Research Square

Preprints are preliminary reports that have not undergone peer review. They should not be considered conclusive, used to inform clinical practice, or referenced by the media as validated information.

Performance Analysis for Cooperative Jamming and Artificial Noise Aided Secure Transmission Scheme in Vehicular Communication Network

Bin Qiu (qiubin1122@126.com)

Guilin University of Electronic Technology https://orcid.org/0000-0002-8523-7431

Chao Jing

Guilin University of Technology

Research

Keywords: Vehicular communication, imperfect channel state information (CSI), physical layer security (PLS), artificial noise (AN), cooperative jamming, secrecy throughput, power allocation

Posted Date: July 28th, 2020

DOI: https://doi.org/10.21203/rs.3.rs-45614/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

RESEARCH

Performance Analysis for Cooperative Jamming and Artificial Noise Aided Secure Transmission Scheme in Vehicular Communication Network

Bin Qiu[1,2*†] and Chao Jing[2,3]

*Correspondence: qiubin1122@126.com
[2]College of Information Science and Engineering, Guilin University of Technology, Jiangan Road, 541004 Guilin, China
Full list of author information is available at the end of the article
†Equal contributor

Abstract

Vehicular communication has emerged as a supporting technique for improving road traffic safety and efficiency in the intelligent transportation system (ITS). However, the wireless vehicular communication links may suffer from an eavesdropping threat due to the wireless broadcasting nature and high-mobility of vehicles. In practice, artificial noise (AN) assisted beamforming scheme can be utilized for fighting against multiple malicious eavesdroppers. Unfortunately, channel estimation errors caused by the high-mobility of vehicles may lead to noise leakage at the legitimate receiver, thus resulting significant loss in the secrecy performance. In this paper, a joint cooperative jamming and AN aided secure transmission scheme is proposed in vehicular communication network by considering the imperfect channel state information(CSI). In this scheme, cooperative jammers are utilized for further enhancing physical layer security. We derive the closed-form expressions of the connection and secrecy outage probabilities in the presence of AN leakage and signal offset using a stochastic geometry approach. Furthermore, the proposed scheme is capable of maximizing the secrecy throughput in terms of relative vehicular velocity for balancing both the reliability and security of the legitimate link. We further comprehensively analyze the effect of key system parameters on secrecy performance through asymptotic analysis. Finally, the effectiveness of the proposed scheme is validated by numerical results.

Keywords: Vehicular communication; imperfect channel state information (CSI); physical layer security (PLS); artificial noise (AN); cooperative jamming; secrecy throughput; power allocation

Introduction

Vehicular communication is believed as a emerging technology to improve the road safety, transport efficiency and driving experience in the intelligent transportation system (ITS) and future autonomous transport system [1, 2]. Messages can be disseminated quickly by exploiting the paradigm of vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications in vehicular network [3]. However, due to the broadcast nature of wireless medium, malicious vehicles may eavesdrop or jam the vehicular communication links for their own profit, which can threaten driving safety and jeopardize ITS efficiency [4, 5]. Therefore, the information security is a key issue in the development applications of vehicular network [3, 4, 5]. This motivates the research on vehicular communication from the perspective of communication security [6].

Recently, the information security has gained a lot of attention in vehicular network [7, 8], where improving the communication security is usually focused by the cryptographic methods on upper layers at the expense of increased computational and communication overheads. Motivated by this, physical layer security (PLS) has been envisioned a supporting technique for guaranteeing security of vehicular communication [9]. Based on the celebrated theoretical analyses of PLS, artificial noise (AN), secure beamforming, and cooperative security strategies have been proposed for enhancing the secrecy performance [10]. Among all these strategies, AN aided multi-antenna transmission strategy is of great significance PLS approach to degrade the eavesdropping channel [11, 12, 13]. In [14], both sectoring and AN schemes for secrecy enhancing were investigated in the wireless network, where the reliability-security tradeoff was analyzed. In [15], a AN-aided multi-antenna secure transmission scheme was studied in presence of randomly distributed eavesdroppers with perfect channel state information (CSI). However, both [14] and [15] ignored the impact of imperfect CSI on designing the AN. In particular, such a given perfect CSI assumption is hard to justify in vehicular network due to an error of estimation, outdated CSI, and limited CSI feedback [16, 17, 18, 19]. Considering the influence of imperfect CSI caused by the high-mobility of vehicles on signal transmission, the AN may leak into the legitimate channel (i.e., AN leakage problem) [19], which affects link reliability and leads to erroneous security evaluation in vehicular network.

Following the idea of AN, cooperative jamming (CJ) was investigated as an effective method to further enhance secrecy of wireless communications [20]. In the CJ scheme, the friendly jammers are capable of emitting jamming signals to protect information security of the legitimate users against malicious eavesdroppers [21, 22, 23]. However, in most of the above works, a common assumption is that source node is equipped with single antenna. Different from the above works, our work mainly focus on the AN aided multi-antenna secure transmission. The works in [24, 25, 26, 27] provided a CJ strategy for guaranteeing security in multi-antenna transmission system. However, only a jammer and a limited number of eavesdropping nodes are considered in the proposed works, which leads to a limited application scope.

Motivated by [26], we focus on designing a joint CJ and AN aided secure transmission scheme for vehicular communication network under an imperfect CSI, where the communication is exposed to the jammers and eavesdroppers with unknown number and locations. In this paper, we derive the closed-form expressions of the connection and secrecy outage probabilities in the presence of AN leakage and signal offset using a stochastic geometry approach. Furthermore, for balancing the reliability and security of the legitimate link, the closed-form expression for security throughput is gave out in terms of relative vehicular velocity and the optimal power allocation ratio is optimized for the reliability-security tradeoff. Finally, the effects of the key system parameters (e.g., the number of transmit antennas, the relative vehicular velocity, the density ratio of jammers and eavesdroppers, the power allocation ratio, the power of jammers) on the secrecy performance are comprehensively analyzed.

The remainder of this paper is organized as follows. Section II presents the system model. Section III proposes a joint CJ and AN aided secure transmission scheme. Section IV presents the performance metrics. The numerical results and discussions

for the proposed scheme are providesd by MATLAB in Section V. Finally, the conclusions are drawn in Section VI.

Notations: We use bold lowercase and uppercase letters to denote column vectors and matrices, respectively. $\mathbf{I}_n$ denotes the $n \times n$ identity matrix. $Pr\{\cdot\}$, $\|\cdot\|$, $|\cdot|$, and $(\cdot)^T$ denote probability, Euclidean norm, absolute value, and transpose, respectively. $\exp(\lambda)$, $T(N, \lambda)$ and $\mathcal{CN}\left(\mu, \sigma^2\right)$ denote exponential distribution with parameter λ, gamma distribution with parameters N and λ, and circularly symmetric complex Gaussian distribution with mean μ and variance σ^2, respectively. $\mathcal{L}(\cdot)$ denotes the Laplace transforms of a random variable. Finally, $C^{m\times n}$ denotes the $m \times n$ complex number domain.

1 System Model

Figure 1 Joint CJ and AN aided secure transmission model. Legends: Alice aims to transmit confidential message to Bob, in the presence of randomly located passive eavesdropper Eves trying to capture the confidential information. In addition, there also exist cooperative jammers (Charlies) emit interference signals to confuse Eves.

As shown in Fig. 1, we consider a joint CJ and AN aided secure transmission model in vehicular communication network, where a vehicle (Alice) aims to transmit confidential message to another legitimate vehicle (Bob), in the presence of randomly located passive eavesdropper vehicles (Eves) trying to capture the confidential information. In addition, there also exist cooperative jammers (Charlies) emit interference signals to confuse Eves. Note here Charlies act as pure cooperative jammers without information forwarding [25]. The sets of Eves and Charlies are defined as $\mathcal{K} = \{1, 2, \ldots, K\}$ and $\mathcal{C} = \{1, 2, \ldots, C\}$. For convenience, we refer to the k-th Eve as E_k and the c-th Charlie as C_c. We assume that each Charlie and Alice are equipped with N_c and N_a antennas, respectively. Each Eve and Bob are all equipped with single antenna [26]. Without loss of generality, the spatial locations of Eves and Charlies are denoted as characterized by two independent homogeneous Poisson Point Processes (PPPs) Φ_e and $\Phi_c$with the intensities λ_e and λ_c over the two-dimensional plane, respectively.

All the communication links undergo a standard path-loss characterized by the exponent α and the channels are quasi-static Rayleigh fading, where the fading coefficients are assumed to vary from one block to another, while keeping constant during a transmission block for simplicity [18, 28]. All fast fading channels from Alice to Bob and E_k are denoted by $\mathbf{h}_{a,b} \in \mathbb{C}^{N_a}$ and $\mathbf{h}_{e,k} \in \mathbb{C}^{N_a}$, respectively, and those from Charlie to Bob and E_k are denoted by $\mathbf{h}_{c,b} \in \mathbb{C}^{N_c}$ and $\mathbf{h}_{c,k} \in \mathbb{C}^{N_c}$. We assume Bob estimates the intended channel with estimation errors [16]. In this case, we use a first-order Gauss-Markov model to depict the fast fading variation [29], the exact intended channel $\mathbf{h}_{a,b}$ can be modeled as

$$\mathbf{h}_{a,b} = \widetilde{\mathbf{h}}_{a,b} + \mathbf{e}_{a,b}, \tag{1}$$

where the estimated value $\widetilde{\mathbf{h}}_{a,b} \sim \mathcal{CN}\left(0, \rho^2 \mathbf{I}_{N_a}\right)$ is independent of the channel estimation errors $\mathbf{e}_{a,b} \sim \mathcal{CN}\left(0, (1-\rho^2)\mathbf{I}_{N_a}\right)$. We consider $\rho \in [0, 1]$ as channel estimation accuracy [16]. Note that $\rho = 0$ indicates that no CSI is obtained at all,

while $\rho = 1$ means a perfect channel estimation. For the Jakes' fading model, ρ is given by $\rho = J_0(2\pi f_d T)$, where $J_0(\cdot)$ is the zero-order Bessel function of the first kind, T is the block duration time, and $f_d = \nu f_c/c$ is the maximum Doppler frequency with $c = 3\times10^8$ m/s, ν being the relative vehicular velocity, and f_c being the carrier frequency [16]. For simplicity, the CSI of Charlies and Eves are available [28]. Specifically, we assume that $\mathbf{h}_{e,k} \sim \mathcal{CN}(0, \mathbf{I}_{N_a})$ and $\mathbf{h}_{c,k} \sim \mathcal{CN}(0, \mathbf{I}_{N_c})$.

2 Secure Transmission Scheme

For confusing Eves while ensuring a secure transmission, Alice adopts the AN-aided beamforming transmission strategy to emit confidential information along with AN. Let $[\mathbf{w}_a,\ \mathbf{W}_a]$ constitute an orthogonal basis, where $\mathbf{w}_a = \widetilde{\mathbf{h}}^*_{a,b}/\left\|\widetilde{\mathbf{h}}_{a,b}\right\|$ is the beamforming precoding vector with $\widetilde{\mathbf{h}}_{a,b}$ being the estimate of channel $\mathbf{h}_{a,b}$, and $\mathbf{W}_a \in \mathbb{C}^{N_a\times N_a-1}$ denotes an AN beamforming matrix onto the null-space of $\widetilde{\mathbf{h}}_{a,b}$, i.e., $\widetilde{\mathbf{h}}^H_{a,b}\mathbf{W}_a = 0$. The AN-aided transmitted signal vector $\mathbf{s}_a$ can be formulated as

$$\mathbf{s}_a = \sqrt{P_a\theta}\mathbf{w}_a x + \sqrt{P_a(1-\theta)/(N_a-1)}\mathbf{W}_a\mathbf{z}_a, \tag{2}$$

where $\theta \in [0,1]$ is the ratio of information-bearing signal power to Alice' total transmit power P_a . Note that $\theta = 1$ indicates the secrecy beamforming without AN, and $\theta = 0$ denotes that the confidential information transmission is suppressed. $x \sim \mathcal{CN}(0,1)$ indicates the secret message for Bob. $\mathbf{z}_a \in \mathbb{C}^{N_a-1}$ is an AN vector with distribution $\mathcal{CN}(0, \mathbf{I}_{N_a-1})$.

