OBS 기반 광 네트워크에서 정보보호 프로토콜 설계

김수현* · 노선식** · 안정철*

A design of the security protocol in Optical Burst Switching Networks

Soo-hyeon Kim* · Sik-sun No** · Joung-chol Ahn*

요 약

인터넷 사용자의 증가에 따른 데이터 수요와 트래픽 증가에 따라 오늘날의 네트워크는 빠른 전송 속도와 넓은 대역폭을 요구한다. OBS 기반 광 네트워크는 이러한 요구사항을 만족시킬 수 있는 방안으로 활발히 연구가 진행되고 있으나, 도청, 위장, DoS 등의 보안 위협에 취약하다. 본 논문에서는 OBS 기반 광 네트워크에서 존재하는 보안 취약점 및 보안 공격을 분석하며, 이를 기반으로 안전한 서비스 제공을 위해 인증 및 키 분배 가능한 정보보호 프로토콜을 제시한다. 본 논문에서는 OBS 기반 광 네트워크에서 보안 기능을 강화하기 위해 제어 메시지를 이용하여 명시적 인증을 제공하며, 공통키값을 이용하여 제어 메시지를 보호한다.

ABSTRACT

With the expansion of service over the internet, the recent network demands the amount of the more bandwidth and fast transfer rate. Optical Burst Switching has considered as a promising solution for supporting high-speed Internet Service. Because of OBS architecture, it has the security threats such as eavesdropping, masquerading, denial of service and so on. In this paper, We analyze OBS-specific security threats and requirement for supporting security protocol n OBS networks. We propose an authentication and key exchange protocol for supporting the security service. This protocol supports explicit key authentication by using the control messages and protects the control message by using the session key.

키워드

OBS, 보안 취약성, 보안 위협, 인증, 키교환

Ⅰ. 서 론

현재 인터넷을 통한 멀티미디어 전송이 폭발적으로 증가함에 따라 넓은 대역폭에 대한 사용자의 요구가 증가하고 있다. 따라서 이러한 요구의 수용 방안으로 광 네트워크를 코어망으로 하는 차세대 인터넷 망이 주목받고 있다.

광 인터넷 인프라 구축을 위해 제안된 스위칭 기술에는 광 서킷 스위칭(OCS: Optical Circuit Switching), 광 패킷 스위칭(OPS: Optical Packet Switching), 그리고 광 버스트 스위칭(OBS: Opti cal Burst Switching)이 있다. OBS는 OCS의 긴 세션 시간으로 인해서 발생하는 효율성 저하와, 느린 광 스위칭 시간과 광 형태의 버퍼 문제로 인한 OPS의 단점을 보완한 기술로써 국내외적

* 국가보안기술연구소
** 광주대학교

접수일자 : 2005. 10. 28

으로 많은 관심을 받고 있다.

OBS 기반 광 네트워크에서는 IP 등의 패킷을 어셈블한 데이터 버스트를 전송하기 위해 제어 패킷을 생성한다. 제어 패킷(BCP: Burst Control Packet)은 Offset Time, 레이블, 파장, 버스트 길이 등의 정보를 포함하며 데이터 버스트 보다 Offset 시간만큼 먼저 별도의 채널을 통하여 전송된다. 따라서 OBS 기반 광 인터넷은 효과적인 네트워크 자원의 공유, 고속의 데이터 전송이 가능하다.

그러나 이러한 제어 패킷의 송신자 인증 정보 및 메시지의 무결성 결함으로 인해 OBS 네트워크는 스푸핑 및 재전송, DoS, 위장 공격등에 노출되어 있다. 또한 데이터 버스트가 전송될 때 공격자는 빠른 데이터 전송과 낮은 BER을 갖는 광소자의 구조적 특징을 이용하여 트래픽 분석, 도청, 서비스 거부, QoS 저하 등의 공격을 행할 수 있다.

