Analysis of Eavesdropping on Optical 2-D OCDMA Networks

Mauricio Sebastião
CECS-Information Engineering
Federal University of ABC
Santo Andre, Brazil
m.sebastiao@ufabc.edu.br

Anderson Sanches
CECS-Information Engineering
Federal University of ABC
Santo Andre, Brazil
anderson.sanches@ufabc.edu.br

Rafael Nobrega
CECS-Information Engineering
Federal University of ABC
Santo Andre, Brazil
rafael.nobrega@ufabc.edu.br

Hichem Mrabet
Tunisia Polytechnic School
University of Carthage
Tunis, Tunisia
h.mrabet@seu.edu.sa

Ivan Glesk
Faculty of Engineering
University of Strathclyde
Glasgow, United Kingdom
ivan.glesk@strath.ac.uk

Shyqyri Haxha
Dept. of Electronic Engineering
Royal Holloway, Univ. of London
Egham, United Kingdom
shyqyri.haxha@rhul.ac.uk

Antonio Jurado-Navas
Dept. of Comm. Engineering
University of Malaga
Malaga, Spain
navas@ic.uma.es

Thiago Raddo
Dept. of Comm. Engineering
University of Malaga
Malaga, Spain
thiago@ic.uma.es

***Abstract*— Cybersecurity and cyber resilience are becoming crucial for many industries especially in the era of digital transformation. In this work, we report on the security analysis of the physical layer of OCDMA networks based on 2-D codes such as fast frequency-hopping (FFH). We analyze eavesdropping in OCDMA networks using FFH codes spread in both, time and frequency domains that use quadrature phase-shift keying (QPSK). The analysis is based on a newly derived bit error rate (BER) formula considering the eavesdropper's partial knowledge of the 2-D code that is needed to replicate the ONU decoder. An analytical formalism for evaluating the BER performance of the network is derived by considering 2-D codes, QPSK modulation format, avalanche photodiode shot noise, thermal noise, and multiple-access interference among optical network units (ONUs). Numerical results show that the intercepted signal is hard to decode and the information retrieved when the eavesdropper makes more than one error in guessing the used ONU code. It is shown the number of simultaneous ONUs substantially affects the eavesdropper's capability to decode the intercepted signal. The novel 2-D FFH signal encoding is robust against the eavesdropper interception. It offers a feasible solution to increase security levels in practical optical networks.**

***Keywords*— optical networks, security, eavesdropper, CDMA**

I. Introduction

New and traditional industries are connecting to communication networks on an unprecedented scale, increasing the need to ensure more security, regardless of the type of network. The advent of quantum technology will lead to changes to encryption methods providing ultimate levels of security in the physical layer. Currently, there are many emerging technologies targeting secure communication such as quantum key distribution, and quantum optical code-division multiple-access (CDMA) [1], [3]. The latter proposes a novel scheme to support higher security levels in optical networks by leveraging quantum and CDMA techniques [3]. While quantum technology has sparked a great deal of interest by the industry and research community, its maturity, practicality, and secure key distribution are still to be developed [2]. As an alternative, many technologies have been proposed so far. For example, a hybrid optical CDMA (OCDMA) free-space optics (FSO) technique to increase security in networks was proposed in [4]. Albeit the network supports privacy and security, FSO is not fully suitable for the last mile access networks due to its current limited range. A similar hybrid network was proposed in [5], but with a limited number of simultaneous users. Despite a new family of codes has been proposed to improving the security in OCDMA networks [2], the encoder and decoder complexity are high. Improvement of the physical layer security was addressed in [6], but for coherent coding techniques only. Furthermore, a meticulous security analysis was carried out in [7]. Despite the analysis addressed different types of OCDMA coding techniques, it did not cover the 2-D fast frequency hopping (FFH), which stands out owning to its demonstrated practical implementation and feasibility [8]. FFH is an elegant coding technique to be implemented in OCDMA networks. FFH was initially proposed by [9] and since then received a substantial attention [10]-[13]. OCDMA networks based on 2-D FFH have distinct advantages such as asynchronous transmission, soft blocking capabilities, and support to multiple-data rates [10]. It is well known, OCDMA can help improve the data security in optical networks against attacks by eavesdroppers intending to gain access to the transmitted data by tapping into the fiber link. However, in case of a weak network security, an eavesdropper can use modified optical receivers for signal interception, code guessing and then misuse the gained information.

