

II INTERNATIONAL SCIENTIFIC CONVENTION  
“II ICC UCLV 2019”

JUNE 23<sup>th</sup> – 30<sup>th</sup>, 2019  
CAYOS DE VILLA CLARA. CUBA.



IoT- AI WORKSHOP 2019

**Performance improvement for a physical-layer-security technology  
based on FTN Signaling on DVB-S2**

**Julio C. Pérez García<sup>1</sup>, Erik Ortiz Guerra<sup>2</sup>, Daniel D. Iglesias de la Torre<sup>3</sup>**

1- Julio C. Pérez García. UCLV, Cuba, e-mail address: [juliocpg@uclv.cu](mailto:juliocpg@uclv.cu)

2- Erik Ortiz Guerra. UCLV, Cuba, e-mail address: [erik@uclv.edu.cu](mailto:erik@uclv.edu.cu)

3- Daniel D. Iglesias de la Torre. UCLV, Cuba, e-mail address: [danielit@uclv.cu](mailto:danielit@uclv.cu)

**Abstract:** The expansion of devices and technologies for Internet of Things (IoT) applications brings with its great challenges to ensure secure communications. Traditional cryptographic systems cannot be applied directly on constricted devices. Physical layer security mechanisms attract increasing attention, which could be implemented in parallel with higher layer methods. FTN (faster-than-Nyquist) signaling is a promising technology to improve transmission speed without increasing bandwidth, but introduce inter-symbol interference (ISI). FTN signaling can be used as a form of artificial noise to achieve security in the physical layer. The ISI that is introduced due to FTN signaling can be reversed to some degree by the receiver, but cannot be completely removed, causing a degradation in the bit error ratio (BER). In this paper we propose to adjust the value of the roll-off factor of the pulse shaping filter in each symbol, exploiting the gain in terms of spectral efficiency caused by the FTN signal in order to improve performance in terms of BER. The results show that the proposed scheme can significantly improve the performance in terms of BER. Guaranteeing, in coexistence with other security mechanisms and despite the presence of potential eavesdroppers, a reliable and secure flow of information on DVB-S2 scenarios.

**Keywords:** Physical layer security; Faster-than-Nyquist signaling; inter-symbol interference; bit error ratio.

**II INTERNATIONAL SCIENTIFIC CONVENTION  
“II ICC UCLV 2019”**

**JUNE 23<sup>th</sup> – 30<sup>th</sup>, 2019  
CAYOS DE VILLA CLARA. CUBA.**



## **1. Introduction**

Internet-of-Things (IoT) aims to provide connectivity for thousands of devices, anywhere, with anything and at any time possible. In most IoT applications, the security of communication is an essential requirement. Security protocols must be implemented in a highly efficient way due to the power and processing constraints which characterizes many IoT devices. Existing standard protocols for security protection cannot be directly applied in the very constrained devices. Consequently, there is an increasing need for secure communication solutions [1].

The design of the secure physical layer attracts increasing attention [1-3]. The physical layer security (PLS) has the potential to enable secret communication and reliable authentication, as well as to avoid computational complexity. These techniques are designed to enhance security against eavesdropping attacks. The original approach is to exploit the random nature of the wireless channel. In [4] it was shown that it is possible to establish a secure transmission, if the eavesdropper observes a degraded version of the channel between the legitimate source and the receiver.

Some authors in [5, 6] propose methods to achieve PLS by using artificial noise. The idea of artificial noise is to affects the eavesdropper more than legitimate receivers with noise or interference. Recent works [2, 3], consider degrading the channel by introducing controlled inter-symbols interference (ISI) in a way that it can be reversed in the intended receiver. In this case, the common approach is to violate the Nyquist ISI criterion by using faster-than-Nyquist (FTN) signaling.

Authors in [2], propose a physical layer security technique based on FTN signaling for the Premium service of DVB-S2 [7]. The proposed technique allocates different symbol interval to each symbol. The authorized receivers can decode the coded FTN signal by using the symbol interval pattern information. However, it is very hard for the receivers without symbol interval pattern to decode the transmitted coded FTN signal [2].

