Physical Layer Security Techniques Applied to Vehicle-to-Everything Networks

Leonardo B. da Silva, Evelio M. G. Fernández and Ândrei Camponogara

Abstract— **Physical Layer Security (PLS) is an emerging concept in the field of secrecy for wireless communications that can be used alongside cryptography to prevent unauthorized devices from eavesdropping a legitimate transmission. It offers low computational cost and overhead by injecting an interfering signal in the wiretap channels of potential eavesdroppers. This paper discusses the benefits of the Artificial Noise and Cooperative Jamming techniques in the context of Vehicle-to-everything (V2X) networks, which require secure data exchange with small latency. The simulations indicate that messages can be safely delivered even with devices that have low available power.**

Keywords— **Physical Layer Security, Vehicle-to-everything, Artificial Noise, Cooperative Jamming, Wireless communication networks.**

I. Introduction

Urban mobility is one of the main focuses of the Internet of Things (IoT) when applied to smart cities, due to the necessity for more responsive and safe traffic control. Generally, the solutions proposed in this scope involve the wireless communication between not only the vehicles themselves, but also with pedestrians, infrastructure, and networks. This paradigm is known as Vehicle-to-everything (V2X) and it can be standardized by protocols such as C-ITS (Cellular Intelligent Transportation System) and WAVE (Wireless Access for Vehicular Environment) that are based on the IEEE 802.11p amendment, and the Cellular-V2X (C-V2X) that implements the 5G standard from 3GPP (3rd Generation Partnership Project) [1].

A. Problem Outline

Due to the ever-changing location of most of the involved communication nodes and the time-sensitive nature of the data involved (brake position, vehicle speed, traffic volume, accident reports, etc), the transmission needs not only to occur at high rates, but also offer reliability through high secrecy, low packet loss, and small delay. Furthermore, those nodes have to be affordable to justify their implementation on a city-wide scale, thus having low power consumption and the most cost-efficient embedded processing unit possible [2].

Since the main source of information security in today's landscape is provided through cryptography, the secrecy constraint can negatively affect most of these criteria. As a result of the growth in the availability of portable and connected equipment with high processing capabilities, the safety measures implemented need to match this computational power with proportionally longer and more complex keys to not be vulnerable to brute-force attacks from well-equipped malicious devices [2], [3]. This approach, however, is not sustainable, because it produces increasingly long authentication routines, due to the raise in computational overhead and processing cost as a result of the implemented security algorithms.

B. Overview of the proposed solution

To counterbalance this issue, this paper studies the use of Physical Layer Security (PLS) techniques as an additional protection applied at the Physical Layer to increase the secrecy of wireless communications in a V2X environment. PLS offers low processing cost when compared with cryptography, which is more oriented towards the computational side of the network stack on the Application Layer [1].

Since cryptography techniques provide security in different sections of the wireless protocols, PLS is proposed as a complement to them, rather than a replacement [1]. Through the use of both approaches on the same node, it is possible to offer high secrecy without the necessity of infinitely growing key complexity.

The PLS has its origins on the analytical proposal of Wyner's wiretap channel [4], where it is described a communication between two legitimate nodes that is spied on by an eavesdropper through an unauthorized channel called wiretap. In the modern literature, these devices are usually referred to as a transmitter called Alice, an authorized receiver Bob, and the set of K eavesdroppers named Eves.

In the wiretap channel model shown in Fig. 1, the original message m is encoded and transmitted by Alice as the signal $\mathbf{s}_a$, that reaches Bob through the main channel $\mathbf{h}_{AB}$. The received signal $\mathbf{y}_B$ is then decoded by Bob, obtaining the estimated message $\hat{m}$. Additionally, the k-th Eve can intercept $\mathbf{s}_a$ through the wiretap channel $\mathbf{h}_{AE,k}$, obtaining the signal $\mathbf{y}_{E,k}$ that when decoded produces z.

