Novel virtual user scheme to increase data confidentiality against eavesdropping in OCDMA network

Vishav Jyoti* **and R. S. Kaler**

Department of Electronics and Communication, Thapar University, Patiala 147004, India

**Corresponding author: vishavjyoti.phd@thapar.edu*

Received May 30, 2011; accepted August 18, 2011 posted online October 18, 2011

We propose a novel technique to increase the confidentiality of an optical code division multiple access (OCDMA) system. A virtual user technique is analyzed and implemented to make an OCDMA system secure. Using this technique, an eavesdropper will never find an isolated authorized user's signal. When authorized users and virtual users transmit data synchronously and asynchronously, network security increases by 25% and 37.5%, respectively.

OCIS codes: 060.2330, 060.4510, 060.4785.

doi: 10.3788/COL201109.120602.

All-optical networks can satisfy the ever-increasing bandwidth demand from private and business users. In these installations, it is extremely important that data transmitted over fibers cannot be sifted along the path by unauthorized users. Physical layer security is thus becoming an impelling request in the next generation of optical networks.

Eavesdropping is the data interception by an attacker to obtain unauthorized access to routing messages that are not intended for them[1]. This attack jeopardizes the integrity and confidentiality of the data because such packets might be modified and analyzed before being forwarded to the legitimate user[2].

In recent years, security has been one of the major issues in optical code division multiple access (OCDMA) networks because of the ease of eavesdropping despite the optical pulse in OCDMA being encoded into a noise-like signal by the optical encoder according to a unique optical code[3,4].

If multiple codes operate simultaneously, it is almost impossible for an eavesdropper to obtain meaningful information due to the multiple access interference (MAI) caused by all the transmitting users. However, a single transmitting user is vulnerable to an interception attack[5,6].

We describe a simple and feasible approach against eavesdropping by introducing a dummy user in parallel with the primary OCDMA user to block the access to a single transmitting user in this letter, and consider a star network, in which data from all users are collected at some central point and then distributed to all users. This architecture is typical of a local area network (LAN), which is simple and cheap. A typical broadcast star LAN carries individual user signals over approximately 50% of the total fiber length, which gives an eavesdropper plenty of opportunities to tap into individual user signals. Only when a single user is transmitting in a multiuser network can the confidentiality be compromised. Therefore, the security performance of a single-user system is discussed. When more than one user is transmitting, the MAI is high, making it difficult for the eavesdropper to extract any intelligible information in the multiuser transmitting system.

A key observation is that if, at any time, only one user is transmitting, the eavesdropper can detect the data. Thus, user transmissions are only confidential if other signals are being transmitted simultaneously[3]. To increase security, the notion that the presence of multiple users makes deciphering data bits more difficult is exploited.

As shown in Fig. 1, a virtual user environment is created in the network to enhance the confidentiality of an OCDMA system, in which a virtual user will always transmit in parallel with the authorized user. The pseudo random noise is given as the data input to the virtual user. Both users are encoded using different codes and then multiplexed together before sending the signal in the optical fiber. Thus, the virtual user acts as interferer and appears as an authorized user to an eavesdropper; this would hinder eavesdropping. Hence, multiple users make sifting the data bits more difficult.

For synchronous transmissions, two simultaneous transmissions, both OCDMA encoded and modulated using on-off keying (OOK), are considered. Each operates

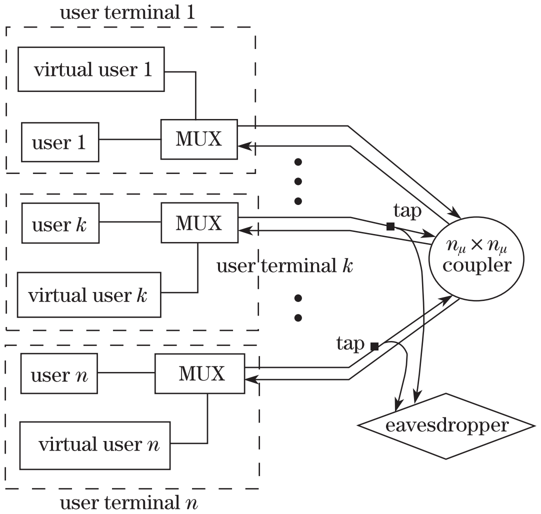


Fig. 1. An eavesdropper tapping into the optical fiber cannot isolate an individual user. MUX: multiplexer.

