On the Physical Layer Security of IoT Devices over Satellite.

Joan Bas[⋆], Ana Pérez-Neira[⋆†]
[⋆]*Array and Multi-Sensor Processing Department*, CTTC/CERCA,Castelldefels,Spain
[†] *Signal Theory and Communications Department*, Universitat Politècnica de Catalunya, Barcelona, Spain
E-mail: {joan.bas, ana.perez}@cttc.es

***Abstract*—The security in satellite communications is a key issue due to the large footprint of the beams. This is specially critical in IoT devices that transmit data directly to satellite. Take into account that IoT devices are characterized by transmitting packets of short length. Consequently, it means that it is not feasible to augment the security level of the IoT packets via complex cryptographic algorithms. Otherwise, their packet lengths may be increased in a non-negligible way which could augment their collision probabilities, latencies and energy consumptions. For this reason, this paper proposes to take advantage of the time-packing technique. By doing so, it is possible to use the overlapping degree among the pulse-shapes to boost the secrecy-capacity. In particular, the overlapping degree between the pulse-shapes introduces an artificial interference that degrades the eavesdropper's channel. In this regard, it is necessary to highlight that there is a residual co-channel interference in the satellite beams. So, it means that these two sources of impairments make difficult to estimate the legitimate user's transmission parameters by the eavesdropper.**

***Index Terms*—IoT, Satellite, Physical-Layer security, High-Spectral Efficient Systems**

I. Introduction

Currently, the forecast for the European market for IoT is a yearly 19.8% increase up to reach $241 billion in 2025. This strong growing will be concentrated in verticals from manufacturing, utilities, retail and transportation [1], [2]. However in order to monetize the potential services over IoT is necessary to guarantee the security of the communications. This is specially important in IoT devices that transmits directly to satellite.

M2M communications are characterized by the transmission of short length packets in a bursty and asynchronous way through a wireless channel. Moreover, IoT devices have strict energy constraints in order to extend their battery life-time. It implies that to guarantee the security of their communications it is not possible resort to complex cryptographic schemes. Otherwise, the packet length of the IoT protocols may be increased in a non-negligible way which could augment their collision probability, latency and energy consumption [3]. Given that they will be deployed at large-scale it is realistic to consider that potential eavesdroppers may be interested in the information transmitted by the IoT devices. This situation is critical in satellite communications due to the large dimensions of their footprints. Hence multiple eavesdroppers may overhear the transmitted information. As a result, it is proposed to use a complementary technique to the cryptographic one to increase the security level of the M2M communications.

In this regard physical-layer security methods may complement higher-layer encryption techniques by exploiting the characteristics of wireless channels. For this purpose, it is resorted to the secrecy-capacity metric. More specifically, it was shown in [4] that reliable information-theoretic security could be achieved, whenever the eavesdropper's channel be a degraded version of the legitimate user's channel. In this case, if the secrecy rate is chosen below the secrecy-capacity, then reliable transmissions can be achieved in perfect secrecy. However, the time-varying fading effect of wireless channels degrades the secrecy-capacity. In this situation, it is used the ergodic capacity to measure the secrecy-capacity [5].

In order to make difficult the overhearing process of the eavesdroppers, this paper proposes to resort to time-packing strategy [6]- [7]. Thus, the time-duration of the transmitted frames are reduced which: i) improves the interception probability of the packets, ii) augments the spectral efficiency of the M2M communications without increasing the transmission bandwidth, iii) diminishes the effect of Doppler spread in Non-GEO communications, and iv) permits to use the overlapping degree among the pulse-shapes to boost the secrecy-capacity. This overlapping degree introduces a multi-path channel known by the legitimate user but ignored by the eavesdropper. This strategy of security is similar to the Artificial Noise (AN) one [5]- [9], but without wasting energy for jamming the eavesdropper's channel.

This paper is divided as follows. Section I explains the signal models of the legitimate and eavesdropper users as well as the satellite channel model. Next, Section II analyzes the mutual information of the legitimate user and the eavesdropper. After that Section III defines the secrecy-capacity when the *plaintext* of the IoT devices is encoded using time-packing strategy. Finally, the sections of results and conclusions come.

