Photonic Reservoir Computing to Detect Anomalies and Intrusions in Optical Networks

Josep Torné Chertó

Supervisor: Prof. Dr. Ir. P. Bienstman

Counsellor: Chonghuei Ma

Master's dissertation submitted in order to obtain the academic degree of
Master's degree in Telecommunications Engineering

Faculty of Engineering and Architecture
Universiteit Gent

Academic year 2019–2020

Acknowledgement

First of all I would like to thank my Supervisor Prof. Dr. Ir. Peter Bienstman for giving me the opportunity to do my master thesis under his mentorship and also for the guidance and the patience during the development of it. My deepest gratitude also goes to my counsellor Chonghuei Ma for being always disposed to help me with any problem I could face and his efficiency in doing so. Also, I want to mention Emmanuel Gooskens for teaching me how to work Pythorch and for his examples, that have been the basis of my work. As well my acknowledgements go to Kristien de Meuler for the time she spent helping me to get along with the software infrastructure of the department.

Moving to a more personal zone, I special thank my family for encouraging me to do what I want no matter the circumstances. And finally, thanks to my Erasmus friends that even they didn't help me in this task, probably the opposite, have made me feel like at home.

Josep Torné Chertó, May 2020

Permission for use on loan

Josep Torné Chertó, May 2020

Photonic Reservoir Computing to Detect Anomalies and Intrusions in Optical Networks

by

Josep Torné Chertó

Master's dissertation submitted in order to obtain the academic degree of
Master's degree in Telecommunications Engineering

Academic Year 2019–2020

Supervisor: Prof. Dr. Ir. P. Bienstman
Counsellor: Chonghuai Ma

Faculty of Engineering and Architecture
Universiteit Gent

Abstract

Optical networks are a critical infrastructure subjected to attacks at its physical layer. Different methods have been presented to prevent, detect and solve these attacks. The work in this thesis attempts to offer an alternative to the detection task.

The current systems in charge of detecting intrusions in optical networks rely on the metrics obtained from OPM equipment. This equipment has a high cost, making the massive deployment through the optical network unfeasible. Photonic reservoir computing is a technology that has been able to solve tasks as header recognition, channel equalization, etc. with a good performance and a cost that allows it to be deployed over all the network.

In this thesis, it is designed and assessed a photonic reservoir computing system able to detect and classify attacks in optical networks. All the work has been done by means of software simulation.

Keywords

Attack detection, machine learning, optical network security, photonic reservoir computing

Photonic Reservoir Computing to Detect Anomalies and Intrusions in Optical Networks

Josep Torné Chertó
Supervisor: : Prof. Dr. Ir. P. Bienstman
Counsellor: Chonghuai Ma

***Abstract*—Optical networks are a critical infrastructure subjected to attacks at its physical layer. Different methods have been presented to prevent, detect and solve these attacks. The current systems in charge of detecting intrusions in optical networks rely on the metrics obtained from OPM equipment. This equipment has a high cost, making the massive deployment through the optical network unfeasible. Photonic reservoir computing is a technology that has been able to solve tasks as header recognition, channel equalization, etc. with a good performance and a cost that allows it to be deployed over all the network. In this thesis it is designed and assessed by simulation a photonic reservoir computing system able to detect and classify attacks in optical networks.**

***Index Terms*—Attack detection, machine learning, optical network Security, photonic reservoir computing**

I. INTRODUCTION

Due to their data transmission capacity, optical networks are a fundamental part of the communication systems of a wide range of services. As a consequence, they have become a target of malicious attacks against the services they support. As it has been reported [1], the intrusions focus the physical layer due to its easy access and the cascade effect on the upper layers.

The most reported and one of the harmful attacks of the physical layer is the insertion of harmful signals to the fibre. This insertion can be done accessing the patch-panel or by means of creating a temporal coupler as described in [2]. If the signal overlaps the spectrum of the channel it is considered in-band jamming and unfilterable noise is added to the signal. An out-band jamming occurs when the signal is placed outside the used spectrum increasing the nonlinear effects of the optical network, and also reducing the gain of the amplifiers. Other types of attacks have been reported like a polarization modulation attack [3]: a polarization scrambling is introduced that is fast enough to make the polarization recovery algorithms unable to restore polarization state.

The efforts for protecting the optical physical layer can be classified in three tasks: *(i)* assurance by means of modelling the consequences of the attacks and minimizing its effects; *(ii)* assessment through the detection, classification, and localization of the attacks; and *(iii)* recovery using attack source neutralization, and network reconfigurations.

The assessment of the attacks has taken different approaches along time. Initially, it was based on power detection, spectrum analysis, reflectometry methods, and even manual detection, but due the heterogeneity of the networks and the attacks they presented a bad performance. Lately, machine learning algorithms that use metrics from optical performance monitoring (OPM) equipment have shown a high accuracy detecting the signature and intensity of attacks [3]–[5]. Although the good performance of these systems, OPM equipment is too costly to be deployed massively in the network.

Reservoir computing has been used to solve similar problems in other fields like the detection of attacks in electrical smart grids [6]. Also, photonic reservoir computing networks have state of the art performance solving problems such as speech recognition, time series forecasting and, Boolean logic operation [7]–[10]. In view of the above and taking into account that the cost of photonic reservoir computing makes possible to deploy it massively in the network, an attack detection for jamming attacks using this technology is presented.

II. LITERATURE OVERVIEW

The current methods to detect intrusions in optical networks rely on applying machine learning to the OPM equipment metrics. In [3] a supervised approach is studied, obtaining artificial neural networks (ANN) as the optimal algorithm. Also, the importance of the parameters that are fed to the are studied, concluding that, with seven parameters, the system is able to detect with almost a 100% of accuracy polarization scrambling, in-band and out-band jamming attacks. An unsupervised approach [4] has also been postulated in order to create a truly autonomous system that does not rely on previous information of the network, but its performance is still far to match its supervised counterpart.

Reservoir computing is a framework that derives from recurrent neural networks with the particularity that the part that allows having a temporal dynamic behaviour remains fixed, the reservoir. This allows the system to have an analog system as a reservoir. Photonics offers inherent parallelism and huge bandwidth making them very useful to exploit this advantage. Originally, a non-linearity was needed in each node of the reservoir but in [11] it was demonstrated that passive linear optical networks can act as a reservoir and the non-linearity can be added at the readout with the photodetector.

III. SYSTEM DEFINITION

A. Optical network attack simulation

VPI software has been used to simulate the optical-fiber link and asset the effects of the jamming intrusions. The same system has been used to simulate the in-band and out-band jamming using different parameterizations of the components. An overview of the system can be seen on Figure 1

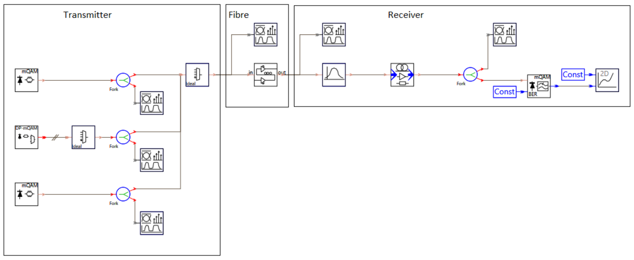

Fig. 1. Scheme of the optical fibre transmission link.

The transmitter is a WDM system with nine 4QAM at 25 GBauds carriers. The carrier central frequencies are equally spaced 100 GHz with an initial central at 192.9 THz. The signal is transmitted through a dispersion-managed fibre span with two-stage EDFAs before (Booster) and after (Line Amplifier) and also x-polarizer at its input. The length of the fibre is 100Km with an attenuation of 0.2dB/Km. The receiver is formed by a Gaussian band-pass filter, a costume module that saves the electric field of the signal and a coherent receiver that analyses the BER of the signal.

For both jammings, the intrusion signal it is multiplexed at the transmitter simulating access to the patch panel. In the case of in-band jamming, it is centred at 192.9 THz with a bandwidth of 100GHz (Figure 2) and in outband jamming, it is centred at 193.8 THz with a bandwidth of 25GHz (Figure 2).

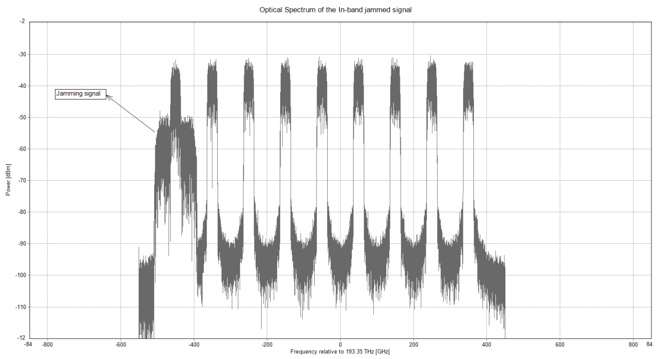

Fig. 2. Inband jamming in a WDM optical link.

The effects of the jamming signal have been studied by means on how the BER of the signal under test varies and it has been observed that it gets more affected when the intrusion is done inband (Figure 4 and Figure 5). Taking into account this study it has been decided to use a power of 1 mW for the inband jamming and of 10 mW for the outband jamming to train the photonic reservoir computing network.

B. Photonic reservoir computing simulation

For designing and optimizing the photonic reservoir computing system, the Photontorch platform has been used [12].

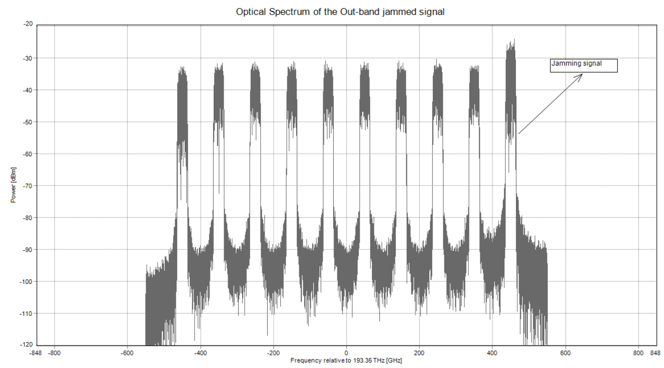

Fig. 3. Outband jamming in a WDM optical link.

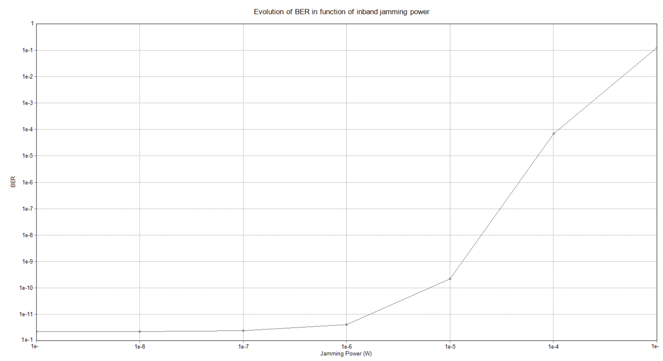

Fig. 4. BER versus the power of the inband jamming signal.

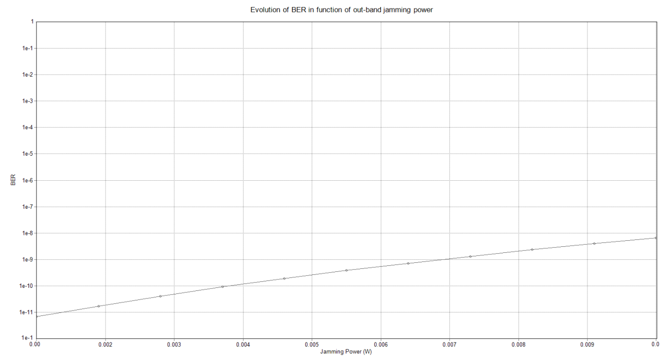

Fig. 5. BER versus the power of the outband jamming signal.