FTN signaling improves the transmission rate, without fulfilling the Nyquist criterion for transmissions without ISI, while not increase the bandwidth [8, 9]. However, due faster symbol rate destroys the orthogonality between symbols, it necessarily generates ISI,

**II INTERNATIONAL SCIENTIFIC CONVENTION  
“II ICC UCLV 2019”**

**JUNE 23<sup>th</sup> – 30<sup>th</sup>, 2019  
CAYOS DE VILLA CLARA. CUBA.**



which degrades transmission performance. To reduce the ISI and detect the transmitted symbols, the receiver should know and utilize the information about symbol rate or ISI factor [5].

The ISI that is introduced due to FTN signaling can be reversed to some degree by the receiver, but cannot be completely removed, causing a degradation in the bit error ratio (BER), which affects the system performance. A portion of the spectral efficiency gain due to FTN signaling could be used to improve bit error ratio (BER). One way to do this is to increase the roll-off factor of the pulse shaping filter in symbols with shorter duration [3].

In this paper we propose to adjust the value of the roll-off factor of the pulse shaping filter in each symbol, in a way that maintains the spectral efficiency constant. Employing a fraction of the spectral efficiency gain obtained from using FTN signaling to improve performance in terms of BER. Simulations are conducted to demonstrate that by adjusting the roll-off factor for each symbol, the performance in the system channel is improved in terms of BER for a legitimate receiver, and the security metrics are not degraded.

## **2. System Model**

For linear modulated digital systems, the transmitted signal can be represented as:

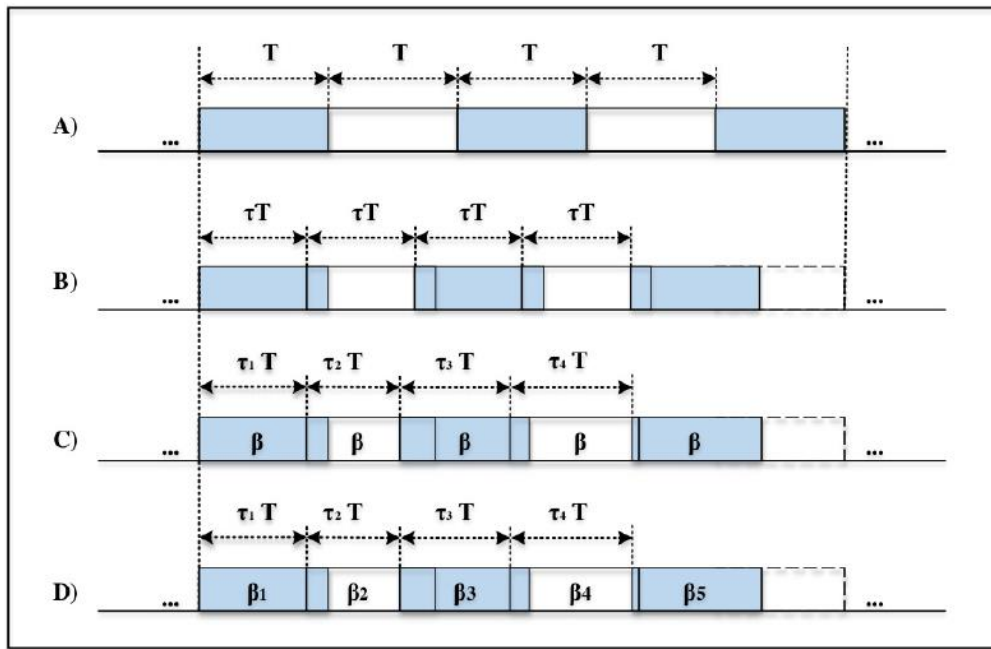
$$s(t) = \sqrt{\tau E_s} \sum_{i=-\infty}^{\infty} x[n] * g(t - n\tau T), \quad (1)$$