This work has received funding from the Spanish Ministry of Science, Innovation y Universities under project TERESA-TEC2017-90093-C3-1-R (AEI/FEDER,UE); and from the Catalan Government (2017 SGR 891 and 2017 SGR 1479

978-9-0827-9703-9/19/$31.00 ©2019 IEEE

II. Signal Models

In this section we present the signal models of the legitimate user, eavesdropper, and the communication channel for a satellite link.

A. Signal Model of the Legitimate and Eavesdropper

In the following we provide the mathematical expressions that describe the signal model of the legitimate user and the eavesdropper. In the satellite field, we have the forward and the return links. In our scenario the forward link transmits the message from the Earth-Station to the IoT device, i.e. the legitimate user. On the return link, the IoT device sends the information to the Earth-Station, which takes the role of legitimate user. In both situations the eavesdropper could be located either at the space or at the terrestrial surface. In any case, the message at the k-th time instant is given by

$$x_d[k] = s_d[n] \cdot p_d[k], \qquad -L_p/2 < k < L_p/2 \tag{1}$$

where $s_d[n]$ and $p_d[k]$ are the n-th modulated symbol and the pulse that shapes the information message, whereas L_p is the number of samples of the pulse shape. Next, under flat fading conditions, the signal received by the legitimate user, denoted as $y_l[k]$, is

$$y_l[k] = h_l[k] \cdot x_d[k] + h_l[k] \cdot \sum_{\substack{q=-N_I \\ q \neq 0}}^{N_I} x_d[k - q \cdot M_{TP}] + \eta_l[k], \tag{2}$$

where $h_l[k]$ is the channel impulse response from the transmitter to the legitimate user, N_I is the number of time-packed interference symbols before and after the current symbol to estimate, and M_{TP} is the separation between consecutive pulses according to the time-packing strategy. If M denotes the oversampling factor, then the overlapping degree between pulses, denoted as τ, will be:

$$\tau = 1 - \frac{M_{TP}}{M}, \qquad (0 < M_{TP} \leq M) \tag{3}$$

Note that for $M_{TP} = M$, the overlapping degree is zero $\tau = 0$, and we have the Nyquist sampling case. Next, $\eta_l[k]$ represents the additive noise plus the residual co-channel interference term from other beams, which it is formulated as

$$\eta_l[k] = \sqrt{I_l} \cdot \sum_{p=0}^{K_I - 1} h_{l,p}[k] \cdot x_p[k] + \sqrt{P_{n_l}} \cdot \upsilon_l[k], \tag{4}$$

being $h_{l,p}$ the channel between the p-th interference signal, denoted as x_p, and the legitimate user, whereas I_l and P_{n_l} are the power of the co-channel interference and the Additive White Gaussian (AWG) noise. Similarly, the signal model that receives the eavesdropper, $y_e[k]$, will be:

$$y_e[k] = h_e[k] \cdot x_d[k] + h_e[k] \cdot \sum_{\substack{q=-N_I \\ q \neq 0}}^{N_I} x_d[k - q \cdot M_{TP}] + \eta_e[k], \tag{5}$$

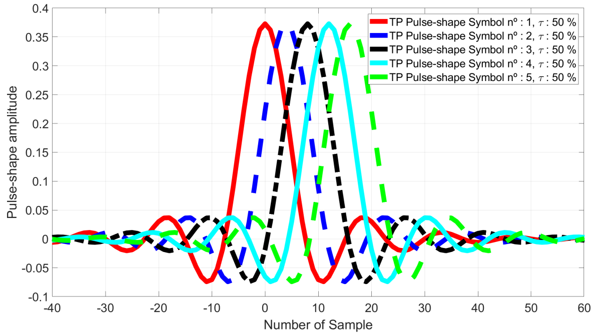

Fig. 1. Time-packed pulse-shape, τ=50% of overlapping. Pulses with ISI.