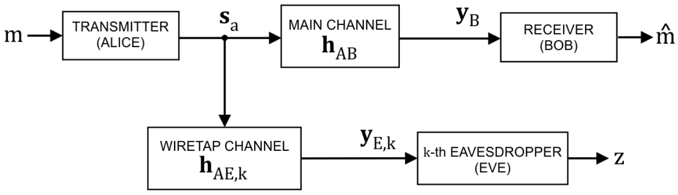


Fig. 1: The wiretap channel generic model based on [4]

L. B. da Silva, E. M. G. Fernandez, Â. Camponogara, Electrical Engineering Department, Federal University of Paraná (UFPR), Curitiba, PR, Brazil, e-mails: leonardobarbosa@ufpr.br, evelio@ufpr.br and andrei.camponogara@ufpr.br. This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001.

The main focus of PLS is to guarantee that the mutual information between m and z is as close to zero as possible. When this condition is met, even if z is know, it is impossible for Eve to infer the contents of the original message.

Wyner then presents a set of parameters that enable the use of the physical imperfections of the channel, such as noise and fading, to provide information secrecy by raising the level of confusion on undesired nodes. Rendering them unable to distinguish between the message and the interference.

Currently, plenty of techniques to provide security at the physical layer level have been proposed in the literature [3]. This paper will focus on two approaches first presented in [5]:

- **Artificial Noise (AN):** This approach uses a portion of the transmitter node's power to inject artificially generated noise in the eavesdropper's channel;
- **Cooperative Jamming (CJ):** This approach expands the AN model by proposing a connected network where nearby relay nodes (Charlies) send a jamming signal to the eavesdropper's channel.

To demonstrate the viability of PLS applications in a V2X network, it is common to create stochastic geometric models that randomly generate streets and distribute communication nodes in a predefined area to represent an urban mobility scenario [6], [7]. When implementing these methods, metrics such as the Signal-to-Interference Ratio (SIR) are used to define the threshold of confusion necessary to provide secrecy at the physical layer. The SIR on each eavesdropper can then be evaluated to determine the secrecy outage probability (SOP) of the data transmission with different densities of the involved nodes in the simulated network. This work contributes to the state of the art by comparing the SOP in simulations that implement AN and CJ techniques for the same stochastic geometry model.

In this paper, Section II describes the stochastic algorithms implemented to model a V2X network that includes streets and communication nodes (vehicular and planar). Section III presents the analytical basis of the AN and CJ techniques, while also introducing the SIR and SOP metrics. In Section IV, the results of numerical simulations are shown to illustrate the benefits of the considered PLS techniques on the generated V2X networks. Finally, Section V states some final remarks.

Notation: $\mathbf{I}_N$ is an identity matrix of order N, Poisson(n) is a Poisson distribution with mean number of arrivals n, $\mathcal{CN}(m, n)$ is a complex normal distribution with average m and covariance n, $\exp(n)$ is an exponential distribution with mean n and Gamma(m, n) is the gamma distribution with form m and scale n.

II. The V2X network model

As mentioned previously, vehicular networks are dynamic, with devices changing location constantly. Thus, a deterministic model is not well-suited for this application. A common alternative is the use of stochastic geometry to represent this random spatial nature through a variety of different processes to distribute the streets and communication nodes within the desired coverage area [8].

A viable option is the use of Poisson processes, as they are memoryless counting processes for integer arrivals [9]. In other words, each set of elements generated will be independent with a Poisson distributed integer number of uniformly spaced nodes. The intensity of the arrivals in these processes are represented by λ and the expected number of elements is the product of the said intensity and the Lebesgue measure, which in this context is essentially the spatial measurement associated with the object that the points will be distributed on. For instance, the Lebesgue measure to populate a circle is its area and for a line is the length. One realization of the resulting spatial model derived from the use of different variations of the Poisson processes is represented in Fig. 2.