As previously mentioned the system is formed by a passive linear photonic network that acts as a reservoir and readout that adds the non-linearity.

For the reservoir, a passive photonic integrated circuit with a four-port architecture with sixteen nodes has been used (Figure 6) and the readout consists in a photodetector that combines the complex-valued states of the nodes into real-valued intensities.

In order to train the reservoir computing network, the complex fields from the different VPI simulations (inband jamming, outband jamming or without jamming) are loaded.

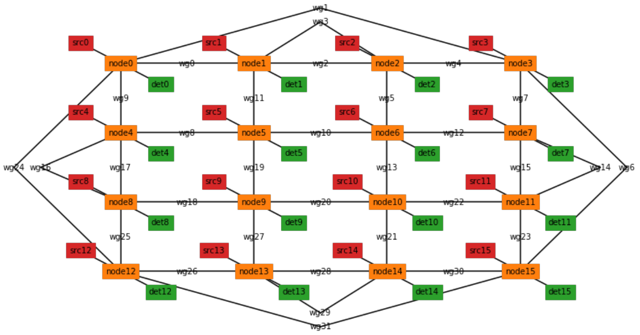

Fig. 6. Representation of the four-port reservoir architecture..

Then the cases are concatenated in pairs and a target tensor identifying each one is created to train and test the system. Finally, the signal and the target samples are shuffled in blocks.

With the tensors previously created the readout is trained using a binary cross-entropy loss preceded by a sigmoid and an AdamW optimizer. When doing the testing of the system, it was observed that the samples that tend to be classified incorrectly were placed after a changing of the scenario. In order to solve this problem, and taking into account that it is not necessary to detect the intrusion at the rate of the input samples, the outputs were grouped in groups and its mean was assigned to each of them.

IV. Results

The photonic reservoir computing system was tested for all the pairs of scenarios (inband jamming with no jamming, outband jamming with no jamming, and inband jamming with outband jamming) using different jamming signals (modulated ones and lasers). In all of them, the system was able to classify the scenario without any error.

After it was validated that the system worked correctly, different scenarios with lower jamming powers than the one used to train the reservoir computing network were tested. The limit of correct detection was found when the inband jamming power was under 1e-06, but in that scenario, the BER was under 1e-10 (in normal conditions operates with a BER around 1e-11) so it was considered a reasonable assumption that there was no jamming. In order to validate the results a transient analysis was also done, where a jamming signal was turned on and off.

Comparing the results with other approaches, the same accuracy is achieved as in the system using OEM metrics and supervised training of the algorithm [3] and a better performance when it is compared to the system unsupervised trained [4]. Although, the system is only able to classify between two cases while the other ones are able to classify until 7 different cases.

V. Conclusions

An attack detection system using photonic reservoir computing that is able to detect jamming attacks has been demonstrated. Even though it is not able to classify more than two scenarios simultaneously, its lower cost compared to OEM equimpent based methods allows it to be deployed massively in the network.

The following steps regarding this topic should be validating the simulated results in a real scenario. Also, the intrusion signal was only studied when it is added at the patch panel, but it can be also placed along the fibre making use of a temporal coupler. Another extension of the work is improving the system in order that it is able to classify and detect more than two scenarios at the same time and introducing the polarization scrambling attacks.

References

[1] InfoGuard, ”Data security in the converged enterprise network,” White Paper, Dec. 2018.

[2] T. Uematsu, H. Hirota, T. Kawano, T. Kiyokura, and T. Manabe, “Design of a temporary optical coupler using fiber bending for traffic monitoring,” in *IEEE Photon. J.*, vol. 9, no. 6, pp. 1–13, Dec. 2017.

[3] Carlos Natalino, Marco Schiano, Andrea Di Giglio, Lena Wosinska and Marija Furdek, “Experimental Study of Machine-Learning-Based Detection and Identification of Physical-Layer Attacks in Optical Networks” in *Journal of Lightwave Technology*, vol. 37, no. 16, pp. 4173-4182, 15 Aug.15, 2019, doi: 10.1109/JLT.2019.2923558.

[4] Marija Furdek, Carlos Natalino, Marco Schiano, and Andrea Di Giglio, “Experiment-based detection of service disruption attacks in optical networks using data analytics and unsupervised learning,” Proc. SPIE 10946, Metro and Data Center Optical Networks and Short-Reach Links II, 109460D (1 February 2019)

[5] M. Bensalem, S. K. Singh, and A. Jukan, “On detecting and preventing jamming attacks with machine learning in optical networks,” under submission in *IEEE GLOBECOM*. IEEE, 2019.

[6] K. Hamedani, L. Liu, S. Hu, J. Ashdown, J. Wu and Y. Yi, “Detecting Dynamic Attacks in Smart Grids Using Reservoir Computing: A Spiking Delayed Feedback Reservoir Based Approach,” in *IEEE Transactions on Emerging Topics in Computational Intelligence*, doi: 10.1109/TETCI.2019.2902845.

[7] L. Appeltant, M. C. Soriano, G. Van der Sande, J. Danckaert, S. Massar, J. Dambre, B. Schrauwen, C. R. Mirasso, and I. Fischer, “Information processing using a single dynamical node as complex system,” in *Nature communications*, 2:468, 9 2011.

[8] Kristof Vandoorne, Pauline Mechet, Thomas Van Vaerenbergh, Martin Fiers, Geert Morthier, David Verstraeten, Benjamin Schrauwen, Joni Dambre, and Peter Bienstman, “Experimental demonstration of reservoir computing on a silicon photonics chip. Nature communications,” 5:3541, 1 2014.

[9] L. Larger, M. C. Soriano, D. Brunner, L. Appeltant, J. M. Gutierrez, L. Pesquera, C. R. Mirasso, and I. Fischer, “Photonic information processing beyond Turing: an optoelectronic implementation of reservoir computing,” in *Optics Express*, 20(3):3241, 1 2012.

[10] Quentin Vinckier, Franois Duport, Anteo Smerieri, Kristof Vandoorne, Peter Bienstman, Marc Haelterman, and Serge Massar, “High-performance photonic reservoir computer based on a coherently driven passive cavity,” in *Optica*, 2(5):438–446, 2015.

[11] Kristof Vandoorne, Pauline Mechet, Thomas Van Vaerenbergh, Martin Fiers, Geert Morthier, David Verstraeten, Benjamin Schrauwen, Joni Dambre, and Peter Bienstman, “Experimental demonstration of reservoir computing on a silicon photonics chip,” in *Nature communications*, 5:3541, 1 2014.

[12] Floris Laporte, Joni Dambre, and Peter Bienstman, “Highly parallel simulation and optimization of photonic circuits in time and frequency domain based on the deep-learning framework PyTorch,” Scientific reports 9.1 (2019): 5918.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

Due to their data transmission capacity, optical networks are a fundamental part of the communication systems of a wide range of services. As a consequence, they have become a target of malicious attacks against the services they support. As it has been reported [1, 2], the intrusions focus the physical layer due to its easy access and the cascade effect on the upper layers.

The efforts against these attacks can be classified depending on their aim: prevention, detection or recovery. This thesis focuses in the detection problem when the attacks are done by means of an intrusion signal, this signal can be used to disrupt communication and also to listen to the information carried by means of cross-talk.

Different approaches have been presented to solve that problematic. The first ones were based on power detection, spectrum analysis, reflectometry methods, and even manual detection. They presented problems of generalization due the heterogeneity of optical networks and the attacks, also their performance decreased when the signal was nosy.

Recently, machine learning algorithms that use metrics from optical performance monitoring (OPM) equipment have shown a high accuracy detecting the signature and intensity of attacks [3, 4, 5]. Although the good performance of these systems, OPM equipment cost makes the massive deployment of this systems unfeasible.

In this thesis, a new technique to solve the detection problem is presented using reservoir computing (RC). This technology is very suitable for photonic networks because their inherent parallelism and huge bandwidth. Also, its performance has been validated achieving state of the art in tasks as speech recognition, time series forecasting and, Boolean logic operation [11, 12, 13, 14]. The advantages over previous systems is a lower energy consumption and a lower cost of deployment. Furthermore, outside the photonics field, RC has already been used in similar tasks like the detection of false data injection in electrical smart grids [10].

1.2 Optical networks attacks

As previously mentioned, the attacks in optical networks usually aim its physical layer to affect in cascade the upper layers. Even though the disturbances of the physical layer affect the current Wavelength Division Multiplexed (WDM) systems, they become even more remarkable with new physical-layer paradigms like quantum key distribution (QKD) and space division multiplexing (SDM). This, combined with the huge data-rates carried today and its tight requirements, make the managing of the security at the optical physical layer a key issue on optical networks.

The managing of the security in optical networks can be divided into three main tasks:

- The security assurance by means of modelling the consequences of the attacks and minimize its effects by means of data encryption and scrambling techniques [6, 7, 8, 9].

- The security assessment through the detection, classification, and localization of the attacks [3, 4, 5].
- The attack recovery using attack source neutralization, and network reconfigurations [15, 16].

The system presented in this project aims to offer an alternative to the current security assessment systems.

1.2.1 Types of attacks

The most reported and one of the harmful attacks in the optical physical layer is the insertion of intrusion signals to the fibre. These signals increase the nonlinear effects of the system, reduce the gain of the amplifiers and add unfiltrable noise at the spectrum they use. The consequences are a degradation of the quality of the channel that can even make it useless.

The insertion of the intrusion signal can be done accessing the patch-panel and also by means of creating a temporal coupler as described in [17].

The jamming attacks can also be classified depending if the spectrum used matches the transmitted channel:

- Inband jamming: The harmful signal overlaps the spectrum of the channel adding unfiltrable noise that reduces the optical signal-to-noise ration (OSNR). In this case, normally, the intrusion signal has a higher bandwidth than the useful signal in order to affect a broader spectrum. As a consequence, the power spectral density (PSD) of the intrusion signal is lower compared to the useful signal. An example of the received optical spectrum of a system suffering inband jamming can be seen in figure 1.1.

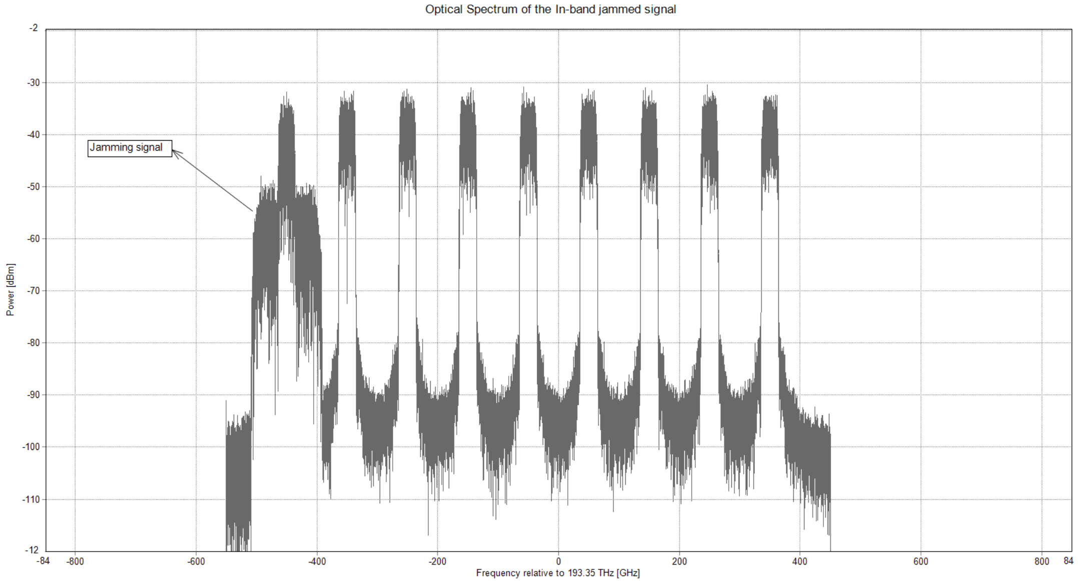

Figure 1.1: Inband jamming in a WDM optical link.

