DATA SECURITY IN OPTICAL CDMA SYSTEMS
Jaswinder Singh

Address for Correspondence
Dept. of Electronics & Communication Engineering
Beant College of Engineering & Technology, Gurdaspur, India
E-mail j_singh73@rediffmail.com

ABSTRACT
Data security is one of the most crucial requirements in present day communication systems. While the digital systems rely on encryption techniques, the optical CDMA systems are inherently secure since their operation involves unique code assignment to the users. This is because of the fact that only the matched code receivers are able to decode the transmissions whereas the receivers with unmatched codes will not be able to retrieve any signal. In this paper, the different scenarios of breach of data security have been explored and the various techniques proposed for assuring the data security have been discussed.

I. INTRODUCTION
Data security is one of the most crucial requirements in present day communication systems. Encryption has been the most reliable technique employed for data security in digital systems but encryption employs the need of generation of public and the private keys which make the terminal equipments more complex. The optical CDMA systems whereas employ unique codes as addresses assigned to different users and these codes are used to code the transmitted bits such that only the intended receiver with the desired code will be able to retrieve the information. This hence assures data security in optical CDMA systems. The first and foremost feature that is desired of the codes is that the codes should be orthogonal to each other so that these have the minimum cross-correlation to each other. The second desired feature is that the off-peak auto-correlation should also be the smallest. Keeping in view these conditions, many code families have been designed so far satisfying the auto- and cross-correlation properties. While optical CDMA is inherently secure but still under some situations, the data is susceptible to breach. The various such situations of data breach are described below.

II. TYPES OF BREACH
Figure 1 shows the generalized optical CDMA system and its structural and functional components [1]. The transmitter uses an electro-optic converter which converts the base band data to optical signal. This is then encoded by the CDMA encoder which transmits a code for the coded bit. The coded signal through the coupler is fed to the network along with the coded signals from the other users. The receiver uses a decoder that utilizes the time-shifted version of the same code as that has been used in the transmitter. The decoded signal is then converted to the electrical form by the optical to electrical converter. A threshold detector decides on the bit.

The OOK systems are most prone to the security breach since the eavesdropper can wait for the instant when only the targeted user is present in the network. So the transmission can be detected by employing data-rate power detection. This is the most serious threat in the optical CDMA
systems. This is why the OOK signaling is not secure at all for optical CDMA systems. Even if antipodal signaling (transmitting both the ‘1’ and the ‘0’ bits) is employed, in the above case, this also presents two possible signals. Hence, this is also not secure under the circumstances discussed above.

**III. SCHEMES TO IMPROVE DATA SECURITY**

Tancevski and Andonovic (1996) [2] have studied the hybrid wavelength/time spreading systems using extended quadratic congruence sequences for wavelength hopping and prime sequences for time spreading. The system security has been evaluated using the above codes. Shake (2005) [3] emphasized that the user data security against an eavesdropper is a very critical issue, as the data can be tapped even without the knowledge of the user optical code by the analysis of the data pattern, i.e. by a data-rate power measurement. Wang et al. (2007) [4] have described a code-shift-keying scheme to increase security against an eavesdropper. A similar work using code switching in the spectral phase coded OCDMA system has been carried out by Leaird et al. (2005) [5]. Many other proposals for increasing the security have been suggested and evaluated by Prucnal et al. (2008) [6], Glesk et al. (2007) [7], Nasaruddin and Tsujioka (2008) [8]. Prucnal et al. (2008) have carried out code swapping on bit-by-bit basis. In Glesk et al. (2007), either of the two codes is transmitted depending on a RF code swapping sequence. It has been shown by Nasaruddin and Tsujioka (2008) that by increasing the number of codes reserved per user for encoding, the probability of breaking of the user code by an eavesdropper is reduced. All the above techniques (Prucnal et al. (2008), Glesk et al. (2007), Nasaruddin and Tsujioka (2008)) hence are based on reserving additional codes for a user i.e. the number of codes assigned per user are increased in order to reduce the chances of an eavesdropper to detect and analyze the data patterns of a user.

The authors have proposed two codes families of 3-D wavelength/time/space codes for optical CDMA systems and have also shown that using the proposed codes, very secure system can be designed.

The various techniques proposed in the literature for improving the data security are listed below.

- Antipodal signaling
- Code Swapping using some random sequence
- Code swapping using RF sequence
- Bit-by-bit Code shifting
- Single code keying with offset bit
- Single code keying with overlapped offset bit

This is shown in figure 2. The coders can be reconfigured by using tunable delay elements. Both the bits are transmitted using 1-bit and 0-bit coders. With code swapping, more than one code is used for each bit and the code is swapped according to some RF sequence or random sequence. The code can be switched on bit-by-bit basis. The code swapping or code shifting techniques use reconfigurable coders. The authors had proposed a reconfigurable coder based on 3-D GRZ1-BCDD codes [9] which is shown in figure 2. Single code keying uses the same code for transmission of both the ‘1’ bits as well as ‘0’ bits for synchronous optical CDMA systems. It can use either of the two schemes i.e. offset bit transmissions or overlapped offset bit transmissions. The offset bit transmissions though are slightly complex but this results in higher throughput.

**IV. CONCLUSIONS**

Data security is one of the most crucial requirements in present day communication systems. While the digital systems rely on encryption techniques, the optical CDMA systems are inherently secure since their operation involves unique code assignment to the users. In this paper, the different scenarios of breach of data security have been explored and the various techniques proposed for assuring the data security have been discussed.
Fig. 2. Reconfigurable Encoder/Decoder using AWG’s to encode the 1-bit and 0-bit [9].

REFERENCES


