*Maejo Int. J. Sci. Technol.* **2012**, *6*(02), 238-248

***Maejo International Journal of Science and Technology***

**ISSN 1905-7873**
Available online at www.mijst.mju.ac.th

*Full Paper*

# Simulation analysis of security performance of DPSK-OCDMA network via virtual user scheme

**Vishav Jyoti** * **and Rajinder Singh Kaler**

Department of Electronics and Communication Engineering, Thapar University, Patiala-147004, Punjab, India

* Corresponding author, e-mail: vishavjyoti@gmail.com

*Received: 27 July 2011 / Accepted: 26 June 2012 / Published: 6 July 2012*

**Abstract**: A novel technique to enhance the security of an optical code division multiple access (OCDMA) system against eavesdropping is proposed. It has been observed that when a single user is active in the network, an eavesdropper can easily sift the data being transmitted without decoding. To increase the security, a virtual user scheme is proposed and simulated on a differential phase shift keying (DPSK) OCDMA system. By using the virtual user scheme, the security of the DPSK-OCDMA system can be effectively improved and the multiple access interference, which is generally considered to be a limitation of the OCDMA system, is used to increase the confidentiality of the system.

**Keywords:** DPSK, eavesdropping, OCDMA

## INTRODUCTION

The potential for enhanced data security is one of several advantages of the optical code division multiple access (OCDMA) [1]. If multiple codes operate simultaneously, it is almost impossible for an eavesdropper to get meaningful information because of multiple access interference (MAI) caused by all transmitting users. However, a single transmitting user is vulnerable to the eavesdropper's attack. At first, the notion that an OCDMA encoded signal is similar to a noise waveform makes it difficult for an eavesdropper to read the transmitting data. Nevertheless, the single-user on-off keying OCDMA (OOK-OCDMA) system can be easily attacked by a simple energy detector without any knowledge of the code [2, 3].

Therefore, the OCDMA system with a modulation format based on code shift keying (CSK) was introduced where data bits '0' and '1' were encoded by two different codes to improve its security against simple energy detection [2, 4]. However, the CSK-OCDMA system could be

*Maejo Int. J. Sci. Technol.* **2012**, *6*(02), 238-248

attacked by a differential phase-shift keying (DPSK) demodulator followed by a balanced photodetector [5]. To provide security against a standard power detector, a DPSK-OCDMA system was implemented [6]. However, eavesdroppers can still detect the data from the encoded signals by using a DPSK demodulator [5]. In this study, a DPSK-OCDMA network is considered to ensure data security against differential eavesdropping.

An unauthorised access is basically a threat to the network confidentiality when an individual user is isolated during transmission. An eavesdropper in an OCDMA network can isolate an individual user's signal from various locations within the network [7]. In a network where only a single user is transmitting, an eavesdropper can isolate the individual user's signal at a location within the network before multiplexing or coupling the multiple users' signals. An eavesdropper can also isolate an individual user's signal when a single user is active in the network while all other users are idle. In this paper, a novel technique is proposed and simulated to make the OCDMA system less vulnerable to eavesdropping by creating a virtual user environment in the DPSK-OCDMA network.

## PROPOSED MODEL

In the OCDMA system, the data from all users is multiplexed before transmission onto an optical fibre. In the case when a single user is active in the network while all others are not transmitting, an eavesdropper can easily sift the data by tapping into an optical fibre. This problem can be solved by a virtual user scheme as shown in Figure 1. In this scheme, a virtual user is created that is always transmitting in parallel with the authorised users. Therefore, at the time when only a single user is transmitting and all other users are idle, the virtual user is the source of multiple access interference that makes the eavesdropper's task difficult. Pseudo random noise is given as the data input to the virtual user and the data are encoded using a unique optical code from the code set used. Further, this encoded stream is multiplexed with the other user's data stream before transmitting the signal onto the optical fibre. This virtual user will serve as an interferer because it appears as an authorised user to an eavesdropper, thus hindering eavesdropping. Therefore, an eavesdropper can never isolate an individual user's signal because there is always an active virtual user in the network that serves as interferer, and deciphering the data bits when multiple users are present is more difficult [8]. In an OCDMA network, MAI is generally considered as a limitation but in a virtual user OCDMA system, it can be advantageously used to increase the confidentiality of the system.

This scheme was already analysed with OOK-OCDMA [9]. It was seen that irrespective of the encoding scheme, OCDMA system with OOK modulation format is not secure. A prototype virtual user scheme was proposed to enhance the security of OOK-OCDMA against simple energy detector when a single user is active in the network [9]. This proposed virtual user scheme increased security but imposed a bandwidth constraint on the system because a virtual user was incorporated with each user.