본 논문에서는 OBS 기반 광 네트워크에서 존재하는 보안 취약점 및 보안 공격을 분석하며, 안전한 서비스 제공을 위해 OBS 망에서 인증 및 키를 할당, 분배 가능한 정보호호 프로토콜을 제시한다. 본 논문에서는 제어 패킷을 이용하여, 명시적 인증을 제공하는 공개키 기반 인증/ 키교환 프로토콜을 제안한다. 각 OBS 노드는 제어 패킷를 통해 설정된 세션키 값을 이용하여 버스트에 관한 정보를 암호화 하여 전송함으로써, 도청등의 공격을 방지 할 수 있으며, 인증 서비스를 위한 추가적인 메시지를 최소화함으로써 대역폭 낭비를 방지 할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서 OBS 기반 광 네트워크에 대하여 기술하고, 3장에서 OBS 기반 광 네트워크에서 보안 취약점에 대하여 기술한다. 4장에서는 보안성 강화를 위한 인증 및 키교환 프로토콜을 제시한다.

Ⅱ. OBS 기반 광 네트워크

OBS 기반 광 네트워크는 IP 도메인과 Optical 도메인을 인터페이스 시켜주는 에지 라우터와 Optical 도메인에서의 데이터 버스트 전송을 담당하는 코어 라우터들로 구성된다. OBS 기반 광 네트워크에서 전송 채널은 제어 패킷(Burst Control Packet:BCP) 전송을 위한 제어 플레인의 신호 패킷 채널 그룹(Control Packet Channel Group: CCG)과 데이터 버스트 전송을 위한 데이터 플레인의 데이터 버스트 채널 그룹(Data Burst Channel Group: DCG)으로 구분된다. (그림 1)은 OBS기반 광 네트워크의 구조를 나타낸다.[1,2]

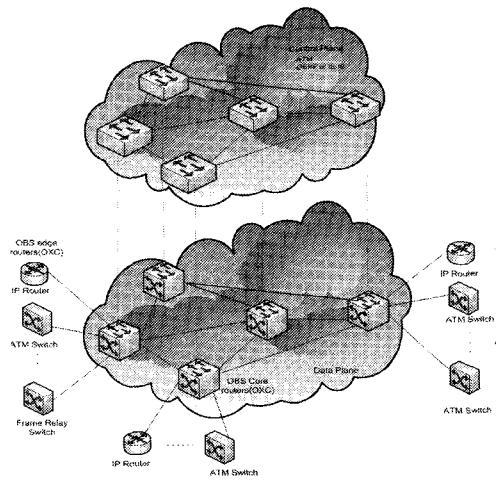

그림 1. OBS 기반 광 네트워크의 구조
Fig. 1 Architecture of Optical Burst switching networks

OBS망에서는 기존의 광 전송망이 광전변환을 통해 데이터를 전송함으로써 전송지연이 발생하는 단점을 보완하기 위해 데이터 버스트 채널 그룹을 통해 전송되는 데이터 버스트는 광전변환없이 목적지 노드에 도달할 수 있도록한다. 이를 위해 필요한 제어 신호는 제어 채널 그룹을 통해 제어 패킷으로 전송된다. OBS망을 구성하는 각 라우터들은 제어 패킷을 수신하여 패킷 정보에 따라 데이터 채널을 스위칭 한다. 따라서 각 라우터는 데이터 버스트가 도착하기 이전에 데이터 버스트에 대한 채널을 미리 스위칭해야 하는데, 이때 제어 패킷의 도착 시간과 데이터 버스트의 도착 시간과의 차이를 Offset Time이라고 한다.

IP 도메인의 IP 라우터로터 IP패킷이 OBS 망의 입력 에지 라우터에 Legacy 네트워크 인터페이스를 통하여 도착하면 입력 에지 라우터는 다수의 IP 패킷을 모아 데이터 버스트를 형성한다. 데이터 버스트가 생성되면 이를 위한 제어 패킷(BCP)를 생성한다. 제어 패킷은 Offset Time, 레이블, 파장, 버스트 길이 등의 정보를 포함하여 데이터 버스트 보다 Offset Time 만큼

먼저 제어 플레인의 CCG 채널을 통하여 전송된다. 제어 패킷 생성 과정에서 라우팅, 레이블 할당, 파장 할당 및 파장스케줄링이 수행된다. 데이터 버스트는 Offset Time 만큼 대기한 후 제어 패킷이 설정해 놓은 경로를 따라 DCG채널을 통하여 전송된다. (그림 2)는 OBS에서 광 전송 경로를 설정하는 과정을 나타낸다. [1,2]