Concurrently, the zero-forcing technique is utilized at Charlies. These external jamming signals generated by Charlies will further enhance security performance [25]. The jamming signal $\mathbf{s}_c$ at each Charlie should be properly designed to jam Eves while eliminating the additional interference at Bob. Therefore, $\mathbf{s}_c$ can be design as

$$\mathbf{s}_c = \sqrt{P_c/(N_c-1)}\mathbf{T}_c\mathbf{z}_c, \tag{3}$$

where P_c denotes the transmit power of each Charlie. $\mathbf{T}_c \in \mathbb{C}^{N_c\times(N_c-1)}$ constitutes an orthonormal basis for the null-space of $\mathbf{h}_{c,b}$, i.e., ${\mathbf{T}_c}^H\mathbf{h}_{c,b} = 0$. $\mathbf{z}_c \sim \mathcal{CN}(0, \mathbf{I}_{N_c-1})$ is a Gaussian jamming signals vector. Alice and Charlies simultaneously transmit confidential and jamming signals. The received signals at Bob and E_k can be respectively expressed as

$$y_b = \sqrt{P_a\theta}\left\|\widetilde{\mathbf{h}}_{a,b}\right\| d_{a,b}^{-\frac{\alpha}{2}} x + \mathbf{e}^T_{a,b}\mathbf{W}\mathbf{x}^T_a d_{a,b}^{-\frac{\alpha}{2}} + n_b, \tag{4}$$

$$\begin{aligned} y_k = &\sqrt{P_a\theta}\mathbf{h}^T_{e,k} d_{e,k}^{-\frac{\alpha}{2}}\mathbf{w}_a x \\ &+\sqrt{P_a(1-\theta)/(N_a-1)}\mathbf{h}^T_{e,k}\mathbf{W}_a d_{e,k}^{-\frac{\alpha}{2}}\mathbf{z}_a \\ &+\sum_{c\in\Phi_c}\sqrt{P_c/(N_c-1)}\mathbf{h}^T_{c,k}\mathbf{T}_c d_{c,k}^{-\frac{\alpha}{2}}\mathbf{z}_c + n_e,\ k\in\Phi_E, \end{aligned} \tag{5}$$

where $d_{a,b}$, $d_{e,k}$ and $d_{c,k}$ denote the propagation distance from Alice to Bob, from Alice to the E_k, and from the C_c to the E_k, respectively. $n_b \sim \mathcal{CN}\left(0, \sigma_b^2\right)$ and $n_k \sim \mathcal{CN}\left(0, \sigma_e^2\right)$ are independent variables denoting the terminal Gaussian noises.

$\mathbf{W} = [\mathbf{w}_a \;\; \mathbf{W}_a]$, and $\mathbf{x}_a = [\sqrt{P_a\theta}x \quad \sqrt{P_a(1-\theta)/(N_a-1)}\mathbf{z}_a]$. According to (4)-(5), the signal-to-interference-plus-noise ratios (SINRs) at Bob and E_k can be given by

$$\gamma_b = \frac{P_a\theta\left\|\widetilde{\mathbf{h}}_{a,b}\right\|^2 d_{a,b}^{-\alpha}}{P_a\theta\|\mathbf{e}_{a,b}\mathbf{w}_a\|^2 d_{a,b}^{-\alpha} + P_a(1-\theta)\|\mathbf{e}_{a,b}\mathbf{W}_a\|^2 d_{a,b}^{-\alpha}/(N_a-1)+\sigma_b^2}, \tag{6}$$

$$\gamma_{e,k} = \frac{P_a\theta\left|\mathbf{h}_{e,k}^T\mathbf{w}_a\right|^2 d_{e,k}^{-\alpha}}{P_a(1-\theta)\left\|\mathbf{h}_{e,k}^T\mathbf{W}_a\right\|^2 d_{e,k}^{-\alpha}/(N_a-1)+I_c+\sigma_e^2}, \; k \in \Phi_E, \tag{7}$$

where $P_a\theta\|\mathbf{e}_{ab}\mathbf{w}_a\|^2$ and $P_a(1-\theta)\|\mathbf{e}_{a,b}\mathbf{W}_a\|^2/(N_a-1)$ denote signal offset caused by the channel estimation error and AN leakage, which give rise to a serious reduction in security performance. According to stochastic knowledge, we obtain that $\left\|\widetilde{\mathbf{h}}_{a,b}\right\|^2 \sim \Gamma(N_a, \rho^2)$, $\|\mathbf{e}_{a,b}\mathbf{w}_a\|^2 \sim \exp(1-\rho^2)$, $\|\mathbf{e}_{a,b}\mathbf{W}_a\|^2 \sim \Gamma(N_a-1, 1-\rho^2)$, $\left\|\mathbf{h}_{e,k}^T\mathbf{W}_a\right\|^2 \sim \Gamma(N_a-1, 1)$, $\left|\mathbf{h}_{e,k}^T\mathbf{w}_a\right|^2 \sim \exp(1)$, and $\left\|\mathbf{h}_{c,k}^T\mathbf{T}_c\right\|^2 \sim \Gamma(N_c-1, 1)$ [31]. The SINRs γ_b and $\gamma_{e,k}$ are changed dynamically by channel estimation accuracy ρ and power allocation ratio θ. As such, capacities of the k-th eavesdropper link and the legitimate link can be expressed as

$$C_{e,k} = \log_2(1+\gamma_{e,k}), C_B = \log_2(1+\gamma_b). \tag{8}$$

In consideration of the non-colluding scenario, the maximal eavesdropping capacity depends on the maximal capacity among all the Eves, i.e., $C_E = \max_{k\in\Phi_E}\{C_{e,k}\}$.

3 Secrecy Performance Analysis

In this section, secrecy throughput is introduced as a crucial performance metric for evaluating the reliability-security rate of the legitimate link (bps/Hz) [16, 32, 33]. Adopting Wyner' wiretap encoding scheme [14], we use R_b and R_s to denote the transmitted codeword rate and secrecy rate, respectively. Furthermore, the redundant information rate R_{e}=R_b−R_s is used to provide secrecy against Eves. Therefore, the secrecy throughput T can be given by

$$T = (1-P_{top})(1-P_{sop})R_s, \tag{9}$$

where the P_{top} denotes the connection outage probability (COP) and P_{sop} denotes the secrecy outage probability (SOP).

3.1 Connection Outage Probability (COP)

A connection outage occurs when the instantaneous capacity of the legitimate link cannot support the codeword rate, i.e., $C_B < R_b$. We consider the worst case where

both the estimate errors and the AN leakage are modeled as independent Gaussian noise [31]. Thus, the COP P_{top} can be given by

$$\begin{aligned}
P_{top} &= \Pr\left\{C_B \le R_b\right\} \\
&= \Pr\left\{\log_2(1+\gamma_b) \le R_b\right\} \\
&= \Pr\left\{\left\|\hat{\mathbf{h}}_{a,b}\right\|^2 \le \tfrac{\beta_{R_b}}{P_a\theta d_{a,b}^{-\alpha}}(P_a\theta\|\mathbf{e}_{a,b}\mathbf{w}_a\|^2 d_{a,b}^{-\alpha}\right. \\
&\qquad \left. +P_a(1-\theta)\|\mathbf{e}_{a,b}\mathbf{W}_a\|^2 d_{a,b}^{-\alpha}/(N_a-1)+\sigma_b^2)\right\} \\
&= \Pr\left\{\left\|\hat{\mathbf{h}}_{a,b}\right\|^2 \le \tfrac{\beta_{R_b}}{P_a\theta}(P_a\theta\|\mathbf{e}_{a,b}\mathbf{w}_a\|^2\right. \\
&\qquad \left. +P_a(1-\theta)\|\mathbf{e}_{a,b}\mathbf{W}_a\|^2/(N_a-1)+\sigma_b^2 d_{a,b}^{\alpha})\right\} \\
&\overset{(a)}{=} \Pr\left\{\left\|\hat{\mathbf{h}}_{a,b}\right\|^2 \le \tfrac{\beta_{R_b}}{P_a\theta}(P_a(1-\rho^2)+\sigma_b^2 d_{a,b}^{\alpha})\right\},
\end{aligned} \tag{10}$$

where $\beta_{R_b} = 2^{R_b}-1$, (a) is due to the fact that $\|\mathbf{e}_{a,b}\mathbf{w}_a\|^2 \sim \exp(1-\rho^2)$ and $\|\mathbf{e}_{a,b}\mathbf{W}_a\|^2 \sim \Gamma(N_a-1, 1-\rho^2)$. Since $\widetilde{\mathbf{h}}_{a,b} \sim \mathcal{CN}\left(\mathbf{0}, \rho^2\mathbf{I}_{N_a}\right)$, $\left\|\widetilde{\mathbf{h}}_{a,b}\right\|^2 \sim \Gamma(N_a, \rho^2)$ and its cumulative distribution function (CDF) is given by

$$\Pr\left(\left\|\widetilde{\mathbf{h}}_{a,b}\right\|^2 \le x\right) = 1 - \sum_{k=0}^{N_a-1}\left(\frac{x}{\rho^2}\right)^k \frac{1}{k!}\exp\left(-\frac{x}{\rho^2}\right), \tag{11}$$

Then, the equation (10) can be re-written as

$$\begin{aligned}
P_{top} &= 1 - \sum_{k=0}^{N_a-1}\left(\tfrac{\beta_{R_b}}{P_a\theta\rho^2}(P_a(1-\rho^2)+\sigma_b^2 d_{a,b}^{\alpha})\right)^k \\
&\qquad \times \tfrac{1}{k!}\exp\left(\tfrac{\beta_{R_b}}{P_a\theta\rho^2}(P_a(1-\rho^2)+\sigma_b^2 d_{a,b}^{\alpha})\right) \\
&\overset{(b)}{=} \frac{\gamma(N_a, \frac{\beta_{R_b}}{P_a\theta\rho^2}(P_a(1-\rho^2)+\sigma_b^2 d_{a,b}^{\alpha}))}{\Gamma(N_a)}
\end{aligned} \tag{12}$$

where $\gamma(N,x) = \int_0^x t^{N-1}e^{-x}dx$ denotes the lower incomplete Gamma function and $\Gamma(x) = \int\limits_0^\infty t^{x-1}e^{-t}dt$ denotes the regularized Gamma function [34, eq.(8.350.1), eq.(8.310.1)]. (b) holds for the fact that $\gamma(N,x) = \Gamma(N)\left[1 - e^{-x}\sum\limits_{m=0}^{N-1}\frac{x^m}{m!}\right]$ when N takes integer values greater than one [35]. From (12), it is easily obtained that a higher connection performance can be achieved by increasing the parameter θ. Meanwhile, the connection performance can be heightened significantly when the channel estimation accuracy ρ increases.

3.2 Secrecy Outage Probability (SOP)

A secrecy outage inevitably occurs when the capacity of the equivalent wiretap link exceeds the redundant information rate, i.e., $C_E < R_e$. Therefore, the SOP P_{sop} is given by

$$\begin{aligned} P_{sop} &= \Pr\left(C_E > R_e\right) \\ &= 1 - \Pr\left(\max_{k\in\Phi_E}\gamma_{e,k} < \beta_{R_e}\right) \\ &= 1 - \Pr\left\{\max_{k\in\Phi_E}\bar{\gamma}_{e,k} < (I_{c,k}+\sigma_e^2)\beta_{R_e}d_{e,k}^{\alpha}\right\} \\ &= 1 - {}_{\Phi_c}\left({}_{\Phi_e}\left(\prod_{e\in\Phi_e}\Pr\left(\bar{\gamma}_{e,k} < (I_{c,k}+\sigma_e^2)\beta_{R_e}d_{e,k}^{\alpha}|\Phi_c\right)\right)\right) \\ &\overset{(a)}{=} 1 - {}_{\Phi_c}\left(\exp\left(-2\pi\lambda_e\int_0^{\infty}\Pr\left(\bar{\gamma}_{e,k} > (I_{c,k}+\sigma_e^2)\beta_{R_e}d_{e,k}^{\alpha}|\Phi_c\right)rdr\right)\right), \end{aligned} \tag{13}$$

where $\bar{\gamma}_{e,k} = P_a\theta(\left|\mathbf{h}_{e,k}^T\mathbf{w}_a\right|^2 - \beta_{R_e}\Phi\left\|\mathbf{h}_{e,k}^T\mathbf{W}_a\right\|^2)$, $I_{c,k} = \sum_{c\in\Phi_c}P_c\left\|\mathbf{h}_{c,k}^T\mathbf{T}_c\right\|^2 d_{c,k}^{-\alpha}/(N_c-1)$, $\beta_{R_e} = 2^{R_e}-1$, and (a) is obtained by utilizing the probability generating functional (PGFL) of PPP [33]: $\mathbb{E}_{\Phi}\left[\prod_{k\in\Phi}f(x)\right] = \exp\left[-\lambda\int_{R^2}(1-f(x))dx\right]$ and $\int_{R^2}f(x)dx = 2\pi\int_0^{\infty}xf(x)dx$. According to[36], the CDF of $\bar{\gamma}_{e,k}$ is expressed as:

$$F_{\bar{\gamma}_{e,k}}(x) = 1 - (1+\beta_{R_e}\Phi)^{1-N_a}e^{-\frac{x}{P_a\xi}}e^{-\sigma_e^2 s}. \tag{14}$$

Thus, for the SOP of the E_k, we have

$$\Pr\left(\bar{\gamma}_{e,k} > I_{e,k}\beta_{R_e}d_{e,k}^{\alpha}|\Phi_c\right) = (1+\beta_{R_e}\Phi)^{1-N_a}\mathcal{L}_{I_{c,k}}(s)\,e^{-\sigma_e^2 s}, \tag{15}$$

where $s = \frac{\beta_{R_e}d_{e,k}^{\alpha}}{P_a\theta}$, and $\mathcal{L}_{I_{c,k}}(s)$ denotes the Laplace transforms of random variable $I_{c,k}$ evaluated at s. Furthermore, let $x \triangleq \left\|\mathbf{g}_{c,k}^T\mathbf{T}_c\right\|^2 \sim \Gamma(N_c-1,1)$, using ([36], Eq. (38)), the $\mathcal{L}_{I_{c,k}}(s)$ is given by

$$\begin{aligned} \mathcal{L}_{I_{c,k}}(s) &= {}_{I_{c,k}}\left[e^{-sI_{c,k}}\right] \\ &= {}_{I_{c,k}}\left[\int_0^{\infty}e^{-sP_cd_{c,k}^{-\alpha}x/(N_c-1)}\frac{x^{N_c-2}}{\Gamma(N_c-1)}exp(-x)\right] \\ &= \exp\left(-\pi\lambda_cC_{\alpha,N_c}(P_cs/(N_c-1))^{\frac{2}{\alpha}}\right). \end{aligned} \tag{16}$$

where $C_{\alpha,N_c} = \frac{\Gamma\left(N_c-1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)}{\Gamma(N_c-1)}$. Therefore, by substituting (16) into (15), we can obtain:

$$\begin{aligned} \Pr\left(\bar{\gamma}_{e,k} > I_{e,k}d_{e,k}^{\alpha}|\Phi_c\right) &= (1+\beta_{R_e}\Phi)^{1-N_a} \\ &\times e^{-\sigma_e^2 s}\exp\left(-\pi\lambda_cC_{\alpha,N_c}(P_cs/(N_c-1))^{\frac{2}{\alpha}}\right). \end{aligned} \tag{17}$$

