# LAN 에서의 키이 분배 시스템

°이 창 순*, 문 상 재**
* 대구공업전문대학, ** 경북대학교

# Key distribution system for LAN

°Chang Soon LEE*, Sang Jae MOON**
*Daegu Technical Junior College, ** Kyungpook National University

요 약 문

IEEE 802.10 의 SILS 키이관리 응용에 적용될 수 있는 D-H 형태의 키이분배 시스템을 제안한다. 제안된 키이 분배방식에서는 신분 인증과 키이 생성이 동시에 수행되며, 멱승 연산도 2 번만이 필요하다. 그리고 전체 프로토콜의 수행은 3-way 통신으로 이루어진다. 본 연구에서 제안하는 상호 신분 인증 및 키이 분배 방식은 비밀키이의 소유자만이 상호 통신의 결과로 생성된 키이 값을 정확히 알 수 있다는 사실을 바탕으로 한다. 이와같은 인증과 키이 분배 기능을 동시에 수행하는 프로토콜은 LAN 과 같은 통신망에 아주 적합한 키이 분배 시스템이다.

## 1. 서 론

최근 그 이용이 증가하고 있는 근거리 통신망에서는 어느 국(station)에서나 임의의 주소를 사용하여 다른 국으로 정보의 전송이 가능하고, 또한 임의의 국에서 전송되는 모든 데이타를 엑세스할 수 있다. 따라서 적법 통신자로의 가장이나 정보의 불법 변경 및 도청이 아주 용이하여 상대자의 신분 인증, 데이타 발신처 인증 등을 포함한 정보보호가 더욱 절실하다. 정보보호를 위하여는 설비면에서의 물리적인 대책이나 제도적인 면에서의 법적인 대책에 비해 기술면에서의 정보보호 대책인 암호화시스템

(cryptosystem)의 사용이 보다 효과적이고 경제적인 방법이다[1,2]. 암호화시스템에는 크게 두가지가 있다. 하나는 암호화 및 복호화에 동일한 키이를 사용하는 대칭 키이 암호화시스템(symmetric key cryptosystem) 이고, 다른 하나는 암호화 키이와 복호화 키이가 서로 다른 비대칭 키이 암호화시스템(asymmetric key cryptosystem)이다[3]. 대칭 키이 암호화시스템은 속도가 빠르고, 구현방법 등에 있어서 비대칭 키이 암호화 시스템에 비해 우수하나 가장 문제가 되는 것이 키이관리(key management)이다. 반면에 비대칭 키이 암호화시스템을 두 통신자간의 키이를 분배하는데 사용하면 처리 속도는 상대적으로 느리지만 키이관리 및 인증(authentication) 등의 기능들이 효과적으로 수행될 수 있다[1]. 그래서 일반적으로 정보보호를 위한 암호화시스템의 구현에서는 키이의 분배에는 비대칭 키이 암호화시스템을 이용하고, 이 분배된 암호화 키이를 사용하는 실제 정보의 송수신에는 대칭 키이 암호화시스템을 이용한다. 또한 일반적인 키이 생성 및 신분 확인 과정은, 상대자의 신분 확인을 거친 후 세션키이를 생성하거나 세션키이를 생성한 후 그 키이를 사용한 사전 통신이나 본 통신 중에 상대자를 확인하는 순서로 이루어진다. 그러나 상대자의 인증과 키이분배가 동시에 이루어진다면 키이 분배 과정에서 발생될 수 있는 각종 위협이 미연에 방지될 수 있다. 따라서 LAN과같은 컴퓨터 통신망에서는 누구나 쉽게 전송되는 정보에 접근 할 수 있어 키이 분배와 신분 인증이 동시에 수행되는 키이 분배 시스템의 사용이 요구된다[4].

한편 LAN 에서의 정보보호를 위하여 IEEE 802.10(security working group) 에서는 SILS(standard for interoperable LAN security) 키이관리(key management), SILS 시스템/보호 관리(system/security management) 및 SILS SDE(secure data exchange) 의 3 영역으로 나누어 연구하고 있다[5].

