mathematics

MDPI

Article

Physical Layer Security Based on Non-Orthogonal Communication Technique with Coded FTN Signaling

Myung-Sun Baek [1] and **Hyoung-Kyu Song** [2,3,*]

[1] Department of Electrical Engineering, Sejong University, Seoul 05006, Republic of Korea; msbaek@sejong.ac.kr
[2] Department of Information and Communication Engineering, Sejong University, Seoul 05006, Republic of Korea
[3] Department of Convergence Engineering for Intelligent Drone, Sejong University, Seoul 05006, Republic of Korea
[*] Correspondence: songhk@sejong.ac.kr

Abstract: In recent years, ensuring communication security at the physical layer has become increasingly important due to the transmission of sensitive information over various networks. Traditional approaches to physical layer security often rely on artificial noise generation, which may not offer robust solutions against advanced interception techniques. This study addresses these limitations by proposing a novel security technique based on non-orthogonal signaling using Faster-than-Nyquist (FTN) signaling. Unlike conventional FTN methods that utilize fixed symbol intervals, the proposed technique employs variable symbol intervals encoded as secure information, shared only with legitimate receivers. This encoding enables effective interference cancellation and symbol detection at the receiver, while preventing eavesdroppers from deciphering transmitted signals. The performance of the proposed technique was evaluated using the DVB-S2X system, a practical digital video broadcasting standard. Simulation results demonstrated that the proposed method maintains smooth communication with minimal performance degradation compared to traditional methods. Furthermore, eavesdroppers were unable to decode the transmitted signals, confirming the enhanced security. This research presents a new approach to physical layer security that does not depend on generating artificial noise, offering a path to more secure and efficient communication systems.

Keywords: physical layer security; FTN; non-orthogonal signaling; IDD; DVB-S2X

MSC: 68W40

check for updates

Citation: Baek, M.-S.; Song, H.-K. Physical Layer Security Based on Non-Orthogonal Communication Technique with Coded FTN Signaling. *Mathematics* **2024**, *12*, 3800. https://doi.org/10.3390/math12233800

Academic Editor: Cheng-Chi Lee

Received: 20 October 2024
Revised: 21 November 2024
Accepted: 28 November 2024
Published: 30 November 2024

1. Introduction

In recent years, a huge amount of private information has been transmitted and shared through many kinds of communication and broadcasting platforms, such as the internet of things (IoT), the digital broadcast network, and the wireless sensor network (WSN) [1–4]. Because important and private information such as clinical records, bank accounts, and credit card information can be transmitted and shared over the communication network, communication security is required. Traditionally, cryptographic protocols have been researched and adopted to secure digital communication systems [5–9]. Physical layer security has recently become an emerging hot topic in digital communication and broadcasting systems [10], and various physical layer security technologies have been investigated [11–19]. Trappe briefly introduced the issues and opportunities for applying physical layer security to real systems [11], and Yener et al. provided an overview of research results in information-theoretic security [12]. However, most existing studies have used an artificial noise generation scheme to obtain physical layer security function [13–16]. Although the authors of [17,18] described some analysis and service models for physical layer security, these did not depict clear analytic and mathematical results.

Furthermore, recently, various physical layer security techniques have been investigated. The authors of [20] proposed a mixed integer linear program (MILP)-based security technique for physical layer security in elastic optical networks. The proposed technique can provide high-level encryption operation results. However, its limitation is that it is impractical for large-scale networks, due to its very high computational complexity and the fact that it requires a lot of resources. The authors of [21] proposed a method to enhance physical layer security using an intelligent reflecting surface (IRS). This technique improves security performance by using a convolutional neural network (CNN)-based model, even when the instantaneous channel information of the eavesdropper is unknown. However, applying a CNN-based algorithm requires a large amount of high-quality data, and since IRS technology is still in its early stages, this could pose a challenge to its practical implementation. The authors of [22] proposed a method based on RF fingerprint technology to enhance the security of IoT devices. The proposed technology can identify internet of things (IoT) devices with a high accuracy through RF fingerprints by utilizing a machine learning-based model. However, RF fingerprints are greatly affected by environmental conditions such as channel conditions and signal-to-noise ratio (SNR), making it difficult to operate stably. In addition, frequent environmental changes based on such uncertainties lead to the limitation that machine learning training must be performed frequently. Therefore, there are limitations in practicality.

This paper presents a novel physical layer security technique based on non-orthogonal signal processing. For the non-orthogonal signaling, Faster-than-Nyquist (FTN) signaling is considered [23,24]. FTN signaling is a communication technique that enhances spectral efficiency [25–28]. FTN signaling can simply accomplish high spectral efficiency based on a faster symbol rate than the Nyquist rate. However, because the use of a faster symbol rate than the Nyquist rate destroys the orthogonality between symbols, inter-symbol interference (ISI) is inevitably generated. To reduce the ISI and detect the transmitted symbols, the receiver should know and utilize the information about symbol rate or ISI values. In the turbo equalizer based on the Bahl, Cocke, Jelinek, and Raviv (BCJR) algorithm, the ISI filter values are used for BCJR tap coefficients in FTN signaling [29,30].

In this paper, a physical layer security technique based on FTN signaling is proposed. Unlike general FTN signaling, the proposed technique uses a different symbol interval for each transmission symbol. Therefore, each symbol has a different symbol position and interference value. Furthermore, the information about the symbol interval is shared between the transmitter and legitimate receivers. The legitimate receivers can remove the interference and detect the transmitted symbols. However, the eavesdropper cannot execute the interference cancellation operation. Furthermore, the eavesdropper cannot even find the position of each symbol. In this paper, we introduce three transmission schemes. The first scheme is symbol-wise coded FTN signaling. In this scheme, the symbol interval values are randomly generated. The number of symbol interval values is equal to the frame length of the transmitted signal, and the generated symbol interval is allocated to each symbol. The second method is block-wise coded FTN signaling. Block-wise coded FTN signaling divides a transmission frame into symbol blocks of identical length, and different symbol intervals are assigned to the respective symbol blocks. Symbols in the same block have an identical symbol interval. The third method is variable-length block-wise coded FTN signaling. The third scheme adjusts the block length according to the symbol interval of the block. In blocks with short symbol intervals, interference values are high due to the large overlapping area between adjacent symbols. Therefore, the third method assigns short block lengths to blocks with short symbol intervals and long block lengths to blocks with long symbol intervals.

