

ESCUELA POLITÉCNICA NACIONAL
REDES DE COMUNICACIONES ÓPTICAS
TALLER No.9

Integrantes: Castillo Jorge, Juela Danny

1. TEMA:

SEGURIDAD EN REDES DE COMUNICACIONES ÓPTICAS

2. REQUERIMIENTO PREVIOS

- Conocimiento de Comunicaciones Ópticas.

3. DESARROLLO DE LA PRÁCTICA

- *Describe los principales problemas, inconvenientes y amenazas de seguridad en redes ópticas.*
 - *Describe los problemas de seguridad en las distintas porciones de la red (e.g., acceso, metro, etc.)*

Ataques a la capa de Aplicación

En este nivel, los ataques están enfocados hacia la denegación de servicio (DoS), códigos maliciosos entre otros. [1]

- **DNS Spoofing:** Es un método para alterar las direcciones de los servidores DNS que utiliza la potencial víctima y de esta manera poder tener control sobre las consultas que se realiza. Es una falsificación de la relación "Nombre de dominio - IP" ante una consulta de resolución de nombre, donde se da una dirección IP falsa a un cierto nombre DNS o viceversa.
- **Sniffing:** Es una técnica que consiste en escuchar o capturar toda información que circula por la red, esta información se almacena y se interpreta para poder descubrir datos sensibles como contraseñas, información bancaria, etc. El Sniffing se puede realizar mediante software (programa que escucha el tráfico que circula por una tarjeta de red) o por hardware (conectarse físicamente a una red y escuchar el tráfico).
- **Eavesdropping:** Es un proceso mediante el cual un atacante únicamente contempla la adquisición o interceptación del tráfico que circula por la red en texto claro o cifrado, es una variante de Sniffing. Es un ataque completamente pasivo, lo que le hace muy difícil de detectar el ataque, de forma que el atacante puede capturar información privilegiada y/o claves para acceder a información sin que nadie se dé cuenta, hasta que el atacante utiliza dicha información captura convirtiéndola en un ataque activo.
- **DoS (Denial of Services):** Es un término que traducido al español se conoce como "Denegación de Servicios". Este tipo de ataques consiste en generar una gran cantidad masiva de peticiones al servidor, provocando así una sobrecarga del mismo y por consiguiente la alteración del servicio a los usuarios que son legítimos. Este tipo de ataques son fáciles de detectar, pues basta con identificar la dirección IP del ordenador que está realizando las peticiones masivas al servidor y bloquear el acceso al mismo. De esta forma, la sobrecarga desaparece y se puede restablecer fácilmente el servicio a los usuarios legítimos.
- **DDoS (Distributed Denial of Service):** Es un término que traducido al español como "Denegación distribuida de servicios". Un ataque DDoS es más complejo de detectar a diferencia del ataque DoS, puesto que son varios los ordenadores que realizan llamadas masivas y constantes al servidor. Cada uno de ellos con una dirección IP determinada y localizados en diferentes lugares del mundo.
- **DNS:** El DNS es una fuente de información de red muy valiosa. DIG es una utilidad para la obtención de información del servicio de nombres DNS, permite copiar una base de datos entera de nombres (dominio) desde un servidor DNS, para su posterior análisis. Asimismo, sus características avanzadas facilitan extraer toda la información asociada al protocolo DNS, no permitiendo únicamente la realización de peticiones, como nslookup (programa utilizado para saber si el DNS está resolviendo correctamente los nombres y las IPs).