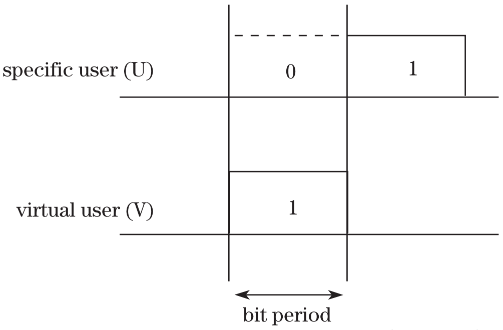


Fig. 2. Two users transmitting synchronously.

Table 1. Different Combinations of Both Users Transmitting Synchronously

Specific User (U) Transmits in a Bit Period	1	1	0	0
Virtual User (V) Transmits in a Bit Period	0	1	0	1
Probability of Both Events Occurring Together, $P_{\rm Com}$	1/4	1/4	1/4	1/4
Detection of an Eavesdropper for a Specific User (U)	True	True	True	False

at data rate D bit/s. A simpler calculation is when all users transmit synchronously (i.e., the beginning and ending times for the transmission of each bit is the same for both users), as shown in Fig. 2.

In a given bit period, equally like "1" and "0" are assumed. The probability that a specific user (U) transmits a "1" or "0" during a given bit period is

$$P_{\rm U}(1) = 1/2 \text{ or } P_{\rm U}(0) = 1/2.$$

Similarly, the probability that a virtual user (V) transmits a "0" or "1" during the same bit period is shown as

$$P_{\rm V}(0) = 1/2 \text{ or } P_{\rm V}(1) = 1/2.$$

Assuming that the value of each data bit is independent of the other data bits and the user bits, the probability that a specific user (U) transmits a "1" while a virtual user (V) transmits a "0" on any particular bit is simply the product of these two probabilities. Thus, the probability of both events occurring together is

$$P_{\rm Com} = P_{\rm U}(1) \times P_V(0) = 1/2 \times 1/2 = 1/4.$$

Hence, there are basically four cases. All other cases are shown in Table 1.

Table 1 shows that if the specific user is transmitting a bit "1", the eavesdropper will correctly detect the data despite what is being transmitted by the virtual user by a simple energy detector.

However, if the specific user is transmitting a "0" in a bit period, it will depend on the virtual user whether an eavesdropper will correctly detect the data or not.

In one out of four cases, in which the specific user transmits a "0" and the virtual user transmits a "1", a simple power detector by the eavesdropper will falsely detect "1" when the authorized user is actually transmitting a "0".

Hence, this virtual user technique will increase the security of an OCDMA by 25% using OOK when both users transmit synchronously.

In asynchronous or non-synchronous transmissions, two simultaneous transmissions, both OCDMA encoded and modulated using OOK, are considered. Each operates at data rate D bit/s. When all users transmit asynchronously, the beginning and ending time for the transmission of each bit is different for both users. Thus, when one user transmits a "1", the other user may transmit fractions of two consecutive bits during the transmission time of the "1" bit due to the lack of synchronization among users, as shown in Fig. 3.

In a given bit period, equally like "1" and "0" are assumed. The probability that a specific user (U) transmits a "1" or "0" during a given bit period is

$$P_{\rm U}(1) = 1/2 \text{ or } P_{\rm U}(0) = 1/2.$$

Similarly, the probability that a virtual user (V) transmits fractions of two consecutive bits (00, 01, 10, 11) during the same bit period is

$$P_{\rm V}(00) = 1/4,\ P_{\rm V}(01) = 1/4,\ P_{\rm V}(10) = 1/4,$$
$$\text{and } P_{\rm V}(11) = 1/4.$$

Assuming that the value of each data bit is independent of the other data bit and the user bits, the probability that a specific user (U) transmits a "1" while the virtual user (V) transmits two consecutive "0" on any particular bit interval is simply the product of these two probabilities.

Thus, the probability of both events occurring together is

$$P_{\rm Com} = P_{\rm U}(1) \times P_{\rm V}(0) = 1/2 \times 1/4 = 1/8.$$

Hence, there are basically eight cases. All other cases are shown in Table 2.

Table 2 shows that if the specific user (U) is transmitting a bit "1", then the eavesdropper will correctly detect the data of the authorized user despite what is being transmitted by the virtual user.

However, if the specific user is transmitting a "0" in a bit period, then it depends on the virtual user whether an eavesdropper will correctly detect the data or not.

In three out of eight cases, in which the specific user transmits a "0" and the virtual user (V) transmits anything other than "00", a simple energy detector will falsely detect "1" when the authorized user is actually transmitting a "0."

Hence, this virtual user technique will increase the security of OCDMA by 37.5% using OOK when both users transmit asynchronously.

