Optical Engineering

SPIEDigitalLibrary.org/oe

Isolated user security enhancement in optical code division multiple access network against eavesdropping

Vishav Jyoti
Rajinder Singh Kaler

SPIE

Isolated user security enhancement in optical code division multiple access network against eavesdropping

Vishav Jyoti and Rajinder Singh Kaler
Thapar University, Electronics and Communication Engineering Department, Patiala 147004, India
E-mail: vishavjyoti@gmail.com

Abstract. A novel virtual user system is modeled for enhancing the security of an optical code division multiple access (OCDMA) network. Although the OCDMA system implementing code shift keying (CSK) is secure against a conventional power detector, it is susceptible to differential eavesdropping. An analytical framework is developed for the CSK-OCDMA system to show eavesdropper's code interception performance for a single transmitting user in the presence of a virtual user. It is shown that the eavesdropper's probability of correct bit interception decreases from 7.1×10^{-1} to 1.85×10^{-5} with the inclusion of the virtual user. Furthermore, the results confirm that the proposed virtual user scheme increases the confidentiality of the CSK-OCDMA system and outperforms the conventional OCDMA scheme in terms of security. © *2012 Society of Photo-Optical Instrumentation Engineers (SPIE).* [DOI: 10.1117/1.OE.51.9.090501]

Subject terms: eavesdropping; optical code division multiple access; security.

Paper 120959L received Jul. 4, 2012; revised manuscript received Aug. 9, 2012; accepted for publication Aug. 13, 2012; published online Sep. 6, 2012.

1 Introduction

Enhanced information security is often said to be inherent in optical code division multiple access (OCDMA) technology.[1,2] It is difficult for an eavesdropper to get any meaningful information from the noise-like OCDMA encoded signal without knowing the code used, but the literature revealed otherwise. The research done on the security shows that the confidentiality of an OCDMA network can be easily compromised whenever an eavesdropper gets isolated user access.[3] An eavesdropper in an OCDMA network can isolate a single user's signal at various locations within the network. One way to isolate an individual user's signal is to put a tap before the multiplexer, i.e., the signal is tapped out even before it gets multiplexed with the multiple user signals. The network confidentiality is also pretty susceptible when only one user is transmitting and all the other users are sitting idle in the same time period.[3,4]

It is found that an isolated OCDMA user with on-off keying (OOK) data modulation format does not have any security of information transmission.[5,6] The code interceptor can easily read the data bits by simply integrating energy over the bit period. In Ref. 4, a virtual user scheme was developed to prevent the isolation of a single user in the network. It was shown that the virtual user scheme increases the security of OOK-OCDMA against a simple power detector.

Moreover, the vulnerability of an OOK-OCDMA system to a simple energy detector is also avoided by code shift keying.[6,7] But it is demonstrated in Ref. 8 that the confidentiality of a code shift keying (CSK)-OCDMA can be easily compromised by a differential eavesdropper.

In this letter, a novel technique has been proposed to enhance the security of a CSK-OCDMA network against differential detection. The underlying principle of the proposed technique is that the obscuration of the targeted signal by forcing the eavesdropper to detect multiple signals simultaneously can increase the level of confidentiality significantly in an OCDMA network.

2 Virtual User Technique

By forcing the eavesdropper to detect multiple signals simultaneously, the eavesdropping attack on the targeted signal can be hindered. Therefore, the level of confidentiality will automatically increase when the eavesdropper is deliberately made to detect multiple user signals in the same time instant. This can be done by incorporating a virtual user in the system as shown in Fig. 1. In this scheme, a virtual user is present in parallel with each authorized user. This dummy user is same for all users using the same codeword. The pseudo random noise is given as the data input to the virtual user and the data is encoded using a unique optical code from the code set used. Both the legitimate signal and the virtual user signal are multiplexed together before being sent on the optical fiber. The virtual user attached to the authorized user will transmit whenever it finds out that a particular user is the only active one in the network. The transmission of a particular virtual user depends on the feedback sent to it by the intelligent feedback control (IFC). It sends the 'ON' feedback signal to the virtual transmitter of that particular user as soon as it detects an isolated user signal. The IFC allows the virtual user to transmit as long as all the other users in the network are not transmitting; otherwise it will send the 'OFF' signal to the active virtual transmitter. So, when only a single user is transmitting while all other users are sitting idle at the same time, the virtual user is the source of multiple access interference which makes the eavesdropper's task difficult. Moreover, the technique is bandwidth efficient as it does not impose any additional bandwidth penalty as compared to conventional CSK-OCDMA network.