Ⅲ. OBS 기반 광 네트워크에서의 보안 취약점

OBS 네트워크에서 별도의 신호 패킷 채널 그룹(CCG)을 통해 제어 패킷이 전송되며, 데이터 버스트 채널 그룹(DCG)을 통해 데이터 버스트가 전송된다. OBS 네트워크는 각 채널 그룹 특성에 의해서 다음과 같은 보안 취약점 및 공격이 존재한다. [3,4]

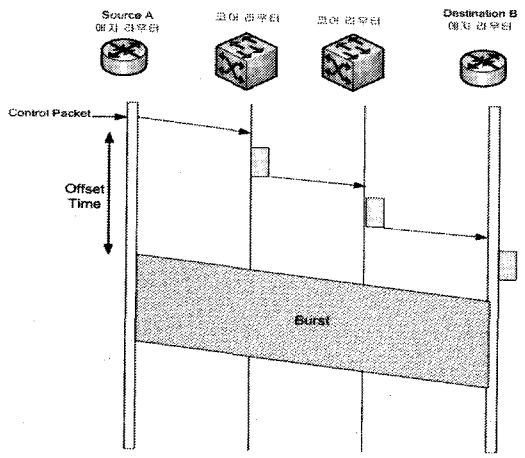

그림 2. 광 전송 경로 설정 과정
Fig, 2 Set up of optical connection

3.1. 신호패킷 채널 그룹에서의 보안 취약점

제어 패킷은 라우터/스위치와 라우터/스위치 간에는 신호 패킷 채널을 통해 광신호로 전송된다. 따라서 다음과 같은 공격이 가능하다.

- 신호대역내 전파 방해 : 공격자는 수신자로 하여금 전송된 데이터를 정확하게 해석하지 못하게 하기 위하여 신호대역내 전파 방해 신호를 삽입하여 공격할 수 있다.
- 신호대역외 전파방해 : 공격자는 위조된 신호를 삽입하거나 교차 변조 효과를 이용하여 통신 신호에 약하게 하여 서비스를 제공하지 못하도록 공격할 수 있다.
- 도청: 공격자는 인접 신호로부터 유도되는 교차 크로스토크를 수신하거나 공유자원의 분기를 이용하여 허가없이 정보를 수신할 수 있다.

  또한 제어 패킷은 경로를 구성하는 라우터/스위치에서 목적지까지 다음 경로를 설정하고 데이터 버스트에 대한 라우터/스위칭 테이블을 변경하기 위해 광전변환을 통해 전기적인 신호로 변환된다. 이러한 변환 과정 및 제어 패킷을 해독하는 과정에서 다음과 같은 공격이 가능하다.
- 인증되지 않은 제어 패킷: 제어 패킷은 송신자 인증 정보를 제공하지 않으므로 공격자는 스푸핑 공격을 위해 제어 패킷에 액세스 할 수 있다.
- 데이터 변조(Data Integrity): 제어 패킷은 무결성을 제공하지 않으므로 공격자는 제어 패킷의 데이터 내용을 변조하거나 제거 할 수 있다.
- 트래픽 분석: 제어 패킷은 버스트 길이와 라우팅, 파장과 같은 정보를 포함하고 있다. 공격자는 제어 패킷을 스푸핑하여 네트워크 트래픽의 특성, 파장 할당 정보, 패킷 사이즈 등을 분석할 수 있다.
- DOS(Denial of Service) 공격: 광 전송 경로는 제어 패킷을 이용하여 설정된다. 공격자가 위장하여 제어 패킷을 가로채어 파장을 선점하게 되면 데이터 버스트 서비스를 방해하게 된다.
- 라우팅 프로토콜 공격 : 효율적인 패킷 라우팅을 위해서 OBS 네트워크는 MPLS(Multiple Protocol Label Switching), deflection routing과 같은 다양한 라우팅 프로토콜을 이용한다. 다음 홉을 결정하기 위해서 빠른 테이블 룩업 알고리즘을 이용하며, 제어 패킷은 IP 네트워크와 같은 홉 바이 홉 기반 라우팅을 통해 전송된다. 공격자는 DOS 공격이나 위장을 통해 라우팅 프로토콜 동작을 방해 가능하다.

