광케이블 도청 : 방법 및 예방책

M. Zafar Iqbal, Habib Fathallah, Nezih Belhadj

요약 - 광통신은 일반적으로 생각하듯이 안전하지 않다. 감지되는 것을 피하면서 광섬유 링크로부터 정보를 뽑아 내거나 정보를 입사하는 방법들이 알려져 있다. 성공적으로 도청된 광섬유는 감지가 어렵기 때문에 사건이 거의 보고되지 않았다. 본 논문에서 우리는 많은 알려진 광광섬유 도청 방법에 대해 강조한다. 우리는 '굴곡' 방법에 의해 도청된 광섬유의 광학적인 특성에 대한 시뮬레이션과 물리적인 실험과 함께 개념의 증거를 보고한다. 우리는 또한 지략이 있는 도청자가 기존의 기술로 광섬유 링크의 안전을 위태롭게 할 수 있는 시각화된 시나리오를 제시한다. 광섬유 도청을 방지할 수 있는 수단이나 광섬유로부터 도청된 정보의 중요성을 없애는 수단에 대해서도 또한 논의되었다.

색인 용어- 광 광섬유 도청, Layer 2 암호화, 도청, 굴곡 도청.

I. 서 문

일반의 인식과는 반대로, 광광섬유는 도청으로부터 본질적으로 안전하지 않다. 오늘날 광섬유를 통해 전달되는 막대한 량의 임무에 중요하고 민감한 정보가 어떠한 확고하고 지략 있는 도청자에게 노출된다.

광섬유 도청은 정보의 추출이나 정보의 주입에 의해 광 광섬유의 안전이 위태롭게 될 수 있는 과정이다. 기본적으로 광섬유 도청은 침입성 및 비침입성이 될 수 있다. 전자는 광섬유가 절단되어 도청 메커니즘으로 다시 연결되는 것이 필요하고, 후자는 광섬유를 절단하거나 서비스의 방해를 초래하지 않고 도청을 하는 것이다. 비침입성 기술이 본 연구의 초점이다.

도청 과정 자체가 꽤 간단한 반면에 도청된 광섬유를 감지하는 것이 매우 어렵기 때문에 광섬유 도청에 대한 단지 몇 건의 사건만 보고될 수 있다. 도청 사건에 대한 주요한 보고가 아래에 있다:

- 2000, 도이치 텔레콤의 세 개의 주요 간선이 독일 프랑크푸르트 공항에서 누설되었다 [1].

- 2003, 버라이존 광 네트워크에 연결된 불법 도청 장비가 발견되었다 [1].

- 2005, USS 지미 카터 잠수함을 해저 케이블로 도청하기 위해서 특별하게 개조되었다 [2], [3].

아래의 섹션에서 우리는 침입성 및 비침입성 도청 기술에 대한 간략한 개요를 제시한다 [4]. 그리고 나서, 우리는 광섬유 굽힘에 의한 신호 손실에 대한 숫자로 된 시뮬레이션을 제시하고, 우리의 실험실에서 개발된 시험 제작품에서 도청의 물리적인 시연에 대한 보고서를 제시한다.

여기에서 우리는 또한 시험 제작품의 설계, 하드웨어 및 소프트웨어에 대해서 설명한다. 우리는 또한 실제 환경에서 가능한 도청 시나리오를 논의하고 그렇게 하기 위해 필요한 자원을 강조한다.

978-1-4577-1169-5/11/ㄴ26.00

마지막으로 우리는 도청에 대비하여 광 광섬유 링크를 보호하기 위한 몇 가지 해결방안을 제안한다.

