Safety Modeling and Performance Analysis of Urban Scenarios Based on Poisson Line Process

Kong Shi[1(✉)] and Xinyu Gu[2]

[1] Beijing University of Posts and Telecommunications, Beijing, China
18801372153@163.com
[2] Purple Mountain Laboratories, Beijing University of Posts and Telecommunications, Nanjing 211111, China
guxinyu@bupt.edu.cn

Abstract. Secrecy Performance is one of the focus of research on physical layer security in vehicle-to-everything (V2X). Poisson line process (PLP) is regarded as a more suitable model to study the vehicle communication performance of urban scenarios. However, due to the high theoretical difficulty in the analysis of PLP, research in this area has not been widely conducted yet. In this paper, we take a secure transmission scheme that can improve physical layer security as an example, use PLP model to model urban scenarios. We analyze the performance of coverage probability, secrecy probability and secrecy throughput and draw some effective conclusions to improve secrecy performance. We import a typical urban scenario - part of the map data of Xi'an urban area in China, compare the performance derived by PLP and two-dimensional Poisson point process (2D PPP) model with those modeled on the real urban map respectively, it is demonstrated that PLP is more suitable as the model for urban scenarios.

Keywords: Poisson line process · urban scenario · safety performance analysis · stochastic geometry

1 Introduction

As the number of vehicles increases worldwide, traffic problems can no longer be ignored. We need intelligent transportation systems to update and disseminate information related to road safety and traffic congestion through communication transmission between vehicles or between vehicles and other devices, to improve people's travel efficiency and driving experience. Under this trend, vehicle-to-everything (V2X) technology has become an important technical means to improve the existing transportation system.

Security problems in the process of vehicle communication cannot be ignored. Vehicle communication involves the exchange of information about the user's identity, location and trajectory, and securing vehicle communication is crucial to ensure the user's personal safety. There are two popular strategies for

F. Gao et al. (Eds.): ChinaCom 2022, LNICST 500, pp. 231–246, 2023.
https://doi.org/10.1007/978-3-031-34790-0_18

vehicular security: password-based solutions and physical layer security (PLS)-based solutions [1]. Among them, password-based solutions may face challenges due to the strict latency requirements in vehicle communication, especially for large-scale access scenarios. However, physical layer security-based solutions can complement the former very well [2]. In [3], the authors provide a comprehensive overview of the PLS strategy adopted for V2X, presenting the security threats and the basic principles of PLS techniques. The authors in [4] investigated the PLS performance of mobile vehicle networks, derived exact closed-form expressions for secrecy performance and verified the secrecy performance under different conditions.

Based on the well-known PLS theory analysis, artificial noise (AN) and cooperative jamming (CJ) strategies have been proposed to improve the secrecy performance [5]. In [6], AN schemes for secrecy enhancement are investigated and the balance between communication reliability and security is analyzed. The authors in [7] proposed a practical uncoordinated cooperative jamming scheme to enhance the physical layer security of single-input-single-output eavesdropping channels. In [8], in addition to applying AN and CJ approaches, a full-duplex legal receiver is applied to further enhance the physical layer security. The authors in [9] investigates the confidential transmission of cooperative interference and artificial noise schemes by considering two types of eavesdroppers.

The stochastic geometry not only has high analytical and computational efficiency, but also provides assistance in assessing the influence of system parameters on network performance. There have been many studies applying stochastic geometry to analyze the performance of vehicular communication. It has also been widely used to study the physical layer security. In urban scenarios, the location of nodes on each road is usually irregular and can be considered as a one-dimensional Poisson point process, and the number of roads is usually irregular and can be modeled as Poisson line process (PLP). The authors in [10] presents the evolution history of PLP theory, discusses in detail the basic features and application of PLP, PLCP and other models in wireless domain. The authors in [11] propose a transmitter selection criterion to enhance the reliability performance of downlink transmission in a wireless vehicular network using Manhattan Poisson line process model.

In this paper, the secrecy performance analysis is performed using the current emerging PLP model for urban scenarios.

2 System Model

In the actual urban scenarios, vehicles travel along the road. In order to reflect the random distribution of roads, we use PLP to model the urban roads, and since in most urban areas, the roads are mostly distributed perpendicular or parallel to each other, we model the urban roads as some straight lines that are randomly distributed and parallel or perpendicular to each other - Manhattan Poisson line process (MPLP), with road distribution density λ_l. MPLP belongs to a special case of PLP. Since vehicles are randomly distributed on each road,

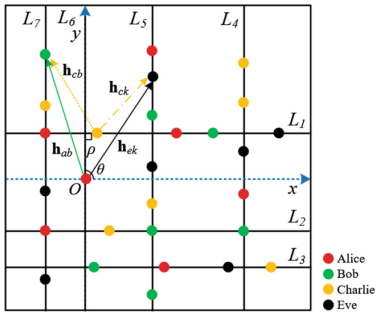

Fig. 1. MPLP model.

we model the vehicles on each road as a one-dimensional Poisson point process (1D PPP) with a vehicle density of λ_v.