By plugging (17) into (13), we can obtain the SOP as shown in (18)

$$\begin{aligned} P_{sop} = & \ 1 - \exp\left(-2\pi\lambda_e \right. \\ & \times \int_0^\infty \Pr\left(\bar{\gamma}_{e,k} > I_{e,k} d_{e,k}^{\alpha} | \Phi_c\right) r dr) \\ = & \ 1 - \exp\left(-2\pi\lambda_e \int_0^\infty (1+\beta_{R_e}\Phi)^{1-N_a} \right. \\ & \times \exp\left(-\pi\lambda_c C_{\alpha,N_c}\left(\frac{P_c\beta_{R_e} r^a}{P_a\theta(N_c-1)}\right)^{\frac{2}{\alpha}}\right) r dr\Bigg) \\ = & \ 1 - \exp\Bigg(-\pi\lambda_e(1+\beta_{R_e}\Phi)^{1-N_a} \\ & \times \int_0^\infty \exp\left(Ar - Br^{\frac{a}{2}}\right) dr\Bigg) \end{aligned} \tag{18}$$

where $A = -\pi\lambda_c C_{\alpha,N_c}\left(\frac{P_c\beta_{R_e}}{P_a\theta(N_c-1)}\right)^{\frac{2}{\alpha}}$ and $B = \frac{\beta_{R_e}\sigma_e^2}{P_a\theta}$. In especial, the thermal noise can be neglected in the interference-limited network [37], i.e., $\sigma_e^2 = 0$. We can further obtain the simple expression of SOP, i.e., P_{sop}^{int}, as follows:

$$P_{sop}^{\text{int}} = 1 - \exp\left(\frac{\pi\lambda_e(1+\beta_{R_e}\Phi)^{1-N_a}}{A}\right). \tag{19}$$

From (19), it is easily observed that the expression of SOP is inversely proportional to the cooperative jammer density λ_c. Therefore, the secrecy performance can be enhanced by increasing λ_c. In contrast, we can easily obtain that the P_{sop}^{int} is an increasing function with respect to the eavesdropper density λ_e. In addition, the P_{sop}^{int} increases as the power allocation ratio θ increases. This is due to the fact that a higher θ denotes a lower power allocated to the AN for confusing Eves.

3.3 Secrecy Throughput

Using the definition given by (9), we can obtain a closed-form expression for the secrecy throughput in the interference-limited network, as shown in (20).

$$\begin{aligned} T = & (1 - \frac{\gamma(N_a, \frac{\beta_{R_b}}{P_a\theta\rho^2}(P_a(1-\rho^2)+\sigma_b^2 d_{a,b}^{\alpha}))}{\Gamma(N_a)}) \\ & \times \exp(\frac{\pi\lambda_e(1+\beta_{R_e}\Phi)^{1-N_a}}{A})(R_b - R_e). \end{aligned} \tag{20}$$

From (20), it is observed that the performance of secrecy throughput depends on some key system parameters, e.g., the channel estimation accuracy ρ, the power allocation ratio θ, the number of antennas N_a and N_c. To evaluate the effect of N_a and N_c on the secrecy performance, next we will derive the asymptotic expression of T when $N_a \to \infty$ and $N_c \to \infty$. As such, the singal-to-interference (SIR) at E_k can be re-written as

$$\gamma_{e,k}^{\infty} = \frac{P_a\theta\left|\mathbf{h}_{e,k}^T\omega\right|^2 d_{e,k}^{-\alpha}}{P_a(1-\theta)d_{e,k}^{-\alpha} + I_{c,k}^{\infty}}, \tag{21}$$

where $I_{c,k}^{\infty} = \sum_{c\in\Phi_c} P_c d_{c,k}^{-\alpha}$ because of utilizing $\lim_{N_a\to\infty} \left|\mathbf{h}_{e,k}^T\omega\right|^2 = N_a - 1$ and $\lim_{N_c\to\infty} \left\|\mathbf{h}_{c,k}^T\mathbf{T}_c\right\|^2 = N_c - 1$. We denote $\overline{\gamma_{e_k}^{\infty}} = P_a\theta\left|\mathbf{h}_{e,k}^T\omega\right|^2 - P_a(1-\theta)\beta_{R_e}$, then

$$\begin{aligned}
&\Pr\left(\gamma_{e,k}^{\infty} < \beta_{R_e}\right) \\
&= \left(\overline{\gamma_{e,k}^{\infty}} < \beta_{R_e} I_{c,k}^{\infty} d_{e,k}^{\alpha}\right) \\
&= 1 - e^{\beta_{R_e}(1-N_a)\Phi}\mathcal{L}_{I_{c,k}^{\infty}}\left(\frac{\beta_{R_e} d_{e,k}^{\alpha}}{P_a\theta}\right),
\end{aligned} \tag{22}$$

where

$$\mathcal{L}_{I_{c,k}^{\infty}}(s) = \exp\left(-\pi\lambda_c\Gamma(1-\frac{2}{\alpha})p_c^{\frac{2}{\alpha}} s^{\frac{2}{\alpha}}\right). \tag{23}$$

Hence,

$$\begin{aligned}
&\Pr\left(\gamma_{e,k}^{\infty} < \beta_{R_e}\right) \\
&= \left(\overline{\gamma_{e,k}^{\infty}} < \beta_{R_e} I_{c,k}^{\infty} d_{e,k}^{\alpha}\right) \\
&= 1 - e^{\beta_{R_e}(1-N_a)\Phi}\mathcal{L}_{I_{c,k}^{\infty}}\left(\frac{\beta_{R_e} d_{e,k}^{\alpha}}{P_a\theta}\right),
\end{aligned} \tag{24}$$

By plugging (24) into (13), we can have

$$\begin{aligned}
P_{sop}^{asy} &= 1 - \exp(-2\pi\lambda_e e^{\beta_{R_e}(1-N_a)\Phi} \\
&\quad \times \textstyle\int_0^{\infty} \exp\left(-\Gamma(1-\frac{2}{\alpha})\pi\lambda_c\left(\frac{P_c\beta_{R_e}}{P_a\theta}\right)^{\frac{2}{\alpha}} r^2\right) r dr) \\
&= 1 - \exp(-\pi\lambda_e e^{\beta_{R_e}(1-N_a)\Phi} \textstyle\int_0^{\infty} \exp(Cr)\, dr) \\
&= 1 - \exp(\frac{\pi\lambda_e e^{\beta_{R_e}(1-N_a)\Phi}}{C}),
\end{aligned} \tag{25}$$

where $C = -\Gamma(1-\frac{2}{\alpha})\pi\lambda_c\left(\frac{P_c\beta_{R_e}}{P_a\xi}\right)^{\frac{2}{\alpha}}$. Therefore, the asymptotic expression T^{asy} can be given by

$$\begin{aligned}
T^{asy} &= \frac{\gamma(N_a, \frac{\beta_{R_b}}{P_a\theta\rho^2}(P_a(1-\rho^2)+\sigma_b^2 d_{a,b}^{\alpha}))}{\Gamma(N_a)} \\
&\quad \times \exp\left(\frac{\pi\lambda_e e^{\beta_{R_e}(1-N_a)\Phi}}{C}\right)(R_b - R_e).
\end{aligned} \tag{26}$$

According to the above analysis, we have derivated the asymptotic expression of the secrecy throughput. It can be observed from (12) and (18) that the power allocation ratio θ keeps a tradeoff between the COP and the SOP. In other words, selecting an appropriate θ can improve the reliability-security tradeoff. Specifically, from the results in (20) and (26), channel estimation errors caused by high-mobility of vehicle in dynamic vehicular network may lead to noise leakage at the legitimate receiver, thus resulting significant loss in the secrecy throughput. In the next section, we will investigate the security performance through numerical simulation.

4 Numerical Simulation Results and Discussions

In this section, several numerical results are provided to verify the theoretical analysis. In particular, the effects of key system parameters such as: the number of transmit antennas N_a and N_c, the relative vehicular velocity v, the ratio of λ_c/λ_e, and the power allocation ratio θ, on security performance are presented in the figures below. Unless otherwise stated, the following main simulation parameters are adopted [27]: $P_c = P_v = 30$ dBm, $\alpha = 4$, and $N_a = N_c = 4$. Additionally, $R_b = 5$ bps/Hz, $R_e = 3$ bps/Hz, and $\rho = 1$

Figure 2 The COP versus the power allocation ratio θ for different number of antennas. Legends:($N_a = 2, 4, 5, 8$).

Fig. 2 presents the relationship between the COP of legitimate link P_{cop} and the power allocation ratio θ for different number of antennas, i.e., $N_a = 2, 4, 5, 8$. We observed that as the parameter θ increases, the P_{cop} is always decreasing for different number of antennas N_a. The results match the analytical expression in (12) very well. Furthermore, by fixing the parameter θ unchanged, adding transmit antennas can be to the benefit of decreasing the COP. It is because that increasing the transmit power of the information-bearing signal or adding antennas is beneficial to improve connection performance.

Figure 3 The COP versus the relative vehicular velocity v for different transmitted codeword rate R_b. Legends:($R_b = 5$ bps/Hz, $R_b = 4.8$ bps/Hz, $R_b = 5.2$ bps/Hz).

Fig. 3 presents the COP of legitimate link P_{cop} versus the relative vehicular velocity v for different transmitted codeword rate R_b. It is shown that increasing the parameter R_b will weaken the connection performance of the legitimate link. Furthermore, the connection performance can be weakened significantly when the relative vehicular velocity v increases. It is due to the fact that channel estimation errors caused by high-mobility of vehicles in dynamic vehicular network may lead to noise leakage at the legitimate receiver, thus resulting significant loss in the connection performance.

Figure 4 The SOP versus the number of antennas for different power of jammer P_c. Legends:($P_c = 30$ dbm, $P_c = 20$ dbm, $P_c = 10$ dbm).

Fig. 4 illustrates the SOP of legitimate link P_{sop} versus the number of antennas $N = N_a = N_c$ for different power of jammer P_c. From Fig. 4, it is observed that the SOP P_{sop} declines rapidly at fist and then tends to stabilization with increasing the number of antennas N from all considered jammer power. It is because that when the parameter N becomes large, increasing the number of antennas is conducive to improving secrecy performance. However, when the parameter N becomes sufficiently large, there also exists secrecy performance floor phenomenon. Hence, the result confirms the accuracy of our asymptotic analysis at high N in (25). Furthermore, one can readily observe that increasing the power of cooperative jammer can be also beneficial to enhance secrecy performance in Fig. 4.

Figure 5 The SOP versus power allocation ratio θ for different density ratio. Legends:($\lambda_c = 0.1\lambda_e$, $\lambda_c = 0.5\lambda_e$, $\lambda_c = \lambda_e$, $\lambda_c = 5\lambda_e$).

Fig. 5 shows the relationship between the SOP and the power allocation ratio θ for different density ratio of cooperative jammers and Eves. We can observe that the SOP P_{sop} increases as the parameter θ increases. This is because that a higher θ denotes a lower transmission power allocated to the AN for confusing Eves. Furthermore, the SOP P_{sop} is shown to decrease with the increase of the density ratio of cooperative jammers and Eves. It is because that when the density ratio increases, more cooperative interference signals can be used for guaranteeing security.

Figure 6 The secrecy throughput versus power allocation ratio θ for different density ratio. Legends:($\lambda_c = 0.1\lambda_e$, $\lambda_c = 0.2\lambda_e$, $\lambda_c = 0.05\lambda_e$).

Fig. 6 shows the secrecy throughput versus power allocation ratio θ for different density ratio of cooperative jammers and Eves. As shown in Fig. 6, it is observed that the security throughput rises at first and then decrease as the power allocation ratio θ increases. This implies that there exists an optimum θ^* for maximizing security throughput. This is due to that the power allocation ratio has a reliability-security tradeoff. A smaller θ stands for allowing more transmission power allocated to AN signal, which obtains a higher security performance while impairing the reliability performance. Conversely, a larger θ stands for allowing more power allocated to information-bearing signal, which obtains a higher reliability performance while impairing the security performance. This reveals that selecting an appropriate θ can improve the secrecy throughput. Furthermore, the tendency that the secrecy throughput declines as the density ratio decreases can be observed in Fig. 6, which can be attributed to the increasing SOP. The result is consistent with Fig. 2 and Fig. 5.

Figure 7 The secrecy throughput versus the relative vehicular velocity v. Legends:($P_c = 30$ dbm, $P_c = 20$ dbm, without CJ).

