OSI 네트워크 계층에서의 보호 프로토콜 구현

°손 연석, 박 영호, 문 상재
경북대학교 전자공학과

The Implementation of security protocols in OSI network layer

°Yean-Seak Son, Young-Ho Park, Sang-Jae Moon
Dept. of Electronics, Kyungpook National University

요 약 문

본 논문에서는 ISO/IEC의 표준안인 네트워크 계층 보호 프로토콜(NLSP)과 보호연관 프로토콜(SA-P)를 분석하여, 네트워크 계층에서의 NLSP 위치에 따른 주소, 분할 및 재조립 기능에 대해서 구체적으로 정의하고, 보호연관 프로토콜 표준의 키 토큰 교환 방식의 문제점을 해결한 새로운 키 토큰 교환 방식을 제시한다. 본 키 토큰 교환 방식에서는 Matsumoto-Imai 키 분배 프로토콜을 사용한다. 또한, 새로운 키 토큰 교환 방식을 적용한 네트워크 계층에서의 보호 프로토콜을 구현한다. 구현된 보호 프로토콜에서는 보호 알고리듬으로 DES, SHA, DSS를 사용한다.

1. 서 론

컴퓨터통신망의 보호체계를 위해서 ISO 7498-2[1]에서는 OSI 참조모델의 보호 구조를 정의하고 있다. 컴퓨터통신망에서 종단간 보호를 위해서는 제 4계층인 트랜스포트 계층과 제 7계층인 응용 계층에서 보호서비스를 제공하는 것이 적합하며 물리적인 보호는 제 1계층인 물리 계층에서 보호서비스를 제공하는 것이 적합하다.[2-4] 또한, 인터네트워크와 같이 중간 시스템을 고려해야 하는 경우에는 제 2계층인 데이타 링크 계층과 제 3계층인 네트워크 계층에 보호서비스를 제공하는 것이 적합하다. 그러나 데이타 링크 계층에서는 비밀보장 서비스만 제공되는 것에 반해 네트워크 계층에서는 부인봉쇄 서비스를 제외한 대부분의 보호서비스가 제공되므로 네트워크 계층에 보호서비스를 제공하는 것이 유리하다.

OSI 참조모델에 기초한 네트워크 계층에서의 보호 프로토콜로는 NIST (national institute of standards on technology)의 SP3(security protocol 3)[5]과 ISO(international standard for organization)/IEC(international electrotechnical conference)의 네트워크 계층 보호 프로토콜(NLSP, network layer security protocol)[6]이 있다. 네트워크 계층 보호 프로토콜은 네트워크 계층에서 보호 서비스를 제공하기 위하여 네트워크 계층의 부계층으로 동작되며, 네트워크 계층 상단, 네트워크 계층 하단 그리고 네트워크 계층 중간에 위치할 수 있다. 그러나 네트워크 계층 보호 프로토콜 표준에서는 NLSP의 위치에 따른 구체적인 기능 및 특성에 관하여 기술하지 않고 있다. 또한, 네트워크 계층 보호프로토콜 표준에서는 네트워크 계층 보호 프로토콜을 지원하기 위해서 보호연관 프로토콜(SA-P, security association-protocol)[7]을 권고하고 있다. 보호연관 프로토콜 표준에서는 키 토큰 교환을 위해 Diffie-Hellman형 키 분배 방식[8]을 사용하고 있다. D-H 방식을 변형하지 않고 사용할 경우 세션키를 발생시킬때 마다 같은 키가 생성되므로 한번만이라도 세션키가 불법 유출되면 더 이상 두 통신자간의 비밀 정보 교환은 불가능하다. 따라서 보다 안전한 키 토큰 교환 방식을 적용한 보호연관 프로토콜이 요구된다.

본 논문에서는 네트워크 계층에서 NLSP의 위치에 따른 주소, 분할 및 재조립 기능에 대해서 구체적

으로 정의하며, 보호연관 프로토콜 표준의 키 토큰 교환 방식의 문제점을 해결한 새로운 키 토큰 교환 방식을 제시한다. 본 키 토큰 교환 방식에서는 Matsumoto-Imai[9] 키 분배 프로토콜을 이용한다. 또한, 새로운 키 토큰 교환 방식을 적용한 네트워크 계층에서의 보호 프로토콜을 구현한다. 구현된 보호 프로토콜에서는 보호 알고리듬으로 DES(data encryption standard)[10], SHA(secure hash algorithm)[11], DSS(digital signature standard)[12]를 사용한다.

2. 네트워크 계층 보호 프로토콜

NLSP는 네트워크 계층에서 보호 서비스를 제공하기 위하여 종단 시스템 및 중간 시스템에서 구현될 수 있으며 네트워크 계층의 부계층으로 동작된다. NLSP는 비접속 네트워크 계층 보호 프로토콜(NLSP-CL) 및 접속 네트워크 계층 보호 프로토콜(NLSP-CO)로서 동작 가능하다. NLSP-CL은 데이타 발신처 인증, 접근제어, 비접속 비밀보장, 트래픽 흐름 비밀보장 그리고 비접속 무결성 서비스들을 제공하며 NLSP-CO는 대등 실체 인증, 접근제어, 접속 비밀보장, 트래픽 흐름 비밀보장 그리고 회복기능을 갖는 접속 무결성 서비스들을 제공한다.