The scenario is equipped with four vehicles, as shown in Fig. 1, which are the transmitting vehicle (Alice), the legitimate receiving vehicle (Bob), the eavesdropping vehicle (Eves) and the jamming vehicle (Charlies). We assume that each Alice and Charlie is equipped with N_a and N_c antennas respectively. Each Eve and Bob is equipped with only one antenna [12]. The fast fading channels from Alice to Bob and Eve are denoted by $h_{ab} \in C^{N_a}$ and $h_{ek} \in C^{N_a}$ respectively, and the fast fading channels from Charlie to Bob and Eve are denoted by $h_{cb} \in C^{N_c}$ and $h_{ck} \in C^{N_c}$ respectively. We call the channel h_{ab} the legitimate channel and h_{ek} the eavesdropping channel, where $h_{ab} \sim CN(0, I_{N_a})$, $h_{ek} \sim CN(0, I_{N_a})$ and $h_{ck} \sim CN(0, I_{N_c})$. According to the knowledge of stochastic geometry, we can get the following channel distribution, that is, $\|h_{ab}\|^2 \sim \Gamma(N_a, 1)$, $\|h_{ek}^T w_a\|^2 \sim exp(1)$, $\|h_{ek}^T W_a\|^2 \sim \Gamma(N_a - 1, 1)$ and $\|h_{ck}^T T_c\|^2 \sim \Gamma(N_c - 1, 1)$ [13]. Where $CN(p, q)$ denotes a circularly symmetric complex Gaussian distribution with mean p and covariance q. $\Gamma(k, \mu)$ denotes a gamma distribution with shape parameter k and scale parameter μ. $exp(a)$ denotes an exponential distribution with mean a. $|\cdot|$ and $\|\cdot\|$ denote the absolute value and the two-parameter number, respectively.

In order to make the theoretical results more convincing, we selected a typical urban scenario, a part of roads in the urban area of Xi'an, China, to verify the applicability of PLP on real urban roads. This part of the map was downloaded with openstreetmap, as shown in Fig. 2, and all the road data of this part of the map was saved as osm files, and the osm files were converted into readable xml files, which store all the road information, and then vehicle modeling was performed on these real roads. The schematic diagram of the real roads displayed with sumo-gui software is shown in Fig. 3.

3 Secure Transmission Scheme

We use the PLP to analyze the performance of the secure transmission scheme proposed in [14] with the addition of interfering vehicles and artificial noise (AN). The idea of this secure transmission scheme is as follows.

Fig. 2. Map of some roads in Xi'an city, China.

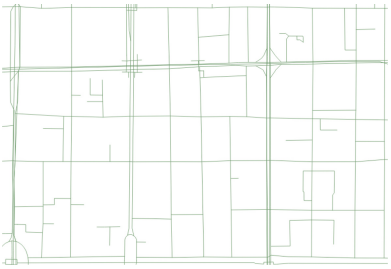

Fig. 3. Modeling diagram of some roads in Xi'an, China.

In order to ensure that the confidential information is transmitted to the legitimate receiving vehicle Bob while causing a certain degree of interference to Eves, Alice transmits confidential messages with AN to Bob, where the predefined channel distribution prevents Bob from receiving interference from AN. Eves tries to capture the confidential information and also receives interference from AN. Charlies transmits jamming signals to interfere with Eves, and due to the preset channel distribution, Bob does not receive the jamming information from Charlies.

The total transmission signal vector s_a formed by the superposition of the confidential information and AN can be expressed as $s_a = \sqrt{P_a\theta}w_a x + \sqrt{\frac{P_a(1-\theta)}{N_a-1}}W_a z_a$, $\sqrt{P_a\theta}w_a x$ denotes the portion of confidential information to be transmitted and $\sqrt{P_a(1-\theta)/(N_a-1)}W_a z_a$ denotes the portion of increased AN interference. where $\theta \in [0,1]$, denotes the ratio of the confidential information power to the total transmit power P_a. $\theta = 1$ means that the message sends only confidential information without AN, and $\theta = 0$ means that the message sends no confidential information to be transmitted. $x \sim CN(0,1)$ denotes the vector of confidential information to be sent to Bob, and $z_a \in C^{N_a-1}$ is an AN vector whose distribution satisfies $CN(0, I_{N_a-1})$. $[w_a, W_a]$ constitutes an orthogonal vector, $w_a = h_{ab}/\|h_{ab}\|$, which is a beamforming precoding vector of h_{ab}, and $W_a \in C^{N_a \times N_a-1}$ denotes the beamforming matrix of AN, which forms a null vector with h_{ab}, that is, $h_{ab}^H W_a = 0$. This setting determines that the AN information will not bring interference to the legitimate receiver Bob.

Meanwhile, the interference signal generated by Charlies will further enhance the security performance. The interference signal of Charlies s_c is designed to interfere Eves without generating interference to Bob. s_c can be expressed as $s_c = \sqrt{\frac{P_c}{N_c-1}} T_c z_c$, where P_c denotes the transmitting power of each Charlie. $T_c \in C^{N_c \times N_c - 1}$ and h_{cb} form the null vector, that is, ${T_c}^H h_{cb} = 0$. This setting determines that Charlies do not interfere Bob. $z_c \sim CN(0, I_{N_c-1})$ is a Gaussian interference signal vector. The received signals from Bob and Eve are denoted as