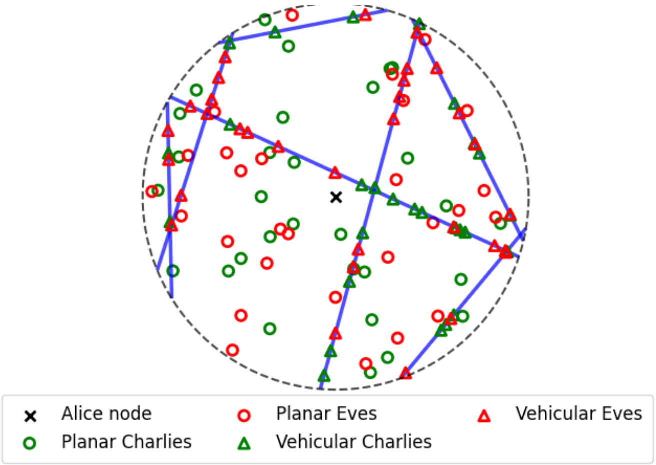


Fig. 2: Spatial simulation of the modeled V2X network. The color green indicates the Charlies implemented in CJ techniques and the Eves are in red. The planar devices are generated by PPPs represented by circles (○) with intensity λ = 10^{-6}/m^2 for both node types. Through a PLP, the streets (blue lines) have been modeled with an intensity of λ_l = 10^{-3} /m, and the vehicular devices are originated from PLP-driven Cox Processes indicated with triangles (△) of intensity u = 10^{-3}/m for both Charlies and Eves. A single Alice is indicated with a black × at the origin.

In this model, the wireless devices of pedestrians and connected infrastructure are considered free to be positioned in the whole area A of the modeled network, which is a circle of radius r = 3 km. Thus, these “planar nodes“ are generated by 2-D Poisson Point Processes (PPP) and the expected amount of elements is given by Poisson$(\lambda \cdot A)$. The set of planar nodes is indicated by Φ, thus the planar Eves and Charlies are respectively represented by Φ_E and Φ_C.

The streets are represented by uniformly distributed lines with density $\mu_l = \lambda_l / \pi$ generated by a Poisson Line Process (PLP) Φ_l based on the second method of the Bertrand paradox [10], in which a set of expected Poisson$(\mu_l \cdot 2\pi r)$ midpoints are created [11], each with a random radius $P \in [0, r)$ and angle $\theta \in [0, 2\pi)$. From these coordinates, a segment perpendicular to P is traced between two points at the edge of the circle of radius r. This effectively means that a pair of 1-D PPP points are created in the perimeter of the circular area for each modeled street.

On those PLP-generated lines, a Cox process of intensity u is implemented, which is used to create the “vehicular nodes“ on each segment [12]. These elements represent vehicles whose spatial distribution are constrained to a street by a 1-D PPP. Considering a street of length l, the number of vehicles in it is given by Poisson$(u \cdot l)$.

The set of vehicular Eves and Charlies on each street l are respectively denoted by ψ_E and ψ_C. Based on these, the total nodes of each type can be obtained by evaluating the sets on the whole range of Φ_l [6], resulting in $\Psi_E = \{\psi_E(l)\}_{l\in\Phi_l}$ for Eves and $\Psi_C = \{\psi_C(l)\}_{l\in\Phi_l}$ for Charlies.

Furthermore, a single deterministic transmitter (Alice) is included at the origin of the circle. This point is selected to simplify the distance calculations between a legitimate device and the Eve nodes, which can be planar or vehicular. This measurement is one of the parameters for the SIR calculations, that are considered to determine the effectiveness of the PLS. For the CJ case, auxiliary nodes (Charlies) are also modeled, some as planar and others as vehicular devices. Note that the distance between Charlies and Eves influences the power of the interference injected on the unauthorized channels as part of the jamming technique.