where $h_e[k]$ is the channel impulse response from the transmitter to the eavesdropper and $\eta_e[k]$ represents the additive noise plus the residual co-channel interference term from other beams, which it is formulated as

$$\eta_e[k] = \sqrt{I_e} \cdot \sum_{p=0}^{K_I - 1} h_{e,p}[k] \cdot x_p[k] + \sqrt{P_{n_e}} \cdot \upsilon_e[k], \tag{6}$$

being $h_{e,p}$ the channel between the p-th interference signal and the eavesdropper. At this point, we show in Fig.1, five consecutive pulse-shapes when their overlapping degree is $\tau = 50\%$. Note the presence of ISI when the pulses overlap among them. Generally, the presence of ISI in a communication channel has been considered as an impairment. Nevertheless, this type of ISI can be controlled by the transmitter. After presenting the signal models of the legitimate user and the eavesdropper, we introduce the satellite channel model and re-interpret it in terms of security. The following section details it.

B. Satellite Channel Model

Regarding the statistical channel, we assume that the channel amplitude has some time variations. If this variation is small, then it can be modeled as a Rician distribution [10]-[12]. The Rician channel is the superposition of a constant signal and another one that varies in a random way as:

$$h_{Rician} = a + \sqrt{2 \cdot \sigma^2} \cdot h_{Random} \tag{7}$$

Being a the parameter that models the Line Of Sight (LoS) component whereas h_{Random} is a Complex Gaussian signal of zero mean and deviation σ. In this situation, if r denotes the channel's envelope, i.e. $r = |h_{Rician}|$, then the Rician probability distribution function is described as [12]:

$$f(r|K,P) = \frac{2 \cdot r \cdot (K+1)}{P} \cdot e^{\left(-K - \frac{(K+1) \cdot r^2}{P}\right)} \cdot \\ \cdot I_0\left(2 \cdot r \cdot \sqrt{\frac{K \cdot (K+1)}{P}}\right), (r \geq 0) \tag{8}$$

where P is the channel power; equated as $P = a^2 + 2 \cdot \sigma^2$, whereas K is the so called vanishing factor of the Rician distribution and represents the relationship between the LoS power component and the random one and it is computed as:

$$K = \frac{a^2}{2\sigma^2} \tag{9}$$

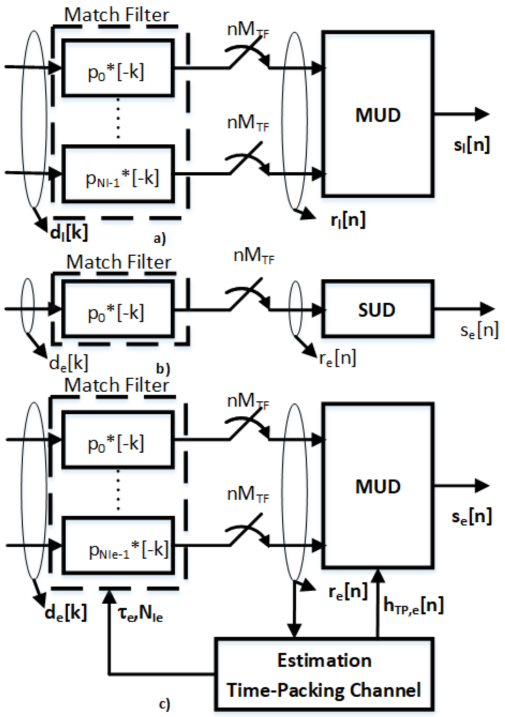

Fig. 2. Receiver architectures for the a) legitimate user, b) eavesdropper without estimating time-packing multi-path interference and c) eavesdropper able to estimate the time-packing interference.

Thus, from (9) if the vanishing factor $K \to \infty$, then the deviation of the random component of the channel goes to zero, i.e. $\sigma \to 0$, and so, the power of the LoS component tends to P. Conversely, if $K \to 0$, then the LoS component of the channel goes to zero, i.e. $a \to 0$, whereas the power of its random part goes to P, i.e. $2 \cdot \sigma^2 \to P$. Note from (8) that if we increase the K parameter the distribution of the signal tends to a Gaussian one which mean closes to the power of the LoS component and smaller variance. In this situation the channels of the legitimate user and the eavesdropper are practically the same and so, the secrecy-capacity is reduced. This case happens in satellite communications since the magnitude of the vanishing factor K is around $K \in \{17-20\}$ dB [13], [14]. At this point we have to remark that we have no assumed that the eavesdropper and legitimate user's channels could be located in different environments [15]. Otherwise, the geographic positions and the elevation angles of the legitimate user and the eavesdropper may impact on the secrecy-capacity. However, this part has been considered out of the scope of this work.