2.1 NLSP 보호연관

NLSP의 동작은 보호 서비스 선택 정보, 보호 알고리듬 식별자 그리고 암호키와 같은 보호관리 정보에 의해 제어되며 이러한 보호관리 정보들을 보호속성이라 한다. 두 통신 객체간에 보호를 제어하는 보호 속성들의 집합이 보호연관이며 통신 객체들은 NLSP 동작을 위해 보호연관을 공유해야 한다. 통신 객체 사이에 협상을 통하여 동일한 보호속성 정보를 공유하는 과정을 보호연관 설정이라 한다. NLSP의 보호 연관 속성은 다음과 같다.

a) SA(security association) identification
b) Indicator of whether the NLSPE initiated or responded to the SA
c) UN address of peer NLSP entity
d) NLSP address of entities served through the remote peer
e) Security services selected for the SA (for NLSP-CL and NLSP-CO)
f) Parameter protection
g) Label mechanism attributes
h) Security services selected for the SA (for NLSP-CL)
i) Security services selected for the SA (for NLSP-CO)
j) CO protocol related attributes

NLSP는 SDT PDU 캡슐화를 사용하여 사용자 데이타 및 프로토콜 제어 정보를 보호한다. 캡슐화는 ISN(integrity sequence number), 패딩, ICV(integrity check value), 그리고 암호화에 기초하여 이루어지며 이러한 기능은 보호연관 속성에 의해서 적용된다.

2.2 NLSP의 기능 및 절차

NLSP-CO와 NLSP-CL에서의 보호는 모든 서비스 파라미터 보호, NLSP 사용자 데이타 보호, 그리고 비보호가 있다. 모든 NLSP 서비스 파라미터 보호는 주소와 사용자 데이타를 포함하는 모든 파라미터들을 보호하며 보호연관 속성 Param_Protec이 True일 때 선택된다. NLSP 사용자 데이타 보호의 경우 사용자 데이타는 보호하나 다른 NLSP 서비스 파라미터들은 보호하지 않으며 보호연관 속성 Param_Protec이 False일 때 선택된다. 비보호의 경우 모든 NLSP 서비스 파라미터들은 UN(underlying network) 서비스 파라미터들로 복사되며 모든 NLSP 절차들은 수행되지 않는다. NLSP에서 사용되는 PDU는 SDT PDU, CSC PDU, 그리고 SA PDU의 세 가지 방식이 있다. SDT PDU 구조는 그림 1과 같다. SDT PDU는 비보호 헤더, 암호화 동기, 캡슐화되기 전 옥테트 스트링 및 ICV 영역으로 구성된다. 보호연관 PDU는 프로토콜 식별자, PDU 길이, PDU 형태, 보호연관 식별자, 보호연관 프로토콜 형태 및 보호연관 내용 영역으

로 구성되어 있으며 그림 2와 같다. 접속 보호 제어 PDU는 프로토콜 식별자, 길이, PDU 형태, 보호연관 식별자, 내용 길이와 CSC PDU 내용 영역으로 구성되며 그림 3 같다.

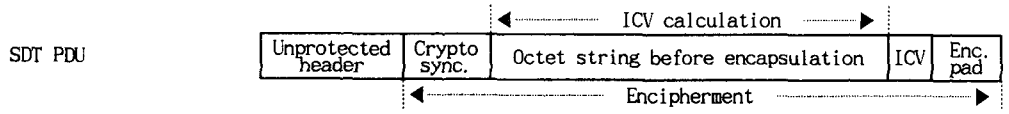


그림 1. SDT PDU의 구조

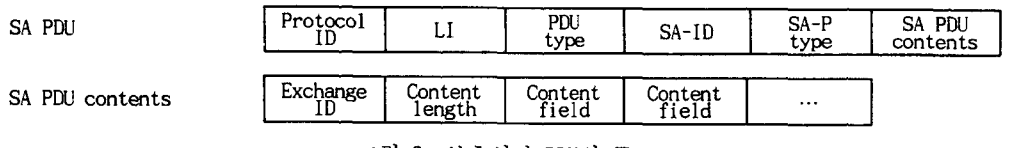


그림 2. 보호연관 PDU의 구조

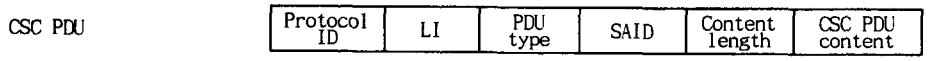


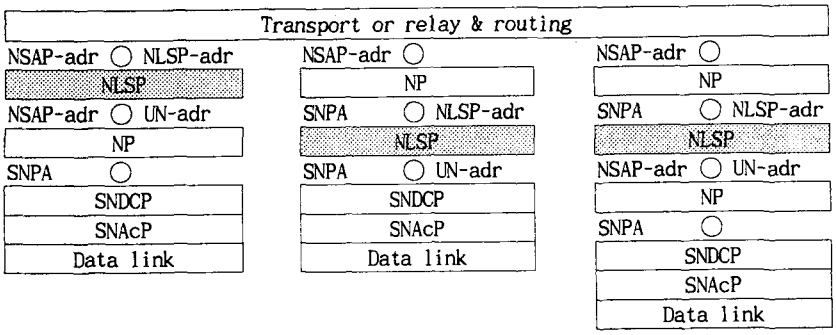
그림 3. 접속보호제어 PDU의 구조

3. 네트워크 계층 보호 프로토콜 위치 분석

네트워크 계층 보호 프로토콜은 네트워크 계층의 부계층으로 동작한다. 네트워크 계층 보호 프로토콜은 네트워크 계층 상단, 네트워크 계층 하단 그리고 네트워크 계층 중간에 위치할 수 있다. 본 장에서는 NLSP 객체의 위치에 따른 NLSP 주소, 네트워크 계층의 분할 및 재조립 기능에 관하여 분석한다.