II. 광섬유 도청 방법

A. *광섬유 굽힘*

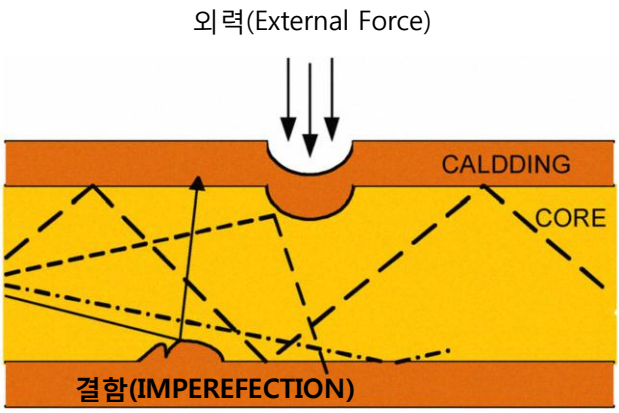
이 방법에서는 굽힘을 위해 케이블을 벗겨서 광섬유로 만든다. 이 방법은 전 반사로 더 잘 설명되는 광 광섬유를 통한 빛의 전달 원리를 이용한다. 이것을 달성하기 위해서 중심부의 피복 인터페이스에서의 빛의 투사각이 전 반사에 대한 임계각보다 더 커야 한다. 그렇지 않으면 어떤 빛은 광섬유의 피복을 통해서 광섬유 밖으로 방사될 것이다. 임계각은 중심부 및 피복의 굴절률의 함수이고 아래의 방정식으로 표시된다:

$\theta c = Cos\ -1\ (\mu_{피복} / \mu_{중심부})$ $(단, \mu_{cl} < \mu_c)$

광섬유 굽힘 기술에서 광섬유는 구부려져서 투사각이 임계각보다 작아져서 빛이 방사된다. 명백하게 추가적인 두 가지 유형의 광섬유 굴곡이 있다:

1) 마이크로 벤딩

외력이 가해지면 예리하지만 미세한 굴곡을 초래하고 이것은 수 마이크론의 축 방향 변위와 수 밀리미터의 공간 파장의 변위를 초래한다 (그림 1). 그렇게 방사된 빛은 도청에 사용된다.



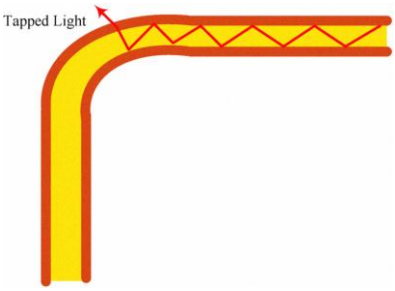
(그림 1). 마이크로 벤딩

2) 매크로 벤딩:

각 광섬유 유형에 관련하여 최소 허용 굴곡 반경이 있다. 더 작은 굴곡 반경은 빛의 방사를 초래할 것이다 (그림 2). 이 특성은 광섬유로부터 빛을 추출해 내는데 이용될 수 있다. 정상적으로, 단일 모드 광 광섬유는 특별히 개발된 유형을 제외하고는 6.5에서 7.5 cm 미만의 굴곡 반경을 허용하지 못할 것이다. 반면에 멀티 모드 광섬유는 3.8cm의 작은 굴곡 반경을 허용할 수 있다.

978-1-4577-1169-5/11/ㄴ26.00

도청된 빛



(그림 2). 매크로 벤딩

B. *광학적 스플릿팅*

광학 신호의 일부를 빼내기 위해서 목표 광섬유가 스플릿터로 삽입된다. 하지만 이 방법은 경보를 발생시키는 광섬유의 절단을 포함하기 때문에 침입성이다. 하지만, 이 유형의 감지되지 않은 도청은 수 년간 지속될 수 있다.

C. *에바네센트 결합*

이것은 목표 광섬유와 리시버 광섬유 각각의 중심부의 가장자리까지 피복을 연마하며 그들을 같이 위치시킴으로써 목표 광섬유로부터 리시버 광섬유로의 신호 포획을 수반한다. 이것은 약간의 신호가 수령 광섬유로 누출되는 것을 허용하게 된다. 하지만, 이 방법은 현장 상황에서 실행하기가 매우 어렵다.

D. *V 홈 절단*

V-홈은 광섬유의 중심부에 가까운 피복에 있는 절단 부분이고, 광섬유 내에서 전달되는 빛과 V-홈의 면 사이의 각도가 임계각보다 더 크다. 피복에서 이동되면서 V-홈에 겹쳐지는 빛의 일부분이 광섬유 밖으로 누출되는 전 반사를 초래한다.

E. *산란*

브래그 격자가 광섬유의 중심부에 식각되어 광섬유 밖으로 약간의 신호가 반사되도록 한다. 이것은 UV 여자기 레이저에 의한 자외선의 겹침과 간섭을 일으킴으로써 이루어진다.