III. PLS Techniques

The PLS techniques presented in this paper are part of the key-less-based class [2], which implements secure information transmission by making the unauthorized channel's capacity (C_E) lower than that of the legitimate channel's (C_B). This relationship can be presented by evaluating these values through the Shannon-Hartley theorem, which produces the secrecy capacity (C_S) metric as

$$C_S = C_B - C_E = \log_2(1+\gamma_B) - \log_2(1+\gamma_E), \quad (1)$$

where γ_B and γ_E are, respectively, the SIRs of Bob and Eve. Based on this expression, it can be inferred that in order to guarantee that C_B is sufficiently larger than C_E, the value of γ_E must be as low as possible. The approach utilized by AN and CJ is the injection of artificially generated interference in the eavesdropper channels.

Typically, this injection is implemented with multi-antenna networks, as it enables the use of beamforming to selectively direct the transmission to legitimate receivers with minimum noise and high efficiency [3]. The unintended receivers on the other hand, intercept a signal that contains the secret message as well as AN. Therefore, secrecy is provided when the distinction between them by the Eves is improbable.

The wireless channels in this paper are modeled with complex normal distributions ($\mathcal{CN}$) which implies in a Rayleigh small-scale fading model. This decision provides simpler analytical equations and also proposes a more pessimistic scenario, in which there is no Line-of-Sight (LoS) available. By evaluating the metrics in these worst-case conditions, it is possible to verify that even then the secrecy can be guaranteed.

A. Artificial Noise

In the AN scenario, the legitimate communication is established between a single transmitter Alice and a receiver Bob. Additional nodes (both planar and vehicular) that try to obtain Alice's signal are then considered eavesdroppers and their channels will be affected by the AN.

The signal transmitted by the Alice node with N_A antennas is composed of two terms: the first contains a message x intended for Bob and the second is based on a zero-forcing vector for the unauthorized devices [13], i.e,

$$\mathbf{s}_a = \sqrt{\phi P_t}\frac{\mathbf{h}_a}{\|\mathbf{h}_a\|}x + \sqrt{\frac{(1-\phi)P_t}{N_A-1}}\mathbf{W}_a\mathbf{n}_a, \quad (2)$$

where $\mathbf{h}_a/\|\mathbf{h}_a\|$ is the beamforming vector with the normalization of the Alice's channel estimation $\mathbf{h}_a \in \mathbb{C}^{N_A\times 1}$, that will be modeled as $\mathcal{CN}(0, \mathbf{I}_{N_A})$. The AN is formed by the null-space orthonormal basis $\mathbf{W}_a \in \mathbb{C}^{N_A\times(N_A-1)}$ and the noise signal $\mathbf{n}_a \in \mathbb{C}^{(N_A-1)\times 1}$.

The distribution of the available power, P_t, between the two terms of (2) is controlled by $\phi \in \{0,1\}$. $\phi = 0$ means that all power is allocated to noise generation and no message is sent. Conversely, when ϕ = 1 the AN is not active and P_t is allocated entirely for data transmission.

B. Cooperative Jamming

The Cooperative Jamming extends the AN case, maintaining the single Alice-Bob authorized transmission with multiple Eves, however, adding auxiliary nodes in the network. These devices, typically called Charlies, can also be either planar or vehicular, just like the Eves. In contrast, they are responsible for providing additional security by sending jamming signals that further decrease the channel quality of the Eves.

For simplicity, it is considered that only Alice will transmit messages in the scenarios evaluated in this paper. Hence, the signals sent by the Charlie nodes are made of only the AN (zero-forcing) portion, as follows

$$\mathbf{s}_c = \sqrt{\frac{P_c}{N_C-1}}\mathbf{W}_c\mathbf{n}_c, \quad (3)$$

where N_C is the number of antennas of each Charlie and P_C is the power available for jamming. Notice that since these nodes are not transmitting messages, all the available power is directed towards CJ. Additionally, $\mathbf{W}_c \in \mathbb{C}^{N_C\times(N_C-1)}$ is the null space orthonormal matrix and $\mathbf{n}_c \in \mathbb{C}^{(N_C-1)\times 1}$ is the artificial noise component.