*Maejo Int. J. Sci. Technol.* **2012**, *6*(02), 238-248

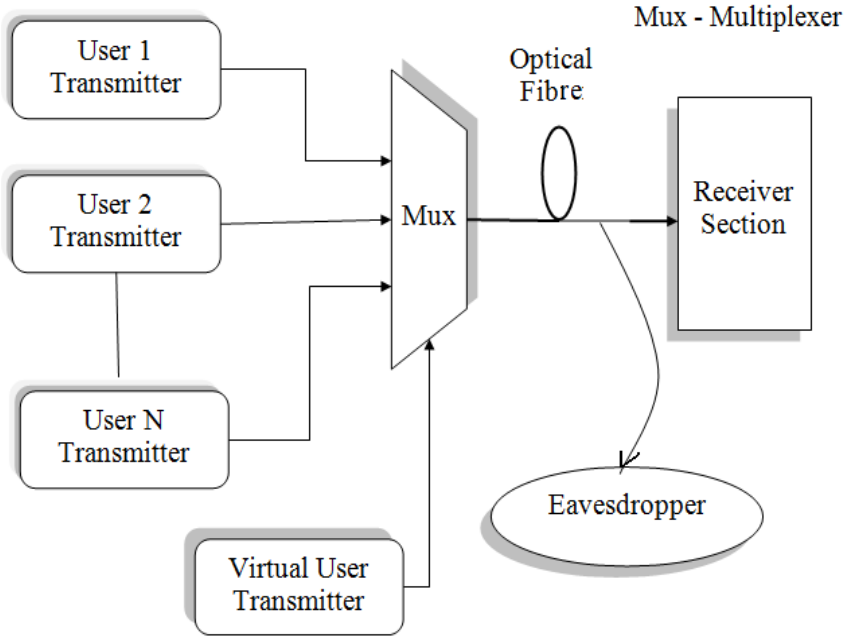



**Figure 1.** Proposed virtual user environment model for OCDMA network

In this article, the virtual user scheme is analysed with DPSK-OCDMA, which is vulnerable to a differential eavesdropper. Here, we propose a bandwidth-efficient virtual user scheme where all the authorised users have a common virtual user. The proposed scheme helps to make the system inherently secure against eavesdropping without affecting the system performance or imposing any additional bandwidth penalty.

The bit error rate (BER) for DPSK-OCDMA can be evaluated for both the single user and virtual user cases as given below [10]. For single-user OCDMA network, BER becomes:

$$BER_{single} = \frac{1}{4}\left(1 + erf\left(\frac{-A_g w}{\sqrt{2(\sigma_{th}^2)}}\right) + erfc\left(\frac{A_g w}{\sqrt{2(\sigma_{th}^2)}}\right)\right)$$

where $w$ is the code weight, $A_g$ is the peak power of a single chip and $\sigma_{th}^2$ is the thermal noise. The erf(x) is the error function defined as:

$$\text{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}\,dt \qquad -\infty < x < \infty$$

and erfc(x) is the complementary error function:

$$\text{erfc}(x) = 1 - \text{erf}(x)$$

For virtual user with single user, BER becomes:

$$BER_{virtual} = \frac{1}{4}\left(1 + erf\left(\frac{-A_g w - A_g \frac{w^2}{2L}}{\sqrt{2\sigma_1^2}}\right) + erfc\left(\frac{A_g w + A_g \frac{w^2}{2L}}{\sqrt{2\sigma_1^2}}\right)\right)$$

*Maejo Int. J. Sci. Technol.* **2012**, *6*(02), 238-248

where

$$\sigma_1^2 = A_g^2 \frac{w^2}{2L}\left(1 - \frac{w^2}{2L}\right) + \sigma_{th}^2$$

and $L$ is the code length. Thus,

$$BER_{virtual} = \frac{1}{4}\left(1 + erf\left(\frac{-A_g w - A_g \frac{w^2}{2L}}{\sqrt{2\left(A_g^2 \frac{w^2}{2L}\left(1 - \frac{w^2}{2L}\right) + \sigma_{th}^2\right)}}\right) + erfc\left(\frac{A_g w + A_g \frac{w^2}{2L}}{\sqrt{2\left(A_g^2 \frac{w^2}{2L}\left(1 - \frac{w^2}{2L}\right) + \sigma_{th}^2\right)}}\right)\right)$$

This scheme has certain advantages over the code switching scheme since, for the same number of users, twice as many codes are needed in the code switching scheme and the increase in the number of codes adds complexity to the network, which may also increase the cost of network management [7]. On the other hand, unlike the case for the code switching scheme, the introduction of one virtual user would not affect the system performance because the number of authorised users is not halved with respect to a standard OCDMA transmission.