Ataques a la capa de Transporte

Los ataques en la capa de transporte van asociados al funcionamiento de los protocolos TCP y UDP. Escaneo de puertos, inundaciones UDP, DoS por sobrecarga de conexiones, son algunos de los ataques a dicha capa. A continuación, se detalla los ataques y vulnerabilidad que presenta este nivel: [1]

- **Fingerprinting:** Es una técnica que permite extraer información de un sistema concreto, para aprender más sobre su configuración y comportamiento. El objetivo primordial suele ser obtener el sistema operativo que se ejecuta en la máquina destino de la inspección, con esta facilitará la búsqueda de vulnerabilidades asociadas al mismo.
- **Escaneo de Puertos:** Es el proceso de analizar por medio de un programa el estado de los puertos, tanto UDP como TCP, de una máquina conectada a una red de comunicaciones, detecta si un puerto está abierto, cerrado, o protegido. El escaneo se utiliza para determinar las características de una red o sistema remoto, con el objetivo de identificar los equipos disponibles y alcanzables desde Internet, así como los servicios que ofrece; permite saber los sistemas existentes, los servicios ofrecidos por ellos, cómo están organizados los equipos, que sistemas operativos ejecutan, cual es el propósito de cada uno. Es utilizado por los administradores de la red para analizar posibles problemas de seguridad, y también por los atacantes que intentan comprometer la seguridad de la red.
- **UDP Flood:** El ataque de inundación UDP es una Denegación de Servicio (DoS) mediante el User Datagram Protocol (UDP). Básicamente, este ataque consiste en generar grandes cantidades de paquetes UDP contra la víctima elegida. El ataque de inundación UDP puede ser iniciado por el envío de un gran número de paquetes UDP a puertos aleatorios en un host remoto. Para un gran número de paquetes UDP, los sistemas de las víctimas se verán, obligados a enviar muchos paquetes ICMP (informa de incidencias en la entrega de paquetes o de errores en la red). Esto impide que el ICMP sea alcanzable por otros clientes. Además, el atacante puede falsificar la dirección IP de los paquetes UDP, garantizando que los ICMP de retorno no lleguen a su fin.
- **TCP SYN Flood:** Dentro de los ataques DoS, existe uno asociado directamente al protocolo TCP. Consiste en el envío masivo de paquetes de establecimiento de conexión (SYN) contra un sistema. La recepción de estas solicitudes provoca que el sistema destino, objetivo del ataque, reserve cierta cantidad de memoria (buffers) para almacenar las estructuras de datos asociadas a cada una de las nuevas conexiones en curso. El protocolo TCP requiere del establecimiento de una conexión, que se realiza en tres pasos. Tras la recepción del paquete SYN, responderá con su paquete SYNACK, permaneciendo a la espera del paquete final (ACK) que confirma el establecimiento de la conexión TCP. El atacante no enviará nunca ese ACK esperado, por lo que la memoria del destino es copada en su totalidad por conexiones falsas, no siendo posible el establecimiento de conexiones de clientes reales, y por tanto anulándose el servicio.
- **Connection Flood:** Los servicios TCP orientados a conexión, que son la mayoría (TELNET, FTP, HTTP, SMTP, NNTP) tienen un límite máximo de conexiones simultáneas soportadas; cuando este límite se alcanza, cualquier conexión nueva es rechazada. De forma similar al SYN Flood, si un atacante es capaz de monopolizar el límite definido con conexiones de su propiedad, que simplemente son establecidas, pero por las que no se realiza ninguna comunicación posterior, el sistema no proporcionará servicio. Al igual que antes, las conexiones expiran progresivamente con el paso del tiempo, pero un ataque constante de apertura de conexiones mantendrá continuamente el límite en su valor máximo. La diferencia está en que en este caso la conexión se ha establecido y por tanto se conoce la identidad del atacante (dirección IP), y a su vez, la capacidad del sistema o sistemas atacante/s debe ser lo suficientemente elevada como para mantener abiertas todas las sesiones que colapsan el servidor atacado.
- **Land:** Este ataque permite bloquear un sistema, mediante el envío de un paquete SYN cuya dirección IP fuente y destino es la misma. Existe una variación de este ataque, basada en que los puertos origen y destino también son iguales. Este ataque, que está dirigido a aplicaciones vulnerables, bloquea los sistemas o los vuelve inestables.
- **Teardrop:** Un "ataque por fragmentación" consiste en saturar el tráfico de la red (denegación de servicio) para aprovechar el principio de fragmentación del protocolo IP. Este protocolo se utiliza para fragmentar paquetes grandes en varios paquetes IP más pequeños. Cada uno de ellos tiene un número de secuencia y un número de identificación común. Cuando recibe datos, el destinatario