In this paper, we carry out an analytical study of the physical layer security of OCDMA networks based on 2-D FFH signal techniques and advanced modulation formats. For the first time we address eavesdropping issues in 2-D OCDMA networks affected by the signal interception and optical network unit (ONU) code guessing by an eavesdropper. The 'interception receiver' procedure is characterized by the erroneous replica of the decoder design by the eavesdropper. We investigate how the intercepted signal-to-interference-plus-noise ratio (SINR)

978-3-903176-54-6 © 2023 IFIP

obtained by the eavesdropper performs under two network scenarios, i.e., changing multiple-access interference (MAI), and the MAI along with avalanche photodiode (APD) shot noise and thermal noise. To do so, we derive a new bit error rate (BER) analytical formalism. Numerical results show that the reliability of the intercepted signal by the eavesdropper is dramatically reduced if the eavesdropper makes more than 1 error in guessing the code of the targeted ONU. It is further shown that it is hard to guess correctly the unique sequence assigned to each ONU for time-spread and frequency-hopping patterns such as FFH. Also shown is the network reliability against eavesdropping increases as the number of simultaneous ONUs increases. OCDMA networks based on 2-D FFH are therefore regarded as a promising way for increasing security needs in optical networks while offering feasible and practical implementation.

II. Interception Receiver Structure

This subsection addresses the 2-D FFH encoding and decoding devices employed at the optical line terminal (OLT) and optical network units (ONUs), respectively, which compose the FFH-OCDMA network and is shown in Fig. 1. The understanding of such device structures gives important clues on how successful the eavesdropping process from the interception receiver will be.

Nonetheless, before proceeding with the 2-D FFH encoder/decoder details itself, it is interesting to analyze the signal evolutions from generation until reception. The traffic on the 2-D OCDMA network in the downstream direction comes from the OLT to the ONUs (including the interception receiver of the eavesdropper) through broadcast. At the OLT side, the data information bits from the metro or a long-haul network are quadrature phase shift keying (QPSK) modulated. Sequentially, the optical pulses are simultaneously encoded in sequential time slots and disjoint wavelength subbands by FFH encoders. The OLT holds encoders matched to decoders used by the ONUs. The tuning set of each pair of encoder-decoders will determine the code sequence used. Therefore, a unique code sequence, in which each chip (encoded pulse) signaling interval occupies one wavelength slot, is assigned to each ONU. After attributing code sequences to ONUs, the next step is to access the fiber channel and delivery the OLT data information signals superposed to the ONUs. Here, it is considered that all optical fiber impairments are appropriately compensated. Despite the ideal channel characteristics, the simple superposition of the data information signals produces MAI, which is delivered to each ONU. As well known, MAI severely affects the data recovery at the ONU receiver side. However, when the wavelength translation introduced at the transmitter is removed by the FFH decoder at the desired ONU only the additional energy generated by the MAI within the chip period at which the autocorrelation peak is formed has an impact on the overall network performance. Then, the decoded information along with MAI is sent to the demodulation unit present at each ONU (that is not shown in Fig. 1 for the sake of simplicity).

The 2-D OCDMA network is based on multiple Bragg gratings (MBGs) encoders/decoders and was originally proposed by Fathallah [9]. In fact, the encoding process is based on a series of MBGs to generate FFH patterns in which jumps occur at wavelengths that change for every temporal chip of the code sequence. These gratings spectrally and temporally slice an incoming broadband pulse into several components, generating then optical frequency patterns. This attractive encoding scheme [14] stands out not only due to its good performance [9], [10] but also for its practical feasibility based on optical intensity manipulation of the incoherent signal and detection at the receiver side via intensity modulation / direct detection (IM/DD) approaches. In addition to its asynchronous transmission nature, the passive all-optical encoding scheme based on MBGs implies potential low-cost and robust implementation of FFH-OCDMA networks [9].