Fig. 7 illustrates the secrecy throughput versus the relative vehicular velocity v, where $\lambda_c = 10\lambda_e$, $\theta = 0.6$. For a given jammer power P_c, it can be noticed that the secrecy throughput decreases as the relative vehicular velocity v increases, which implies that the imperfect CSI caused by high-mobility of vehicles is not conducive to enhancing the secrecy throughput performance. Furthermore, as the power of cooperative jammer increases, a prominent increase in the security throughput can be observed. As expected, the joint CJ and AN aided secure transmission scheme always outperforms the without CJ transmission scheme. This means that the cooperative jammers are utilized for further enhancing physical layer security.

5 CONCLUSION

In this paper, a joint CJ and AN aided secure transmission scheme with imperfect CSI has been investigated in vehicular communication network. In this scheme, the

closed-form expressions of the COP and the SOP have been provided. We have quantified the secrecy throughput performance for maintaining the reliability-security tradeoff of the legitimate link. Meanwhile, there exists an optimal solution of power allocation that yields the maximum security throughput under different relative vehicular velocity. Furthermore, the performance of the proposed scheme has been demonstrated by numerical results. More importantly, our results indicated that the cooperative jammers can be utilized for further enhancing physical layer security, which will be to the benefit of the information security in vehicular communication network.

Methods/Experimental

The following parameters are used in all simulations using MATLAB software unless stated otherwise: $P_c = P_v = 30$ dBm, $\alpha = 4$, and $N_a = N_c = 4$, $R_b = 5$ bps/Hz, $R_e = 3$ bps/Hz, and $\rho = 1$.

Abbreviations

ITS: Intelligent transportation system; V2V: Vehicle-to-vehicle; V2I: Vehicle-to-infrastructure; CSI: Channel state information; SINRs: Signal-to-interference-plus-noise ratios; SIR: Singal-to-interference-ratio; PLS: Physical layer security; SOP: Secrecy outage probability; COP: Connection outage probability; AN: Artificial noise ; CJ: Cooperative jamming.

Availability of data and materials

All the data and computer programs are available.

Author's contributions

All authors have contributed to the work presented in this paper. Particularly, the contribution can be stated as follow: BQ designed the communication scenarios and the simulations. BQ and CJ wrote the paper. All authors read and approved the final manuscript . . .

Funding

This work was supported in part by the National Natural Science Foundation of China under Grant 61802085, in part by Guangxi Natural Science Foundation under Grants 2018GXNSFBA281057, 2015GXNSFBA139260 and 2019JJA170095, in part by Guangxi key Laboratory Fund of Embedded Technology and Intelligent System under Grant 20190207, and Guangxi Key Laboratory of Trusted Software under Grant kx202011.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]Guangxi Key Laboratory of Embedded Technology and Intelligent System, Guilin University of Technology, Jiangan Road, 541004 Guilin, China. [2]College of Information Science and Engineering, Guilin University of Technology, Jiangan Road, 541004 Guilin, China. [3] Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Jinji Road, 541004 Guilin, China.

References

1. L. Li, D. Wen, and D. Y. Yao, A survey of traffic control with vehicular communications. IEEE Trans. Intell. Transp. Syst., 15(1), 425-432(2014)
2. L. Zhao, F. Wang, K. Zheng, and T. Riihonen, Joint optimization of communication and traffic efficiency in vehicular networks. IEEE Trans. Veh. Technol., 68(2), 2014-2018(2019)
3. S. Chen, J. Hu, Y. Shi, and L. Zhao, LTE-V: A TD-LTE-based V2X solution for future vehicular network. IEEE Internet Things J., 3(6), 997-1005(2016)
4. C. J. Rapson, B.C. Seet, P. H. J. Chong, and R. Klette, Safety assessment of radio frequency and visible light communication for vehicular networks. IEEE Wireless Commun., 27(1), 186-192(2020)
5. D.W. Wang, P. Y. Ren, Q. H. Du, L. Sun, and Y. C. W, Security provisioning for MISO vehicular relay networks via cooperative jamming and signal superposition. IEEE Trans. Veh. Technol., 66(12), 10732-10747(2017)
6. Y. Ai, M. Cheffena, A, Mathur, and H. J. Lei, On physical layer security of double Rayleigh fading channels for vehicular communications. IEEE Wireless Commun. Lett., 7(6), 1038-1041(2018)
7. H. Xiao, A. T. Chronopoulos, and Z. Zhang, An efficient security scheme for vehicular communication using a quantum secret sharing method. IEEE Trans. Veh. Technol., 69(1), 1101-1105(2020)
8. Z. Zhang, K. Long, S. Member, and J. Wang, On swarm intelligence inspired self-organized networking: Its bionic mechanisms, designing principles and optimization approaches. IEEE Commun. Surv. Tuts., 78(3), 387-394(2014)
9. N. Kaur and S. Kad, A review on security related aspects in vehicular ad hoc networkss. Procedia Computer Science, 78, 387-394(2016)
10. Y. Wu, L. P. Qian, H. W. Mao, et al., Secrecy-driven resource management for vehicular computation offloading networks. IEEE Netw., 32(3), 84-91(2018)
11. A. Hyadi, Z. Rezki, and M. S. Alouini, An overview of physical layer security in wireless communication systems with CSIT uncertainty. IEEE Access, 4, 6121-6132(2016)

12. X. Zhou and M. R. McKay, Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation. IEEE Trans. Veh. Technol., 59(8), 3831-3842(2010).
13. Q. Xu, P. Ren, H. Song, and Q. Du, Security enhancement for IoT com- munications exposed to eavesdroppers with uncertain locations. IEEE Access, 4, 2840-2853(2016)
14. Y. J. Tolossa, S. Vuppala, G. Kaddoum, and G. Abreu, On the uplink secrecy capacity analysis in D2D-enabled cellular network. IEEE Syst. J., 12(3), 2297-2307(2018)
15. X. Zhang, X. Zhou, and M. R. McKay, Enhancing secrecy with multi antenna transmission in wireless ad hoc networks. IEEE Trans. Inf. Forensics Security, 8(11), 1802-1814(2013)
16. B. Qiu, H. Xiao, A. T. Chronopoulos, D. Zhou, and S. Ouyang, Optimal access scheme for security provisioning of C-V2X computation offloading network with imperfect CSI. IEEE Access, 8, 9680-9691(2020)
17. T. -X. Zheng, and H. -M. Wang, Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers. IEEE Trans. Veh. Technol., 65(10), 9680-9691(2016)
18. L. Liang, J. Kim, S. C. Jha, K. Sivanesan, and G. Y. Li, Spectrum and power allocation for vehicular communications with delayed CSI feedback. IEEE Wireless Commun. Letters, 6(4), 458-461(2017)
19. S. Guo, and X. Zhou, Robust resource allocation with imperfect channel estimation in NOMA-based heterogeneous vehicular networks. IEEE Trans. Commun., 67(3), 2321-2332 (2019)
20. S. C. Lin, T. H. Chang, Y. l. Yang, Y. W. Hong, and C. Y. Chi, On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: the noise leakage problem. IEEE Trans. Wireless Commun., 10(3), 901-915 (2011)
21. W. Liu, X. Y. Zhou, S. Durrani, and P. Popovsk, Secure communication with a wireless-powered friendly jammer. IEEE Trans. Wireless Commun., 15(1), 401-415(2016)
22. P. Mu, X. Hu, B. Wang, and Z. Li, Secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers under secrecy outage probability constraint. IEEE Commun. Lett. vol., 19(12), 2174-2177(2015)
23. F. Jameel, S.Wyne, G. Kaddoum, and T. Q. Duongi, A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. IEEE Commun. Surv. Tuts., 21(3), 2734-2771(2019)
24. X. Hu, P. Mu, B. Wang, and Z. Li, On the secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers. IEEE Trans. Veh. Technol., 26(5), 4457-4462(2019)
25. R. Ma, S. Yang, M. Du, and J. Ou, Improving physical layer security jointly using full-duplex jamming receiver and multi-antenna jammer in wireless networks. IET Commun., 13(10), 1530-1536(2019)
26. L. Hu, H. Wen, B. Wu, J. Tang, F. Pan, and R. -F. Liao, Cooperative jamming aided secrecy enhancement in wireless networks with passive eavesdroppers. IEEE Trans. Veh. Technol., 67(3), 2108-2117(2018)
27. H. -H. Song, H. Wen, L. Hu, S. Chen, Z. Zhang, and R. Liao, Secure cooperative transmission with imperfect channel state information based on BPNN. IEEE Trans. Veh. Technol., 67(11), 10482-10491(2018)
28. L. Hu, H. Wen, B. Wu, et al., Cooperative jamming for physical layer security enhancement in internet of things. IEEE Internet Things J., 5(1), 219-228(2018)
29. L. M. Wang, and X. L. Liu, Secure cooperative communication scheme for vehicular heterogeneous networks. Veh. Commum., 12, 46-56(2018)
30. Z. X. Liu, X. Han, Y. Liu, and Y. Wang, D2D-based vehicular communication with delayed CSI feedback. IEEE Access, 6, 52857-52866(2018)
31. Y. Yang, W. Wang, H. Zhao, and L. Zhao, Transmitter beamforming and artificial noise with delayed feedback: secrecy rate and power allocation. J. Commun. Netw., 14(4), 374-384(2012)
32. H. M. Wang, C. Wang, T. -X. Zhang, and T. Q. S. Quek, Impact of artificial noise on cellular networks: A stochastic geometry approach. IEEE Trans. Wireless Commun., 15(11), 7390-7404(2016)
33. L. Wang, J. M. Liu, M. K. Chen, G. Gui, and H. Sari, Optimization-based access assignment scheme for physical-layer security in D2D communications underlaying a cellular network. IEEE Trans. Veh. Technol., 67(7), 5766-5777, (2018)
34. X. Liu, K. Zheng, X. Liu, X. Wang, and G. Dai, Towards secure and energy-efficient CRNs via embracing interference: a stochastic geometry approach. IEEE Access, 6, 36757-36770(2018)
35. I. S. Gradshteyn, I. M. Ryzhik, A. Jeffrey, D. Zwillinger, and S. Technica, Table of Integrals, Series, and Products, 7th ed. New York, NY, USA: Academic(2007)
36. J. Men, J. Ge, and C. Zhang, Performance analysis for downlink relaying aided non-orthogonal multiple access networks with imperfect CSI over Nakagami-m fading. IEEE Access, 5, 998-1004(2017)
37. Y. Chen, X. Ji, K. Huang, J. Yang, X. Hu, and Y. Xu, Artificial noise-assisted physical layer security in D2D-enabled cellular networks. EURASIP J. Wireless Commun. Netw., 2017(2017)
38. W. Wang, K. C. Teh, and K. H. Li, Artificial noise aided physical layer security in multi-antenna small-cell networks. IEEE Trans. Inf. Forensic Secur., vol. 12, no. 6, pp. 1470-1483(2017)

Fig.1

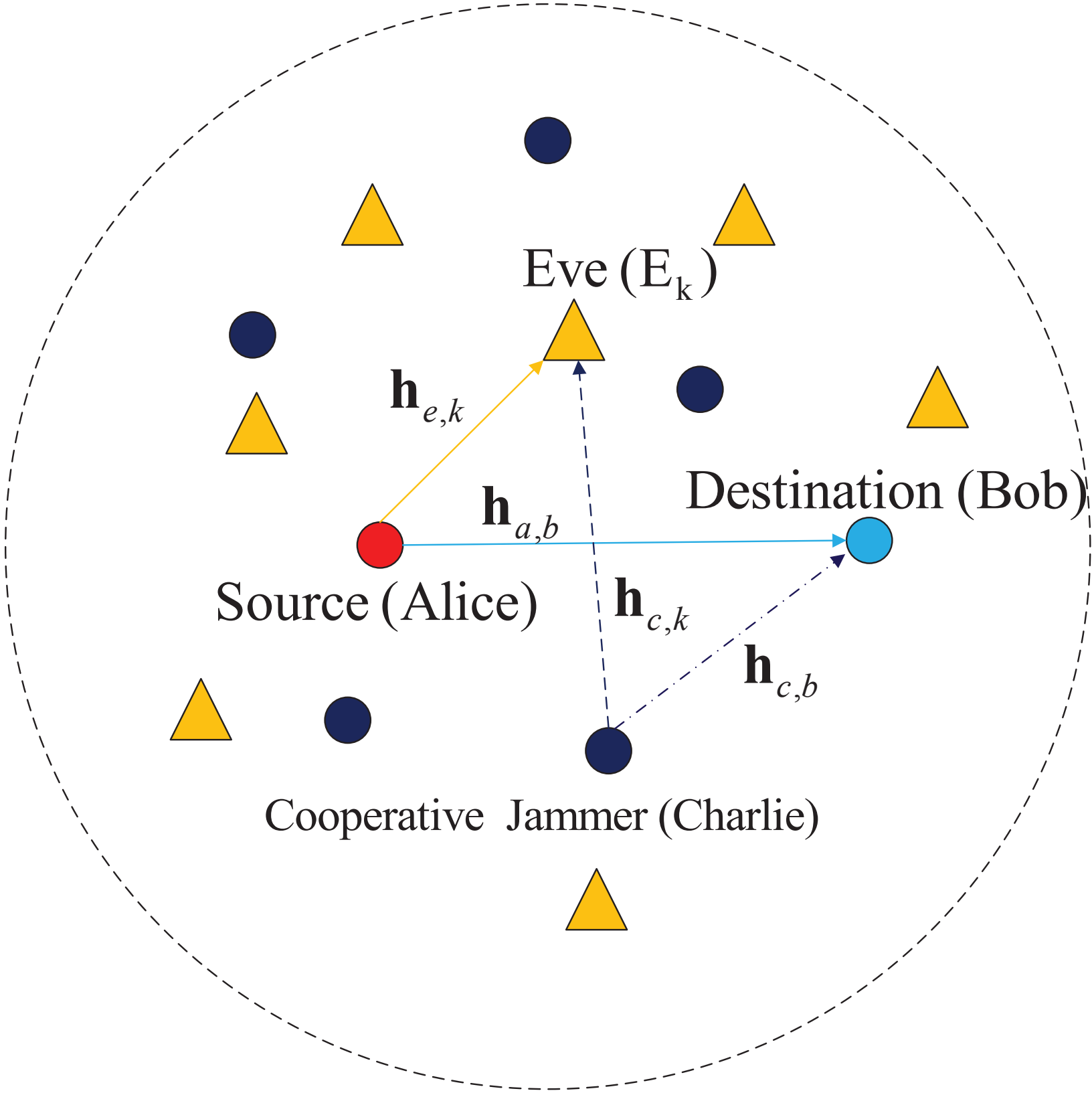

Eve (E_k)
$\mathbf{h}_{e,k}$
$\mathbf{h}_{a,b}$
Destination (Bob)
Source (Alice)
$\mathbf{h}_{c,k}$
$\mathbf{h}_{c,b}$
Cooperative Jammer (Charlie)