puede volver a ensamblarlos gracias a los valores de compensación que contienen. El ataque por fragmentación más conocido es Teardrop. Este método se basa en introducir información de compensación falsa en los paquetes fragmentados. En consecuencia, durante el reensamblado, quedan fragmentos vacíos o superpuestos que pueden desestabilizar el sistema.

Ataques a la capa de Red

Esta capa no está exenta de los ataques que los usuarios malintencionados efectúan contra las vulnerabilidades del modelo OSI. A continuación, se presenta los principales ataques o vulnerabilidades. [1]

- **Footprinting:** Es la técnica utilizada para la recopilación de información sobre los sistemas informáticos y las entidades a las que pertenecen. Para obtener esta información, un hacker podría utilizar varias herramientas y tecnologías. Esta información es muy útil para un hacker que está tratando de romper un sistema conjunto.
- **IP Spoofing:** Se basa en la generación de paquetes IP con una dirección de origen falsa, se puede hacer envío de paquetes con este tipo de direcciones para que desde la misma máquina se disponga de un sistema destino objetivo, porque existe un dispositivo de filtrado que permite el tráfico de paquetes con esta dirección de origen, o porque existe una relación de confianza entre esos dos sistemas.
- **SMURF:** Este ataque se aprovecha de las bondades de una dirección broadcast, cuando un atacante tiene la opción de enviar un paquete de datos a dicha dirección, puede provocar que todos los sistemas pertenecientes a dicha red respondan simultáneamente con el objetivo de paralizar la red. Pero si se asocia esta técnica con IP Spoofing, al enviar un paquete ICMP con la dirección IP de origen de la máquina a atacar y dirección de destino la dirección de broadcast de una red con un elevado número de máquinas, todas las repuestas de la red de broadcast se dirigirán realmente a la dirección IP del sistema “spoofeado”.
- **Ping of Death:** El ping de la muerte, funciona enviando un paquete de ping tan grande que puede ocasionar que el buffer de memoria se desborde, el resultado obtenido puede ser el reinicio de la máquina o el apagado. Para realizar este ataque es necesario disponer de una herramienta que lo implemente o modificar el límite impuesto en el código fuente del cliente de ping.
- **Routing Protocols:** En este ataque se aprovecha las vulnerabilidades de los protocolos de enrutamiento, de tal forma que se introducen paquetes de actualización de rutas, pudiendo así manipular los caminos por donde seguirá el tráfico de acuerdo a las intenciones del atacante.

Ataques a la capa de Enlaces de Datos

Los ataques a la capa de enlace de datos, se centra en el protocolo ARP (Address Resolution Protocol), VLAN y en STPN (Spanning Tree Protocol), que a continuación se mencionan: [1]

- **ARP Spoofing:** Address Resolution Protocol (ARP por sus siglas en inglés) es un protocolo de capa 2 en el modelo OSI, que se encarga de resolver direcciones IP y MAC. El principal objetivo del ataque ARP Spoofing, es la de enviar mensajes ARP falsos a la red. Esta técnica tiene la finalidad de asociar la dirección MAC del atacante con la IP del host atacado como por ejemplo el router. De esta forma, cualquier tráfico dirigido al router, será erróneamente enviado al atacante que podrá realizar captura de todos los datos. Con el ARP Spoofing o envenenamiento de tablas ARP puede infiltrarse en una red, con el objetivo de que un atacante pueda husmear los paquetes de datos que pasan por la LAN (red de área local), modificar el tráfico, o incluso detenerlo.
- **VLAN Hopping:** Es un tipo de ataque de red en el que un atacante que está conectado a un puerto de acceso (conectado a una VLAN en particular) puede obtener acceso al tráfico de red de otras VLAN.