To illustrate this, the information capacity (C) of an OCDMA network may be given as [11]: $C = K.\ [\ 1 - \log_2 (1+e^{-SNR})\ ]$, where K = number of users and SNR is the signal to noise ratio which depends on MAI noise. For the code switching scheme, the number of users is halved because two codes are used in encoding for each user. Therefore, the system capacity is halved. For the proposed scheme, however, only one user is added to form a virtual user environment and this does not affect the system performance.

**SIMULATION SET-UP**

The security enhanced DPSK-OCDMA system implementing a virtual user environment is shown in Figure 2. An OCDMA system based on spectral coding with a DPSK modulation format for a single transmitting user was simulated using the OptSim software. The simulation parameters considered for DPSK-OCDMA are given in Table 1. Here, the case when a single user is transmitting while all other are idle and the virtual user is active in the network was considered.

First, an OCDMA system with DPSK signalling and balanced detection was simulated. The DPSK system with balanced detection is an attractive modulation format for long-haul transmission as compared to the OOK modulation [12,13]. The DPSK format is a subset of the phase-shift keying (PSK) format in which the information carrying part for the DPSK encoded data is the phase difference applied to the carrier corresponding to two consecutive data bits. If the previous bit is 0, no phase shift is applied for encoding the current bit. If the previous bit is 1, the phase of the carrier for the current bit is applied with a phase shift of 180 degrees [14].

Next, a virtual user was created which was always transmitting in parallel to the authorised user. The outputs of the authorised and virtual users were combined by the optical multiplexer before transmission. A conventional single mode optical fibre having a length of 25 km was used for transmission, after which the DPSK modulated signal entered the receiver section of the topology.