$$\begin{aligned} y_b &= {h_{ab}}^H s_a {d_{ab}}^{-\frac{\alpha}{2}} + {h_{cb}}^H s_c {d_{cb}}^{-\frac{\alpha}{2}} + n_b \\ &= \sqrt{P_a \theta} || h_{ab} || {d_{ab}}^{-\frac{\alpha}{2}} w_a x + n_b, \end{aligned} \tag{1}$$

$$\begin{aligned} y_k =& \sqrt{P_a \theta} {h_{ek}}^T {d_{ek}}^{-\frac{\alpha}{2}} W_a x + \sqrt{\frac{P_a(1-\theta)}{N_a - 1}} {h_{ek}}^T W_a {d_{ek}}^{-\frac{\alpha}{2}} z_a \\ &+ \sum_{c \in \varphi_c} \sqrt{\frac{P_c}{N_c - 1}} {h_{ck}}^T T_c {d_{ck}}^{-\frac{\alpha}{2}} z_c + n_e, \ k \in \varphi_E, \end{aligned} \tag{2}$$

where d_{ab}, d_{ek} and d_{ck} denote the propagation distances from Alice to Bob, Alice to Eve and Charlie to Eve respectively. $n_b \sim CN(0, {\sigma_b}^2)$ and $n_e \sim CN(0, {\sigma_e}^2)$ denote the independent Gaussian noise variables received by Bob and Eve respectively. α denotes the path loss factor.

According to (1) (2), the SINR (Signal to Interference plus Noise Ratio) received by Bob and Eves respectively is as follows.

$$SINR_b = \frac{P_a \theta \left\| h_{ab} \right\|^2 {d_{ab}}^{-\alpha}}{{\sigma_b}^2}, \tag{3}$$

$$SINR_{ek} = \frac{P_a \theta \left| {h_{ek}}^T w_a \right|^2 {d_{ek}}^{-\alpha}}{\frac{P_a(1-\theta)}{N_a - 1} \left\| {h_{ek}}^T W_a \right\|^2 {d_{ek}}^{-\alpha} + I + {\sigma_e}^2}, \ k \in \varphi_E, \tag{4}$$

where $\frac{P_a(1-\theta)}{N_a-1} \| {h_{ek}}^T W_a \|^2 {d_{ek}}^{-\alpha}$ is the interference to Eves caused by AN. The channel capacity of the legitimate channel and the eavesdropper channel can be expressed as $C_B = log_2(1 + SINR_b)$ and $C_{ek} = log_2(1 + SINR_{ek})$ respectively. They will be used to derive the following performance indicators.

4 Secrecy Performance Analysis

The eavesdropping code can be designed by choosing these two code rates, namely the coding rate R_b and the confidential information rate R_s [15]. R_b and R_s are fixed before data transmission, and the redundancy rate $R_e = R_b - R_s$ is artificially added to interfere Eves. We use the secrecy throughput proposed in [11] to quantify the secrecy performance, which contains coverage probability and secrecy probability.

4.1 Coverage Probability

The coverage probability represents the probability that a legitimate receiver will successfully receive the message sent by the transmitting vehicle and is defined as the probability that C_B can support R_b. The expression of the coverage probability is

$$\begin{aligned} P_c &= P\left[C_B = \log_2\left(1 + SINR_b\right) > R_b\right] \\ &= P\left(SINR_b > \beta = 2^{R_b} - 1\right), \end{aligned} \tag{5}$$

where $SINR_b$ is the SINR received at Bob, $R_b = log_2(1+\beta)$, β is a threshold and $\beta = 2^{R_b} - 1$.

First we derive expressions for the coverage probability under PLP model. We choose an Alice and a Bob as typical vehicles respectively. We assume that Alice is at the round point $(0, 0)$, the distance between Alice and Bob is s_n, y_n is the projected distance of s_n on the y-axis, and x_n is the projected distance of s_n on the x-axis. When discussing the coverage probability for Bob, Eves are not considered, and the preset channel makes Bob receive no interference information from Charlies, so Eves and Charlies do not appear in the model. The expression of P_c is derived as follows.

$$\begin{aligned} & P_c = P\left(SINR_b > \beta\right) \\ &= \int_{s_n} P\left(SINR_b > \beta \mid s_n\right) f_{S_n}\left(s_n\right) ds_n \\ &= \int_{y_n} \int_{s_n} P\left(SINR_b > \beta \mid Y_n\right) f_{Y_n}\left(y_n\right) \cdot f_{S_n}\left(s_n \mid y_n\right) ds_n dy_n \\ &\overset{(a)}{=} \int_0^{\infty} \int_{y_n}^{\infty} P\left(SINR_b > \beta \mid Y_n\right) f_{Y_n}\left(y_n\right) \cdot f_{S_n}\left(s_n \mid y_n\right) ds_n dy_n, \end{aligned} \tag{6}$$

where step (a) follows $s_n \geq y_n$. Next we derive $f_{Y_n}(y_n)$, $f_{S_n}(s_n \mid y_n)$, and $P(SINR_b{>}\beta \mid Y_n)$ respectively, where y_n is the real numerical representation of Y_n and s_n is the real numerical representation of S_n.