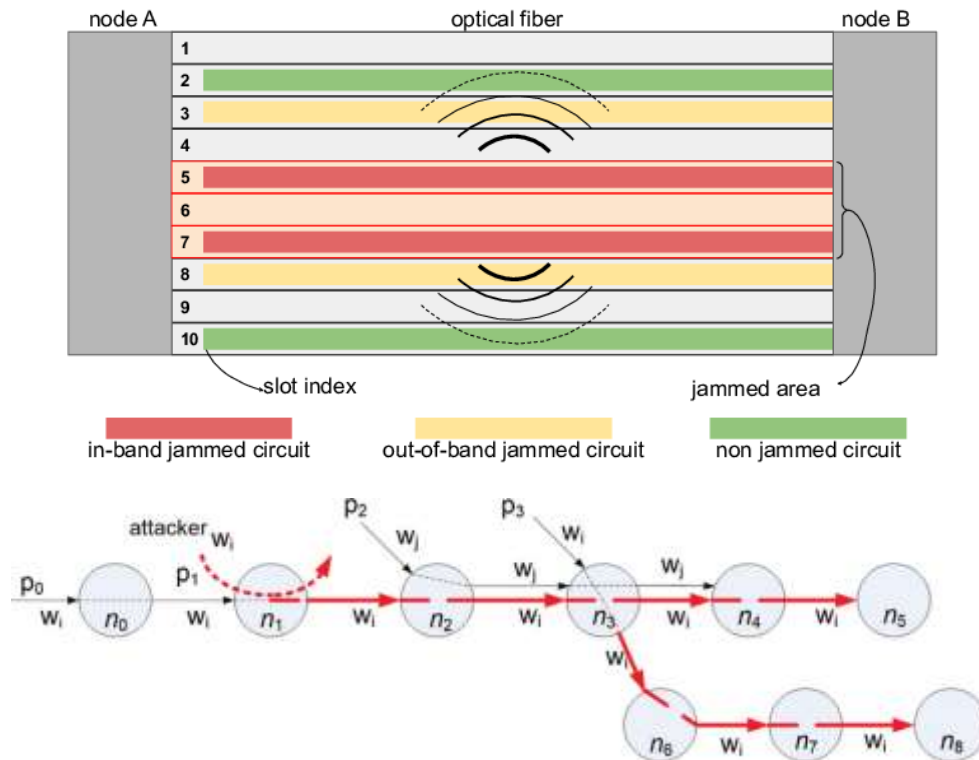
Normalmente, una computadora conectada a un puerto de acceso de conmutador puede obtener tráfico solamente desde la VLAN relacionada con ese puerto de conmutador. Mediante el ataque VLAN Hopping, un atacante puede detectar el tráfico de red de otra VLAN utilizando un analizador de protocolo (sniffer) o enviar tráfico desde una VLAN a otra VLAN. Este ataque requiere que el puerto este configurado con el modo Trunking “automático”.

Ataques a la capa Física

Los ataques en la capa física están enfocados a daños provocados en los dispositivos que pertenecen a la red. Desde una simple desconexión de cable de fibra hasta un incendio se puede considerar ataque en dicha capa.