III. 시뮬레이션

A. *방법론:*

SMF -28 광 광섬유에서의 곡률 손실을 정확하게 추산하기 위해서 High-Order Finit Element Method 에 근거한 주파수 도메인에서의 full vectorial Maxwell solver와 스트레칭 PML (완벽히 매치된 레이어) 기술의 수정의 허용이 이용된다. 그래서 전파 상수와 굴절 도파관에서의 모드의

978-1-4577-1169-5/11/ㄴ26.00

전기장의 벡터의 계산이 이루어진다. 곡률 손실은 기본 모드의 전파 상수의 허수 부분으로부터 계산된다. 총 손실은 두 직교 기본 모드의 손실을 더하여 계산된다. 이 방법에 의해 계산된 결과는 매우 정확하고 [5]에서 입증되었다.

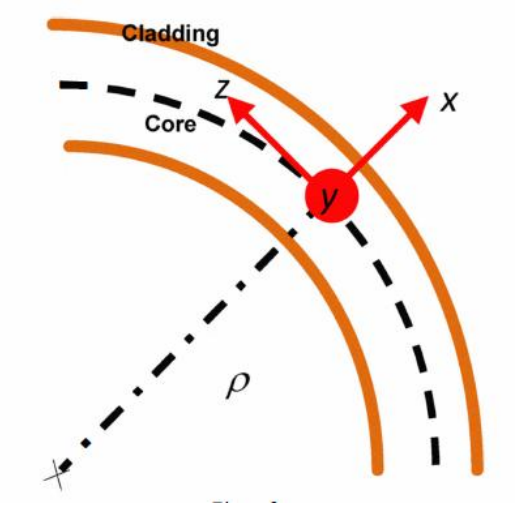
B. *시뮬레이션 데이터:*

SMF-28 광섬유에 대해서, 중심부 반경 및 굴절률은 각각 : rc = 4.15 11m 및 nc=1.4493

여기에서 피복에서는, 그들은 각각 : rei = 62.25 11m 및 ncl=I.444.

공기의 굴절률은 1이다.

그림 3에서 보여지듯이 곡률 반경 p는 x 축을 따른 것이고, 모드는 y축을 따라 분극화되고 전파는 z축을 따라간다.



(그림 3)

C. *파워 손실 계산:*

그림 4는 1 미터 굽힘 광섬유에 대해 숫자로 표시된 추정 곡률 손실을 곡률 반경의 함수로 나타낸다. 손실의 대수 의존성 대 곡률 반경이 관찰되었다. 더 작은 곡률 반경 (p < 10mm)에 대해서, 손실은 40 dB/m를 초과한다. 보다 더 일반적인 곡률 반경 (p> 15mm)에 대해서는 손실은 1 dB/m 미만이다.

IV. 광섬유 도청 실험

A. *광섬유 도청에서의 단계*

전체적인 도청 작업은 아래의 단계로 이루어진다 :

i. 광섬유로부터 광학 신호를 빼내기.

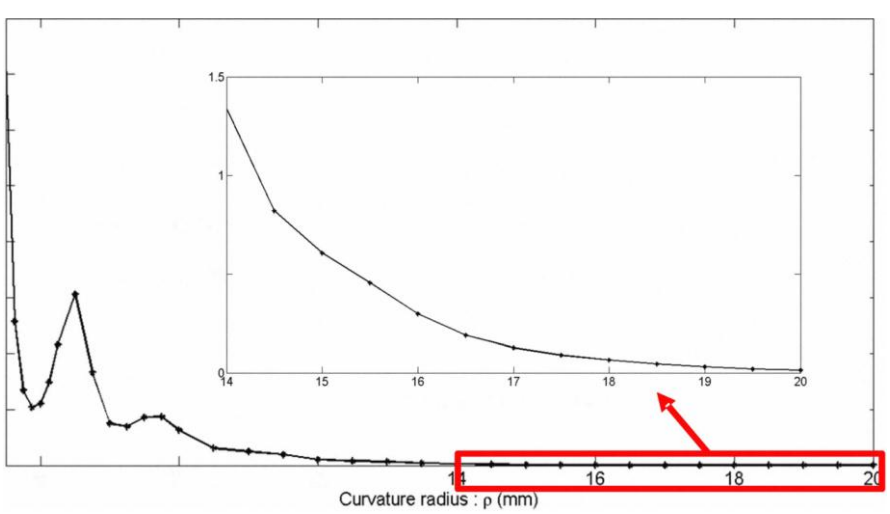
ii. 신호 감지하기.

978-1-4577-1169-5/11/ㄴ26.00

iii. 전송 메커니즘 감지하기 (프로토콜).