3.1 NLSP 주소

네트워크 계층 내에서 NLSP 객체는 네트워크 계층의 상단, 하단 및 중간에 위치할 수 있으며 주소는 그림 4와 같다. NLSP 서비스 인터페이스에는 NLSP 서비스와 UN 서비스가 있다. NLSP 객체는 NLSP 서비스 사용자와 UN 사이에 위치하고 대응 SAP(service access point)는 NLSP-SAP와 UN-SAP이다. NLSP가 네트워크 계층 상단에 위치하는 경우, NLSP 서비스 사용자는 트랜스포트 객체이며 트랜스포트 객체를 식별하는 NSAP 주소는 NLSP 주소와 UN 주소와 동일하다. NLSP가 네트워크 계층 하단에 위치하는 경우, NLSP 서비스 사용자는 네트워크 계층이며 네트워크 객체를 식별하는 SNPA는 NLSP 주소와 UN 주소와 동일하다. NLSP가 네트워크 계층 중간에 위치하는 경우 상위 부계층은 NLSP 서비스 사용자로서 다른 네트워크 서비스 사용자를 식별하며 중계 및 경로 설정 기능을 담당한다. 상위 부계층을 식별하는 SNPA는 NLSP 주소와 동일하고 하위 네트워크의 NSAP 주소는 NLSP 객체를 식별하는 UN 주소이다. NLSP가 네트워크 계층 상단에 위치하는 경우는 종단 시스템간에만 사용될 수 있으며, NLSP가 네트워크 계층 하단에 위치하는 경우는 신뢰할 수 있는 중간 시스템과 연결된 경우나 네트워크 릴레이가 없는 종단간 통신 시스템에 사용된다. 네트워크 계층 중간에 위치하는 경우는 두 통신 시스템간에 신뢰할 수 있는 중간 시스템과 신뢰할 수 없는 중간시스템에 사용할 수 있으며 가장 융통성이 있고 어떤 환경에서도 동작할 수 있다.



NSAP : Network service access point
SNPA : Subnetwork point of attachment
SNAcP: Subnetwork access point
SNDCP: Subnetwork dependent convergence protocol

그림 4. NLSP 부계층을 갖는 네트워크 계층에서의 주소

3.2 분할 및 재조립

분할은 네트워크 계층내의 NLSP 위치에 따라 NLSP의 처리 이전 및 이후에 처리될 수 있다. 첫번째로 그림 5와 같이 NLSP가 네트워크 계층 상단에 위치하는 경우, NLSP 객체는 상위 계층으로부터 전송된 NSDU를 캡슐화하여 SDT PDU를 구성한다. 네트워크 계층 프로토콜은 SDT PDU를 하나의 데이타로 간주하여 헤더를 부착하여 NPDU를 구성하며, 또한 분할 기능을 수행하여 상대 객체에게로 전송한다. 두번째로 그림 6과 같이 NLSP가 네트워크 계층 하단에 위치하는 경우, 네트워크 계층 프로토콜은 상위 계층에서 전송된 NSDU에 헤더를 부착하여 NPDU를 구성하며 분할 기능을 수행한다. NLSP 객체는 분할된 각 NPDU를 캡슐화하여 SDT PDU를 구성하여 상대 객체에게 전송한다. 세번째로 그림 7과 같이 NLSP가 네트워크 계층 중간에 위치하는 경우, 상위 네트워크 계층 프로토콜은 중계 기능 및 NPDU 구성을 담당하며 하위 네트워크 계층 프로토콜은 분할 기능을 담당하게 된다. 따라서 상위 네트워크 계층 프로토콜은 전송된 NSDU에 헤더를 부착하여 NPDU를 구성하며, NLSP 객체는 NPDU를 캡슐화하여 SDT PDU를 생성한다. 그리고 하위 네트워크 계층 프로토콜은 SDT PDU에 대해서 분할 기능을 수행한 후 상대 객체에게 전송한다. 각각의 경우에 대하여 상대 객체에서의 재조립 기능은 송신 역과정으로 이루어진다.

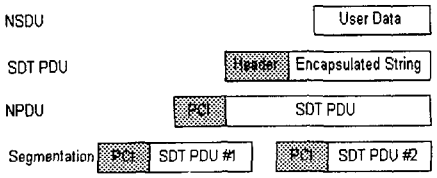


그림 5. 네트워크 계층 상단 위치

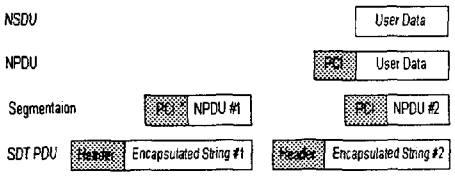


그림 6. 네트워크 계층 하단 위치

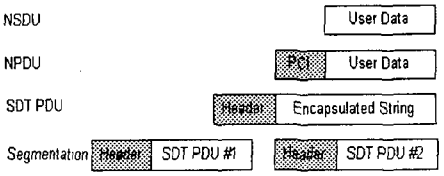


그림 7. 네트워크 계층 중간 위치

4. 새로운 보호연관 프로토콜

보호연관 프로토콜은 키 토큰 교환, 상호 인증, 보호속성 협상, 그리고 보호연관 해제의 4가지 논리적 기능 블럭으로 분류된다. 키 토큰 교환은 현재의 통신 세션을 위한 키 생성 및 분배 과정이며, 상호 인증은 보호연관이 설정되는 동안 NLSP 확인표 및 디지탈 서명을 교환하여 다른 객체를 인증하는 과정이다. 보호 속성 협상은 안전한 데이타 전송을 위한 보호서비스, 보호 메카니즘등과 같은 보호속성을 협상하는 과정이며, 보호연관 해제는 통신자간의 데이타 전송이 완료되면 설정된 보호연관을 해제하는 기능이다.

