# Performance Analysis of DFTs-OFDM based QAM/QNSC Transmission System under Jamming Attack

Ke Zhang, Yajie Li, Mingrui Zhang, Shuang Wei, Wei Wang,
Yongli Zhao, Jie Zhang
*Beijing University of Posts and Telecommunications*
*Beijing, 100876, China*
jie.zhang@bupt.edu.cn

Yongyuan Liu
*Beitsing Communications Technology Co., Ltd.*
*Beijing, 100088, China*

***Abstract*—We devise an implementation of jamming attack and analyze performance through simulation and experimentation in DFTs-OFDM QAM/QNSC. The results show that the system have certain robustness under jamming attack with low power.**

***Keywords—jamming attack, performance analysis, physical cipher, QNSC***

## I. Introduction

Optical networks are vulnerable to attacks at the physical layer, typically aimed at disrupting the service or gaining unauthorized access to carried data. Thus, physical layer security issues are becoming increasingly important [1]. Quantum noise stream cipher (QNSC) is proposed to overcome physical layer security risks [2]. Besides, it allows high transmission rates and long distances owing to the encoding and decoding are performed in digital signal processing (DSP). The security originates from the noise in the transmission system including quantum noise and amplifier spontaneous emission noise. The security of quadrature amplitude modulation (QAM) based QNSC (QAM/QNSC) has been analyzed in [3], which shows that data and keys can be secured through specific parameter settings in transmission system. Moreover, the QNSC based on Discrete-Fourier-Transform Spread Orthogonal Frequency Division Multiplexing (DFTs-OFDM) we propose in [4] provides superior transmission and security performance.

However, there are several typical physical layer attacks which could compromise the security of QNSC systems, such as fast correlation attack, collective attack, message falsification and jamming attack. Fast correlation attack is an attack method that uses the correlation between the output sequence of the key generator and the output sequence of Linear Feedback Shift Register (LFSR) to obtain the seed key. The performance of the long distance QNSC system under the fast correlation attack is analyzed in [5]. It shows that the security can be ensured in QNSC system through maintaining a high-level noise masking and timely updating the seed keys. It is verified that QNSC system can achieve nonzero secure rate even if Eve intercepts useful information by collective attacks [6]. The information-theoretic security of message falsification is proved basing on the time-translational symmetry of the Y00 signals modulated by pseudo-random number generators [7].

The jamming attack is an implementation method of signal insertion attacks, which degrades the transmission performance of legitimate connection and even results in service denial in the worst case. However, the performance of QNSC under jamming attack has not been analyzed.

In this paper, we devise an implementation of jamming attack and evaluate the security performance of DFTs-OFDM QAM/QNSC transmission system under the jamming attack. Simulation results demonstrate that the system can prevent jamming attack from disruption of the legitimate transmission under the jamming signal with the power lower than -2.5dBm and linewidth less than 2000kHz. At a transmission distance of 100km, the performance loss at the transmitter and receiver is about 0.6dB and 0.7dB respectively when the jamming is implemented with the power of -1dBm. Last, we conduct an experimental verification in the DFTs-OFDM-based QAM/QNSC transmission system. Consequently, the system has a certain robustness under the jamming attack.

## II. Principle of QAM/QNSC and Jamming Attack

### *A. Principle of QAM/QNSC*

QAM/QNSC is a physical layer encryption technique that encrypts the amplitude and phase of the data. The data is divided into two paths, in-phase (I) and orthogonal (Q) component. Then the original data stream is mapped into QPSK symbols. n-bit I and Q data are encrypted by modulating their amplitudes with m-bit basis states, so that both I and Q have $2^M$ ( $M = n + m - 1$ ) levels of different amplitudes. The I and Q paths are orthogonal. As a result, $M$ -bit encrypted I and Q data, namely $2^M \times 2^M$ QAM data are generated. Specifically, 1-bit plaintext (0, 1) and 4-bit base (1110, 0100) generate the ciphertext message (0110, 1100) after encryption. And signals are mapped into the 64 QAM constellation. For the 4-bit ciphertext of the I/Q channel, the first bit is the result of the XOR of 1-bit plaintext and the lowest bit of the corresponding base, and the last is the lower 3-bit of the 4-bit base.