Where  $n$  is the index of the time slot,  $x[n]$  is the data symbol transmitted in time slot  $n$ ,  $E$  is the energy of the data stream,  $\tau$  is the factor of compression in time such that:

$0 < \tau \leq 1$ , notice that  $\tau T$  is the symbol interval. The factor  $\sqrt{\tau}$ , keeps the transmission power constant. In the full text, pulse shaping filter is assumed having unit energy. A root-raised cosine (RRC) pulse is considered for  $g(t)$ . In what follows, we assume that the pulse shaping filter is RRC, which is widely used in FTN systems. As shown in [10], as the value of the roll-off factor is increased, the impulse response it is rapidly damped, contributing to weakened the ISI.

Fig. 1A represents the Nyquist signaling, where a train of orthogonal pulses are transmitted. Fig. 1B show a traditional FTN signaling with a fixed factor of compression

( $\tau$ ). In FTN systems,  $\tau < 1$  which allows sending more symbols per unit of time, which improves bandwidth utilization but causing pulse time overlap (ISI). Signal represented in Fig. 1C was proposed in [2] to achieve PLS, where each symbol is transmitted with different factor of compression and a fixed roll-off factor value ( $\beta$ ). In the bottom illustration, Fig. 1D, and are dynamically modified to add artificial noise.



**Fig. 1.** Signal model. A) Nyquist Signaling. B) Traditional FTM Signaling. C) Signaling proposed in [2]. D) Proposed modification.

For each pulse the acceleration factor,  $\tau_i$ , is randomly selected from a suitable interval according to a predefined distribution, constituting the secret pattern. In practice, this pattern can be obtained from a pseudo-random generator, initialized with a common seed shared by the transmitter and the receiver. The selection process of the roll off factor of each symbol is described in next section.

## 2.1 Roll-off factor selection

In this section we describe the process of selecting the value of the roll-off factor, ( $\beta$ ), for each symbol. For the proposed scheme, the  $\beta$  is increased in the symbols that have a higher  $\tau$  value, so that the spectral efficiency does not fall below a given value. The

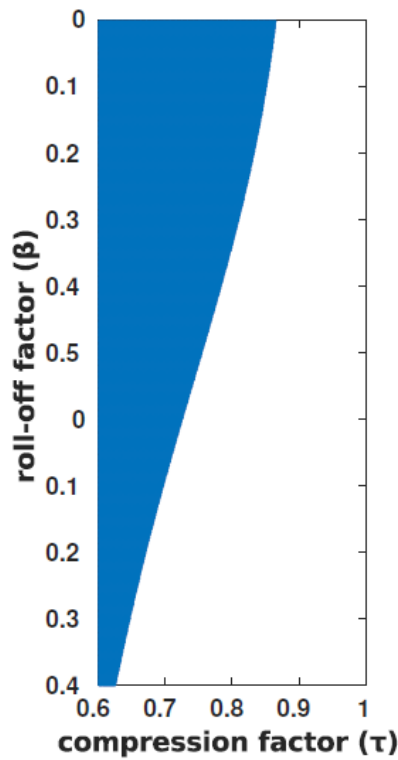
**II INTERNATIONAL SCIENTIFIC CONVENTION  
“II ICC UCLV 2019”**

**JUNE 23<sup>th</sup> – 30<sup>th</sup>, 2019  
CAYOS DE VILLA CLARA. CUBA.**



minimum roll-off factor, ( $\beta_{min}$ ) that does not produce errors caused by the ISI is determined by simulation and the maximum value ( $\beta_H$ ) for a given spectral efficiency is obtained analytically. These results allow to guarantee that the value of the chosen  $\beta$  does not cause errors because of the ISI and does not affect spectral efficiency either.

The simulation of the  $10^7$  bits transmission is performed to determine  $\beta_{min}$ . Values of  $\tau$  are selected in the interval  $[0.6; 1]$  with increments of 0.01 and values of the  $\beta$  are varied in the interval  $[0; 0.5]$  with increments of 0.01. Fig. 2 shows a region (colored in blue) for which some bit error occurs in the transmission due to the ISI. With Fig. 2 it is possible to determinate  $\beta_{min}$  for a given  $\tau$  by interpolation with the border of the error region.