IV. 프레임/ 패킷을 감지하기 위한 소프트웨어 처리 및 그것으로부터 원하는 데이터 추출하기.

그 실험은 광학 이더넷을 통하여 비디오를 하나의 컴퓨터에서 다른 컴퓨터로 전송하는 것을 수반하였다. 연결 광섬유는 피복으로 벗겨져서, 기본적으로 총 인터넷 반사의 원리를 위반하는 약간의 빛의 방사를 유도하는 광섬유를 구부리는 "클립 온 커플러"라고 불리는 장치로 눌러진다. 이 장치는 이 포획된 빛을 단방향 이더넷 미디어 컨버터로 보내고 궁극적으로는 이더넷 프레임은 제 3의 PC에서 원래의 비디오 프레임의 사본을 재 구성할 수 있게 처리된다. 우리는 비디오 스트리밍 및 재생을 위해 VLC를 사용하였다. 패킷을 포획하기 위해서 Wire-Shark 프로토콜 분석기 및 포획된 패킷으로부터 비디오 클립핑을 재 구성하기 위해서 'Chaosreader'를 사용하였다.



(그림 4) . 곡률 손실의 수치적 추산을 곡률 반경 함수로 표시

B. *절차*

위에서 언급된 하드웨어 및 소프트웨어는 그림 (5) 에서와 같이 연결된다. 비디오 소스로부터 목적지까지의 방향으로 벗겨진 광섬유 가닥은 클립-온-커플러의 클램프 아래에 놓여진다. 클램프는 눌러져서 약간의 빛 투입을 초래하고 이더넷 프레임을 읽고 Wire-Shark이 설치된 제 3의 PC에 투입하는 단방향 미디어 컨버터를 여장한다. Wire-Shark은 이더넷 프레임을 변환하고 소스와 목적지 MAC 주소와 같은 정보를 제공한다. 그것은 또한 이더넷 프레임 유효 하중을 처리하고 그것으로부터 IP 패킷을 취득한다. 패킷으로부터 취득한 정보는 IP 주소, 시그널링 프로토콜 메시지 및 유효 하중 비트 등을 포함한다. 그렇게 포획된 패킷은 "pcap" (패킷 포획) 형식의 파일에 저장된다. 이 파일은 그 이후에 원본 파일을 재 구성하여 재 구성된 파일의 색인을 생성하는 "chaosreader" 라고 불리는 소프트웨어에 의해 처리된다. 우리의 포획된 비디오에 대해서, 우리는 대용량의 * .DAT 파일에 대한 색인에서 본다. VLC 소프트웨어에서 이 파일을 열면 비디오 스트림의 포획된 부분을 열게 된다.

