Security Performance of LDPC and Polar Codes in UV Wireless Communications

Xuetong Liang, Min Zhang, Xicong Li, Lin Ai
State Key Lab of Info. Photon. & Opt. Comm.
Beijing University of Posts and Telecommunications
Beijing, China
Email: mzhang@bupt.edu.cn

Zabih Ghassemlooy
Optical Communications Research Group,
Faculty of Engineering and Environment
Northumbria University
Newcastle, England
Email: z.ghassemlooy@northumbria.ac.uk

Abstract- **The growing demand for access to high-capacity wireless communication systems opens up the need for the alternative and complementary technology of optical wireless communications including ultraviolet (UV). In modern wireless communications networks the users and data security, which is extremely important in order to ensure users' data protection and confidentiality, has become a hot topic. In this paper, we investigate security in a UV communications system by adopting two well-known coding schemes of low-density parity-check (LDPC) and polar codes (PCs). We show that the UV system with coding offers enhanced security performance compared to the un-coded system with the PCs offering a higher security level and a longer transmission span compared to the LDPC.**

Keywords- UV communication; security gap; LDPC codes; polar codes

I. INTRODUCTION

With the wide spread use of smart devices, the use of wireless communications has become critical nowadays due to the limited available radio frequency (RF) spectrum. Optical wireless communications covering the ultraviolet (UV), visible and infrared (IR) bands can alleviate the spectrum congestion, thus becoming a potential alternative to future communication demands [1]. The IR technology has been used in short-and medium-range free space communications. However, the link performance is susceptible to interference. Additionally, the ambient lights (Sun and others indoor lights) may significantly degrade the IR link performance. Alternatively, the UV communications (UVC) technology could be used in a free space channel in either line of sight (LOS) or non-LOS (NLOS) configuration, with reduced pointing, acquisition and tracking issues and lower noise levels. The UVC technology has been used commercially for both indoor and outdoor applications air purifications.

For outdoor applications, UV links - with specific properties of atmospheric scattering and radiation in the solar blind region (200-280 nm) – offering higher transmission data rates can be used in combination with the existing RF technology, thus providing new communications diversity with higher user's capacity [2]. However, the UV spectrum also suffers from atmosphere scattering as it interacts with the atmosphere's aerosol constituents. The scattering feature is used as an advantage in UV systems to establish a NLOS link in outdoor environments, which leads to much reduced requirements for acquisition, pointing, and tracking [3].

In the past several years, considerable amount of theoretical and experimental research works have been reported on UVC with increased transmission link span [4], [5] and improved mobility [6]. In addition, UVC networks are proposed [7]. However, the broadcasting nature of UVC (as in RF systems) makes security a potential problem in real practical applications, which needs investigating in order to a high level of data protection and confidentiality. The security problem becomes much more serious as the number of users increases. To provide high-level of security, the data must be encrypted or systematically scramble at the cost of increased level of system complexity. In order to reduce the complexity and still achieve the required security level, channel coding has been used at the physical layer [8], [9].

In UVC networks, the traditional cryptographic techniques cannot be used due to energy limitations. It also leads to the risk of disruption or control of the entire network. Thus, the introduction of security at the physical layer in UVC systems. In [8] a special model for the physical layer security was introduced as illustrated in Fig. 1.

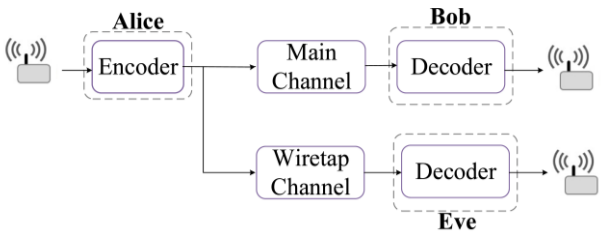

Figure 1. The block diagram of the wiretap channel

In this scheme, Alice send messages to Bob through the main channel, and at the same time Eve can eavesdrop the message through the wiretap channel. In order to increase both reliability and security of the communications link, a coding

scheme was introduced by Wyner [1], where the security gap was considered to be as smaller as possible. To achieve this and improve the link performance, channel coding schemes including Reed-Solomon (RS), low-density parity-check (LDPC), and polar codes (PCs) have been adopted in UVC [10][11]. Both RS and LDPC codes were adopted in [9] to increase and the transmission span by about 32% and 78%, respectively. Using PCs, the link span increased further by 10%.