Assume that the road where Bob is located is parallel to the y-axis, the vehicles obey the 1D PPP distribution on this road with density λ_v. y_n is the vertical distance from Bob to the x-axis, according to the Probability Distribution Function (PDF) of 1D PPP [16],

$$f_{Y_n}\left(y_n\right) = 2\lambda_v exp\left(-2\lambda_v y_n\right). \tag{7}$$

The conditional CDF for s_n is as follows.

$$\begin{aligned} & F_{S_n}\left(s_n \mid y_n\right) \\ &= P\left(\sqrt{{X_n}^2 + {y_n}^2} < s_n \mid Y_n\right) \\ &= F_{X_n}\left(\sqrt{{s_n}^2 - {y_n}^2} \mid y_n\right) \\ &\overset{(b)}{=} 1 - exp\left(-2\lambda_s \sqrt{{s_n}^2 - {y_n}^2}\right), \end{aligned} \tag{8}$$

where step (b) because the vertical distance of the road where Bob is located from the y-axis is x_n, and x_n obeys the 1D PPP distribution with density λ_s. $f_{S_n}(s_n \mid y_n)$ can be derived from $F_{S_n}(s_n \mid y_n)$ as follows.

$$f_{S_n}(s_n \mid y_n) = \frac{2\lambda_s s_n}{\sqrt{s_n^2 - y_n^2}} exp\left(-2\lambda_s \sqrt{s_n^2 - y_n^2}\right). \tag{9}$$

The expression of $P(SINR_b > \beta \mid Y_n)$ is derived as follows.

$$\begin{aligned} &P(SINR_b > \beta \mid Y_n) \\ &= P\left(\frac{P_a \theta \left\|h_{ab}\right\|^2 {s_n}^{-\alpha}}{{\sigma_b}^2} > \beta \mid Y_n\right) \\ &= P\left(\|h_{ab}\|^2 > \frac{\beta {s_n}^{\alpha} {\sigma_b}^2}{P_a \theta} \mid Y_n\right) \\ &\overset{(c)}{=} \sum_{k=0}^{N_a - 1} \left(\frac{\beta {s_n}^{\alpha} {\sigma_b}^2}{P_a \theta}\right)^k \cdot \frac{1}{k!} \cdot exp\left(-\frac{\beta {s_n}^2 {\sigma_b}^2}{P_a \theta}\right). \end{aligned} \tag{10}$$

Step (c) because $\|h_{ab}\|^2 \sim \Gamma(N_a, 1)$, according to the CDF of gamma distribution, $P(\|h_{ab}\|^2 \leq x) = 1 - \sum_{k=0}^{N_a - 1} \frac{x^k}{k!} \cdot exp(-x)$. According to (6) (7) (9) (10), we can derive P_c under the PLP model.

To verify that PLP model is more applicable to urban scenarios, we compare P_c under PLP modeling with that under 2D PPP modeling. We derived the expressions for the coverage probability P_c under 2D PPP modeling as follows.

Due to space limitation, some of the derivation procedures similar to MPLP are not repeated in the 2D PPP derivation. Only the simple derivation results of 2D PPP are given here. Under the 2D PPP model, assuming Alice is at the circle point $(0, 0)$ and the distance from Bob to Alice is r.

$$P_c = P(SINR_b > \beta) = \int_0^{\infty} P(SINR_b > \beta \mid r) f_r(r) dr. \tag{11}$$

$$f_r(r) = 2\pi\lambda r exp\left(-\lambda \pi r^2\right). \tag{12}$$

$$P(SINR_b > \beta \mid r) = \sum_{k=0}^{N_a - 1} \left(\frac{\beta r^{\alpha} {\sigma_b}^2}{P_a \theta}\right)^k \frac{1}{k!} \cdot exp\left(-\frac{\beta r^{\alpha} {\sigma_b}^2}{P_a \theta}\right). \tag{13}$$

P_c under the 2D PPP model are derived from (11) (12) (13).

4.2 Secrecy Probability

Secrecy probability is defined as the probability that the capacity of the eavesdropping channel is lower than the rate redundancy R_e. The expression of secrecy probability is

$$\begin{aligned} P_{sec} &= P\left[C_E = log_2(1 + SINR_e) < R_e\right] \\ &= P\left(SINR_e < \gamma = 2^{R_e} - 1\right), \end{aligned} \tag{14}$$

where $SINR_e$ is the SINR received at Eves, $R_e = log_2(1+\gamma)$, γ is a threshold and $\gamma = 2^{R_e} - 1$.

First we derive P_{sec} under Poisson line process modeling model. We choose an Alice and an Eve as typical vehicles respectively. Suppose Eve is at the round point $(0,0)$, s_n is the distance between Alice and Eve, y_n is the projected distance of s_n on the y-axis and x_n is the projected distance of s_n on the x-axis. When discussing P_{sec} for Eves, we do not consider Bob. The expression of P_{sec} is derived as follows.

$$\begin{aligned} P_{sec} &= P\left(SINR_e < \gamma\right) \\ &= \int_0^{\infty} \int_{y_n}^{\infty} P\left(SINR_e < \gamma \mid Y_n\right) f_{Y_n}\left(y_n\right) f_{S_n}\left(s_n \mid y_n\right) ds_n dy_n. \end{aligned} \tag{15}$$

