****

**Interconexión de Redes de Telecomunicación**

**Máster en Ingeniería de Telecomunicación**

**Seguridad de las redes ópticas**

Autores: Andrés Ruz Nieto

Fecha: 22/04/2022

**Índice**

[1. INTRODUCCIÓN 1](#_Toc101627276)

[2. VULNERABILIDADES DE LAS REDES DE FIBRA ÓPTICA 1](#_Toc101627277)

[1. Inserción de *splitters* 1](#_Toc101627278)

[2. ECA 2](#_Toc101627279)

[3. Ataques de interferencia de alta potencia 2](#_Toc101627280)

[4. Alien Wavelength Attacks (AWA) 3](#_Toc101627281)

[5. Ataques de inserción de señales en redes de velocidad de línea mixta (SIA-MLR) 3](#_Toc101627282)

[3. PROBLEMAS DE SEGURIDAD EN LAS REDES DEL FUTURO 4](#_Toc101627283)

[1. Software Defined Networks (SDN) 4](#_Toc101627284)

[2. Redes de centro de datos 4](#_Toc101627285)

[4. CONCLUSIONES 4](#_Toc101627286)

[REFERENCIAS 5](#_Toc101627287)

# INTRODUCCIÓN

En este trabajo se va a hablar a cerca de distintas vulnerabilidades que se pueden dar en las redes ópticas. Se realizará una lista de debilidades de este tipo de redes que se pueden explotar para realizar distintos ataques. En la actualizad estas redes son las más usadas por todo el mundo por lo que conocer y saber cómo evitar estas flaquezas de la red es extremadamente importante.

# VULNERABILIDADES DE LAS REDES DE FIBRA ÓPTICA

A continuación, se enumerarán diferentes ataques que se pueden realizar sobre la red, principalmente en la capa física, describiéndolos y dando una posible solución.

Existen muchos métodos para extraer información de una infraestructura de fibra óptica. Se pueden encontrar ataques que producen una interrupción del enlace, existen mecanismos para controlar la red ante este tipo de ataques. También existen ataques que no requieren un cambio en la infraestructura, la mayoría de estas vulnerabilidades se deben a las propiedades físicas de las fibras ópticas.

## Inserción de *splitters*

Un *splitter* es un componente pasivo que divide una señal de entrada en *n* señales de salida ([Figura 1](#Figura1)). Para insertar un *splitter* en la red es necesario cortar el enlace e introducir el dispositivo en mitad. Dependiendo de su duración, la interrupción puede ser fácilmente detectable por los sistemas de monitorización de la red del proveedor de servicios.