In this paper, we investigate and compare the bit error rate (BER) and the security performance of UVC using LDPC and PCs. The simulation based results show that the UVC link with Pcs offers improved security and BER performance compared with the LDPC. The rest of the paper is organized as follows. In Section I, we introduce the basic structure of the UVC and analyze the characteristics of security coding. The decoding and encoding of LDPC and PCs are introduced in Section III. The UV system BER and security performance are outlined in Section IV, whereas conclusion is presented in Section V.

II. PRELIMINARY

A. UV Communications

The schematic diagram of the UVC system employing both LDPC and PCs is shown in Fig. 2. It consists of the transmitter (Tx), the UV channel, and the receiver (Rx). The data stream is encoded prior to intensity modulation of the UV light emitting diode. At the Rx, following transmission through the wireless channel a photomultiplier tube (PMT) is used to regenerate the electrical signal from the received optical signal, which is then decoded to recover the data information. The received signal is given by:

$$y(t) = h(t) \otimes x(t) + n(t) \tag{1}$$

where, $h(t)$, $x(t)$ and $n(t)$ are channel transfer function, transmitted signal and the additive white Gaussian noise, respectively.

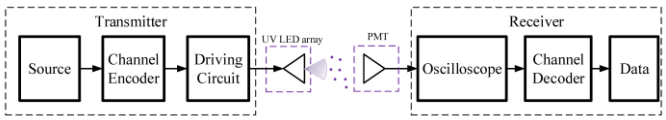

Figure 2. Block aiagram of UV communication with channel coding

B. Security Gap

In order to reduce the impact of path loss and increase the transmission link span channel coding have been widely used [10]. The purpose of channel coding adopted in this context is two folds i.e., to improve the link performance and minimize the probability of eavesdropper, which is different to the traditional channel coding. For improved link security, it is stated that the security gap (SG) must be as small as possible [12].

In general, the relationship between the BER performance following channel coding and the signal to noise ratio (SNR) is illustrated in Fig. 3. The concept of the security gap, which is used to measure the communication security performance, is best illustrated in Fig. 3. P_e^B and P_e^E represent the average probability of errors (i.e., the BER) following decoding of Bob's and Eve's messages, respectively. $P_{e,\min}^E$ and $P_{e,\max}^B$ are the threshold levels. If BER > $P_{e,\min}^E$ of ≈ 0.5，then Eve will not be able to recover the message, whereas if the BER < $P_{e,\max}^B$ (i.e., ≈ 0) then Bob can complete the reliable communications. Therefore, the following conditions must be hold [8]:

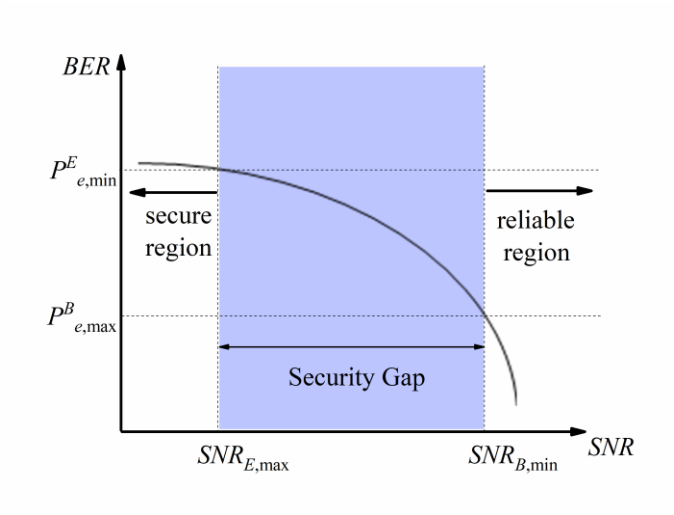

Figure 3. The security gap defined in terms of BER and SNR in [8]

$$P_e^B \le P_{e,\max}^B \text{ (reliability)} \tag{2}$$

$$P_e^E \ge P_{e,\min}^E \text{ (security)} \tag{3}$$

Note that, there are two *SNR* levels of $SNR_{E,\max}$ and $SNR_{B,\min}$, which hold true for (3) and (2) as defined in [12]. Instead of considering the absolute values of *SNR*s, we define the security gap (SG) as:

$$SG = SNR_{B,\min} - SNR_{E,\max} \quad \text{(dB)} \tag{4}$$

As can be observed from Fig. 3, the steeper the slope, the smaller is the SG. The performance of security code improves with the decrease of SG. Note that, a SG as low as a few dB is sufficient for BER > 0.5 for the eavesdropper [11].