The derivation of (15) is similar as (6), we do not repeat the detailed derivation process here. Next we will derive $f_{Y_n}(y_n)$, $f_{S_n}(s_n \mid y_n)$ and $P(SINR_e{<}\gamma \mid Y_n)$ respectively. $f_{Y_n}(y_n)$ is derived in (7) and $f_{S_n}(s_n \mid y_n)$ is derived in (9) without repeating the derivation. $P(SINR_e{>}\gamma \mid Y_n)$ is derived as follows.

$$\begin{aligned} & P\left(SINR_e > \gamma \mid Y_n\right) \\ & \overset{(b)}{=} P\left(\frac{P_a \theta \left|{h_{ek}}^T w_a\right|^2 {s_n}^{-\alpha}}{\frac{P_a(1-\theta)}{N_a-1}\left\|{h_{ek}}^T W_a\right\|^2 {s_n}^{-\alpha} + I + {\sigma_e}^2} > \gamma \mid Y_n\right) \\ & \overset{(c)}{=} E_I\left[P\left(\left|{h_{ek}}^T w_a\right|^2 > \gamma \frac{(1-\theta)}{\theta} + \frac{\gamma\left(I + {\sigma_e}^2\right){s_n}^{\alpha}}{P_a \theta} \mid Y_n, I\right)\right] \\ & \overset{(d)}{=} exp\left(-\frac{\gamma(1-\theta)}{\theta}\right) exp\left(-\frac{\gamma {\sigma_e}^2 {s_n}^{\alpha}}{P_a \theta}\right) L_I\left(s \mid Y_n\right)\Big|_{s=\frac{\gamma {s_n}^{\alpha}}{P_a \theta}}. \end{aligned} \tag{16}$$

The interference $I = \sum_{c \in \varphi_c} \frac{P_c}{N_c - 1}\left\|h_{ck}^T T_c\right\|^2 d_{ck}^{-\alpha}$ in step (b). Step (c) is derived since $\left\|h_{ek}^T W_a\right\|^2 \sim \Gamma\left(N_a - 1, 1\right)$ and the mean value of $\left\|h_{ek}^T W_a\right\|^2$ is $N_a - 1$. Step (d) is derived due to $\left|h_{ek}^T w_a\right|^2 \sim \exp(1)$ and the mean value of $\left|h_{ek}^T w_a\right|^2$ is 1 and $E_I\left(e^{-AI}\right) = L_I(s)|_{s=A} = \int_I e^{-AI} f_I(I) dI$, where $A = \frac{\gamma s_n^{\alpha}}{P_a \theta}$. $f(I)$ is PDF of I, and $L_I(s)$ is the Laplace transform of I. I is divided into two parts, which are the interfering vehicles I_0 on the same road as the typical vehicle Eve (referred to as typical road in the following paper) and the interfering vehicles I_n on the other roads, the expression of $L_I(s)$ is as follows.

$$L_I\left(s \mid Y_n\right) = L_{I_0}\left(s \mid Y_n\right) \cdot L_{I_n}\left(s \mid Y_n\right). \tag{17}$$

The expression of $L_{I_0}(s|Y_n)$ is derived as follows.

$$
\begin{aligned}
&L_{I_0}\left(s \mid Y_n\right)=E\left[e^{-sI_0}\right] \\
&=E\left[E_{G_{0I_0}}\left[\prod_{I_0} exp\left(-s\frac{P_c}{N_c-1}G_{0I_0}x^{-\alpha}\right)\right]\right] \\
&\overset{(a)}{=}E\left[\prod_{I_0}\left(1+\frac{sP_cx^{-\alpha}}{N_c-1}\right)^{-(N_c-1)}\right] \\
&\overset{(b)}{=}exp\left[-2\lambda_v\int_{s_n}^{\infty}\left(1-\left(1+\frac{sP_cx^{-\alpha}}{N_c-1}\right)^{-(N_c-1)}\right)dx\right].
\end{aligned}
\tag{18}
$$

G_{0I_0} represents the channel between Charlies and Eves. Step (a) is derived due to $||h_{ck}^T T_c||^2 \sim \Gamma\left(N_c-1,1\right)$ and the Moment Generating Function (MGF) of gamma distribution, step (b) is derived from the Probability Generating Function (PGF) of the 1D PPP [17], and assume that the distance $x>s_n$ from the interfering vehicle to the round point.

Then the expression of $L_{I_n}(s \mid Y_n)$ is derived as follows.

$$
\begin{aligned}
&L_{I_n}\left(s \mid Y_n\right)=E\left[\prod_{y} L_{I_0}\left(s \mid Y_n\right)\right] \\
&=exp\left[-2\lambda_s\int_0^{s_n} 1-exp\left(-2\lambda_v\int^{\infty}\sqrt{s_n^2-y^2}\right.\right. \\
&\left.\left.1-\left(1+\frac{sP_c\left(x^2+y^2\right)^{-\frac{\alpha}{2}}}{N_c-1}\right)^{-(N_c-1)}dx\right)dy\right].
\end{aligned}
\tag{19}
$$

where assuming that the coordinates of the interfering vehicle position (x,y) satisfies $x^2+y^2>{s_n}^2$. $L_I(s \mid Y_n)$ is derived from (17)–(19). $P(SINR_e>\gamma \mid Y_n)$ is derived from (16)–(19), and then

$$
P_r\left(SINR<\gamma \mid Y_n\right)=1-P\left(SINR_e>\gamma \mid Y_n\right). \tag{20}
$$

P_{sec} for the Poisson line process modeling can be derived from (7) (9) and (15)–(20).