For performance evaluation, the digital video broadcasting–satellite–second generation extensions (DVB-S2X) system [31] is considered. To improve the DVB-S2X system, there have been efforts to apply an FTN signaling scheme to the DVB-S2X system [32–34]. Therefore, the proposed technique is applied to the DVB-S2X system, and a performance evaluation of the designed system is carried out.

The contributions of this study are summarized as follows:

Introduction of a novel physical layer security technique: a novel security method is proposed that exploits the non-orthogonality of Faster-than-Nyquist (FTN) signals with variable symbol intervals to enable secure communication without relying on artificial noise.

Development of coded FTN signaling schemes: three innovative schemes (symbol-wise coded FTN signals, block-wise coded FTN signals, and variable-length block-wise coded FTN signals) are introduced to balance complexity, bit error rate (BER) performance, and interference management.

Application to real communication systems: the proposed technique is integrated into a DVB-S2X system to demonstrate its practical applicability and effectiveness in a real digital broadcasting environment.

The rest of this paper is organized as follows. Section 2 presents the FTN system model. Section 3 describes the proposed physical layer security techniques based on coded FTN signaling. Next, the DVB-S2X system operation with a coded FTN signaling and iterative decoding and detection (IDD) scheme is described in Section 4. The simulation results are reported in Section 5, followed by some concluding remarks in Section 6.

2. System Model with FTN Signaling

In FTN signaling, a transmission signal can be described as follows:

$$z(t) = \sum_k w_k \cdot\ f(t - k\tau\ T) \tag{1}$$

where $f(t)$ is a baseband transmit pulse, whose bandwidth is $(1+\alpha)/(2T)$ for a roll-off factor α; w_k is the k-th transmit symbol, which is one of M-QAM symbols $\mathbf{c} = [c(1), \cdots, c(m), \cdots, c(M)]$; and τ is the FTN factor which controls the symbol interval. τT is the symbol interval $(0 < \tau \leq 1)$; the symbol interval τT is shorter than or equal to the Nyquist pulse interval, T, and the pulses are not orthogonal for $\tau < 1$. In the case of $\tau = 1$, Equation (1) becomes the conventional Nyquist signaling. In addition, $f(t)$ has the unit energy, $\int_{-\infty}^{\infty} |f(t)|^2 dt = 1$. For a practical model, a root-raised cosine (RRC) pulse is considered for $f(t)$.

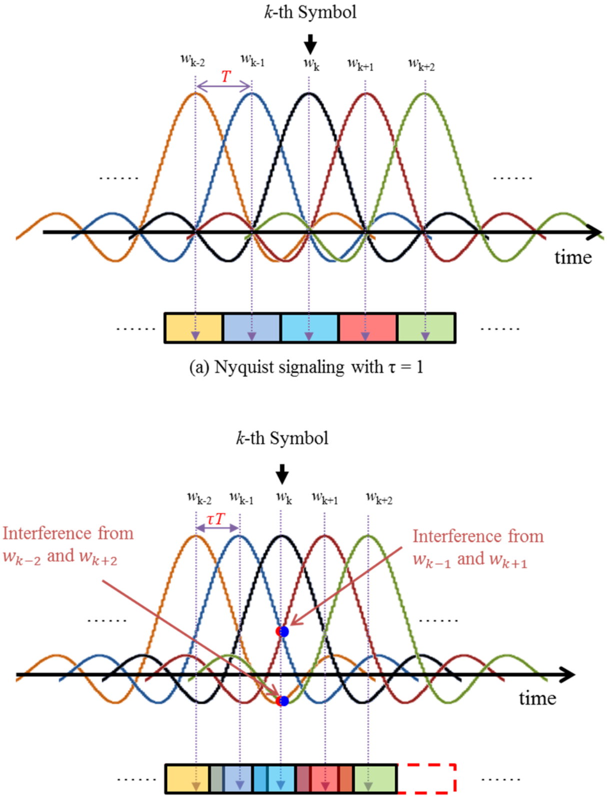
Under an additive noise channel, the matched filter output at the receiver can be written as:

$$\begin{aligned} y(t) &= r(t) * f^*(-t) \\ &= (z(t) + n(t)) * f^*(-t) \\ &= \left(\sum_k w_k \cdot\ f(t - k\tau T) \right) * f^*(-t) + \eta(t) \end{aligned} \tag{2}$$

where $\eta(t)$ is the filtered additive Gaussian noise.

Figure 1 describes the signal waveforms of general Nyquist signaling and FTN signaling, respectively. In Figure 1a, since the general symbol time is adopted, the symbols are transmitted and received without interference. However, in Figure 1b, since a faster symbol time generates interference, in the detection of the k-th symbol w_k, there are two previous and following symbols as interferences, which are $[w_{k-2}, w_{k-1}, w_{k+1}, w_{k+2}]$.

Pulse shaping filters are superimposed according to the reduced symbol interval, and the number of interference symbols and the coefficients of the superimposed pulses are determined according to the value of τ.



(a) Nyquist signaling with τ = 1

(b) FTN signaling with τ = 4/5

Figure 1. Signal wave comparison between general communication and FTN signaling.

3. Physical Layer Security Technology Based on Coded FTN Signaling

In coded FTN signaling, specific code values are allocated to the τ. Consequently, a different τ value is applied to each symbol. In this Section, three coded FTN signaling methods are introduced, considering physical layer security, complexity of signal processing, and bit error rate (BER) performance.

3.1. Symbol-Wise Coded FTN Signaling

In this symbol-wise coded FTN signaling, each symbol has a different symbol interval. Let us consider the transmission frame with K symbols (i.e., K is the length of transmission frame). In this system, the specific τ code can be written as follows:

$$\boldsymbol{\tau}_{\text{code}} = [\tau_1 \ \tau_2 \ \ \tau_3 \cdots \ \ \tau_{K-1} \ \ \tau_K] \tag{3}$$

where different values can be allocated to different τ_k such as $\tau_k = 0.8, \tau_{k+1} = 0.7$. The different τ_k value is allocated to each symbol as

$$z_{\text{code}}(t) = \sum_k w_k \cdot f\left(t - \sum_{m=0}^{k} \tau_m \cdot T\right). \tag{4}$$

The transmission signal concept comparison between general FTN signaling and coded FTN signaling with τ_{code} is described in Figure 2. Because general FTN signaling uses an identical τ value for all the transmission symbols, the ISI value for all the symbols can be easily calculated based on the one τ. By using the calculated ISI value, the interference cancellation and signal detection processes are performed. However, in coded FTN signaling, since a different τ value is used for each symbol, interference cancellation and signal detection can be accomplished when the receiver has the overall $\boldsymbol{\tau}_{\text{code}}$. Furthermore, according to the combinations of different τ values, various τ_{code} values can be generated and utilized as shown in Figure 2.