C. Received Signals

By considering that the channel estimation $\mathbf{h}_a$ is precisely the main channel established between Alice and Bob, $\mathbf{h}_{AB}$, it is implied that the receiver node is not affected by the interference from AN or CJ. That happens because the orthonormal basis $\mathbf{W}_a$ and $\mathbf{W}_c$ are null when applied to the authorized channels, resulting in the relationships $\mathbf{h}_{AB}^{\dagger}\mathbf{W}_a = 0$ and $\mathbf{h}_{AB}^{\dagger}\mathbf{W}_c = 0$, respectively. Therefore, the signal received by Bob can be expressed as

$$\mathbf{y}_B = \sqrt{\phi P_t}\,\|\mathbf{h}_a\|\,D_{AB}^{-\alpha/2}\,x, \quad (4)$$

where D_{AB} is the distance between the devices and $\alpha > 2$ is the path loss exponent considering an NLoS scenario. The distances are obtained through simple trigonometry based on the coordinates randomly generated by the stochastic processes described in Section II.

For the signal intercepted by the eavesdroppers, it is evaluated a set of $K = (\Phi_E + \Psi_E)$ Eves, containing both planar and vehicular nodes. Similar considerations are adopted for the Charlies in the CJ scenario, resulting in $C = (\Phi_C + \Psi_C)$.

As discussed when $\mathbf{s}_a$ was presented, Alice sends a signal containing the secret information and AN. Since authorized Alice-Eves channels are not expected in the beamforming sense, the orthonormal basis are not null, thus the Eves receive interference. When the Cooperative Jamming is taken into consideration, Eves are also affected by the interference generated by the nearby Charlies through the $\mathbf{s}_c$ signals. With that in mind, the signal obtained by the k-th Eve is given by

$$\begin{aligned}\mathbf{y}_{E,k} = {} & \sqrt{\phi P_t}\,\mathbf{h}^{\dagger}_{AE,k}\,D^{-\alpha/2}_{AE,k}\,x \\ & + \sqrt{\frac{(1-\phi)P_t}{N_A-1}}\,\mathbf{h}^{\dagger}_{AE,k}\,\mathbf{W}_a\,D^{-\alpha/2}_{AE,k}\,\mathbf{n}_a \\ & + \sum_{c\,\in C}\sqrt{\frac{P_c}{N_C-1}}\,\mathbf{h}^{\dagger}_{c,k}\,\mathbf{W}_c\,D^{-\alpha/2}_{c,k}\,\mathbf{n}_c\,,\end{aligned} \tag{5}$$

which is composed of essentially three terms. The first is the intercepted secret message itself, the second term is the AN signal generated by Alice, and the third term is a sum of all the interference injected by the Charlie nodes. Since CJ only affects the last term of (5), the AN scenario can be obtained by simply adopting that the sum in this term is equal to zero.

From (4) and (5), it is possible to determine the SIR of Bob and the K Eves. Thus, the SIR of Bob can be determined as

$$\gamma_B = P_t\phi\ \|\mathbf{h}_a\|^2\,D^{-\alpha}_{AB}, \tag{6}$$

and the SIR for each Eve can be obtained from (5) as follows

$$\gamma_{E,k} = \frac{P_t\ \phi\ \left|\mathbf{h}^{\dagger}_{AE,k}\,\mathbf{h}_a/\|\mathbf{h}_a\|\right|^2 D^{-\alpha}_{AE,k}}{\frac{P_t\ (1-\phi)}{N_A-1}\ \left\|\mathbf{h}^{\dagger}_{AE,k}\,\mathbf{W}_a\right\|^2 D^{-\alpha}_{AE,k} + I_c}, \tag{7}$$