본 연구에서는 IEEE 802.10 의 SILS를 간략히 분석하고, SILS 키이관리 프로토콜에 적용될 수 있는 D-H[6] 형태의 키이 분배 프로토콜을 제안한다. 제안된 키이 분배 방식에서는 신분 인증과 키이 분배가 동시에 수행되며, 기본 원리는 비밀키이의 소유자만이 상호 통신의 결과로 생성된 키이 값을 정확히 알 수 있다는 사실을 바탕으로 한다. 멱승은 2 번만 계산되고 3-way 통신으로 신분 인증과 키이 분배가 동시에 이루어진다.

## 2. LAN 에서의 정보보호

IEEE 802.10 의 SILS는 802 LANs 에서의 정보보호에 관하여 기술하고 있는데 3 부분으로 구성되어 있다. 즉 SDE, 키이관리 및 시스템 관리이다. 이들은 서로 독립적으로 수행되도록 되어있어 각각의 SILS SDE, SILS 키이관리 및 SILS 시스템/보호 관리로 구현될 수 있다. SDE 은 계층 2 에서 안전한 정보교환을 위한 서비스를 제공하는 OSI 표준 참조 모델(US 7498-1)의 계층 2 의 프로토콜에 해당한다. 그리고 키이관리 프로토콜은 계층 2 에서 정보를 암호화하기 위한 암호화 키이 관리 서비스를 제공하는 계층 7 의 프로토콜이다. 시스템/보호 관리는 보호 프로토콜들을 안전하게 관리하기 위한 계층 7 의 서비스들이다. 그림 1 은 IEEE 802 구조와 ISO 표준 참조 모델간의 계층 비교를 도시한 그림이다. IEEE 802 LAN 표준은 MAC 계층과 LLC 계층을 두어 LAN 프로토콜을 제공하고 있으며,MAC 계층은 OSI 계층 1 전부와 계층 2의 일부분을 구성하며 4 가지의 서로 다른 물리적인 매체에 대한 표준 엑세스를 제공한다.

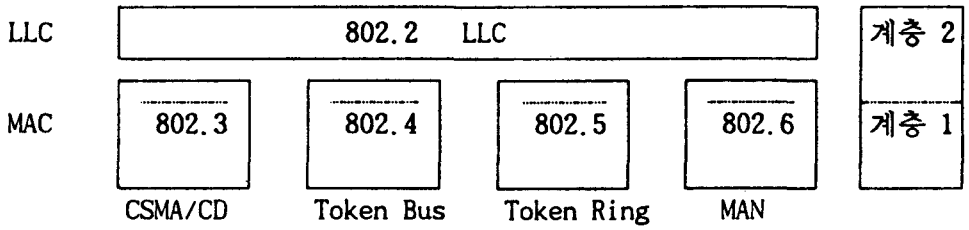


그림 1. IEEE 802 와 OSI 사이의 계층 비교

### 2.1 SILS 키이관리

키이관리 응용은 SILS에 정의되어 있는 키이관리 프로토콜이 제공하는 서비스를 이용하여 SDE 부계층이 어떤 보호 서비스를 제공하려 할 때 사용할 키이를 관리한다. 그리고 제공하려는 보호 서비스의 종류 및 여기에 관련되는 각종 정보와 속성을 결정하여 SMIB 내에 저장 관리한다. 그림 2 에서 키이관리 응용이 SMIB 를 경유하여 키이를 SDE 프로토콜에 제공하는 경로를 보여주고 있다. 또한 그림 2 의 USER Stack 에는 기존의 LAN에서의 통신을 위한 각종 프로토콜이 저장되어 있다.