- Outband jamming: The harmful signal is placed outside the used spectrum and reduces the quality of the other channels by means of power reduction and increase of non-linearities due to the limitations of erbium-doped fibre amplifiers (EDFA). In this jamming, the harmful signal usually has the same bandwidth than the useful signal and equal or higher power. An example of the received optical spectrum of a system suffering outband jamming can be seen in figure 1.2.

Apart from the insertion of harmful signals, there are attacks that do not require fiber intrusion. One of them is the application of a fast polarization scrambling, whose effect is making polarization recovery algorithm unable to restore polarization state [3].

The system presented in this thesis is only able to identify and classify the jamming attacks due to the fact that the photonic reservoir computing systems used is not sensitive to the polarization of the signal.

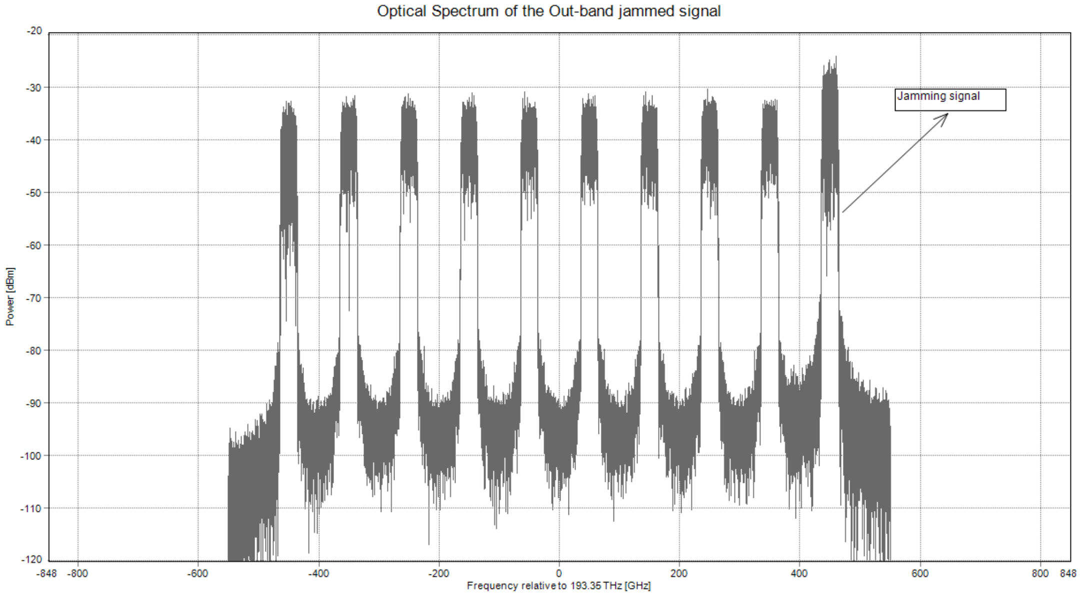

Figure 1.2: Outband jamming in a WDM optical link.

1.2.2 Attack detection approaches

The recent approaches in the assessment of the network attacks have been done by means of processing the metrics obtained form OPM equipment, usually by means of machine learning (ML) algorithms.

In [5] the OPM equipment used is a WDM analyzer that obtains the power and OSNR for all the channels. Using these metrics, different ML algorithms have been tested concluding that ANN is the one that offers better performance, with an accuracy of 100% in outband jamming attack detection and an accuracy of 99% when it also locates the attack by identifying the channel jammed. Additionally, a novel resource reallocation scheme that utilizes the statistical information of attack detection accuracy to lower the probability of successful jamming of lightpaths while minimizing lightpaths' reallocations is proposed.

In [3, 4] the metrics that are fed to the ML algorithms are obtained from the coherent receiver. These can be seen in Table 1.1.

Acronym	**Unit**	**Description**
CD	ps/nm	Chromatic Dispersion
DGD	ps	Diferential Group Delay
OSNR	dB	Optical Signal to Noise Ratio
PDL	dB	Polarization Dependent Loss
Q-factor	dB	Q factor
BE-FEC	Bits	Block Errors before FEC
BER-FEC	Bps	Bit Error Rate before FEC
UBE-FEC	Blocks	Uncorrected Block
BER-POST-FEC	Bps	Bit Error Rate after FEC
OPR	dBm	Optical Power Received
OPT	dBm	Optical Power Transmitted
OFT	MHz	Optical Frequency Transmitted
OFR	MHz	Optical Frequency Received

Table 1.1: Metrics obtained from the OPM equipment [4].

In [3] different supervised learning algorithms are tested in order to identify the type of attack between inband jamming, outband jamming and polarization scrambling. Another classification is done depending if the intensity of the attack is high or low. It is revealed that the optimum machine learning algorithm for detecting attacks is ANN with a 99.9% of accuracy. Finally, the importance of the different metrics that the coherent receiver facilitates is studied, revealing that with only seven of them is enough to achieve the same performance as using all of them. In Figure 1.3 it is shown the evolution of the accuracy of the ANN in function of the numbers of parameters it uses, ordering them in function of its impact.

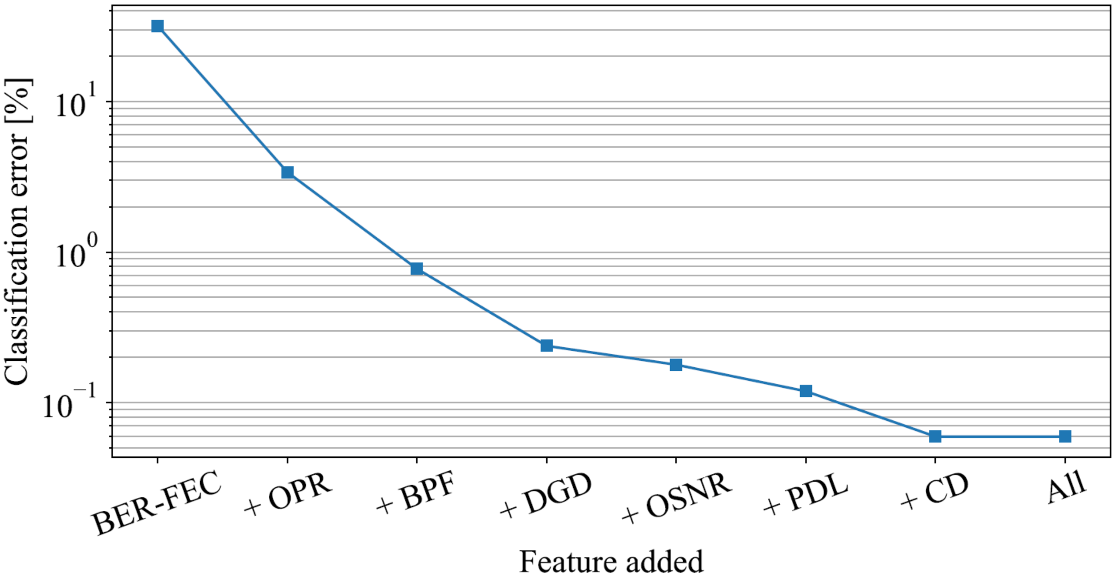

Figure 1.3: ANN classification error in function of parametrs used [3]

An unsupervised ML approach is described in [4] to detect insertions of harmful signals in the system without prior knowledge of the attacks in order to have a truly autonomous system that does not rely on previous information of the network. Although it defines a system that offers an accuracy of 92% (with a false negative rate of 7,69%), its performance is still far from the supervised methods [3].

1.3 Reservoir computing

Reservoir Computing (RC) is an artificial intelligence framework that derives from Recurrent Neural Networks (RNN), which in turn are a class of Artificial Neural Networks (ANN). The main characteristic of this system is that the part that allows having a temporal dynamic behaviour remains fixed.

Having a part of the network fixed presents advantages in front of other RNN approaches like reducing the time of convergence time and consuming less power due to the fact the fewer parameters are trained. Furthermore, these networks allow the use of an analogue system for the fixed part. This last advantage has been exploited in photonics because of its inherent parallelism and its huge bandwidth.

1.3.1 Machine learning

Machine Learning is the study of algorithms that are able to learn to solve tasks without being expressly programmed to do so. Depending on the approach they take in learning, they can be classified in the following:

- Reinforcement learning: The algorithm interacts with the environment and improves using the feedback of its actions.
- Supervised learning: The algorithm uses the input data and the expected output to learn the correspondence between them.
- Unsupervised learning: The algorithm uses only input data and learns their structure.

Various machine learning models have been defined and improved along time in order to adapt to the needs and the technology available, but lately, the one that is catching more attention is ANN because of its performance and customization. These networks are based on a primitive scheme of how the brain works, consisting of interconnected nodes, also called neurons, which compute an output from the inputs they receive (similar to the neurons and the synapses in biology).

The most common node and the one that give a better overview of ANN are the perceptrons. Its basic structure consists of applying an activation function, in order to add a nonlinearity in the system, to a weighted sum of the inputs plus the bias as can be seen in Figure 1.4.

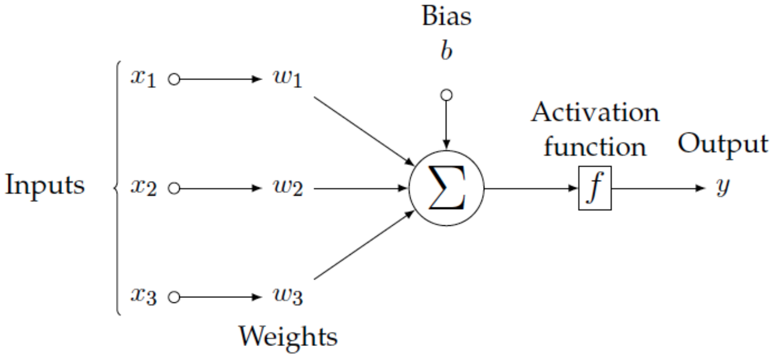

Figure 1.4: Scheme of the model of the perceptron.

The equation (1.1) represents the mathematical operation of the perceptron. Being **x** the vector representing the inputs, **w** the vector of weights, **x**·**w** the dot product, b the bias, *f()* the activation function and y the output.

$$y = f(\mathbf{w} \cdot \mathbf{x} + b) \tag{1.1}$$

An activation function need to present a nonlinearity in order that the system is able to detect nonlinear patterns. Apart of this, the following properties are desirable: smooth, continuous, derivable and almost linear. In order to get an overview of them the following three of the most significant functions are presented:

$$sigmoid(x) = \frac{1}{1 + e^x} \tag{1.2}$$

$$tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}} \tag{1.3}$$

$$ReLU(x) = max(0, x) \tag{1.4}$$

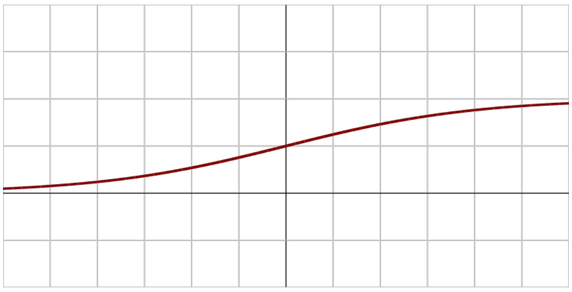

Figure 1.5: Sigmoid function.