Fig.2

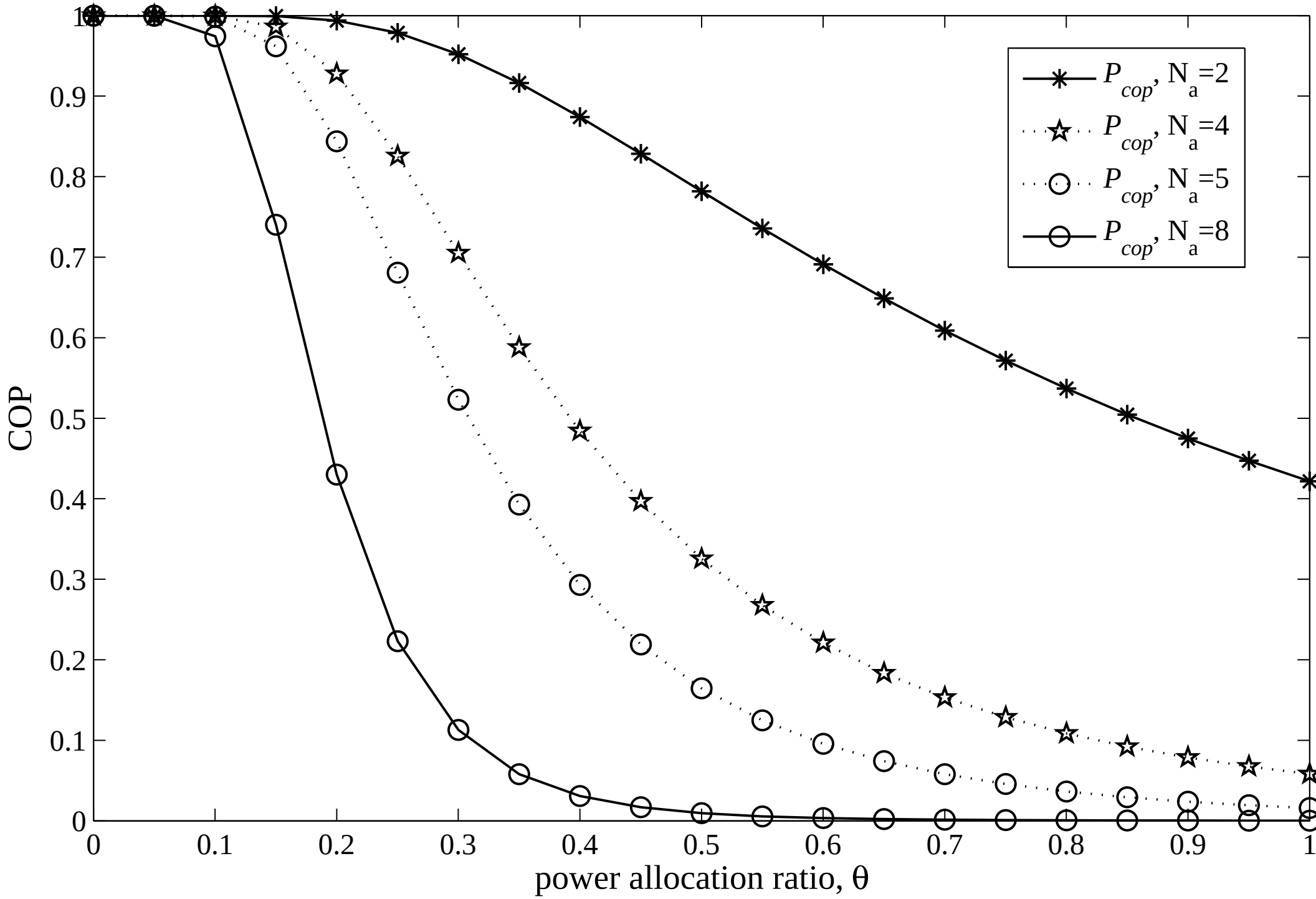

COP
power allocation ratio, θ
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
P_{cop}, N_a=2
P_{cop}, N_a=4
P_{cop}, N_a=5
P_{cop}, N_a=8

Fig.3

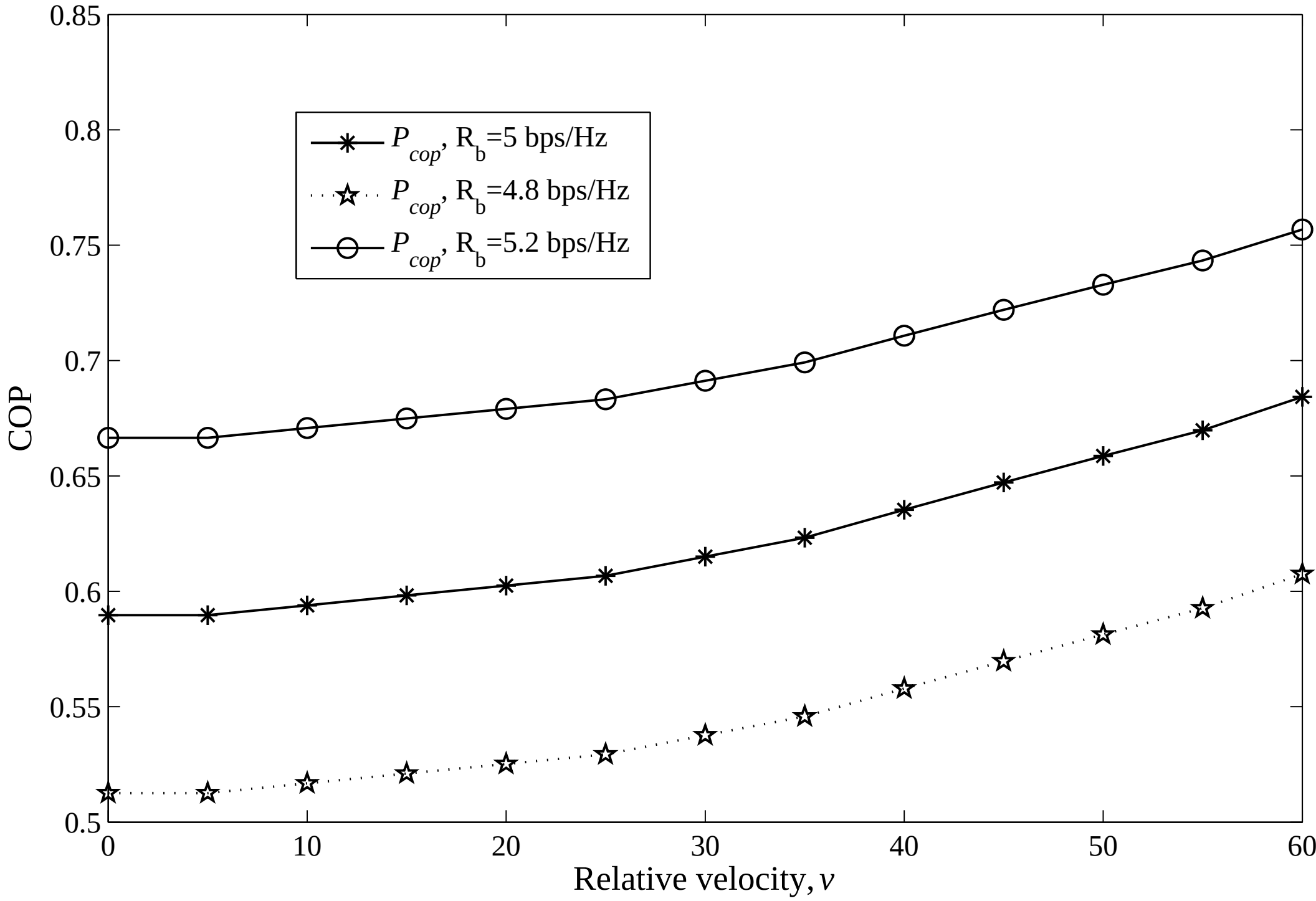

0.85
0.8
0.75
0.7
0.65
0.6
0.55
0.5
COP
0
10
20
30
40
50
60
Relative velocity, v
P cop, Rb=5 bps/Hz
P cop, Rb=4.8 bps/Hz
P cop, Rb=5.2 bps/Hz

Fig.4

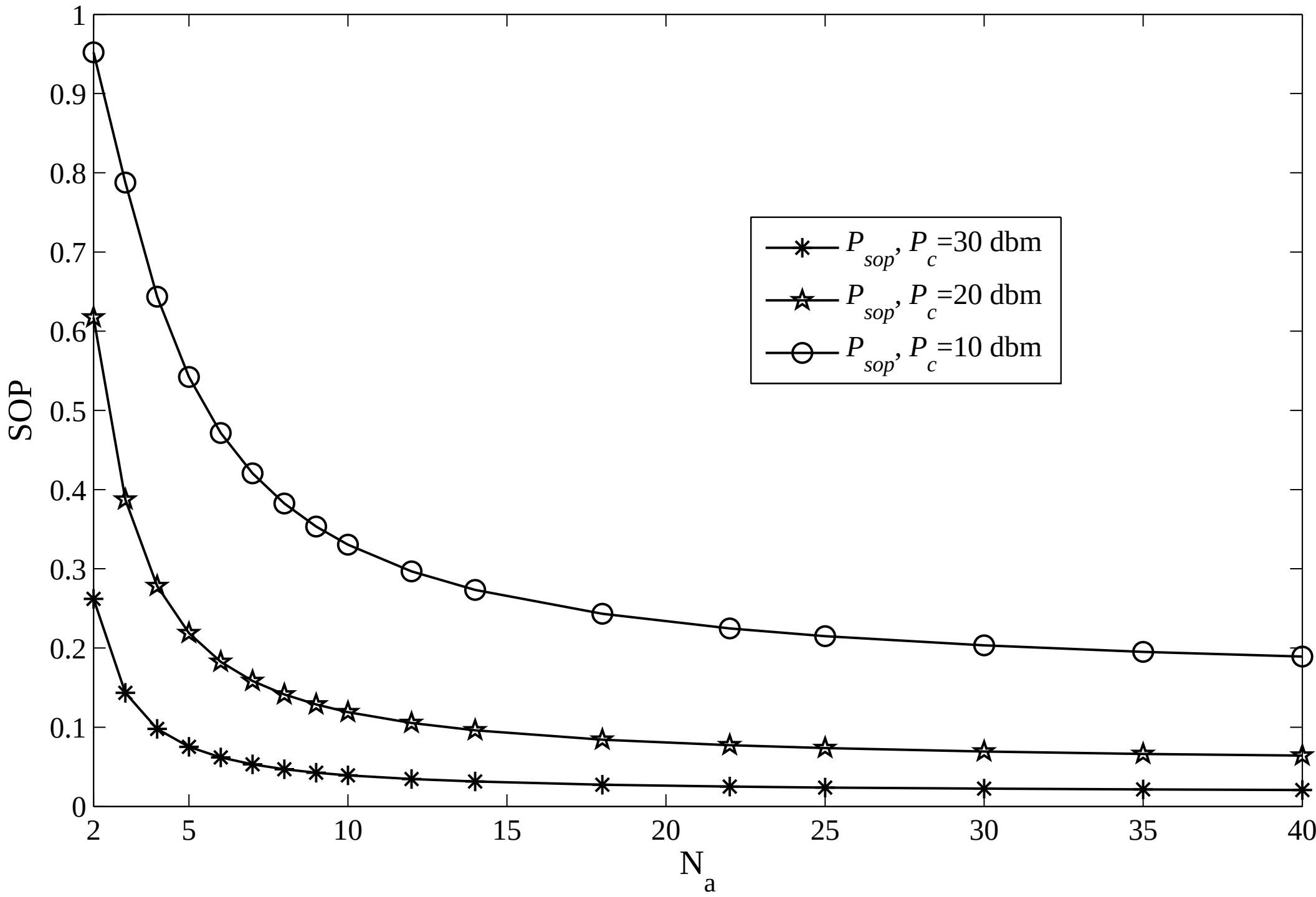

1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
SOP
2
5
10
15
20
25
30
35
40
N a
P sop, P c =30 dbm
P sop, P c =20 dbm
P sop, P c =10 dbm