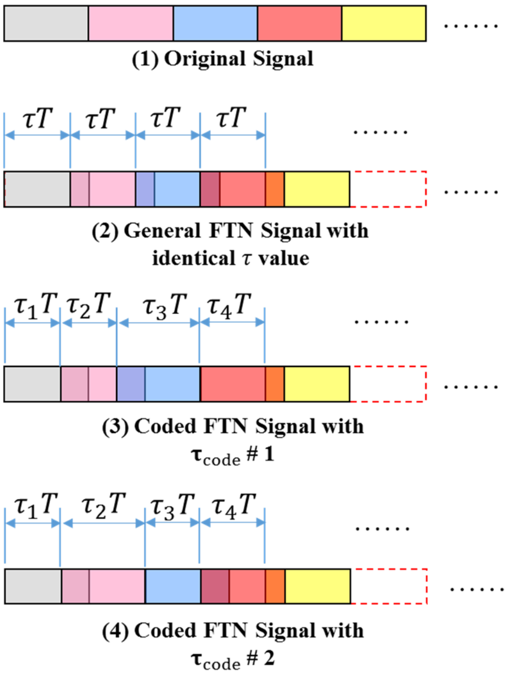

(1) Original Signal
τT τT τT τT
(2) General FTN Signal with identical τ value
$\tau_1 T$ $\tau_2 T$ $\tau_3 T$ $\tau_4 T$
(3) Coded FTN Signal with $\boldsymbol{\tau}_{\text{code}}$ # 1
$\tau_1 T$ $\tau_2 T$ $\tau_3 T$ $\tau_4 T$
(4) Coded FTN Signal with $\boldsymbol{\tau}_{\text{code}}$ # 2

Figure 2. Comparison between general FTN signaling and coded FTN signaling.

The information about the τ_{code} is released to the legitimate receivers, and the legitimate receivers then operate the interference cancellation and signal detection process based on the released τ_{code}.

3.2. Block-Wise Coded FTN Signaling

For the convenience of implementing the proposed coded FTN signaling, this subsection considers a block-wise coded FTN signaling method, where a block consists of some transmission symbols. In this block-wise coded FTN signaling, the same τ value is assigned to symbols in the same symbol block. The $\boldsymbol{\tau}_{\text{code}}$ of the block-wise coded FTN signaling is described as follows:

$$\boldsymbol{\tau}_{\text{code}} = [\boldsymbol{\tau}_{\text{blk}1}\boldsymbol{\tau}_{\text{blk}2}\boldsymbol{\tau}_{\text{blk}3}\cdots\boldsymbol{\tau}_{\text{blk}L-1}\boldsymbol{\tau}_{\text{blk}L}] \tag{5}$$

where L is the number of symbol blocks, $L = K/B$; B is the number of symbols in a symbol block; and $\boldsymbol{\tau}_{\text{blk}l}$ is the l-th τ block, which can be written as

$$\boldsymbol{\tau}_{\text{blk}l} = [\underbrace{\tau_l\tau_l\tau_l\cdots\tau_l}_{\text{length: } B}]. \tag{6}$$

In Equation (6), the l-th τ block with a length of B has an identical τ_l. Since the identical symbol time can be used for consecutive B symbols, the implementation efficiency of the coded FTN signaling can be improved. However, in symbol blocks with low τ values, all the B symbols have a short symbol time, and relatively high interference occurs continuously in the symbol block. Therefore, performance degradation occurs in symbol blocks with low τ values.

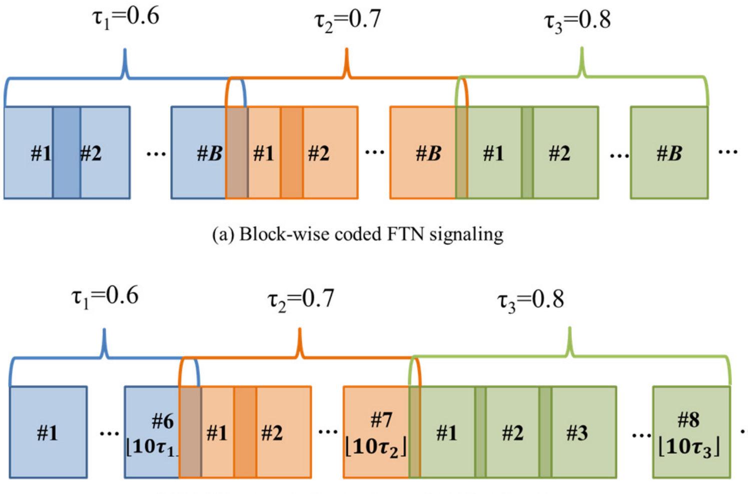
3.3. Variable-Length Block-Wise Coded FTN Signaling

This subsection considers the performance improvement method for the coded FTN signaling. As mentioned above, in block-wise coded FTN signaling, the symbol block with a low τ value degrades the overall system performance because of the continuously high ISI. To solve this problem, this scheme adjusts the symbol block length according to the τ value. To prevent high ISI being generated from a low τ value, this method assigns a short symbol block length to a symbol block with a low τ value. In the opposite case, a long symbol block length is assigned.

In this paper, the symbol block length is selected as follows:

$$B_l = \lfloor 10 \times \tau_l \rfloor \tag{7}$$

where the B_l and τ_l are the block length and τ value for the l-th block, and $\lfloor \Delta \rfloor$ is the largest integer not exceeding Δ. Therefore, in the case of $\tau_l = 0.55$, $B_l = 5$. Figure 3 shows the conceptual diagrams of the block-wise coded FTN signaling and the variable-length block-wise coded FTN signaling. In the case of block-wise coded FTN signaling, an identical block length is assigned to all symbol blocks regardless of τ value; while in Figure 3b, a different block length is assigned to each symbol block according to its τ value.



(a) Block-wise coded FTN signaling

(b) Variable-length block-wise coded FTN signaling

Figure 3. Conceptual diagram for block-wise coded FTN and variable-length block-wise coded FTN signaling.