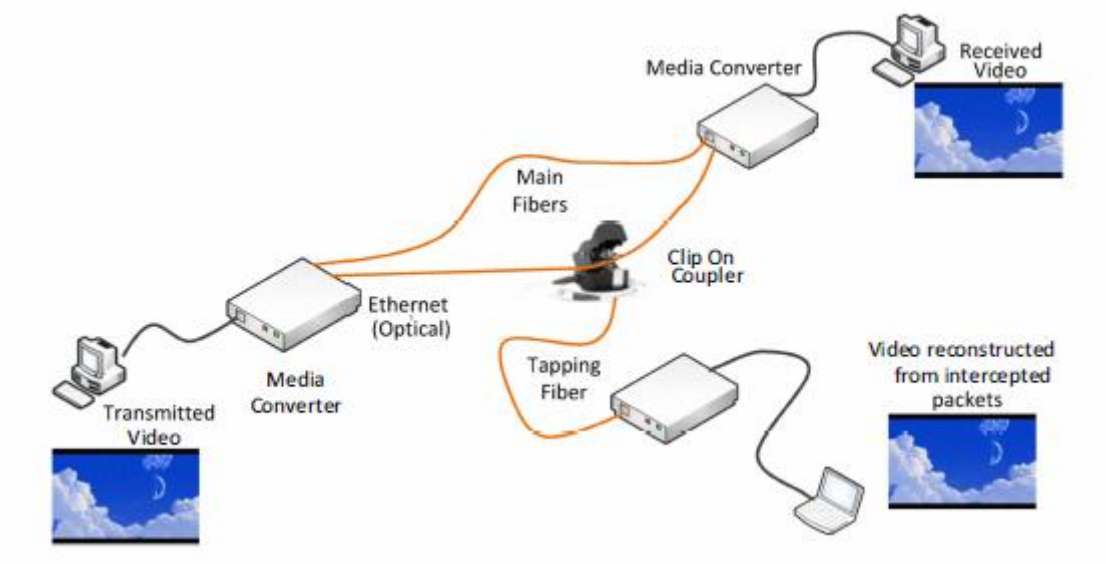
978-1-4577-1169-5/11/ㄴ26.00 ©2011 IEEE

C. *가능한 도청 행위*

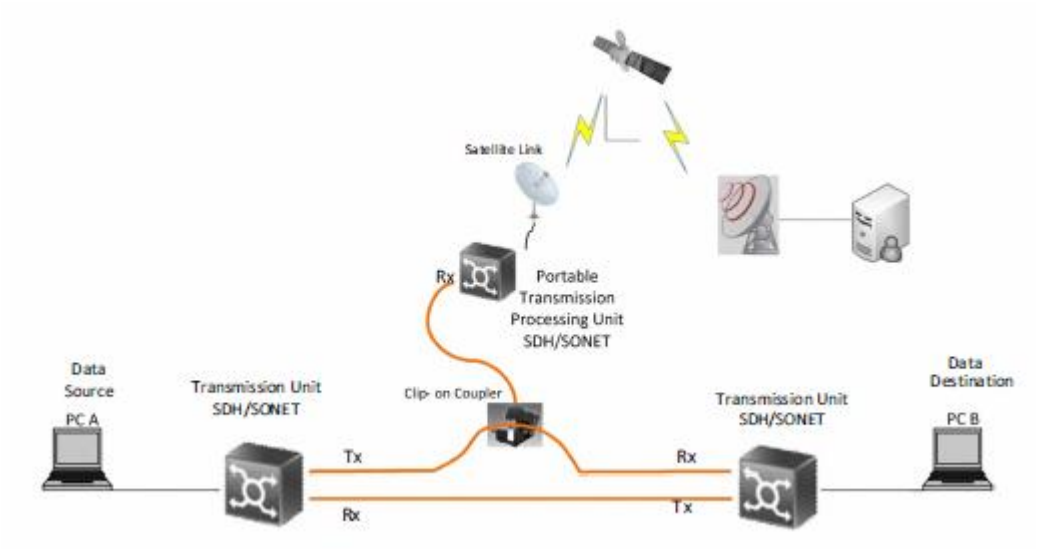
비디오 재생 이외에, 여기에서 설명된 그 실험 설정은 다양한 무료, 상업용 혹은 자체 개발된 소프트웨어를 이용하여 IP 공격, 암호 훔치기, VoIP 전화 청취 및 이메일 재 구성과 같은 많은 도청에 사용될 수 있다.

V. *더 많은 도청 시나리오*

여기에서 보고된 실험은 부속품, 특히 소프트웨어를 쉽게 구할 수 있어서 이더넷 네트워크에서 수행되었다. 하지만, 아래와 같은 여러 가지의 실제적인 도청 시나리오를 상상할 수 있다:



(그림 5). 굽힘 도청을 위한 실험 설정



(그림 6). 원격 처리 시나리오가 있는 도청

978-1-4577-1169-5/11/ㄴ26.00 ©2011 IEEE

A. *도청 전송 네트워크*

두 가지의 가장 많이 쓰이는 장거리 및 메트로 네트워크를 통한 광 광섬유 전송의 표준인 SDH 및 SONET과 같은 전송 네트워크로부터 의미 있는 정보를 얻을 수 있다. 아주 고속의 데이터는 저장되고 처리되기가 힘들지만 첨단의 SDH 프로토콜 분석기는 사용할 수 있어서 저 수준의 지류 신호를얻는데 사용될 수 있다 [6]. 이것은 어느 정도 데이터 속도 문제를 완화한다. 그러한 장치는 네트워크를 통해 흐르는 다양한 유형의 트래픽을 얻기 위해서 더 개발될 수 있다. 예를 들면, 그것은 어떤 VC4 컨테이너 스트림 위에서 맵핑된 이더넷 스트림을 추출할 수 있다.