Finally, after presenting the signal models of the legitimate user, eavesdropper and channel we detail, in the following section, the computation of their mutual information.

III. Analysis of Mutual Information

In the process of computing the mutual information, we have considered that the legitimate user has exact knowledge of the time-packing multi-path interference (See Fig. 2a). Regarding the eavesdropper we have assumed two possible scenarios: i) it is not able to resolve the time-packed interference (See Fig. 2b) and ii) it estimates the time-packed multi-path interference (See Fig. 2c).

A. Mutual Information of the Legitimate user's detector

The analysis conducted in this section takes from granted that optimal MAP decoding is feasible, which means that the law of the detector is governed by the exact conditional probability density functions. Without loss of generality, the mutual information can be defined as:

$$I(\mathbf{s}[n]; y_l[n]) = H(y_l[n]) - H(y_l[n]|\mathbf{s}[n]), \tag{10}$$

where $\mathbf{s}[n] = [s_{-N_I} \cdots s_{N_I}]$, $H(y_l[n])$ is the entropy of the received signal, and $H(y_l[n]|\mathbf{s}[n])$ represents the entropy of the received signal conditioned to the transmitted symbols. Assuming that the co-channel interference and the noise are Gaussian distributed, the entropy of $H(y_l[n]|\mathbf{s}[n])$ is:

$$H(y_l[n]|\mathbf{s}[n]) = log_2(\pi \cdot e \cdot (P_{n_l} + I_l)), \tag{11}$$

being P_{n_l} the variance of the AWG noise and I_l the power of the co-channel interference that observes the legitimate user. Resorting to MonteCarlo integration, $H(y_l[n]|\mathbf{s}[n])$ can be approximated according to [16] as follows:

$$H(y_l[n]|\mathbf{s}[n]) = \frac{-1}{N}\sum_{n=0}^{N-1} log_2(p(y_l[n]), \tag{12}$$

where $y_l[n]$ is the n-th realization of the received signal and $N = 10^6$ is the number of realizations. Next, if we apply Bayes rule, then we obtain,

$$p(y_l[n]) = \sum_{\mathbf{s} \in A^{N_I}} p(y_l[n]|\mathbf{s}[n]) \cdot p(\mathbf{s}[n]) \tag{13}$$

being A the alphabet of the transmitted symbol with a cardinality Q. The expression $p(\mathbf{s}[n])$ stands for the probability of the received signal conditioned to the transmitted symbols and $p(\mathbf{s})$ represents the a priori probabilities of the symbols. If it is assumed that all transmitted symbols are equiprobable and independent, then:

$$p(\mathbf{s}[n]) = p(s_{-N_I}; \cdots; s_{N_I}) = \frac{1}{Q^{N_I}}, \tag{14}$$

Under the Gaussian assumption, the conditional probability becomes,

$$p(y_l[n]|\mathbf{s}[n]) = \frac{1}{\pi \cdot (I_l + P_{n_l})} \cdot e^{-\frac{\left| y_l[n] - h_l[n] \sum\limits_{\substack{q=-N_I \\ q \neq 0}}^{N_I} h_q[n] \cdot s_q \right|^2}{P_{n_l} + I_l}} \tag{15}$$

being $h_q[n]$ the channels that results from the convolution between the pulse shapes of the current symbol to estimate and the q-th time-packed interference symbol, and it is formulated as:

$$h_q[n] = p[k] * p[k - q \cdot M_{TP}]|_{k=n \cdot M_{TP}} \tag{16}$$

After showing the mutual analysis of the legitimate user's detector we analyze the eavesdropper's mutual information in the following section.

B. Mutual Information of the Eavesdropper's detector

In this scenario we have considered two possible architectures for the eavesdropper: i) it unknowns the time-packed multi-path interference, and ii) it has some strategy to estimate the time-packed multi-path interference. In the first case the time-packed multi-path interference is considered as noise whereas in the second one it is partially known. The following sections detail both cases.