3 Eavesdropper's Probability of Correct Bit Interception in Presence of Virtual User

In this section, an analytical framework is developed to analyze the security performance of an isolated user signal in an OCDMA network in the presence of a virtual user. For CSK-OCDMA, the probability that a pulse belonging to a virtual user overlaps with one of the pulses of the desired user is given by Refs. 9 and 10,

$$q = \frac{w^2}{L \times \lambda}, \tag{1}$$

where L is length of code, λ is the number of wavelengths, and w is weight of the code.

0091-3286/2012/$25.00 © 2012 SPIE

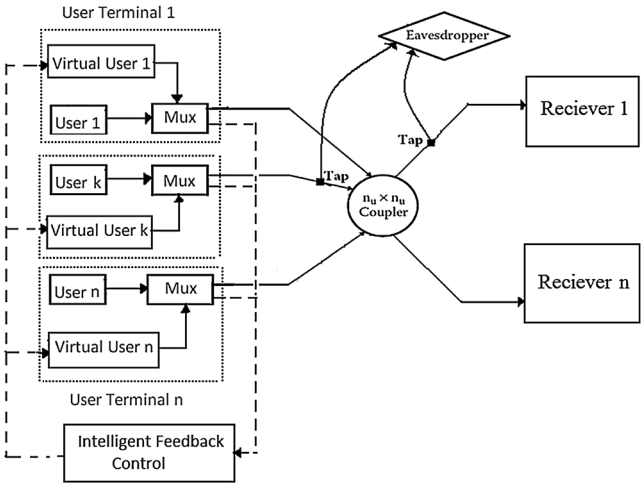

Fig. 1 OCDMA network with virtual user environment.

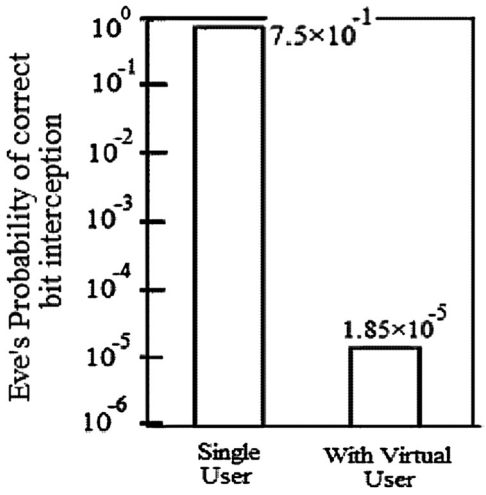

Fig. 2 Eavesdropper's probability of correct bit interception.

In optical orthogonal codes, two code words cannot overlap at more than one pulse position. There are w^2 ways of pairing the w pulses of an authorized user with its virtual user.

One virtual user is created and it generates w hit-of-one over a bit period. The probability of having a pulse's peak v in anyone of $(L-1)$ undesired time slot location is

$$P_r(v) = \binom{w}{v}\left[\sum_{i=0}^{v}(-1)^i\binom{v}{i}\left(1-q+\frac{vq}{w}-\frac{iq}{w}\right)\right]. \quad (2)$$

The probability that t time slot locations have pulse intensity of at least w and remaining $(L-1-t)$ have intensity less than w is given by

$$P_r(w,t) = \binom{L-1}{t}[P_r(w)]^t\left[\sum_{j=0}^{w-1}P_r(j)\right]^{L-1-t}. \quad (3)$$

The probability of correct bit interception at eavesdropper is, when virtual user is active

$$P(\text{virtual}) = \left[\sum_{j=0}^{w-1}P_r(j)\right]^{L-1} + \frac{1}{2}(L-1)[P_r(w)]\left[\sum_{j=0}^{w-1}P_r(j)\right]^{L-2}. \quad (4)$$

Figure 2 shows the probability of correctly detecting the transmitted bit for both cases when first, only a single user is transmitting, and second, when a virtual user is active along with an isolated user.

It is shown that an eavesdropper's probability of correct bit interception decreases from 7.1×10^{-1} to 1.85×10^{-5} with the inclusion of a dummy user. The interference caused by the virtual user degrades the code intercepting performance of an eavesdropper. One can see that the obscuration of the targeted signal in this scenario would significantly increase the level of confidentiality.