3.2. 데이터 버스트 채널 그룹 보안 취약점

데이터 버스트는 Offset Time 동안 IP 계층의 버퍼를 이용하여 대기 후 신호 패킷에 의해 설정된 광전송

경로에 전송된다. 광 네트워크에 사용되는 광 전송 시스템은 매우 빠른 데이터율와 낮은 비트 에러율에 인해 서비스 거부 공격이 가능하다. 따라서 데이터 버스트 채널은 광 소자[3]에 의해 발생할 수 있는 아래와 같은 보안 공격이 가능하다.

- 트래픽 분석 및 도청: 공격자는 수동적으로 네트워크의 트래픽을 분석할 수 있다.
- 서비스 거부 : 광 신호는 공격자에 의해 절취될 수 되어 서비스를 방해할 수 있다.
- QoS 감소 : 공격자는 광 신호를 공격하여 광 신호의 전송을 방해하여 QoS를 감소시킬 수 있다.

또한 라우터와 스위치에 사용되는 WSS (Wave length Selective Swithes)는 크로스 토크(Cross talk)에 취약하며 각 Amplifier는 spora dic 공격에 취약하다.

광 네트워크는 대용량의 다양한 포맷의 데이터를 빠른 속도 및 투명하게(Transparency)전송할 수 있다. 따라서 (그림 3)에서 나타난 바와 같이 이러한 특성으로 인해 망에 가해진 공격이 빠르게 전파될 수 있다.

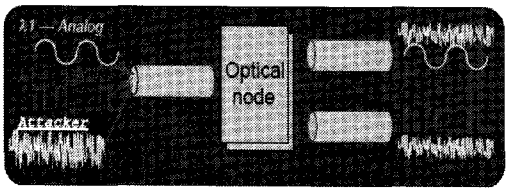

그림 3. 데이터 버스트 채널 공격
Fig. 3 Attack of Data Burst Channel

Ⅳ. 인증 및 키교환 프로토콜

본 논문에서는 3장에서 언급한 보안 취약점 및 보안 공격을 기반으로 안전한 서비스 제공을 위해 인증/키교환 프로토콜을 제안한다. 인증 및 키교환 프로토콜은 아래와 같은 보안 요구 조건을 만족하도록 설계되어야 한다.

4.1. 보안 요구사항

1) OBS 프로토콜과의 호환성

OBS 기반 네트워크망의 구성요소를 변경하지 않고 최소한의 비용으로 보안 서비스를 제공해야 한다.

2) 상호 개체 인증

통신에 참여하고 있는 두 개체가 서로 상대방의 신분을 확인하는 과정으로 서로 다른 개체에 대한 위장(masquerade)을 방지하기 위하여 요구된다.

3) 공개키 인증서의 상호 교환

모든 공개키 기반 인증 및 키 설정 프로토콜을 지원하기 위해서 사용된 공개키의 정당성에 대한 확인 과정이 반드시 필요하다. 이를 해결하기 위한 방법으로 공개키 인증서를 상호 교환해야 하며 공개키 인증서는 인증된 기관에서 발급받아야 한다.

4) 세션키에 대한 상호 동의 및 제어

OBS 노드는 상대방과 자신의 정보 모두를 사용하여 각각 세션키를 생성하여야 한다. 다른 한 개체가 우연히 또는 고의적으로 약한키를 선택하는 것을 방지하기 위해 각각의 OBS 노드의 정보는 세션키에 영향을 미치는 정도가 동일하여야 한다.

5) 키 인증(key authentication)

함축적 키 인증: 통신에 참여하지 않는 다른 개체가 설정된 세션키를 얻을 수 없도록 하기 위해 대응되는 키가 가능한 한 참여하는 개체만이 계산할 수 있어야 한다.

명확한 키 인증: 대응되는 키를 가능한 한 참여하는 개체만이 계산할 수 있어야 하고 실제로도 계산되어야 한다.

6) 키 신규성에 대한 상호 확신

이전 메시지의 재사용으로 이전의 키를 재 설정하는 것 (replay attack)을 방지해야 한다.