4.1 새로운 키토큰 교환 방식

각 NLSP 객체는 현재의 통신 세션을 위한 세션키를 생성하기 위해 키토큰 교환을 수행한다. NLSP 객체들은 세션키와 대칭키 알고리듬을 사용함으로써 키 토큰 교환 이후의 통신에 대한 비밀보장을 제공한다. 세션키는 대칭키 알고리듬과 결합하여 보호연관 프로토콜 인증과 보호연관 속성 협상을 지원하기 위해 사용된다. 또한 이 값은 보호연관의 키와 ISN(integrity sequence number)속성으로서 사용되기 위하여 위치정보의 교환이나 사전에 약속된 정보를 통하여 참조된다. 표준에서는 D-H 방식을 키 토큰 교환에 사용하고 있다. 그러나 D-H 방식을 변형하지 않고 사용할 경우 세션키를 발생시킬때 마다 같은 키가 생성되는 문제가 발생한다.

본 절에서는 보호연관 프로토콜에 사용된 키 토큰 교환 방식의 문제점을 해결하기 위하여 Matsumoto-Imai(MI) 키 분배 방식을 이용함으로써 보다 안전한 보호연관 프로토콜을 제안한다.

첫째: 객체 A와 B는 비밀키 X_A와 X_B, $1<X_A, X_B<p-1$를 발생하고 공개키 Y_A와 Y_B를 교환한다.
여기서 $Y_A = a^{X_A} \bmod p$ 이고 $Y_B = a^{X_B} \bmod p$ 이다.

둘째: 객체 A와 B는 각각 임의 불규칙 정수 K_A와 K_B, $1<K_A, K_B<p-1$,를 발생시켜 W_A(키 토큰 5)와 W_B(키 토큰 6)를 생성하여 서로 교환한다.
여기서 $W_A = a^{K_A} \bmod p$ 이고 $W_B = a^{K_B} \bmod p$이다.

세째: 두 통신자는 동일한 키 $Z_A = W_B^{X_A} Y_B^{K_A} = Z_B = W_A^{X_B} Y_A^{K_B} = a^{X_A K_B + K_A X_B} \bmod p$를 얻는다.

MI 방식을 이용한 키 토큰 교환 방식은 그림 8과 같다.

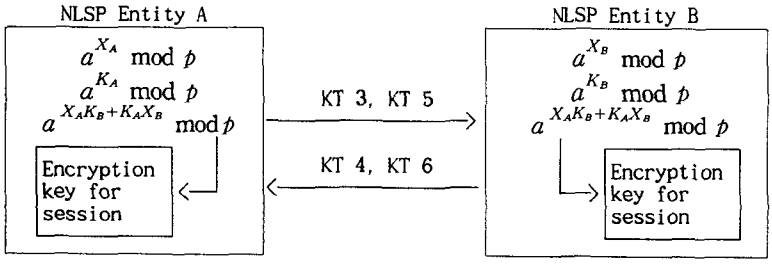


그림 8. MI 방식을 이용한 키 토큰 교환

이 방식에서는 임의 불규칙 정수 K_A와 K_B만 같지 않으면 생성되는 세션키는 서로 다르다. 또한, 비밀키 X_A와 X_B가 노출되어도 세션키는 분석되지 않는다. K_A와 K_B를 모르고서 세션키 $Z_A(Z_B)$를 안다는 것은 원래의 이산대수 문제 만큼 어렵게 되므로 더욱 안전한 통신이 가능하다.

4.2 보호연관 프로토콜 인증

보호연관이 설정되는 동안 NLSP 객체는 다른 NLSP 객체를 인증하기 위하여, 인증 확인표와 공개키 쌍이 필요하다. 이를 위해 두 NLSP 객체는 확인표 및 디지탈 서명을 교환한다. 확인표는 최소한으로

NLSP 객체의 식별정보와 객체의 공개키를 위한 식별정보를 포함한다. 확인표는 TA에 의해 확인된 것으로서 TA의 인증 서명을 갖고 있으며, SA-P에 관여된 모든 NLSP 객체는 확인표를 발행하는 TA의 공개키를 가져야 한다. 각 NLSP 객체는 상호 인증을 위하여 확인표 내의 공개키에 대한 비밀키를 알고 있음을 증명함으로써 이루어진다. 즉 객체 A의 비밀키 A 이외의 객체는 알 수 없으므로 객체 A의 신원 확인이 가능하다. 이를 위해 NLSP 객체는 먼저 확인표 교환과 TA의 서명 검증을 통해 각 객체에 대한 공개키를 획득한다. 다음으로 각 NLSP 객체는 확인표 및 보호 연관 속성에 대하여 디지탈 서명을 한 후 암호화하여 전송하며 수신한 NLSP 객체는 암호문을 복호화한 후 검증 과정을 수행한다.

