Mobile Networks and Applications (2020) 25:643–649
https://doi.org/10.1007/s11036-019-01224-8

Physical Layer Security Performance of Mobile Vehicular Networks

Lingwei Xu[1,2] · Xu Yu[1] · Han Wang[3] · Xinli Dong[4] · Yun Liu[1] · Wenzhong Lin[2] · Xinjie Wang[5] · Jingjing Wang[1,6]

Published online: 19 April 2019

Abstract
Vehicular communication is an emergent technology with promising future, which can promote the development of mobile vehicular networks. Due to the broadcast nature of wireless channels, vehicular user mobility, and the diversity of vehicular network structures, the physical layer security issue of the mobile vehicular networks is a major concern. In this paper, the physical layer security performance of the mobile vehicular networks over *N*-Nakagami fading channels is investigated. Exact closed-form expressions for the probability of strictly positive secrecy capacity (SPSC), secrecy outage probability (SOP), and average secrecy capacity (ASC) are derived. Monte-Carlo simulation is used to verify the secrecy performance under different conditions. We further investigate the relationship between secrecy performance and the system parameters.

Keywords Mobile vehicular networks · Physical layer security · Aaverage secrecy capacity · Strictly positive secrecy capacity · Secure outage probability

1 Introduction

Since mobile user spend significant amounts of time in vehicles, the mobile vehicular computing and communication applications have increased dramatically in recent years [1–3]. Mobile vehicular communication has attracted wide research interest in the development of a wide range of applications based on user quality of experience (QoE) [4–6].

To support various types of mobile vehicular applications, the fifth generation (5G) mobile communication technologies are promising candidates [7]. A novel and practical 5G-enabled smart collaborative vehicular network architecture was introduced in [8]. [9] exploited 5G mmWave communication for vehicle positioning.5G-enabled software defined vehicular networks were proposed in [10].

Due to the vehicular user mobility, the physical layer security of 5G mobile vehicular networks is of significant interest [11–13]. An integrated network architecture was proposed for secure group communication in vehicular networks [14]. Based on a cooperative authentication method, [15] proposed an anonymous authentication protocol for vehicular networks. Closed-form expressions for the probability of strictly positive secrecy capacity (SPSC) over Rician fading channels were derived in [16], and secrecy outage probability (SOP) over correlated log-normal fading channels was investigated in [17]. In [18], the probability of SPSC with multiple eavesdroppers over log-normal fading channels. Closed-form expressions for the probability of SPSC and a lower bound on the SOP over generalized Gamma fading channels were derived in [19]. In [20], in the presence of an eavesdropper, the transmission of confidential messages in a single-input multiple-output (SIMO) system over identically independent Generalized-*K* fading channels was investigated. The physical-layer security of cooperative wireless networks with amplify-and-forward (AF) and decode-and-forward (DF) relaying were investigated in [21]. In [22], the outage probability (OP) of single-relay and multi-relay selection schemes in the presence of an eavesdropper was analyzed. [23] investigated the secure performances over non-small-scale fading channels, considering

✉ Xinjie Wang
wangxinjie@qut.edu.cn

✉ Jingjing Wang
kathy1003@163.com

[1] Department of Information Science and Technology, Qingdao University of Science and Technology, Qingdao 266061, China

[2] Fujian Provincial Key Laboratory of Information Processing and Intelligent Control, Minjiang University, Fuzhou 350121, China

[3] College of Physical Science and Engineering, Yichun University, Yichun 336000, China

[4] Qingdao Branch, China United Network Communications Corporation, Qingdao, China

[5] College of Information and Control Engineering, Qingdao University of Technology, Qingdao 266520, China

[6] State Key Laboratory of Millimeter Waves, Southeast University, Nanjing 210096, China