III. CHANNEL CODING

To provide security the main concept is to hide the data information from the eavesdroppers by means of puncturing. In this way, the data bits are punctured in the encoder that can only be recovered by means of channel observations of the transmitted bit stream at the decoder. Therefore, with a low SNR level at the eavesdropper's end the reconstruction of punctured data bits is challenging since channel observations are noisy. Alternatively, channel coding schemes have been used to provide a sufficient level of data security. In the following, we outline two coding schemes widely used in wireless transmissions and evaluate their capabilities in

This study is supported by NSFC Project No.61471052

reducing the transmission energy loss and in improving the error correcting ability, thus higher data security.

A. LDPC Codes

LDPC codes, proposed by Gallager in 1962, is a linear block code with a sparse parity check matrix, with enhanced error correction capability and reduced encoding and decoding complexities. An example of a parity check matrix is given by:

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \tag{5}$$

Tanner graph of H is depicted in Fig. 4, where CN and VN are the check and variable nodes, respectively.

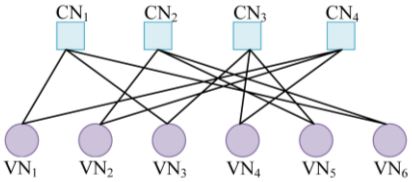

Figure 4. Tanner graph of the H matrix given in (5) example codes

The encoding can be described as:

$$c = uG \tag{6}$$

where c is the output, u is the input block and G is the generator matrix, which can be obtained from H. The details of construction and algorithm of LDPC codes are given in [10].

B. Polar Codes

PCS are one of newest channel coding scheme proposed by Arikan in 2008 [13], which offers improved channel capacity by means of channel combining and channel splitting. In this scheme, channels are divided into two parts of reliable and unreliable, where the information is transferred over the reliable channels. Traditionally, the block lengths are defined as $N = 2^n$, and following coding the information bits can be presented by the non-symmetric code word as given by:

$$x_1^N = u_1^N G_N \tag{7}$$

where u a properly prepared N-bit row-vector, and G_N is an $N \times N$ generator matrix given by:

$$G_N = F^{\otimes n} \tag{8}$$

$$F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \tag{9}$$

where $F^{\otimes n}$ is the Kronecker power.

Considering the complexity of decoding, the successive cancellation (SC) decoding algorithm is used to achieve the symmetric channel capacity. SC decoding estimates bits sequentially starting with u_0. The likelihood for each bit is given as:

$$L_N^{(i)} = \frac{W_N^{(i)}\left(y_1^N, \hat{u}_1^{i-1} \middle| 0\right)}{W_N^{(i)}\left(y_1^N, \hat{u}_1^{i-1} \middle| 1\right)} \tag{10}$$

where y_1^N is received values, W_N is the combination channel and $\hat{u}_1^{i-1}$ is the previously decoded bits in a successive order.

We define the likelihood density per each splitting channel $W_N^{(i)}$ as $L_N^{(i)}$, and by applying the hard decision to (9) we have:

$$\hat{u}_1^N = \begin{cases} 0, \; if \; L_N^{(i)}(y_1^N, \hat{u}_1^{i-1} \geq 1) \\ 1, \qquad otherwise \end{cases} \tag{11}$$

The message received can be decoded by using the recursive algorithm.

IV. SIMULATION RESULTS

In this section, we compare the BER performance of the UV system and the security gap when using both LDPC and PCs. We have adopted the system model given in [14] for the UVC. In order to analyze the BER performance of LDPC and PCs, a coding and decoding platform was built in MATLAB. The code rates for the LDPC and PCs were set to 0.5, whereas the code lengths were set to 960 and 1024, respectively. We used a data format of non-return to zero on and off keying for intensity modulation of the UV light source. The key parameters are shown in Table 1, which are based on measurements reported in the literature.