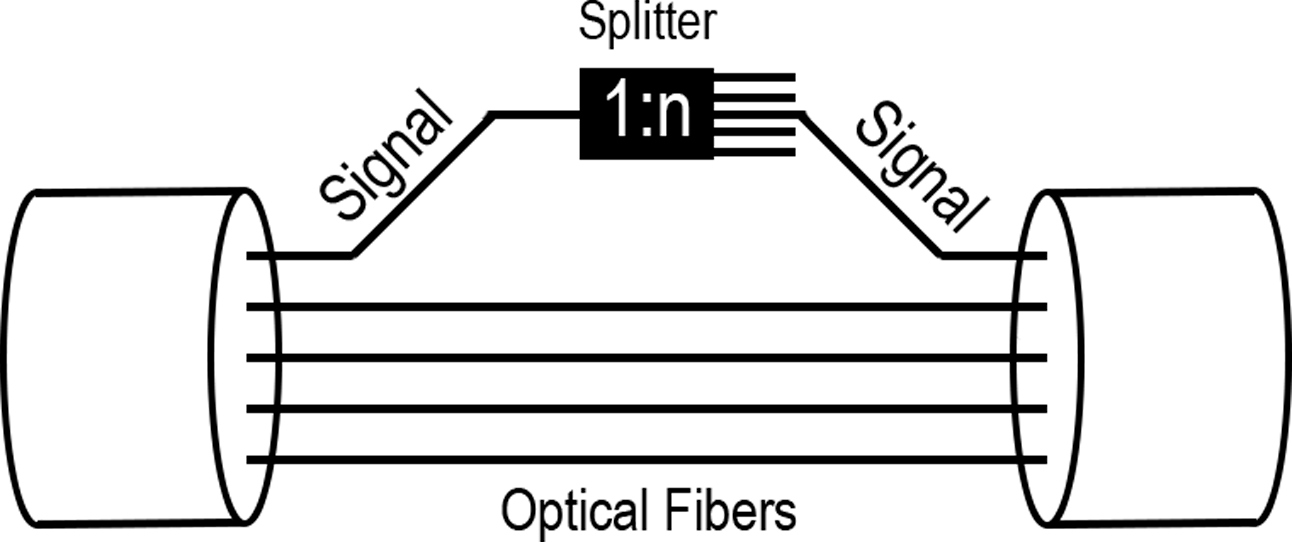


Figura 1: Splitter en fibra óptica

El mal funcionamiento de los servicios por parte del usuario puede ser insignificante, a no ser que se trate de una red óptica pasiva en cuyo caso se debería reconstruir toda la red, esto supone una larga interrupción. Si este ataque se realiza en el momento adecuado (aprovechando una interrupción del servicio planificado o accidental) se podría introducir un splitter sin ser detectado, además una correcta instalación del dispositivo es casi indetectable debido a que las pérdidas de inserción son muy pequeñas.

En caso de medir las pérdidas mediante un OTDR, la detección puede producirse si el divisor no está situado adecuadamente en la red de distribución óptica (al principio o final del enlace, cerca de otro divisor…). Si este ataque se lleva adecuadamente es muy eficaz ya que los divisores pueden estar en funcionamiento varios años sin ser detectados.

Un estudio sobre este ataque realizado en [1](#B1), concluye que el *splitter* más adecuado para realizar este tipo de ataques es uno que tenga una relación de división superior a 90:10 debido a la baja pérdida que se inserta. Aunque teóricamente, no se deberían producir cambios de atenuación, en las redes reales sí pueden producirse, por ejemplo, en caso de que se cambie la posición de una fibra en un casete debido a la instalación de una nueva fibra. Mediante SNMP se monitoriza el estado del enlace y se notifican todas las interrupciones de este, especialmente cuando son superiores a cinco segundos. Cabe destacar que la inserción de un splitter conlleva la interrupción inesperada de la red sin motivo alguno seguido de un pequeño incremento de la atenuación en el trayecto. El sistema es el responsable de detectar este suceso o al menos de notificar al operador de lo ocurrido.

## ECA

El ECA (*Eavesdropping via Channel Access*) es un método bastante común para realizar ataques de espionaje accediendo directamente al canal óptico a través de la “escucha” de la fibra. Una de las formas de realizar este ataque es eliminando el revestimiento que tiene la fibra óptica y doblándola para que la señal se escape del núcleo ([Figura 2](#Figura2)) y llegue a un fotodetector para capturar la información.

Mano de una persona

Descripción generada automáticamente con confianza media

Figura 2: Fiber Tapping - <https://youtu.be/PbipefyfkNY>

En el mercado se pueden encontrar dispositivos de escucha que se enganchan a una fibra óptica y provocan microcurvaturas para poder realizar una escucha de las comunicaciones ([Figura 3](#Figura3)). Además, estos dispositivos provocan pérdidas menores a 1dB y pueden pasar desapercibidos para los sistemas de gestión de redes (NMS) más utilizados.

Mano sosteniendo un aparato electrónico

Descripción generada automáticamente con confianza media

Figura 3: Dispositivo para realizar Fiber Tapping - <https://youtu.be/PbipefyfkNY>

Para detectar este tipo de ataques, es necesario mejorar los NMS con alarmas de detección de intrusiones activadas por los cambios en pérdidas de inserción de las conexiones de una fibra óptica.

Otra forma de realizar un ECA es a través de los puertos de monitorización que suelen estar presentes en diferentes componentes de la red. La señal óptica se refleja en un divisor para permitir la conexión de dispositivos de monitorización sin interrumpir el tráfico.