4.3 보호 연관 속성 협상

NLSP 객체는 보호연관 속성을 협상하기 위하여 보호 서비스 목록, 라벨 집합, 키와 ISN, 그리고 그밖의 보호연관 속성을 협상한다. 이를 위해 시작 NLSP 객체는 확인표, 보호서비스 목록, 라벨 집합, 키/ISN, 그밖의 보호속성 등에 대해 디지탈 서명을 한 후 암호화하여 전송한다. 수신 NLSP 객체는 SA PDU를 복호화한 후 디지탈 서명에 대한 검증을 함으로써 상대 객체를 인증하며 전송된 보호연관 속성을 선택한다. 이 과정에서 객체 A의 비밀키는 A 이외의 객체는 알 수 없으므로 객체 A의 신원 확인이 가능하며, SA PDU는 보호하여 전송된다.

보호 서비스 목록 협상을 위해 시작 NLSP는 로컬 보호 정책에 기초하여 하나 이상의 가능한 보호 서비스 선택 요소로 구성된 집합을 구성한다. 또한 수신 NLSP 객체는 제안된 서비스 집합중 사용 가능한 것이 있으면 선택된 보호서비스를 시작자에게 돌려주고 사용가능한 것이 없으면 보호연관 거부에 대한 이유를 지시하는 상태를 되돌려준다.

라벨 집합 협상을 위해 시작 NLSP 객체는 보호 라벨를 제시하여 보호연관의 보호하에 전송한다. 수신 NLSP 객체는 제안된 라벨 집합이 보호연관 보호하에서 전송되었는지를 결정하며, 제안된 라벨 집합 중에서 하나 이상의 라벨이 가능하면 제안된 참조 집합의 부분집합을 되돌려주고 그렇지 않다면 보호연관 거부에 대한 이유를 지시하는 상태를 되돌려준다.

키와 ISN 선택을 위해 시작 NLSP 객체는 키 토큰 결과 비트열의 부분을 선택하여 전송한다. 키/ISN은 키 토큰 결과 비트열내의 초기 비트 위치에 의해 식별되며 길이는 보호 서비스와 연관된 매개변수에 의해 결정된다. 수신 NLSP 객체는 키/ISN으로 사용될 키 토큰 결과 비트열의 부분을 로컬 보호 정책에 기초하여 결정한다. 그밖의 SA 속성 협상은 매개변수의 보호, 사용된 No_Header 옵션 등과 같은 SA 속성 값들을 결정한다. 시작 NLSP 객체는 제안된 SA 속성 집합을 Miscellaneous flag 영역을 이용하여 수신 NLSP 객체에게 전송한다.

4.4 보호 연관 속성 해제/중지

NLSP 객체나 로컬 보호 관리자는 더 이상 보호연관이 유효하지 않거나 필요하지 않은 경우, 상대 객체에게 보호연계 해제/중지 요청 PDU를 보낸다. 이때 보호연관의 해제/중지의 개시자가 반드시 보호연관의 개시자일 필요는 없다. 보호연관의 해제/중지에 대한 이유를 알리고 싶은 경우 그 이유를 알린다. 시작 NLSP 객체는 확인표, 세션키, 보호연관 해제/중지 이유 영역에 대하여 서명하고 암호화한 SA PDU를 전송함으로써 보호연관 해제/중지를 요청하게 된다.

5. 보호 관리 정보 구성 및 시뮬레이션

5.1 보호 관리 정보의 구성

두 통신 객체간의 통신을 보호하기 위하여 두 통신 객체는 암호 알고리듬, 암/복호 키, 인증 기법 및 보호 라벨 등과 같은 보호 관리 정보를 공유해야 한다. 이 보호 관리 정보들을 SMIB로 구축하기 위하여, 본 논문에서는 ASSR, SA-P 정보, NLSP 정보로 구분하여 구성한다.

먼저 ASSR은 통신 당사자간 동의된 보호 규칙의 집합으로 상호 동의하여 정의할 필요가 있는 모든 매개변수들을 포함하고 있다. ASSR은 유일한 식별자를 가지며 이 식별자는 모든 사용자에게 알려지고 보호연관 설정 과정에서 이 식별자만을 교환함으로써 ASSR에서 정의한 보호연관 속성에 대해 동의한다. 보호연관 설정 과정에서 개시자는 여러개의 ASSR 식별자를 전송하며 응답자는 하나를 선택하게 된다. 본 논문에서는 두 통신자간에 ASSR을 미리 공유하고 있다고 가정하고, 한 개의 ASSR만을 정의하였다. 본 논문에서 사용한 ASSR은 그림 9와 같다. 그림 9에서 보호 알고리듬, 디지탈 서명 및 키 정보의 발생은 보호연관 프로토콜 통신을 보호하기 위하여 동적으로 설정할 수 있는 정보로서 SA PDU 교환 과정을 통하여 협상하도록 설계하였다. 따라서 각 동적 정보에 따른 여러 개의 ASSR을 정의하는 번거러움을 줄일 수 있다.