7) 사용자 신분의 기밀성

사용자의 신분을 추적하기 위해 주고 받는 데이터가 가로채임을 당하는 것을 방지하기 위해서 주고 받는 데이터를 암호화해서 보내야 한다.

8) 알려진 키 비밀성 (Known Key Secrecy)

이전 세션키를 사용하여 새로운 세션키를 만들 수 없어야 한다.

9) 키노출 위장에 대한 안전성 보장

한 사용자의 개인키가 노출되었을 때, 그 값을 아는 공격자가 해당 사용자에게 임의의 타인으로 위장할 수 없어야 한다.

10) 부인 봉쇄(non-repudiation)

중요한 데이터나 키 전송 관련된 부인할 수 없는 증거가 보장되어야 한다.

11) 대역폭 사용의 효율화

프로토콜 메시지를 가능한 짧게 유지해야 한다.

12) 연산 부하의 최소화

키 생성하는데 걸리는 연산 부하를 최소화해야 한다.

4.2. 인증 및 키교환 프로토콜 설계

본 논문에서는 제어 패킷을 이용하여, OBS 네트워크에서 명시적 인증을 제공하는 공개키 기반 프로토콜을 제안한다.

OBS 노드 각각은 자신의 인증서 및 각 링크에 연결된 상대방의 노드 인증서를 가지고 있으며, 인증서의 초기 발급은 신뢰기관(Trusted Third Party)에 의존한다고 가정한다. 인증서에 대한 검증은 별도의 인증서버(Authentication Server)를 두고 인증과정 중에 온라인으로 접속하여 수행하거나, 초기 장비 설치시 인증서를 검증하기 위한 별도의 프로그램 및 키를 오프라인으로 주입할 수 있다.

공개 키를 이용하여 세션키 생성을 위한 키교환 프로토콜은 Diffie-Hellman 또는 RSA가 가장 널리 사용되었지만, Diffie-Hellman은 응답 공격(reply attack)에 취약한 단점을 갖고 있으며 RSA (Rivest-Shamir-Adleman)는 강도를 향상시키기 위하여 키의 길이를 증가시켜 고속망에 사용하기에는 부적합하다. 이에 대한 대안으로 ECC (Ellptic Curve Cryptography)가 사용될 수 있으며, ECC는 RSA에 비해 작은 비트 크기로 RSA와 동등한 안전성을 제공함으로써 오버헤드를 줄일 수 있다. 따라서 본 논문에서는 세션키 생성을 위해 (그림 4)와 같이 ECC 상에서의 Diffie-Hellman을 변형한 키교환 프로토콜을 이용하며 사용되는 기호는 다음과 같다.

- P_A, P_B : A와 B의 공개키
  $P_A=S_A \times G$, $P_B=S_B \times G$
- S_A, S_B : A와 B의 비밀키
- n : 매우 큰 솟수 값(prime number)
- nA,nB : n 보다 작은 랜덤 정수(random number)
- O : 덧셈에 대한 항등원
- G : nG = O를 만족하는 유한체 타원곡선의 가장 작은 값
- K_{AB} : A,B 구간에서 A,B가 제어 패킷의 암복호에 사용하는 공통키
- KBC: : B,C 구간에서 B,C가 제어 패킷의 암복호에 사용하는 공통키
- *Info* : 제어 패킷의 Offset Time, 레이블, 파장, 버스트 길이 정보