Since the legitimate parties share the key in advance, the I and Q data can be received correctly by the signal processing based on the pre-shared key. However, the eavesdropper cannot recover the data without the key, thus it can be seen that QAM/QNSC ensures security.

### *B. Implementation of jamming attack*

Jamming attack can be achieved by inserting jamming signal into a legitimate channel within or outside the signal bandwidth, called in-band or out-of-band jamming. It may increase nonlinear effects and crosstalk in fiber and cause gain competition between the jamming signal with high power and weaker legitimate signal in optical amplifier, which significantly degrades the transmission performance. An in-band jamming signal overlaps with the useful optical channel and adds unfilterable noise. Fig. 1 shows an implementation

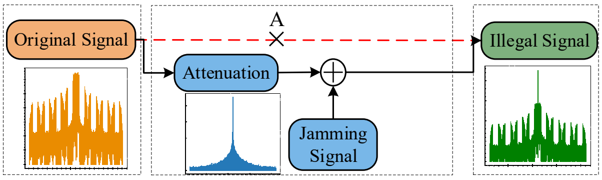

Fig. 1 Implementation of jamming attack

method of in-band jamming attack established to quantify the influence of jamming attack on transmission performance.

- The attacker Eve cuts off the optical fiber in point A and intercepts the original signal from legitimate transmitter Alice. The example of power spectrum of original signal is shown in Fig.1. The total power of the original signal is $P_{OS}$ as the frequency integration of the power spectrum.
- Eve attenuates the original signal. The attenuation coefficient ( $AC$ ) is freely chosen by Eve.
- Eve generates a jamming signal with variable linewidth and power $P_{JS}$ . The example of power spectrum of jamming signal is shown in Fig. 1.
- Eve inserts jamming signal into the center of bandwidth of attenuated original signal to generate the illegal signal which is then transmitted through the cut optical fiber from point A to Bob. The power spectrum of illegal signal is obviously different from the original signal as shown in Fig. 1.

Since the original signal is attenuated, the jamming signal can cause a gain competition in optical amplifier where the high-powered signal robs weaker original signal of gain. Besides, the jamming signal can also increase nonlinear effects in fiber. Therefore, the BER calculated by legitimate receiver Bob increases. This paper considers the power of the illegal signal ( $P_{IS}$ ) is equal to $P_{OS}$ in which case Bob cannot detect Eve by monitoring the power variation of received signal only. The power of the illegal signal is equal to $P_{OS}$ (dBm) if $AC$ (dB) and $P_{JS}$ (dBm) satisfy the following formula:

$$10^{P_{JS}/10} = 1 - 10^{(P_{IS}-AC)/10} \tag{1}$$

## III. Simulation Setup and Results Analysis

### A. DSP in DFTs-OFDM QAM/QNSC Transmission System

Fig. 2(a) shows the DSP in transmitter and receiver of DFTs-OFDM QAM/QNSC system. At the transmitter, the pseudo-random binary sequence (PRBS) is modulated into QPSK data, followed by encryption of the QPSK data using a key shared by both legitimate parties to generate an encrypted QAM/QNSC signal. Then, by applying a 256-point DFT, the I/Q signal is transmitted to two different sub-bands, which retain some subcarriers around zero frequency called guard interval are reserved. A 1024-point IDFT is used to generate the DFTs-OFDM signal by padding the high-frequency portion with zeros. After the IDFT data from frequency domain to time domain, the cyclic prefix (CP) of 32-symbol length is inserted to resist the inter-symbol interference caused by polarization mode dispersion during transmission, and finally the analog signal obtained by D/A is transmitted to the fiber link. At the receiver side, the detected signal is operated by carrier recovery [8]. Then, the CP is removed after timing synchronization and the data is converted from the time domain to the frequency domain by 1024-point DFT. Channel estimation and equalization are performed on the signal. After frequency domain equalization, 256-point IDFT is applied to recover the encrypted QAM/QNSC signals. Then, the encrypted signals are decrypted into QPSK signals. Finally, the QPSK signals are demodulated into binary data.