Fig. 5 shows the simulated the BER performance versus the transmission distance for the UV link with LDPC and PCs for $P_{e,max}^{B}$ of 10^{-6} and a range of elevation angle of 0° (i.e., the LOS), 5°, and 10°. Also shown for comparison is the plot for the un-coded UV link. As can be seen, the coded system offer increased transmission span compared to the un-coded system. For the LOS propagation channel at a BER of 10^{-4} (which is below the forward error correction limit of 10^{-3}) the link span increases by 18% and 57% for the LDPC and PCs, respectively compared to the un-coded link. For the NLOS propagation channel and for the elevation angle between the Tx and the Rx of 5°-5° and 10°-10°, respectively the simulation results are very similar for the coding schemes. However, PCs still outperform LDPC and the un-coded link. The link span increases by 20% and 47% for LDPC and PCs, respectively compared to the un-coded link at the elevation angle of 5°-5°, and increases by 10% and 35%, respectively at the elevation angle of 10°-10°. Considering the background noise and the limited transmit average power, the effective communication distance is 20 m, which is more or less as in a LOS link, however, it can be extended by increasing the transmit power and applying relay-assisted scheme [4], [5].

Fig. 6 shows the simulated average BER performance for the eavesdropper (i.e., Eve) as a function of the SG for un-

coded, and coded UV communications. It can be observed from Fig. 6 that using PCs the BER performance is more sensitive to the SG for the PCs when compared with the un-coded and LDPC code plots. The SG values for un-coded, and coded UV links and for two reliability threshold levels are presented in Table 2. From Table 2 and Fig. 6, it can be observed that the link with PCs offers the lowest SG values of 3.5 and 5.5 for the $P^{E}_{e,min}$ of 0.4 and 0.5, respectively compared to un-coded and LPDC-based UV systems. For example, assuming $P^{B}_{e,\max}$ is 10^{-6} and $P^{E}_{e,\min}$ is 0.4, Eve cannot recover the message when the difference between the *SNRs* for Bob and Eve is more than 3.5 dB, while it is 20 dB and 23 dB, respectively for LDPC codes and un-coded links. Note that, for PCs, the channel is divided into two parts with and without noise. The intended users are given the preference to noiseless channel for transmitting their data. This is reflected in the simulation results for lower *SNR*s.

TABLE I. SIMULATED UV COMMUNICATION SYSTEM PARAMETERS

Parameter	Value	Parameter	Value
Wavelength	265 nm	PMT Gain	6.32×10^{5}
Transmit average power	2.1 mW	Modulation	OOK
LDPC codes	(960, 480)	Polar codes	(1024, 512)
PMT radiant sensitivity (at 265nm)	62 mA/W	Optical filter transmission	20%

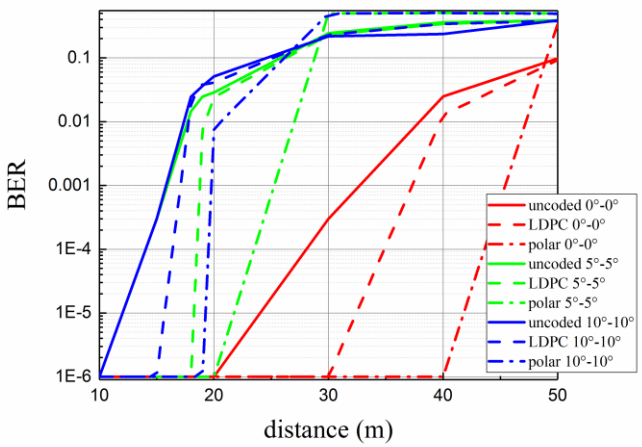

Figure 5. Simulation results of LDPC codes and polar codes in UV communication system with different evevation angles

TABLE II. SECURITY GAP IN DIFFERENT $P^{E}_{e,\min}$ WITH LDPC CODES AND POLAR CODES

Eve's BER	conditions	Security gap (dB)
$P^{E}_{e,\min}$ =0.4	Un-coded	23
	LDPC codes	20
	Polar codes	3.5
$P^{E}_{e,\min}$ =0.5	Un-coded	40
	LDPC codes	30
	Polar codes	5.5

V. CONCULUSION

Security is an important issue in modern wireless communication networks. Steps must be taken to provide both reliability and security at the physical and network layers. In this paper, we considered ultraviolet wireless communications system with both LDPC and polar codes and evaluated its security performance and compared to an un-coded ultraviolet link. Simulation resulted showed that using the polar codes the UV communication system offered improved performance in terms of the BER compared to the un-coded and LDPC code based links.

