論 文

Time Quantum을 이용한 LAN에서의 암호화 키이 분배방식

正會員 柳 煌 彬* 正會員 李 載 廣**

An Encryption Key Distribution System in LAN Environment Using Time Quantum

Howang Bin Ryou* Jae Gwang Lee** *Regular Members*

요 약

본 논문에서는 근거리 통신망에서의 정보보호 취약성, 요구 서비스, 정보보호 적용대안에 대하여 정리하고, 근거리 통신망에 적합한 새로운 키이 분배 방식을 제안하였다. 제안된 방식은 Time Quantum을 암호화 키이에 적용하여 암호화 키이 사용시간과 키이를 이용한 암호화 메세지 양을 제한하였다. 제안된 방식은 키이 concurrency와 상대방에 대한 인증을 더욱 확실하게 할 수 있으며, 프레임 단위 도청으로 인하여 암호화 키이 노출이 발생하더라도 전체 전송 메세지의 내용을 알 수 없으므로 정보보호 및 안정성을 더욱 강화하는 특징을 갖도록 하였다.

Abstract

This paper examines the security vulnerability, demanded service, layering consideration for local area networks(LANs), and proposes a new key distribution system suitable to local area networks. The new key distribution system is applicable to time quantum in encryption key and then the time used and the quantity of encryption message using the encryption key are limited. A system suggested in this paper can achive some higher concurrency of key and authentication of the opposite party. Even through a encryption key expose by reason of wiretapping of a frame unit, It has achived some more security and safety, because the contents of all traffic messages are not known.

I. 서 론

컴퓨터 보급의 확산과 정보통신 기술의 발달로 인하여 컴퓨터 자원의 이용도와 컴퓨터 시스템의 신뢰도를 높이기 위해 전송 매체를 이용한 컴퓨터 통신망을 구성하여 많은 사용자들이 사용하고 있으며, 이용 추세가 날로 증가하고 있다. 또, 각종 정보를 대용량 정보 매체에 저장하여 통신망을 통한 검색 서비스를 가능하게 하는 등 각종 부가 통신 서비스가 출현하게 됨으로써 컴퓨터 통신망을 통한 정보 교환이 일반화되어가고 있다. 이와 같이 각종 정보가 컴퓨터 통신

*光云大學校 電子計算學科
Dept. of Computer Science, Kwangwoon Univ.
**群山實業專門大學 電子計算科
論文番號 : 92-64(接受1992. 3. 16)

망을 통하여 전송됨에 따라 정보를 공동으로 이용한다는 긍정적인 면도 있지만 정보의 관리면에서 권한을 가지지 않은자에게 정보의 누출, 불법 변경, 파괴, 개인의 프라이버시 침해나 컴퓨터 바이러스와 같은 위험이 정보화 사회의 발전에 중대한 장해 요인으로 대두되고 있다.[1]

정보 시스템에서 처리, 축적, 전송되는 정보에 대한 보호를 위해서는 컴퓨터 통신망등 정보 시스템 전반에 대한 물리적인 안전 대책뿐만 아니라 교육, 법, 제도 면의 대책 등을 통하여 인적 및 정보 자원의 관리에 대한 정보 보호 확립은 중요한 과제라고 할 수 있다. 이 가운데 가장 경제적이면서, 보안 수준에 따라 정보 보호 대책을 제공할 수 있는 방법이 암호법(cryptoyraphy)으로서 이를 연구하는 암호학이 현대의 중요한 학문 분야의 하나로 자리잡게 되었다.

컴퓨터 통신망중에서 이용자가 날로 증가하고 있는 LAN 환경에서도 정보의 내용 변경, 정보의 불법적 유출, 순서변경, 미확인 수신자 및 발신자등의 위협을 내포하고 있기 때문에 정보 보호의 필요성이 증가하고 있다.[10] 이에 따라 IEEE에서는 1988년 봄에 개최된 예비 회의에서 표준화 작업을 추진키로 하였다. 그리고 "IEEE 802 Technical committee"와 "IEEE technical committee on security and privacy"의 후원하에 802.10(Security working Group)을 구성하여 LAN에서의 정보 보호를 위한 프로토콜 작성 작업을 시작하게 되었다. IEEE 802.10에서 적용하고 있는 표준안인 SILS(Standard for Interoperable LAN Security)는 LAN 환경에서의 정보 보호를 위한 프로토콜로서 SILS 모델, 데이타의 안전한 교환을 위한 프로토콜, 키이 관리 프로토콜, 시스템/정보 보호 관리 프로토콜등 4분야로 구분하여 진행 중에 있다.[8]

근거리 통신망은 물리층에서 전송매체는 공통으로 이용하며 LLC에서 PDU(Protocol Data Unit)(즉, 패킷, 프레임)전송을 방송(Broadcasting)형태로 행해진다. 따라서 어떤 국이든 PDU의 액세스가 가능하므로 정보보호가 취약하다.

근거리 통신망에서의 정보보호는 논리적으로 peer entity간에 오가는 PDU에 행해지는 공격(attack)에 대해 필요하다. PDU에 대한 공격에는 PDU를 관찰하여 그 내용을 알아내려는 수동적(passive) 공격과 PDU에 대한 처리(PDU수정, 전송 순서 변경, 가짜 PDU 삽입 등)를 행하는 능동적(active)공격이 있다.