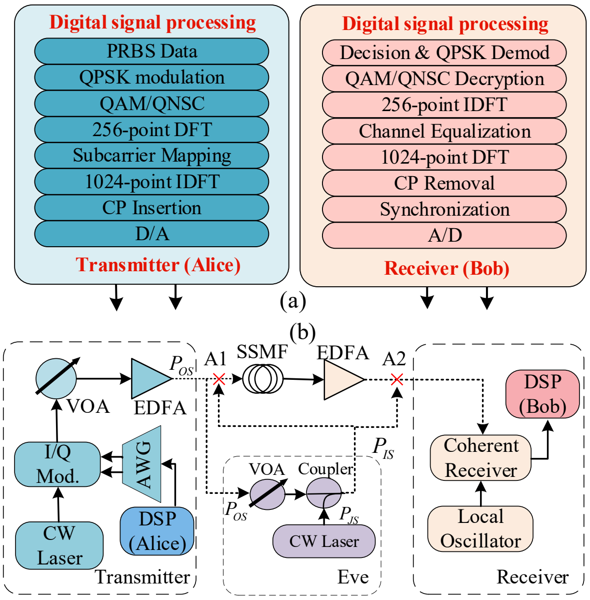

Fig. 2 Simulation setup: (a) DSP in transmitter and receiver; (b) QAM/QNSC under jamming attack

### B. Simulation setup

Fig.2(b) shows the simulation flow-process of the $2^M \times 2^M$ QAM/QNSC under jamming attack. A continuous wave (CW) laser sends a beam at 1550nm with 10dBm power into an I/Q modulator. At the transmitter, the I and Q data are converted by an arbitrary waveform generator (AWG) to an electrical signal at the sampling rate of 10GSa/s. Then, the optical signal goes through the variable optical attenuator (VOA) and is amplified by an erbium-doped fiber amplifier (EDFA) into 0dBm. The attacker Eve intercepts the signal after this EDFA and attenuates it with attenuation of $AC$ . Afterwards, Eve generates a jamming signal by CW laser with $P_{JS}$ power and linewidth and inserts it into the attenuated signal through a power combiner at transmitter (point A1) and receiver (point A2). $P_{JS}$ and $AC$ satisfy the Eq. (1). Finally, the illegal signal is transmitted through a 100km standard single-mode fiber (SSMF) with the attenuation of 0.2dB/km. At the receiver, the received optical signal is amplified into 0dBm, and then detected by a coherent optical receiver which is combined with a CW laser. The received I/Q signals are captured by a 40GSa/s oscilloscope.

### C. Simulation results analysis

To analyze the transmission performance of DFTs-OFDM based QAM/QNSC system under jamming attack, we analyze the effect of different jamming signal power, different jamming signal linewidth and different transmission distance on the system.

Fig.3(a) shows BER performance of QNSC-based single-carrier modulation system and DFTs-OFDM based QNSC system (multi-carrier modulation system). The QPSK data are encrypted into 256×256 QAM. It is indicated by the yellow dotted line that for single-carrier system, the BER increases significantly with increasing power of the jamming signal when the power is injected with a linewidth (LW) 100kHz. When the jamming power is -1 dBm, the BER is about 0.5, which means that Bob does not get any information. As for DFTs-OFDM based QNSC system, we simulate the scenarios where the jamming signal linewidth are 0.1MHz, 1MHz, 1.5MHz, and 2MHz and the results are represented by solid lines. With these parameter configurations, the BERs change relatively stably and are less than 7% hard-decision forward error correction (HD-FEC) threshold of 3.8E-3. It can be clearly seen that the BER increases slowly with the increase of the jamming signal power. However, BER still increases with $P_{JS}$ and linewidth, as the bandwidth of guard interval in DFTs-OFDM is limited. We set 40 subcarriers in the guard interval. Besides, the gain competition and nonlinear effects in fibers still affect the transmission performance.