**Fig. 2.** Error region for noiseless uncoded FTN.

On the other hand, equation 2 is used to derive spectral efficiency, ( $\eta$ ), in coded communication systems [11].

$$\eta = \frac{\frac{k}{n} \cdot \frac{1}{\tau}}{\frac{1+\beta}{2T}} = \frac{2T \cdot \frac{k}{n}}{\tau(1+\beta)} \quad (2)$$

In equation 2,  $R$  is the transmission ratio,  $W$  is the system bandwidth,  $\frac{k}{n}$  is the code rate and  $T$  is the Nyquist symbol interval. With equation 3, we derive the value of  $\beta_H$  for a given spectral efficiency.

$$\beta_H = \frac{2T \cdot \frac{k}{n}}{\tau\eta} - 1 \quad (3)$$

The value of the selected roll-off factor for each symbol is determined as the average of  $\beta_H$  and  $\beta_{min}$  if this value does not affect the spectral efficiency. Equation 4 shows how to determine that value.

$$\beta = \begin{cases} \beta_{min}, & \beta_{min} < \beta_H \\ \min \left\{ \left( \frac{\beta_H - \beta_{min}}{2} \right), 1 \right\}, & \text{otherwise} \end{cases} \quad (4)$$

### 3. Numerical Results

The comparison between using the technique proposed in [2], and our proposal is shown in the following. Fig. 3 depicts the DVB-S2 system with coded FTN signaling used to develop the comparison. For baseband modulation an optimal binary scheme BPSK is considered. Channel coding is performed using a BCH code (32400; 32208) and LDPC code (64800; 32400).

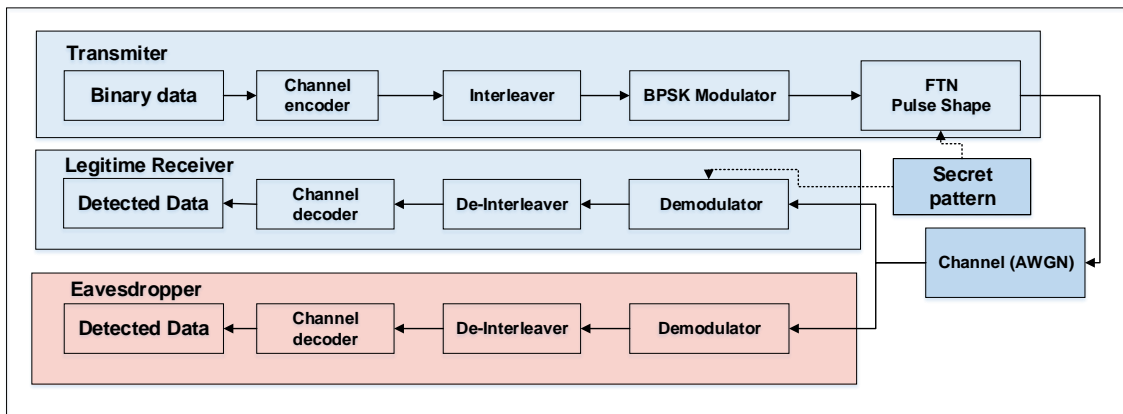


Fig. 3. DVB-S2 system communication model with FTN signaling.

For BCH and LDPC codification and decodification process, the generator polynomial and parity-check matrix proposed by the standard DVB-S2 [7] are used. The signal-to-

noise ratio (SNR) associated to the AWGN channel was varied by taking discrete dB values in the range [2,20], with increment step of 1 dB.

Several scenarios are simulated in which the eavesdropper knowledge about the FTM secret pattern is varied. Three cases are considered: (i) the eavesdropper has the distribution of  $\tau$  values for secret pattern, (ii) the eavesdropper knows the distribution and the range of  $\tau$  values for secret pattern (iii) the eavesdropper knows 75 % of the secret pattern.