*Maejo Int. J. Sci. Technol.* **2012**, *6*(02), 238-248

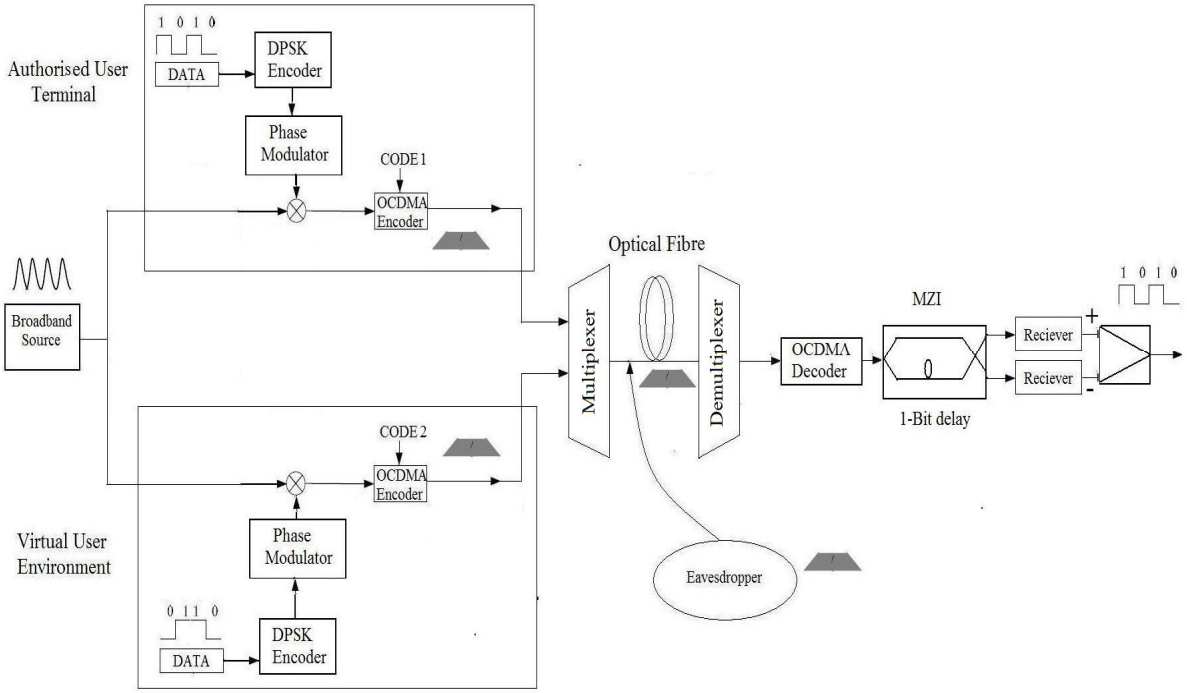



**Figure 2.** Security enhanced DPSK-OCDMA system with virtual user environment for single transmitting user

**Table 1.** Simulation parameters

| Parameter | Value |
|---|---|
| Bit rate (Data rate) | 2.5 Gbps |
| Number of optical sources | 12 mode-locked lasers |
| Wavelength range | 1550–1552.2 nm |
| Wavelength spacing | 0.2 nm |
| Repetition rate of laser pulses | 2.5 Gbps |
| Input power | 1 –5 mW |
| Drive type of electric generator | On-off |
| Signal type of electric generator | Voltage |
| Modulation type | Phase modulation (with a phase shift of $\pi$) |
| Codes used | Zero cross correlation codes (ZCC) |
| Code weight | 3 |
| Code length | 12 |
| Fibre length | 25 km |
| Attenuation | 0.25 dB/km |
| Amplifier gain | 30 dB |
| Delay in MZI | 0.4 ns (1-bit delay) |

*Maejo Int. J. Sci. Technol.* **2012**, *6*(02), 238-248

At the receiver, a spectrally encoded signal was decoded by an authorised user sharing the same zero-cross correlation (ZCC) code [15,16] with the transmitter. One of the consequences of the DPSK format was that optical intensity remained constant during all bits, and thus the direct-detection receivers could not be used to detect the PSK signals. The demodulator consisted of a delay line interferometer that had a 1-bit delay; therefore, 2 bits could be compared at one time [17]. Differential time delay was set to the bit duration. Two outputs of the interferometer corresponded to 'constructive port' and 'destructive port' where maximum power appeared at the former when there was no phase change between adjacent bits, and at the latter when the phase in adjacent bits differed by $\pi$. Then two outputs of the demodulator were input to a balanced receiver that transformed the optical field into an electric current. Next, the output electrical signal from one of the receivers was inverted and both electrical signals were combined by an electrical summer.

After transmission, an eavesdropper employing a simple energy detector and a differential detector was placed. At the differential detector, the incoming signal was split into two paths and combined again with 1-bit difference between the two paths followed by a balanced photo detector [17].

## RESULTS AND DISCUSSION

For both the DPSK-OCDMA and virtual user DPSK-OCDMA schemes, eye diagrams, BER and signals at different locations in the network were measured. The input signal of an authorised user is shown in Figure 3.

The input spectrum consisted of 12 wavelengths. After applying the ZCC code, only three wavelengths passed through the encoder as shown in Figure 4. The code weight was 3 as justified by the encoded spectrum and the code length was 12 as justified by the input spectrum.

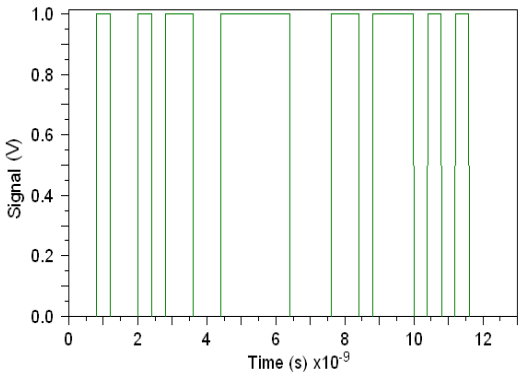
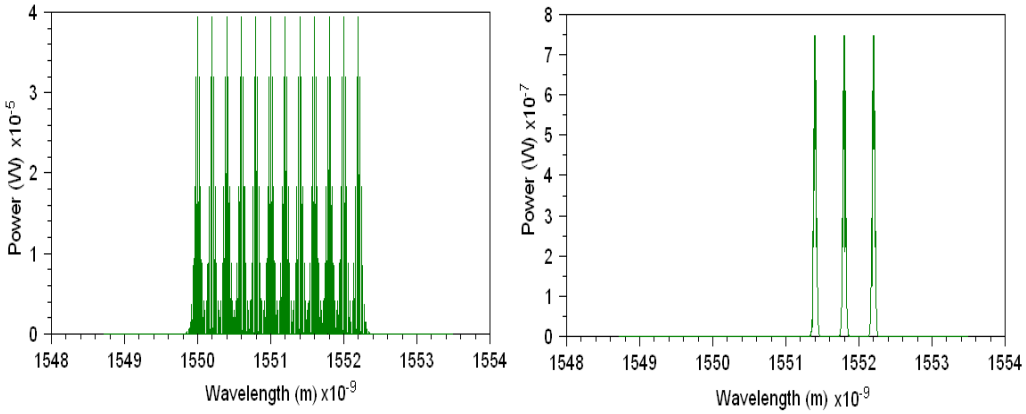