원격으로 처리된 도청:

두 가지의 중요한 원격 처리에 대한 동기가 있다. (1) 여러 Gbps의 매우 높은 비트 전송률의 장거리 전송 링크를 도청할 때, 저장 용량의 역할이 중요해 진다. 이것은 포획된 패킷이 신속히 하드 디스크를 채울 것이라는 사실 때문이다. (2) 네트워크 포렌식 전문가는 현장에 배치하기에는 너무 귀중한 물자이다. 그들을 현장에 배치될 수 없는 최첨단의 자원이 설치된 어떤 원격 처리 위치에 그들을 배치하는 것이 더 바람직하다. 상상력을 이용하여, 광섬유로부터 빼낸 데이터의 어떠한 원격 처리 시나리오를 쉽게 생각할 수 있다.

1) 무선 이더넷을 이용하기:

Wi-Fi를 이용하여, 도청 랩톱은 다른 방에 있을 수 있고, 혹은 도청기가 설치된 건물 밖의 승합차에도 있을 수 있다. 포렌식 전문가는 더 좋은 자원에 접속할 수 있는 비교적 안전한 위치에서 작업할 수 있다.

2) 마이크로 웨이브/위성 링크 사용하기:

우리의 실험 설정은 방향성 마이크로 웨이브 링크에서 이더넷 트래픽을 맵핑함으로써 수정되었다. (그림 6). 그 처리는 만약 위성 링크가 사용되면 수십 킬로미터나 혹은 심지어 수천 킬로미터 떨어져서도 수행될 수 있다.

3) 신호 주입

우리가 앞에서 설명한 산란법을 이용함으로써, 어떤 종류의 커플링 기술을 이용하여 신호를 광섬유 안으로 주입하는 장치를 제작하는 것이 이론적으로 가능하다. 광섬유를 파손하지 않고 혹은 심지어 악성 정보를 주입하지 않고 광섬유를 채워 넣기 위해서 정교한 기술을 개발할 수 있다.

VI. 도청 방지

아래에서 광섬유 도청을 방지하거나 그 영향을 없애는 세 가지의 기본 범주 및 각각의 하위 범주에 대한 논의가 고려되었다.

978-1-4577-1169-5/11/ㄴ26.00

A. *케이블 감시 및 모니터링*

1) 광섬유 주의의 신호 모니터링 하기

오직 모니터링 신호만 전송하는, 주변에 광섬유가 있는 광케이블을 제작한다. 이 방법을 이용하는 것은 케이블의 원가를 증가시킬 것이지만 그 광섬유를 구부리려는 어떠한 시도가 있으면 모니터링 신호가 손실되게 할 것이고 그 케이블은 경보를 발생시키는 데 사용 되어진다. [7].

2) 전기 전도체:

다른 방법은 전기적 전도체를 정보를 전송하는 광섬유 케이블 속으로 통합하여 넣는 것으로 구성된다. 케이블을 허락 없이 만지면, 전기 전도체들 사이의 정전 용량이 변경되고 이것이 경보를 발생시키는데 사용될 수 있다.

3) 모드의 전력 모니터링

이것은 빛이 전파되는 모드에서 감쇠가 그 모드의 함수가 되는 멀티 모드 광섬유에 적용된다. 도청기는 어떤 모드에 영향을 주고 모든 다른 모드가 영향을 받게 한다. 이것은 에너지가 전도 모드에서 비전도 모드로 재 분배되게 하고 광섬유 중심부 및 피복에서의 전력 분배가 변경된다. 모드의 전력에서의 이 변화는 모드에 포함된 전력을 측정함으로써 리시버 측에서 이용될 수 있고, 도청이 있는지를 결정할 수 있다 [8].

4) 광학적 평균 전력 측정

광섬유는 광학적 평균 전력 수준의 감지에 의해 감시될 수 있다. 주어진 기준 값으로부터의 변화에 의해 경보를 발생시킬 수 있다. 하지만 이것은 광학 신호가 코드화 되어 그것이 그것의 정보 내용과 독립적인 불변 평균 전력을 가져야 할 것을 필요로 한다 [8].