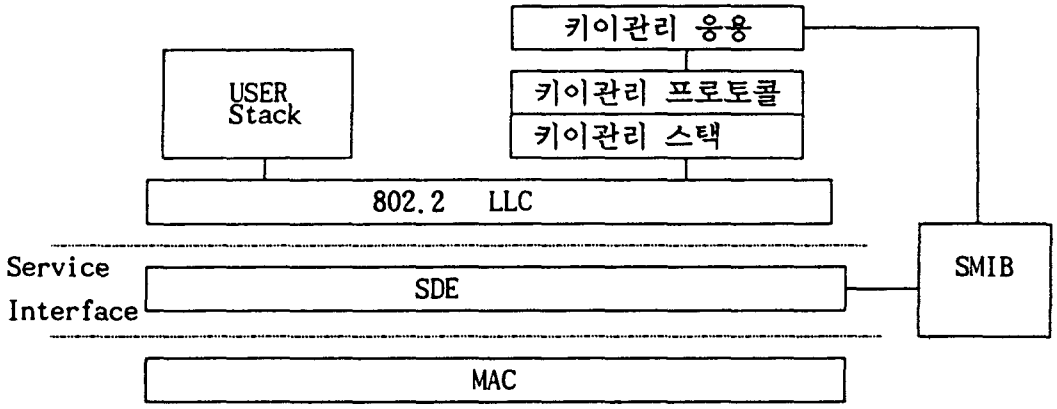


그림 2. SMIB 의 사용과 SDE 부계층의 위치

키이관리 프로토콜의 구체적인 표준화는 아직 이루어져 있지 않으며, 다음의 프로토콜 함수들(functions)이 정의 된다. 즉 문자들의 조합인 키이를 만들어내는 키이 생성(generation), 키이를 사용할 실체(entity) 에게 해당 키이를 전달하는 분배(distribution), 현재의 키이나 과거의 키이를 사용하여 새로운 키이를 생성하기 위하여 준비하는 변경(update), 키이 분배를 위하여 키이를 적절한 형태로 변형시키는 변환(translation), 나중에 키이 생성과 분배에 따른 여러 사항들(키이 내용, 시간, 전송)에 대한 증명을 위하여 믿을 수 있는 제 3 자에게 키이를 등록하는 증명(notarization)함수들이다.

## 2.2 SILS SDE

정보의 송수신 과정에서 발생될 수 있는 각종 위협들, 즉 비인가자에 대한 정보 누출, 적법한 통신 상대자로 가장함, 데이타의 불법적인 변경 및 비인가자에 의한 자원의 사용 등을 막기위한 보호 서비스가 필요하다. 그래서 IEEE 802.10 의 SILS 에서는 계층 2 의 LLC 부계층과 MAC 부계층 사이에 SDE 부계층을 두어 위의 보호 서비스를 제공하고 있다. 그림 2 는 SILS 에서 보호 서비스를 제공하는 SDE 부계층의 위치를 보여주고 있다. SDE 부계층에서 제공되는 보호 서비스와 그 제공방법을 요약하면 다음과 같다.

데이타 비밀성(data confidentiality) 은 불법적인 노출로부터 정보를 보호하는 보

호 서비스이며 LLC PDU를 암호화 하는 것으로 제공되며, 여기에 필요한 암호화 키이 생성과 암호화 알고리듬의 종류 선택은 키이관리에서 결정된다.

비연결형 데이타 무결성(connectionless integrity)는 데이타의 재사용,삽입,변경 및 삭제 등을 검출하는 보호 서비스로 무결성 확인 필드를 SDE PDU 내에 둠으로써 제공된다. 그리고 키이관리에서 확인 알고리듬을 선택한다.

데이타 발신처 신분 확인 (data origin authentication) 은 전송된 데이타의 발신처를 인증하기위한 보호 서비스이며 SDE PDU 내의 보호 헤드인 Station ID 필드를 이용하여 제공된다.

엑세스 제어(access control) 는 자원의 불법적인 사용을 막기위한 보호 서비스이며 SDE 부계층이 SMIB 와 상호 연관하여 제공한다.

SDE 부계층은 단일 형식의 PDU를 사용하며 그 구조는 그림 3 과 같다.