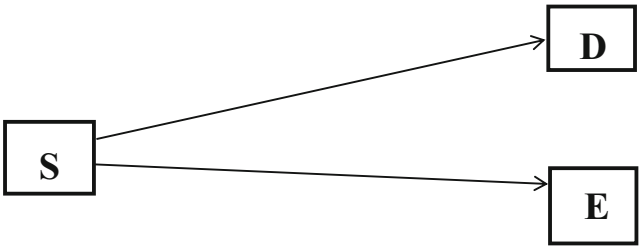

Fig. 1 The system model

Table 1 Simulation Parameters

m_D	1	1	2
m_E	2	1	1
G_D	5 dB	5 dB	5 dB
G_E	5 dB	5 dB	5 dB
N_D	2	2	2
N_E	2	2	2

the independent log-normal fading, correlated lognormal fading, or independent composite fading. [24] proposed two schemes to improve the sum rate of secondary users (SUs) while guaranteeing the secrecy rate of primary user (PU). By aligning the jamming signal together with interference among users cooperatively, an anti-jamming scheme was proposed in [25]. The authors proposed an artificial noise assisted interference alignment scheme with wireless power transfer in [26].

However, the effects of mobile communication is far severe than what can be modeled using the classical Rayleigh, Rician, Nakagami, log-normal and Generalized-*K* fading channels. They are not the best channel models for practical mobile scenarios. The *N*-Rayleigh and *N*-Nakagami fading channels were adopted in [27–29] to provide a realistic mobile channel model. In [30–32], the OP performance of mobile cooperative networks with incremental AF and DF protocols was investigated.

To date, research on physical layer security has focused on Rayleigh, Rice, Nakagami-*m* log-normal and Generalized-*K* fading channels. To the best of our knowledge, physical layer security over *N*-Nakagami fading channels has not been considered in the literature. As a consequence, the main contributions of this paper are as follows:

1. For practical mobile scenarios, it is well known that *N*-Nakagami fading channels are more general and flexible, and include the Rayleigh and Nakagami-*m* fading channels. Thus, we investigate the secrecy performance of the mobile vehicular networks model over *N*-Nakagami fading channels.
2. Closed-form expressions are derived for the average secrecy capacity (ASC), a lower bound on the SOP, and the probability of SPSC over *N*-Nakagami fading channels.
3. Monte-Carlo simulation is used to verify the accuracy of the theoretical results obtained.

The rest of the paper is organized as follows. The mobile vehicular networks model is presented in Section 2, and closed-form expressions for the ASC are derived in Section 3. A lower bound on the SOP and the probability of SPSC are presented in Sections 4 and 5, respectively. Monte-Carlo simulation results are provided in Section 6 to verify the analysis in the previous sections. Finally, some concluding remarks are given in Section 7.

2 System model

The mobile vehicular networks model is shown in Fig. 1. It consists of a mobile source (S) vehicle, a mobile eavesdropper (E) vehicle, and a mobile destination (D) vehicle, all of which are equipped with a single antenna. The S vehicle acts as a

