하, "피호출 정보보호 시스템") 쪽으로 전송한다.

$Y_a = ID_a^{Sa} \cdot g^{CaRaIDb} \bmod n$

$Z_a = g^{IDaIDbRa} \bmod n$

$C_a = HASH(Z_a, ID_a, ID_b, T_a)$,

[T_a = time stamp, R_a = 가입자 a가 선택한 난수]

피호출 정보보호 시스템은 Y_a와 Z_a를 통해 상대방에 대한 인증을 수행한다.

$Y_a^{IDa} / Z_a^{Ca} = ID_a \bmod n$

인증이 올바르게 수행이 되면 피호출 정보보호 시스템은 호출 정보보호 시스템 쪽으로 다음과 같은 데이터 패킷을 전송한다.

$Y_b = ID_b^{Sb} \cdot g^{CbRbIDa} \bmod n$

$Z_b = g^{IDaIDbRb} \bmod n$

$C_b = HASH(Z_a, ID_a, ID_b, T_a)$,

[T_b = time stamp, R_b = 가입자 b가 선택한 난수]

호출 정보보호 시스템은 Z_B와 Y_B를 통해 착신자에 대한 확인을 하게 된다.

$Y_a^{IDa} / Z_a^{Ca} = ID_a \bmod n$

발신측과 착신측에서 모두 인증이 이루어 지면 비밀 통신을 위해 사용될 세션키 생성 단계에 들어간다. 양쪽 정보보호 시스템은 교환한 초기값을 통해 최초의 데이터 패킷을 암호화할 세션키를 생성한다.

$SSK_{1st} = (Z_a)^{Rb} = (Z_b)^{Ra} = g^{RaRbIDaIDb} \bmod n$

이 과정에서는 각각의 정보보호 시스템이 상호간의 인증과 세션키 생성을 위해 임의의 데이터 패킷을 생성했기 때문에 프로토콜의 시퀀스 번호가 변경된다. 즉 호 설정 단계까지의 패킷은 DTE에서 생성된 패킷이므로 정상적인 패킷 시퀀스 번호를 유지하고 있으나, SSK_{1st}를 얻기 위해서 발신 및 착신 DTE와는 관계없는 정보보호를 위한 데이터 패킷이 정보보호 시스템으로 부터 생성되어 상대방에게 전달된다. 이 경우에도 시퀀스 번호는 계속 유지되어야 하므로 정보보호 시스템에서는 이에 대한 관리가 이루어져야 한다. 이를 위해서 정보보호 시스템에서는 호 설정이 이루어진 시점에서 X.25 프로토콜 계층 2의 프레임에 대한 시퀀스 번호인 N(S), N(R) 값과 계층 3의 패킷에 대한 시퀀스 번호인 P(S), P(R)값을 유지하고 있어야 한다. 호 설정이 이루어지고 나면 정보보호 시스템에서는 세션키 생성 및 인증을 위해 Y_A 및 Y_B 생성하게 되는데, 이 때 패킷 헤더 및 프레임 헤더의 시퀀스 번호는 현재 유지되고 있는 시퀀스 번호를 참조하

여 패킷 교환기에서 유지하고 있는 시퀀스 번호와 동일한 값을 갖도록 해야 한다.

Y_A 및 Y_B를 교환하여 초기 세션키 SSK_{1st}를 얻은 정보보호 시스템들은 DTE가 전송하는 데이터에 대해 암호화 대상 패킷인지 아닌지를 판별하게 된다. 암호화 대상이든 아니든 시퀀스 번호를 변경해야 하는데, DTE로 부터 통신망으로 가는 패킷의 경우는 정보보호 시스템이 관리하는 시퀀스 번호와 DTE가 전송한 시퀀스 번호만큼의 차이를 정보보호 시스템에서 보상해서 통신망으로 전송한다. 데이터 패킷에 적용될 세션키를 매 패킷 마다 다르게 하기 위한 방법의 하나로, 암호화된 데이터의 일부를 추출하여 정보보호 시스템내의 세션키 생성기의 시드(seed)로 사용하며, 정보보호 시스템의 세션키 생성기에서는 시드를 이용하여 다음 데이터 패킷을 암호화하기 위한 세션키를 생성한다. 이 후의 과정은 암호화, 세션키 시드 추출, 시퀀스 번호 변경 및 새로운 세션키 생성이 반복된다.