**Figure 3.** Input signal of authorised user

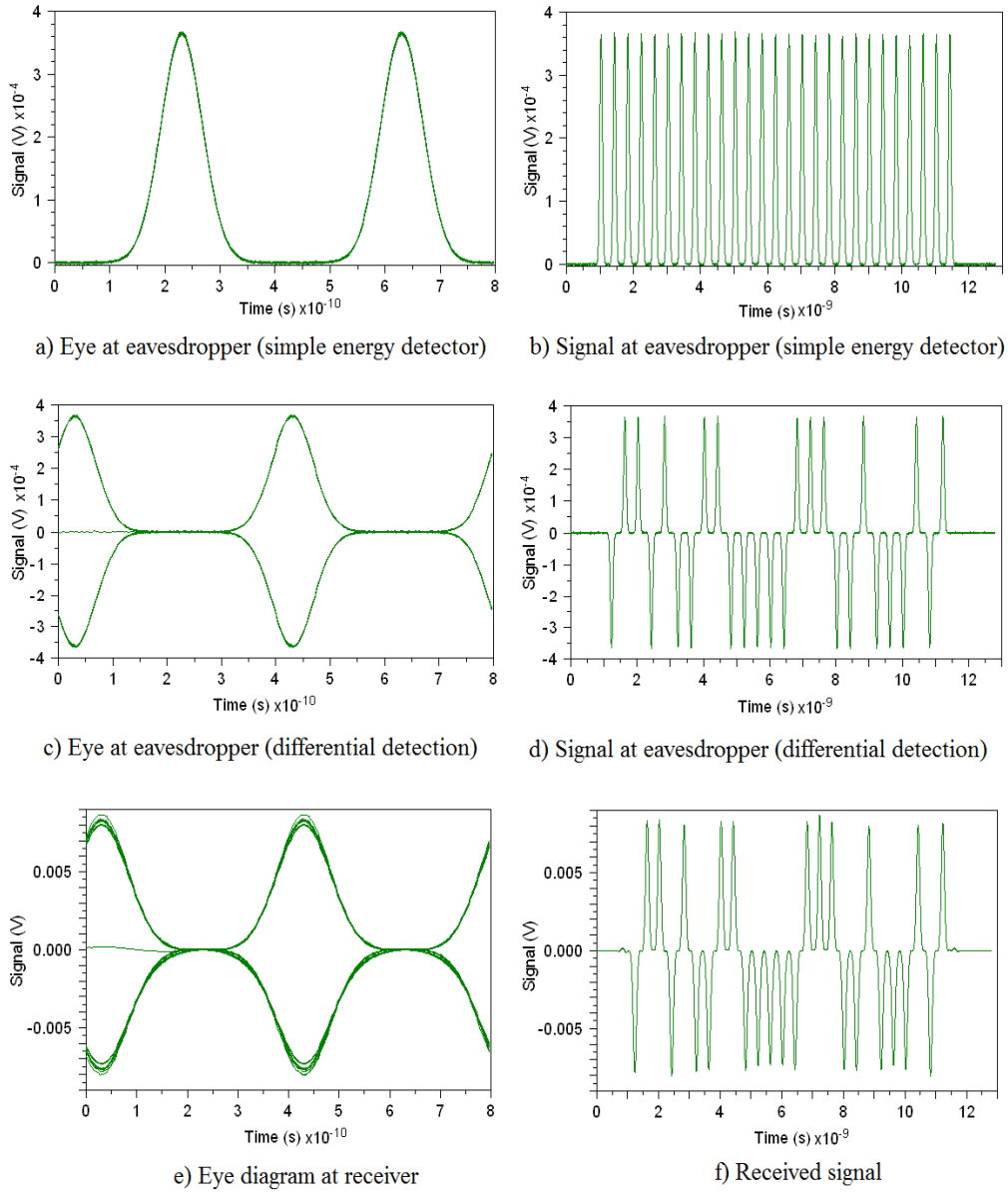
Figure 5(a) shows an eye diagram at the eavesdropper using a simple energy detector when only one user was transmitting. There was no eye opening (which is required) and no intelligible signal was present at the eavesdropper, as shown in Figure 5(b). There was no eye at all because the optical intensity remained constant during all bits, which demonstrates the ability to enhance security by using the DPSK-OCDMA system [4]. At the differential eavesdropper, differential detection was simulated directly without decoding. In this case, the differential detector clearly decoded the data signal without even knowing the code. A clear eye diagram was observed for the DPSK