Secret capacity ( $C_S$ ) and secrecy outage probability ( $P_{OUT}$ ) are selected as security metrics for the comparison between the technique proposed in [6] (fixed  $\beta$ ), and our proposal (adjusting  $\beta$ ). Fig. 4 shows the results in terms of  $C_S$ .

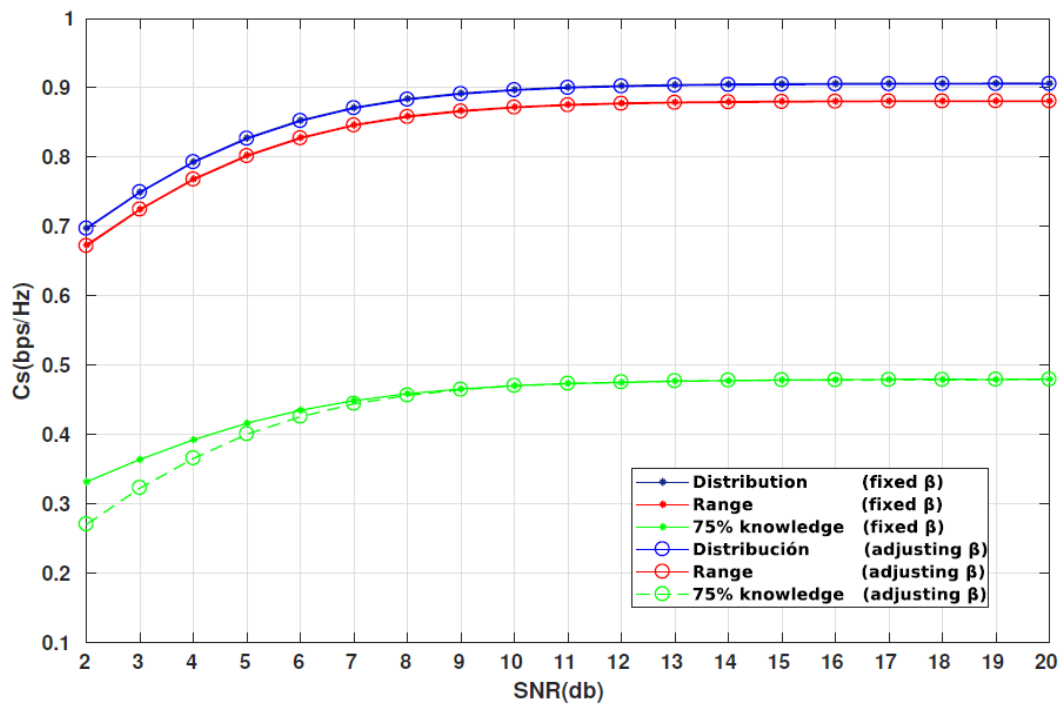
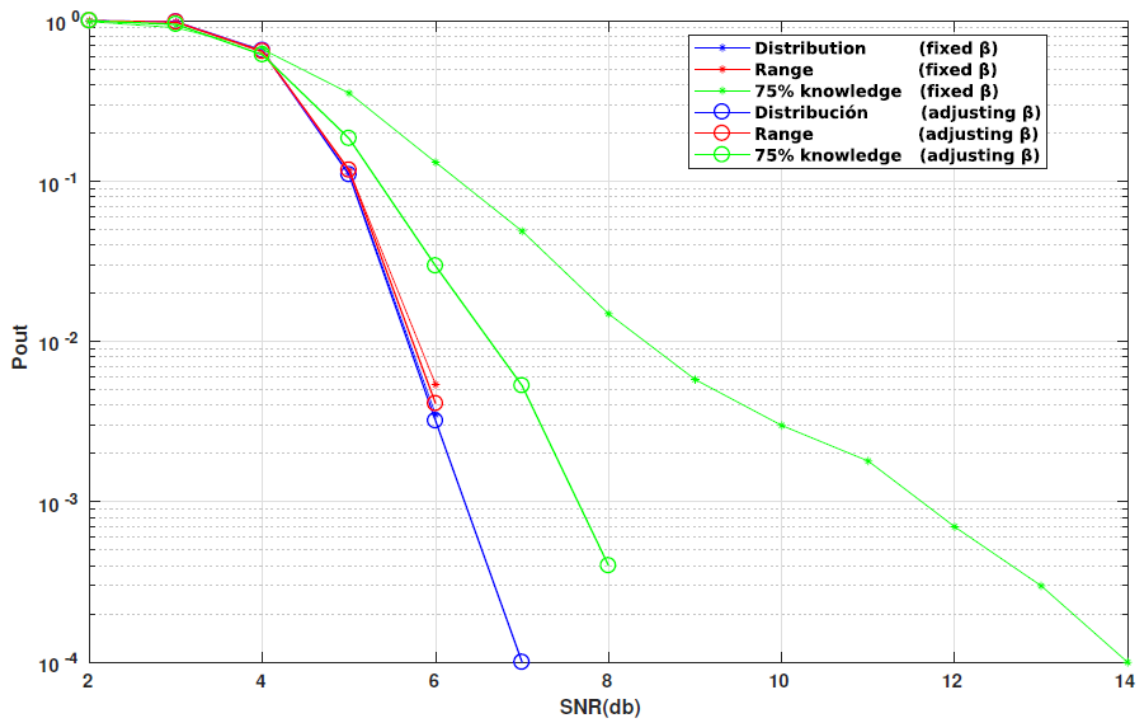