이러한 공격에 대한 정보보호를 위해서는 암호 알고리즘을 이용한 키이 관리 프로토콜이 필요한데 SILS에서는 사용자의 요구를 충족시키고 제한 사항을 최소화하기 위해 암호화 및 키이 관리 알고리즘을 독립적으로 동작할 수 있도록 개발 중에 있다. 하지만 현재까지는 구체적인 작업활동의 결과가 없는 상태이다. 키이 관리 기능은 키이 생성, 분배, 저장 및 폐기로 구분할 수 있는데 키이를 이용한 암호법은 키이의 비밀성(secrecy)과 인증성(Authenticity)을 기초로 한다. 이를 위해 암호화 키이를 안전하게 분배하는 것은 중요하다. 근거리 통신망에 적합한 키이 분배 전략은 중앙 집중형 키이 제어이다.[4] 중앙집중형 키이 분배 방식에는 Needham과 Schroeder가 제안한 방식이 있다.[2] 이 방식은 키이 교환 후에 Handshake 절차를 수행해야 하며 키이 concurrency을 달성하기 어렵다. 또 과거의 세션 키이를 알고 있는 제3자가 사용자로 가장하여 분배 절차를 따르면 언제나 깨어질 수 있는 단점을 가지고 있다. 이를 개선하기 위해 Denning과 Sacco에 의해 time stamp를 사용한 방법이 제안되었다.[3] 이 방법은 사용자의 부주의 등에 의해 과거의 세션 키이가 노출된다 하더라도 현재의 세션에서 재전송 공격을 막을 수 있으나, 지리적으로 떨어진 두 시스템간의 시스템 클럭의 차이를 점검하는 것이 거의 불가능한 문제점을 가지고 있다.

본 논문에서는 근거리 통신망에서의 정보보호 취약성, 요구 서비스, 정보보호 적용 대안에 대하여 기술하였다. 또 기존의 키이 분배 방식을 개선하고, 근거리 통신망에 적합한 새로운 키이 분배 방식을 제안하고 타 방식과의 차이점을 연구하였다. 제안된 방식은 근거리 통신망에서의 기본 전송 단위인 PDU(패킷, 프레임)의 도청이나 엿듣기를 통하여 암호화 키이나 PDU의 노출이 발생하더라도 전체 전송 메세지의 내용을 알 수 없게 되어 있어 정보 보호 및 안전성을 더욱 강화하는 특징을 가지고 있다.

Ⅱ. LAN에서의 정보 보호 서비스와 대안

1. LAN 프로토콜콜에서의 정보 보호 취약성과 요구 서비스

컴퓨터 통신망의 모델로서 ISO 7498 OSI 기본 참조 모델은 통신 프로세스의 기능을 7계층으로 구분하여 각 계층은 고유의 통신 서비스를 제공하는 것으로

정의하고 있다.[6] 이 모델에서 각 entity가 다루는 정보형태는 PDU(Protocol Data Unit)이다. PDU는 각 계층의 PCI와 데이타 부분으로 되어 있으며 각 계층의 데이타 부분은 상위 계층의 PDU와 같다. 이의 관계는 그림 1.과 같다.

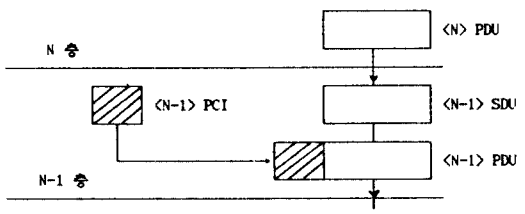

그림 1. SDU와 PDU
Fig 1. SDU and PDU

ISO 정보보호 구조는 ISO 7498을 근거로 한 ISO 7498-2가 작성되었다.[7] 이 구조는 기본 정보보호 서비스로 액세스 제어 (access control), 인증(authentication), 데이타 기밀보호(data confidentiality), 데이타 무결성(data integrity), 부인봉쇄(non-repudiation)를 제공하는데 근거리 통신망에서는 부인봉쇄를 제외한 나머지 서비스가 데이타 링크 계층에서 제공되어야 한다. 데이타 링크 계층에서 제공하는 서비스는 WAN과 LAN이 유사하나 LAN은 그 특성상 다른 속성을 가지고 있다. WAN의 경우 데이타 링크 계층에서 링크간에 점 대 점(point-to-point) 패킷 교환이 이루어지고 데이타의 방송(Broadcasting) 기능은 네트워크 계층에서 이루어 지는데 반해, LAN에서는 데이타 링크 계층에서 방송 기능을 수행한다.

즉, LAN에서는 어떤 한 국에서 주소 기능을 이용하여 다른 국으로 PDU를 전송할 수 있으므로 권한을 가지지 않는 자의 자원의 불법 이용이나 정당한 사용자로의 위장등의 위협이 발생할 수 있다. 또, 모든 국들은 임의의 국에서 전송되는 모든 데이타를 액새스하는 것이 가능하므로 권한을 가지지 않은 자가 데이타를 변조할 수 있다. 주소 공간의 경우 WAN에서는 데이타 링크 계층의 주소를 국부적으로 지정 및 관리가 가능하나 LAN에서는 계층 2에서 유일한 주소를 가져야 하고 이 주소가 정당한지 여부를 구별하기 어려우므로 권하을 가지지 않은자의 자원 이용이나 정당한 사용자로의 위장 등이 가능하게 된다.

또, LAN에서는 기기들이 지리적으로 분산되어 있으므로 도청이나 Wiretapping등에 취약하여 권한을 가지지 않은 자에 의한 데이타 변조등의 위협이 발생한다. 이러한 Wiretap는 근거리 통신망 구성상 전체국에 위협을 끼치게 된다. 따라서, LAN에서의 정보보호 서비스를 제공하기 위해서는 먼저 LAN 특성에 맞는 정보 보호 프로토콜이 필요하다. LAN 환경에서 일어날 수 있는 위협 형태에는 데이타 변조, 정당

표 1. 근거리 통신망 정보 보호 위협 및 요구서비스
Table 1. a security threat & a demand service in LAN

LAN 속성	약 점	위 협	요구 서비스
데이타송신	어느 국이든 주소를 이용하여 다른 국에 정보 송신 가능	정당한 사용자를 가장, 권한을 가지지 않은 자의 자원 이용	데이타 발신처 인증 액세스 제어
데이타수신	어느 국이나 모든 정보 전소엥 대한 액세스 가능	데이타 변경, 권한을 가지지 않은자에게 정보 누출	무연결 데이타 무결성, 데이타 기밀보호
주소공간	주소관리를 이용한 명확한 제어가 안됨	정당한 통신상대로 가장, 권한을 가지지 않은자의 자원 이용	데이타 발신처 인증, 액세스 제어
지리적 분산	엿듣기,도청	데이타 변경, 권한을 가지지 않은 자에게 정보 누출	무연결 데이타 무결성, 데이타 기밀 보호

한 사용자로의 가장, 권한을 가지지 않은 자에 의한 정보 자원 액세스, 권한을 가지지 않은 자에게의 정보의 노출등이 있다. 이러한 공격이나 위협중에서 데이타 변조를 보호하기 위해서는 데이타 무결성 서비스가 필요하고 정당한 사용자로의 가장을 막기 위해서는 데이타 발신처에 대한 인증 서비스가 필요하다. 또, 권한을 가지지 않은자에 의한 정보 자원 사용을 막기 위해서는 액세스 제어 서비스가 요구되며, 데이타의 노출이나 도청등을 막기 위해서는 데이타에 대한 기밀 보호 서비스가 필요하다. 이를 요약하면 표 1.과 같다.

