2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

GSMP 프로토콜의 보안에 관한 연구

권헌진*, 백현규*, 차영욱*
*안동대학교 컴퓨터공학과 대학원

e-mail : imp@andong.ac.kr, imi@andong.ac.kr,
ywcha@andong.ac.kr

A Study of the GSMP Security

Heun-Jin Kwon*, Baek, Hyun-Gyu*, Young-Wook Cha*
*Dept of Computer Engineering, Andong National University

요약

본 논문은 IETF에서 레이블 스위치를 제어하기 위하여 표준화가 진행 중인 GSMP 프로토콜에 보안 서비스를 추가하여 네트워크에서 가능한 공격이나 위협과 같은 보안 문제에 대한 해결책을 검토하고 있다. GSMP 프로토콜의 Adjacency 메시지를 통하여 스위치와 컨트롤러사이에 동기화 설정과정에 보안 서비스를 위한 정보요소를 추가하여 GSMP 프로토콜에서 메시지 인증, 기밀성, 무결성 보안 서비스를 제공한다. 인증 서비스를 제공하여 메시지에 대한 정당성을 검증하고 기밀성과 무결성 서비스를 제공하여 메시지의 변조나 재생과 같은 공격을 막을 수 있을 것이다.

1. 서론

네트워크 기술이 급속도로 발전하면서 인터넷의 사용은 폭발적으로 늘어났고, 정보교환의 양이 늘어나면서 서비스의 안정성과 비밀성에 사용자들의 관심은 더욱 더 높아지고 있다. 서비스의 안정성과 비밀성을 보장하기 위하여 불법적인 사용자로부터 데이터나 자원을 보호하는 것이 필요하게 되었으며, 데이터나 자원의 불법적인 사용을 막기 위해서는 프로토콜에 보안 서비스를 추가하여 사용하므로 사용자의 정당성을 검증하고 데이터의 유출을 막을 수가 있다.

본 논문에서는 IETF에서 레이블 스위치를 제어하기 위해 표준화가 진행 중에 있는 GSMP(General Switch Management Protocol) 프로토콜에 암호학적 방법으로 레이블 스위치의 안정적인 제어를 통하여 자원을 관리할 수 있도록 하려고 한다. 레이블 스위치는 프레임 또는 셀 스위치로 셀 또는 프레임에 있는 레이블을 이용하여 연결형 스위칭을 지원하는 스위치이다. 현재 IETF에서 정의되어 있는 GSMP 프로토콜의 보안 서비스는 GSMP 패킷 encapsulation 방법에 의존하고 있다[2]. 본 논문에서는 이런 encapsulation 의존적인 보안 서비스를 GSMP 프로토콜의 일부분으로 수용하여 독립적인 보안 서비스를 제공하고자 한다.

본 논문의 2장에서는 보안과 GSMP 연구 동향에 대하여 고찰을 하고 3장에서는 GSMP 프로토콜의 보안에 관하여 제안하며, 4장에서 결론과 앞으로의 연구과제에 대하여 살펴 볼 것이다.

2. 보안과 GSMP 연구 동향

네트워크 상에서 여러 가지 보안 위협과 공격이 가능하다. 이런 위협은 도청을 통한 통신의 보안을 침해하고 불법적인 정보의 변조를 통해 수신자를 혼란시키고 위장을 통해 제3자의 신원으로 송신자나 수신자 모두를 속이거나 메시지의 생성이나 삭제로 네트워크의 접근을 막아 DOS(Denial of Service)를 초래하는 것이다. 이런 위협을 막기 위해서 정보의 기밀성, 무결성, 인증과 같은 보안 서비스가 필요하다[1][3].

정보의 기밀성 서비스는 원래의 정보를 읽을 수

있는 올바른 키를 가진 사용자만 허락하는 키 종속 암호화 기능을 사용해 정보를 전송하여 정보의 허가되지 않은 공개를 막는데 필요한 서비스이며, 정보의 무결성 서비스는 제3자에 의해 메시지의 삽입이나 삭제, 재생에 대한 공격을 찾아 정보의 변조를 발견하는데 유용한 서비스이다. 인증 서비스는 위장 공격에서 공격자가 다른 사용자로 가장하고 권한을 얻어 허가되지 않은 정보나 자원에 접근하는 것을 막는데 사용되는 서비스이다. 데이터 원본 인증은 메시지가 주장하는 자원으로 원본이라는 것을 증명하는데 사용된다[4][5][6].