Fig. 4. Secrecy capacity for different eavesdroppers' knowledge as a function of the SNR.

As shown in Fig. 4, in all cases the  $C_S$  increases with the improvement of the channel conditions in terms of SNR. For SNR values above 10 dB, even when the eavesdropper knows 75 % of secret pattern a  $C_S$  higher than 0.4 bps/Hz can be achieved. In the best case, the secrecy rate approaches to 1 bps/Hz which is the maximum transmission rate of the system. This means that, under such conditions, almost all the available transmission

capacity can be used while guaranteeing perfect secrecy. In general terms, both techniques have similar performance in  $C_s$  terms for all scenarios.

On the other hand, Fig. 5 shows the results in terms of  $P_{OUT}$ . Secret rate threshold level of 50 % of the maximum secret capacity is chosen. As can be seen in Fig. 5, as the SNR ratio increases  $P_{OUT}$ , which is due to the improved performance of the main channel but not on the wiretap channel. For SNR values above 8 dB, when the eavesdropper knows 75 % of secret pattern, with a fixed value of  $\beta$ , it needs more than 3 dB to achieve the same performance in term of  $P_{OUT}$  that if we adjust  $\beta$  in each symbol.



**Fig. 5.** Secrecy outage probability for different eavesdroppers' knowledge as a function of the SNR.

Fig. 6 shows the BER results at the data collector and at the eavesdropper for the cases described previously. In Fig. 6, the black lines show the results for the main channel. As it is seen, it is the one that performs better in terms of BER, with a rapid decrease of the BER as the SNR increases for both techniques. On the other hand, the total or partial lack of knowledge of the secret pattern severely affects the BER perceived by eavesdropper. Even for the case of 75% knowledge of the secret pattern the BER computed at the

eavesdropper is significantly high (greater than 0.05). For SNR values lower than 10 dB, with a fixed value of  $\beta$  it needs more than 3 dB to achieve the same performance in term of BER that if we adjust  $\beta$  in each symbol.