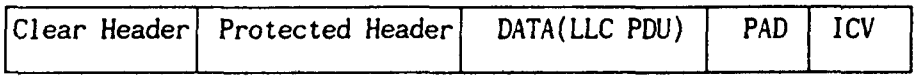


그림 3. SDE PDU 의 구조

본 상호 신분 인증기능을 가진 키이 분배 프로토콜을 LAN 시스템의 SILS 에 적용하기 위해서는 SDE PDU 의 Clear Header 부분의 SDE_표시기 안전성 서비스를 위하여 예약된 DSAP로 채우고 SAID 에는 모두 0 으로 채우면 된다. 여기에 필요한 프로토콜의 프리미티브 함수들은 다음과 같다.

```
Key_gen(DSAP,SSAP)  /* 키이 분배를 위한 프로토콜 call */
{
  random_gen(k)  /* 랜덤 수 K 를 구하는 함수 */
  mult_mod(a,b,c)   /* c = a*b mod p-1 계산 함수 */
  expo_mod(a,b,c)  /*  c = a^b  mod p 연산 함수  */
  H = h(a)          /* H = h(a) : h 는 해쉬함수  */
  comp(H1,H2,c)     /* H1 = H2 면 c = 1 이고, 아니면 c = 0 (비교 함수) */
}
```

3. 키이 분배 시스템

인증과 키이 생성이 동시에 이루어 지는 프로토콜에서도 계산량이 적고, 상호 교환되는 정보량이 적고 그리고 통신 횟수가 적을수록 바람직하다.

Bauspieβ등[4]의 방식은 영지식 증명을 이용하여 신분 인증과 키이 분배를 동시에 수행하는 키이 분배 방식인데, 영지식 증명의 이용으로 상대적으로 안전도는 높으나 이를 위해 많은 통신 횟수가 요구되어 컴퓨터 통신망에는 적합지 않다[7]. 그리고 Gunter 등[8]의 방식은 D-H 형태의 인증 기능을 가진 키이 분배 프로토콜인데, 통신 횟수는 적으나 상대적으로 계산량은 많은 편이다.

본 장에서는 D-H 형태의 키이 분배 방식을 이용하여 신분 인증과 키이 생성을 동시에 수행하는 프로토콜을 제안한다. 제안된 방식에서는 3-way 통신으로 신분 인증과 키이 분배가 모두 이루어지고, 2 번의 멱승을 필요로 하므로 계산량이 적다. 여기서 제안하는 상호 신분 인증 기능을 가진 키이 분배 시스템은 적법한 비밀키이의 소유자만이 상호 통신의 결과로 생성된 키이 값을 정확히 알 수 있다는 사실을 바탕으로 한다. 두 통신자 A 와 B 사이의 상호 신분 인증 기능을 가진 안전한 키이 생성과정은 다음과 같다.

먼저 통신망의 각 가입자들의 공개키이는 다음과 같이 준비한다.

두 통신자 A 와 B는 각각 비밀키이 $X_A$ 와 $X_B$, $1 < X_A, X_B < p-1$ 를 발생하고 $Y_A$ 와 $Y_B$ 를 공개한다. 여기서 $Y_A = \alpha^{-X_A} \bmod p$ 이고 $Y_B = \alpha^{-X_B} \bmod p$ 이다.

첫째 : 통신자 A 는 랜덤수 $K_A$ , $1 < k_A < P-1$, 를 선택하여

$V_A = Y_B^{K_A} = \alpha^{K_A \cdot X_B^{-1}} \bmod p$ 를 계산하여 상대자 B 에게 전송 한다.

둘째 : 통신자 B 도 랜덤수 $K_B$, $1 < K_B < P-1$, 를 선택하여

$V_B = Y_A^{K_B} = \alpha^{K_B \cdot X_A^{-1}} \bmod p$ 를 계산하고, A 로부터 수신한 $V_A$ 로부터

세션키이 $Z_B = R_B^{X_B \cdot K_B} = \alpha^{K_A \cdot K_B} \bmod p$ 를 얻는다.

셋째 : B 는 서명 시스템의 challenge 값에 해당하는 $V_A$ 를 $Z_B$ 와 함께 해쉬함수에 입력하여 $H_{B1} = h(Z_B, V_A)$ 를 구하여 A 에게 전송한다.

네째 : 통신자 A 도 둘째 과정의 B와 같이 세션키이 $Z_A = \alpha^{K_B \cdot K_A} \bmod p$ 얻는다.

$H_{A1} = h(Z_{AB}, V_A)$ 를 구하여 $H_{A1} \equiv H_{B1}$ 인가를 검사한다. 만약 같으면 B 를 인

증하고, 자신을 확인 시키기 위하여 $H_{A2} = h(Z_A, V_B)$ 를 구하여 B 에게 전송한다. 같지 않으면 통신을 중단한다.