Fig. 3(b) indicates that a higher order of QAM can result in a higher sensitivity to jamming signal. For different order of QAM/QNSC, Eve inserts jamming signal with -10dBm to 0dBm power and 100kHz linewidth. We can see that the BER maintains below 3.8E-3 while $P_{JS}$ is less than -1dBm. Meanwhile, a higher M leads to a higher BER. The $P_{JS}$ are -0.28dBm, -0.59dBm and -0.74dBm while $M$ are 6,8,10 as 3.8E-3 BER. The result indicates that DFTs-OFDM based QNSC system has good BER performance under jamming attack with low power. Thus, DFTs-OFDM in QAM/QNSC improves the tolerance of the system to jamming attacks.

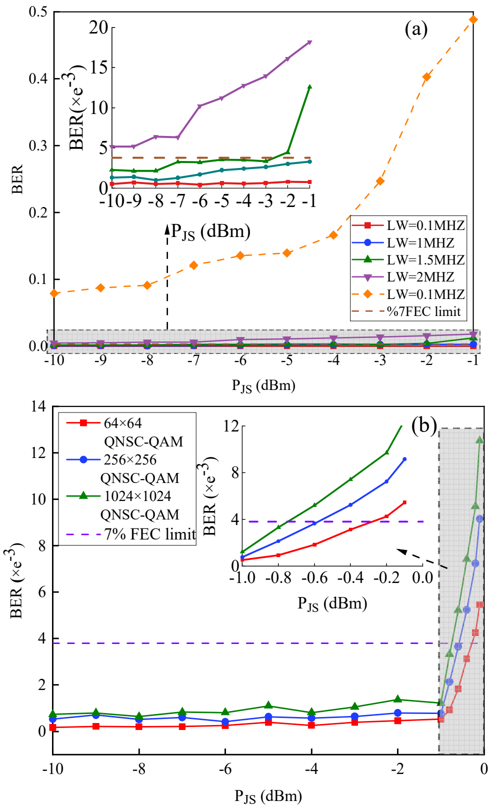

Fig. 3 BER of jamming attack with different power (a) 256×256 QAM with different LW;(b) $2^M \times 2^M$ QAM with linewidth=100kHz

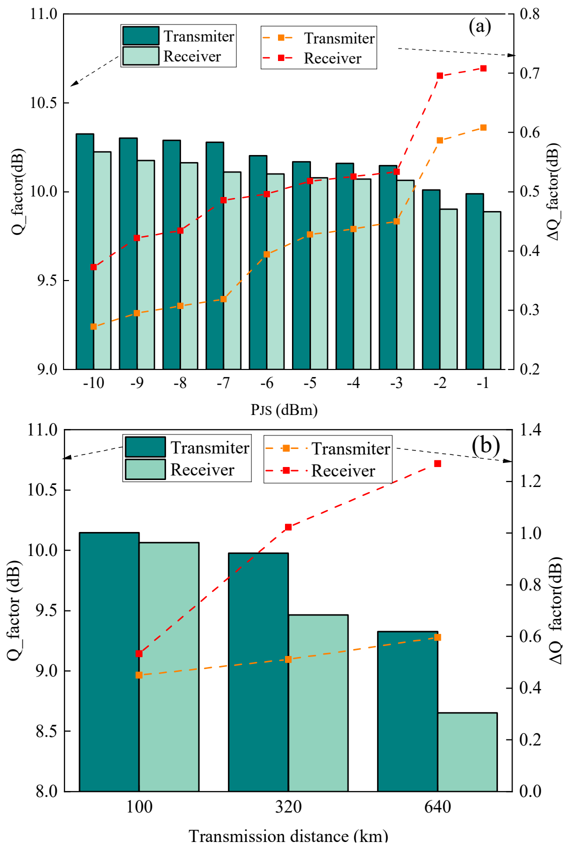

Fig. 4 Q-factor and ΔQ-factor results (a) with 100km;(b) with $P_{JS} = -3dBm$

Fig. 4 shows the variation of Q-factor of 256×256 QAM with 100kHz linewidth. In Fig. 4(a), Q-factor of the system without jamming attack is 10.6dB. It can be observed that the additional loss of the system is increased due to the additional nonlinear effects caused by the jamming signal. The loss adds 0.6 dB at the transmitter and 0.7 dB at the receiver, in which $P_{JS} = -1$ dBm. Meanwhile, the loss increases with the increase of the injected jamming signal power both at the transmitter and receiver, as shown by the red line and the yellow line in Fig. 4(a).