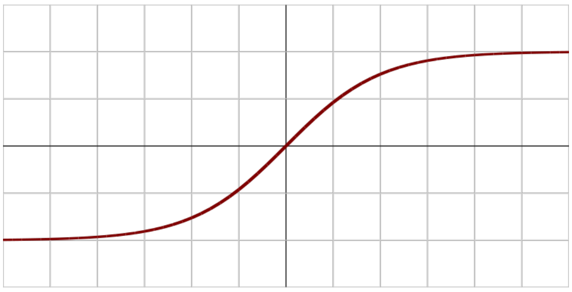

Figure 1.6: Tanh function.

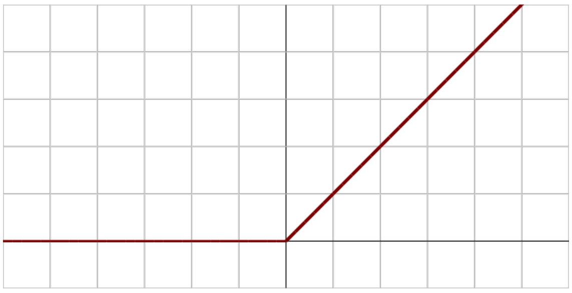

Figure 1.7: ReLU function.

The learning takes place by adapting the network to solve a particular task based on particular samples. This adaptation is done by means of adjusting the weights of the network and the threshold (bias parameter) in order that the output minimizes the error perceived.

Practically, this is done by defining a cost function that is evaluated periodically and whose gradient allows the backpropagation to update the weights.

The cost function measures the quality of a particular set of parameters based on how well the output of the network agrees with the ground truth labels in the training data. Depending on the task different loss functions are used:

- In regression the network predicts continuous,numeric variables. Absolute loss (L1 distance), square loss (L2 distance) and Hubber Loss are among the most popular.
- In classification the network predicts categorical variables. Hinge loss, Cross-entropy loss and Focal loss are the most used.

Once defined the loss function, the gradient is computed and then backpropagated through the network to obtain gradients for each parameter. With these gradients an optimizer updates the weights. The optimizers that have shown better performance are the ones with an adaptative learning rate as root mean square propagation (RMSProp) and adaptive moments (Adam).

The neurons are usually aggregated to form layers and depending on its position in the information flow are called input layers (the ones that receive the input signal), hidden layers (the intermediate layers) and output layers (the ones that display the output).

Two main types of networks can be defined in function on how the nodes are connected:

- The feed-forward neural networks (FFNN) where the information flows only forward, from the input layer to the output layer through the hidden ones.
- The RNN where the connections are also recursive (the state of the nodes is used in future iterations) allowing the system to exhibit a temporal behaviour.

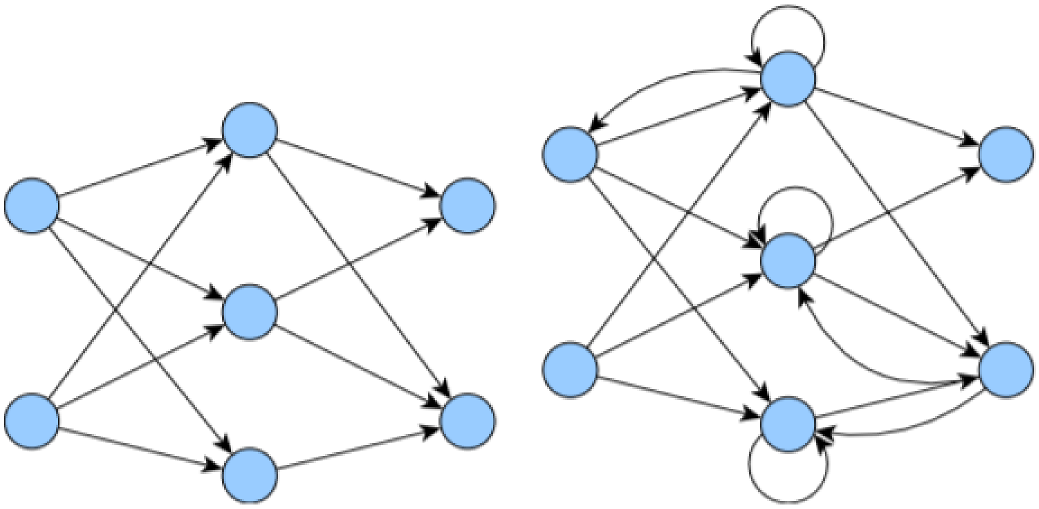

Figure 1.8: Architecture of a FFNN (left) and a RNN (right).

1.3.2 Reservoir computing

Reservoir computing, originally appeared as a solution to decrease the complexity of the training in an RNN and its computational cost by reducing the parameters of the network that need to be trained. Even though the actual RNN have solved most of these issues, RC is still relevant due to its use in analogue computation.

The first approach in Reservoir Computing was done by Buonomano [18] and it was reinvented independently by Jaeger with echo state machines (ESM) [19] and Maass with liquid state machines (LSM) [20]. These systems are composed of three sections:

- An input layer where the signal is decoupled in order to be fed to the system.
- A reservoir that transforms the input signal to a higher dimensional space using recurrent connections, it remains fixed and needs to be made up of non-linear units

and be able to store information.

- A readout that combines the outputs of the Reservoir as an artificial neural network.

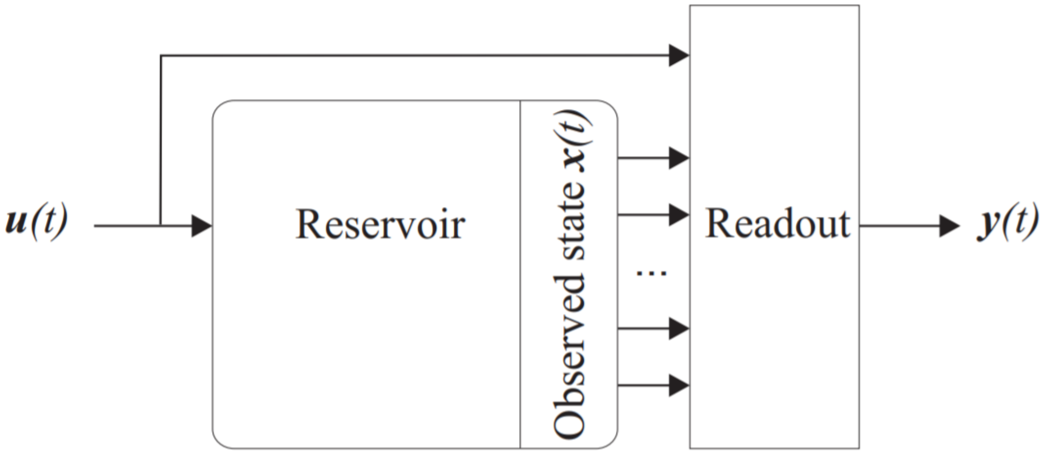

Figure 1.9: Schematic representation of a reservoir computing system.

1.3.3 Photonic reservoir computing.

As previously mentioned RC has found its place with analogue systems and photonics is presented as an interesting candidate because of its huge bandwidth, inherent parallelism, low computational and energy consumption and time-depend non-linearities.

In photonic RC we can differentiate between two approaches, the delay-based [21] and the spatially distributed. On the first one, the reservoir is formed by only a hardware node with a feedback loop and different virtual nodes are created by means of time multiplexing using a masking signal.

The systems usually use Mach-Zehnder modulators and the feedback loop can be done by means of an optoelectronic system or in the optical domain using couplers and circulators. An scheme can be observed in Figure 1.10

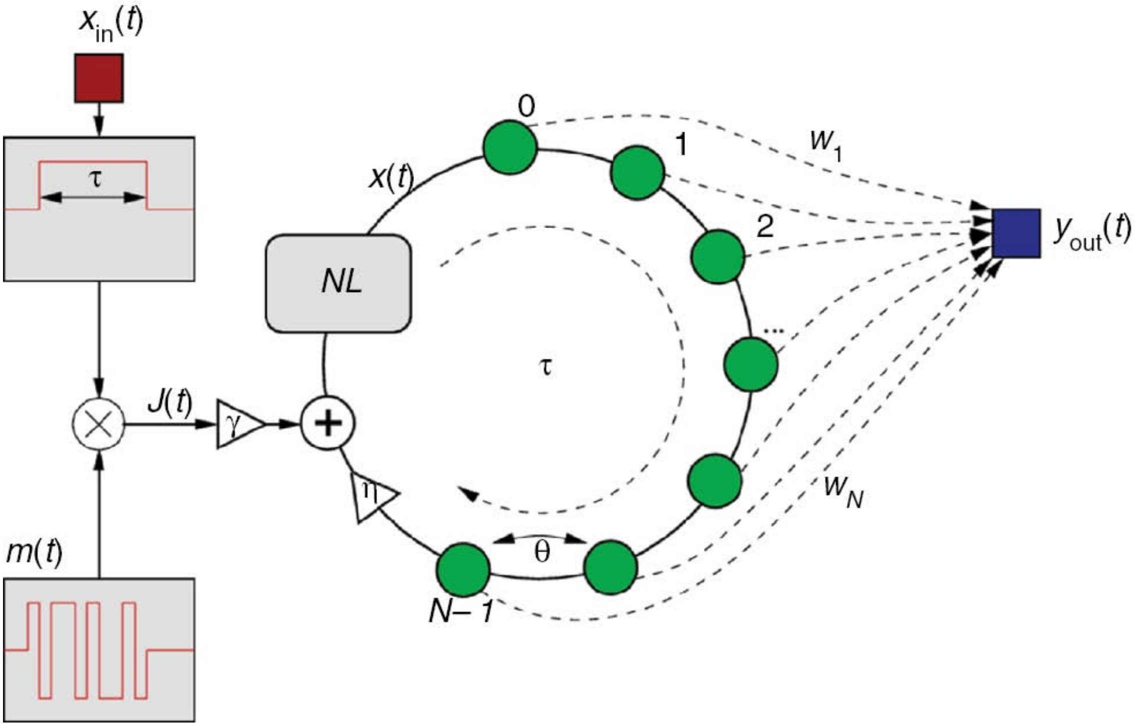

Figure 1.10: Structure of a delay-based reservoir computing.

The second approach is more intuitive and it is composed of different physical nodes interconnected in the optical domain that are fed to the readout. Some of the nodes that have been studied are semiconductor optical amplifiers (SOAs) [22], photonic crystal cavities [23] and microring resonators [24]. The previous nodes present nonlinearities that mimic the activation function, but it has been also demonstrated that passive linear optical networks can act as a reservoir and the nonlinearity can be added at the readout [25].

In passive photonic reservoir computing the reservoir is a linear network formed by passive photonic integrated circuit (PIC) components like combiners, splitters and long waveguides (spirals) that interconnect the nodes. The nonlinearity is introduced through the use of a photodetector that combines the complex-valued states of the nodes to real-valued intensities.

Even though these networks don't offer the same performance in highly nonlinear tasks in comparison with non-linear photonic networks, they offer benefits as simplicity of production and operation with less power requirements, which in turn makes that the temperatures of the system more stable allowing an easy thermal management control. These advantages made them a good choice when mass production and operation is needed. Some of the tasks where these systems have demonstrated to be an important alternative are bit-sequence processing tasks, header recognition and equalization.