통신망으로부터 패킷을 수신한 정보보호 시스템은 수신된 패킷이 복호화 대상인지 아닌지를 판별하여, 복호화 대상이 아닌 경우에는 시퀀스 번호를 변경하여 수신 DTE로 전송한다. 데이터 패킷의 경우는 이미 생성된 세션키를 이용해서 복호화한 뒤, 시퀀스 번호를 변경하여 수신 DTE로 전송한다.

암호화 및 복호화의 과정을 단계별로 나타내면 다음과 같다.

[발신측]

단계 1: 호출 정보보호 시스템은 발신 DTE가 송신한 호 요구 패킷을 통신망으로 전송한 뒤, 통신망으로부터 호 접속 패킷을 기다린다.

단계 2: 호 설정이 완료되면 현재 패킷의 시퀀스 번호를 저장한 뒤 초키 세션키를 생성하기 위하여 다음과 같은 정보를 생성한다.

$$Y_a = ID_a^{Sa} \cdot g^{CaRaIDb} \bmod n$$
$$Z_a = g^{IDaIDbRa} \bmod n$$

Y_a와 Z_a로 구성된 데이터 패킷에 대해 현재 저장 중인 시퀀스 번호를 증가시켜 패킷 헤더를 구성한 뒤 통신망으로 전송한다.

단계 3: 피호출 정보보호 시스템이 생성한 Y_b와 Z_b를 수신한 뒤 이를 통해 B에 대한 인증을 확인하고 초기 세션키 SSK_{1st}를 구한다. 이 때 Y_b와 Z_b를 통해 올바른 인증을 할 수 없다면 호 해제 요구 패킷을 전송한 뒤 해제 확인 패킷을 기다린다.

단계 4: 발신 DTE가 전송한 패킷에 대해, 암호화 대상 여부를 판별하여 제어 패킷인 경우 패킷 헤더의 시퀀스 번호만을 변경하여 통신망으로 전송한다.

단계 5: 암호화 대상인 데이터 패킷에 대해서는 SSK_{1st}를 이용해서 다음과 같이 암호화한다.

$$C = E(SSK_{1st}, M),$$

{C = 암호문, E = 암호화, M = 평문 메시지}

단계 6: 호출 정보보호 시스템은 패킷 헤더의 시퀀스 번호를 변경한 뒤 통신망으로 전송한다. 또한 암호화된 데이터의 일부를 추출, 세션키 생성기를 통해 다음 메시지의 암호화를 위한 세션키를 생성한다.

[착신측]

단계 1: 착신 DTE는 착신 호 패킷을 수신한 뒤, 호 수락 패킷을 통신망으로 전송한다.

단계 2: 호 설정이 완료되면 피호출 정보보호 시스템은 현재 패킷의 시퀀스 번호를 저장한 뒤 초키 세션키를 생성하기 위하여 다음과 같은 정보를 생성한다.

$$Y_b = ID_b^{Sb} \cdot g^{CbRbIDa} \bmod n$$
$$Z_b = g^{IDaIDbRb} \bmod n$$

단계 3: 피호출 정보보호 시스템은 송신측에서 전송한 Y_a와 Z_a를 통해 A에 대한 인증을 확인한다. 이 때 올바른 A가 아닐 경우, 호 해제 요구 패킷을 전송하고, 호 해제 확인 패킷을 기다린다.

단계 4: A에 대한 인증이 확인되면 초기 세션키 SSK_{1st}를 구하고, Z_b와 Y_b로 구성된 데이터 패킷에 대해 현재 저장 중인 시퀀스 번호를 증가시켜 패킷 헤더를 구성한 뒤 통신망으로 전송한다.

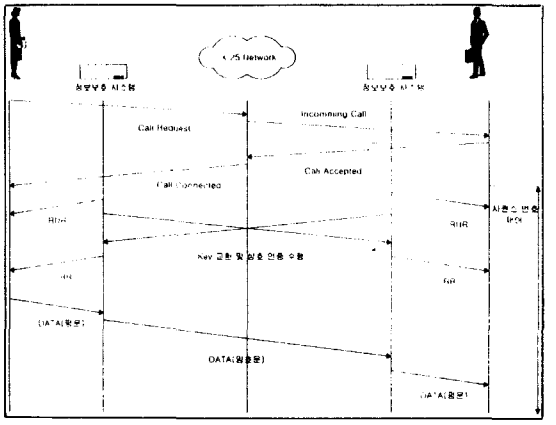
단계 5: 통신망으로부터 수신한 패킷에 대해 복호화 대상 여부를 판별하여 제어 패킷인 경우 패킷 헤더의 시퀀스 번호만을 변경하여 착신 DTE로 전송한다.