다섯째 : B 는 A 인증용 $H_{B2} = h(Z_B, V_B)$ 를 구하여 $H_{A2} \equiv H_{B2}$ 이면 A 를 인증한다.

다음 그림 4 은 위의 프로토콜을 도시한 것이다.

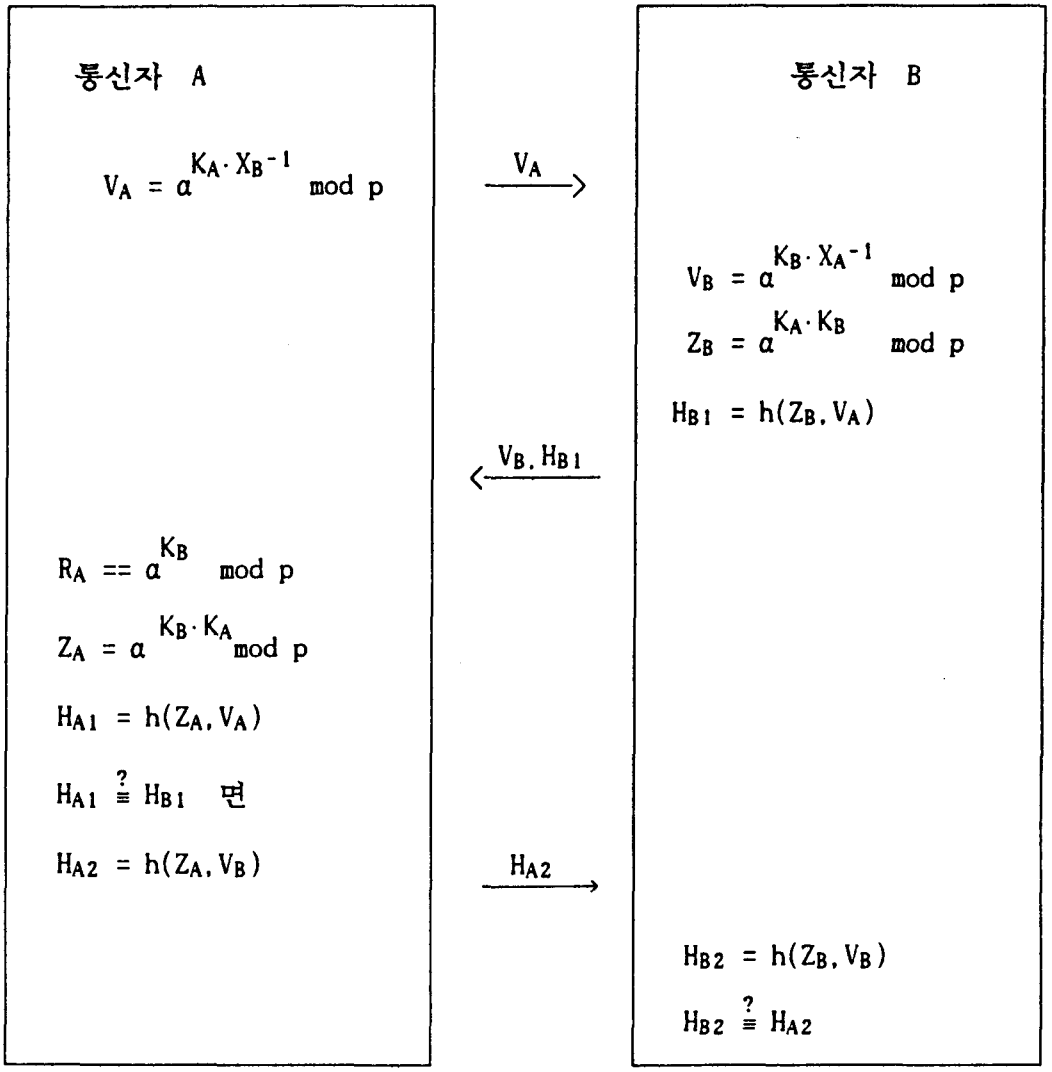


그림 4. D-H 형태의 상호 신분 인증을 가진 키이 분배 프로토콜

그림 4 의 프로토콜을 살펴보면 공개 전송정보 $V_A$ 및 $V_B$ 로부터 $K_A$ 와 $K_B$ 를 계산하는 것은 원래의 이산대수 문제를 푸는 것만큼이나 어려우며, $V_A(V_B)$ 로부터 $\alpha^{K_A}$( $\alpha^{K_B}$) 를 계산하는 문제도 이산대수 문제이다. 그리고 해쉬함수 h 는 일방성함수이므로