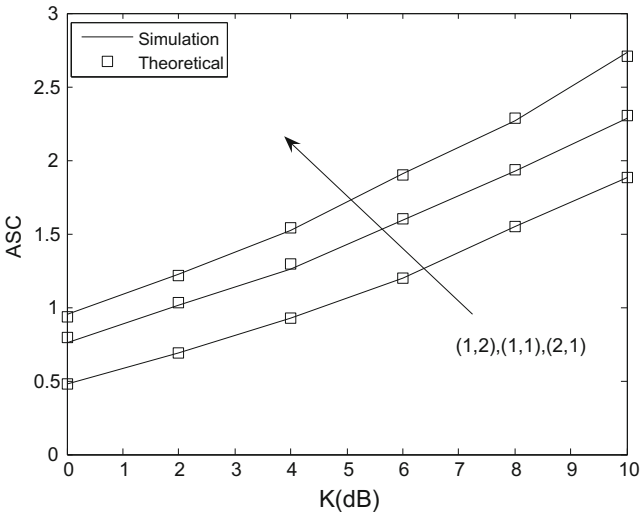

Fig. 2 ASC performance versus *K*

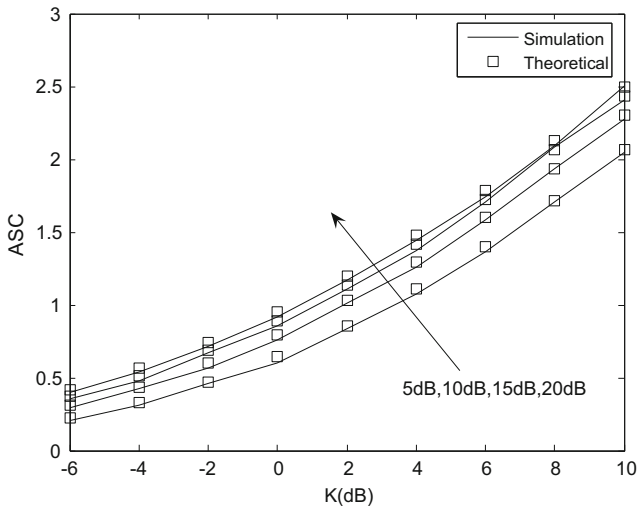

Fig. 3 ASC performance versus *K*

Table 2 Simulation Parameters

m_D	1
m_E	1
G_D	5 dB
G_E	5 dB
N_D	2
N_E	2

legal transmitter, the D vehicle acts as a legitimate receiver. When the S vehicle communicates with the D vehicle, the E vehicle can wiretap the information.

We use $h = h_k$, $k \in \{D,E\}$, to represent the complex channel coefficients of the S → D and S → E links, respectively. The probability density function (PDF) of h is given as [28].

$$f(h) = \frac{2}{h\prod_{i=1}^{N}\Gamma(m_i)} G_{0,N}^{N,0}\left[h^2\prod_{i=1}^{N}\frac{m_i}{\Omega_i}\middle|_{m_1,\ldots,m_N}^{-}\right] \tag{1}$$

where $G[\cdot]$ is Meijer's G-function.

S transmits the signal x, and the received signals r_D and r_E are given as

$$r_D = \sqrt{G_D E}h_D x + n_D \tag{2}$$

$$r_E = \sqrt{G_E E}h_E x + n_E \tag{3}$$

where E is the energy used by S, the mean and variance of n_D and n_E are 0 and $N_0/2$.Here, we use G_D and G_E to represent the relative geometrical gain of the S → D channel and the S → E channel, respectively [33].

D receives the signal-to-noise ratio (SNR) as

$$\gamma_D = KG_D|h_D|^2\overline{\gamma} \tag{4}$$

$$\overline{\gamma} = \frac{E}{N_0} \tag{5}$$

$$\overline{\gamma_D} = KG_D\overline{\gamma} \tag{6}$$

where K is the relative SNR gain.

The received SNR at the E is given as

$$\gamma_E = G_E|h_E|^2\overline{\gamma} \tag{7}$$

$$\overline{\gamma_E} = G_E\overline{\gamma} \tag{8}$$

The cumulative distribution function (CDF) of γ_k is given as

$$F_{\gamma_k}(r) = \frac{1}{\prod_{i=1}^{N}\Gamma(m_i)} G_{1,N+1}^{N,1}\left[\frac{r}{\overline{\gamma_k}}\prod_{i=1}^{N}\frac{m_i}{\Omega_i}\middle|_{m_1,\ldots,m_N,0}^{1}\right] \tag{9}$$

and the corresponding PDF is given as

$$f_{\gamma_k}(r) = \frac{1}{r\prod_{i=1}^{N}\Gamma(m_i)} G_{0,N}^{N,0}\left[\frac{r}{\overline{\gamma_k}}\prod_{i=1}^{N}\frac{m_i}{\Omega_i}\middle|_{m_1,\ldots,m_N}^{-}\right] \tag{10}$$

3 Average secrecy capacity

The instantaneous secrecy capacity is given as [34].