단계 6: 복호화 대상인 데이터 패킷에 대해서는 데이

터 패킷의 일부를 추출, 세션키 생성기를 통해 다음 메시지의 복호화를 위한 세션키를 생성하고, 현재 암호화된 데이터에 대해서는 SSK_{1st}를 이용해서 다음과 같이 복호화 한다.

$M=D(SSK_{1st}, C)$, [M=평문 메시지, D=복호화, C=암호문]

단계 7:피호출 정보보호 시스템은 패킷 헤더의 시퀀스 번호를 변경한 뒤 DTE로 전송한다.



(그림 5) 키 교환, 인증 및 암호화
(Fig. 5) Key exchange, authentication and encryption

시퀀스 번호를 제어하여 안전한 통신에 필요한 키의 교환 및 암호화를 하는 방안에서는 정보보호 시스템에서 키 교환 및 인증에 필요한 패킷을 생성하여 서로 교환함으로써 송, 수신 DTE와 정보보호 시스템 사이의 시퀀스 번호가 다르게 된다. 이러한 시퀀스 번호의 변경은 프로토콜의 투명성을 유지하기 위해서 반드시 정보보호 시스템에서 올바르게 관리가 되어야 한다. 이러한 패킷 헤더의 변경은 정보보호 시스템에서 이에 대한 세심한 관리가 요구된다는 단점이 있으나, 프로토콜의 투명성을 유지할 수만 있다면 정보보호 시스템에서 생성하는 패킷을 이용, 정보보호에 필요한 많은 데이터를 전송할 수 있다는 장점이 있다. 이는 기존의 통신망이나 프로토콜에 정보보호 시스템을 적용할 경우, 세션키를 비롯 많은 정보보호 관련 데이터를 상대방에게 전송하기가 어려운 점을 감안할 때 유효하게 사용할 수 있으리라 생각된다. 다음절에서는 패킷 헤더나 프로토콜의 변경 없이 X.25 프로토콜에서 제공하는 기능을 이용하여 호 설정 과정에서 상대방의 인증 및 초기 세션키를 사용하는 방법을 제안하고자 한다.

3.3 Fast Select Option을 이용

2장에서 설명한 바와 같이 X.25 프로토콜에서는 여러 가지 기능(facility)이 존재하며 가입자는 자신들의 필요에 따라 패킷망 가입시 필요 기능을 신청함으로써 사용할 수 있다. Fast Select는 호 설정 단계 패킷들의 사용자 영역을 128 옥텟까지 사용할 수 있다. ((그림 4), (그림 5) 참조)

0	0	0	1	0	0	0	0
논리채널번호							
0	0	0	0	1	0	1	1
호출주소길이				피호출주소길이			
피호출주소							
호출주소							
0	0	기능영역길이					
기능영역							
사용자 데이터 영역(128 Byte)							

(그림 6) FSO의 호 요구 및 착신호 패킷
(Fig. 6) Call request/incoming call packet in fast select option

0	0	0	1	0	0	0	0
논리채널번호							
0	0	0	0	1	1	1	1
호출주소길이				피호출주소길이			
피호출주소							
호출주소							
0	0	기능영역길이					
기능영역							
사용자 데이터 영역(128 Byte)							

(그림 7) FSO의 호 수락 및 호 접속 패킷
(Fig. 7) Call accept/call connect packet in fast select option

이 때는 인증 및 키 전송을 위한 데이터 패킷의 내용을 호 설정 단계의 사용자 영역에 추가하여 전송함으로써 3.2에서와 같이 정보보호 시스템에서 추가적인 데이터 패킷 전송이 필요 없다. 따라서 패킷과 프

레임의 시퀀스 번호를 제어할 필요가 없다. 그러나 이 방안은 가입자들이 Fast Select Option 기능을 갖고 있어야 한다는 조건이 있다.

Fast Select Option을 이용하여 키 교환 및 암호화를 하는 방법은 가입자 사이의 키 교환을 위한 정보와 인증 정보가 호 설정 패킷내의 사용자 데이터 영역에 삽입되며 이러한 정보를 통해 초기 세션키를 생성한 뒤, 발신측과 착신측의 암호화, 복호화를 위한 절차는 3.2와 동일하다.