Figure 4 shows a block/flow diagram of the proposed technique. The block/flow diagram shows the end-to-end system design for the proposed methodology, highlighting the coded FTN signaling scheme for physical layer security. The flow is divided into the following key steps: The system starts with a channel encoder to prepare the input data by adding error correction codes to ensure reliable transmission. The data are then processed by an interleaver to rearrange the data sequence in order to increase the burst error tolerance. Next, an M-ary mapper converts the encoded data into modulation symbols such as QPSK or 16-QAM for efficient transmission. Then, an oversampler using the coded FTN coefficient τ adjusts the symbol spacing to enable non-orthogonal signals. Here, the oversampling interval for each symbol is adjusted according to the coded FTN τ value, so that different τ values can be assigned to each symbol for the coded FTN. The signal is then passed through a pulse-shaping filter which is root-raised cosine (RRC). Finally, the signal is transmitted through the channel and is subject to noise and interference during transmission. At the receiver side, the signal is first processed by a matched filter (RRC) to extract the transmitted pulses. The filtered signal is downsampled using the coded τ and aligned for further processing. Then, the interference canceller removes the interference using the coded τ values shared by the legitimate transmitter and receiver. The cleaned signal is demodulated by the M-ary demapper to convert the symbols back into data bits. The bits are resequenced by the deinterleaver to restore the original order. Finally, the channel decoder recovers the original data and corrects the errors that occurred during transmission.

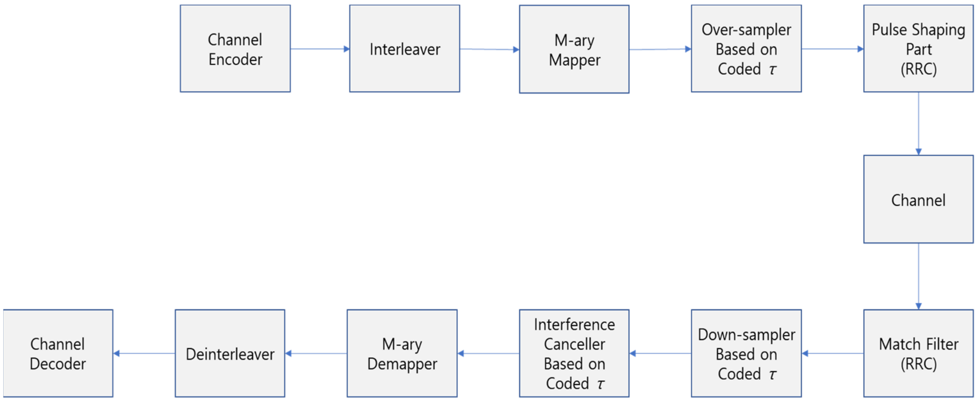


Figure 4. Block/flow diagram of the proposed technique.

4. DVB-S2X System Operation with Coded FTN Signaling and IDD

Figure 5 depicts the DVB-S2X system with the coded FTN signaling. The input data are modulated through the encoder, interleaver and modulator. The modulated data symbols are filtered by the FTN pulse-shaping filter, which uses the $\boldsymbol{\tau}_{\text{code}}$ for FTN signaling. The received signal is filtered and down converted by the matched filter. For downsampling, the symbol rate information $\boldsymbol{\tau}_{\text{code}}$ is required. For interference cancellation and signal detection, the IDD scheme is considered. In the IDD scheme, to regenerate the transmitted signal, an FTN filter is used, and the FTN filter requires information about the FTN symbol rate. Therefore, for the sampling and interference cancellation, the $\boldsymbol{\tau}_{\text{code}}$ is used in the receiver. In Figure 5, the gray dotted block represents IDD. As shown in the figure, the signal decoded through the low-density parity check (LDPC) decoder is remodulated, and FTN signaling is applied to regenerate the transmission signal. After that, the error value between the regenerated FTN signal and the remodulated signal is calculated, and then removed from the received signal iteratively.

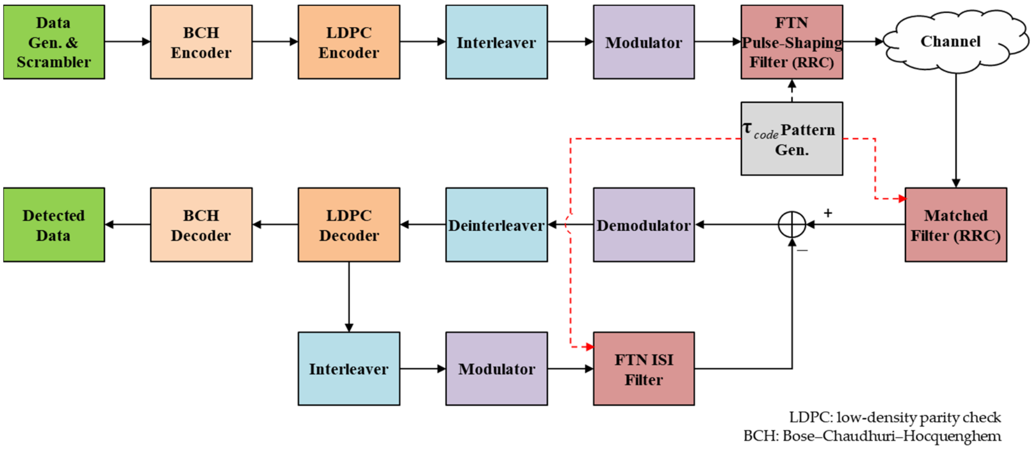


Figure 5. DVB-S2X System with Coded FTN signaling.

As shown in Equation (4), the transmitted physical layer security signal z_{code} is received after additive noise, and filtered by the matched filter. After the log-likelihood ratio (LLR) of the received signal is calculated, the deinterleaver and LDPC decoder are operated. Then, the regeneration process of the decoded signal is executed. In the signal modulation process of the transmitter, the decoded information is interleaved and modulated. The coded FTN signal is regenerated by using the coded FTN, filtering with the $\boldsymbol{\tau}_{\text{code}}$, as follows:

$$\hat{y}(t) = \left(\sum_k \hat{w}_k \cdot f\left(t - \sum_{m=0}^{k} \tau_m T \right) \right) * f^*(-t) \tag{8}$$

where $\hat{w}_k$ is the k-th remodulated symbol. The interference value sampled at k-th time is calculated by using the regenerated coded FTN signal $\hat{y}_k$ and the remodulated signal $\hat{w}_k$, as follows:

$$e_k = \hat{y}_k - \hat{w}_k \tag{9}$$

In the second iterative process, the interference value e_k is removed from the received signal as follows:

$$\widetilde{y}_k = y_k - e_k \tag{10}$$

where y_k is the received signal sampled at k-th time. After the interference cancellation, the identical demodulation/ decoding and interference calculation processes are operated.