1.4 Objectives

As mentioned in this introduction, optical networks are vulnerable to attacks in the physical layer that can derive in affections to the infrastructures that they support. One of the most important part in order to overcome these attacks is to detect and classify them to take the appropriate measures, but this is no trivial due to the heterogeneity of the attacks and the network.

The current methods to solve that task offer a very good performance detecting and classifying the attacks, but they relay in metrics obtined from high cost equipment that makes non-viable to deploy them massively in the network.

Passive photonic reservoir computing systems have demonstrated to be able to perform state of the art tasks in optical networks and also reservoir computing has been used in a similar problem in another field. Moreover, they are able to be mass-produced and deployed with little power consumption.

At the light of the previously mentioned, in this thesis is intended to design and evaluate an alternative to the actual attack detection methods based on the use of passive photonic reservoir computing systems in order to allow the deployment of these systems throw all the network.

All the work will be done by means of simulation, first modelling the optical network and the attacks with VPI and then feeding the complex electric field obtained to a passive photonic reservoir network designed and optimized with Photontorch.

Chapter 2

Optical network attack simulation

2.1 VPI Software

In order to model a complete optical link and the jamming attacks, different components with different characteristics and effects need to be modeled. With the aim to overcome this difficulty, there are software that offer predefined components and allow the user to connect and configure them.

VPI is one of the most complete optical transmission simulators by having a wide range of predefined components and optical systems that can be interconnected and parameterized. It is worth mentioning that it also includes demos of optical links that can be used as a foundation for similar links.

Regarding the customization of the optical network, it offers the possibility to define custom components using Python or Matlab that can operate over the optical domain and the electric one.

Finally, it allows the assessment of the performance of the link by checking characteristics of the signal as the spectrum or the eye diagram and also quality measures like the bit error rate (BER).

2.2 Jamming attacks set-up

In order to study the effects of the jamming attacks, we have designed a complete optical-fibre transmission link that can be divided into three stages: the transmitter, the fibre and the receiver.

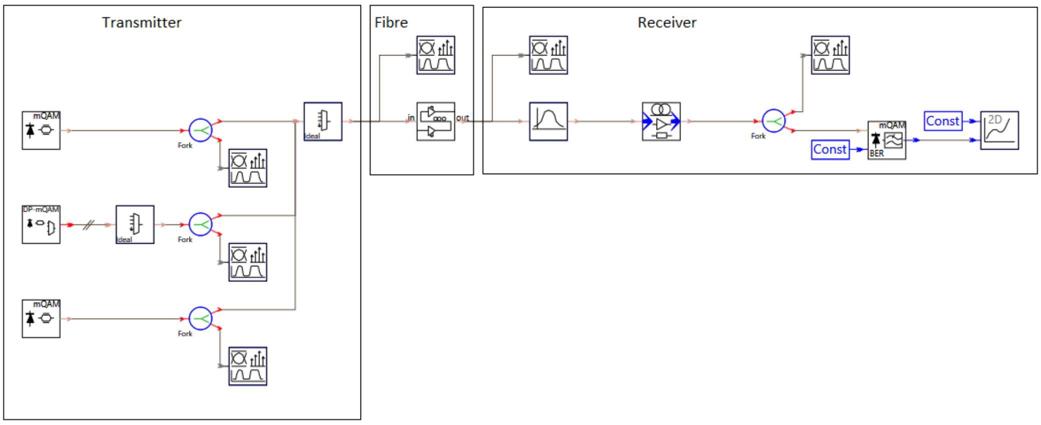

Figure 2.1: Scheme of the optical fibre transmission link.

The transmitter represents a WDM system that multiplexes nine 4QAM carriers at 25 GBauds with a transmission power of 0dBm. The carrier central frequencies are equally spaced 100 GHz with an initial central frequency at 192.9 THz.

The number of carriers, its central frequency and the bandwidth used was decided based on previous studies, like [3] in order to make the results obtained comparable. The 4QAM modulation was chosen in order to represent a system with a coherent modulation and the fact that the signal is not polarization multiplexed like in previous works is because the passive photonic reservoir network used is not sensitive to the polarization of the signal.

As we can see in figure 2.2 the transmitter transmits three signals:

- The signal under test whose central frequency is placed at 192.9 THz. It will be the carrier that will be fed to the reservoir so the BER for the different scenarios will be monitored.
- The multiplexed signals that is composed for eight carriers equally spaced at 100 GHz starting at 193 THz.
- The jamming signal that will simulate an intrusion on the patch panel and whose parameters will be specified in the next section.

The transmitters of the signal under test and the multiplexed signals are VPI modules based on Mach-Zehnder modulators.

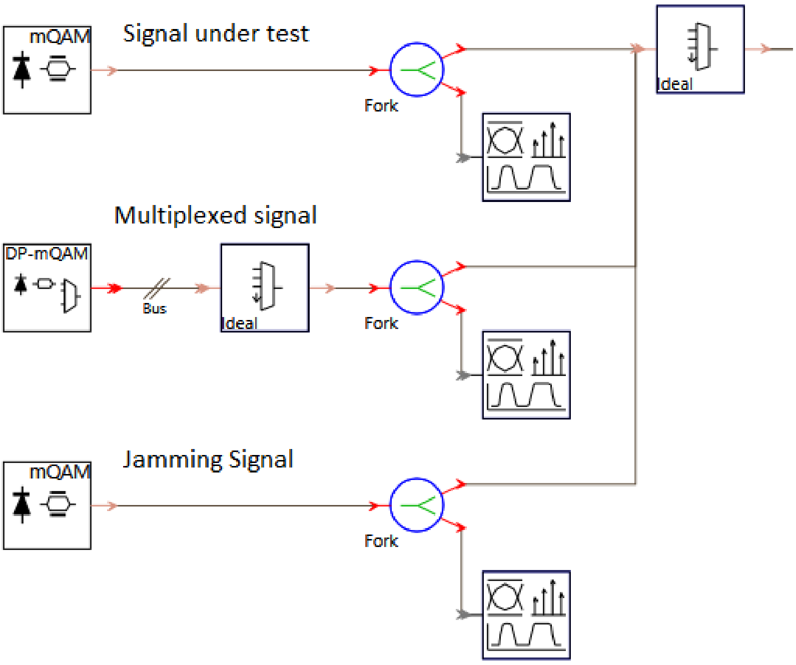

Figure 2.2: Signals multiplexed in the transmitter.

The VPI module used as the fibre is a dispersion-managed fibre span with two-stage EDFAs before (Booster) and after (Line Amplifier) and also x-polarizer at its input. The length of the fibre is 100Km with an attenuation of 0.2dB/Km. A scheme of it can be seen in figure 2.3.

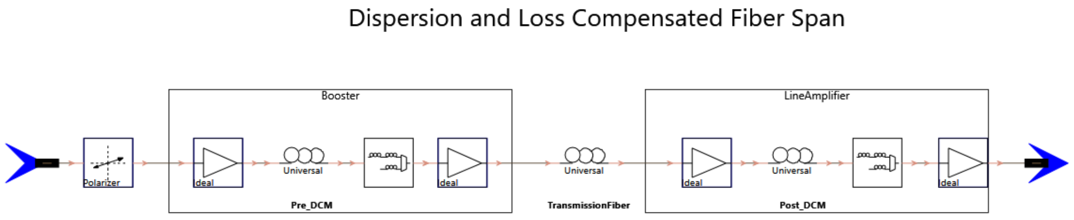

Figure 2.3: Scheme of the fibre module.

The receiver is formed by a Gaussian band-pass filter centered at the central frequency of the signal under test, a costume module that saves the electric field of the signal and a coherent receiver that analyses the BER of the signal as can be seen in figure 2.4.

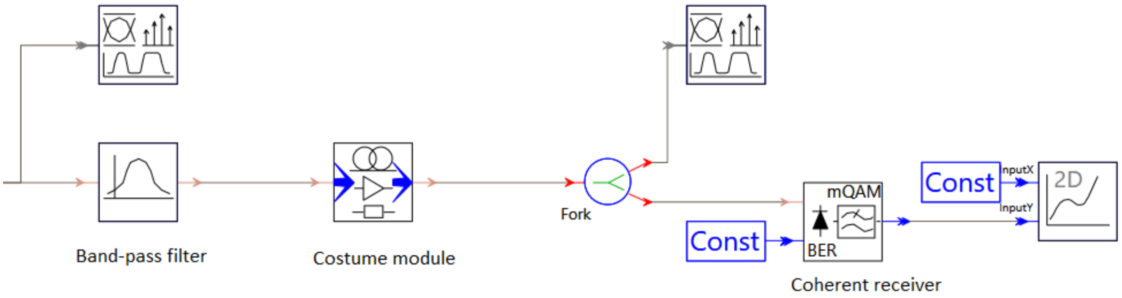

Figure 2.4: Scheme of the fibre module.

Finally, the general parameters used in the simulations are a sampling rate of 200 GHz during 40.96 ns. Furthermore, a transient analysis has been done to validate the results using the same sampling rate and introducing a jamming signal that is turning on and off every 8 ns during 8 cycles (128 ns).

2.3 Outband and inband jamming parametrization

As explained in previous sections, two types of jamming will be analyzed: the inband, when the signal overlaps the frequency of the signal under test, and the outband, when an extra carrier is added to the system. Both intrusion signals are added to the multiplexer, simulating an access in the patch-panel. In order to model the intrusion signal two approaches have been taken into account: when the jamming signal is a modulated signal (Figures 1.1 and 1.2) and when it is a CW laser (Figures 2.5 and 2.6).

In the case of in-band jamming, an intrusion signal centred at 192.9 THz is added, being a 4QAM transmitter at 100 GBauds when the signal is modulated and a laser with 100GHz of linewidth when a CW laser is used.

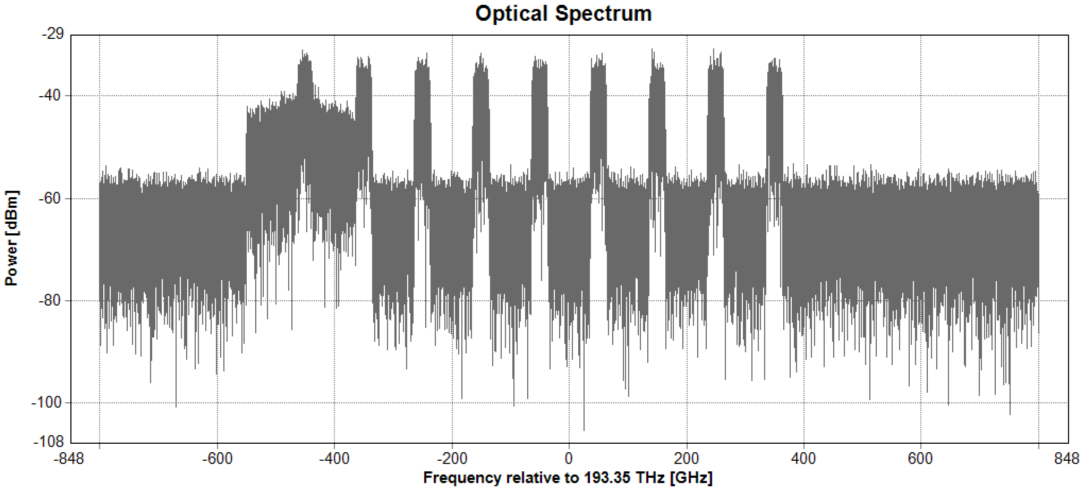

Figure 2.5: Inband jamming in a WDM optical link with a CW laser.