Fast Select Option을 이용한 정보보호 방안은 위에서 보듯이 별도의 패킷 전송이나 시퀀스 번호 변경은 필요로 하지 않는다는 점에서 우수하나, 모든 사용자들이 Fast Select Option을 사용해야만 올바른 통신이 이루어진다. 이미 가입자의 기능들이 정의되어 있는 환경과 일반 사용자들의 경우에는 3.2에서 제시한 방법을 사용하는 것이 유용하리라 생각되며 위성통신에서의 X.25 프로토콜을 사용하는 곳이나 기업의 사설 패킷망과 같은 곳에서는 상대적으로 X.25의 기능 영역을 변경하기가 용이하리라 생각되므로 3.3에서 제시한 방식이 정보보호를 위해 적합하리라 생각된다.

4. 선택적인 통신 모드 설정

X.25와 같이 가상 회선을 이용하여 다수의 가입자가 하나의 실회선을 통해 통신하는 경우에 비밀 통신을 원하는 가입자가 있을 수 있고 그렇지 않은 가입자도 있을 수 있게 된다. 또한 어느 한쪽의 통신자가 정보보호 시스템이 없는 경우에는 정상적인 통신이 될 수 없는 상황도 발생할 수 있다. 이는 중요 정보를 위한 회선을 따로 사용하여 정보보호 시스템이 설치된 가입자들만 통신을 하도록 하는 방안도 있을 수 있으나 회선의 효율을 높이기 위해 여러 사용자가 사용할 수 있도록 설계된 가상 회선의 장점을 살릴 수 없다는 문제가 발생한다. 따라서 하나의 실회선을 통해 여러 가입자들이 정보보호 시스템을 통해 비밀 통신 및 평문 통신을 할 수 있다면 회선의 효율을 높임과 동시에 장비의 효용성도 함께 증가시킬 수가 있다. 본 논문에서는 호 설정 단계, 가입자의 주소 테이블 및 Fast Select Option을 이용하여 선택적으로 비밀 통신을 할 수 있는 방안을 제시하고자 한다.

4.1 호 설정 단계를 이용하는 방안

호 설정 단계의 호 요구 및 착신 호 패킷의 사용자 데이터 영역에 평문 통신 및 비밀 통신 선택을 위한 플래그를 추가하고, 이 플래그를 정보보호 시스템이 인식함으로써, 선택적으로 통신 모드를 선택할 수 있다. 이 경우, 정보보호 시스템이 설치되어 있는 사용자들은 통신을 하고자 하는 상대방의 환경-정보보호 시스템이 있는지의 여부-을 알아야 한다.

양 쪽 사용자 모두가 정보보호 시스템을 보유하고 있는 경우는 비밀 통신과 평문 통신이 모두 가능하며, 이는 발신자가 원하는 통신 모드에 따라서 호 요구 패킷의 사용자 영역에 자신이 원하는 통신 모드에 해당하는 플래그를 추가하게 되고, 정보보호 시스템은 그 플래그에 따라 동작 상태를 결정하게 된다. 한 쪽만이 정보보호 시스템을 보유하고 있을 경우는 평문 통신만을 하게 되며, 발신측에 정보보호 시스템이 있는 경우에는 평문 통신을 나타내는 플래그를 사용자 데이터 영역에 추가하며, 정보보호 시스템은 평문 통신 모드로 동작하게 된다. 수신측에 정보보호 시스템이 있는 경우에는, 발신측에서 사용자 데이터 영역에 플래그를 추가 할 수 없기 때문에 이 영역에 통신 모드를 나타내는 플래그가 존재하지 않게 되며, 착신측 정보보호 시스템은 평문 통신 모드로 동작하게 된다.

호 설정 단계의 사용자 데이터 영역을 이용하는 방안은 정보보호 시스템을 보유한 가입자들 사이에서도 비밀 통신 뿐만 아니라 평문 통신이 가능하도록 하며, 어느 한쪽 사용자 만이 정보보호 시스템을 소유하고 있는 상황에서, 일방적인 암호화로 인한 통신 불능 상태를 방지하여 정상적인 평문 통신을 할 수 있다.