H 값으로부터는 어떤 정보도 얻지 못한다. A 를 가장한 공격자 C 가 랜덤 수 $K_A'$ 를 발생시켜 $V_A = \alpha^{K_A' \cdot X_B^{-1}} \bmod p$ 를 B 에게 전송하더라도 $X_A$ 를 알지 못하면 $V_B$ 로부터 $\alpha^{K_B} \bmod p$ 의 계산은 어렵다. 위의 이유들과 함께 세션키이 $Z_A(Z_B)$ 는 전적으로 해당 세션의 랜덤 수에만 의존하므로 impersonation attack 은 불가능하다. 또한 어떤 방법으로든 과거의 $Z_A'(Z_B')$를 알았다해도 공개정보와 해당 전송정보Z' 와 V' 로부터 현재의 세션키이를 계산해 낼 수 있는 정보는 없다.

위와 같은 이유로 생성된 키이 $Z_A$ 와 $Z_B$ 는 적법한 통신자 A 와 B 만이 얻을 수 있고, $H_{A1}$ 과 $H_{B1}$을 적법 통신자 A 와 B 이외에는 생성하지 못한다. 따라서 제 3 자가 $H_{A1}$ 이나 $H_{B1}$을 추측하여 알지 못하는 한 신분 확인과정을 통과하지 못한다.

위의 프로토콜을 수행하는 데에는 2 번의 멱승과 2 번의 해쉬함수 연산만이 필요하다. 그리고 일반적으로 디지틀 서명법을 이용한 위와같은 프로토콜에서는 키이관리센타도 생성된 키이를 알 수 있으나 여기서는 불가능하다.

## 4. 결 론

본 연구에서는 LAN에서의 보호 서비스를 규정하고 있는 IEEE 802.10 를 살펴보고 이에 적용할 수 있는 신분 인증 기능을 가진 키이 분배 시스템을 제안하였다. 제안된 키이 분배 방식은 LAN 과 같은 통신망에 적합한 방식이다. 이 프로토콜은 3-way 통신으로 수행되며, 계산량에서도 멱승이 2번으로 적다. 그리고 키이 분배 단계에서부터 상대자의 신분 확인이 가능하므로 미연에 각종 위협을 방지할 수 있어 여러 경우에 활용될 수 있다.

## 참고 문헌

1. M.E.Hellman, "An Overview of Public Key Cryptography," IEEE Comm. Society Mag., Vol.16, No.6, pp.24-32, Nov. 1978.

2. D.B.Newman Jr., J.K.Omura, and R.L.Pickholtz, "Public-Key manage- ment for Network Security," IEEE Network Mag., Vol.1, No.2, pp.11-16, Apr. 1987.
3. Henk C.A. van Tilborg, *An Introduction to Cryptology*, Boston, Kluwer Academic Publishers, Chap.6-7, 1987.
4. F.Bauspieβ and H.J.Knobloch,"How to Keep Authenticity Alive in a Compuer Network," Eurocrypt'89, pp.38-46, 1989.
5. IEEE 802.10, *Standard for interoperable Local Area Network (LAN) Security (SILS)*, P802.10/D6, Sep. 1989.
6. W.Diffie and M.E.Hellman,"New Directions in Cryptography," IEEE Trans. Inform. Theory, IT-22, pp.644-654, 1976.
7. Y.Yacobi and Z.Schmuely,"On Key Distributions," Crypto'89, pp.335-346, 1989.
8. C.G.Gunter,"An Identity-based Key-exchange Protocol," Eurocrypto'89, pp.29-37, 1989.