where I_c is the sum of the interference injected by the Charlies given by

$$I_c = \sum_{c\,\in\,C}\frac{P_c}{N_c-1}\|\mathbf{h}^{\dagger}_{c,k}\,\mathbf{W}_c\|^2\,D^{-\alpha}_{ck}, \tag{8}$$

which is non-zero only in the CJ scenario. The products $\mathbf{h}^{\dagger}_{AE,k}\cdot\mathbf{h}_a/\|\mathbf{h}_a\|$ and $\mathbf{h}^{\dagger}_{AE,k}\cdot\mathbf{W}_a$ from the Alice-Eve channel and also $\mathbf{h}^{\dagger}_{ck}\cdot\mathbf{W}_c$ from Charlie-Eve produce independent identically distributed $\mathcal{CN}$ random variables with unitary variance [6]. This enables the approximations $\left|\mathbf{h}^{\dagger}_{AE,k}(\mathbf{h}_a/\|\mathbf{h}_a\|)\right|^2 \sim \exp(1)$, $\|\mathbf{h}^{\dagger}_{AE,k}\mathbf{W}_a\|^2 \sim \text{Gamma}(N_A-1,1)$ and $\|\mathbf{h}^{\dagger}_{c,k}\ \mathbf{W}_c\|^2 \sim \text{Gamma}(N_C-1,1)$.

D. Performance metric

Considering that Alice transmits codewords at a rate R_b with a secrecy rate $R_S \leq C_S$, the redundancy rate can be defined as $R_e = R_b - R_S$. Then a secrecy outage event occurs when the channel capacity of any Eve is higher than the redundancy rate that Alice can provide, i.e., $C_E > R_e$.

In a multiple passive Eves scenario, whose Channel State Information (CSI) are unknown, the secrecy performance is addressed in terms of the Secrecy Outage Probability (SOP), since the only available information about the Alice-Eve channel is its statistics. This metric defines the probability that Thus, the SOP is defined as

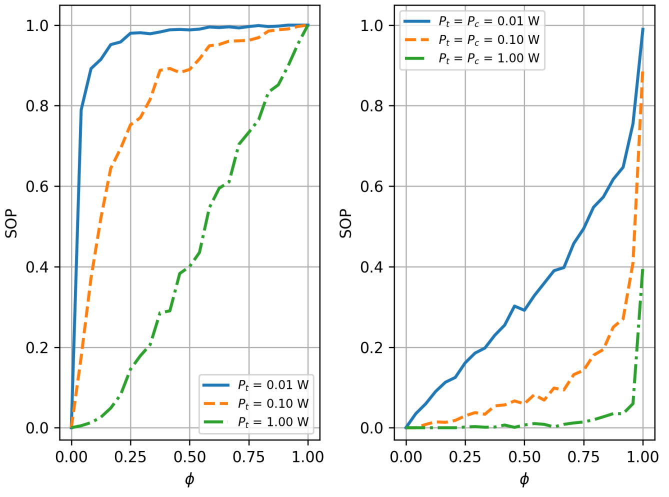
$$SOP = 1 - \Pr\left(\max_{k\in K}\gamma_{E,k} < \beta\right), \tag{9}$$

which is the complement of the probability that the highest SIR among all Eves is less than the threshold $\beta = 2^{R_e} - 1$. This means that higher values of secrecy can be obtained by implementing the aforementioned PLS techniques to reduce $\gamma_{E,k}$ as much as possible.

IV. Numerical Results

Various Python numerical simulations with different parameters were performed to evaluate the relationship between the SOP and the decrease of the SIR for the k-th Eve. Since the V2X network model is randomly generated, the coordinates of each node and street change with each run. To provide more consistent results, the curves presented below are the average of twenty-five realizations of each simulation configuration.

Fig. 3 illustrates the SOP for different P_t and P_c values, ranging from 10 mW (10 dBm) to 1 W (30 dBm). As expected, when the devices have more power available for interference, the SOP is greatly reduced. However, for the AN scenario secrecy is still not guaranteed when ϕ grows. For CJ, the SOP increases in a much slower rate due to the larger amount of nodes jamming the signal received by the Eves.