4.2 주소 테이블 참조 방안

이 방안은 비밀 통신을 원하는 가입자의 주소를 미리 정보보호 시스템에 등록시켜 호 요구 패킷을 수신한 정보보호 시스템은 수신 주소 영역의 주소와 관리하고 있는 테이블 내에 주소가 있는지를 판별하여, 주소가 있을 경우 비밀 통신을 수행하는 한다. 수신측에서도 착 신호 패킷의 송신 주소 영역의 주소와 정보보호 시스템 내의 테이블 주소를 비교하여 주소가 있을 경우 마찬가지로 비밀 통신을 수행한다. 이 테이블 참조 방식은 비밀 통신을 원하는 가입자가 발

생할 때마다 장비 내에 가입자의 주소를 등록시켜야 하며 어떤 주소에 대해 비밀 통신이나 평문 통신으로 결정되면 정보보호 시스템의 테이블을 변경하기 전까지는 바꿀 수가 없다. 또한 가입자의 수가 증가할수록 정보보호 시스템에 등록시킬 주소도 증가할 수 있으며, 이에 따라 호 요구 및 착신 호 패킷의 주소와 테이블내의 주소를 비교하는데 소요되는 시간 증가 및 시스템의 메모리문제도 발생할 수 있다. 그러나 이 방안은 구현이 용이하다는 장점을 가지고 있다. 또한 4.1과 같이 사전에 상대방이 정보보호 시스템이 있는지의 여부를 확인할 필요는 없으나 선택적인 비밀 통신을 위해 비밀 통신 가입자의 주소를 초기에 정보보호 시스템에 등록시키는 과정이 필요하다.

4.3 Fast Select Option 이용 방안

4.1과 4.2에서 제안한 방안은 각각 상대방의 통신 환경, 즉 정보보호 시스템이 설치되어 있는지를 알아야 하는 단점이 있었다. 본 절에서는 패킷망에 접속된 가입자들이 Fast Select Option 기능을 사용하여 이러한 단점을 해결할 수 있는 방안을 제시하고자 한다. 2장에서 언급한데로 Fast Select Option은 호 설정 패킷들의 사용자 영역을 128 옥텟까지 확장시켜 줌과 동시에 호 접속 및 호 수락 패킷에도 사용자 데이터를 사용할 수 있다는 점을 이용하여 선택적인 비밀 통신을 상대방의 통신 환경을 모르는 상태에서도 가능하도록 할 수 있다. Fast Select Option은 정보보호 시스템을 설치하여 비밀 통신을 하는 경우와 같이 어떤 부가 정보의 전송이 필요한 경우, 사용자 영역을 이용하여 실현할 수 있다. Fast Select Option을 사용하여 선택적인 비밀 통신을 하는 경우는 4.1에서 제시한 방법과 동일하나 상대방이 정보보호 시스템을 보유하고 있는지의 여부를 알 필요는 없다.

5. 결 론

본 논문에서는 패킷망의 대표적인 프로토콜인 X.25를 통해 프로토콜의 투명성을 유지하면서 키 분배 및 인증을 수행하는 방법을 제안하였다. 제안된 두 가지 방식은 사용자들의 통신 환경, 통신망 환경 등에 따라 선택적으로 사용할 수 있으리라 생각된다. 또한 제안된 시스템은 기존의 X.25를 사용하는 통신 환경에 아무런 영향을 주지 않고 단말기와 통신망 사이에 접속됨으로써 단말기와 통신망이 정보보호 기능을 수행하기 위해 변경될 필요는 없다. 또한 정보보호 시스템이 가질 수 있는 사용 제약을 없애기 위해 선택적으로 통신 모드를 설정하는 것이 가능하도록 제안함으로써 정보보호 시스템의 범용성을 갖출 수 있었다.

본 논문에서 사용된 키 분배 방식이나 사용자 인증 알고리즘은 RSA 공개키 암호 방식을 기반으로 하여, 이산대수 문제 및 합성수의 소인수 분해 문제를 이용하여 제안하였으나, 설계하고자 하는 시스템의 안전성 및 효율성의 비중에 따라 통신망의 환경에 적합하며 사용하기에 편리한 것으로 대치할 수도 잇을 것이라 생각된다.[12][13][14] 그러나 시스템의 성능을 고려할 때 키 분배 과정은 공개키 암호 방식을 이용하여 초기의 세션키를 공유한 뒤, 암호 알고리즘의 경우는 비밀키 암호 방식을 사용하는 것이 일반적이다.

본 논문에서 제안한 정보보호 시스템을 구현시 하드웨어의 구성은 범용 프로토콜 제어용 프로세서와 16 비트 CPU를 결합하여 제작할 수 있으리라 생각되며, 추가적으로 공개키 암호 방식을 이용한 키 분배를 위해 스마트 카드와 인터페이스 되는 부분도 필요할 것이다.