<표 1> GSMP 메시지

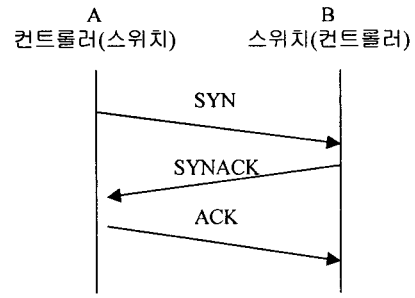
기능	메시지
동기화	Adjacency
연결관리	Add Branch Delete Tree/Branch Delete All Input/Output Port Move Input/Output Branch Report Connection State Reservation Request Delete Reservation Delete All Reservation
구성관리	Switch Configuration Port Management All Port Configuration Label Range Service Configuration
장애관리	Port Up/Down Invalid Label New Port Dead Port Adjacency Update
성능관리	Connection Activity Port Statistics Connection Statistics

GSMP 프로토콜은 레이블 스위치를 관리 운영하기 위해 제안된 프로토콜로써 연결 관리, 구성 관리, 장애 관리, 성능 관리 기능 및 동기화 기능을 갖는 프로토콜이다. 연결 관리 기능은 컨트롤러가 스위치에 연결을 설정하고, 삭제, 수정 및 확인하는데 사용되는 기능을 수행하고, 구성 관리 기능은 컨트롤러가 스위치의 가용성을 확인하고 사용할 수 있게 하는 기능을 수행한다. 장애 관리 기능은 비동기적인 이벤트가 발생하면 스위치가 컨트롤러에게 알리는 기능을 수행하며, 성능 관리 기능은 컨트롤러가 스위치의 포트, 연결, QoS에 대한 통계정보의 검색과 유지 보수 기능을 수행한다. 연결, 구성, 장애, 성능 관리 기능은 컨트롤러와 레이블 스위치 사이에 마스트/슬래이브의 관계를 갖는 비대칭성 방식으로 동작한다. 대칭성 방식으로 동작하는 동기화 기능은 컨트롤러와 스위치 사이의 링크에 대한 상태의 동기화를 유지시킨다[2]. GSMP 프로토콜에 정의되어 있는 각 기능별 메시지는 <표 1>과 같다.

3. GSMP 보안

컨트롤러와 스위치사이의 링크 상태에 대한 동기화를 설정하기 위해서 Adjacency 메시지를 주고받게 된다. 동기화 기능은 비대칭적으로 수행되므로 (그림 1)과 같이 컨트롤러와 스위치 모두가 A또는 B의 역할을 수행할 수 있다. 동기화의 세부 기능은 Adjacency 메시지의 코드필드에 동기화 요구(SYN), 동기화 응답(SYNACK), 응답(ACK) 그리고 리셋응답(RSTACK)로 정의된다.

먼저 송신자 A가 수신자 B에게 동기화 요구(SYN) 메시지를 보내고 수신자 B는 다시 동기화 요구(SYN) 메시지에 대한 동기화 응답(SYNACK) 메시지를 송신자 A에게 보낸다. 그리고 A가 B에게 응답(ACK)을 보냄으로 컨트롤러와 스위치사이에 동기화가 설정된다. 동기화가 설정이 된 후에 컨트롤러는 GSMP 메시지를 이용하여 스위치를 제어하게 된다.

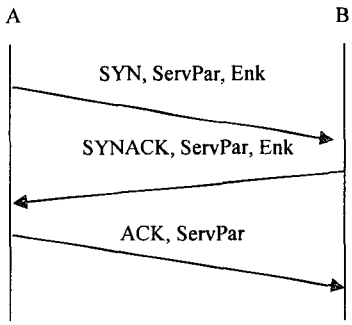


(그림 1) 동기화 설정 절차

본 논문에서는 이 동기화 과정에서 Adjacency 메시지에 보안 서비스를 위한 IE(Information

Element)들을 추가하고 GSMP 프로토콜에 보안 서비스를 제공하여 컨트롤러와 스위치간의 안정된 제어 통신을 수행하려고 한다. GSMP 보안을 위한 정보교환 및 협상절차는 (그림 2)와 같다.