An inherent feature of the 2-D FFH scheme is that the frequency changes at a significantly higher rate than the information rate, which means that each pulse in a code sequence is transmitted at an exclusive wavelength. To better illustrate this concept, a possible network architecture based on the FFH-CDMA scheme employing MBGs is illustrated in Fig. 2. Initially, a broadband short pulse modulated with QPSK, which represents the data information bit, is generated. Then, this broadband pulse, shown in Fig. 2a, is sent to the MBGs-based encoder when the value of the data information bits is “1”, otherwise no power is sent for the transmission of data bit “0”. Subsequently, the MBGs generate independent frequency pulses and place each of them in an appropriate time-slot, depicted in Fig. 2b and Fig. 2c, respectively, following a scheme previously established by the FFH-based code generator. The output signal established by the wavelength reflections of the MBGs forms the code sequence and is ready to be transmitted over the

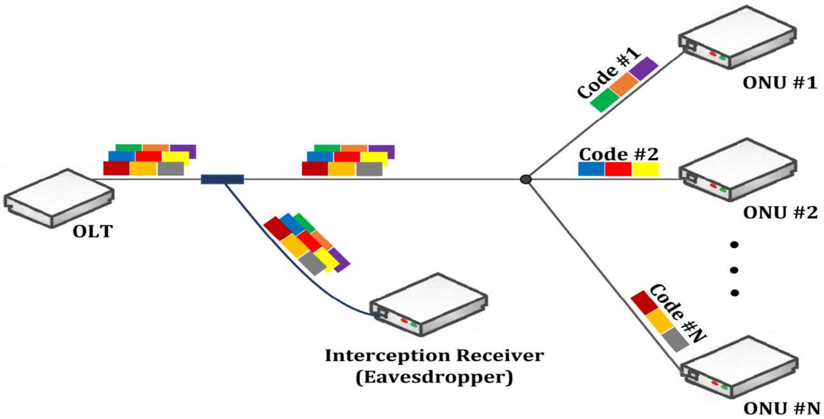

Fig. 1. Block diagram of the FFH-OCDMA system considering an interception receiver added by the eavesdropper.

network. Furthermore, the MBGs produce the frequency spectrum slicing while the temporal position of the MBGs produces the respective time delays. Indeed, the time-frequency pulses are determined by the order in which they are tuned to the respective MBGs following the concept of first-in, first-reflected [9].

It is worth pointing out that the chip duration and the number of gratings in the encoder establishes the nominal data information bit rate of the network, i.e., all reflected pulses of a data bit should leave the encoder before the next bit's pulses enter [10]. Moreover, the impulse response of each Bragg grating is defined as the inverse Fourier transform of the grating complex reflectivity, where the incident pulses associated with the transmitted data information bit are normally much narrower than the response duration of the grating. This encoding process is based on a convolution of an incoherent short pulse modulated by the data source with the response of each Bragg grating. At the decoder side, Fig. 2d, the wavelengths are placed in the reverse order of those in the encoder to accomplish the decoding function. Then a matched filter based-decoder removes the translation between the wavelengths and realigns all pulses from the received signal into a single pulse as illustrated in Fig. 2e.

Assuming the pulses are positioned correctly, they form a well-defined pattern given by the autocorrelation property (similarity level between the transmitted and received desired data information signal). If they are not, the pulses form an interfering background signal defined by the cross-correlation property representing the MAI as shown in Fig. 2e. Then, the decoded information is sent to the QPSK demodulation unit (not illustrated here). Afterward, the bit decision in each QPSK channel is made based on a comparison between the integrator output level and a threshold level previously established.

III. FFH Network With Interception Receiver

In this section, it is presented a detailed description of the 2-D OCDMA network under an eavesdropper interception receiver as shown in Fig. 1. The eavesdropper can tap the OLT signals in several locations of the FFH-OCDMA network. Nonetheless, it is considered here that the eavesdropper monitors the aggregated downstream traffic from OLT to the ONUs. The goal is to analyse how different MAI levels will impact the reliability of the intercepted signal during the eavesdropping. At the OLT side, the data information signal to be send to each ONU are QPSK modulated and simultaneously encoded in sequential time slots with disjoint wavelength sub-bands by the FFH encoders.

Then, a unique code sequence characterized by each chip signaling interval occupying one wavelength slot is assign to each data information signal. In this manner, each information bit from the m data information signals is encoded into a code sequence as

$$c_m(t) = \sum_{l=1}^{k} p\left(\frac{t - lT_c}{T_{c0}}\right) e^{j\omega_{m,l}t}, \tag{1}$$

where L is the code length, $p(t)$ is the chip signaling waveform, T_c is the chip period, $T_{c0} = T_c/f_c$ is the half-width of the pulse, f_c is the pulse compression factor, and $\omega_{m,l}$ is the l-th chip's wavelength related to m-th ONU. In addition, the optical field amplitude $c_m(t)$ is normalized so that $|c_m(t)|^2$ gives the instantaneous power [10].