위 표에서 기술한 정보 보호 서비스들은 암호화 기술에 의해 제공될 수 있다. 즉, 기밀보호 서비스를 제공하기 위한 방법은 전송되는 데이타를 암호 알고리즘을 이용하여 암호화함으로서 데이타의 노출을 방지할 수 있으며, 무결성 서비스는 기밀보호를 위한 암호화 결과로서 실현될 수 있으며, 전송되는 데이타에 대한 암호화 검사(cryptographic checksum)에 의해 무결성 서비스가 가능하다. 발신처 인증 서비스는 송신자 주소의 복사본을 계층 2의 SDU의 Prefix 또는 Suffix로써 암호화된 데이타 영역에 포함시킴으로써 제공될 수 있다. 액세스 제어 서비스는 암호화 키이와 같은 암호화 연관(cryptographic Association)의 관리 및 응용을 통해 가능하다. 즉, 전송되는 PDU(프레임, 패킷)가 암호화되면 암호법과 암호화 키이를 알고 있는 국만이 정확한 데이타의 수신이 가능하지만 이러한 기능을 가지지 않은 국들은 보호되는 자원들을 액세스할 수 없게 된다. 이것은 하나의 채널을 모든 사용자가 공동으로 이용하는 LAN환경에서의 정보 보호 서비스를 제공하는데 있어 중요한 문제이다.

2. LAN 프로토콜에서의 정보 보호 대안

LAN 표준(IEEE 802)에서 MAC 프로토콜(IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.6)은 4가지의 서로 다른 물리적인 매체에 대한 표준 액세스를 제공하고 있으며, LCC는 데이타 링크 계층의 상위 서브 계층에서 매체 액세스 방법들에 대해 공통이다. 이 프로토콜들은 OSI 기본 참조 모델의 계층 1과 계층 2에 해당된다. 여기서 정보 보호 프로토콜의 적용 가능성을 살펴보면 그림 2.과 같다.

그림 2.에서 정보 보호 프로토콜 적용 가능성은 크게 두가지로 나눌 수 있는데 첫째는 기존 프로토콜에 정보 보호 프로토콜을 직접화시키는 것이다.(그림 2.의 ①과 ③) 이때는 기존 프로토콜의 모든 정보의 액세스가 가능하지만 기존 프로토콜을 수정해야 하는

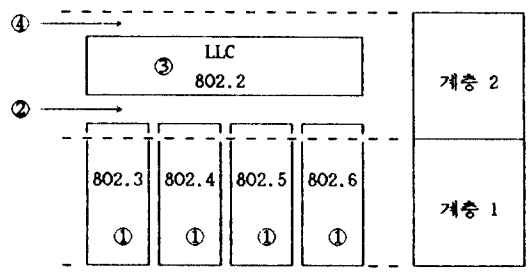

그림 2. LAN 환경에서의 정보 보호 프로토콜 적용 대안
Fig 2. Alternatives for the placement of LAN security protocol

어려움이 있다. 둘째는 계층 사이에 정보 보호 프로토콜을 적용하는 것이다.(그림 2.의 ②와④) 이때는 지정된 서비스 프리미티브와 연관된 프로토콜 제어 정보만을 액세스하면 된다.

IEEE 802.10 SILS에서는 LCC와 MAC사이(그림 2.의②)에 SDE(Secure Data Exchange)정보 보호 프로토콜을 적용하고 있다. SDE가 정보 보호 서비스를 제공하기 위해서는 키이 관리 프로토콜이 필요하다. 키이 관리 응용과 SDE간의 통신 경로로서 SMIB를 이용한다. 즉, 계층 및 시스템 관리를 위해 각 프로토콜에서 타이머, 버퍼크기, 윈도우 크기등 관리되는 객체(object) 정보를 정의하여 이 정보들을 관리 정보 베이스(MIB:Management Information Base)에 저장하여 사용한다. 특히 정보 보호 서비스를 위해 사용되는 객체는 권한을 가지지 않은자에게 노출되지 않도록 별도로 관리할 필요가 있으므로 정보보호 관리정보베이스(SMIB:Security MIB)를 정의하여 사용한다. 이의 구조를 보면 그림 3.와 같다.

그림 3.에서 데이타 교환 사용자 스택은 정보 보호 서비스를 제공하기 이전의 사용자간의 데이타 교환 규약 집합이다. SMIB와 SDE의 관계는 SDE에서 정보 보호 서비스를 제공할 때 키이 관리 응용을 통하여 분배받은 키이를 SMIB가 SDE에 제공하게 된다. 이 정보에 의해 사용자간의 데이타 교환시에 제공되는 정보보호 서비스가 영향을 받는다.