The IDD process is repeated up to a predetermined repetition number in consideration of the detection performance and the processing time.

5. Experimental Design and Performance Evaluation

5.1. Experimental Design

This subsection covers the experimental design to evaluate the performance of the proposed coded FTN signal. The simulations were performed using a DVB-S2X system with the following configuration:

LDPC code parameters: an LDPC code length of 64,800 bits with a code rate of 2/3 was used.

Baseband modulation: two modulation schemes were considered, namely, Quadrature Phase Shift Keying (QPSK) and 16-Quadrature Amplitude Modulation (16-QAM).

Pulse shaping: Root Raised Cosine (RRC) pulses with a roll-off factor of 0.35 were applied, as specified in the DVB-S2X standard [31].

Symbol interval parameter ($\boldsymbol{\tau}_{\text{code}}$): for all three of the coded FTN signal techniques, the τ values were randomly generated in the range of 0.5 to 1, with an interval of 0.05.

The average τ value (E[$\boldsymbol{\tau}_{\text{code}}$]) in the symbol-wise coded FTN signal was set to 0.75. Block lengths (B) of 3, 5, and 10 symbols were evaluated in the block-wise coded FTN signal, and the average τ value was also set to 0.75.

For the variable-length block-wise coded FTN signal, the block length was dynamically determined based on the τ value using Equation (7).

Comparison Benchmarks: the performance was compared with a regular FTN signal system [31] with a fixed τ value of 0.75. The performance of a conventional DVB-S2X system without an FTN signal was also included for reference.

Eavesdropping Mode: to evaluate the security, an eavesdropping mode was simulated, where the receiver attempted to decode the coded FTN signal using a regular FTN receiver with τ = 0.75.

Table 1 describes the parameters for the experimental design. The parameters this paper chose are the commonly used parameters in DVB-S2X systems.

Table 1. Parameters for the experimental design.

Parameter	Value/Description
LDPC Code Length	64,800 bits
LDPC Code Rate	2/3
Baseband Modulation	QPSK, 16-QAM
Pulse Shape	RRC with 0.35 roll-off factor
τ Range	0.5 to 1 (0.05 intervals)
Conventional DVB-S2X	Without FTN signaling
Eavesdropper Configuration	General FTN receiver with τ = 0.75

5.2. Performance Evaluation

Figures 6 and 7 describe the performance of the DVB-S2X system with symbol-wise and block-wise coded FTN signaling schemes, according to the baseband modulation. Figure 6 shows the BER performances of the DVB-S2X systems with 16-QAM. In Figure 6, the performance of the symbol-wise coded FTN signaling is about 0.3–0.6 dB better than that of the block-wise coded FTN signaling at BER = 10^{-5}. However, in the case of the symbol-wise coded FTN signaling, since the symbol interval should be changed at every symbol time, the implementation complexity becomes high. For the block-wise coded FTN signaling, because the symbol interval is fixed for the block length, a simpler implementation is possible. However, in the case of symbol blocks with a low $\boldsymbol{\tau}_{\text{blk}l}$ value, high interference causes performance degradation. Therefore, in the case of B = 10, although the symbol interval can be fixed for ten symbols, the performance is the worst, because of high ISI. In the block-wise coded FTN signaling, since the symbols with low τ values can be successively transmitted, the performance degradation value is higher. However, both symbol-wise coded FTN signaling and block-wise coded FTN signaling show smooth operation without serious problems such as error floor, excessive performance degradation, and so on. From the simulation results, it can be shown that the eavesdropper mode cannot demodulate and decode the signal transmitted from the coded FTN signaling system. In Figure 7, the BER performances of QPSK modulation are described. Compared with 16-QAM, the performance degradation of block-wise coded FTN signaling is lower, since the QPSK is more reliable from an ISI standpoint than the 16-QAM. However, the BER performance tendency is similar in that the longer the block length, the worse the BER performance.

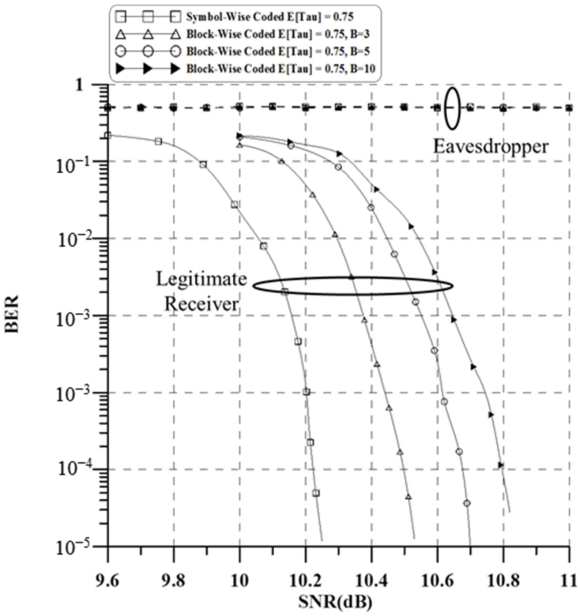


Figure 6. BER performances of symbol-wise coded FTN signaling and block-wise coded FTN signaling in DVB-S2X system with 16-QAM.