Fig.5

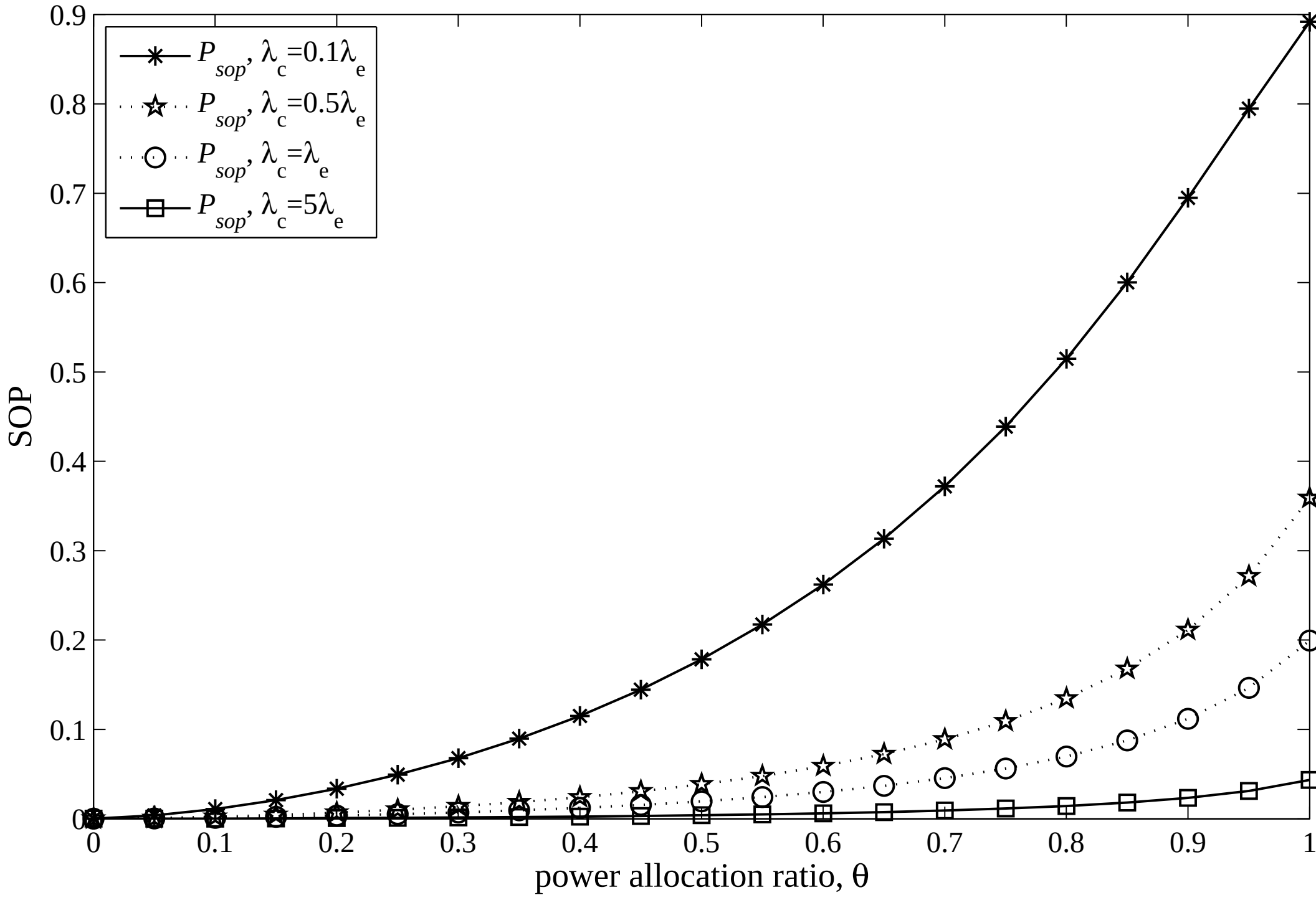

P_{sop}, λ_c=0.1λ_e
P_{sop}, λ_c=0.5λ_e
P_{sop}, λ_c=λ_e
P_{sop}, λ_c=5λ_e
SOP
power allocation ratio, θ
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1

Fig.6

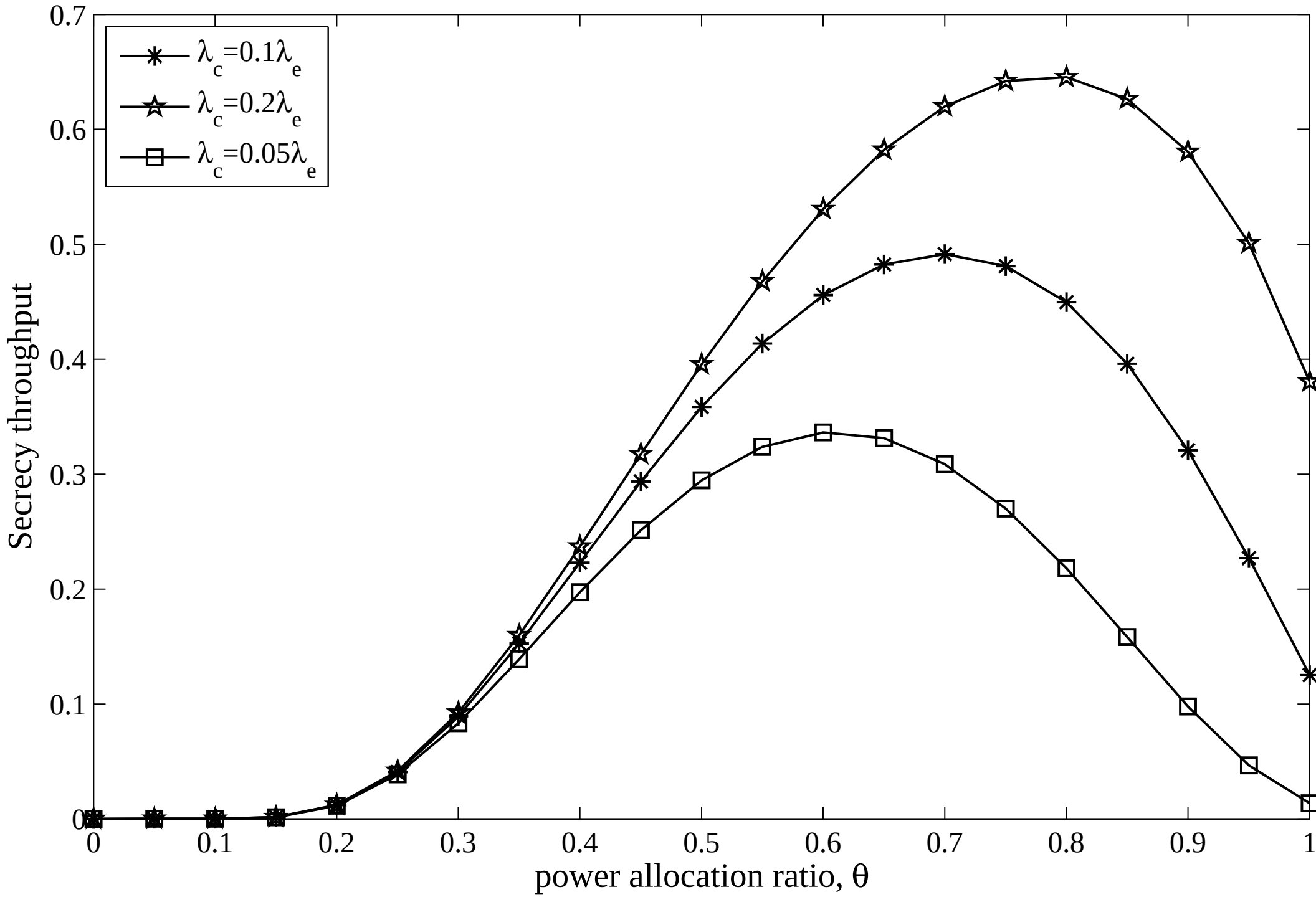
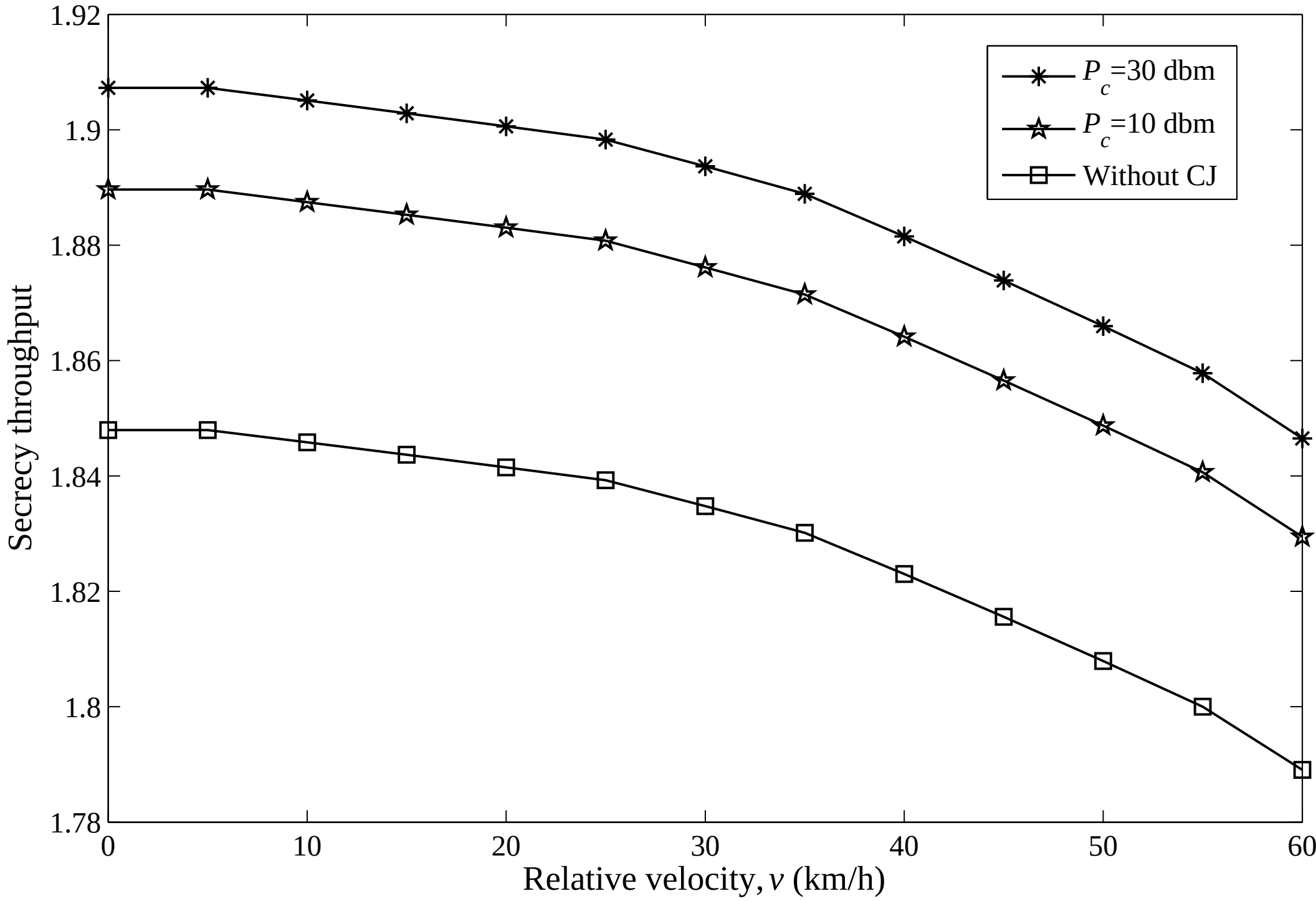

λc=0.1λe
λc=0.2λe
λc=0.05λe
Secrecy throughput
power allocation ratio, θ
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1

Fig.7


1.92
1.9
1.88
1.86
1.84
1.82
1.8
1.78
Secrecy throughput
0
10
20
30
40
50
60
Relative velocity, v (km/h)
P c =30 dbm
P c =10 dbm
Without CJ

