LETTER

Anti-Interception Vortex Microwave Photon Transmission with Covert Differential Channel

Yuanhe WANG[†], ***Nonmember and*** **Chao ZHANG**[†a)], ***Senior Member***

SUMMARY With the emphasis on personal information privacy protection in wireless communications, the new dimension low-interception covert transmission technology represented by the vortex wave with Orbital Angular Momentum (OAM) has received attention from both academia and industry. However, the current OAM low-interception transmission techniques all assume that the eavesdropper can only receive plane wave signals, which is a very ideal situation. Once the eavesdropper is configured with an OAM sensor, the so-called mode covert channel will be completely exposed. To solve this problem, this paper proposes a vortex microwave photon low-interception transmission method. The proposed method utilizes the differential operation between plane and vortex microwave photons signals to construct the covert differential channel, which can hide the user data in the mode domain. Compared with the traditional spread spectrum transmission, our proposed covert differential channel schemes need less transmitted power to achieve reliable transmission, which means less possibility of being intercepted by the eavesdropper.

key words: *wireless communications, secure communications, anti-interception, vortex microwave photon*

1. Introduction

Along with the rapid development of weak signal detection technology, the openness of wireless communications signal makes the traditional electric field strength signal hard to be hidden from the eavesdroppers [1]. In this background, Orbital Angular Momentum (OAM) based low-intercept secure communications technology, in which the physical dimension of OAM is independent of the electric field strength, has received attention from the industry [2]. Among OAM techonologies, the vortex microwave photons transmission with intrinsic OAM is the focus of wireless communications research, especially in the covert transmission with new dimensions [3]–[5].

The current covert transmissions with OAM assume that the eavesdropper is not aware of the existence of the OAM signal and still adopts the traditional plane wave sensor. Once the eavesdropper knows that the legitimate transmission link utilizes the OAM vortex wave transmission scheme, it can receive and intercept user information by configuring OAM sensors, and the vortex mode channel will no longer have the covert characteristic. To solve this problem, this paper proposes a low-intercept vortex microwave photon transmission method with covert differential channels, which utilizes the difference between plane wave and vortex microwave photons signals to construct the covert channel combined with the spread spectrum. The proposed scheme can achieve a higher capability of anti-interception transmission.

2. Principle and Architecture

The principle of covert differential channel transmission is shown in Fig. 1. The differential operation between the plane wave (Mode 0) signal $x^{(0)}(t)$ and the vortex microwave photon (Mode 1) signal $x^{(1)}(t)$ constructs a covert differential channel. The spread sequences allocated to Mode 0 and Mode 1 are $c^{(0)}[k]$ and $c^{(1)}[k]$, where $c^{(i)}[k] \in \{-1, 1\}$, $i = 0$ or 1 which denotes Mode 0 or Mode 1 respectively. Mode 0 directly transmits the spread sequence signal that $x^{(0)}(t) = \sum_{0 \le k \le G_0 - 1} c^{(0)}[k]\, g(t - kT_c)$, where G_0 is the length of the spread code, T_c is the chip period, $g(t)$ is the rectangular function with the width T_c. The transmitted signal on Mode 1 is

$$\begin{aligned} x^{(1)}(t) &= s_0 \sum_{0 \le k \le G_0 - 1} \left(c^{(0)}[k] \oplus c^{(1)}[k] \right) g(t - kT_c) \\ &= s_0 \sum_{0 \le k \le G_0 - 1} c^{(C)}[k]\, g(t - kT_c) \end{aligned}, \quad (1)$$

where s_0 is the user data, "$\oplus$" is XOR operation that $f(x) \oplus g(x) = -f(x)g(x)$. The differential operation between $c^{(0)}[k]$ and $c^{(1)}[k]$ forms the covert differential signal $c^{(C)}[k] = c^{(0)}[k] \oplus c^{(1)}[k]$. Then the user data are recovered with $c^{(C)}[k]$ by the Direct Sequence Spread Spectrum (DSSS) technology. The above is the recovery process, and the transmitting process of user data is vice versa. Take Fig. 1 as an example, the spread sequences are "-,+,+,-,-,+,+,-" and "-,+,+,-,+,-,-,+", where "+" and "-" represent "+1" and "-1" respectively. When transmitting

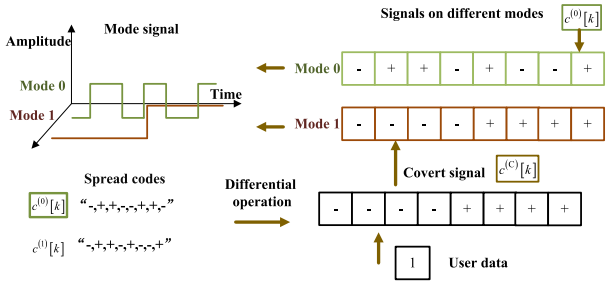

Fig. 1 Principle of covert differential channel transmission.

Manuscript received December 14, 2023.
Manuscript revised May 1, 2024.
Manuscript publicized June 14, 2024.

[†]Labs of Avionics, School of Aerospace Engineering, Tsinghua University, Beijing, 100084, P. R. China.
a) E-mail: zhangchao@tsinghua.edu.cn

DOI: 10.1587/transfun.2023EAL2108

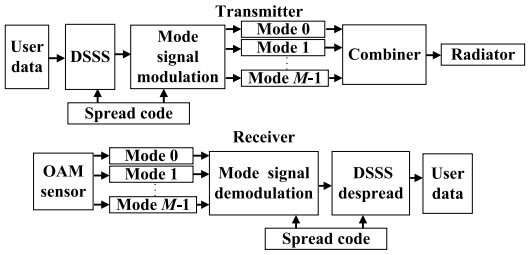

Fig. 2 System architecture of anti-interception transmission.

the user data, the covert signal is the result of differential operation between the $c^{(0)}[k]$ and $c^{(1)}[k]$. The signal on Mode 0 ($x^{(0)}(t)$) directly transmits the spread sequence that "-,+,+,-,-,+,+,-". The user data are spread by the $c^{(C)}[k]$ and transmitted on Mode 1.