Un ataque a los sistemas físicos de una red de comunicaciones puede ocasionar una sucesión de problemas que pueden llegar a tener mayor impacto que los ataques ocasionados en la parte lógica. Este tipo de ataques se describe en los siguientes apartados teniendo en cuenta la estructura de la red GPON. [1]

Tipo de ataque	Método	Descripción	Componente
Interrupción del servicio	Interferencia en banda	Aprovecha la saturación de ganancia en amplificadores ópticos.	Fibra
	Interferencia fuera de banda	La inserción de energía se realiza en una longitud de onda fuera de la ventana de la señal.	Fibra
	Crosstalk intencional	Utilizada para manipular la información propagada conjuntamente en otros canales o información específica.	Splitter Filtro Switch Combiner
	Gain Competition	Al inyectar una señal óptica mayor a una determinada longitud de onda utilizada es decir subutilizada lo que logran es aumentar su potencia óptica logrando cegar a los receptores	Amplificador
Eavesdropping	Observar sin autorización	Interceptar la señal óptica. Se accede físicamente. Fibras expuestas en un extremo sería muy complicado porque siempre están controladas.	Fibra
	Objetivo: Analizar pasivamente el tráfico en la red	Obtener la información mediante el método de observación. Dividir el acceso a la fibra en la mitad del tramo y acceder a las fibras individuales. -Flexión de la fibra -División óptica - Corte de ranura en V -Dispersión Óptica	Tap divisor que separa la luz en dos o más salidas



- *Indique los mecanismos para proveer servicios de seguridad en redes de comunicaciones ópticas.*
 - *Indique aspectos o consideraciones técnicas deben ser cubiertas para que una red de comunicaciones ópticas se considere segura y/o resiliente.*

Mecanismos de seguridad

Los mecanismos de seguridad son herramientas técnicas y métodos que se utilizan para implementar un servicio de seguridad, es decir, es un procedimiento que está diseñado para detectar, prevenir o recobrase de un ataque de seguridad. [1]

Existen muchos y variados mecanismos de seguridad. Su selección depende del tipo de sistema, de su función y de los factores de riesgo que lo amenazan.

- **Mecanismos preventivos**

Son aquellos cuya finalidad consiste en prevenir la ocurrencia de un ataque informático. Básicamente, se concentran en el monitoreo de la información y de los bienes, registro de las actividades que se realizan en la organización y control de todos los activos y de quienes acceden a ellos.

- **Mecanismos detectores**

Son aquellos que tienen como objetivo detectar todo aquello que pueda ser una amenaza para los bienes. Ejemplos de éstos son las personas y equipos de monitoreo, quienes pueden detectar cualquier intruso u anomalía en la organización.

- **Mecanismos correctivos**

Los mecanismos correctivos se encargan de reparar los errores cometidos o daños causados una vez que se ha cometido un ataque, o en otras palabras, modifican el estado del sistema de modo que vuelva a su estado original y adecuado.

- **Mecanismos disuasivos**

Se encargan de desalentar a los perpetradores de que cometan su ataque para minimizar los daños que puedan tener los bienes.

- *De existir, indique la normativa o estándares (e.g., de la ITU) vigentes relacionados con aspectos de seguridad en redes ópticas.*
 - *Describa los estándares y describa los aspectos técnicos y procedimentales que considere más relevantes.*

La recomendación G.984.3 de GPON describe el uso de un mecanismo de seguridad de la información para asegurar que los usuarios puedan acceder únicamente a los datos destinados a ellos. Actualmente existen dos mecanismos de seguridad, ambos considerandos como opcionales.

- Autenticación de la ONU/ONT mediante contraseña (PLOAM)
- Cifrado en el tráfico descendente (desde CO al cliente), mediante AES (128 bit)

El tráfico ascendente no se considera en riesgo debido a que el tráfico ascendente presenta una arquitectura punto a punto, por lo que el tráfico enviado desde la ONT a la OLT no puede ser escuchado ni interceptado por otros ONTs. [1]

La arquitectura de protección de GPON se considera que mejora la fiabilidad de las redes de acceso. Sin embargo, la protección se considera como un mecanismo opcional porque su implementación depende de la realización de sistemas económicos. Hay dos tipos de conmutación de protección, conmutación automática y conmutación forzada. El primero es activado por la detección de fallos, tales como pérdida de señal, pérdida de trama, degradación de señal y así sucesivamente. El segundo es activado por eventos como el desvío de fibra, reemplazo de fibra, etc.