## Ataques de interferencia de alta potencia

Los ataques de interferencia de alta potencia o High-Power Jamming (HPJ) Attacks consisten en insertar una señal óptica de mucha potencia, aproximadamente entre 5 y 10 dB más de las señales útiles. En las redes ópticas compuestas por multiplexores ópticos de adición y caída (OADM) sin ninguna funcionalidad de bloqueo de longitud de onda, las señales de alta potencia pueden afectar a las señales de un usuario que se propagan por la misma fibra óptica, amplificadores… En los conmutadores ópticos, las señales de interferencia pueden afectar a las señales legítimas en la misma longitud de onda aumentando la diafonía dentro de la banda. Las señales que atraviesan los mismos enlaces físicos que la señal interferente pueden sufrir fuera de banda en las fibras ópticas y los amplificadores.

En las fibras ópticas, las señales de interferencia originan una diafonía fuera de banda al filtrarse a los canales vecinos y aumentar los efectos no lineales.

En los amplificadores de fibra dopada con erbio, una señal de interferencia fuera del rango de trabajo puede causar la llamada “competición de ganancia” en la que las señales originales pierden ganancia debido a que la señal interferente es más fuerte mientras que la señal maligna se amplifica aún más.

Para reducir los efectos de los HJP se pueden emplear OADM reconfigurables (ROADM) con atenuadores ópticos variables (VOAs) para regular la potencia de salida de las señales. Además, los ROADM basados en la conmutación selectiva de longitudes de ondas (WSS) podrían utilizarse con un alto aislamiento de los puertos, aunque, con el aumento de la demanda de tráfico, el aislamiento de los WSS también debería incrementarse de forma equivalente lo que resultaría ser muy costoso. [[3]](#B3)

## Alien Wavelength Attacks (AWA)

Para permitir la actualización de la red y la transmisión eficiente de las conexiones de alta capacidad a través de la infraestructura existente, los operadores se ven obligados a implementar Alien Wavelength (AW). Cuando no existe el soporte para las AW cada conexión es terminada y regenerada por un nodo en el borde del dominio. Por otro lado, las AW pueden atravesar múltiples dominios sin conversiones ópticas-electrónicas-ópticas (OEO). Otro ejemplo de uso de las AW es la actualización de los sistemas de línea heredados con transpondedores de nueva generación de 100G. Este tipo de soluciones están muy extendidas en los despliegues actuales.

La presencia de AW genera una vulnerabilidad importante para la seguridad de la red dependiendo de la gestión de estas. Alrededor del 40% de las redes actuales siguen siendo redes fijas punto a punto basadas en OADM en las que el sistema de control y gestión no tiene información sobre el rendimiento de los canales ajenos por lo que no se puede controlar la potencia y la frecuencia de la señal. Además, si los nodos de la red se basan en divisores y WSS en una configuración de difusión y selección, las longitudes de AW se lanzan a la red sin filtrar. En estos sistemas, las AW pueden aprovecharse para realizar diversos métodos de ataque lo que supone un gran riesgo para los proveedores de la red. En las redes más inteligentes, las AW son gestionadas por el NMS, es decir, un canal se configura como una onda de longitud “amiga”, lo que permite al sistema de gestión tener información de los parámetros de la señal, aunque sigue sin tener control sobre sus valores. En las redes de nueva generación, se define una interfaz dedicada para alojar AW con la función de sintonizar sus niveles de potencia.

## Ataques de inserción de señales en redes de velocidad de línea mixta (SIA-MLR)

Las redes de velocidad de línea mixta (MLR) son una solución intermedia y rentable para la actualización gradual de la red desde los 10 Gbps hasta las redes de 40/100/200 Gbps al permitir la coexistencia de diferentes formatos de modulación sobre la infraestructura existente. Una de las principales vulnerabilidades de seguridad de estas redes proviene a partir de los efectos no lineales entre las señales de 40/100/200 Gbps y los canales vecinos de 10 Gbps. Específicamente, los canales de 10 G con modulación OOK deterioran la calidad de los canales de mayor velocidad binaria y modulación de fase, debido a la modulación de fase cruzada. En el caso de los canales multiplexados por polarización, la modulación de polarización cruzada afecta además a la transmisión óptica incluso más que en las de modulación de fase cruzada. Aunque técnicamente es posible tener canales de 10 Gbps y 40/100/200 Gbps con una separación de 50 GHz, esto impone una penalización adicional de la OSNR para los canales de 40/100/200 Gbps. La gravedad de esta penalización depende del formato de modulación, la potencia de entrada en el canal y de las bandas de guarda. En la mayoría de las redes desplegadas no es posible cambiar el formato de modulación o las potencias de entrada, dejando sólo la opción de utilizar bandas de guarda entre los canales de 40/100/200 Gbps. Un posible ataque de degradación del servicio en las redes MLR podría producirse al insertar un canal OOK cerca de un canal de 40/100/200 Gbps sin permitir una banda de guarda suficiente. De esta forma, la señal atacante podría deteriorar significativamente la OSNR de las señales originales.