In the next step, the encoded data information signals are injected into the optical fiber. It is important to point out that the simple superposition of data information signals produce MAI and manifests itself as background noise to each OCDMA decoder present in the ONUs. At each ONU side, the wavelength translation introduced at the OLT transmitters is removed by the specific ONU's decoders. Then, the composed data information

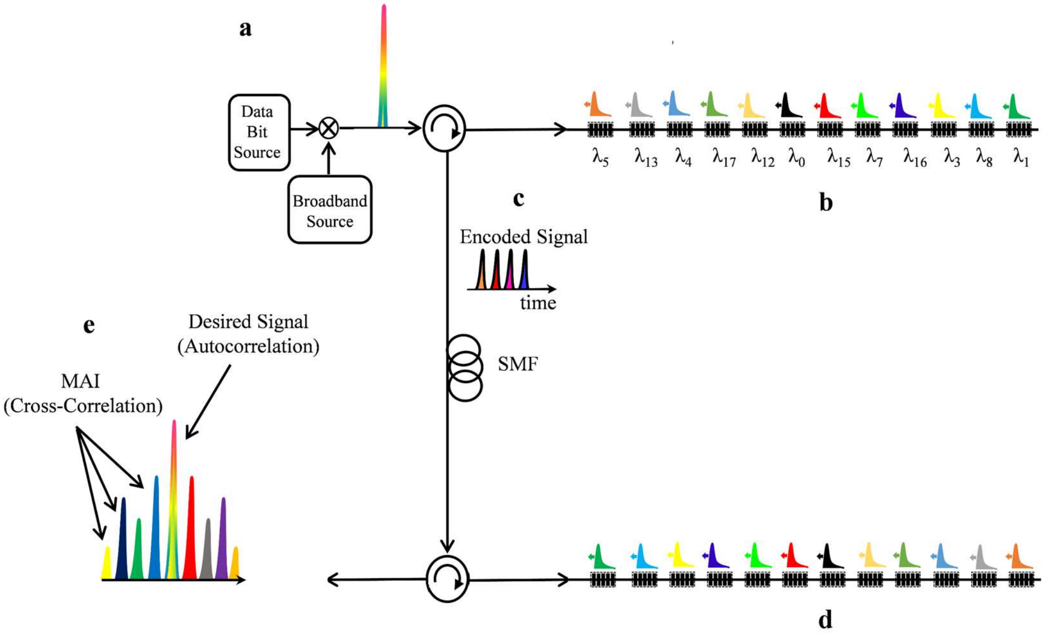
a
Data Bit Source
Broadband Source
λ_5 λ_{13} λ_4 λ_{17} λ_{12} λ_0 λ_{15} λ_7 λ_{16} λ_3 λ_8 λ_1
b
c
Encoded Signal
time
SMF
e
Desired Signal (Autocorrelation)
MAI (Cross-Correlation)
d

Fig. 2. Block diagram of the FFH-OCDMA system considering an interception receiver added by the eavesdropper.

signal is applied to a matched filter with impulse response $h_n(t)$ given by the inverse Fourier transform of the reflectivity spectrum of the MBGs which are part of the decoders. In all simulations, the encoders/ decoders are modeled using multiple apodized fiber Bragg gratings (i.e., *sinc* reflectivity profile) via the transfer matrix method [10]. Hence, the desired ONU decoder n outputs an autocorrelation optical signal given by

$$E_{ac\_n}(t) = \int_{-\infty}^{\infty} c_n(\tau) h_n(t-\tau) d\tau, \tag{2}$$

where $-L+1 \leq \tau \leq L-1$ is the chip delay. It is important to mention that the residual energy generated by the MAI within the autocorrelation peak degrades the overall network performance.

A similar expression can be obtained for the cross-correlation signal between the n and k data information signals, which reads as

$$E_{cc\_n,k}(t) = \int_{-\infty}^{\infty} c_k(\tau) h_n(t-\tau) d\tau. \tag{3}$$

Assuming that there are K interfering data information signals active in the network, the received optical field at the decoder output of the desired ONU n is

$$E_n(t) = E_{ac\_n}(t) + \sum_{k=1(k\neq n)}^{K} E_{cc\_n,k}(t-\tau_k), \tag{4}$$

where τ_k is the relative network transit delay of the k-th interferer.