In order to analyze the impact of jamming signal variation with different transmission distances ( $L$ ), $L$ is set to 100 km, 320 km and 640 km respectively and $P_{JS} = -3$ dBm. The results are shown in Fig. 4(b). The Q-factor are 10.6dB, 10.49dB and 9.92dB while $L$ are 100km, 320km, 640km, respectively. It can be obtained that the additional loss caused by the jamming attack is increasing as the transmission distance increases. At the transmitter, the additional losses are 0.45dB, 0.51dB and 0.6dB respectively while $L$ are 100km, 320km and 640km, and the losses at the receiver are 0.53dB, 1.02dB and 1.27dB respectively. The jamming attack at the receiver will cause more loss to the system. This is because

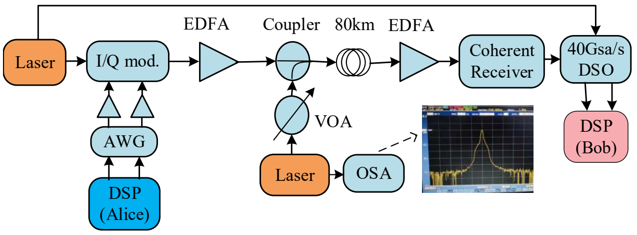

Fig. 5 Experiment setup of 10-Gbit/s QAM/QNSC with DFTs-OFDM

the signal quality decreases after the signal is transmitted through the optical fiber. According to our proposed attack, when the same attenuation is implemented at the receiver and the transmitter, the latter will cause greater loss.

## IV. Experiment Setup and Discussions

### A. Experiment setup of 10-Gbit/s QAM/QNSC with DFTs-OFDM

We experimentally demonstrate a 10-Gbaud QAM/QNSC with DFTs-OFDM digital coherent transmission with the device's parameters shown in Table.1. The experiment platform for QNSC transmission with DFTs-OFDM is shown in Fig. 5. At the transmitter, a laser with linewidth of 100 kHz and central wavelength of 1550 nm launches a signal with optical power of 10 dBm into an I/Q modulator. The transmitter-side DSP generates I and Q data. The data is uploaded to an arbitrary waveform generator (AWG). The I and Q data generated by the AWG are then amplified by two RF amplifiers (RFA) and modulated by an I/Q modulator. The generated optical signal is then amplified by an erbium-doped fiber amplifier (EDFA) to a power of 0 dBm. This signal is coupled to another laser signal by a coupler to obtain illegal signal and sent to a fiber optic link for propagation, using a standard single-mode fiber with a loss of 0.2 dB/km and a dispersion size of 17 ps/km/nm. At the receiver, the optical signal transmitted over the fiber optic link is amplified to 0 dBm by an EDFA. The state of the optical polarization is controlled using a polarization controller (PC) to obtain the desired polarization state. The same laser as the transmitter is used as the local oscillator (LO). The received optical signal is combined with the LO and detected using a coherent receiver. The detected I and Q signals are converted to digital signals by a digital signal oscilloscope (DSO).

### B. Experimental results and discussions

To analyze the performance, an experiment of QNSC with DFTs-OFDM system is conducted. Compared with the simulation setup, the experimental laser used has a constant linewidth of 100 kHz. Fig. 6(a) shows the BER of QAM/QNSC with different ciphertext space at BTB. It can be observed that the BERs increase as the order of QAM/QNSC increases. However, all can achieve the error-free condition of Bob's FEC. Meanwhile, BER shows an increasing trend as the jamming signal power increases. Fig. 6(b) shows the BER of 1024×1024 QAM with different transmission distance of 0km and 80km. For the distance of 80km, BER increases significantly with the increasing power of the jamming signal. BER will exceed 7% FEC limit as $P_{JS}$ is greater than-1.5dBm. This is different from the simulation results. This is caused by the unideal experimental conditions. For example, there are various linewidth broadening mechanisms in the actual laser, so that the laser linewidth generally cannot reach its theoretical value.