*Maejo Int. J. Sci. Technol.* **2012**, *6*(02), 238-248




a) Input Spectrum b) Encoded Spectrum

**Figure 4.** Wavelength spectrum before and after encoding




a) Eye at eavesdropper (simple energy detector)

b) Signal at eavesdropper (simple energy detector)

c) Eye at eavesdropper (differential detection)

d) Signal at eavesdropper (differential detection)

e) Eye diagram at receiver

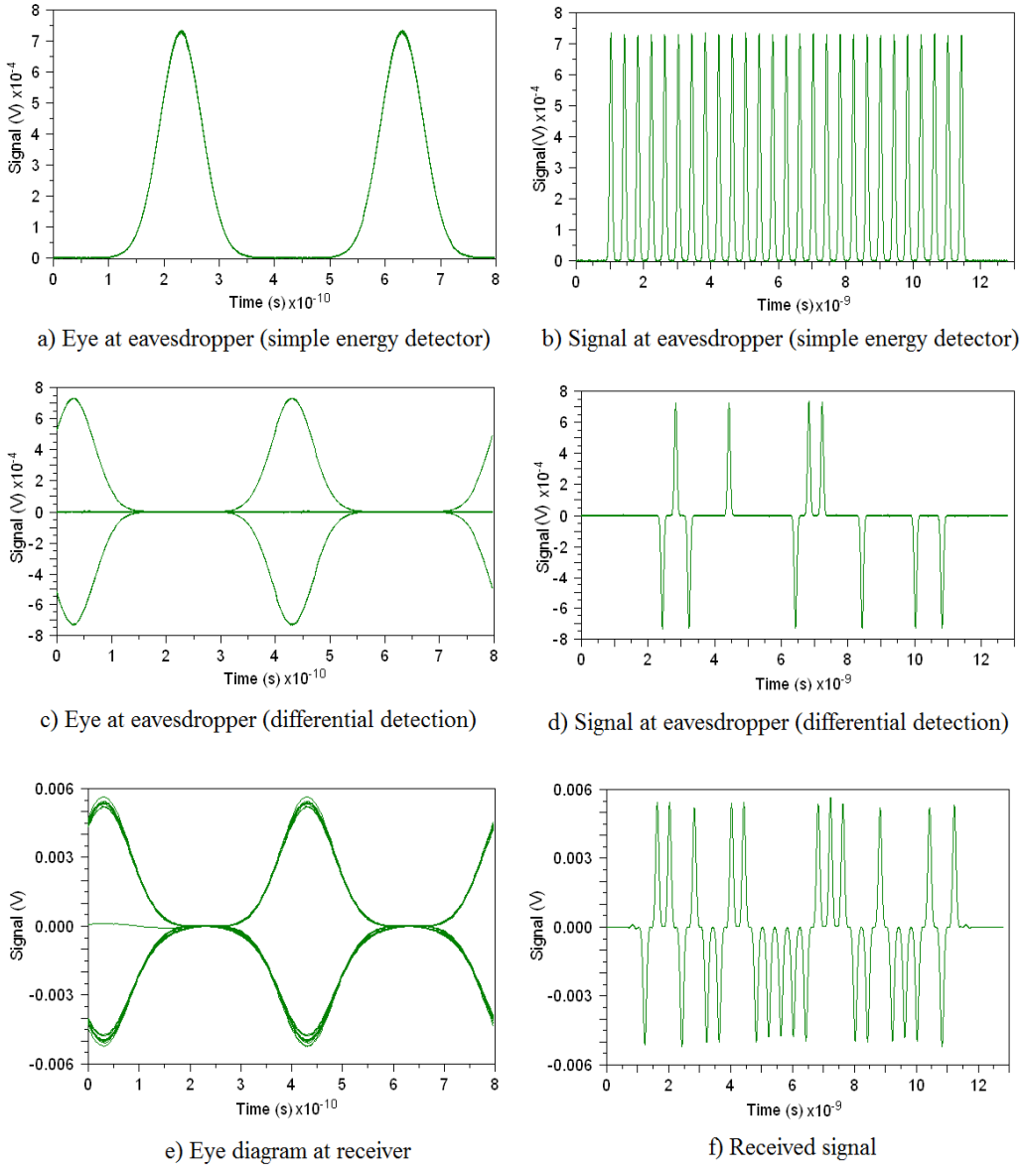
f) Received signal

**Figure 5.** Eye diagrams and signals at various points when a single user is transmitting in DPSK-OCDMA network

*Maejo Int. J. Sci. Technol.* **2012**, *6*(02), 238-248

eavesdropper as shown in Figure 5(c), and the detected signal waveform is shown in Figure 5(d). At the authorised receiver, differential detection was simulated after the OCDMA decoder. In Figure 5(e) also, a clear eye diagram is observed. The received signal is shown in Figure 5(f). It can be seen that the signals at the DPSK eavesdropper and the receiver completely overlap each other. This indicates that an eavesdropper can easily intercept the transmitted information by using differential detection. Therefore, the DPSK-OCDMA system is not secure for a single transmitting user in the presence of differential eavesdropping.