4 Results and Discussion

Although CSK improves the security against an energy detector, it is experimentally shown in Ref. 8 that single user CSK-OCDMA signal can be easily intercepted by a differential eavesdropper. In this work, a single user CSK-OCDMA system is simulated in differential eavesdropping environment with and without the virtual user. The carrier signal consists of eight wavelengths starting from 1550 nm to 1551.4 nm spaced 0.2 nm apart. The pseudo random bit sequence data of length 2^7 bits with 2^5 points per bit modulates the carrier signal to generate the modulated optical input signal. For the code switching scheme, both the bits "0" and "1" are encoded, so a code is used for encoding bit "1" and the complementary code is used for encoding bit "0" (see Ref. 4). Each encoder employs spectral encoding using Walsh Hadamard codes.[11] A virtual user created in parallel to the legitimate user produces the same effect as CSK. Different code from the code-set is assigned to the virtual user. Therefore, it appears as one of the authorized users to the eavesdropper. The differential eavesdropper is implemented by combining the received signal with its one bit delayed version followed by balanced detection.[7]

For both CSK and virtual user CSK, the variation of the eavesdropper's bit error rate (BER) with respect to received power is shown in Fig. 3. It is seen that the BER for

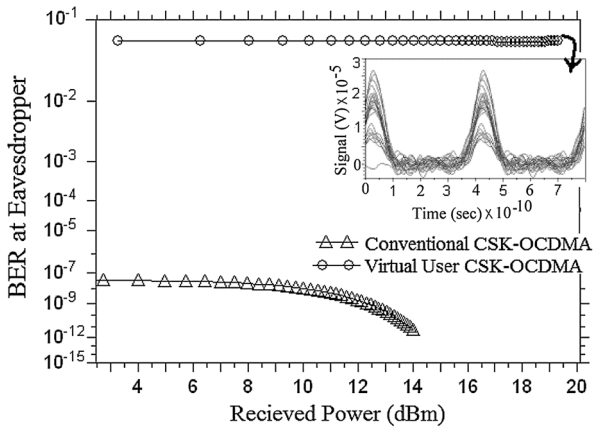

Fig. 3 BER versus received power at eavesdropper.

Table 1 BER at eavesdropper.

Received power (dBm)	BER at eavesdropper	
	Conventinal scheme	Proposed scheme
4	3.34×10^{-8}	4.03×10^{-2}
6	2.90×10^{-8}	4.03×10^{-2}
8	2.26×10^{-8}	4.03×10^{-2}
10	1.07×10^{-8}	4.03×10^{-2}
12	1.67×10^{-9}	4.03×10^{-2}
14	9.06×10^{-12}	4.03×10^{-2}

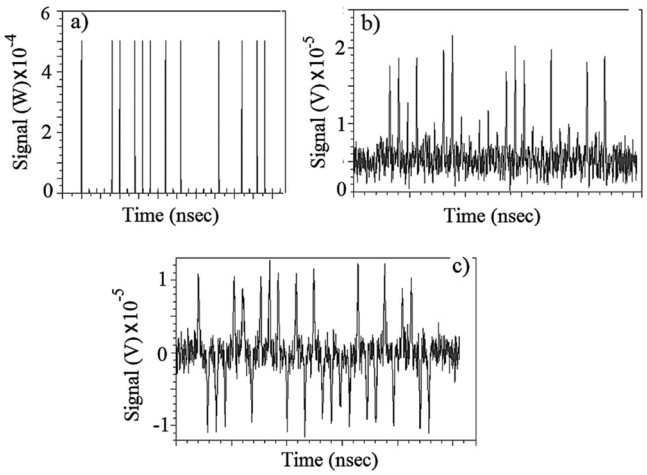

Fig. 4 (a) Input signal, (b) signal at eavesdropper, and (c) received signal.

conventional CSK at the differential interceptor is low which further decreases with the increase in received power, whereas the BER for the virtual user CSK is high and remains unchanged with an increase in received power. This confirms that the virtual user CSK scheme provides robustness against differential eavesdropping to which the ordinary CSK is susceptible.[8] The values of BER at the eavesdropper obtained for both the conventional and proposed scheme have been compared in Table 1 for different values of received power. The BER for the conventional CSK receiver varies from 3.34×10^{-8} to 9.06×10^{-12} while for the proposed scheme the BER remains constant at 4.03×10^{-2}. Low values of BER for the conventional CSK receiver make it possible for the eavesdropper to correctly detect the transmitted information, whereas the high BER using a virtual user scheme denotes that the information is unintelligible to the eavesdropper. Moreover, the virtual user scheme was analyzed for OOK in the presence of a simple power eavesdropper in Ref. 4 and the constant BER obtained at the eavesdropper was 5.6×10^{-3}. In this work, a more sophisticated differential eavesdropper is analyzed for CSK scheme and an improved constant BER of 4.03×10^{-2} is achieved.