둘째, SA-P 정보는 보호연관 프로토콜을 수행하기 위하여 두 통신 객체간에 공유되어야 할 정보로서 보호연관 프로토콜에서 정의한 사전 설정 정보인 지원 메카니즘, 비대칭 알고리듬에 대한 비대칭 키 쌍, TA의 확인표, TA의 공개키 및 TA의 공개키를 이용하는 비대칭 알고리듬으로 구성되어 있다. 또한 다음과 같이 가정하고 정의한다.

i) 지원 메카니즘은 ASSR에서 정의한 e)에서 j)까지의 메카니즘 모듈을 그대로 사용한다.

ii) 각 보호 알고리듬의 특성들은 두 통신자 간에 미리 공유하고 있다고 가정하고 구현시 그 식별자만을 교환함으로써 보호 알고리듬에 대해 동의하게 된다. 또한 각 알고리듬에 대한 키 정보는 각 알고리듬 특성에 의존하며 키 토큰 교환 실험에서 생성된 공유 세션키 열을 참조한다.

iii) 키 토큰 교환과 인증을 지원하기 위하여 모든 통신 객체는 신뢰할 수 있는 센타인 TA가 존재하며, TA에 대한 전적인 신뢰가 보증된다고 가정한다. 인증을 위해 사용되는 TA의 확인표는 두 객체간의 통신 이전에 TA로부터 제공되었다고 가정한다. 확인표는 NLSP 객체 식별자, 객체의 공개키, 보호관련 매개변수, 그리고 TA의 인증 서명 영역으로 구성되어 있다.

마지막으로 NLSP 정보는 ASSR과 함께 NLSP를 지원하기 위한 정보로서, SA PDU의 교환을 통하여 협상된 보호연관 속성들을 포함하고 있다.

```
a) ASSR-ID : 1.0002.03.4.11

b) Selected definition module
   (PE or DO) Auth: none, low, high
   AC           : none, low, high
   Confid       : none, low, high
   Integ        : none, low, high
c) Security Label
   - Sensitivity level
    {Unclass, Integrity, Confidentiality, Secret}
    • Label->sensitivity = Unclass
      implies Auth=none, AC=none, Confid=none, Integ=none
    • Label->sensitivity = Integrity
      implies Auth=none, AC=none, Confid=none, Integ=high
    • Label->sensitivity = Confidentiality
      implies Auth=none, AC=none, Confid=high, Integ=none
    • Label->sensitivity = Unclass
      implies Auth=high, AC=high, Confid=high, Integ=high
d) Protection of all service parameters
   for security service selected: Integ=high or Conf=high
e) Mechanism module - security labels for access control
   for security service selected: AC= high or Conf= high
   Label_Def_Auth     : XYZ
   Explicit indication : Yes
f) Mechanism module - Integrity Check Value
   for security service selected: Integ>none or Auth=high
                or Mechanism security label(Confid = high)
   ICV_Alg_ID    : XYZ
   ICV_Blk_size  : x octets
   Rekey after   : 10,000 PDUs
   Key distribution mechanism: asymmetric
g) Mechanism module - Integrity sequence number
   for security service selected: Integ=high or Auth=high
   ISN_Len    : 4 octets
h) Mechanism module - Encipherment
   for security service selected: Conf > low
   Enc_Alg_ID    : XYZ
   Enc_Blk_size  : x octets
   Rekey after   : 10,000 PDUs
   Key distribution mechanism: asymmetric
i) Mechanism module - Connection authentication
   for security service selected: AC>low or PE Auth>low
   Enc_Alg_ID    : XYZ
   Enc_Blk_size  : x octets
   Key distribution mechanism: asymmetric
j) Mechanism module - Asymmetric key distribution
   for mechanism encipher or integrity check value
   PKC_Alg_ID    : XYZ
```

그림 9. NLSP에서의 ASSR

5.2 새로운 키 토큰 교환 실험

보호연관 설정을 위한 첫번째 SA PDU 교환인 키 토큰 교환에서는 MI 키 분배 알고리듬을 이용하였다. GF(p)에서 모든 가입자에게 공통으로 알려진 공개인수인 512비트 원시원 α와 소수 p의 값은 다음과 같다.

α = 17e4 a2d6 f551 6389 c514 5639 96f 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

p = 9505 e383 51fc 6769 8fcb e0a8 da98 95b2
e74f c59e ce12 6073 8e49 b2da 49b2 32cc
0f8f dc9e 9769 21da 2947 f4ef f5b4 ba61
33d7 34d7 6689 3bd0 801b 1643 4df4 2465

키 토큰 교환 실험에서, 두 통신 객체가 위의 원시원 α와 법 p를 이용하여 비밀 세션키를 생성하는 과정은 다음과 같다. 두 객체 A와 B는 각각 비밀키 X_A와 X_B, $1<X_A, X_B<p-1$를 발생하고 공개키 Y_A와 Y_B를 교환한다. 여기서 $Y_A=\alpha^{X_A} \bmod p$ 이고 $Y_B=\alpha^{X_B} \bmod p$이다. 다음은 객체 A와 B의 비밀키와 교환된 공개키다.

Entity A	Secret Key	1d 7616 2994
	Public Key	3279 c5ce c348 8336 ae0f faef 859d 8e11 ddfb 1d91 9109 191c df32 107e 89eb b35c a11b a13b a5ba 747a f5bf cbc8 0ea9 1071 8b32 7866 3a3b 8950 6d01 d245 acd8 ad02
Entity B	Secret Key	11 ca69 1718
	Public Key	4959 d340 8c3c 3511 9f21 1188 3ad1 396b 238f 98e7 454f d0fa 24fc cb53 3a94 5539 ba66 6c97 a164 9822 02bf a9ae f0fe 259b 9d70 963f a339 dfa0 073b 5f56 4cda 94f0

객체 A는 임의 불규칙 정수 $K_A, 1<K_A<p-1$, 를 발생하고 키 토큰 5($W_A=\alpha^{K_A} \bmod p$)을 계산하여 객체 B에게 전송한다. K_A, W_A의 값은 다음과 같다.