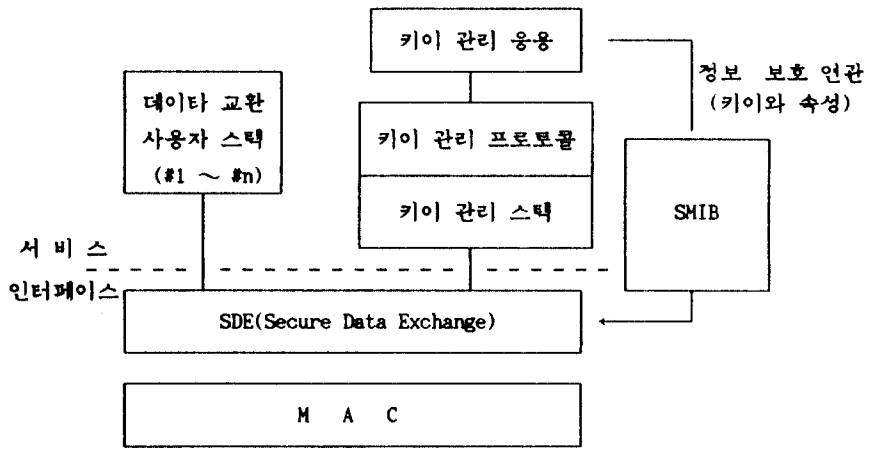

그림 3. SDU와 SMIB 구조
Fig 3. structure of a SDE and a SMIB

Ⅲ. 암호화 키이 분배 방식

1. 암호화 키이 관리 전략

정보 보호 서비스 제공을 위한 암호시스템에서 암호 알고리즘 자체는 공개되는 것이 일반적이므로 암호시스템의 안정성은 암호화 키이 비밀유지에 결정된다. 따라서 암호화 키이의 안전한 관리 전략은 아주 중요하며 다음과 같은 방식이 있다.[4]

1.1 중앙집중형(centralized) 키이 관리 방식

구축된 통신망 가운데 하나의 KDC(Key Distribution Center)를 두어, n명의 사용자가 있을 경우에 미리 n개의 비밀 키이를 KDC에 등록하여 두고, 이후에 비밀통신을 위해 사용되는 세션 키이는 사용자와 KDC만 알고 있는 비밀 키이로 암호화하여 분배하는 방식이다. 상대방에 대한 인증은 KDC와 사용자 자신만이 비밀 키이를 알고 있기 때문에 KDC가 보증한다. 이 방법은 KDC가 정지되거나 통신 회선에 이상이 있을 경우 더 이상의 키이 서비스를 받을 수 없고 비밀 통신을 위한 키이 요구가 빈번할 때는 KDC가 통신망에서의 성능 장애 요인이 될 수 있다.

1.2 완전 분산형(Fully Distributed) 키이 관리 방식

이 방법은 통신망에서 각 노드가 KDC의 역할을 수행하는 방법이다. 따라서 각 노드의 사용자는 다른 노드의 사용자들의 키이를 사전에 가지고 있어야 한다. 이 방법은 n명의 사용자가 있을 경우, 각 사용자는 서로 다른 각 사용자와 통신을 하기 위해n(n-1)/2회의 키이 교환이 필요하다.

1.3 계층형(Hierarchical) 키이 관리 방식

이 방법은 키이 분배 기능을 local, region 및 global로 분할하는 경우이다. 즉, Local은 자기 영역내의 KDC 역할을 수행하고 region은 모든 local의 KDC 역할을 수행하며 gobal는 모든 region의 KDC 역할을 수행한다. 예를 들어 사용자 A, B가 지리적으로 멀리 떨어져 있어서 A, B가 같은 KDC에 등록할 수 없을때 A, B는 각각의 KDC을 가지기 때문에 A, B가 통신을 위해서는 먼저 A, B의 KDC간에 암호화 키이 교환이 이루어져야 된다. 이후 A, B는 자기 KDC에 의해 암호화 키이를 받아 통신을 수행하는 방법이다.

암호화 키이 관리는 키이 생성, 분배, 저장 및 폐기로 나누어 생각할 수 있는데, 이 중 가장 중요한 것은 통신하고자 하는 상대방에게 안전하게 키이를 분배하는 문제이다. 암호화 키이를 안전하게 분배하기 위한 방법은 데이타를 보호하기 위하여 사용되는 암호 알고리즘으로 암호화하여 분배하는 방법이 사용된다.

근거리 통신망 구조에는 스타형, 링형 그리고 버스형이 있는데 스타형은 네트워크 제어 기능이 중심노드 또는 교환기를 통하여 수행된다. 따라서 중심노드에

서 다른 모든 노드들 까지, 노드들간의 모든 네트워크 메세지 통화의 경로가 중심노드에 의해서 수행된다. 링형 네트워크는 메세지가 순환구성된 링을 노드 단위로 이동될 때 RIU가 주소를 비교, 정보를 수신한다. 순환형태의 점 대 점(point-to-point) 선로구조에서 노드들 가운데 제어 노드가 네트워크 제어를 엑세스할 수 있도록 되어있어 제어노드가 메세지 전송을 허용해야만 전송이 가능하다. 버스형 구조에서도 제어노드에 의한 네트워크 제어를 수행한다. 네트워크 시스템 관리면에서는 CSMA/CD방식의 SMAE (System Management Application Entity)를 통한 계층 운영이나 토큰 방식의 SM(System Manager)을 통한 시스템 운영에서 각 스테이션의 관리는 서버 스테이션이 담당한다. 따라서 LAN 환경에 적합한 키이 분배 방식으로는 키이 분배 센터(KDC) 의한 중앙집중형 키이 관리 방식이 가장 바람직하다.

2. Needham과 Schroeder에 의한 키이 분배 방식

중앙집중형 키이 분배 전략을 근간으로 하여 사용자간의 인증을 제 삼자인 인증서버(AS:Authentication Server)가 보증하는 방식이다. 단일 키이 시스템(관용키이)으로서 초기 상태는 사용자 A, B가 비밀 키이(TK:Terminal Key)를 하나씩 비밀리에 등록해야 한다. 그리고 나서 A, B간에 정보 보호 통신을 하기 위해서 AS로 부터 세션 키이(SK:Session Key)를 분배 받는다. 분배 순서는 다음과 같다.

순서 1) A→AS : A, B, I_A

먼저 사용자 A는 AS에게 B와의 정보 보호 통신을 요청한다. 이 I_A는 A가 AS와의 통신에서 이전의 통신이 아님을 확인하기 위해 추가한 확인 정보이다.