5) OTDR

도청이 광학적 신호의 일부분을 추출하는 것을 수반하기 때문에, 광학적 시간 도메인 반사 미터(OTDR)는 신호 전력의 감소를 보이는 광섬유 흔적 (그림 7) 안에서 위치를 관찰함으로써 도청이 있는지 알아내는데 사용될 수 있다. [8]

978-1-4577-1169-5/11/ㄴ26.00

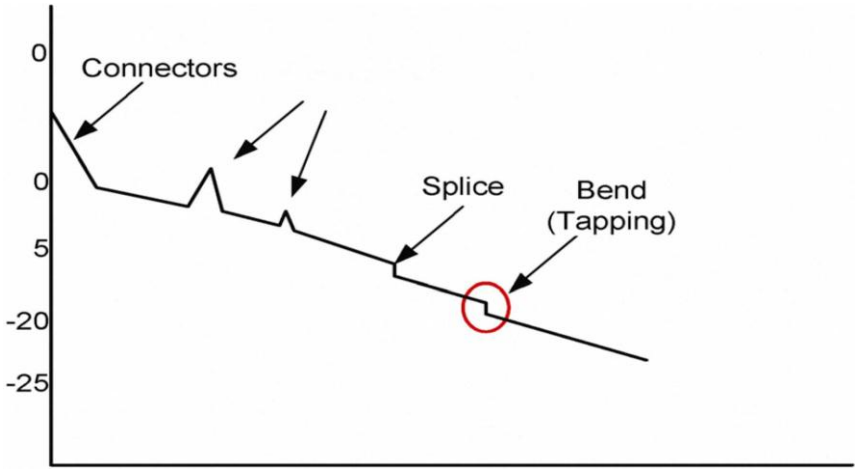


그림 7. OTDR 파형에서 해킹 위치 확인

6) 파일럿 톤 방법:

파일럿 톤은 통신 데이터처럼 광섬유를 따라 이동한다. 그들은 전송 중단을 감지하기 위해서 사용된다. 파일럿 톤 방법은 전파 방해 공격을 감지하기 위해 사용될 수 있다. 하지만, 파일럿 톤의 캐리어 파장이 공격받지 않으면, 이 방법은 전파 방해 공격을 감지하는데 효과적이지 못하다. 파일럿 톤 방법은 도청된 채널에 있는 파일럿 톤이 영향을 받는지 아닌지를 밝힘으로써 도청 공격을 감지한다. 도청 공격이 상당한 신호의 감소를 야기하면 파일럿 톤은 영향을 받는다 [8].

B. *하이 벤드 광섬유:*

이런 광섬유는 보통 저 손실 고 굴절 반경 광섬유라고 불리는데, 광섬유 핀칭 혹은 벤딩으로 인해 야기되는 고 손실을 제한하여, 꼬임, 당김 및 다른 물리적인 광섬유의 조작이 덜 손상을 끼치게 함으로써 네트워크를 보호한다. 다양한 제조 기술에 근거한 여러 가지의 상이한 디자인이 있다 [9].

C. *암호화*

비록 암호화가 도청을 방지할 수는 없지만, 그것은 도청자가 그 정보를 이해할 수 없게 하여 도난 당한 정보를 쓸모 없게 만든다. 암호화는 Layer 2 및 Layer 3 유형으로 분류될 수 있다.

1) Layer 3 암호화

Layer 2 암호화의 예는 IP 패킷의 암호화를 수반하는 IP 보안 프로토콜이다. 그것은 최종 사용자에서 실행되어야 해서 처리 지연을 초래한다. 그것은 세션의 처음에서 설치되어야 하고 많은 수의 네트워크 요소가 관여되면 전체적인 실행은 복잡할 수 있다. 예를 들면 IP 멀티 미디어 서브 시스템의 개발을 생각해 보라. 최초 개발 시에 서로 다른 노드 사이와 요소 사이의 통신은 안전하지 않다. 많이 사용되는 근본적인 수송 기술은 암호화를 제공하지 않기 때문에 IPsec이 원래의 디자인 속으로 코드화되어야 하는 것은 나중이다.

978-1-4577-1169-5/11/ㄴ26.00

2) Layer 2 암호화

이 유형의 암호화는 Layer 3 실체를 그들이 통신하는 정보를 암호화하는 부담으로부터 해방시킨다. 하나의 가능한 Layer 2 암호화의 소스는 is 광학적I CDMA 인데, 그것은 본질적으로 안전한 것으로 여겨진다 [10 - 12]. 이 가정은 주로 brute force 복호화 방법만을 고려하는 것에 근거한 것이고, 다른 정교한 방법을 간과한다. 성공적인 데이터 가로채기의 가능성은 신호 대 소음의 비율 및 총 가용 시스템 용량의 부분을 포함하는 여러 매개 변수의 함수이다. [12]에서는 증가하는 코드의 복잡성이 도청자가 암호화를 "깨기" 위해 필요로 하는 신호 대 소음의 비율(SNR)을 단지 몇 dB만 증가시킬 수 있는 반면에, 도청자에 의한 100 비트 미만의 처리가 암호화를 깨는데 필요한 SNR을 12 dB까지 감소시킨다는 것을 보여준다. 특히 타임 스프레딩/파장 홉핑 및 일반적으로 O-CDMA는 비밀 유지가 시스템 디자인 및 매개 변수의 실행에 매우 의존하게 한다는 것을 알게 한다.