The mathematical formalism related to the BER needs the electrical current that outputs the photodetector expressed in terms of the auto- and cross-correlation data information signals for the desired ONU. Considering the recovery of the desired data information signal by means of direct detection, the optical field at the receiver goes through the photodetector to produce the following average electrical power as a decision variable

$$\begin{aligned} i_n &= \Re\left\{\frac{\mathcal{R}}{T_{ac}}\int_{T_{ac}} [P_n(t) + P_{N0}]\, dt\right\} \\ &= \Re\left\{\frac{\mathcal{R}}{T_{ac}}\int_{T_{ac}} [E_n(t) \times E_n^*(t) + P_{N0}]\, dt\right\} \\ &= \Re\left\{\frac{\mathcal{R}}{T_{ac}}\int_{T_{ac}} \Big[P_{ac\_n}(t) \right. \\ &\qquad \left. + \sum_{k=1(k\neq n)}^{K} P_{cc\_n,k}(t-\tau_k) + P_{N0}\Big] dt\right\}, \end{aligned} \tag{5}$$

where $\Re$ represents the real part, T_{ac} is the autocorrelation window decision, $*$ denotes the complex conjugate, $\mathcal{R}$ is the responsivity of the photodetector, $P_{ac\_n}(t)$ and $P_{cc\_n,k}(t)$ are the instantaneous powers of the auto- and cross-correlation signals, respectively, and P_{N0} is the instantaneous power of the photodetector noises.

It is worth mentioning that the terms resulting from the multiplication between the auto- and cross-correlation data information signals in (5) are ignored by raising oscillation frequencies whose magnitudes fall out of the receiver bandwidth and, consequently, are filtered by the device.

Further, the terms that compose the decision variable can be expressed individually by the auto- and cross-correlation data information signals components as

$$\mu_{ac\_n} = \Re\left[\frac{\mathcal{R}}{T_{ac}}\int_{T_{ac}} P_{ac\_n}(t) dt\right] \tag{6}$$

and

$$\mu_{cc\_n} = \Re\left[\frac{\mathcal{R}}{T_{ac}}\int_{T_{ac}} \sum_{k=1(k\neq n)}^{K} P_{cc\_n,k}(t-\tau_k)\, dt\right]. \tag{7}$$

Next, since it is not known which coded symbols will be active at any given time, a mean calculation considering all possible coded symbols and random-access delay of every data information signal ($\overline{\mu_{MAI}}$) is required [9]. In this case, the variance related to the interfering signals can be obtained by

$$\sigma^2{}_{MAI_{j,k}} = \left(\mu_{MAI\_j,k} - \overline{\mu_{MAI}}\right)^2 \tag{8}$$

Similarly, the mean interference variance of all data information signals is given by $\sigma_{MAI}^2 = \overline{\sigma^2{}_{MAI\_j,k}}$.

Next, the values of the variances associated with the photodetector and receiver noises are required. Here, it is considered an APD that adds shot noise generated due to the randomness of its gain mechanism and the thermal noise resulting thermal motion of charged carriers due to the fluctuating voltages in the physical resistances in the receiver. Then, the instantaneous power of the photodetector noises is given by

$$P_{N0} = P_{shot} + P_{thermal}. \tag{9}$$

Once both the shot and thermal noises can model as a Gaussian process, the variance of the receiver noise can be expressed as

$$\sigma_{NO}^2 = \sigma_{shot}^2 + \sigma_{th}^2 = \sigma_{shot\_0}^2 + \sigma_{shot\_1}^2 + \sigma_{th}^2, \tag{10}$$

where $\sigma_{shot\_0}^2$ and $\sigma_{shot\_1}^2$ are the shot noise variances for the bit "0" and "1" transmissions, respectively, and σ_{th}^2 is the thermal noise variance.

As it is well known, the shot noise variances associated with the "0" and "1" bit are directly related to the average mean of the desired data information and interfering signals, respectively. In this case, such shot noise variances for the "0" and "1" bit transmissions can be written as

$$\sigma_{shot\_0}^2 = 2qG^2F_e\left(\mu_{cc\_n} + I_s\right) \tag{11}$$

and

$$\sigma_{shot\_1}^2 = 2qG^2F_e\left(\mu_{ac\_n} + I_s\right), \tag{12}$$

where q is the electron charge, G is the APD gain, $F_e = k_{ef}G + (1-k_{ef})[2-(1/G)]$ is the excess noise factor, k_{ef} is the ionization rate and I_S is the APD surface leakage current. The variance of the thermal noise, by its turn, can be expressed by

$$\sigma_{th}^2 = \frac{4k_b T_r B_{ca}}{R_L}, \tag{13}$$

where k_b is the Boltzmann constant, $T_r$is the noise temperature, B_{ca} is the receiver bandwidth and R_L is the load resistance.