순서 2) AS→A : $\{I_A, B, SK, \{SK, A\}^{TKB}\}^{TKA}$

AS는 A로부터의 정보 보호 통신 요구에 따라 사용자 A, B의 터미널 키이(TK)를 확인하고 A, B간에 사용할 세션(SK) 키이를 생성시켜 A에게 보낸다. 이때 A는 수신된 내용을 자신 TK로 복호화 한다. 여기서 A는 각 사용자의 모든 TK를 AS만이 가지고 있으므로 A의 비밀 키이로 암호화된 메세지는 AS만이 생성할 수 있다는 사실로 부터 AS의 인증을 얻을 수 있다. 여기서 I_A는 A에 의해 선택된 random vector이며 AS로 부터 되돌아온 I_A를 자신이 간직하고 있는 I_A와 비교하여 이전에 통신의 응답이 아님을 확인한다(키이의 concurrency 확인). 그리고 B의 TK로 암호화된 부분을 B에게 보낸다.

순서 3) A→B : $\{SK, A\}^{TKB}$

사용자 B는 수신된 메세지를 자신의 비밀 키이인 TK로 복호화하여 통신 상대자는 A이며, 이때 사용되는 세션 키이는 SK임을 확인한다. 이제부터 사용자 A, B는 세션키이를 이용하여 정보 보호 통신을 할 수 있다.

그러나 순서 3)까지 수행 후에 A는 SK가 I_A의 비교에 의해 안전하게 사용할 수 있는 키이임을 확신한다. 그러나 B는 A에게서 자신의 비밀 키이인 TK_B로 암호화된 메세지를 받았기 때문에 AS가 그 메세지를 생성했음을 알 수 있으나 이것이 이전에 A가 B에게 보낸 메세지에 대한 반복이 아니라는 것을 확신할 수 없다. 이를 확인하기 위해서 다음의 handshake절차를 수행한다.

순서 4) B→A : $\{I_B\}^{SK}$

순서 5) A→B : $\{I_B-1\}^{SK}$

먼저 B는 자신이 생성한 random vector I_B를 SK로 암호화하여 A에게 보낸다. 사용자 A는 수신된 내용을 자신의 SK로 복호화하여 I_B값을 1 감소시켜 SK로 암호화 하여 B에게 보낸다. B는 자신의 SK로 복호화하여 자신이 보호하고 있는 I_B의 값보다 1 적은지를 확인한다. 맞으면 제삼자의 개입이 없이 통신 상대자가 정확하게 A임을 확신한다.

이 분배 방식은 AS에게 다수의 사용자가 동시에 SK를 요구할 때는 시스템 성능에 영향을 줄 수 있다. 또 n명의 사용자가 있을 때에는 n개의 unique한 handshake function은 $n(n-1)/2$회에 걸쳐서 비밀리 교환되어져야 한다는 어려움이 있다.

3. Denning과 Sacco에 의한 키이 분배 방식

Needham과 Schroeder에 의해 제안한 방식의 handshake 문제점을 Time stamp를 이용하여 이 절차를 없애고, 또 키이의 concurrency도 얻을 수 있다고 하였다. Time stamp를 이용한 암호화 키이 분배 방식 순서는 다음과 같다.

순서 1) A→AS : A, B

사용자 A는 AS에게 자신의 주소와 통신 상대 B송신한다.

순서 2) AS→A : $\{B, SK, T, Y\}^{KA}$, $Y=\{A, SK, T\}^{KB}$

AS는 사용자 A, B의 키이를 찾아서 세션 키이를 생성하여 Time Stamp T와 함께 A에게 보낸다.

순서 3) A→B : $Y=\{A, SK, T\}^{KB}$

이제 사용자 A는 B는 Time stamp T를 수신하였다. 이때 Time stamp T를 다음 식에 적용시켜 만족할 경우 키이 Concurrency를 확인한다.

$$|Clock - T| < \triangle t1 + \triangle t2 \quad (1)$$

여기서 T : AS에 의한 Time stamp
Clock : A와 B의 시스템 시간(local Clock)
△t1 : A~AS, B~AS간의 시스템 시간의 차이
△t2 : 예상 지연 시간

그러나 (1)식은 다음의 문제점을 가지고 있다. 첫째, 지리적으로 떨어져 있는 시스템간의 시스템 시간의 차이, 즉 △t1의 측정이 불가능하다는 것이다. 둘째, △t2의 설정이 문제가 된다. 통신망에서의 전송 지연 시간은 항상 일정치 않다. 따라서 단일 통신망의 경우에도 문제가 되지만 gateway와 bridge를 이용한 통신 시스템에서는 더 큰 문제가 될 수 있다. 셋째는 시스템의 이상으로 인한 지연시간이 클 경우나 두 시스템간(A~AS, B~AS)의 시간차이가 크면 클수록 이 관계식은 항상 성립하게된다. 따라서 Time stamp를 이용한 방법도 키이의 concurrency를 보장할 수 없을 뿐만아니라 암호화 키이(SK)의 한번의 노출은 그 이후에 전송되는 메세지의 내용이 노출, 수정, 삽입될 수 있다.

Ⅳ. Time Quantum을 이용한 키이 분배 방식

1. 암호화 키이 분배 방식

근거리 통신망 시스템에서 정보 보호 서비스 제공을 위해 중앙집중형 키이 관리전략을 적용한 키이 분배 센타(KDC)를 운용한다. 먼저 키이의 인증을 위해 사용자의 키이를 KDC에 등록해야 하며 이 초기 상태는 그림 4.와 같다.

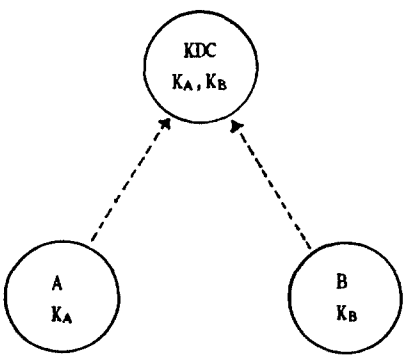

그림 4. 초기 키이 상태
Fig 4. Initial Key State

초기 키이 분배 후에 정보 보호 통신을 수행할 때에 Time Quantum을 이용한 키이 분배는 그림 5.과 같으며, 키이 분배 순서는 다음과 같다.