(a) Artificial Noise

(b) Cooperative Jamming

Fig. 3: SOP versus ϕ (25 realizations) for the AN and CJ with different available power {0.01, 0.1, 1} W. β = 0 dB, α = 3, N_A = N_C = 4, λ_E = λ_C = $10^{-6}/m^2$, μ_E = μ_C = 10^{-3}/m, r = 3 km.

Through the simulation results presented in Fig. 4, it can be easily noted that as β increases the SOP decreases, because the criteria for secrecy failure is becoming more selective. Furthermore, ϕ have an opposing effect when compared to β, suggesting that for higher threshold values to guarantee low SOP, more power needs to be allocated to interference. Because of that, in applications where the devices have limited power (such as IoT and V2X), CJ is a more economic approach as long as there are sufficient nearby auxiliary nodes.

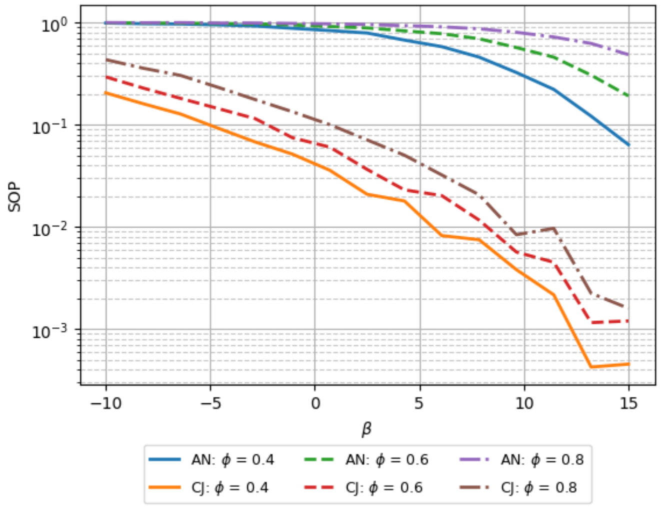


Fig. 4: SOP versus β (50 realizations) for the AN and CJ with different power allocation ratios $\{0.4, 0.6, 0.8\}$. α = 3, $P_t = P_c$ = 20 dBm, $N_A = N_C$ = 4, $\lambda_E = \lambda_C = 10^{-6}/m^2$, $\mu_E = \mu_C = 10^{-3}$/m, r = 3 km.

In Fig. 5, it is evaluated the influence that the proportion of Charlies to Eves have on the SOP. This is achieved by implementing different values of intensities (λ and u) for the Poisson processes that generate these nodes. The SOP grows rapidly in the AN, indicating that the available power is insufficient to guarantee secrecy with the given Eve density. For the CJ cases, however, as the number of Charlie nodes rises, the SOP starts to reduce, making the communication viable even for higher values of ϕ. When there are more Charlies than Eves it is shown that very little power needs to be applied in each device to provide a low SOP.

V. Conclusion

In this paper, a stochastic geometric approach was presented as a method to randomly generate V2X network models. The coordinates of these elements were then used to evaluate the effectiveness of PLS techniques in different realizations of vehicular networks subjected to path loss with NLoS.

Both AN and CJ were introduced based on the analytical signals that the involved nodes transmit. Next, expressions were obtained for the SIR of Bob and the k-th Eve. Finally, the SOP was computed to evaluate the level of information security provided by the presented AN and CJ techniques, providing a comparison between the approaches.

Based on numerical results, it can be concluded that PLS can provide additional security for the V2X networks with relative low power cost, specially when both the techniques are combined. It is also noted that in the CJ scenario, when there are more Charlies in the proximity, the security increases. Therefore, the urban networks are the most benefited by this technique, since it is expected a higher density of wireless devices in the same area in these environments.