Then, assuming that all N data information signals are statistically independent, the SINR at the receiver output can be obtained by [10]

$$SINR = \frac{\mu_{ac\_n}^2}{(N-1)\sigma_{MAI}^2 + \sigma_{NO}^2}. \tag{14}$$

Finally, the minimum BER for the FFH-OCDMA network based on QPSK modulation is given by

$$BER_{QPSK} \approx Q\left(\sqrt{SINR}\right), \tag{15}$$

An analogous behaviour happens at the FFH-OCDMA decoder of the interception receiver used by the eavesdropper. In this case, the eavesdropper intercepts the superposition of the FFH-OCDMA signals provided from the OLT through tapping the fiber and connecting to the interception receiver. The key difference between the desired ONU and eavesdropper is that the latter does not know exactly the ONUs code sequences (even though the eavesdropper knows the modulation format and coding scheme used) and, therefore, faces difficulty to reproduce the matched filter which is part of the decoder for the desired ONU. In situations where the eavesdropper is not fortunate enough to reproduce the matched filter for the desired ONU, it is assumed that the FFH decoder designed by the eavesdropper (located in the interception receiver) holds a certain number of MBGs tuned to different frequencies from the desired ONU. Such differences in the MBGs are referred here as error filtering.

IV. Numerical Simulation and Results

Now, the analysis of potential eavesdropping scenarios will be carried out. To start, it is assumed the eavesdropper knows a great deal about the network resources i.e., the data information rate, the modulation format adopted, and both the codes' generation algorithm and parameters required to project the OCDMA decoders. Nonetheless, this knowledge frequently does not offer the specific code signature employed by each ONU. In most scenarios considered, it is also assumed the eavesdropper partially knows the time spreads and frequency-hopping patterns necessary to replicate a desired ONU decoder. It is also considered chip synchronization, a situation that does not take advantage of the OCDMA concept where completely asynchronous traffic, either of bits or chips, is possible. Nonetheless, this assumption greatly simplifies the formalism, and the obtained expression for the BER reflects the worse possible scenario [10]. In addition, it is assumed the OLT transmits at 10 Gb/s, which is compatible with the next-generation passive optical network 2 (NG-PON2) standardization. Consequently, the code-intercepting receiver can recompose the desired ONU information with several degrees of reliability. The reliability of the information theft can be 'measured' in terms of the code interception performance through a BER.

Now, a suboptimum interception receiver is characterized by the erroneous project (by comparing it to the desired ONU receiver) of one or several wavelengths of the filtering MBGs within the OCDMA decoder. In addition, the impact of the MAI and receiver noises are also accounted for in the interception receiver performance. It becomes necessary to define the two network scenarios to be analyzed. The first and second network scenarios refer to the 2-D OCDMA network limited by MAI and under simultaneous interaction of MAI as well as receiver noises (thermal and shot noises), respectively. First, the BER is investigated as a function of the number of simultaneous ONUs under the MAI. It gives important insights on how the network reliability is impacted due to the interception receiver added to the network by the eavesdropper. We assume the eavesdropper has substantial knowledge of the parameters (but not of the ONUs code sequences), which would be for the eavesdropper the worst-case security scenario to analyze. The results are shown in Fig. 3. Here, the estimated BER obtained after the intercept receiver operating as a matched filter shadowing the 'targeted ONU' is considered as the 'best-case scenario reference' for this eavesdropping receiver. It can be seen (hollow circles), the eavesdropper is able to capture the entire signal of the targeted ONU (BER $< 10^{-12}$) even for the case when 64 simultaneous ONUs are present on the network. It should be noted that any mistake in the filtering process would significantly degrade the intercept receiver reliability.