순서 1) A→KDC : A, $\{A, B, I_A\}^{K_A}$

먼저 A는 암호화 키이를 분배받기 위해서 자신의 주소는 평문, 그리고 자신의 주소, 통신하고자 하는 상대 주소(B), A가 발생한 random vector는 A의 비밀 키이(KA)로 암호화하여 KDC에 전송한다. A의 메세지를 수신한 KDC는 평문으로된 A의 주소를 이용하여 비밀 키이 리스트에서 A의 비밀 키이(KA)를 찾은 다음 이를 이용하여 복호화한다. 이때 평문으로 된 A와 복호화된 A가 똑같으면 KDC는 메세지의 발신자가 정확하게 A임을 알게 되어 A를 인증 하게 된다. 또, 안전한 통신 상대자가 B임을 알고 비밀 키이 리스트에서 B의 비밀 키이(KB)를 찾는다.

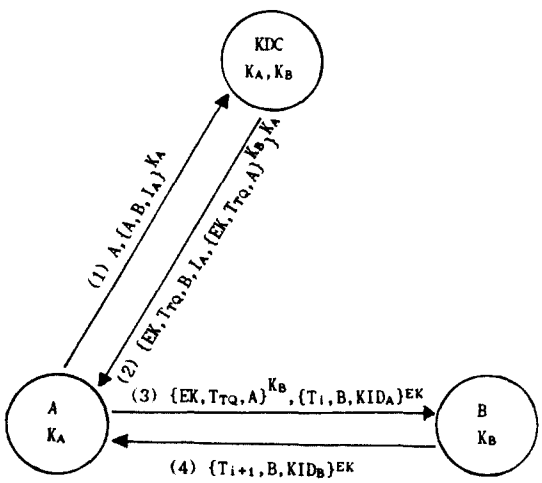

그림 5. Time Quantum을 이용한 키이 분배 방식
Fig 5. Key Distribution system using a Time Quantum

KDC는 A와 B의 비밀 키를 이용하여 메세지 송수신시 사용되는 암호화 키이(EK:Encryption Key)와 T_{TQ}(Time Quantum)를 암호화하여 보낸다. 이를 수신한 A는 KA로 복호화하여 먼저 수신된 I_A와 자신이 기억해둔 I_A와 비교하여 이전에 것이 아님을 확인(A,

KDC간 키이 concurrency)하며 암호화 키이(EK)와 사용시간(T_{TQ})을 알게 된다. 그리고 KDC에게 받은 내용과 함께 자신이 받은 암호화 키이를 이용하여 현재시간, B의 주소, A의 키이 식별자(KID:Key Identifier)를 암호화 하여 B에게 보낸다. 키이 식별자는 A가 발생한 random vector 값이다.

순서 3) A→B : $\{EK, T_{TQ}, A\}^{KB}, \{ti, B, KID_A\}^{EK}$

B는 자신의 KB를 이용하여 복호화하면 암호화 키이(EK), 키이 사용 시간(T_{TQ}), 통신을 원하는 상대(A)를 알게 됨과 동시에 이 메세지가 KDC로 부터 온 것임을 인증하게 된다(B, KDC간 키이 concurrency). 그리고 나서 EK를 이용하여 복호화하면 키이를 보낸시간, A의 키이 식별자를 알게 된다.

순서 4) B→A : $\{t_{i+1}, B, KID_B\}^{EK}$ B는 A가 보낸 시간에 1을 더한 값과 자신의 키이 식별자를 A에게 보낸다. 이를 수신한 EK를 이용하여 복호화하면 EK가 이전에 사용된 키이가 아님을 확신함과 동시에 키이 Concurrency를 보장받게 된다. 그리고 B의 키이 식별자를 알게 된다.

암호화 키이 분배가 완료되면 KDC, A, B 모두가 암호화 키이를 공유하게 된다. 그리고 A는 B의 키이 식별자, B는 A는 키이 식별자를 가지게 되며 송신시 항상 키이 식별자도 함께 보낸다. 이제 A와 B는 EK를 이용하여 메세지를 송수신하고 암, 복호화를 수행하게 된다. 이때 A는 송수신이 한번씩 수행될 때마다 시스템 시간이 다음 조건에 맞는지를 점검한다.

```
while message ≠ null
    if Clock − (Ti + TTQ) ≤ 0
      then EK를 계속 사용
      else KDC로 부터 새로운 EK를 분배 받음
end
```

즉, EK의 사용 시간 동안에는 계속 사용하고 사용 시간이 경과하면 KDC로 부터 다시 새로운 EK를 부여 받는다. 암호화 키이의 사용 시간을 사용 시간(T_{TQ})만큼으로 제한하여 이 키이를 이용하여 암호화하는 메세지의 양도 제한하는 것이다. 만약 EK의 사용시간이 경과하여 새로운 EK를 KDC로부터 분배받았을 경우에 수신측이 복호화시에 어느 EK를 사용할 것인가를 결정할 때에는 키이 식별자를 이용하면 된다.

2. 발신자 인증

키이 분배 방식에서 EK는 인증을 제공하는데 이용된다. 키이 분배가 끝나면 A, B, KDC가 EK를 알게된다. 그래서 EK로 암호화된 모든 메세지는 이 셋 중 하나이다. 그런데 KDC는 EK를 생성, 분배만 하기 때문에 EK로 암호화된 메세지는 KDC로 부터 온 것은 있을 수 없다. 즉, A 아니면 B가 EK로 암호화된 메세지를 송신하게 된다. 따라서 A는 B로 부터, B는 A로 부터 온 것임을 확인함으로써 송신 상대의 정확한 인증을 얻는다. 그런데 여기서 문제점은 발신자(A, B)가 EK로 암호화하여 보낸 메세지가 다시 발신자에게로 온 메세지를 구분해야 한다. 근거리 통신망은 통신 매체를 공통으로 이용하기 때문에 송신자가 생성한 메세지(프레임, 토큰)은 수신자가 수신한 후 송신자에게 되돌아오면 상태를 확인한 후 다른 스테이션이 전송할 수 있게 한다. 이를 위해서는 간단한 부울 플래그 비트를 이용하면 된다. A와 B간이 메세지 송신시에 A는 "1", B는 "0"로 플래그(flag) 비트를 지정하여 메세지를 보낼때 이 플래그도 함께 보낸다. 이렇게 함으로써 수신된 메세지에 대한 인증을 분명하게 할 수 있다.