K_A = 012d df33 a32f 2e6e d7d8 dfc2 cd87 4864
cb66 9e07

W_A = 8cee 9eaa b952 c6ed 8b55 5fd6 57ac f5ab
d05c ba5d 3550 a4e7 0bf2 705a f05e 0adc
d1a7 49ee e90d 2600 c580 76bd 464f 4bda
1bda 058b 5d77 3415 fcca ce9a a736 5a05

객체 B는 임의 불규칙 정수 K_B, $1<K_B<p-1$, 를 발생하고 키 토큰 6($W_B=\alpha^{K_B} \bmod p$)를 계산하여 객체 A에게 전송한다. K_B, W_B의 값은 다음과 같다.

K_B = 9a97 4c82 c667 c09f 2854 211e 32eb d7d1
e7d8 9657

W_B = 5a09 3af7 9165 c04f a38e 1795 d4f2 6c0b
3d89 416f 5a2c 7b0e 9165 c04f 2c0e 3af7
624d b30f 9e58 7c1a b3e7 a82d 9165 c04f
d4f2 6c0b a38e 1795 5a2c 7b02 3d89 416f

두 객체 A, B는 첫번째 SA PDU의 교환을 통하여 동일한 세션키 Z_A와 Z_B를 얻는다. 여기서 Z_A와 Z_B는 다음과 같다.

$Z_A=W_B^{X_A}Y_B^{K_A} \bmod p=\alpha^{X_AK_B+K_AX_B} \bmod p$
= 0a75 c708 4f71 0d9b 831f 3d39 b49a e0b5
1998 96ac a3a9 1481 678f 08aa 7e0a 587a
3fd1 2f9a 04db a278 2662 5b0b ec95 a464
9567 276b 283e 3d51 628c 4323 9e0c f6e3

$Z_B=W_A^{X_B}Y_A^{K_B} \bmod p=\alpha^{X_AK_B+K_AX_B} \bmod p$
= 0a75 c708 4f71 0d9b 831f 3d39 b49a e0b5
1998 96ac a3a9 1481 678f 08aa 7e0a 587a
3fd1 2f9a 04db a278 2662 5b0b ec95 a464
9567 276b 283e 3d51 628c 4323 9e0c f6e3

위의 실험 결과에서 두 객체 A와 B는 동일한 세션 키를 공유함을 알 수 있다. 여기서 분배된 세션키는 SMIB에 저장되고 보호연관 속성 협상에서 참조된다. 또한, 두번째 SA PDU의 교환 과정에서 이 세

션 키의 처음 64 비트는 비밀보장 서비스를 제공하기 위해 비밀보장 알고리듬인 DES의 암복호화 키 값으로 사용되며 두 객체 A와 B는 0a75 c708 4f71 0d9b를 비밀 키 값으로 가진다.

5.3 보호연관 협상 및 해제 실험

보호연관 협상 및 해제 실험은 보호연관 설정을 위한 두번째 SA PDU 교환 실험, 보호연관 중지/해제를 위한 SA PDU 교환 실험으로 나누어진다. 먼저 보호연관 설정을 위한 두번째 SA PDU는 키 토큰 교환 실험에서 협상된 보호알고리듬인 DSS와 SHA를 이용하여 내용 전체에 대하여 서명하고 내용 영역 전체에 대하여 DES로 암호화하여 전송되었다. 수신측에서는 SA PDU를 복호화하고, 확인표 및 디지탈 서명 영역을 검사함으로써 두 통신 객체간의 인증이 이루어졌다. 두번째 SA PDU 교환 과정을 통하여 보호연관 속성들이 협상되고 이 값들은 SMIB에 저장되었다. 그림 10은 보호연관 PDU의 교환을 통해 설정된 보호연관 속성값들을 나타낸 것이다. 다음으로, 보호연관 중지/해제를 위한 보호연관 PDU의 교환 실험이다. 두 통신자는 보호연관 중지/해제를 위한 보호연관 PDU를 교환 후 보호 서비스를 중단하고 보호연관 속성들을 SMIB에 저장하지 않고 버림을 확인하였다.

```
a) SA identification
   Local_SAID: 61616161
   Peer_SAID : 61616162
   SAID_Len  : 4
b) Indicator : initiator or responder
   Initiator : 01
c) Address of peer NLSP entity
   Peer_Adr  : 4900010000c05cf84b01
d) Identifier for the ASSR
   ASSR_ID   : 1.0014.13.5.111
e) Protection QOS selected for the SA
   QOS_Label: 0   AC    : 2   DOAuth  : 2
   CLConf   : 2   CLInt : 2   PEAuth  : 0
   COConf   : 0   COInt : 0   COIntr  : 0
f) Mechanisms selected for the SA
   Label : 1      Conf  : 1   ICV     : 1
   SN    : 0      DOAuth: 1   UNPort  : 0
g) Label mechanism attributes
   Label_Ref      : 167
   Label_Def_Auth : 7a
   Label_Content  : 00f4c6050302020202
h) SN mechanism attributes
   Data_Local_SN  : 00
   Data_Peer_SN   : 00
i) ICV mechanism attributes
   ICV_Alg: 60   ICV_Len: 160
   ICV_Blk: 00   ICV_Kg : 00
   ICV_Gen_Key:  ICV_Check_Key:
j) Encipherment mechanism attributes
   Enc_Alg : 14
   Enc_Blk:  64
   Enc_Kg  : 00
   Enc_Key : 61427a5e16071b7b
   Dec_Key : c84163c8be3be438
```

그림 10. 협상된 보호연관 속성

5.4 보호 데이타 전송 실험

NLSP 객체는 보호연관 프로토콜에 의해 SMIB에 저장된 보호 관리 정보에 기초하여 보호 서비스를 제공한다. 데이타 전송 실험을 위한 메세지는 "This program provides the security service in network layer" 이며 다음과 같다.