IMPLEMENTACION DE MATLAB CON OPTISYSTEM

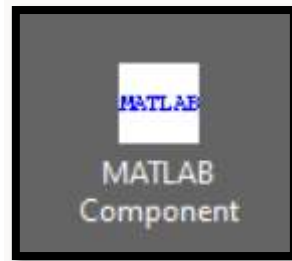


Fig. 1. Componente de Matlab en Optisystem.

Este bloque incorporado dentro de la librería **Matlab Library** habilita la utilización de componentes creados en MATLAB. Su configuración nos permite, mediante comandos elaborados en Matlab o scripts, crear o modificar señales de entrada dentro del bloque, es decir realizar procesamiento de señales. Sus parámetros son:

PUERTOS:

Name and description	Port type	Signal type
Input 1	Input	Optical
Output 1	Output	Optical

PARÁMETROS:

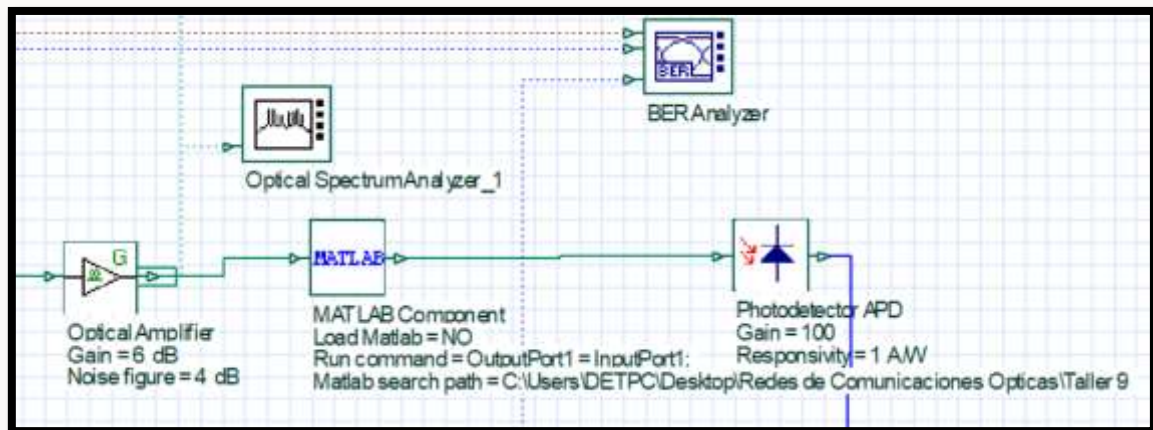


Fig. 3. Bloque de MATLAB component implementado.

Dentro de la pestaña de *main* se configuran los parámetros como se muestran a continuación:

Disp	Name	Value	Units	Mode
<input checked="" type="checkbox"/>	Load Matlab	<input checked="" type="checkbox"/>		Normal
<input checked="" type="checkbox"/>	Run command	<code>OutputPort1 = InputPort1;</code>		Normal
<input checked="" type="checkbox"/>	Matlab search path	<code>C:\Users\DETPC\Desktop\Re</code>		Normal
<input type="checkbox"/>	Sampled signal domain	<code>Time</code>		Normal
<input type="checkbox"/>	Spatial mode domain	<code>Space</code>		Normal

Fig. 4. Configuración de MATLAB component.