Figures 8 and 9 depict the BER performance of the variable-length block-wise coded FTN signaling. For a performance comparison, the DVB-S2 system with a general FTN signaling of $\tau = 0.75$ is inserted. Furthermore, the performance of the conventional DVB-S2 without FTN signaling is also added. Figure 8 shows the BER performance of 16-QAM. The performance of general FTN signaling with $\tau = 0.75$ is about 0.7 dB worse than that of the conventional DVB-S2X system at BER = 10^{-5}. However, in the ideal case, an efficiency gain of more than 30% can be achieved using FTN signaling with τ = 0.75 compared to regular Nyquist signaling. For the coded FTN signaling, compared to regular FTN signaling with τ = 0.75, the performance degradation of the symbol-wise coded FTN signaling is about 0.6 dB, while the performance degradation of the variable-length block-wise coded FTN signaling is about 0.4 dB. Since the variable-length block-wise coded FTN signaling adjusts the block length according to the τ value, the generation probability of a low τ value is lower than that of the symbol-wise coded FTN signaling. In the variable-length block-wise coded FTN signaling, the average τ value of the transmission signaling is about 0.785 (i.e., $E[\tau] = 0.785$). Therefore, by using variable-length block-wise coded FTN signaling, the performance of the coded FTN signaling is improved. Figure 9 shows the BER performances of the QPSK modulation. The performance tendency of the QPSK modulation is similar to that of the 16-QAM, shown in Figure 9. However, for the 16-QAM, the performance of the symbol-wise coded FTN system is about 1.6 dB worse than the typical 16-QAM performance, and for the QPSK, the performance of the symbol-wise coded FTN is only about 0.8 dB worse than the typical QPSK performance. Therefore, the performance degradation values of the QPSK with coded FTN signaling are lower than that of the 16-QAM.

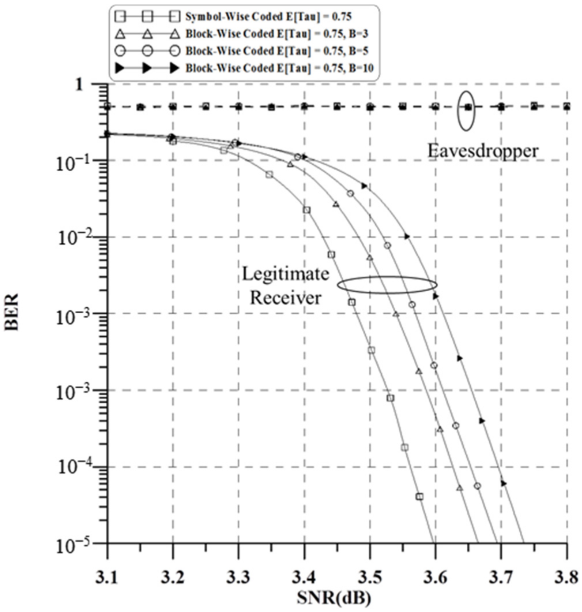


Figure 7. BER performances of symbol-wise coded FTN signaling and block-wise coded FTN signaling in DVB-S2X system with QPSK.

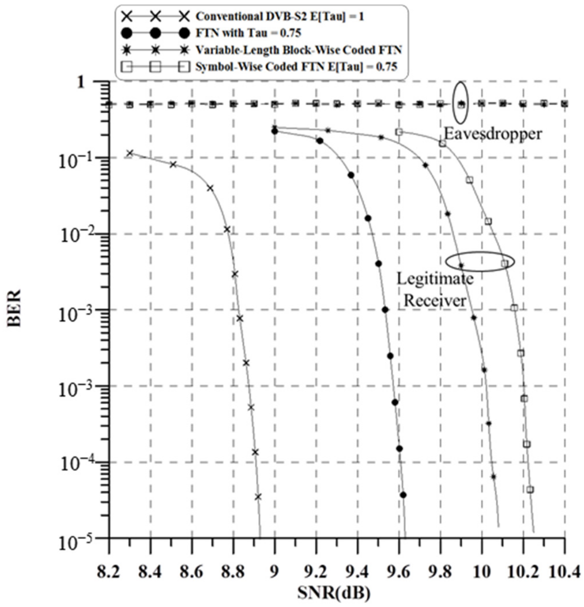


Figure 8. BER performance of variable-length block-wise coded FTN signaling in DVB-S2X system with 16-QAM.

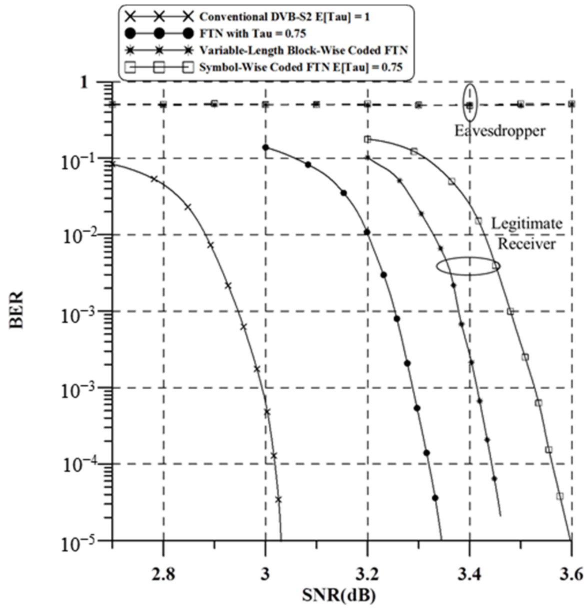


Figure 9. BER performance of variable-length block-wise coded FTN signaling in DVB-S2X system with QPSK.

In addition to the BER vs. SNR analysis, the Peak-to-Average Power Ratio (PAPR) was evaluated for different τ values in the FTN system with the 16-QAM modulation. Figure 10 illustrates the PAPR performance across various τ values (τ = 1, 0.875, 0.75, 0.625, 0.5). The results indicate that as the τ value decreases, the PAPR increases due to enhanced ISI. For τ = 1, which corresponds to the Nyquist signaling condition, the PAPR is minimal. However, when τ is reduced to 0.5, a significant increase in PAPR is observed, highlighting the trade-off between spectral efficiency and power efficiency in FTN signaling.