1) Eavesdropper without estimating time-packed interference: In this scenario the mutual information can be defined as:

$$I(s[n]; y_e[n]) = H(y_e[n]) - H(y_e[n]|s[n]), \tag{17}$$

where $s[n] = s_0$ being s_0 the current symbol to estimate, $H(y_e[n])$ is the entropy of the received signal, and $H(y_e[n]|s[n])$ represents the entropy of the received signal conditioned to the current transmitted symbol. Assuming that the co-channel and the time-packed multi-path interferences plus the additive noise are Gaussian distributed, the entropy of $H(y_e[n]|s[n])$ is:

$$H(y_e[n]|s[n]) = log_2(\pi \cdot e \cdot (P_{n_e} + I_e + I_{TP_e})), \tag{18}$$

being $y_e[n]$ is the n-th realization of the received signal, I_e the co-channel interference that experiments the eavesdropper, whereas I_{TP_e} is time-packed multi-path interference, which it is defined as:

$$I_{TP_e} = E\left[|h_e[k]|^2 \cdot \sum_{\substack{q=-N_I \\ q\neq 0}}^{N_I} |h_q[k]|^2\right]. \tag{19}$$

Next, the probability of the current sample will be:

$$p(y_e[n]) = \sum_{s\in A} p(y_e[n]|s[n]) \cdot p(s[n]) \tag{20}$$

The expression $p(y_e[n]|s[n])$ stands for the probability of the received signal conditioned to the transmitted symbol and $p(s[n])$ represents the a priori probability of the current symbol to estimate. If it is assumed that all transmitted symbols are equiprobable and independent, then:

$$p(s[n]) = p(s_0) = \frac{1}{Q}, \tag{21}$$

Under the Gaussian assumption, the conditional probability becomes,

$$p(y_e[n]|s[n]) = \frac{1}{\pi \cdot (I_e + I_{TP_e} + P_{n_e})} \cdot e^{-\frac{\left|y_e[n] - \sum_{q=-\hat{N}_I}^{\hat{N}_I} h_{e,q} \cdot s_q\right|^2}{P_{n_e} + I_e + I_{TP_e}}} \tag{22}$$

At this point we have derived the mutual information of an eavesdropper that does not estimate the time-packed interference. Next, we show how to compute it when it is estimated the time-packed multipath interference.

2) Smart Eavesdropper: In this case we have assumed that the eavesdropper partially knows the time-packed multi-path interference. Consequently, it means that exists an error in the channel estimation, denoted as P_{TP_e}, which can be equated as:

$$\begin{aligned} P_{TP_e} = E\Bigg[\Bigg| h_e[k] \cdot \sum_{\substack{q=-N_I \\ q\neq 0}}^{N_I} h_q[k] \cdot x_q[k] - \\ \hat{h}_e[k] \cdot \sum_{\substack{q=\hat{N}_I \\ q\neq 0}}^{\hat{N}_I} \hat{h}_q[k] \cdot x_q[k] \Bigg|^2\Bigg] \end{aligned} \tag{23}$$

where $\hat{N}_I$ is the estimation that does the eavesdropper about the number of pulses that generate the time-packed multi-path interference. Next, if it is assumed that the co-channel interference, the additive noise and the partially estimated time-packed multi-path interference are Gaussian distributed, then the entropy of $H(y_e[n]|\mathbf{s}[n])$ is:

$$H(y_e[n]|\mathbf{s}[n]) = log_2(\pi \cdot e \cdot (P_{n_e} + I_e + P_{TP_e})), \tag{24}$$

where $\mathbf{s}[n] = [s_{-\hat{N}_I} \cdots s_{\hat{N}_I - 1}]$. If it is assumed that all transmitted symbols are equiprobable and independent, then $p(\mathbf{s}[n])$ is:

$$p(\mathbf{s}[n]) = p(s_{-\hat{N}_I}; \cdots; s_{\hat{N}_I - 1}) = \frac{1}{Q^{\hat{N}_I}}, \tag{25}$$