In outband jamming, the intrusion signal is centred at 193.8 THz and the intrusion signal can be a 4QAM modulated signal at 25 GBauds or a CW laser with a 25GHz of linewidth.

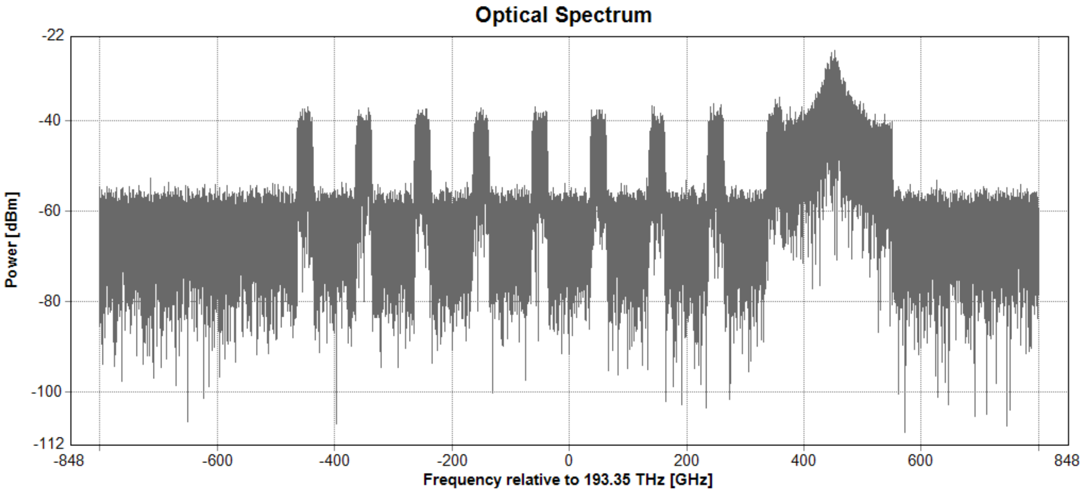

Figure 2.6: Outband jamming in a WDM optical link with a CW laser.

The effects of the intrusion signals have been studied by means of the analysis of the evolution of the signal under test BER when different jamming powers are used. This has been done for both scenarios, inband and outband jamming. The conclusions were that the BER of the signal under test is more affected by the inband intrusions (Figure 2.7) than by the outband ones (Figure 2.8). Taking into account these results it has been decided to use a jamming power of 1 mW for inband intrusion and one of 10 mW for the outband intrusion for the training of the network.

In order to train the photonic reservoir computing network it is also necessary to have samples when there is no jamming to represent the normal conditions of the optical link (Figure 2.9). A simulation has been done and it has been found that the BER in that case is 1.73e-12 a value that is achieved when the inband intrusion power is below 1e-5 mW and when it is lower than 1e-3 mW for outband intrusion .

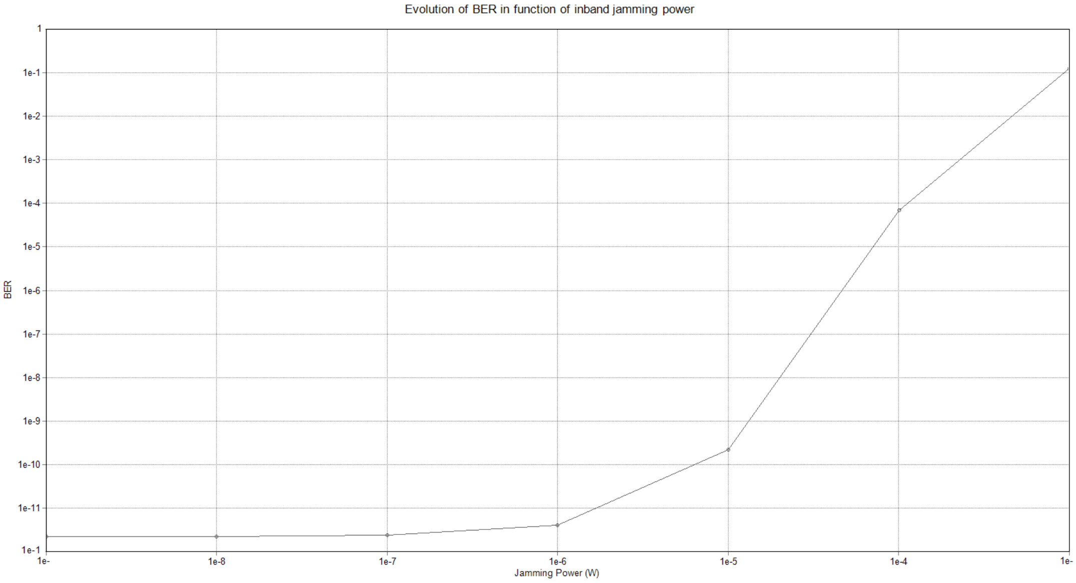

Figure 2.7: BER versus the power of the inband jamming signal.

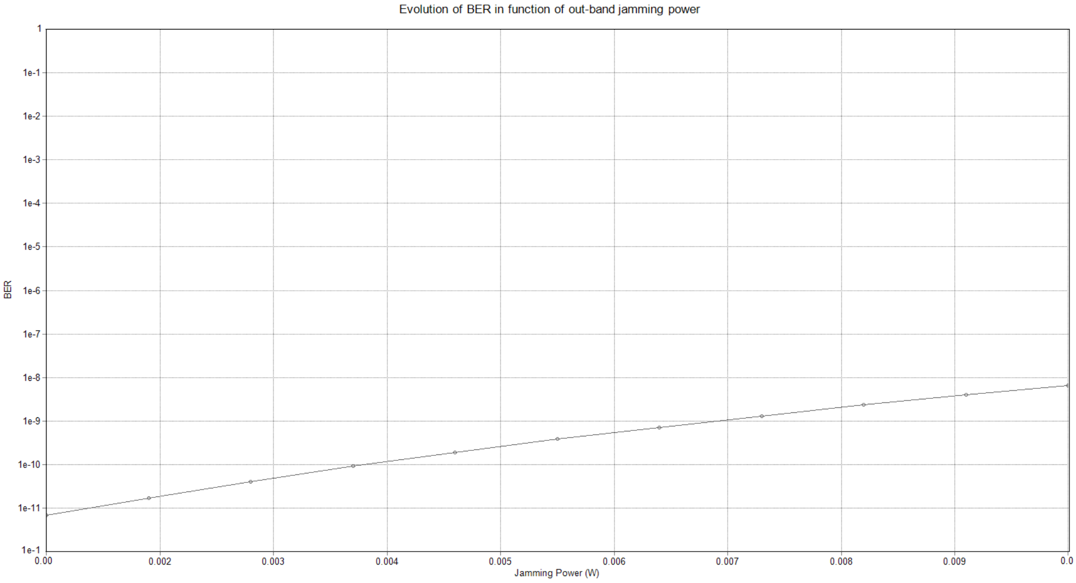

Figure 2.8: BER versus the power of the outband jamming signal.

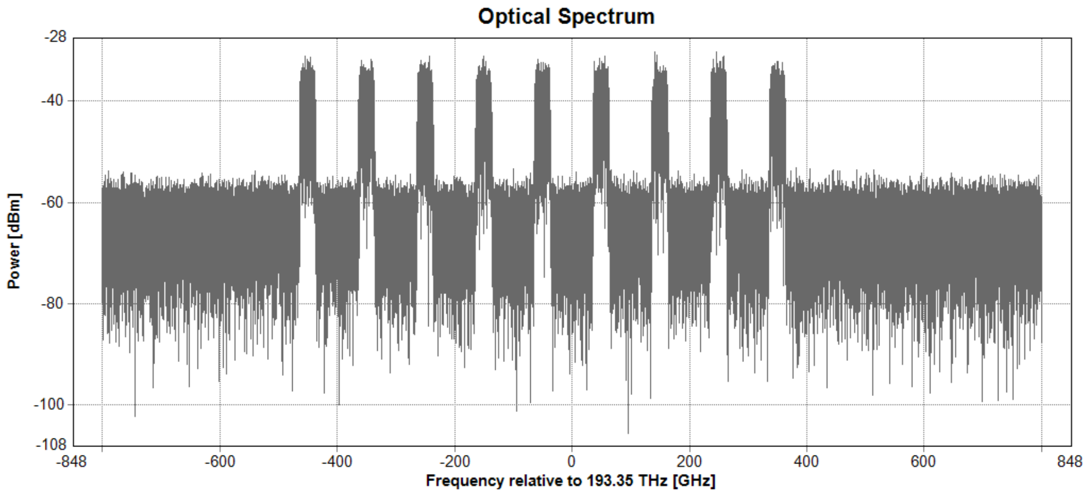

Figure 2.9: Spectrum of WDM optical link

Finally, a transient analysis where the jamming signal is turned on and off in time has been performed in order to verify the performance of the system (Figure 2.10).

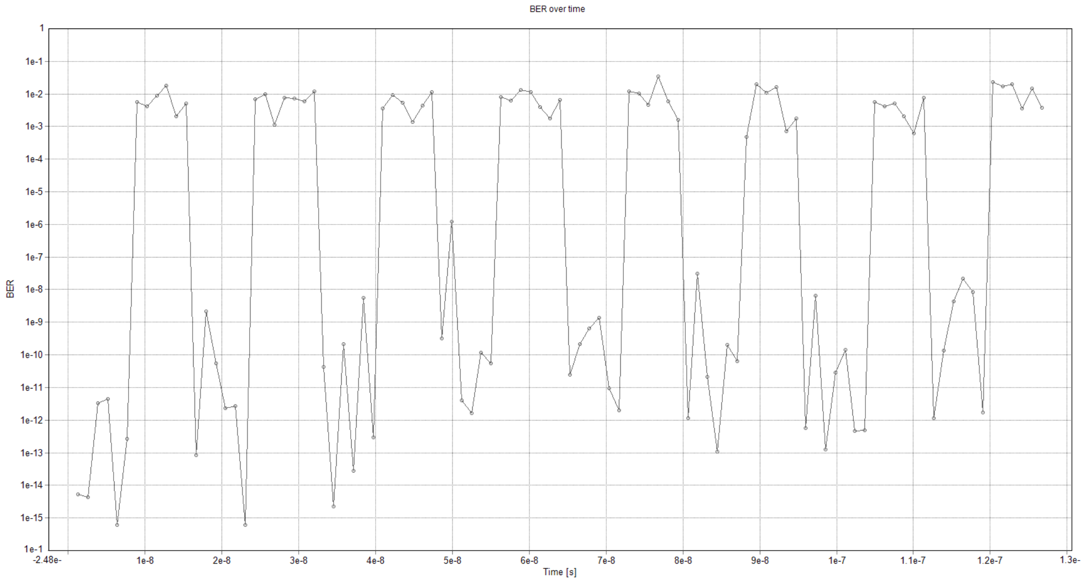

Figure 2.10: Evolution of the BER in the transient analysis.

Chapter 3

Photonic reservoir computing simulation

3.1 Photontorch

Once we have obtained the complex electric field from VPI, we need to feed it to the system that will be in charge of simulating the photonic reservoir computing system. The platform used to design and optimize this system is Photontorch [26].

Photontorch is a photonic circuit simulation software written in Python that relays in PyTorch, a machine learning framework. The PyTorch tensors, which are used to define the S-matrices of the components of the circuit, are arrays that can be placed on the Graphical Processing Unit (GPU) enabling high parallelization of the simulations. Because PyTorch is a tool designed to perform machine learning, the tensors are able to save the gradient enabling backpropagation that is the default optimization method for ANN.