In order to verify that PLP model is more applicable to urban scenarios, we compare P_{sec} under PLP model with those under the 2D PPP model. P_{sec} under 2D PPP model is shown as follows.

Assume that the typical vehicle Eve is at the circle point $(0,0)$ and the distance from Alice to Eve is r.

$$
P_{sec}=P\left(SINR_e<\gamma\right)=\int_0^{\infty} P\left(SINR_e<\gamma \mid r\right) f_r(r)dr. \tag{21}
$$

$$
\begin{aligned}
&P\left(SINR_e>\gamma \mid r\right) \\
&=exp\left(-\frac{\gamma(1-\theta)}{\theta}\right)exp\left(-\frac{\gamma{\sigma_e}^2r^{\alpha}}{P_a\theta}\right)L_I(s \mid r)\Big|_{s=\frac{\gamma r^{\alpha}}{P_a\theta}}.
\end{aligned}
\tag{22}
$$

$$L_I(s \mid r) = exp\left[-2\pi\lambda \int_r^{\infty} x\left(1-\left(1+\frac{sP_c x^{-\alpha}}{N_c-1}\right)^{-(N_c-1)}\right)dx\right]. \tag{23}$$

$$P\left(SINR_e<\gamma \mid r\right) = 1 - P\left(SINR_e>\gamma \mid r\right). \tag{24}$$

P_{sec} under the 2D PPP model are derived from (12) and (21)–(24).

4.3 Secrecy Throughput

We use the secrecy throughput proposed in the literature [11] to quantify the confidentiality performance, which contains both P_c and P_{sec}. The secrecy throughput η is defined as the rate of information, in bps, transmitted from the legitimate source node to the destination node in complete secrecy, and the expression for secrecy throughput η is

$$\eta = P_c \cdot P_{sec} \cdot R_s \tag{25}$$

The relationship between the η and each influencing factor is studied in order to analyze how to choose the appropriate parameters to ensure that the information is reliably transmitted to the receiver while not leaking to the eavesdropper. That is, the confidential information sent by Alice is received by the legitimate receiver Bob, to ensure the transmission quality. Meanwhile, the confidential information sent by Alice is not eavesdropped by Eves as much as possible, so that the confidential information is not leaked, that is, secure transmission is guaranteed.

However, the above two situations cannot be satisfied at the same time, but are mutually restrictive. For example, the more confidential information Alice sends, the more confidential information Bob receives and the greater P_c. But at the same time, the more confidential information Eves receives, the less P_{sec}. The next section analyzes how to select the appropriate parameters to achieve a balance between P_c and P_{sec} by studying the relationship between η and related parameters.

5 Simulation Results and Analysis

In this section, we plot the graphs of coverage probability, secrecy probability and secrecy throughput versus each important parameter under PLP and 2D PPP model respectively. In order to make the theoretical results more convincing, we chose a typical urban scenario - part of the roads in the urban area of Xi'an, China, modeled the vehicles on real roads and simulated the communication performance of the vehicles, compared the performance curves under two models with those under real urban road. The simulation modeling parameters are shown in Table 1.

Table 1. Parameters of Simulation

Parameter	Value
λ_s	0.001
λ_v	0.05
α	7
$noise$	10^{-20}
$P_a(dBm)$	30
$P_c(dBm)$	30

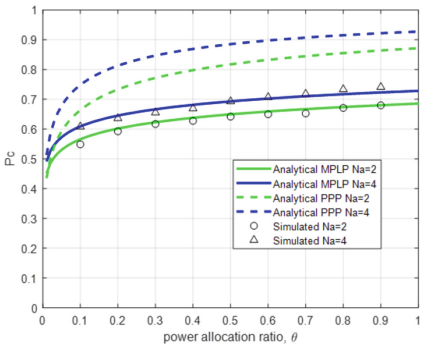

Fig. 4. Coverage probability versus confidential information power ratio θ, $R_b = 3$. (Color figure online)

5.1 Coverage Probability Simulation Results and Analysis

As shown in Fig. 4, the larger θ is, the more confidential information Alice transmits to Bob and the larger P_c is. The curves of different colors in the figure represent different antenna numbers of Alice, the more antennas Alice has, the larger P_c. We can improve the P_c by appropriately increasing θ or N_a.

The solid and dashed lines represent P_c under PLP and 2D PPP model respectively, the black triangles and black circles indicate P_c derived from vehicle modeling on some roads in Xi'an urban area with different N_a. We can find that the curves of the real urban scenario match better with those under PLP model, which indicates that the PLP model is more applicable to the modeling of urban scenarios than 2D PPP. This conclusion can be drawn from all the graphs below, so it is not repeated in the following. And the phenomenon that the theoretical curves fit the curves of the real scenarios proves the correctness of the theoretical formulation derived above. According to $\beta = 2^{R_b} - 1$, different R_b represents different threshold β. We can find in Fig. 5 that the lower β, the larger P_c. We conclude that P_c can be improved by appropriately decreasing the preset R_b value from the figure.