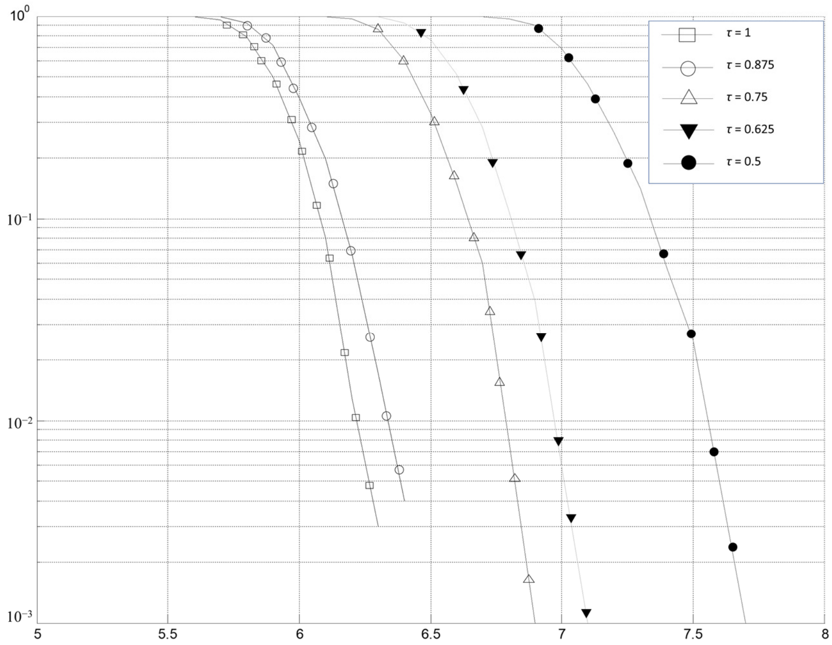


Figure 10. PAPR performance of DVB-S2 system with 16QAM according to τ values.

The state-of-the-art method described in the referenced paper [21] evaluates performance primarily through the secrecy outage probability (SOP) metric, while the proposed technique in our manuscript is evaluated using the BER. This difference in performance metrics makes a direct comparison challenging. However, it is noteworthy that the BER performance of our proposed technique remains highly stable, achieving exceptionally low values as the SNR increases. In contrast, the secrecy outage probability of the state-of-the-art method does not decrease significantly below 0.1, even with an increase in SNR. These results indicate that our proposed technique demonstrates stable performance in terms of reliability and robustness.

6. Conclusions

This paper proposed coded FTN signaling for physical layer security. To improve the implementation efficiency and BER performance, three coded FTN signaling techniques were proposed, and the BER performances of the three techniques were evaluated according to the baseband modulation schemes. From the simulation results, the proposed scheme can accomplish physical layer security without significant degradation and problems. In addition, it was checked that the eavesdropper could not detect and demodulate the transmitted signal with coded FTN signaling in all three of the proposed techniques. Furthermore, because the performance evaluation of the proposed technique was executed using a practical DVB-S2X system, the reliable operation of the proposed technique was efficiently shown. Unlike existing physical layer security techniques with artificial noise generation, since the proposed technique uses non-orthogonality of FTN signaling, a novel methodology is suggested with the proposed technique.

Author Contributions: Conceptualization, M.-S.B.; methodology, M.-S.B.; software, M.-S.B.; validation, M.-S.B. and H.-K.S.; formal analysis, M.-S.B. and H.-K.S.; investigation, M.-S.B. and H.-K.S.; resources, H.-K.S.; data curation, M.-S.B.; writing—original draft preparation, M.-S.B. and H.-K.S.; writing—review and editing, M.-S.B. and H.-K.S.; visualization, M.-S.B.; supervision, H.-K.S.; project administration, H.-K.S.; funding acquisition, H.-K.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Institute of Information and Communications Technology Planning and Evaluation (IITP) grant funded by Korea Government [Ministry of Science and ICT (MSIT)], South Korea, under the Metaverse Support Program to Nurture the Best Talents under Grant IITP-2024-RS-2023-00254529; in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2020R1A6A1A03038540; and in part by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-RS-2024-00438007) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

Data Availability Statement: The data will be made available by the authors upon request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Altowaijri, S.M. Deduplication-Aware Healthcare Data Distribution in IoMT. *Mathematics* **2024**, *12*, 2482. [CrossRef]
2. Blessy, J.J.; Jaison, B.; Nareshkumar, M.D. Nano Functionalized Antenna Based IoT Enabled Devices for Health Care Applications. In Proceedings of the 2024 First International Conference on Electronics, Communication and Signal Processing (ICECSP), New Delhi, India, 8–10 August 2024; pp. 1–6. [CrossRef]
3. He, X.; Gong, Y.; Huang, L.; Wang, J. *Linear Complexity Holographic Beamforming For Satellite Broadcasting*; IEEE Transactions on Vehicular Technology: Piscataway, NJ, USA, 2024. [CrossRef]
4. Kumar, A.; Jadhav, S.; Alsalami, O.M. Reliability and Sensitivity Analysis of Wireless Sensor Network Using a Continuous-Time Markov Process. *Mathematics* **2024**, *12*, 3057. [CrossRef]
5. Ahmed, A.A.; Malebary, S.J.; Ali, W.; Alzahrani, A.A. A Provable Secure Cybersecurity Mechanism Based on Combination of Lightweight Cryptography and Authentication for Internet of Things. *Mathematics* **2023**, *11*, 220. [CrossRef]
6. Khalifa, O.O.; Islam, M.D.R.; Khan, S.; Shebani, M.S. Communications cryptography. In Proceedings of the IEEE RFM, Selangor, Malaysia, 5-6 October 2004; pp. 220–223.
7. Anatoly, S.; Emil, F.; Olha, L. Three-Pass Cryptographic Protocol Based on Permutations. In Proceedings of the 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 25–27 November 2020; pp. 281–284. [CrossRef]
8. Lansky, J.; Sadrishojaei, M.; Rahmani, A.M.; Malik, M.H.; Kazemian, F.; Hosseinzadeh, M. Development of a Lightweight Centralized Authentication Mechanism for the Internet of Things Driven by Fog. *Mathematics* **2022**, *10*, 4166. [CrossRef]