$$C_S = \max\{\ln(1+\gamma_D) - \ln(1+\gamma_E), 0\} \tag{11}$$

The average secrecy capacity (ASC) is the average of C_s. The ASC is given as

$$\begin{aligned}\overline{C_S} &= \int_0^\infty\int_0^\infty C_S(\gamma_D,\gamma_E)f(\gamma_D,\gamma_E)d\gamma_D d\gamma_E \\ &= \int_0^\infty\int_0^\infty C_S(\gamma_D,\gamma_E)f(\gamma_D)f(\gamma_E)d\gamma_D d\gamma_E \\ &= \int_0^\infty \ln(1+\gamma_D)f_D(\gamma_D)F_E(\gamma_D)d\gamma_D \\ &\quad + \int_0^\infty \ln(1+\gamma_E)f_E(\gamma_E)F_D(\gamma_E)d\gamma_E \\ &\quad - \int_0^\infty \ln(1+\gamma_E)f_E(\gamma_E)d\gamma_E \\ &= V_1 + V_2 - V_3\end{aligned} \tag{12}$$

With the help of [35], V_1 is given as

$$\begin{aligned}V_1 &= \frac{1}{\prod_{i=1}^{N}\Gamma(m_i)\prod_{j=1}^{N}\Gamma(m_j)} \times \\ &\int_0^\infty \ln(1+\gamma_D)\frac{1}{\gamma_D}G_{0,N}^{N,0}\left[\frac{\gamma_D}{\overline{\gamma_D}}\prod_{i=1}^{N}\frac{m_i}{\Omega_i}\middle|_{m_1,\ldots,m_N}^{-}\right]G_{1,N+1}^{N,1}\left[\frac{\gamma_D}{\overline{\gamma_E}}\prod_{j=1}^{N}\frac{m_j}{\Omega_j}\middle|_{m_1,\ldots,m_N,0}^{1}\right]d\gamma_D \\ &= \frac{1}{\prod_{i=1}^{N}\Gamma(m_i)\prod_{j=1}^{N}\Gamma(m_j)} \times \\ &\int_0^\infty G_{2,2}^{1,2}\left(\gamma_D|_{1,0}^{1,1}\right)\frac{1}{\gamma_D}G_{0,N}^{N,0}\left[\frac{\gamma_D}{\overline{\gamma_D}}\prod_{i=1}^{N}\frac{m_i}{\Omega_i}\middle|_{m_1,\ldots,m_N}^{-}\right]G_{1,N+1}^{N,1}\left[\frac{\gamma_D}{\overline{\gamma_E}}\prod_{j=1}^{N}\frac{m_j}{\Omega_j}\middle|_{m_1,\ldots,m_N,0}^{1}\right]d\gamma_D \\ &= \frac{1}{\prod_{i=1}^{N}\Gamma(m_i)\prod_{j=1}^{N}\Gamma(m_j)} \times \\ &G_{2,2:0,N:1,N+1}^{2,1:N,0:N,1}\left[\begin{matrix}0,1\\0,0\end{matrix}\middle|\begin{matrix}-\\m_1,\ldots,m_N\end{matrix}\middle|\begin{matrix}1\\m_1,\ldots,m_N,0\end{matrix}\middle|\frac{1}{\overline{\gamma_D}}\prod_{i=1}^{N}\frac{m_i}{\Omega_i},\frac{1}{\overline{\gamma_E}}\prod_{j=1}^{N}\frac{m_j}{\Omega_j}\right]\end{aligned} \tag{13}$$

V_2 is given as

$$\begin{aligned}V_2 &= \frac{1}{\prod_{i=1}^{N}\Gamma(m_i)\prod_{j=1}^{N}\Gamma(m_j)} \times \\ &G_{2,2:0,N:1,N+1}^{2,1:N,0:N,1}\left[\begin{matrix}0,1\\0,0\end{matrix}\middle|\begin{matrix}-\\m_1,\ldots,m_N\end{matrix}\middle|\begin{matrix}1\\m_1,\ldots,m_N,0\end{matrix}\middle|\frac{1}{\overline{\gamma_E}}\prod_{j=1}^{N}\frac{m_j}{\Omega_j},\frac{1}{\overline{\gamma_D}}\prod_{i=1}^{N}\frac{m_i}{\Omega_i}\right]\end{aligned} \tag{14}$$