3. Time Quantum 지정

근거리 통신망에서 메세지 전송은 방송(Broadcasting) 형태이기 때문에 어떤 스테이션이든지 전송되는 모든 메세지를 도청할 수 있다. 그리고 지금까지 이용된 키이 분배 방식에서 분배된 키이는 송신자가 보내고자 하는 메세지 전체에 계속 이용된다. 그래서 한번 노출, 도용된 암호화 키이는 그 시점 이후에 송신되는 모든 메세지를 도청, 수정, 삽입할 수 있다. 이를 개선하기 위하여 한개의 암호화 키이(EK)를 이용하여 암호화하는 메세지 양을 제한한다. 즉 KDC에서 지정시간(T_{TQ}) 만큼만 분배받은 EK로 메세지를 암호화하여 송신한다. 만약 지정한 Time Quantum에서 보내고자하는 메세지가 더 남아있을 때 송신자(A)는 두번째 암호화 키이를 KDC로 부터 분배 절차에 따라 분배 받는다. 그리고 나서 나머지 메세지를 송신할 때는 새로 분배받은 키이를 이용한다. 이때에 수신자(B)는 어떤 암호화 키로 복호화하여야 하는지를 결정해야 한다. 이를 구분하기 위해 키이 식별자를 이용한다. 송신되는 메세지에 키이 식별자도 함께 보내면 어떤 EK를 사용했는지를 바로 알 수 있게 된다. 즉 수신된 메세지의 키이 식별자와 이전의 키이 식별자와의 비교에 의해 EK를 구분할 수 있게 된다. 이때 생각해야 할 점은 Time Quantum의 양 지정에 있다. 만약 양의 지정값이 너무 크면 기존의 키이 분배 방식과 별 차이가 없고 너무 짧으면 빈번한 암호화 키이 분배 절차를 수행하게

된다. 따라서 가장 적합한 Time Quantum양을 지정하는 것이 문제점이다.

4. 키이 관리 구조와 데이타 구조

Time Quantum을 이용한 키이 분배 방식에 적합한 키이 관리 구조는 IBM에서 사용하고 있는 키이 계층 구조를 기본으로 하며 구조는 그림 6.과 같다.

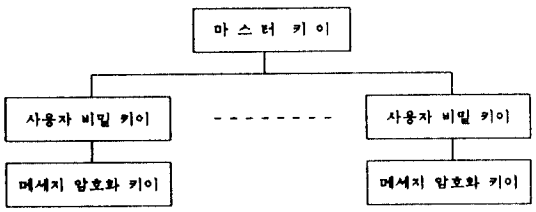

그림 6. 키이 계층 구조
Fig 6. Hierarchical structure of key

이 구조에서 마스터 키이는 사용자 비밀 키이 리스트를 암호화하여 관리하고 사용자 비밀 키이는 KDC와 대화시에 사용되며 메세지 암호화 키이는 사용자간의 메세지 송수신시에 사용된다. 메세지 암호화 키이의 사용시간이 제한되기 때문에 이를 생성, 저장하기 위한 데이타 구조가 필요하다. 암호화 키이 단위의 레코드 구조와 데이타 구조는 그림 7. 및 그림 8.과 같다.

KDC는 먼저 키이 분배 초기 과정이 수행되고 나면 각 노드별 비밀 키이 리스트를 생성한다. 그 후 KDC는 암호화 키이를 제한 시간에 따라 생성, 저장 관리해야 하기 때문에 삽입, 삭제가 용이한 링크 리스트 구조를 이용한다. 암호화 키이 생성시 마다 노드별 삽입이 수행되고 KDC가 지정한 키이 저장 시간이 경과하면 해당 레코드들을 삭제한다. 삭제된 리스트는 다시 필요할 때 사용하며, 이를 수행하기 위한 알고리즘은 다음과 같다.

Procedure MAIN(C, I, Y, TI, S, N)
//{NODE(i), 1≤i≤N}은 비밀 키이 리스트이며 N은 통신망을 구성하고 있는 노드들의 갯수이다. TI는 리스트로부터 제거하고자 하는 시간 지정값이다. //