Figures

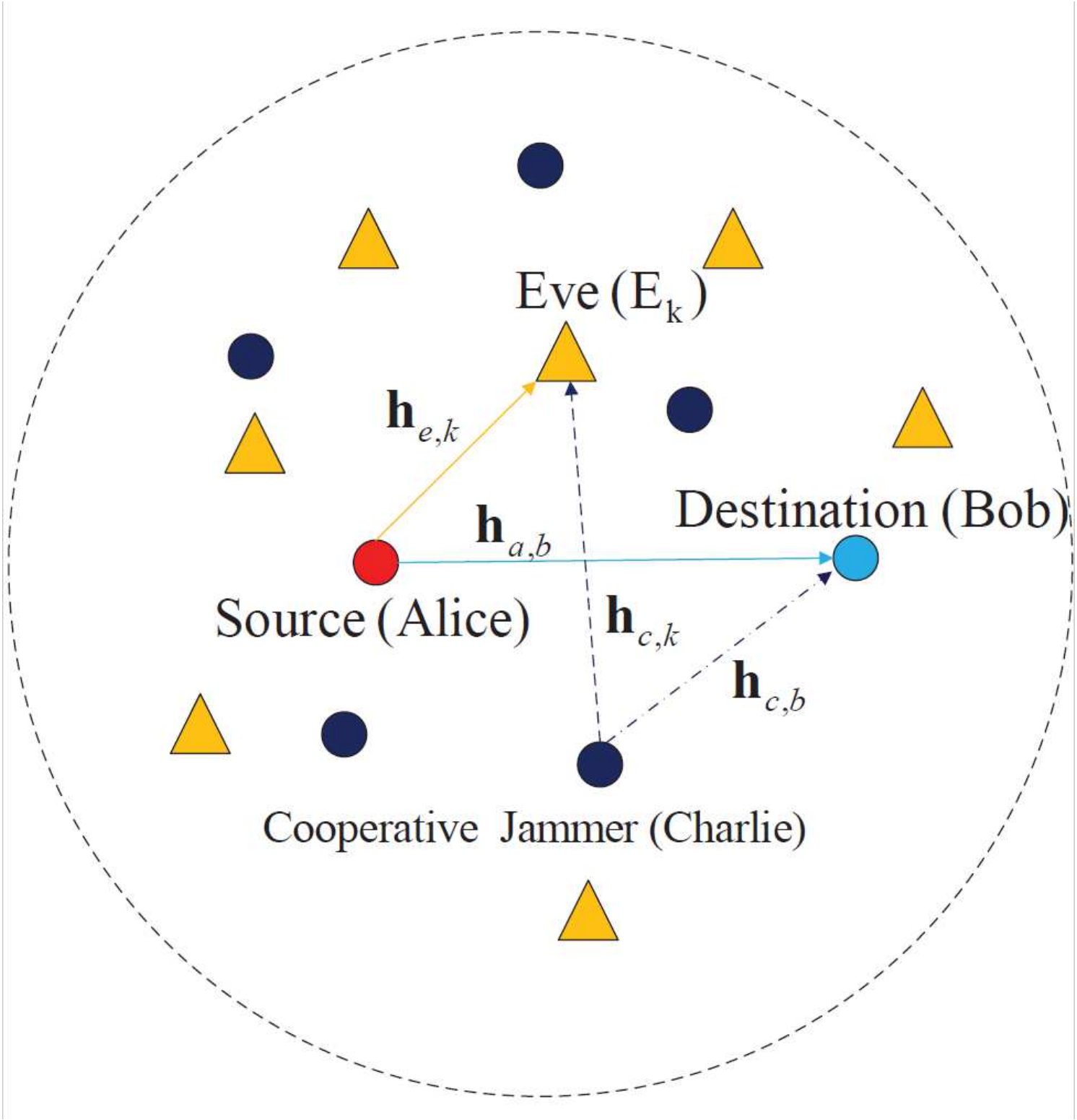


Figure 1

Joint CJ and AN aided secure transmission model. Legends: Alice aims to transmit confidential message to Bob, in the presence of randomly located passive eavesdropper Eves trying to capture the confidential

information. In addition, there also exist cooperative jammers (Charlies) emit interference signals to confuse Eves.

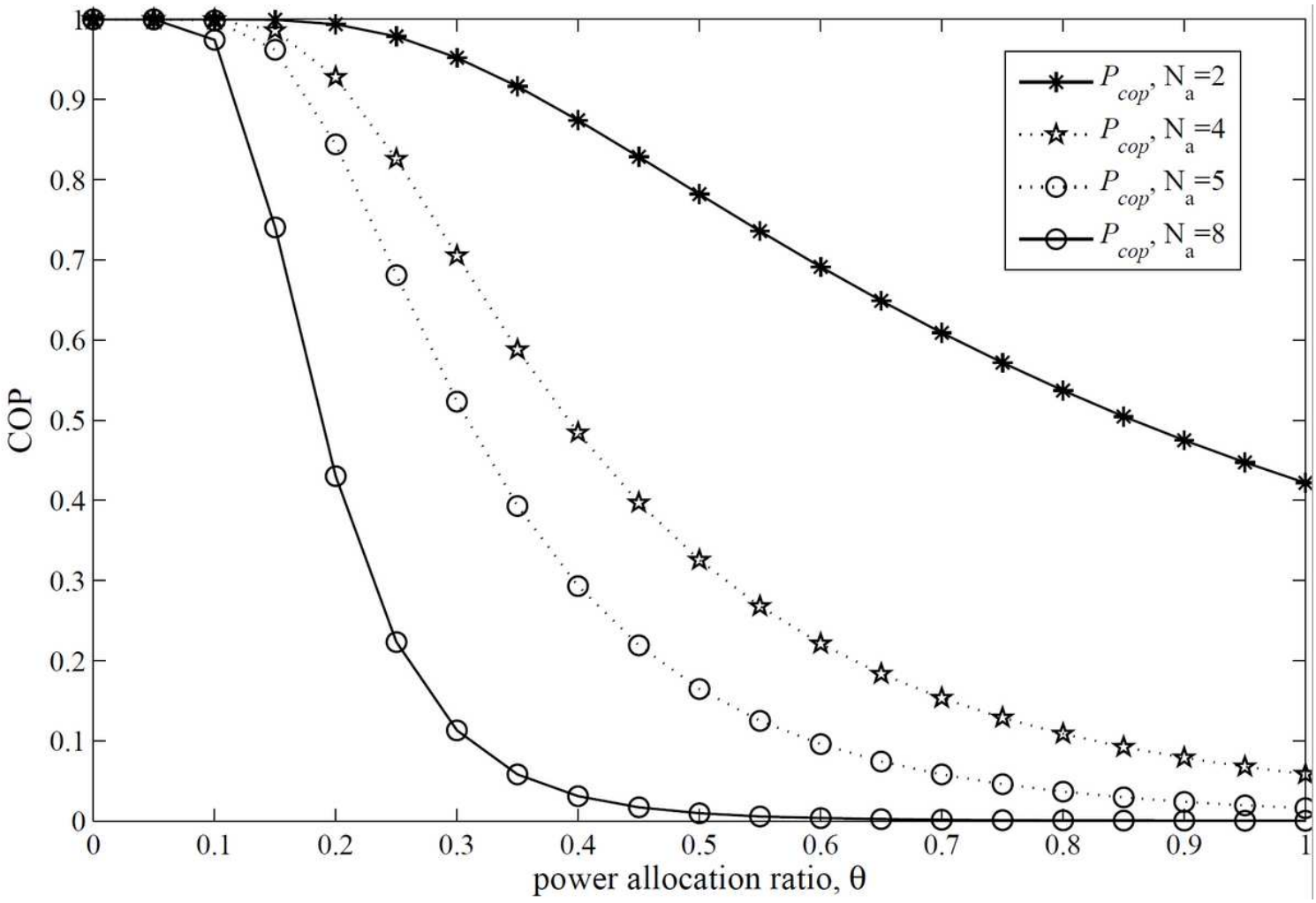


Figure 2

The COP versus the power allocation ratio θ for different number of antennas. Legends:(Na = 2; 4; 5; 8).

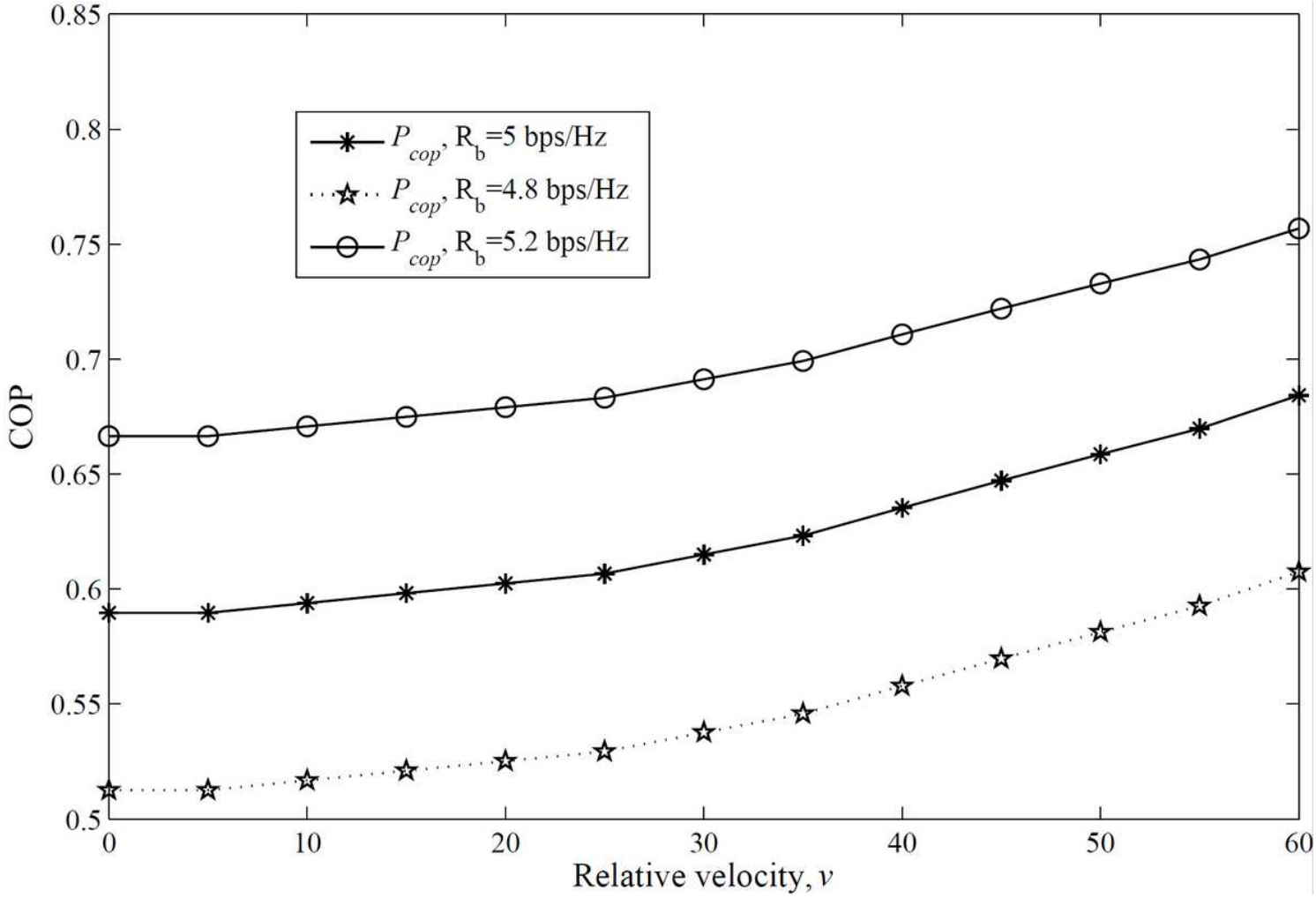


Figure 3

The COP versus the relative vehicular velocity v for different transmitted codeword rate Rb. Legends:(Rb = 5 bps/Hz, Rb = 4:8 bps/Hz, Rb = 5:2 bps/Hz).

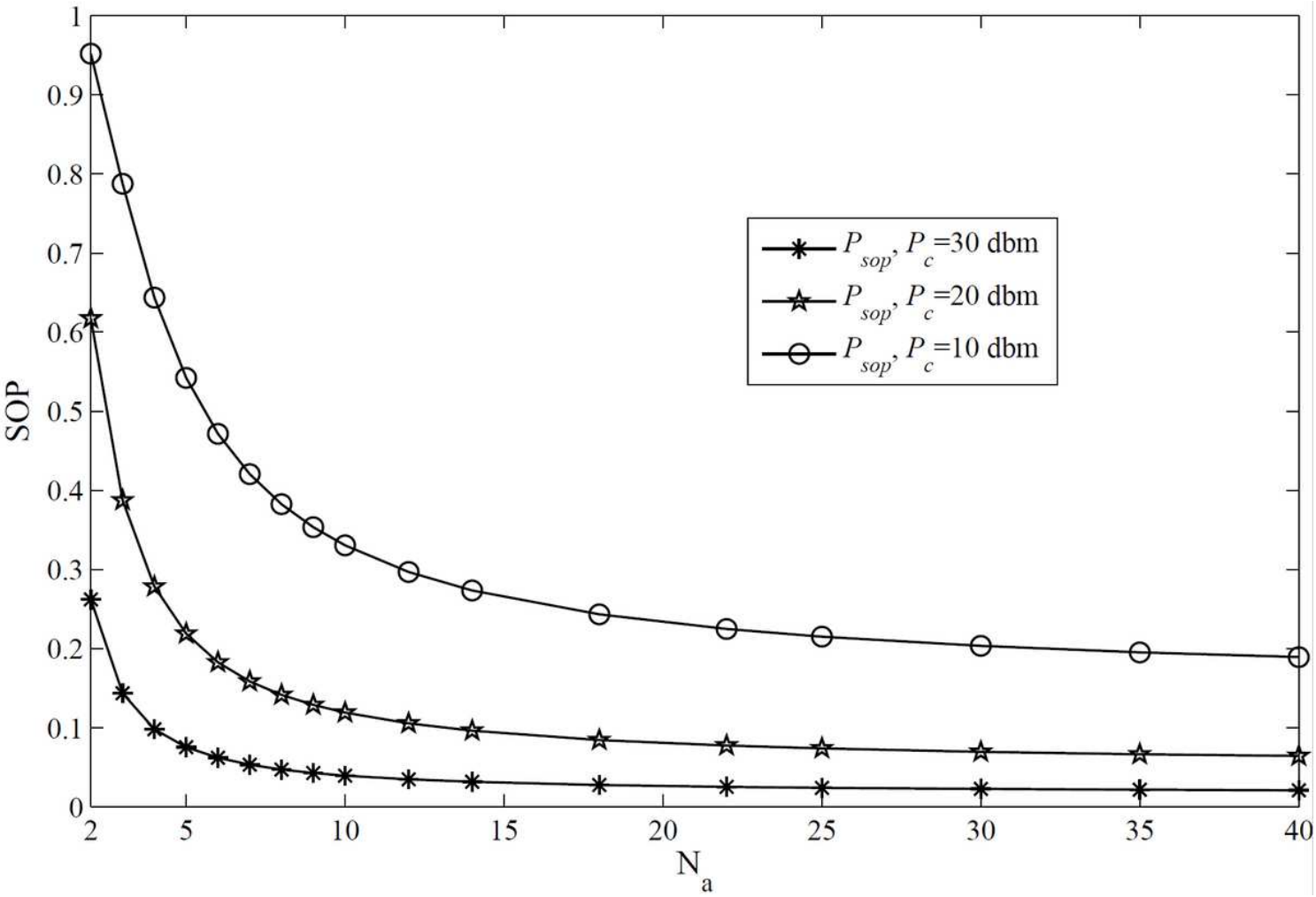


Figure 4

The SOP versus the number of antennas for different power of jammer Pc. Legends:(Pc = 30 dbm, Pc = 20 dbm, Pc = 10 dbm).