In Photontorch the main building block is the component, it contains its ports and the relation to the other ports by means of the scattering matrix. It also keeps track of which of its ports are active, which means that the action depends also on an the internal state. Also networks can also be seen as a component whose S-matrix is composed by the joined S-matrices of each component and its connectivity allowing hierarchical structures.

3.2 Configuration and training

In this section, the procedure of defining, training and testing the attack detection photonic reservoir computing system is explained. The system has been based on an example of PT_central repository developed by the photonics research group at Ghent University.

First of all, the complex electric fields obtained from the different VPI simulations (inband jamming, outband jamming or without jamming) are loaded. As previously mentioned, the system is only able to detect two different scenarios, so these are concatenated. Also, a target array describing the type of scenario (1 or 0) is created. It has been tested that using 1 for the scenario that is expected to have more power and 0 for the one with less power in the target tensor improves the performance of the system.

In order to perform machine learning, it is better to have the two scenarios interspersed, so the concatenated signal and the target array are jointly randomly shuffled in blocks of 256 samples. After that, the signals and their targets are divided into train and test having a size of 98304 and 32768 respectively.

From the previous data, PyTorch tensors from the signal and the target are created matching the architecture of the network. In our case, the architecture used will have sixteen nodes and the electric field will be fed to the inputs 5,6,13 and,14.

After defining the input tensors, the reservoir architecture that will process the tensor to simulate the states need to be created. In our case, a four-port architecture with sixteen nodes that is predefined in the PT_central repository has been used. A representation of the architecture used can be seen in Figure 3.1

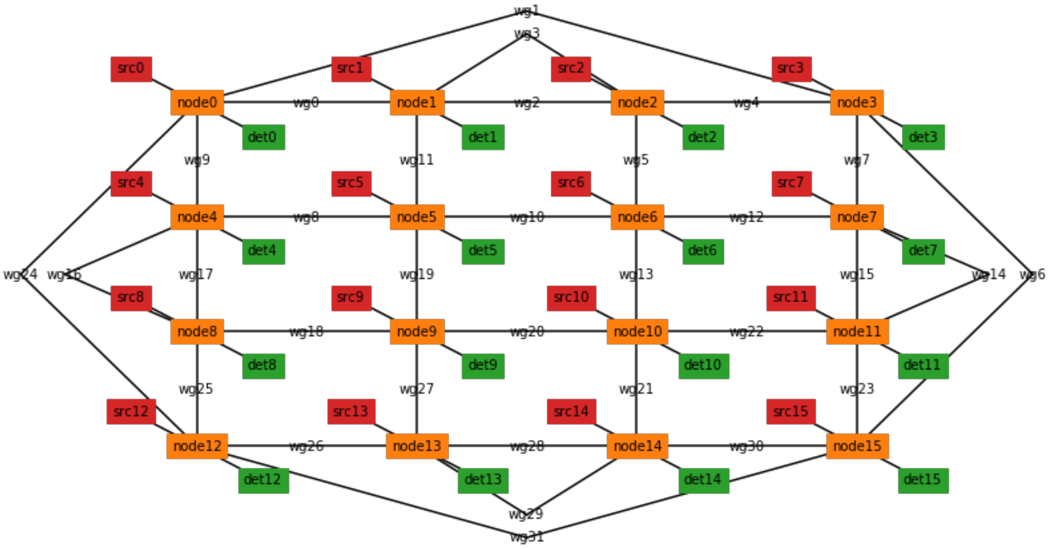

Figure 3.1: Representation of the four-port reservoir architecture.

Now that the signals and the architecture have been defined one can finally simulate the states that will be used for the machine learning. In order to do this the simulation environment is created defining the time of simulation and the wavelength of the signal. After that the tensor is processed with the reservoir architecture and the states are obtained. The output power of these states can be seen in Figure 3.2.

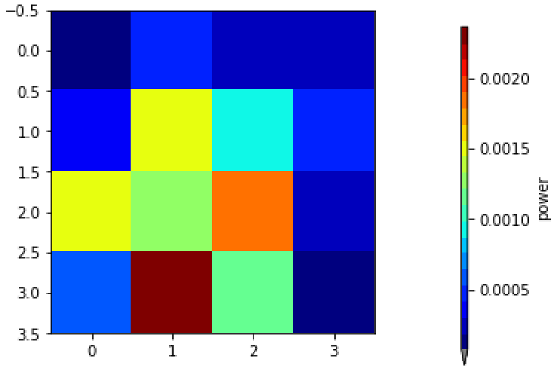

Figure 3.2: Mean output power of the states of the reservoir.

The only remaining part of the system is the readout and it is created also using a model included in PT_central repository. Once loaded, its parameters (weights and bias) are initialized with random values between 0 and 1. The amplitude and the phase of this random initialized reservoir can be seen in Figures 3.3 and 3.4.

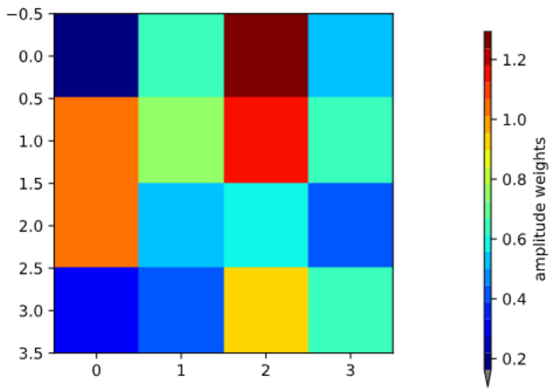

Figure 3.3: Amplitude of the weights of the reservoir.

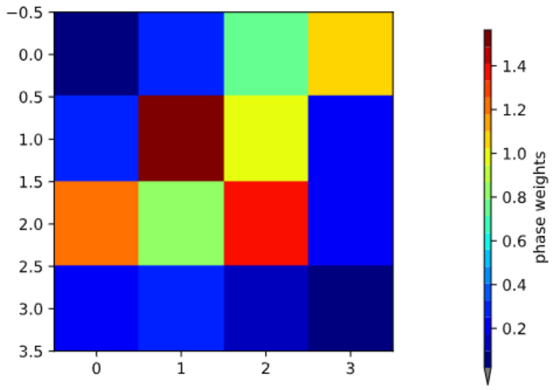

Figure 3.4: Phase of the weights of the reservoir.

It should be noted that the readout weights on their own are not necessarily an indication of node importance. Due to losses, power over the nodes varies. A better indication is to look at the output signal strength of the various nodes, the node amplitude weight times the node power that can be seen in Figure 3.5.

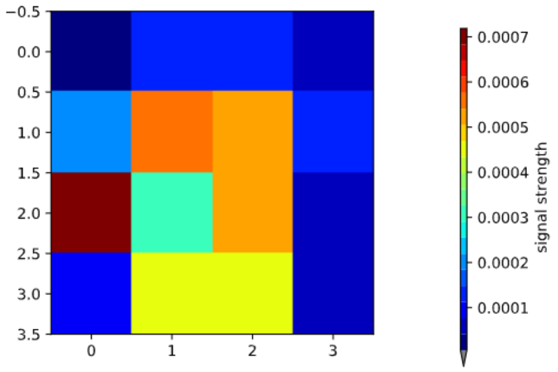

Figure 3.5: Mean output signal strength of nodes after readout.

Finally, the readout is trained using an optimizer based on gradient descent. As can be seen in Figure 3.6. the importance of the nodes has changed due to the training.

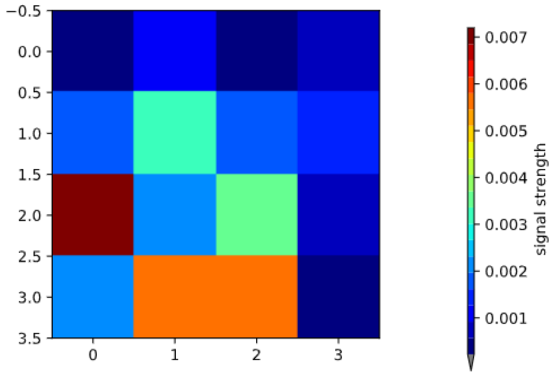

Figure 3.6: Mean output signal strength of nodes after readout after training.

The parameters used in the training are the following:

- The loss function used is the combination of a sigmoid layer with binary cross-entropy.
- The optimizer used was AdamW with decoupled weight decay. In PyTorch the regularization it is done by the optimizer using a L2 penalty.
- One batch was used and the training lasted 10000 training steps for outband jamming

and 20000 for inband jamming.

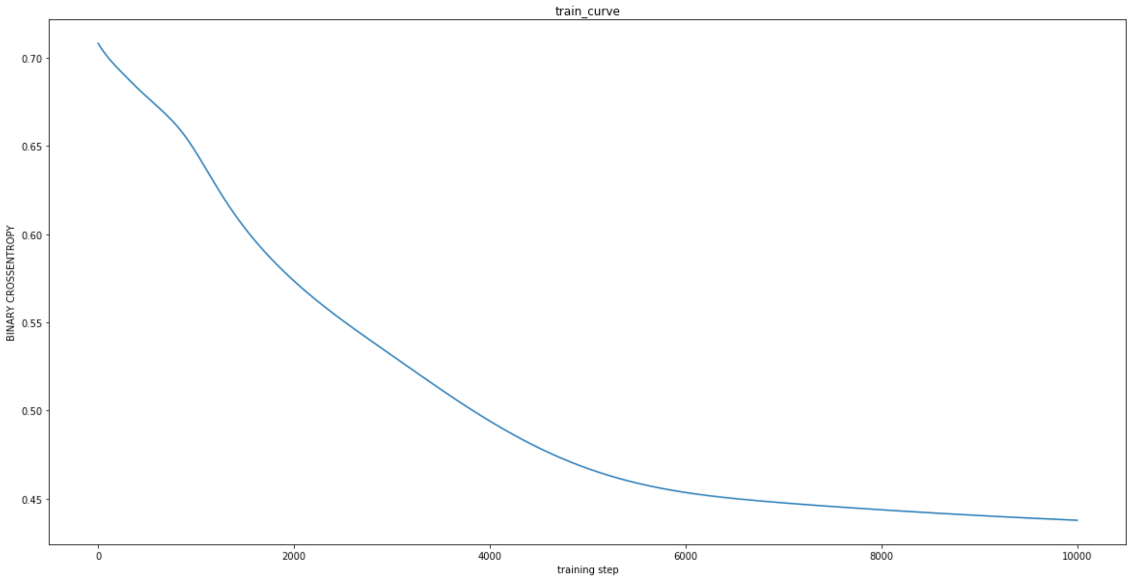

Figure 3.7: Evolution of the cross entropy loss in the readout training.

As previously mentioned a sigmoid is used in traing because cross entropy loss need to have the values of between 0 and 1. Due to that, another sigmoid function needs to be placed on testing to offer the same performance.