## V. Conclusions

In this work, we design an implementation of jamming attack and analyze the performance of the QNSC system under the jamming attack. Simulation results show that the multi-carrier (DFTs-OFDM) system has better performance than the single-carrier system under low-power in-band interference attack. Meanwhile, QAM/QNSC can achieve the error-free condition of HD-FEC threshold of 3.8E-3 under jamming signals with power below -2.5 dBm and linewidth less than 2000 kHz. It can be obtained that the attack at the receiver will cause more loss to the system than the transmitter. The experimental results indicate that the DFTs-OFDM-based QAM/QNSC transmission system has robustness with short transmission distance and low power of jamming signal. The system can achieve error-free transmission when the jamming power is less than -1.5dBm.

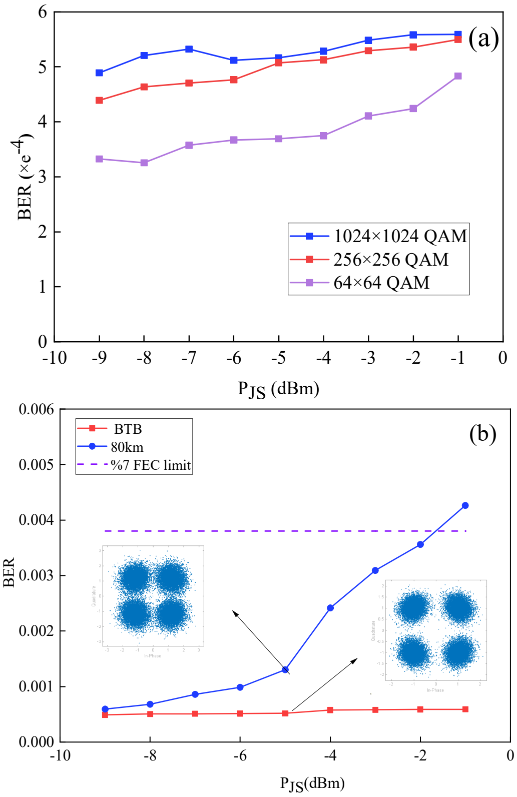

Fig.6 BER performance of (a) QAM/QNSC with different constellation size at BTB (b)1024×1024 QAM at BTB vs 80km

## Acknowledgment

This work is supported in part by NSFC (61831003, 62021005, 62101063), Beijing Natural Science Foundation (4232011), and Project of Jiangsu Engineering Research Center of Novel Optical Fiber Technology and Communication Network, Soochow University (SDGC2117).

## References

[1] N. Skorin-Kapov, et al., "Physical layer security in evolving optical networks." IEEE Commun. Mag. 54(8), 110-117, (2016).

[2] O. Hirota, et al., "Quantum stream cipher by the Yuen 2000 protocol: Design and experiment by an intensity-modulation scheme." Phys. Rev. A 72(2), 022335, (2005).

[3] Y. Chen, et al., "Security analysis of QAM quantum-noise randomized cipher system." IEEE Photonics J. 12(4), 7904114, (2020).

[4] X. Yang, et al., "DFTs-OFDM based quantum noise stream cipher system." Opt. Fiber. Technol. 52, 101939, (2019).

[5] M. Zhang, et al., "Security analysis of a QAM modulated quantum noise stream cipher under a correlation attack." Opt. Express 30(22) (2022) 40645-40656.

[6] K. Wang, J. Zhang, "The security of quantum noise stream cipher against collective attacks." Quantum Information Processing 20.7 (2021).

[7] T. Iwakoshi, "Security Evaluation of Y00 Protocol Based on Time-Translational Symmetry Under Quantum Collective Known-Plaintext Attacks," in IEEE Access, vol. 9, pp. 31608-31617, 2021.

[8] S. Chen, C. Xie and J. Zhang, "Adaptive quadrature-polybinary detection in superNyquist WDM systems." Opt. Express 23 (6) (2015) 7933–7939.