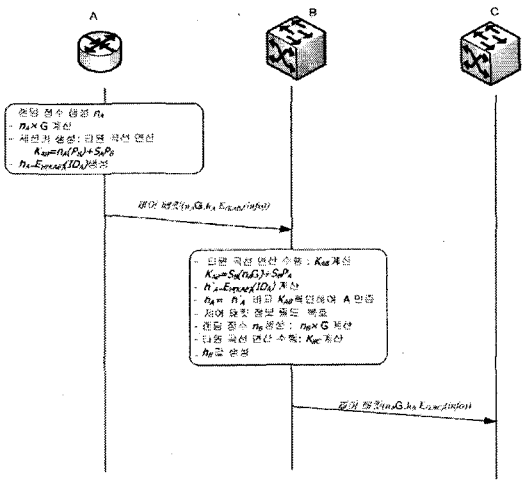

그림 4. 세션키 생성 및 교환 절차
Fig. 4 Session Key Generation and Exchange

먼저 유한체 위의 타원곡선을 선정하고, 임의의 큰 솟수 n를 선택한다. 공개키 연산을 위하여 $nG = O$를 만족하는 생성자 G를 계산한다. A는 랜덤한 정수 n_A를 생성하여 세션키 생성을 위한 n_AG를 계산한다. A는 타원곡선연산 $k_{AB}=n_A(P_B) + S_A(P_B)$ 수행하여 세션키를 생성한다. A는 자신의 ID_A 정보를 계산한 세션키로 해쉬함수를 이용하여 $h_A=E_{h(KAB)}(ID_A)$ 값을 생성한다.

A는 생성한 세션키 k_{AB}를 이용하여 제어 패킷의 정보 필드를 암호화하며 n_AG,h_A 값을 포함하여 제어 패킷을 전송한다. 패킷을 전송받은 B는 타원곡선연산 $k_{AB}=S_B(n_AG)+S_BP_A$ 수행하여 k_{AB}를 생성한다 . $h_A'=E_{h(KAB)}(ID_A)$를 계산하여 h_A와 h_A' 값의 동일 여부를 확인한다. 동일하면 A를 인증하고 전송받은 제어 패킷의 정보를 복호화한다.

B는 B의 제어 메시지의 전송을 위해 난수 n_B를 생성하여 타원 곡선 연산을 수행하여 세션키 $K_{BC:}$ 및 h_B값을 생성한다. 제어 패킷의 정보 필드를 암호화 한 후 전송한다.

V. 결 론

OBS는 Offset Time과 Delayed Reservation를 이용하여 빠른 전송 경로의 설정이 가능하고 네트워크 자원을 효율적으로 공유할 수 있는 장점이 있으나 도청, 위장, DoS 등의 보안 위협에 취약하다.

본 논문에서는 OBS 기반 광 네트워크 망에서보안 취약성 및 보안 요구사항을 분석하고 인증 및 키교환 프로토콜을 설계하였다.

제안된 인증/키교환 프로토콜은 공개키 기반 키교환을 통해 세션키를 생성하는 하이브리드 프로토콜로써 공개키와 랜덤 정수를 이용하여 ECC기반 세션키를 생성한다. 또한 키 생성자에 대한 인증을 제공하기 위해 자신의 ID 정보를 암호화 하여 전송한다. 인증 서비스를 위한 추가적인 메시지를 최소화함으로써 대역폭 낭비를 방지 할 수 있다.

참고문헌

[1] Y.Chen, C. Qiao," Optical Burst Switching- A new area in Optical Networking Research", IEEE Network, 2004.3

[2] Battestilli, H.Perros,"An Introduction to Optical Burst Switching," IEEE commuication megazine, 2003.8

[3] R.Rejeb,I.Pavlosoglous,M.S.Leeson and R.J.Gr een, "Securing All Optical Networks", ICTON 2003

[4] Simon Blake-Wilson, Don Johnson,"Key Agree ment Protocols and their Security An alysis," 6th IMA Conference on Cryptography and Coding, LNCS1355, 1997

저자소개

김수현(Soo-Hyeon Kim)

1999년 전북대학교 정보통신공학과 공학사
2001년 전북대학교 컴퓨터공학과 공학석사
2001～현재 국가보안기술연구소 연구원
※관심분야 : 네트워크보안, 광 네트워크, 무선통신

노선식(Sun-Sik Roh)

1993년 전북대학교 컴퓨터공학과 공학사
1995년 전북대학교 컴퓨터공학과 공학석사
2002년 전북대학교 컴퓨터공학과 공학박사
2002～현재 광주대학교 정보통신학과 교수
※관심분야 : 네트워크보안, 광네트워크, 임베디드시스템

안정철(Joung-Chol Ahn)

1988년 한양대학교 전자공학과 공학사
1990년 전북대학교 전자계산기 공학과 공학석사
1996년 일본동경공업대학 전자물리공학과 공학박사
1996～현재 국가보안기술연구소 팀장
※관심분야 : 무선통신,보안