Under the Gaussian assumption, the conditional probability $p(y_e[n]|\mathbf{s}[n])$ becomes,

$$p(y_e[n]|\mathbf{s}[n]) = \frac{1}{\pi \cdot P_T} \cdot e^{-\frac{\left|y_e[n] - \hat{h}_e[n] \cdot \sum_{\substack{q=-\hat{N}_I \\ q\neq 0}}^{\hat{N}_I} \hat{h}_q[n] \cdot s_q\right|^2}{P_T}} \tag{26}$$

being P_T the power of all interference signals, i.e. $P_T = P_{n_e} + I_e + P_{TP_e}$. Finally, after deriving the mathematical expressions of the mutual information for the legitimate user and the eavesdropper, we formulate the secrecy-capacity in the following section.

IV. Secrecy-Capacity

Generally speaking, secrecy-capacity is determined by the main channel, i.e., the channel between the transmitter and the legitimate user, and the wiretap channel, i.e. the channel between the transmitter and the eavesdropper. The secrecy-capacity for an instantaneous value of the channel in the quasi-static fading scenario is [17], [18]:

$$C_S = I_l(\mathbf{s}[n]; y_l[n]) - I_e(\mathbf{s}[n]; y_e[n]), \tag{27}$$

where the mutual information of the legitimate user and the eavesdropper have been formulated in the previous section. However, the instantaneous secrecy-capacity is different for each channel fading realizations. In order to evaluate the

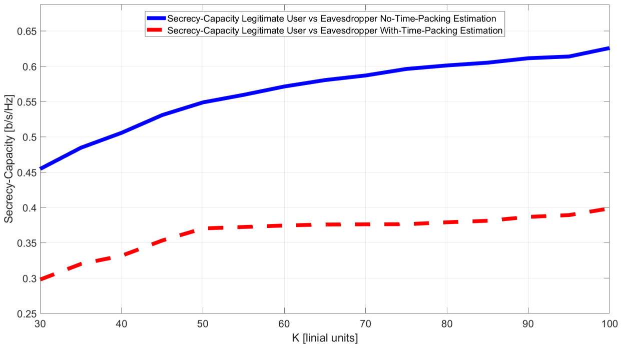

Fig. 3. Secrecy-Capacity of the legitimate user respect the two possible types of eavesdroppers when the overlapping degree is $\tau = 25\%$(See Section II)

security in a long-term sense, i.e. across multiple coherent time slots, average secrecy-capacity was proposed in [19] as performance metric. To be more specific, the average secrecy-capacity is equal to the maximum average instantaneous secrecy-capacity over fading channels and formulated as:

$$\underset{max}{C_S} = \int C_S(h_l, h_e) \cdot p(h_l) \cdot p(h_e) \cdot dh_l \cdot dh_e, \tag{28}$$

After formulating the secrecy-capacity we present the results in the following section.

V. Results

This section evaluates the secrecy-capacity for the legitimate user and the two possible types of eavesdroppers when the transmitted signal is time-packed in terms of the vanishing factor of the Rician channel. Fig.3 shows the secrecy-capacity when the vanishing factor of the channel varies from K=30 to K=100 in steps of 5. The overlapping degree between the consecutive pulses is $\tau = 25\%$. There the residual co-channel interference and the noise power of the legitimate user and the eavesdropper are equal to $I_l = I_e = -15$ dB and $P_{n_l} = P_{n_e} = 10$ dB respectively. The results show that if it used time-packing to encode the transmission data, then exists a secrey-capacity region at large vanishing factors of the Rician channel. As a result, it means that the transmitter can select a rate, so-called secrecy-rate that falls in the outage region of the eavesdropper's capacity. In this situation the eavesdropper is not able to decode the *plaintext* message and so, it is guaranteed the secrecy of the communications.