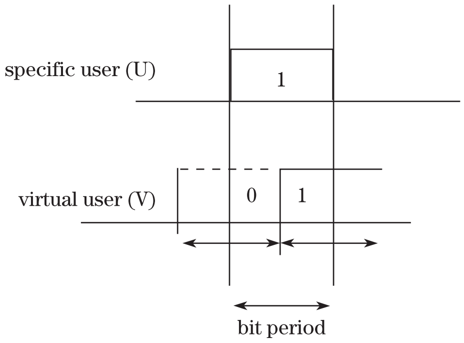


Fig. 3. Two users transmitting asynchronously.

Table 2. Different Combinations of Both Users Transmitting Asynchronously

Specific User (U) Transmits in a Bit Period	Virtual User (V) Transmits in a Bit Period		Probability of Both Events Occurring Together, P_{Com}	Detection of an Eavesdropper for a Specific User (U)
	V_1(Bit 1)	V_2(Bit 2)		
1	0	0	1/8	True
1	0	1	1/8	True
1	1	0	1/8	True
1	1	1	1/8	True
0	0	0	1/8	True
0	0	1	1/8	False
0	1	0	1/8	False
0	1	1	1/8	False

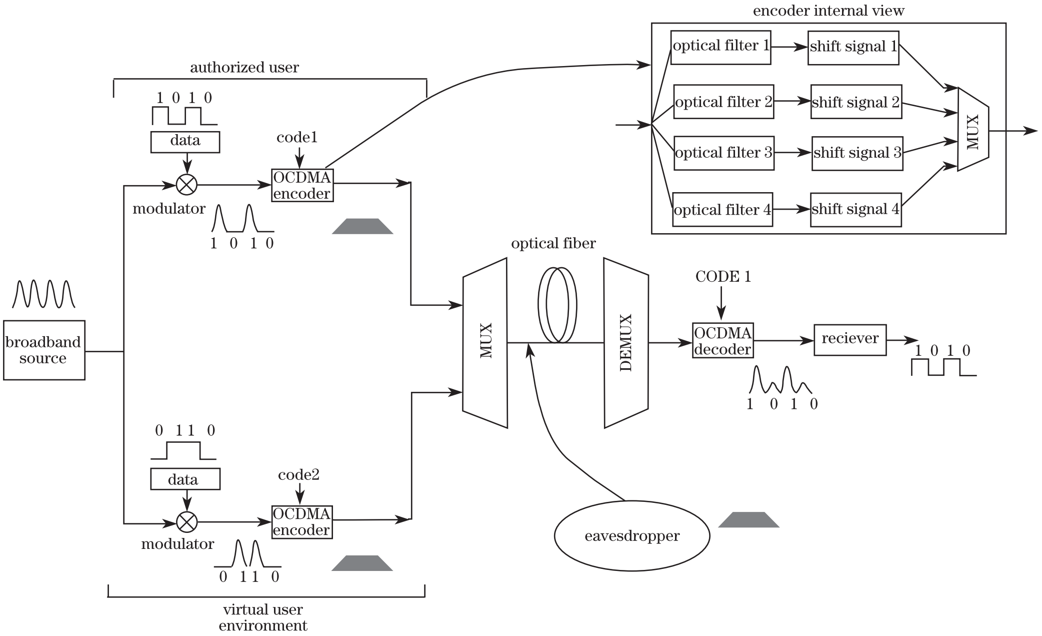


Fig. 4. Simulation setup of OCDMA system in virtual user environment. DEMUX: demultiplexer.

Therefore, the proposed virtual user scheme improves the security, but at the same time sacrifices system performance because the virtual user's signal can be treated as a MAI noise. The BER of the two-dimensional (2D) OCDMA system when only the MAI effect is taken into account is given by[7]

$$P_{\mathrm{b}} = \frac{1}{2}\sum_{i=\mathrm{Th}}^{N-1}\binom{N-1}{i}\left(\frac{w^2}{2n^2}\right)\left(1-\frac{w^2}{2n^2}\right)^{N-1-i},$$

where Th denotes the decision threshold of a receiver (for optimal decision, Th is usually set to code weight); N is the number of users; w is the weight of the code; n is the code length.

An increase in the number of virtual users will increase multiuser interference and, hence, degrades the system performance by increasing the BER of the OCDMA system.

The system performance can be further evaluated in terms of information capacity. The information capacity (C) of an OCDMA system is given by[8]

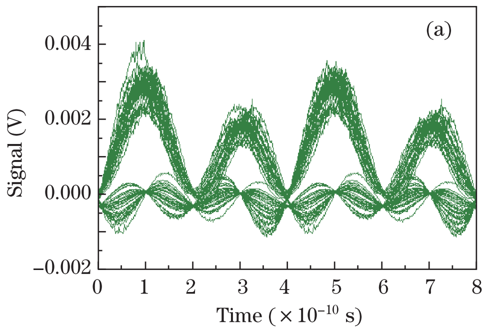
$$C = N\cdot B\left[1-\log_2\left(1+\mathrm{e}^{-\mathrm{SNR}}\right)\right],$$

where N is the number of users and B is the user's bit rate.