For the virtual user scheme where one user was always transmitting in parallel to the authorised user asynchronously, no eye was observed at the simple power detector, as shown in Figure 6(a), and the optical signal had only '1' bit as shown in Figure 6(b). Therefore, the data could




a) Eye at eavesdropper (simple energy detector)

b) Signal at eavesdropper (simple energy detector)

c) Eye at eavesdropper (differential detection)

d) Signal at eavesdropper (differential detection)

e) Eye diagram at receiver

f) Received signal

**Figure 6.** Eye diagrams and signals at various locations when single user is transmitting in virtual user DPSK-OCDMA network

*Maejo Int. J. Sci. Technol.* **2012**, *6*(02), 238-248

not be detected by the direct detection receiver. Figures 6(c) and 6(d) show the eye diagram and detected signal respectively at the differential eavesdropper. The signal present at the DPSK eavesdropper did not overlap the received signal (Figure 6(f)), which indicates that the differential eavesdropper was getting a false data sequence instead of the original one. Figure 6(e) shows that a clear eye diagram was observed at the authorised receiver. The virtual user here served as an interferer making it difficult for an eavesdropper to properly decode the signal even when a single user was active in the network.

Further, Figure 7 shows the variation of BER as a function of input power at 2.5 Gbps for the DPSK-OCDMA network. It can be seen that eavesdropping with the differential detector can be harmful for this scheme as the BER varies from $10^{-9}$ to $10^{-11}$ with an increase in input power. This level of BER at the eavesdropper is sufficient to detect the transmitted signal correctly and the user security is compromised. Hence the above scheme is susceptible to differential eavesdropping. On the other hand, eavesdropping in the presence of the virtual user scheme gives a high value of BER regardless of the input power. Although the virtual user scheme gives a high BER at the eavesdropper, the BER obtained at the authorised receiver is below the threshold level (dotted red line) at all time and thus the information is successfully conveyed without compromising the security. So it is deduced that implementing the OCDMA system with a virtual user scheme ensures high security against eavesdropping with differential detection without affecting the received signal.

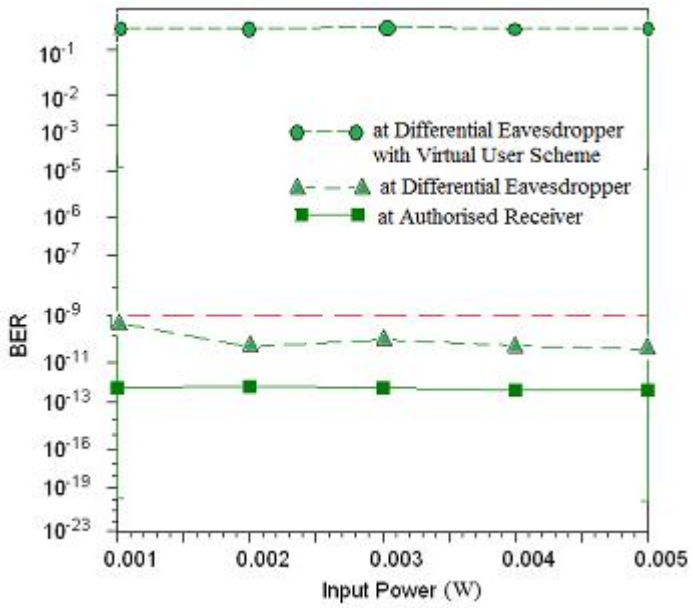



**Figure 7.** BER vs. input power in DPSK-OCDMA network with virtual user scheme

## CONCLUSIONS

The virtual user scheme developed in this work increases the confidentiality of the DPSK-OCDMA system, the system in which a differential eavesdropper can easily read the information transmitted by a single user. The proposed scheme never allows an eavesdropper to isolate a single user's signal while all the other users are dormant or idle. A virtual user alongside an actual user in

an OCDMA system mimics multiple access interference to make eavesdropping difficult. It is clearly seen from the results that the proposed virtual user scheme outperforms the conventional DPSK-OCDMA system in terms of enhanced security against differential eavesdropping. The scheme clearly increases the confidentiality of an OCDMA network without affecting the system performance or incurring any additional bandwidth penalty as compared to DPSK-OCDMA system. Moreover, as compared to the previous virtual user scheme, it is more bandwidth efficient since a common virtual user is created for all the authorised users.