In fact, the covert differential channel with two modes can be extended to M modes ($M > 2$), which can be shown as the mode signal modulation module in Fig. 2. The spread code allocated for Mode m is denoted as $c^{(m)}[k]$, $0 \le m \le M-1$, $0 \le k \le G_0 - 1$. The corresponding signal waveform is $c^{(m)}(t) = \sum_{0 \le k \le G_0-1} c^{(m)}[k]\, g(t - kT_c)$. The signal on mode i is $x^{(i)}(t) = s_0 c^{(0)}(t) \oplus c^{(1)}(t) \oplus \cdots \oplus c^{(M-1)}(t)$ where the Mode i is randomly selected from M modes, s_0 is the user data. The signal on other mode is $x^{(m)}(t) = c^{(m)}(t)$, $m \ne i$.

Receiver firstly obtains and sorts different mode signals by the OAM sensor [5]. Then the covert differential signal can be recovered by the differential operation with different mode signals $y^{(m)}(t)$ $(0 \le m \le M-1)$, which is written as

$$y^{(C)}(t) = y^{(0)}(t) \oplus y^{(1)}(t) \cdots \oplus y^{(M-1)}(t). \tag{2}$$

At last, the spread code sequence is utilized in the DSSS despread module to recover the user data that $\hat{s}_0 = \left[\int_0^{G_0 T_c} c^{(i)}(t)\, y^{(C)}(t)\, dt\right] / (G_0 T_c)$, where the $c^{(i)}(t)$ is the signal of spread code allocated for Mode i that is known at the receiver.

Compared to the DSSS transmission without covert differential channel, the received Signal-to-Noise Ratio (SNR) after DSSS despread can be improved from $G_0\gamma_0$ to $MG_0\gamma_0$, where γ_0 is the received SNR.

From the above analysis, the eavesdropper cannot intercept the user data without knowing the M spread sequences, the transmitted signals on mode domain, and the differential channel modulation method simultaneously.

3. Simulation and Discussion

In order to verify the effectiveness of the proposed scheme, the case that the eavesdropper equipped with OAM sensor is considered. Figure 3 gives the Bit Error Rate (BER) curves with the E_b/N_0 for different transmission schemes. Here, E_b/N_0 is defined as the received SNR after DSSS despread, which is written as $G_0\gamma_0$. In this case, the spread code length is 8, and the numbers of modes are 2 and 3. The difference

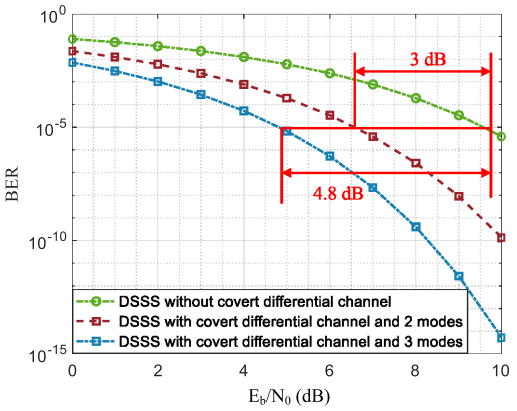

Fig. 3 BER curves with different transmission schemes.

between 2 modes and 3 modes transmissions is that higher received signal power can be obtained with more mode channels. The 3 spread sequences on 3 modes can be given by Walsh codes, i.e., $\{-+-+-+-+\}$, $\{-++--++-\}$ and $\{-+--++-+\}$.

From the simulation, it can be seen that compared to the traditional DSSS transmission, the covert differential channel transmissions with 2 modes or 3 modes respectively enjoy 3 dB or 4.8 dB gain in E_b/N_0 when BER is 10^{-5}. It can be seen that more modes are utilized in the transmission, more gain in the received SNR can be obtained, i.e., less requirement in the transmitted power and possibility of being intercepted can be achieved.

4. Conclusion

In this paper, the vortex microwave photon low-interception transmission with covert differential channel is proposed and the corresponding performance is evaluated. The differential operation between different modes signals constructs the covert channel that hides from the eavesdropper. Compared to the traditional DSSS scheme, our proposed scheme is hard to be intercepted due to less transmitted power needed to achieve the same BER.

References

[1] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security, and intelligence," IEEE Wireless Commun., vol.27, no.5, pp.126–132, Oct. 2020.
[2] C. Zhang and Y. Wang, "Orbital angular momentum: New physical resource and dimension for future MIMO," IEEE Commun. Mag., vol.61, no.10, pp.148–154, Oct. 2023.
[3] C. Zhang and X. Jiang, "Secure high-speed spread spectrum transmission system with orbital angular momentum," IET Communications, vol.14, no.11, pp.1709–1717, 2020.
[4] L. Liang, W. Cheng, W. Zhang, and H. Zhang, "Mode hopping for anti-jamming in radio vortex wireless communications," IEEE Trans. Veh. Technol., vol.67, no.8, pp.7018–7032, Aug. 2018.
[5] C. Zhang, X. Jiang, Z. Wang, Y. Wang, Q. Wu, X. Xie, and W. Tian, "Orbital angular momentum detection device for vortex microwave photons," Commun. Eng., vol.2, no.1, p.11, 2023.