In a virtual user scheme, two codes are used at each transmitter (one for the authorized user and the other for the virtual user) from the given code set. To maintain the desirable BER, as in the case of a simple 2D OCDMA system, the number of users is halved in virtual user OCDMA. Thus, system capacity is halved for the proposed scheme.

Hence, the proposed virtual user system increases security, this has its cost. Reduced system performance is a common side effect of increased security.

The security-enhanced OCDMA system implementing the virtual user environment is shown in Fig. 4. An OCDMA system based on OOK for a single transmitting



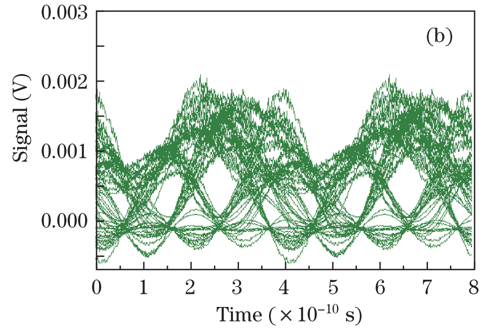


Fig. 5. Eye diagram at eavesdropper. (a) Single and (b) virtual user environments.

user is implemented using the software OptSim.

The broadband signal is composed of the multiplexed output of the four-mode locked laser ranging from 1 550 to 1 551.2 nm, with a wavelength spacing of 0.4 nm. The repetition rate of the lasers is 2.5 Gbps, which is the same as the bit rate. The pseudo random binary sequence (PRBS) generator is used to produce a PRBS, and an on–off type electrical generator is utilized with the non-return-to-zero (NRZ) modulation format. To implement the OOK OCDMA system, amplitude modulation is done at the modulator.

Furthermore, 2D wavelength/time (W/T) matrix codes[9,10] are used for encoding. In an encoder, four optical filters and four shift signals are used to produce the encoded bit stream. The optical filter is used to filter out one spectral wavelength, and the shift signal is used to produce a pulse at a specified chip. The optical MUX combines four displaced pulses to form an encoded signal. Encoders and decoders respectively use delay and inverse delay-line arrays[11], providing delays in terms of integer multiples of chip times. The placement of the delay-line arrays and the amount of each delay are dictated by the specifics of the user signatures.

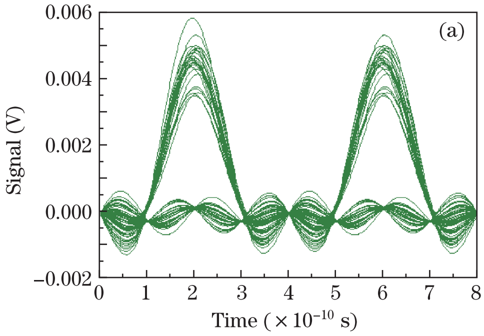
The encoded data from both users are multiplexed and then passed through a 25-km standard single-mode fiber with an attenuation of 0.25 dB/km; it is further followed by a loss-compensating optical amplifier with a gain of 30 dB. The output signal from an optical fiber then passes through a demultiplexer and routed to the user's decoder. At the receiver, only the authorized user code is given to the decoder. The decoded signal finally arrives at the optical receiver and the BER tester. After transmission, an eavesdropper employing a simple energy detector is placed to sift the data.

In Figs. 5(a) and (b), the eye diagrams detected by the eavesdropperfor a single user and virtual user, respectively, are shown. The eye diagram of the single user eavesdropper is open and the signal is correctly detected by the eavesdropper. On the contrary, the eye diagram measured for the eavesdropper in the virtual user environment has many levels, leaving the signal fully distorted, which then prevents a malicious attacker from sifting the transmission. An eavesdropper tapping a signal in a virtual user environment will have significant difficulty in deciphering the transmission without the use of the matching codes.

In Fig. 6, the eye diagrams of the authorized users are shown for the single user and the virtual user. With the matching codes, the signal is correctly decoded in both cases as the eyes are completely open. In the latter case, as observed in Fig. 6(b), some distortion can be seen in the eye diagram due to the MAI caused by the virtual user.