VII. 결론

광섬유 도청은 국가 안보, 금융 기관 혹은 심지어 개인의 사생활 및 자유에 대한 실재하는 위협이다. 도청이 되면, 그렇게 얻어진 정보는 도청자의 동기 및 지략에 따라 많은 다양한 상상할 수 있는 방법으로 사용될 수 있다. 본 논문에서 우리는 '벤드 탭 (굽힘 도청기)'를 이용한 시뮬레이션과 물리적인 실험 둘 다를 통해 개념을 증명하였고, 또한 가용한 기술을 이용하여 이룰 수 있는 많은 광섬유 도청 시나리오의 가능성을 강조하였다. 광섬유로부터 정보를 획득하는 것 이외에도 그것에 정보를 주입하기 위해서 '에바네슨트 스플릿팅'의 경우와 같이 어떤 기술이 사용될 수 있고, 링크 전파 방해를 하고 잘못된 정보를 투입할 수도 있다. 광섬유를 도청하는 것에 대한 명백한 용이성은 예방적인 수단을 정당화하고 또한 본 논문에서도 소개되어 있다.

참고 문헌

[I] Sandra Kay Miller, "빛의 속도로 해킹 ", 보안 솔루션 매거진, 2006년 4월
[2] Davis, USN, RADM John P."USS 지미 카터 (SSN-23): 미래의 SSN 임무 확장하기". 해저 전쟁, Fall 1999 Vol. 2, No. I
[3] 광학적 환상: Sandra Kay Miller 저 정보 보안 발행판: 2006년 11월.
[4] 광학적 네트워크 보안: 감지와 방지를 위한 광섬유 도청 메커니즘 및 방법의 기술적 분석, Keith Shaneman & Dr. Stuart Gray, 2004 IEEE 군사 통신 회의.
[5] R. Jedidi and R. Pierre, 광도파로에서의 곡률 손실의 계산을 위한 High-Order Finite-Element 방법, lLT, Vol. 25, No. 9, pp. 2618-30, 2007년 9월.
[6] FTB-8140 Transport Blazer - 40143 기가 비트 SONETISDH 시험 모듈, EXFO
[7] "도청 방지 전송을 위한 광 광섬유 디자인", 미국 특허 번호 6801700 B2, 2004년 10월 5일
[8] 모든 광학 네트워크 (A ON), 국가 통신 시스템 NCS TIB 00-7, 2000년 8월
[9] DrakaElite, BendBright-접속 코드를 위한 Elite Fiber, Draka Communications, 2010년 7월
978-1-4577-1169-5/11/ㄴ26.00

[10] W. Ford, "컴퓨터 통신 보안", Upper Saddle River, NJ: Prentice-Hall, 1994.
[11] D. R. Stinson, "암호법", Boca Raton, FL: CRC, 1995.
[12] N. Ferguson and 8. Schneier, "실질적인 암호법", Indianapolis, IN: Wiley, 2003.

이 논문은 사우디아라비아 왕국의 사우디 공군이 지원한 연구에 기반한다. **M. Zafar Iqbal는 Prince Sultan Advance Technologies Research Institute (ziqbal@ksu.edu.sa)에서 근무하고 있다. Habiab Fathallah은 King Saud University (hfathallah@ksu.edi.sa)의 부교수이다. Nezih Belhadj는 Laval University (nbelhadj@gel.ulaval.ca)의 박사 후 과정 연구원이다.**

< 번역자 >

김 준 형 : 한국무역협회 통번역 전문위원 5 기
IT, 전자, 보안장비 제조사 해외영업 본부장 역임
종합상사 해외지사장 : 기계, 플랜트, 전자, IT, 석유제품 수출입

978-1-4577-1169-5/11/ㄴ26.00