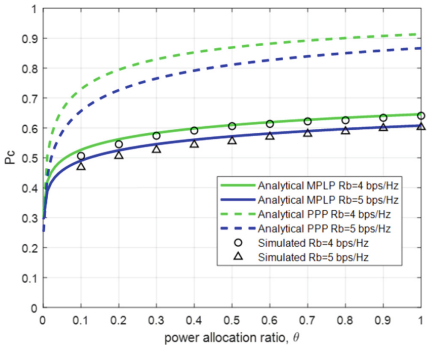

Fig. 5. Coverage probability versus confidential information power ratio θ, $N_a = 2$.

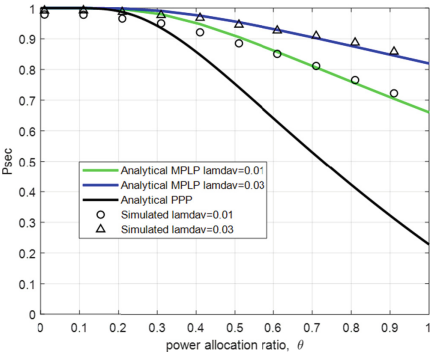

Fig. 6. Secrecy probability versus confidential information power ratio θ, $R_e = 1$, $N_c = 4$. (Color figure online)

5.2 Secrecy Probability Simulation Results and Analysis

As shown in Fig. 6, the larger θ, the more effective information sent to the eavesdropping vehicle Eves, the smaller the interference caused by AN to Eves, the smaller P_{sec}, and the worse the security performance. We can learn that decreasing θ can improve P_{sec} and thus improve security performance.

The blue and green curves in Fig. 6 represent different densities of interfering vehicles, we can find that the higher the density of interfering vehicles, the higher P_{sec}. This is because the greater the density of interfering vehicles, the greater the interference of Charlies to Eves, the greater the P_{sec}, and the better the secrecy performance. Therefore, we can increase P_{sec} by appropriately increasing the density of interfering vehicles, thus improving the secrecy performance. According to $\gamma = 2^{R_e} - 1$, different R_e represents different threshold γ. We can find that in Fig. 7, the larger γ, the higher P_{sec}. We can increase the size of R_e appropriately by changing the preset R_b and R_s to improve P_{sec}. We can find in Fig. 8 that the more N_c, the higher P_{sec}. This is because N_c, the more the interference to Eves, so the higher P_{sec} and the better secrecy performance.

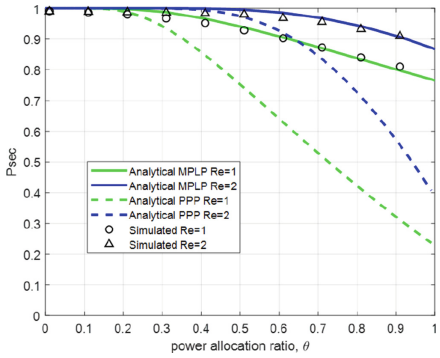

Fig. 7. Secrecy probability versus confidential information power ratio θ, $\lambda_v = 0.02$, $N_c = 4$.

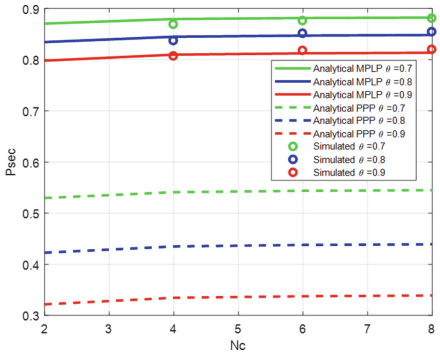

Fig. 8. Secrecy probability versus confidential information power ratio θ, $R_e = 1$, $\lambda_v = 0.02$.

Therefore, we can increase N_c to improve the P_{sec} and thus improve the secrecy performance. Different color curves represent different θ. We can see that the larger θ, the lower the P_{sec}, the reason is that the higher θ, the more secrecy information transmit to Eves, the lower P_{sec}.

5.3 Secrecy Throughput Simulation Results and Analysis

From Fig. 9, it can be seen that η increases and then decreases with the increase of θ. The reason is that as θ increases, the confidential information received by the receiving vehicle Bob increases, and P_c improves. At the same time, the secrecy information received by Eves also increases and the P_{sec} decreases. We can try to choose the parameter θ near the peak point so that Bob receives as much confidential information as possible, and Eves eavesdrops on as little confidential information as possible. The parameters can also be selected appropriately according to the specific needs in different situation. For example, for high security performance requirements, the parameter θ with the peak point a

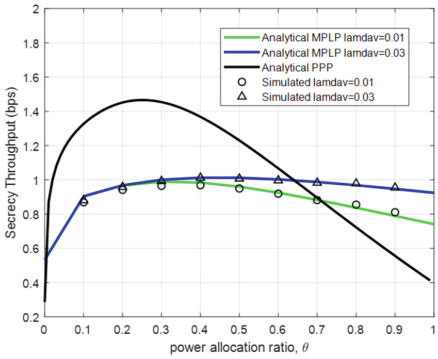

Fig. 9. Secrecy throughput versus confidential information power ratio θ with different interfering vehicle densities, $N_a = 2$. (Color figure online)

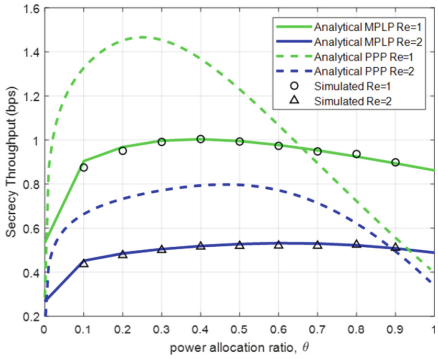

Fig. 10. Secrecy throughput versus confidential information power ratio θ with different R_e, $N_a = 2$.

little to the left can be chosen to achieve a higher P_{sec} at the expense of the P_c appropriately.