The hollow squares curve shows the intercept receiver performance when considering its erroneous filtering. In this case, it is impossible to capture the targeted ONU data information signal without significant BER degradation when all 64 simultaneous ONUs transmit data simultaneously. On the other hand, the full interception of the targeted ONU data information signal can occur when a maximum of 45 ONUs coexist simultaneously in the network. This considerable degradation of the BER is attributed to the decrease in the SINR due to the autocorrelation peak reduction at the intercept receiver. The intercept receiver reliability is reduced drastically if the eavesdropper commits more errors in the decoder device design. Considering 3 (hollow diamonds) and 5 (hollow hexagram) errors in the filtering process, the maximum number of simultaneous ONUs present in the network that allow the intercept receiver to recover entirely the desired ONU data information signal is restricted to 37 and 22, respectively. Furthermore, it can be observed that the BER is unacceptably high for 7 errors (hollow pentagram) and 9 errors (cross) even though the number of simultaneous ONUs is just 13 (minimum limit of ONUs in which the MAI exist).

Next, it is investigated how the intercept receiver performs under MAI and the influence of the receiver noises. The APD provides a gain equal to 100 and has an intrinsic ionization rate of 0.02. The APD surface leakage current is in the range of 10 nA. In addition, the receiver presents a noise temperature of 1100 °K and utilizes a receiver load resistor with a electrical resistance of 1030 Ω. The results obtained are shown in Fig. 4. Again, the matched filter receiver for the target ONU reproduced by the eavesdropper (solid circles) will be utilized as a reference to the intercept receiver performance. Notice that the maximum number of simultaneous ONUs that can coexist on the network is limited to about 42 in order for the eavesdropper to

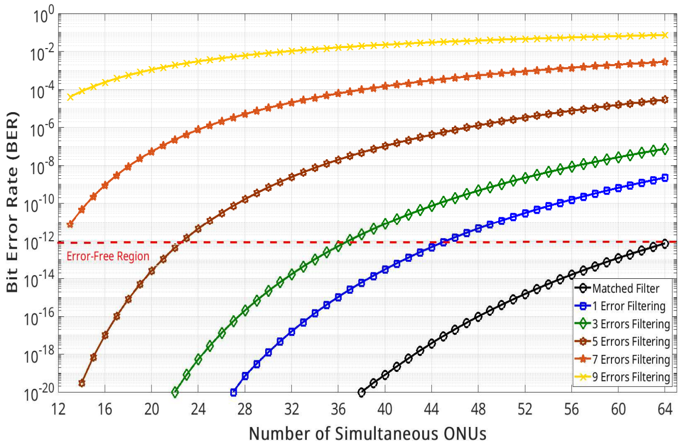

Fig. 3. BER for the MAI scenario as a function of the number of ONUs for different numbers of erroneous wavelengths.

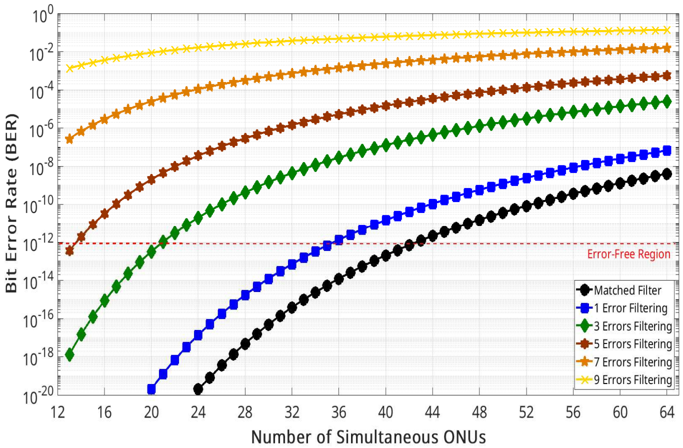

Fig. 4. BER for MAI and photodetector noise as a function of the number of ONUs for different numbers of erroneous wavelengths.

extract the targeted ONU signal. The requirement of low number of simultaneous ONUs in the network for error-free interception becomes necessary due to poor SINR at the intercept receiver. As expected, this further deteriorates as the number of errors in the intercept receiver design increases.

Let us now investigate the intercept receiver performance when the device performs 1 error filtering (solid squares). Observe that the eavesdropper can access the targeted ONU data information signal when 35 simultaneous ONUs coexist on the network. The number is reduced to 21 (solid diamonds) and 13 (solid hexagram) simultaneous ONUs if the eavesdropper makes 3 and 5 filtering errors when designing the intercept receiver, respectively. Such a drastic reduction in the maximum simultaneous ONU limit to decoding the desired ONU information in an error-free manner is due to SINR reduction at the intercept receiver decoder. Lastly, for both 7 (solid pentagram) and 9 (cross) filtering errors, it is not possible to decode the desired ONU data information signal in an error-free fashion.