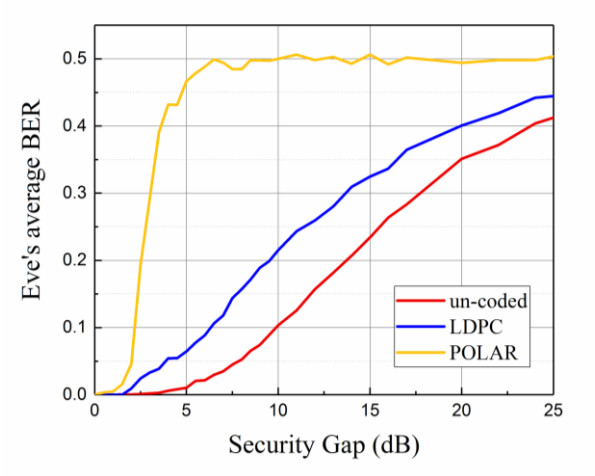

Figure 6. Eve`s BER versus the security gap with LDPC codes and polar codes

VI. ACKNOWLEDGE

This study is supported by Chinese NSFC Project No.: 61471052.

REFERENCES

[1] Uysal, M., Capsoni, C., Ghassemlooy, Z., Boucouvalas, A. C., and Udvary E. G. (Eds.): Optical Wireless Communications – An Emerging Technology, Springer, 2016. ISBN: 978-3-319-30200-3

[2] Z. Xu and B. M. Sadler, "Ultraviolet Communications: Potential and State-Of-The-Art," in IEEE Communications Magazine, vol. 46, no. 5, pp. 67-73, May 2008.

[3] D.M. Junge, "Non-line-of-sight electro-optic laser communications in the middle ultraviolet," M.S. Thesis, Naval Postgraduate School,Monterey, CA, December (1977)

[4] Liao L. Long Distance Non-Line-of-Sight Ultraviolet Communication Channel Analysis and Experimental Verification[D]. UC Riverside, 2015.

[5] Ardakani M H, Uysal M. Relay-assisted OFDM for NLOS ultraviolet communication[C]//Transparent Optical Networks (ICTON), 2015 17th International Conference on. IEEE, 2015: 1-4.

[6] Shi J, Zhang M, Han D, et al. Experimental study of the mobility feature and selective maximal ratio combining algorithm for UV communication[C]//Networks and Optical Communications-(NOC), 2015 20th European Conference on. IEEE, 2015: 1-4.

[7] Song P, Ke X, Song F, et al. Multi-user interference in a non-line-of-sight ultraviolet communication network[J]. Iet Communications, 2016, 10(13): 1640-1645.

[8] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp.1355–1387, Oct. 1975

[9] Csiszar I and Korner J. Broadcast channel with confidential messages[J]. IEEE Transactions on Information Theory, 1978,

[10] Menglong Wu, Dahai Han, Xiang Zhang, Feng Zhang, Min Zhang, and Guangxin Yue, "Experimental research and comparison of LDPC and RS channel coding in ultraviolet communication systems," Opt. Express 22, 5422-5430 (2014)

[11] W. Hu, Z. Luo, D. Han, Q. Chen, L. Ai and M. Zhang, "A scheme of ultraviolet communication system with polar channel coding," 2017 16th International Conference on Optical Communications and Networks (ICOCN), Wuzhen, China, 2017, pp. 1-3.

[12] Klinc D, Jeongseok H, McLaughlin S W, et al.. LDPC codes for the Gaussian wiretap channel[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 532-540.

[13] E. Arikan, "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," in IEEE Transactions on Information Theory, vol. 55, no. 7, pp. 3051-3073, July 2009.

[14] Gang Chen, Zhengyuan Xu, Haipeng Ding, and Brian M. Sadler, "Path loss modeling and performance trade-off study for short-range non-line-of-sight ultraviolet communications," Opt. Express 17, 3929-3940 (2009)