VI. Conclusions

In this paper we have evaluated the technique of time-packing as alternative to the well-known artificial noise technique for increasing the secrecy-capacity of IoT communications over satellite. Note that the satellite channel model has a large Line of Sight (LoS) component. So, it means that the channel of the eavesdropper and the legitimate user could be quite similar in the same beam. However, the use of the time-packing technique introduces an artificial multi-path interference that degrades the eavesdropper's channel. In this case, we have considered two types of eavesdropper: i) without being able to estimate the time-packing multi-path, and ii) equipped with an estimation block of the time-packing interference. In the first case, all interference signals are considered as noise whereas in the second one part of the interference is assumed as noise. In both cases, it is possible to obtain a secrecy-capacity. Finally, comment that in the satellite field there is a residual co-channel interference. This interference limits the resolution of the eavesdroppers although they be equipped with multiple antennas. Consequently, in this paper we have considered that eavesdropper does not have full knowledge of the time-packed multi-path interference. Similar approach was followed in [9]. However, there the rain losses made difficult to obtain perfect channel estimations.

References

[1] European Telecommunications Network Operators' Association (ETNO), "Annual Economic Report 2018", December 2018.

[2] International Data Corporation,"Worldwide Semiannual Internet of Things Guide", December 2018.

[3] D. Minoli, K. Sohraby, J. Kouns,"IoT (IoTSec) Considerations, Requirements, and Architectures", In Proc. Of IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 1006–1007, January 2017.

[4] A.D. Wyner,"The wire-tap channel",Bell. Sys. Tech. J., vol.54,pp.1355-1387,1975.

[5] H. Rahbari, M. Krunz, "Secrecy beyond Encription: Obfuscating Transmission Signatures in Wireless Communications," In Proc. IEEE Communications Magazine, vol. 53, pp. 54–60, December 2015.

[6] A. Modenini, "Advanced transceivers for spectrally efficient communications", Ph.D. dissertation, Jan. 2014.

[7] F. Russek and A. Pralja,"Optimal Channel Shortening for MIMO and ISI Channels", In Proceedings of IEEE Trans. On Wireless Communications, vol.11,n2,pp. 810-818, February 2012.

[8] A. Mukherjee, "Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constrains", In Proc. of IEEE, vol. 103,n.10, pp.1747–1761, October 2015.

[9] G. Zheng, P. Arapglou, B. Ottersten,"Physical Layer Security in Multibeam Satellite Systems", In Proc. Of IEEE Transactions on Wireless Communications, vol.11,n.2,pp. 852–862, February 2012.

[10] Maral, "Satellite Communication Systems: Systems, Techniques and Technology", in Wiley, 5th Edition, 2011.

[11] F. Pérez-Fontán, M. Castro, C. Cabado, J. García and E.Kubista, "Statistical Modeling of the LMS Channel, In IEEE Trans. On Vehicular Technology, vol.50,n6,Nov. 2001,pp.1549-1567.

[12] F.Pérez-Fontán, P.Mariño,"Modeling the Wireless Propagation Channel", Published by Wireless Series on Communications,2008.

[13] ETSI TR 102 376 v.1.1.1 (2005-02), "Digital Video Broadcasting (DVB); User guidelines for the second generation system for Broadcasting, Interactive Service, News Gathering and other broadband satellite applications (DVB-S2)".

[14] ETSI TR 102 768 v1.1.1 (2009-04), "Digital Video Broadcasting (DVB); Interaction channel for Satellite Distribution Systems; Guidelines for the use of EN 301 790 in mobile scenarios.

[15] ITU-R P.618-13, "Propagation data and prediction methods required for the design of Earth-space telecommunication systems, December 2017.

[16] D. M. Arnold, H. A. Loeliger, P. O. Vontobel, A. Kavcic and Wei Zeng, "Simulation-Based Computation of Information Rates for Channels With Memory", Information Theory, IEEE Transactions on , vol.52, no.8, pp.3498-3508, August 2006.

[17] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao,"A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead", In Proc. Of IEEE Journal on Selected Areas in Communications, vol.36, n.4, pp.679-695, April 2018.

[18] Y. Gao, H. Ao, Z. Feng, W. Zhou, S. Hu, X. Li,"Modeling and Practise of Satellite Communication Systems using Physical Layer Security: A Survey", In Proc. Of IEEE International Conference on Computational Science and Engineering (CSE), pp.829-832, July 2017.

[19] P.K.Gopala,L.Lai, and H.E. Gamal,"On the secrecy capacity of fading channels,",IEEE Transcations Inf. Theory,vol.54,no10,pp.4687-4698,Oct. 2008.