The blue and green curves in Fig. 9 indicate different interfering vehicle densities. We can find that the higher the density of interfering vehicles, the higher η, so increasing the density of interfering vehicles can increase η. The different color curves in Fig. 10 indicate different R_e. We can find that the larger R_e, the smaller η. That is because $\eta = P_c \cdot P_{sec} \cdot R_s$, and $R_s = R_b - R_e$. With P_c, P_{sec} andR_b determined, the larger R_e and the smaller R_s, the smaller η.

6 Conclusion

In this paper, we use Poisson line process model to model urban scenarios of V2X, and derive coverage probability, secrecy probability and secrecy throughput based on a secure transmission scheme with the addition of interfering vehicles and artificial noise using stochastic geometry. Some effective conclusions are

drawn to improve secrecy performance by controlling the parameters. At the same time, we verify that the Poisson line process model is more suitable for modeling urban scenarios by modeling vehicles on the real urban map.

Acknowledgement. This work was supported in part by the State Major Science and Technology Special Projects (Grant No. 2018ZX03001024) and in part by the National Key Research and Development Program (Grant No. 2022YFF0610303).

References

1. Chen, X., Ng, D., Gerstacker, W.H., et al.: A survey on multiple-antenna techniques for physical layer security. IEEE Commun. Surv. Tutor. **19**, 1027–1053 (2017)
2. Furqan, H.M., Solaija, M.S.J., Arslan, H.: Intelligent physical layer security approach for V2X communication. arXiv preprint (2019). https://arxiv.org/pdf/1905.05075.pdf
3. ElHalawany, B.M., El-Banna, A.A.A., Wu, K.: Physical-layer security and privacy for vehicle-to-everything. IEEE Commun. Mag. **57**(10), 84–90 (2019). https://doi.org/10.1109/MCOM.001.1900141
4. Xu, L., Yu, X., Wang, H., et al.: Physical layer security performance of mobile vehicular networks. Mob. Netw. Appl. **25**(4) (2019)
5. Wu, Y., Qian, L.P., Mao, H.W., et al.: Secrecy-driven resource management for vehicular computation offloading networks. IEEE Netw. **32**(3), 84–91 (2018)
6. Tolossa, Y.J., Vuppala, S., Kaddoum, G., Abreu, G.: On the uplink secrecy capacity analysis in D2D-enabled cellular network. IEEE Syst. J. **12**(3), 2297–2307 (2018)
7. Hu, X., Mu, P., Wang, B., Li, Z.: On the secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers. IEEE Trans. Veh. Technol. **26**(5), 4457–4462 (2019)
8. Ma, R., Yang, S., Du, M., Ou, J.: Improving physical layer security jointly using full-duplex jamming receiver and multi-antenna jammer in wireless networks. IET Commun. **13**(10), 1530–1536 (2019)
9. Si, J., Cheng, Z., Li, Z., Cheng, J., Wang, H.-M., Al-Dhahir, N.: Cooperative jamming for secure transmission with both active and passive eavesdroppers. IEEE Trans. Commun. **68**(9), 5764–5777 (2020). https://doi.org/10.1109/TCOMM.2020.3003946
10. Dhillon, H.S., Chetlur, V.V.: Poisson line cox process: foundations and applications to vehicular networks (2020)
11. Tang, Z., Sun, Z., Li, C., et al.: Reliability performance of transmitter selection in wireless vehicular networks. In: 2020 IEEE/CIC International Conference on Communications in China (ICCC). IEEE (2020)
12. Hu, L., Wen, H., Wu, B., Tang, J., Pan, F., Liao, R.-F.: Cooperative jamming aided secrecy enhancement in wireless networks with passive eavesdroppers. IEEE Trans. Veh. Technol. **67**(3), 2108–2117 (2018)
13. Yang, Y., Wang, W., Zhao, H., Zhao, L.: Transmitter beamforming and artificial noise with delayed feedback: secrecy rate and power allocation. J. Commun. Netw. **14**(4), 374–384 (2012)
14. Qiu, B., Jing, C.: Performance analysis for cooperative jamming and artificial noise aided secure transmission scheme in vehicular communication network (2020)
15. Klinc, D., Ha, J., McLaughlin, S.W., Barros, J., Kwak, B.-J.: LDPC codes for the Gaussian wiretap channel. IEEE Trans. Inf. Forensics Secur. **6**(3), 532–540 (2011)

16. Krishnan, S., Dhillon, H.S.: Spatio-temporal interference correlation and joint coverage in cellular networks. IEEE Trans. Wirel. Commun. **16**(9), 5659–5672 (2017)
17. Sial, M.N., Deng, Y., Ahmed, J., Nallanathan, A., Dohler, M.: Stochastic geometry modeling of cellular V2X communication on shared uplink channels (2018)