3.3 Results

When doing the testing of the system, it was observed that the samples that tend to be classified incorrectly were placed after a changing of the scenario. In order to solve this problem, and taking into account that it is not necessary to detect the intrusion at the rate of the input samples, the outputs were grouped in groups of 256 samples and its mean was assigned to each of them. Also, originally it was used the mean square error (MSE) as a loss function but for classification is better to use the binary cross-entropy and it showed a better performance. That improvements of the system can be seen in Figuree 3.8

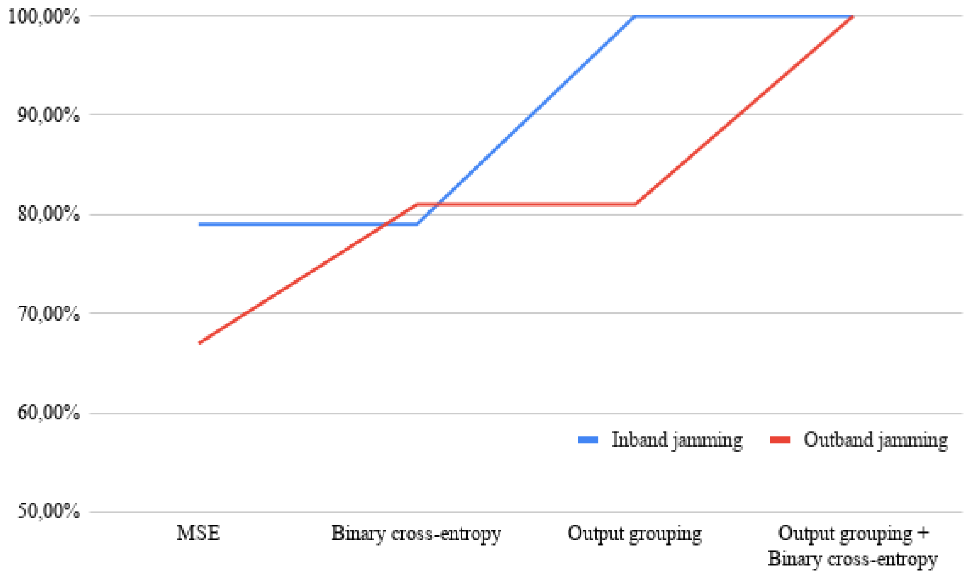

Figure 3.8: Accuracy of the system in function of the loss function and output grouping.

The photonic reservoir computing system was tested for all the pairs of scenarios (inband jamming with no jamming, outband jamming with no jamming, and inband jamming with outband jamming) using different jamming signals (modulated ones and lasers). In all of them, the system was able to classify the scenario without any error.

After the validation of the system for a fixed jamming power, different scenarios with lower jamming powers than the ones used to train the reservoir computing network were tested. The limit of correct detection was found when the inband jamming power was under 1e-06, but in that scenario, the BER was under 1e-10 (in normal conditions operates with a BER around 1e-11) so it was considered a reasonable assumption that there was no jamming.

In order to validate the results a transient analysis was also done, where a jamming signal was turned on and off as shown in figure 2.10 and also the system was able to classify it without errors.

Comparing the results with other approaches, the same accuracy is achieved as other systems using OEM metrics and supervised learning [3, 5] and a better performance when it is compared to the unsupervised learning system [4]. However, the system presented is only able to classify between two cases instead of the seven that is able to detect the system presented at [3]. Also is not able to locate the jamming signal as it was done in [5].

Chapter 4

Conclusions

4.1 Summary

The objective of this thesis was to design a system using photonic reservoir computing that was able to detect jamming attacks in an optical link with a similar performance than the current systems based in OEM equipment. The reasoning behind that was to offer a cheaper solution that could be deployed massively in the network.

The project consisted in two parts:

- Simulating the inband and outband jamming attacks in an optical link with VPI software and studying its effects by means of the BER. And from this study, selecting and obtaining the signals for feeding the reservoir computing system.
- Simulating and training a photonic reservoir computing system in order to detect different jamming attacks. It was done using the Photontorch and PyTorch libraries. Different approaches for the training and testing were taken into account until the desired performance was obtained.

From the first part, it was observed that the inband jamming had more effect on the BER due to noise was added to the signal. Also, it was observed that outband jamming reduced the power of the channel. Because of that channel power difference it was decided to use a high target signal (1) for the inband case and a low target signal (0) for the outband case.

From the simulation of the photonic reservoir computing network, it was observed that taking the mean of various outputs increased the performance and because it is not necessary to know if there is a jamming at sample rate speed it was decided to use it. Also, it was checked that instead of using the MSE as a loss function, binary cross-entropy works better for classification.

In conclusion, the results obtained showed that it is possible to use a four-port reservoir photonic integrated circuit with a photodetector as a readout for detecting and classifying jamming attacks in optical links without errors when only two scenarios are taken into account.

4.2 Perspective

This thesis was a first approach to demonstrate the viability of photonic reservoir computing networks to solve the attack detection problem so there is still lots of future research related to this topic.

In my opinion, due to the fact that all the work was done by simulation the next step should be validating the results obtained in a real scenario.

Also, the intrusion signal was only studied when it is added at the patch panel, but it can be also placed along the fibre making use of a temporal coupler. This case should also be taken into account and check if the system is able to detect them or modifications need to be done.

As previously mentioned, the system is only able to differentiate between two attacks at the same time while other approaches have shown the capacity to differentiate until seven. An improvement of the network could be done in order to increase this number.

Finally, the polarization attacks have not been taken into account, so designing a photonic reservoir computing system which can detect them will be another interesting approach.

Bibliography

[1] D. FitzGerald, "FBI investigates new attack on internet fiber optic cables," in *Wall Street J.*, Jun. 2015. [Online]. Available: https://www.wsj.com/articles/fbi-investigates-new-attack-on-internet-fiber-optic-cables-1435709881

[2] InfoGuard, "Data security in the converged enterprise network," White Paper, Dec. 2018.

[3] Carlos Natalino, Marco Schiano, Andrea Di Giglio, Lena Wosinska and Marija Furdek, "Experimental Study of Machine-Learning-Based Detection and Identification of Physical-Layer Attacks in Optical Networks" in *Journal of Lightwave Technology*, vol. 37, no. 16, pp. 4173-4182, 15 Aug.15, 2019, doi: 10.1109/JLT.2019.2923558.

[4] Marija Furdek, Carlos Natalino, Marco Schiano, and Andrea Di Giglio, "Experiment-based detection of service disruption attacks in optical networks using data analytics and unsupervised learning," Proc. SPIE 10946, Metro and Data Center Optical Networks and Short-Reach Links II, 109460D (1 February 2019)

[5] M. Bensalem, S. K. Singh, and A. Jukan, "On detecting and preventing jamming attacks with machine learning in optical networks," under submission in *IEEE GLOBECOM.* IEEE, 2019.

[6] P. R. Prucnal *et al.*, "Physical layer security in fiber-optic networks using optical signal processing," in *Communications and Photonics Conference and Exhibition*

(ACP), Asia. IEEE, 2009.

[7] X. Hu *et al.*, "Chaos-based partial transmit sequence technique for physical layer security in ofdm-pon," in *IEEE Photonics Technology Letters*, vol. 27, no. 23, pp. 2429–2432, 2015.

[8] Y. Li, N. Hua, Y. Song, S. Li, and X. Zheng, "Fast lightpath hopping enabled by time synchronization for optical network security," in *IEEE Communications Letters*, vol. 20, no. 1, pp. 101–104, 2016.

[9] S. K. Singh *et al.*, "A combined optical spectrum scrambling and defragmentation in multi-core fiber networks," in *IEEE ICC*, 2017.

[10] K. Hamedani, L. Liu, S. Hu, J. Ashdown, J. Wu and Y. Yi, "Detecting Dynamic Attacks in Smart Grids Using Reservoir Computing: A Spiking Delayed Feedback Reservoir Based Approach," in *IEEE Transactions on Emerging Topics in Computational Intelligence*, doi: 10.1109/TETCI.2019.2902845.

[11] L. Appeltant, M. C. Soriano, G. Van der Sande, J. Danckaert, S. Massar, J. Dambre, B. Schrauwen, C. R. Mirasso, and I. Fischer, "Information processing using a single dynamical node as complex system," in *Nature communications*, 2:468, 9 2011.

[12] Kristof Vandoorne, Pauline Mechet, Thomas Van Vaerenbergh, Martin Fiers, Geert Morthier, David Verstraeten, Benjamin Schrauwen, Joni Dambre, and Peter Bienstman, "Experimental demonstration of reservoir computing on a silicon photonics chip. Nature communications," 5:3541, 1 2014.

[13] L. Larger, M. C. Soriano, D. Brunner, L. Appeltant, J. M. Gutierrez, L. Pesquera, C. R. Mirasso, and I. Fischer, "Photonic information processing beyond Turing: an optoelectronic implementation of reservoir computing," in *Optics Express*, 20(3):3241, 1 2012.

[14] Quentin Vinckier, Franois Duport, Anteo Smerieri, Kristof Vandoorne, Peter Bienstman, Marc Haelterman, and Serge Massar, "High-performance photonic reservoir computer based on a coherently driven passive cavity," in *Optica*, 2(5):438–446, 2015.

[15] M. Furdek, N. Skorin-Kapov, and L. Wosinska, "Attack-aware dedicated path protection in optical networks," in *IEEE/OSA J. Lightw. Technol.*, vol. 34, no. 4, pp. 1050–1061, Feb. 2016.

[16] E. Hugues-Salas *et al.*, "Experimental demonstration of DDoS mitigation over a quantum key distribution (QKD) network using software defined networking (SDN)," in *Proc.Opt.Fiber Commun. Conf.Expo.*, 2018, Paper M2A.6.

[17] T. Uematsu, H. Hirota, T. Kawano, T. Kiyokura, and T. Manabe, "Design of a temporary optical coupler using fiber bending for traffic monitoring," in *IEEE Photon. J.*, vol. 9, no. 6, pp. 1–13, Dec. 2017.

[18] D. V. Buonomano and M. M. Merzenich, "Temporal information transformed into a spatial code by a neural network with realistic properties," in *Science*, 267:1028–1030, 1995.

[19] H. Jaeger, "The "echo state" approach to analysing and training recurrent neural networks," Technical report, German National Research Center for Information Technology, 2001.

[20] W. Maass, T. Natschläger, and H. Markram, "Real-time computing without stable states: A new framework for neural computation based on perturbations," in *Neural Computation*, 14(11):2531–2560, 2002.

[21] Appeltant L, Soriano MC, Van der Sande G *et al.*, " Information processing using a single dynamical node as complex system," in *Nat Commun*, 2011;2:468

[22] Kristof Vandoorne, Joni Dambre, David Verstraeten, Benjamin Schrauwen, and Peter Bienstman, "Parallel reservoir computing using optical amplifiers," in *IEEE transactions on neural networks*, 22(9):1469–81, 9 2011.

[23] Martin Andre Agnes Fiers, Thomas Van Vaerenbergh, Francis Wyffels, David Verstraeten, Benjamin Schrauwen, Joni Dambre, and Peter Bienstman, "Nanophotonic reservoir computing with photonic crystal cavities to generate periodic patterns," in *IEEE Transactions on Neural Networks and Learning Systems*, 25(2):344–355, 2014.

[24] Charis Mesaritakis, Alexandros Kapsalis, and Dimitris Syvridis, "All-optical reservoir computing system based on InGaAsP ring resonators for highspeed identification and optical routing in optical networks," volume 9370, page 937033, 2 2015

[25] Kristof Vandoorne, Pauline Mechet, Thomas Van Vaerenbergh, Martin Fiers, Geert Morthier, David Verstraeten, Benjamin Schrauwen, Joni Dambre, and Peter Bienstman, "Experimental demonstration of reservoir computing on a silicon photonics chip," in *Nature communications*, 5:3541, 1 2014.

[26] Floris Laporte, Joni Dambre, and Peter Bienstman, "Highly parallel simulation and optimization of photonic circuits in time and frequency domain based on the deep-learning framework PyTorch," Scientific reports 9.1 (2019): 5918.