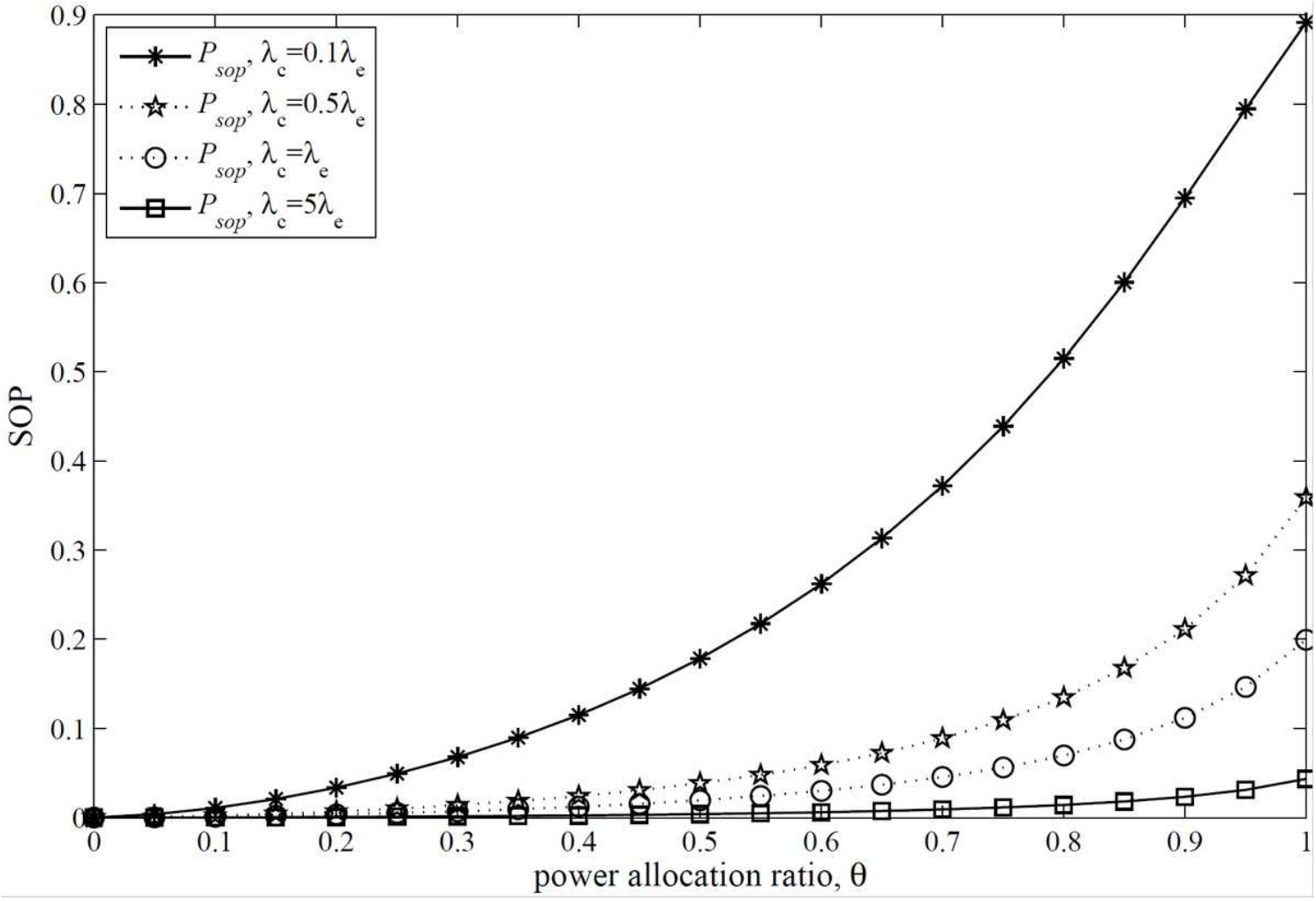


Figure 5

The SOP versus power allocation ratio θ for different density ratio. Legends:(λc = 0:1λe, λc = 0:5λe, λc = λe, λc = 5λe).

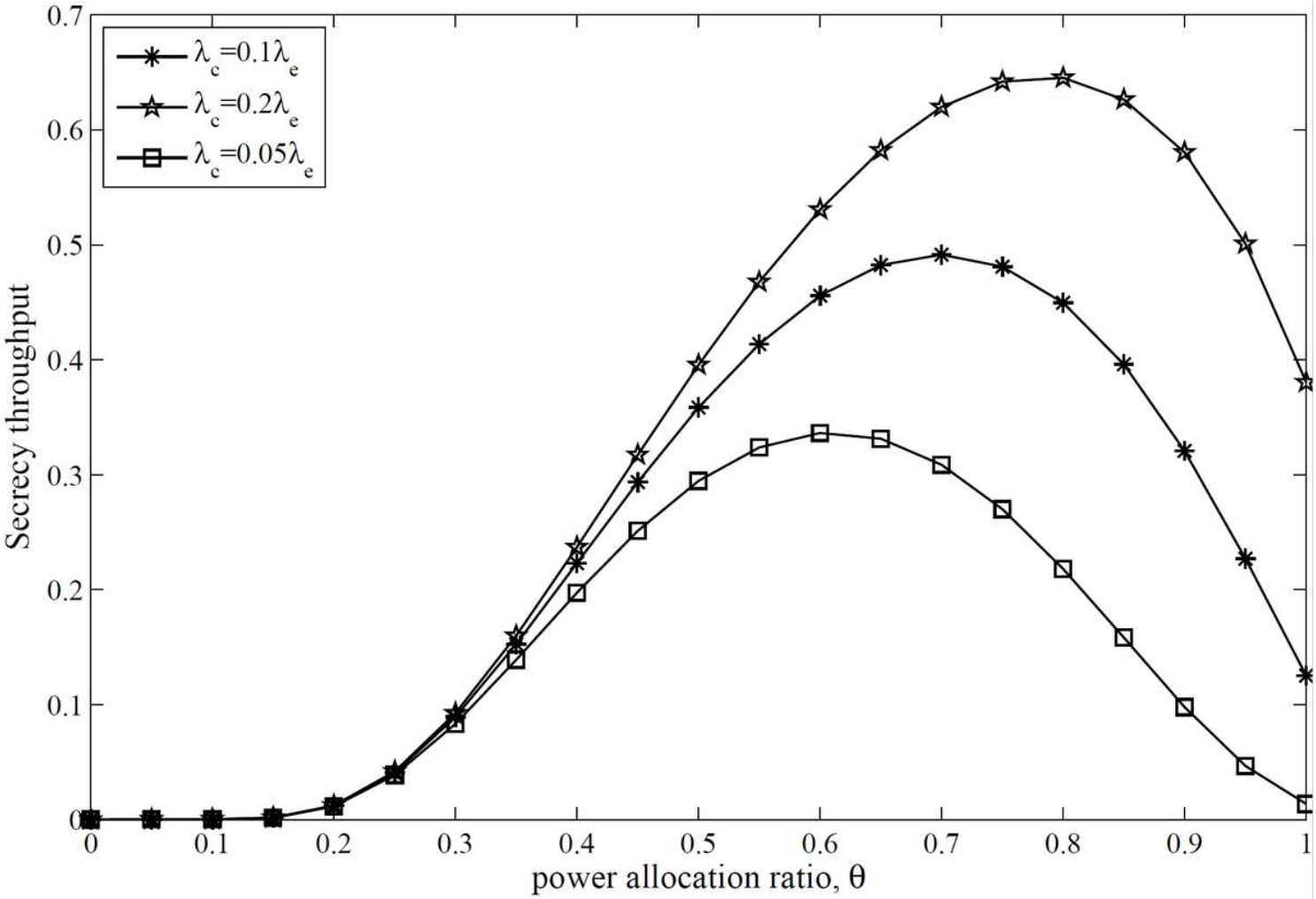


Figure 6

The secrecy throughput versus power allocation ratio θ for different density ratio. Legends:(λc = 0:1λe, λc = 0:2λe, λc = 0:05λe).

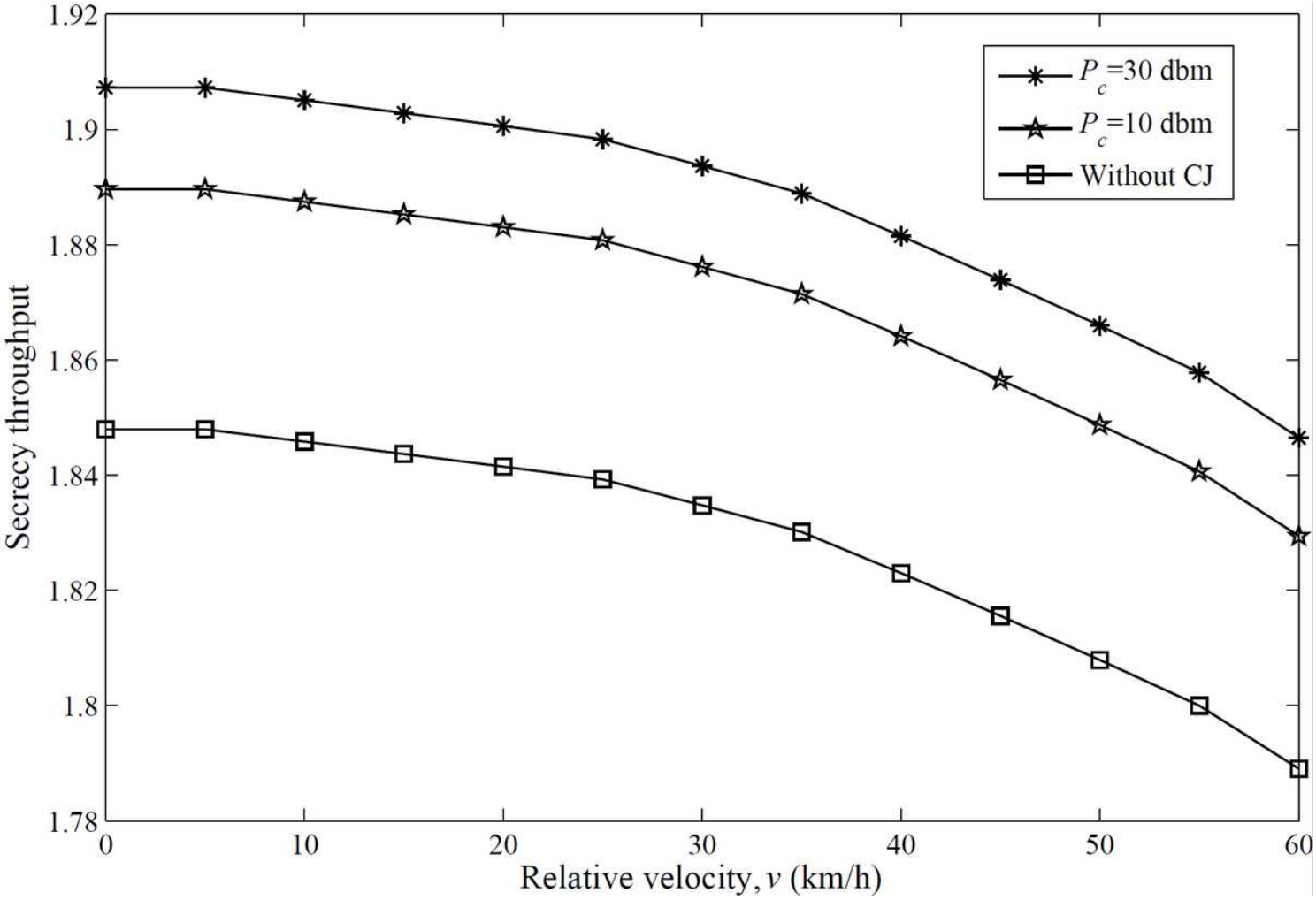


Figure 7

The secrecy throughput versus the relative vehicular velocity v. Legends:(Pc = 30 dbm, Pc = 20 dbm, without CJ).