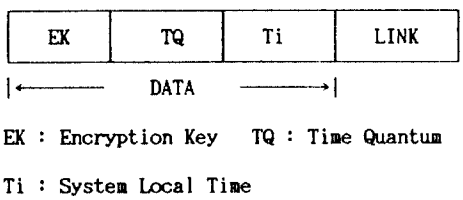

그림 7. 레코드 구조
Fig 7. Record Structure

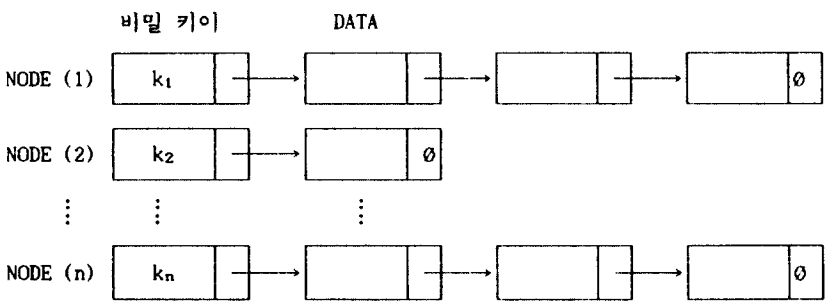

그림 8. 데이타 구조
Fig 8. Data Structure

```
//I는 암호화 키이 생성 또는 제거하고자 하는 노드
의 위치//
  case //원하는 작업 선택//
  : C = 1 : call INIT(N, K)
  : C = 2 : call ADD(I, Y)
  : C = 3 : call DELETE(I, Y, TI)

end

end MAIN
Procedure INIT(N, S)
//비밀 키이 등록과 AVAIL 노드 초기화 작업//
//N은 통신망에 연결된 노드의 수, S는 이용가능한
  AVAIL 노드의 수//
declare NODE(1:N), AVAIL(1:S)
  for i←1 to N do
   NODE(i)←ki//{ki, 1≤i≤k}는 개별 노드로부터
                등록된 비밀 키이//
   LINK(NODE(i))←0//각 노도의 초기 링크값은
                    0으로 지정한다.//

end

  for i←1 to S-1 do //AVAIL 노드초기화//
   LINK(AVAIL(i))←i+1 //링크 리스트 구성//

end

   LINK(S)←0//null 링크//
   AV←AVAIL(1)

end INIT

Procedure GETNODE(I)
//AVAIL 노드 리스트로부터 한개의 노드를 얻는다//
//AVAIL 노드가 있는지 없는지를 점검한다//
  if LINK(AV)=0 then call NO-MORE-NODES
  X←AV //X는 암호화 키이 저장 노드 포인터//
  AV←LINK(AV)

end GETNODE

Procedure ADD(I, Y)
//암호화 키이 생성시 리스트에 추가 작업//
  call GETNODE(X) //새로운 노드(AVAIL)를
                    얻는다//
  DATA(X)←Y //Y는 EK, TQ, Ti로 구성된 레코드//
  LINK(X)←0
//F는 Front 포인터이고 R은 Rear 포인터이다//
  if LINK(NODE(i))=0
    then F(i)←R(i)←LINK(NODE(i)←X
    else LINK(R(i))←X ; R(i)←X

end ADD

procedure DELETE(I, Y, TI)
//유지보수 지정 시간을 초과한 암호화 키이 리스트
  를 삭제하고 삭제한 노드들은 RET(X) 루틴에서
  재사용될 수 있도록 한다.//
  if F(i)=0 then NODE-EMPTY
          else if TI<=Ti(DATA) then
                X←F(i);F(i)←LINK(X)
                Y←DATA(X);call RET(X)

end DELETE
```

V. 결 론

본 논문에서는 근거리 통신망 환경에서의 정보보호의 필요성과 문제점, 이의 해결을 위한 요구 서비스 및 적용 대안을 기술하였다. 또 기존 암호화 키이 분배 방식을 분석하고 문제점을 기술하였다. 이의 해결과 근거리 통신망에 적용이 적합한 새로운 키이 분배 방식으로서 Time Quantum을 이용한 키이 분배 방식을 제안하였다.

제안된 키이 분배 방식은 기존 키이 분배 방식이 가지고 있는 키이의 concurrency와 상대방 인증의 문제점을 해결함과 동시에 기존의 방식은 암호화 키이의 단 한번의 노출이나 도용은 전체 메세지의 내용을 완전히 파악할 수 있으나 제안된 방식은 분배된 암호화 키이의 사용시간을 제한함으로서 키이를 이용하여 송신하는 암호화 메세지 양을 제안하여 한번의 키이 노출이나 도용, 메세지 도청및 누출이 있다 하더라도 전체 메세지의 내용을 알 수 없기 때문에 정보 보호의 안정성을 더욱 높일 수 있다.

본 논문에서 제안한 키이 분배 방식은 근거리 통신망에 직접 적용이 가능하나 SMIB와의 연관 구현과 Time Quantum의 최적 시간 설정 방안은 향후 연구 과제로 남아있다.

《알 림》

본 연구는 1992년도 한국 전자통신 연구소의 "'91 데이타 보호의 기술 기반에 관한 연구"의 연구비 지

원에 의한 연구임.

참 고 문 헌

1. C.P. pfleeger, "Security in computing", Prentice Hall, 1989.
2. R.M. Needham and M.D. Schroeder, "Using Encryption for Authentication in Large Networks of Computer", Comm ACM, vol.21, no.12, pp.993-999, Dec. 1979
3. D.E. Denning and G.M. Sacco, "Time stamps in Key Distribution protocols", Comm. ACM, vol.24, no.8, pp.533-536, Aug. 1981
4. W.F. Ehrsam, S.M. Matyas, C.H. Meyer, and W.L. Tuchman, "A Cryptographic Key Management Scheme for Implementing the Data Encryption Standards", IBM System Journal, vol.17, no.2, pp.106-125, 1978
5. "SDNS security protocol SP3", SDN / 301, Mar. 1988
6. ISO 7498 Information Processing System-open System Interconnect Basic Reference model
7. ISO 7498/2 Information Processing Systems-Open Systm Interconnect- Security Architecture
8. "Standard for Interoperable Local Network (LAN) Security(SILS)", draft p802.10/D5, June 1989
9. P.J. Fortier, "Handbook of LAN Technology", McGraw-Hill, 1989
10. Dennis K. Branstad, "Considerations for security in the OSI architecture", IEEE Network Magazine, 1987
11. Victor L. Voydock and Stephen T. Kent, "security in High-Level Network Protocols", IEEE Communication Magazine, 1985
12. "OSI 통신망 구조에서의 네트워크 안전체제 연구", 과기처 최종 연구 보고서, 아주대학교, 1989
13. 한국과학기술원 시스템공학센터, "컴퓨터망에서의 데이타 암호화 기법 적용에 관한 연구Ⅱ), (Ⅲ), Feb. 1990

柳 煌 彬(Howang Bin Ryou) 正會員

1949年 8月 15日生

1975年 2月 : 仁荷大學校 電子工學科

1977年 7月 : 延世大學校 産業大學院 電氣電子工學科

1989年 2月 : 慶熙大學校 大學院 電子工學科(工學博士)

1975年～1980年 : 金星半導體(株)

1981年～現在 : 光云大學校 電子計算學科 副教授

李 載 廣(Jae Gwang Lee) 正會員

1956年 3月 12日生

1984年 2月 : 光云大學校 電子計算學科 卒業

1986年 2月 : 光云大學校 大學院 電子計算學科 卒業

1990年 2月 : 光云大學校 大學院 電子計算學科 博士課程 修了

1986年～現在 : 全北 群山實業專門大學 電子計算科 副教授