Al habilitar la pestaña de Load Matlab se abrirá un terminal de la siguiente forma:

```

MATLAB Command Window

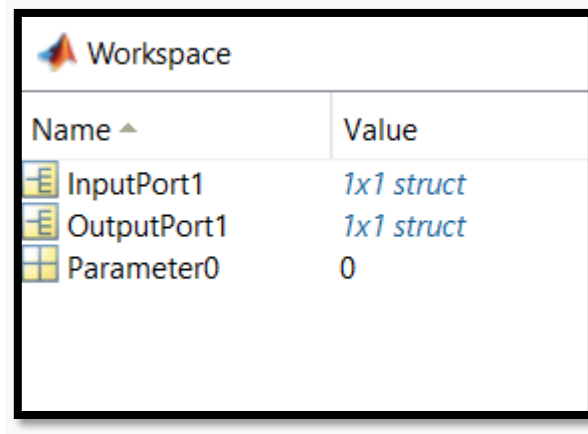
To get started, type doc.
For product information, visit www.mathworks.com.

>> doc
>> workspace
>> |

```

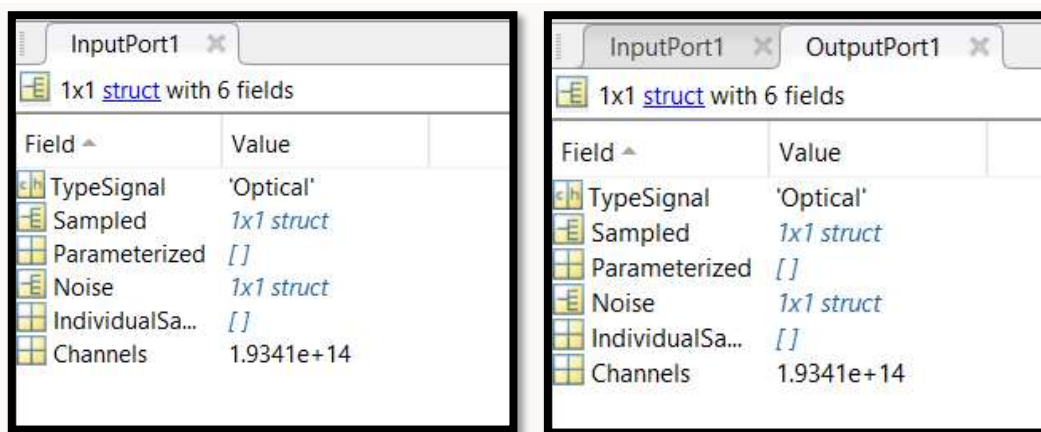
Fig. 5. Command Window de Matlab.

Al escribir *doc* en primer lugar, se procede a ejecutar la simulación y en el terminal se escribe *workspace*.



Name	Value
InputPort1	1x1 struct
OutputPort1	1x1 struct
Parameter0	0

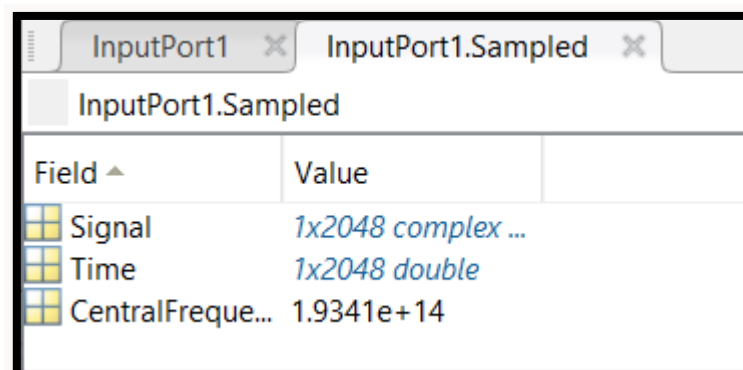
Fig. 6. Variables calculadas.



Field	Value
TypeSignal	'Optical'
Sampled	1x1 struct
Parameterized	[]
Noise	1x1 struct
IndividualSa...	[]
Channels	1.9341e+14

Fig. 7. Contenido dentro de InputPort y OutputPort.

A continuación, se guardan estos parámetros con clic derecho sobre **Sampled**, en cualquier variable. Se escoge la ruta y se muestra su contenido en Matlab.