The BER measurements are performed, as shown in Fig. 7, to compare the performance of the authorized and unauthorized users. Figure 7(a) shows that the BER for both the eavesdropper and the receiver is very low for the single transmitting user, which means that the data are correctly decoded at the eavesdropper without knowing the code used at the transmitter. On the contrary, the BER simulation of Fig. 7(b) shows a large difference in performance between the authorized user (solid line) and the eavesdropper (dotted line). By creating a virtual user environment, in which the authorized user has to transmit with the virtual user, the BER for an eavesdropper is very high (ranging from 10^{-3} to 10^{-2}); this means that the eavesdropper is not able to decode any received signal.

In conclusion, a security-enhanced OCDMA system using the virtual scheme is proposed to protect against eavesdropping. To increase security, the notion that the presence of multiple users makes deciphering the data bits more difficult is exploited. The virtual user scheme



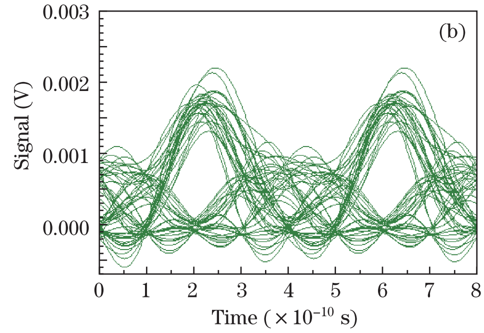


Fig. 6. Eye diagram at authentic receiver. (a) Single and (b) virtual user environments.

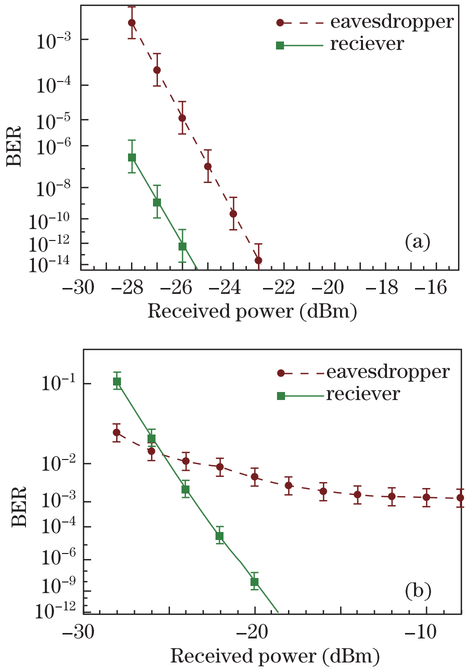


Fig. 7. BER versus received power. (a) Single and (b) virtual user environments.

makes an OCDMA network less vulnerable to eavesdropping by increasing the security of the OCDMA system by 25% and 37.5% for synchronous and asynchronous cases, respectively. Hence, the novel virtual user scheme provides the OCDMA system immunity against eavesdropping when a single user is active in the network and, as in conventional OCDMA schemes, an authorized user clearly decodes the original data.

References

1. A. Teixeira, A. Vieira, J. Andrade, A. Quinta, M. Lima, R. Nogueira, P. André, and G. Tosi Beleffi, in *Proceedings of International Conference of Transparent Optical Networks 2008* 123 (2008).
2. P. R. Prucnal, *Optical Code Division Multiple Access: Fundamentals and Applications* (CRC Press, Cleveland, 2006).
3. T. H. Shake, J. Lightwave Technol. **23,** 655 (2005).
4. A. Stok and E. H. Sargent, IEEE Comm. Mag. **40,** 83 (2002).
5. D. E. Leaird, Z. Jiang, and A. M. Weiner, Electron. Lett. **41,** 817 (2005).
6. X. Wang, N. Wada, T. Miyazaki, G. Cincotti, and K. I. Kitayama, IEEE J. Sel. Top. Quantum Electron. **13,** 1463 (2007).
7. H. Yin and D. J. Richardson, *Optical Code Division Multiple Access Communication Networks Theory and Applications* (Tsinghua University Press, Beijing, 2007).
8. G. Cincotti, N. Kataoka, N. Wada, and K. Kitayama, in *Proceedings of OSA/ACP 2009* TuDD1 (2009).
9. A. J. Mendez, R. M. Gagliardi, V. J. Hernandez, C. V. Bennett, and W. J. Lennon, J. Lightwave Technol. **21,** 2524 (2003).
10. A. J. Mendez, R. M. Gagliardi, H. X. C. Feng, J. P. Heritage, and J.-M. Morookian, J. Lightwave Technol. **18,** 1685 (2000).
11. A. J. Mendez, R. M. Gagliardi, V. J. Hernandez, C. V. Bennet, and W. J. Lennon, J. Lightwave Technol. **22,** 2409 (2004).