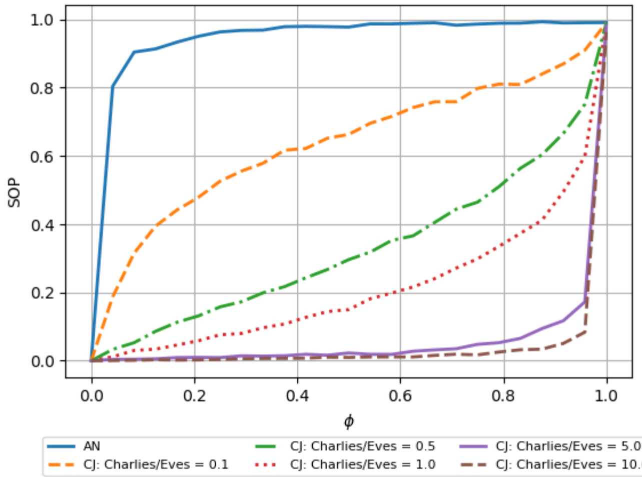


Fig. 5: SOP versus ϕ (25 realizations) for the AN and CJ with different λ_C/λ_E ratios $\{0.1, 0.5, 1, 5, 10\}$. β = 0 dB, α = 3, $P_t = P_c$ = 10 dBm, $N_A = N_C$ = 4, $\lambda_E = 10^{-6}/m^2$, $\mu_E = 10^{-3}$/m, r = 3 km.

References

[1] B. M. ElHalawany, A. A. El-Banna and K. Wu, “Physical-Layer Security and Privacy for Vehicle-to-Everything”, *IEEE Communications Magazine*, vol. 57, n. 10, pp. 84-90, 2019.

[2] 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*, vol. 21, n. 2, pp. 1773-1828, 2019.

[3] A. Sanenga, G. A. Mapunda, T. M. L. Jacob, L. Marata, B. Basutli and J. M. Chuma, “An Overview of Key Technologies in Physical Layer Security”, *Entropy*, vol. 22, n. 11, MDPI, 2020.

[4] A. D. Wyner, “The wire-tap channel”, *The Bell System Technical Journal*, vol. 54, n. 8, pp. 1355-1387, 1975.

[5] R. Negi and S. Goel, “Secret communication using artificial noise”, *VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference*, vol. 3, pp. 1906-1910, 2005.

[6] C. Wang, Z. Li, X. Xia, J. Shi, J. Si, and Y. Zou, “Physical Layer Security Enhancement Using Artificial Noise in Cellular Vehicle-to-Everything (C-V2X) Networks”, *IEEE Transactions on Vehicular Technology*, vol. 69, n. 12, pp. 15253-15268, 2020.

[7] B. Qiu and C. Jing, “Performance Analysis for Cooperative Jamming and Artificial Noise Aided Secure Transmission Scheme in Vehicular Communication Network”, *Research Square Platform LLC*, 2020.

[8] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge: Cambridge University Press, 2012.

[9] R. D. Yates and D. J. Goodman, “Probability and Stochastic Processes: A Friendly Introduction for Electrical and Computer Engineers”, Nashville, TN: John Wiley & Sons, 2005.

[10] J. Bertrand, *Calcul des probabilités*. Gauthier-Villars, 1889.

[11] V. V. Chetlur and H. S. Dhillon, “Coverage Analysis of a Vehicular Network Modeled as Cox Process Driven by Poisson Line Process”, *IEEE Transactions on Wireless Communications*, vol. 17, n. 7, 2018.

[12] C. Choi and F. Baccelli, “Poisson Cox Point Processes for Vehicular Networks”, *IEEE Transactions on Vehicular Technology*, vol. 67, n. 10, pp. 10160-10165, 2018.

[13] L. Hu, H. Wen, B. Wu, F. Pan, R. Liao, H. Song, J. Tang, and X. Wang, “Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things”, *IEEE Internet of Things Journal*, vol. 5, n. 1, 2018.