Field	Value
Signal	1x2048 complex ...
Time	1x2048 double
CentralFreque...	1.9341e+14

Fig. 8. Contenido de las variables guardadas.

```

clc
clear all
close all
load('matlab.mat');
signal=InputPort1.Sampled.Signal;
t=InputPort1.Sampled.Time;

plot(t,signal)

```

Fig. 9. Elaboración de un script en Matlab con las variables almacenadas.

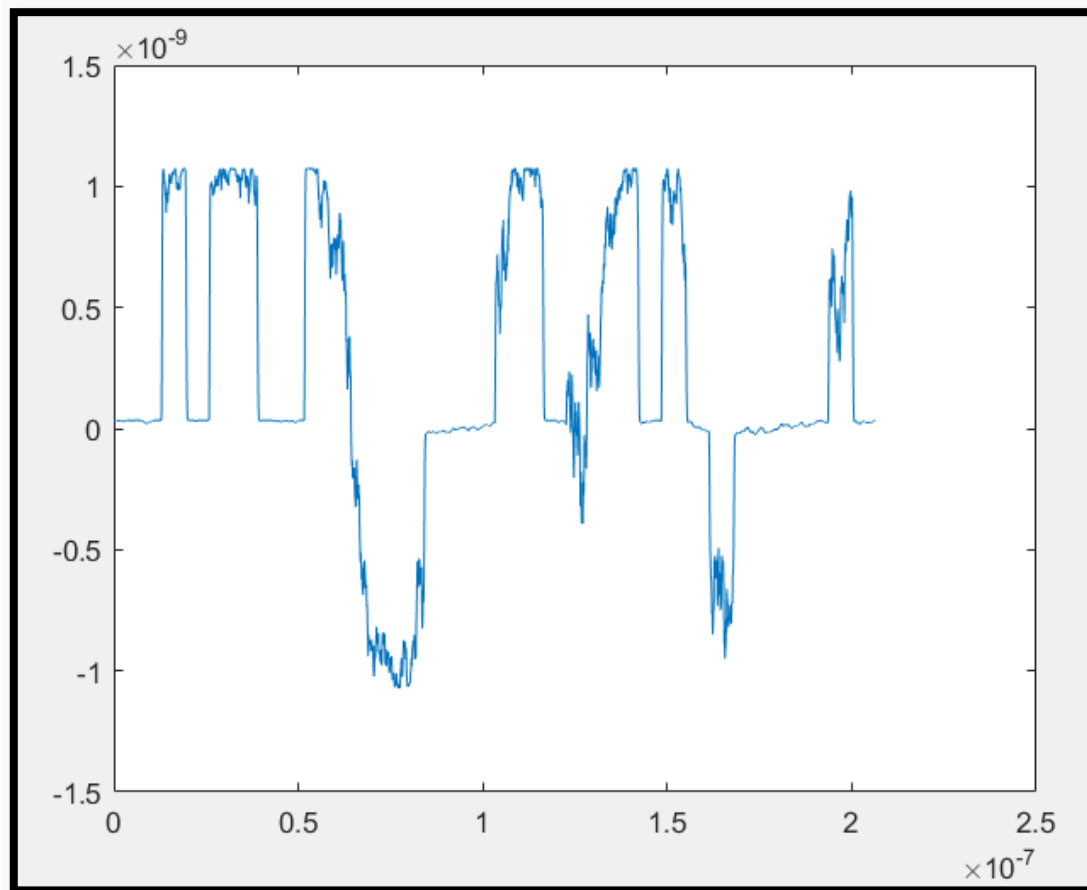


Fig. 10. Verificación de las señales obtenidas.

Uno de los beneficios de la implementación de la señales en Matlab es la obtención de estas variables a fin de realizar procesamiento digital en las mismas, obtener un mejor resultado e implementarlo en el esquema simulado.

REFERENCIAS

[1] J. Sigcho. *ESTUDIO DE LA SEGURIDAD EN REDES GPON*. UNIVERSIDAD NACIONAL DE LOJA. Loja, 2018.