먼저 송신자 A는 수신자 B에게 선택 가능한 보안 서비스에 대한 서비스 파라미터와 A가 생성한 암호화키를 동기화 요구(SYN) 메시지와 함께 보낸다. 수신자 B는 송신자 A에게서 받은 메시지에서 가능한 보안 서비스를 선택하여 송신자 A에게 자신이 선택한 보안 서비스 파라미터와 자신이 생성한 암호화키를 동기화 응답(SYNACK) 메시지와 함께 보낸다. A는 B에게서 받은 메시지에서 B가 선택한 서비스에 대한 가능 여부와 함께 B에게 응답(ACK) 메시지를 보내어 보안협상 완료 및 동기화가 설정된다.



ServPar : 서비스 파라미터{AuthPar, ConfPar, IntePar}
Enk : 암호화 키

(그림 2) 보안 협상 및 동기화 과정

동기화 과정에서 사용한 ServPar 파라미터는 인증 서비스, 무결성 서비스, 기밀성 서비스를 위해 다음과 같이 구성되어 있다. 송신자가 동기화 요구 메시지와 함께 보내는 서비스 파라미터에서 AuthPar 파라미터는 메시지를 인증하기 위해 사용될 암호화 알고리즘의 리스트를 나타내고, ConfPar 파라미터는 메시지의 기밀성을 보장하기 위하기 위해 사용될 암호화 알고리즘의 리스트를 나타낸다. 그리고 IntePar 파라미터는 메시시의 무결성을 보장하기 위해 사용될 암호화 알고리즘의 리스트를 나타낸다. 수신자가 동기화 응답 메시지와 함께 보내는 서비스 파라미터에는 수신자가 선택한 각 서비스에 대한 암호화 알고리즘을 나타낸다. 그리고 응답 메시지와 함께 보내는 서비스 파라미터에는 서비스를 확인하기 위해 선택된 암호화 알고리즘을 다시 보내게 된다. 암호화 알고리즘에서 사용될 암호화키는 키 분배 알고리즘에 의해서 A가 발생한 암호화키와 B가 발생한 암호화키를 조합하여 사용하게 된다. 보안 서비스를 위해 선택된 암호화 알고리즘에 따라 송신자는 GSMP 메시지를 암호화하여 전송하고, 수신자는 암호화된 메시지를 수신하여 선택된 암호화 알고리즘으로 복호화 및 검증을 실행한다. 검증된 메시지에 대해서는 적절한 대응을 하고 검증되지 않는 메시지에 대해서는 폐기를 하게될 것이다.

4. 결론

본 논문에서 레이블 스위치를 관리하기 위한 GSMP 프로토콜에 메시지 인증, 메시지 기밀성, 메시지 무결성과 같은 보안 서비스를 추가해 보았다. GSMP 프로토콜에 보안 서비스를 추가함으로써 패킷 encapsulation과는 독립적으로 보안 서비스를 제공할 수 있게 되었으며, GSMP 프로토콜에 대한 추가적인 보안 서비스로 인해 보다 안정적인 레이블 스위치 관리가 이루어질 수 있다. 이로 인해 자원의 불법적인 사용을 방지하여 서비스의 품질을 높일 수 있다. 다시 말해 이러한 보안 서비스는 예상 가능한 공격과 위협으로부터 메시지를 보호할 수 있게 되며, 잘못된 라우팅으로 인하여 의외적인 메시지 노출시에도 메시지 자체가 암호화되어 있으므로 메시지 내용에 대한 안전성을 보장할 수 있을 것이다.

본 연구에 따른 향후의 연구과제 및 방향은 GSMP 프로토콜에 여러 가지 암호화 알고리즘들을 적용해보고, GSMP 보안 서비스를 위해 가장 효율적인 알고리즘으로 제안된 보안 서비스를 추가하여 실제 GSMP 프로토콜을 구현하는 것이다.

참고 문헌

[1] ATM Forum, "ATM Security Specification Version 1.0," AF-SEC-0100.000, ATM Forum. Feb. 1999.

[2] IETF, "General Switch Management Protocol V3," draft-ietf-gsmp-05, 2000.

[3] Sanjeev Rampal, Cliff X. Wang, "Security Analysis of the MPOA Protocol,", Proceedings of the IEEE Southeastcon '99, Mar. 1999

[4] V. Varadharajan, R. Shankaran, M. Hitchens, " On the design of secure ATM network,"

Computer Communications V.22 N.15-16 , Sep. 1999

[5] Danai Patiyoot, S. J. Shepherd, "Security Issues in ATM Networks,", Operating Systems Review ,V.33 N.4, Oct. 1999

[6] 한치문, 김기현, 김홍근, "ATM Network Security 기술과 데이터 보호방법," 한국정보보호학회지, Nov. 1999.