9. Manal, R.; Tomader, M. Cryptographic methods for eHealth cloud applications using Iot based 5G: Comparison study. In Proceedings of the 2022 5th International Conference on Networking, Information Systems and Security: Envisage Intelligent Systems in 5g//6G-based Interconnected Digital Worlds (NISS), Bandung, Indonesia, 30–31 March 2022; pp. 1–5. [CrossRef]
10. Hoseini, S.A.; Bouhafs, F.; den Hartog, F. A Practical Implementation of Physical Layer Security in Wireless Networks. In Proceedings of the 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2022; pp. 1–4. [CrossRef]
11. Trappe, W. The challenges facing physical layer security. *IEEE Comm. Mag.* **2015**, *53*, 16–20. [CrossRef]
12. Yener, A.; Ulukus, S. Wireless physical-layer security: Lessons learned from information theory. *Proc. IEEE* **2015**, *103*, 1814–1825. [CrossRef]
13. Salem, A.; Hamid, K.A.; Alsusa, A.E. Physical layer security over correlated log-normal cooperative power line communication channels. *IEEE Access* **2017**, *5*, 13909–13921. [CrossRef]
14. Zhang, L.; Zhang, H.; Wu, D.; Yuan, D. Improving physical layer security for MMISP systems via using artifical noise. In Proceedings of the GLOBECOM, San Diego, CA, USA, 6 December 2015; pp. 1–6.
15. Zou, Y.; Zhu, J.; Wang, X.; Leung, V.C.M. Improving physical-layer security in wireless communications using diversity techniques. *IEEE Network* **2015**, *29*, 42–48. [CrossRef]
16. Hyadi, A.; Rezki, Z.; Alouini, M.-S. An overview of phsical layer security in wireless communication systems with CSIT uncertainty. *IEEE Access* **2016**, *4*, 6121–6132. [CrossRef]
17. Cuman, K.; Xing, H.; Xu, P.; Zheng, G.; Dai, X.; Nallanathan, A.; Ding, Z.; Karagiannidis, G.K. Phsical layer security jamming: Theoretical litits and parctical designs in wireless networks. *IEEE Access* **2017**, *5*, 3603–3611. [CrossRef]
18. Torres-Figueroa, L.; Hörmann, M.; Wiese, M.; Mönich, U.J.; Boche, H.; Holschke, O.; Geitz, M. Implementation of Physical Layer Security into 5G NR Systems and E2E Latency Assessment. In Proceedings of the GLOBECOM 2022—2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 4–8 December 2022; pp. 4044–4050. [CrossRef]
19. Boodai, J.; Alqahtani, A.; Frikha, M. Review of Physical Layer Security in 5G Wireless Networks. *Appl. Sci.* **2023**, *13*, 7277. [CrossRef]
20. Savva, G.; Manousakis, K.; Ellinas, G. A Network Coding Optimization Approach for Physical Layer Security in Elastic Optical Networks. *IEEE Trans. Netw. Serv. Manag.* **2024**. [CrossRef]
21. Liu, Y.; Su, Z.; Peng, H.; Luo, X.; Chen, H.-H. Intelligent Reflecting Surface Assisted Physical Layer Security: A Deep Learning Approach. *IEEE Wirel. Commun.* **2024**, *31*, 52–60. [CrossRef]
22. Traynor, Z.A.; Curtin, I.M.; Henggeler, C.T.; Sulyman, A.I. Physical-layer security solutions for IoT devices using Radio Frequency Fingerprints. In Proceedings of the 2024 International Conference on Computing, Internet of Things and Microwave Systems (ICCIMS), Gatineau, QC, Canada, 14 June 2024; pp. 1–4. [CrossRef]
23. Reznev, A. Faster-than-Nyquist Signals for Modern Communication Systems. In Proceedings of the 2024 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Vyborg, Russian, 1–3 July 2024; pp. 1–4. [CrossRef]
24. Baek, S.; Jung, E.-S.; Park, Y.S.; Lee, Y.-T. FTN-Based Non-Orthogonal Signal Detection Technique With Machine Learning in Quasi-Static Multipath Channel. *IEEE Trans. Broadcast.* **2024**, *70*, 78–86. [CrossRef]
25. Matsuyama, T.; Suzuki, T.; Saito, S.; Suganuma, H.; Maehara, F. Throughput Improvement through FTN-based MIMO Signaling in Fixed Wireless Access. In Proceedings of the 2023 11th International Japan-Africa Conference on Electronics, Communications, and Computations (JAC-ECC), Alexandria, Egypt, 18–20 December 2023; pp. 79–82. [CrossRef]
26. Abbasi, S.; Bedeer, E. Low Complexity Classification Approach for Faster-Than-Nyquist (FTN) Signaling Detection. *IEEE Commun. Lett.* **2023**, *27*, 876–880. [CrossRef]
27. Kaekhtin, I.; Zavjalov, S.; Kudryashova, T.; Sinepol, V.; Polozhintsev, B.; Zhabko, G.; Nguyen, D.C. Efficiency of Coherent Processing Algorithms for FTN Signals. In Proceedings of the 2023 International Conference on Electrical Engineering and Photonics (EExPolytech), St Petersburg, Russia, 19–20 October 2023; pp. 214–217. [CrossRef]
28. Baek, M.-S.; Yun, J.; Kwak, S.; Lim, H.; Kim, Y.; Hur, N. Physical layer security based on coded FTN signaling for premium services in satellite digital broadcasting system. In Proceedings of the 2017 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 3–6 September 2017; pp. 147–148. [CrossRef]
29. Che, H.; Bai, Y. M-BCJR algorithm with channel shortening based on ungerboeck observation model for faster-than-Nyquist signaling. *China Commun.* **2021**, *18*, 88–98. [CrossRef]
30. Matar, M.O.; Jana, M.; Mitra, J.; Lampe, L.; Lis, M. A Turbo Maximum-a-Posteriori Equalizer for Faster-than-Nyquist Applications. In Proceedings of the 2020 IEEE 28th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM), Fayetteville, AR, USA, 3–6 May 2020; pp. 167–171. [CrossRef]
31. *ETSI EN 302 307-2 v1.4.1*; Digital Video Broadcasting (DVB); Second Generation Framing structure, Channel Coding and Modulation Systems for Broadcasting, Interactive Services, News Gathering and Other Broadband Satellite Applications; Part 2: DVB-S2 Extensions (DVBS2X). ETSI: Sophia Antipolis, France, 2024.
32. Shang, W.; Lavrenyuk, I.; Makarov, S.; Ovsyannikova, A.; Zavjalov, S.; Yu, D.; Xue, W. Energy Efficiency for Faster-than-Nyquist Data Transmission Using Processing Algorithms with Decision Feedback. *Symmetry* **2024**, *16*, 1001. [CrossRef]

33. Makarov, S.B.; Liu, M.; Ovsyannikova, A.S.; Zavjalov, S.V.; Lavrenyuk, I.; Xue, W.; Xu, Y. A Reduction of Peak-to-Average Power Ratio Based Faster-Than-Nyquist Quadrature Signals for Satellite Communication. *Symmetry* **2021**, *13*, 346. [CrossRef]
34. Li, Q.; Gong, F.-K.; Song, P.-Y.; Li, G.; Zhai, S.-H. Beyond DVB-S2X: Faster-Than-Nyquist Signaling With Linear Precoding. *IEEE Trans. Broadcast.* **2020**, *66*, 620–629. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.