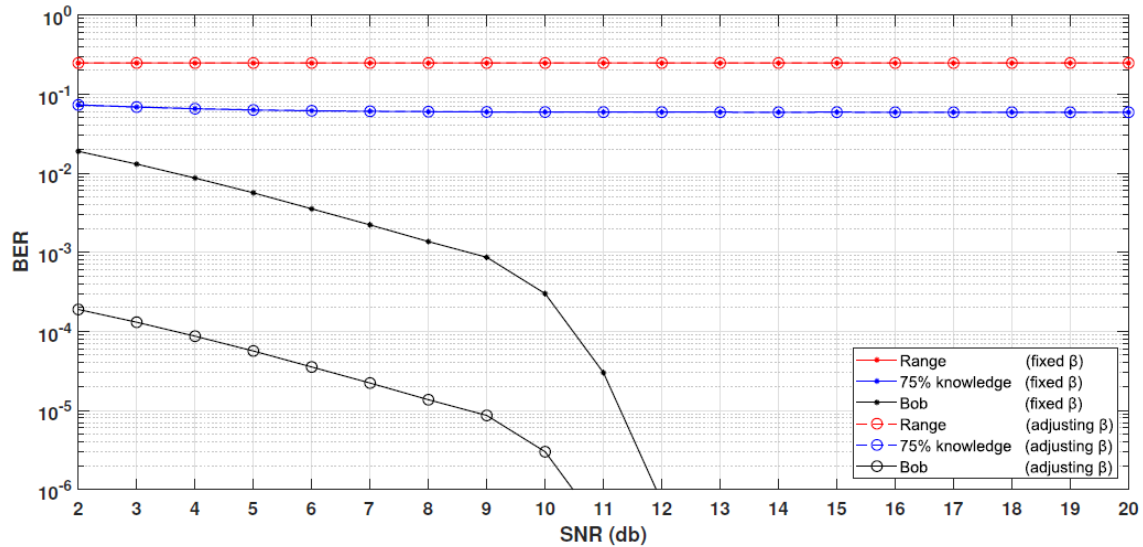


Fig. 6. Bit error ratio (BER) for different eavesdroppers' knowledge as a function of the SNR.

#### 4. Conclusions

This paper proposes a modification of a coded FTN signaling scheme for premium service with DVB-S2 system proposed in [2]. The simulation results show the proposed scheme can accomplish high level of physical layer security without significant degradation and changing the roll-off factor in each symbol is possible to improve the performance of the legitimate users communication in terms or BER of the technology proposed in [2]. Therefore, the proposed modification improves the efficient solution proposed in literature in terms of BER while keep the same level of security.

**II INTERNATIONAL SCIENTIFIC CONVENTION  
“II ICC UCLV 2019”**

**JUNE 23<sup>th</sup> – 30<sup>th</sup>, 2019  
CAYOS DE VILLA CLARA. CUBA.**



**5. References**

- [1] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, 2018.
- [2] M.-S. Baek, J. Yun, S. Kwak, H. Lim, Y. Kim, and N. Hur, "Physical layer security based on coded FTN signaling for premium services in satellite digital broadcasting system," in *2017 IEEE International Conference on Consumer Electronics (ICCE)*, 2017, pp. 147-148: IEEE.
- [3] J. Wang, W. Tang, X. Li, and S. Li, "Filter Hopping Based Faster-Than-Nyquist Signaling for Physical Layer Security," *IEEE Wireless Communications Letters*, vol. 7, no. 6, pp. 894-897, 2018.
- [4] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355-1387, 1975.
- [5] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE transactions on wireless communications*, vol. 7, no. 6, pp. 2180-2189, 2008.
- [6] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6700-6705, 2018.
- [7] A. Morello and V. Mignone, "DVB-S2: The second generation standard for satellite broad-band services," *Proceedings of the IEEE*, vol. 94, no. 1, pp. 210-227, 2006.
- [8] J. E. Mazo, "Faster-than-Nyquist signaling," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1451-1462, 1975.
- [9] J. E. Mazo and H. J. Landau, "On the minimum distance problem for faster-than-Nyquist signaling," *IEEE Transactions on Information Theory*, vol. 34, no. 6, pp. 1420-1427, 1988.
- [10] J. B. Artero, H. J. Kaur, and S. Malhotra, "Analysing behaviour of RRC filter over different modulation formats over AWGN Channel," in *2016 5th International Conference on Wireless Networks and Embedded Systems (WECON)*, 2016, pp. 1-6: IEEE.
- [11] B. Sklar, *Digital communications: fundamentals and applications*. 2001.