# PROBLEMAS DE SEGURIDAD EN LAS REDES DEL FUTURO

La evolución de las redes ópticas mediante la incorporación de funcionalidades de control y gestión programables por software acompañado de una arquitectura de nodos flexible y la expansión de las redes de centro de datos, introducen nuevas vulnerabilidades de seguridad específicas

## Software Defined Networks (SDN)

La introducción de SDNs permite desacoplar los planos de datos y de control, que están integrados en los equipos de red utilizados en la actualidad. Además de las ventajas como el suministro simplificado y automatizado de servicios extremo a extremo, una mejor utilización de los recursos de la red mediante la adaptación de la infraestructura a las necesidades del usuario y una mayor flexibilidad de la red, SDN también puede introducir ciertas vulnerabilidades en la red ya que el controlador SDN sirve como interfaz de control entre el hardware y las aplicaciones SDN (instaladas en los nodos) para realizar ingeniería de tráfico o recopilación de datos. Obtener el control de estas funcionalidades representa un objetivo deseable para los ataques. Los controladores SDN pueden ser empleados para introducir un virus en la red u obtener acceso a los datos, e incluso secuestrar la red.

## Redes de centro de datos

Las empresas de hoy en día dependen del uso de múltiples centros de datos situados en ubicaciones físicas distantes para garantizar la recuperación ante desastres y la continuación del negocio en caso de fallos. Para garantizar una rápida recuperación en caso de desastre, los datos y aplicaciones almacenados deben replicarse en múltiples centros de datos. La replicación síncrona en la que el sistema de almacenamiento que inicia la replicación espera el acuse de recibo (ACK) del sistema receptor, permite recudir al máximo las pérdidas de datos en presencia de fallos. Debido a que cada transferencia debe ser reconocida antes de que pueda iniciarse la siguiente, el proceso es muy sensible a la latencia de red, lo que limita la distancia máxima entre sistemas para realizar las réplicas. El proceso de replicación puede ser objeto de ataques para obtener acceso a los datos no autorizados. Insertar una longitud de onda extra en la fibra, la red puede sufrir un ataque de latencia. Aunque las tramas de la red de transporte óptico (OTN) incluyen la definición de la medición de latencia, en la mayoría de las redes no se implementa la supervisión de la latencia en tiempo real

# CONCLUSIONES

Las redes ópticas son vulnerables a varios tipos de ataques dirigidos a la escucha o a la interrupción del servicio, lo que puede provocar grandes pérdidas de datos o de ingresos. Además, la evolución hacia arquitecturas de nodos flexibles y programables por software crea nuevas vulnerabilidades de seguridad que deben ser identificadas y tenidas en cuenta durante el diseño y el funcionamiento de la red.

# REFERENCIAS

|  |  |
| --- | --- |
| [[1]](https://www.mdpi.com/1424-8220/22/2/588) | Spurny, V.; Munster, P.; Tomasov, A.; Horvath, T.; Skaljo, E. Physical Layer Components Security Risks in Optical Fiber Infrastructures. Sensors **2022**, 22, 588. https://doi.org/10.3390/s22020588 |
| [[2]](https://www.researchgate.net/publication/269268194_Vulnerabilities_and_security_issues_in_optical_networks) | Furdek, Marija & Skorin-Kapov, Nina & Zsigmond, Szilard & Wosinska, Lena. (2014). Vulnerabilities and security issues in optical networks. International Conference on Transparent Optical Networks. 1-4. 10.1109/ICTON.2014.6876451. |
| [[3]](https://ieeexplore.ieee.org/document/9350606) | G. Savva, K. Manousakis, J. Rak, I. Tomkos and G. Ellinas, "High-Power Jamming Attack Mitigation Techniques in Spectrally-Spatially Flexible Optical Networks," in *IEEE Access*, vol. 9, pp. 28558-28572, 2021, doi: 10.1109/ACCESS.2021.3058259. |