## REFERENCES

1. T. H. Shake, "Security performance of optical CDMA against eavesdropping", *IEEE J. Lightwave Technol.*, **2005**, *23*, 655-670.
2. D. E. Leaird, Z. Jiang and A. M. Weiner, "Experimental investigation of security issues in OCDMA: A code-switching scheme", *Electron. Lett.*, **2005**, *41*, 817-819.
3. Z. Jiang, D. S. Seo, S. D. Yang, D. E. Leaird, R. V. Roussev, C. Langrock, M. M. Fejer and A. M. Weiner, "Four-user, 2.5-Gb/s, spectrally coded O-CDMA system demonstration using low-power nonlinear processing", *IEEE J. Lightwave Technol.*, **2005**, *23*, 143-158.
4. X. Wang, N. Wada, T. Miyazaki, G. Cincotti and K. Kitayama, "Asynchronous multiuser coherent OCDMA system with code-shift-keying and balanced detection", *IEEE J. Select. Topics Quantum Electron.,* **2007**, *13*, 1463-1470.
5. B. Dai, Z. Gao, X. Wang, N. Kataoka and N. Wada, "Experimental investigation on security of temporal phase coding OCDMA system with code-shift keying and differential phase-shift keying", Proceedings of Asia Communications and Photonics Conference and Exhibition (ACP), **2010**, Shanghai, China, pp.427-428.
6. X. Wang, N. Wada, T. Miyazaki and K. Kitayama, "Coherent OCDMA system using DPSK data format with balanced detection", *IEEE Photonics Technol. Lett.*, **2006**, *18*, 826-828.
7. P. R. Prucnal, "Optical Code Division Multiple Access: Fundamentals and Applications", CRC Press, Boca Raton, **2006**.
8. Z. Jiang, D. E. Leaird and A. M. Weiner, "Security issues in OCDMA with multiple-user aggregation", Proceedings of Conference on Lasers and Electro-optics (CLEO), **2007**, Baltimore, USA, pp.1-2.
9. V. Jyoti and R. S. Kaler, "A novel virtual user scheme to increase data confidentiality against eavesdropping in OCDMA network", *Chin. Opt. Lett.*, **2011**, *9*, 120602.
10. G. Manzacca, F. Benedetto, V. Sacchieri, G. Giunta and G. Cincotti, "Advanced modulation formats in optical code division multiple access networks", Proceedings of International Conference on Transparent Optical Networks (ICTON), **2007**, Rome, Italy, pp.91-94.
11. G. Cincotti, N. Kataoka, N. Wada and K. Kitayama, "Perspectives of optical coding/decoding techniques in OCDMA networks", Proceedings of Asia Communications and Photonics Conference and Exhibition (ACP), **2009** , Shanghai, China, pp.1-2.
12. X. Wang, N. Wadat, T. Miyazaki and K. Kitayama, "Demonstration of DPSK-OCDMA with balanced detection to improve MAI and beat noise tolerance in OCDMA system", Proceedings

of Optical Fiber Communication Conference and National Fiber Optic Engineers Conference (OFC/NFOEC), **2006**, Anaheim, USA.

13. X. Wang, N. Wada, T. Miyazaki, G. Cincotti and K. Kitayama, "Advanced modulation techniques in OCDMA system", Proceedings of Optical Fiber Communication and Optoelectronics Conference, **2007**, Shanghai, China, pp.100-102.
14. J. S. Chitode, "Principles of Communication", Technical Publications, Pune, **2009**, pp.12-18.
15. M. S. Anuar, S. A. Aljunid, R. Badlishah, N. M. Saad and I. Andonomic, "Performance analysis of optical zero cross correlation in OCDMA system", *J. Appl. Sci.*, **2007**, *7*, 3819-3822.
16. V. Jyoti and R. S. Kaler, "Design and performance analysis of various one dimensional codes using different data formats for OCDMA system", *Optik-Int. J. Light Electron Opt.*, **2011**, *122*, 843-850.
17. B. Dai, Z. Gao, X. Wang, N. Kataoka and N. Wada, "Demonstration of differential detection on attacking code-shift-keying OCDMA system", *Electron. Lett.*, **2010**, *46*, 1680-1682.