V. Conclusions

In this paper, we carried out a security analysis of 2-D OCDMA networks for two distinct scenarios under the presence of an eavesdropper. The ONUs of the OCDMA network are assigned unique 2-D codes such as FFH while using QPSK. The analysis considers a different number of errors encountered by an eavesdropper when intercepting the targeted ONU transmission. An analytical formalism for evaluating the BER performance of the network is derived. The formalism accounts for 2-D codes, advanced modulation formats, APD shot noise, thermal noise, and MAI among data information signals. Numerical results shown that the reliability of the intercepted signal is increased when the eavesdropper commits more than one error in targeting the desired ONU code. It has been shown that the number of simultaneous ONUs in the network plays a key role on the eavesdropper capability to decode the targeted ONU transmission. The larger the number of ONUs, the harder is to correctly guess the targeted ONU code. Thus, the 2-D FFH technique has been demonstrated to be a robust and efficient scheme for providing a practical implementation of OCDMA against signal interception, becoming an interesting technique to increasing the security of optical networks at the physical layer.

References

[1] H. Y. Ahmed., M. Zeghid, T. Sharma, A. N. Khan, W. A. Imtiaz, and S. A. Abd El-Mottaleb., “An efficient algorithm to provide triple play services in passive optical network (PON)-OCDMA network,” Optical and Quantum Electronics, vol 54, 2022.

[2] Y. Tana, et al., “Design and performance analysis of a novel secure communication system based on optical code division multiple access technology,” Optical Fiber Technology, vol. 58, 102254, 2020.

[3] M. Rezai and J. A. Salehi, “Quantum CDMA communication systems,” Tran. on Infor. Theory, vol. 67, no. 8, pp. 5526-5547, 2021.

[4] J. Ji, X. Chen, L. Sun, "Performance analysis and experimental investigation of physical-layer security in OCDMA-based hybrid FSO/fiber wiretap channel," Photonics Journal, vol. 11, no. 3, pp. 1-20, 2019.

[5] J. Ji, Z. Zheng, F. Peng, J. Zhang, B. Wu, M. Xu, K. Wang, “10Gb/s two-user spatial diversity FSO-CDMA wiretap channel based on reconfigurable optical encoder/decoders,” Access, vol. 8, pp. 38941-38949, 2020.

[6] J. Ji, G. Zhang, and K. Wang, et al., “Improvement of physical-layer security and reliability in coherent time-spreading OCDMA wiretap channel,” Opt. Quant. Electron, vol. 50, 215, 2018.

[7] Thomas H. Shake, “Security performance of optical CDMA against eavesdropping,” J. Lightwave Technol. vol. 23, 2005.

[8] H. Ben Jaafar, S. LaRochelle, P. -. Cortes, and H. Fathallah, “1.25 Gbit/s transmission of optical FFH-OCDMA signals over 80 km with 16 users,” in OFC, 2001.

[9] H. Fathallah, L. A. Rusch, and S. LaRochelle, “Passive optical fast frequency-hop CDMA communications system,” J. Lightwave Technol., vol. 17, 1999.

[10] A. L. Sanches, et al., “Performance analysis of single and multirate FFH-OCDMA networks based on PSK modulation formats,” J. Opt. Commun. Netw., vol. 7, pp. 1084-1097, 2015.

[11] T. R. Raddo, A. L. Sanches, J. V. dos Reis, Jr and B. -H. V. Borges, “A new approach for evaluating the BER of a multirate, multiclass FFH-CDMA system,” Comm. Letters, vol. 16, pp. 259-261, 2012.

[12] A. L. Sanches, T. R. Raddo, J. V. dos Reis and B. V. Borges, “Highly efficient FFH-OCDMA packet network with coherent advanced modulation formats,” in IEEE ICTON, 2014.

[13] T. R. Raddo, A. L. Sanches, I. T. Monroy and B. -H. V. Borges, “Multirate IP traffic transmission in flexible access networks based on optical FFH-CDMA,” in ICC 2016.

[14] D. S. Chauhan, G. Kaur, and D. Kumar, “Development of multi diagonal based OCDMA system for free space optical communication system,” Optical and Quantum Electronics, vol 54, 2022.