Figure 3 also shows an eye diagram measured at differential eavesdropper in the presence of a virtual user. It can be seen that the eye diagram has many levels. The high BER and small eye opening indicate that the received signal at the eavesdropper is fully distorted, thus, the transmission is secure.

Figure 4 shows the input signal, output signal at the receiver, and the signal received by the eavesdropper. The signal received at the eavesdropper in the presence of a virtual user is shown in Fig. 4(b). It is seen that the signal is unintelligible at the eavesdropper, thus, the transmitted information is secure. Although the signal at eavesdropper is unintelligible, the signal received at the authorized receiver [Fig. 4(c)] is perfectly intelligible and is the same as the transmitted signal [Fig. 4(a)]. From the results, it is clear that the inclusion of a dummy user in the OCDMA network enhances its isolated user security and increases the system robustness against eavesdropping.

5 Conclusions

In this letter, a virtual user system is proposed to increase the confidentiality of an OCDMA system. Although the single user CSK-OCDMA is secure against a simple energy detector, it is vulnerable to differential detection. An analytical model is developed for determining the eavesdropper's probability of correct bit interception. It is shown that the eavesdropper's probability of correctly detecting the bits decreases from 7.1×10^{-1} to 1.85×10^{-5} in the presence of a dummy user. Furthermore, the CSK-OCDMA system is simulated in a virtual user environment. The results show that the virtual user scheme decreases the vulnerability of CSK-OCDMA against eavesdropping. Hence, the obscuration of the targeted signal by forcing the eavesdropper to detect multiple signals simultaneously can increase the level of confidentiality significantly in an OCDMA network. The proposed scheme clearly increases the security of an OCDMA network while imposing negligible bandwidth penalty on the system.

References

1. P. R. Prucnal, *Optical Code Division Multiple Access: Fundamentals and Applications*, CRC Press, Taylor and Francis Group, Boca Raton, FL (2006).
2. H. M. R. Al-Khafaji, S. A. Aljunid, and H. A. Fadhil, "Improved BER based on intensity noise alleviation using developed detection technique for incoherent SAC-OCDMA systems," *J. Mod. Optic.* **59**(10), 878–886 (2012).
3. T. Shake, "Security performance of optical CDMA against eavesdropping," *J. Lightw. Technol.* **23**(2), 655–670 (2005).
4. V. Jyoti and R. S. Kaler, "A novel virtual user scheme to increase data confidentiality against eavesdropping in OCDMA network," *Chin. Opt. Lett.* **9**(12), 120602 (2011).
5. D. E. Leaird, Z. Jiang, and A. M. Weiner, "Experimental investigation of security issues in OCDMA: a code-switching scheme," *IET Electron. Lett.* **41**(14), 817–819 (2005).
6. X. Wang et al., "Asynchronous multiuser coherent OCDMA system with code-shift-keying and balanced detection," *IEEE J. Sel. Top. Quantum Electron.* **13**(5), 1463–1470 (2007).
7. H. S. Chung et al., "Experimental demonstration of security-improved OCDMA scheme based on incoherent broadband light source and bipolar coding," *Opt. Fiber Technol.* **14**(2), 130–133 (2008).
8. B. Dai et al., "Demonstration of differential detection on attacking code-shift-keying OCDMA system," *IET Electron. Lett.* **46**(25), 1680–1682 (2010).
9. M. Y. Azizoglu, J. A. Salehi, and Y. Li, "Optical CDMA via temporal codes," *IEEE Trans. Commun.* **40**(7), 1162–1170 (1992).
10. E. Narimanov et al., "Shifted carrier-hopping prime codes for multicode keying in wavelength-time O-CDMA," *IEEE Trans. Commun.* **53**(12), 2150–2156 (2005).
11. 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.* **122**(10), 843–850 (2011).