546869732070726f6772616d2070726f766964657320746865207365375726
9747920736572669636520696e206e6574776f726b20bc617965720d

송신측에서는 그림 10의 협상된 보호연관에 기초하여 비보호 헤더, 암호화 동기, 캡슐화되기전 옥테트 스트링, ICV, 및 암호화 패딩 영역을 포함하는 SDT PDU를 구성하여 하위 계층으로 전달한다. 구성된 SDT PDU의 값은 다음과 같다.

0548616161622279d2d5e0c991dd6d4929c0edaf4e19f6c86e6ca8a44ec4848b
1908996b853d03dfbd19478cf7616492f881965922a2eaaf1f1db8ded121c19
dd3e28f148e552d06416f6edfad34eae4807af67ee947b03aa7229a017b6fdb
891e159ba93bbee499bfce6fe890a6088

수신 과정은 송신 과정의 역과정이며 협상된 보호연관 속성에 기초하여 SDT PDU를 처리하고 NLSP 지시 프리미티브를 형성하여 상위 네트워크 계층으로 전달한다.

위의 송수신 과정을 살펴보면, 인증서비스는 키 관리와 결합한 데이타 무결화 메카니즘에 의해 제공됨을 알 수 있다. 무결성 서비스는 전송 PDU의 캡슐화되기 전 옥테트 스트링 영역에 대해서 해쉬함

수를 취해 ICV영역을 형성함으로써 불법적인 방법에 의한 전송 PDU의 손상 유무를 확인할 수 있었다. 비밀보장 서비스는 전송 PDU의 암호화 동기 영역, 캡슐화되기 전 옥테트 스트링 영역, ICV 영역을 암호화 알고리듬인 DES를 사용하여 암호화함으로써 제공된다. DES의 암복호 키는 분배된 세션키를 사용하였다. 또한 통신할 때마다 새로운 세션키를 분배함으로써 불법적인 제 삼자에게 노출없이 전송이 가능하였다. 접근제어 서비스는 캡슐화되기 전 옥테트 스트링 영역에 라벨 영역을 넣어서 전송함으로써 제공할 수 있었다. 그러나 접근제어 서비스는 객체들이 연관되어 있는 통신자간에만 가능하므로, 시스템 관리에 의존적이다.

6. 결 론

본 논문에서는 개방형 시스템에서 종단 및 중간 시스템에서의 안전한 데이타 전송 보호를 위하여, ISO/IEC의 표준안인 네트워크 계층 보호 프로토콜과 보호연관 프로토콜을 분석하여, 네트워크 계층에서 NLSP의 위치에 따른 주소, 분할 및 재조립 기능에 대해서 구체적으로 정의하였고, 보호연관 프로토콜 표준의 키 토큰 교환 방식의 문제점을 해결한 새로운 키 토큰 교환 방식을 제시하였다. 본 키 토큰 교환 방식에서는 Matsumoto-Imai 키 분배 프로토콜을 사용하였다. 또한, 새로운 키 토큰 교환 방식을 적용한 네트워크 계층에서의 보호 프로토콜을 구현하였다. 구현된 보호 프로토콜에서는 보호 알고리듬으로 DES, SHA, DSS 등을 사용하였다. 그리고 키 토큰 교환 실험, 보호연관 협상 및 해제 실험, 보호 데이타 전송 실험을 수행하여 네트워크 계층이 제공하는 보호 서비스를 확인하였다.

참 고 문 헌

[1] ISO, Information Processing - Open System Interconnection - Basic Reference Model - Part 2 : Security Architecture, ISO 7498-2, 1989.

[2] CCITT, Message Handling System : EDI Message System, Draft Recommendation X.435, Version 6.0, Nov. 1990.

[3] ISO/IEC, Transport Layer Security Protocol, ISO/IEC 10736, October 1993.

[4] ISO, Information Processing - Data Encipherment - Physical Layer Interoperability Requirements, ISO 9160, Feb. 1989.

[5] SDNS Program Office, Security Protocol 3(SP3), SDN.301, Revision 1.5, May 1989.

[6] ITU-T/ISO/IEC 11577, Information Technology - Open Systems Interconnection - Network Layer Security Protocol, International Standard, November 1993.

[7] ITU-T/ISO/IEC 11577, Information Technology - Open Systems Interconnection - Security Association Protocol, International Standard, November 1993.

[8] W.Diffie and M.E.Hellman, "New directions in cryptography," IEEE Trans. on Information Theory, vol. IT-22, pp. 644-654, Nov. 1976.

[9] The Transactions of the IECE of Japan. Vol.E69, NO.2 February 1986.

[10] National Bureau of Standard, Data Encryption Standard, U.S.FIPS PUB 46, 00.254-264, 1977.

[11] National Institutes Standard Technology, Specification for a Secure Hash Standard(SHS), FIPS YY Draft, Feb. 1992.

[12] National Institute Standard Technology, Specification for a Digital Signature Standard(DSS), FIPS XX Draft, Aug. 1991.