X.25가 패킷망의 프로토콜로써 뿐만 아니라 망 연동 프로토콜 및 위성 통신에서도 이용되는 만큼 계속적인 정보보호 방안이 연구되어야 한다고 생각되며, 인터넷이나 초고속 정보 통신망의 발전에 따라 이를 제공하는 통신망 프로토콜을 분석하여 최적의 정보보호 시스템을 구축하는 일도 병행되어야 할 것이다. 또한 정보보호 시스템의 설치로 야기될 수 있는 사용자 및 통신망의 불편을 최소화하는 방안도 계속적으로 연구되어야 할 것이다.

참 고 문 헌

[1] Deborah Russell and G. T. Gangemi Sr, "Computer Security Basics," O'Reilly & Associates, Inc., CA, pp. 163-234, July, 1992.

[2] Charlie Kaufman, Radia Perlman and Mike Spenciner, "Network Security," Prentice Hall, New Jersey, pp. 177-202, 1995.

[3] Uyless Black, "*X.25 and Related Protocols*," IEEE

Computer Society Press, CA, pp. 86-90, 1991.

[4] Sherman K. Schlar, "Inside X.25:A Manager's Guide," McGraw-Hill, Inc., NY, pp. 123-138, 1990.

[5] ITU-T Recommendation X.25 "Interface between Data Terminal Equipment(DTE) and Data Circuit-Terminating Equipment(DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit," Helsinki, March, 1993.

[6] David M. Burton, "*Elementary Number Theory*," WCB, IA, pp. 107-182, 1989.

[7] R. L. Rivest, A. Shamir, L. Adleman, "*A Method for Obtaining Digital Signature and Public-Key Cryptosystems*," Comm. ACM, Vol. 21, No. 2, pp. 47-53, 1978.

[8] A. Shamir, "*Identity-based Cryptosystems and Signature Schemes*," Crypto84. pp. 47-53, 1984.

[9] 손기욱, "*ID-Based 키 분배방식 및 회의용 키 분배 방식*," 한국통신정보보호학회 논문지, 제1권, 제1호, pp. 38-46, 1991.

[10] W. D. Jonge, D. Chaum, "*Some variations on RSA signatures & their security*," Crypto 86, pp. 49-59, 1986.

[11] J. Seberry, J. pieprzyk, "Cryptography," Prentice Hall, pp. 22-25, 1989.

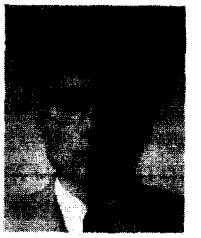
[12] Y. Yacobi, Z. Shmuely, "On Key Distribution System," Crypto 89, pp. 334-355, 1989.

[13] Y. Yacobi, "A Key Distribution:Paradox," Crypto 90, pp. 245-255, 1990.

[14] 이필중, 임채훈, "일반화된 Diffie-Hellman 키이 분배방식의 안전성 분석," 한국통신학회논문지, 91-7, Vol. 7, pp. 575-597, 1991.

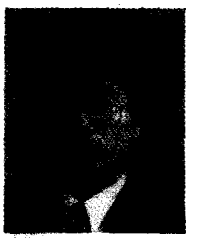
손 기 욱

1990년 성균관대학교 정보공학과 졸업(공학사)
1992년 성균관대학교 대학원 정보공학과 졸업(공학석사)
1992년~현재 한국전자통신연구원 연구원
관심분야:통신망 정보보호, 암호 프로토콜, FPGA 설계



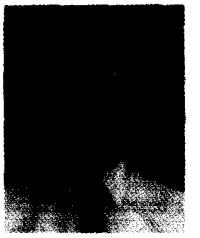
박 응 기

1986년 중앙대학교 전자계산학과 졸업(이학사)
1988년 중앙대학교 대학원 전자계산학과 졸업(이학석사)
1988년~현재 한국전자통신연구원 선임연구원
관심분야:통신망 정보보호, 네트워크 정보보호



이 진 석

1986년 대전산업대학교 전자계산학과 졸업(이학사)
1990년 한남대학교 대학원 수학과 졸업(이학석사)
1986년~현재 한국전자통신연구원 선임연구원
관심분야:컴퓨터 보안, 암호프로토콜, 프로그램 테스팅



신 기 수

1975년 서강대학교 전자공학과 졸업(공학사)
1989년 충북대학교 대학원 전자공학과 졸업(공학석사)
1977년~1980년 삼성전자
1980년~현재 한국전자통신연구원 책임연구원
관심분야:데이터 통신 정보보호, 네트워크 보안, 전자상거래