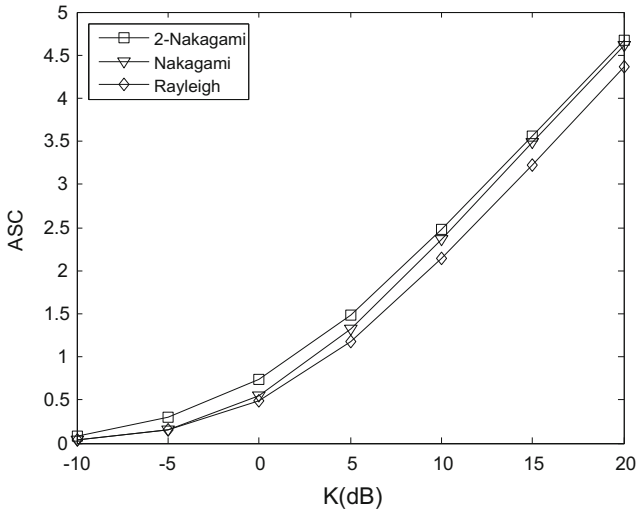

Fig. 4 SPSC performance versus K

and V_3 is given as

$$V_3 = \frac{1}{\prod_{j=1}^{N} \Gamma(m_j)} G_{2,N+2}^{N+2,1}\left[\frac{1}{\overline{\gamma_{\mathrm{E}}}} \prod_{j=1}^{N} \frac{m_j}{\Omega_j}\Big|_{m_1,\ldots,m_N,0,0}^{0,1}\right] \tag{15}$$

4 Secrecy outage probability

The SOP is the probability that the instantaneous secrecy capacity falls below a target threshold,which an important performance measure. The SOP is given as

$$\begin{aligned} F_{\mathrm{SOP}} &= \Pr(C_{\mathrm{S}}(\gamma_{\mathrm{D}}, \gamma_{\mathrm{E}}) < \gamma_{\mathrm{th}}) \\ &= \Pr(\gamma_{\mathrm{D}} < \beta\gamma_{\mathrm{E}} + \beta - 1) \\ &= \int_0^{\infty} F_{\mathrm{D}}(\beta\gamma_{\mathrm{E}} + \beta - 1) f_{\mathrm{E}}(\gamma_{\mathrm{E}}) d\gamma_{\mathrm{E}} \end{aligned} \tag{16}$$

$$\beta = \exp(\gamma_{\mathrm{th}}) \tag{17}$$

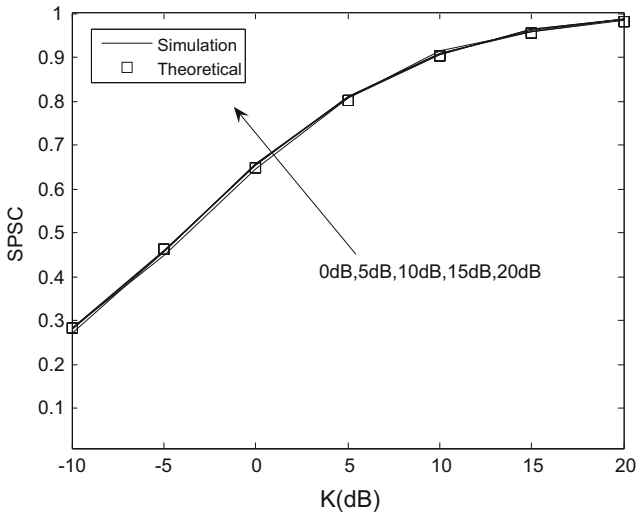

Fig. 5 SPSC performance versus K

Table 3 Simulation Parameters

m_{D}	1
m_{E}	1
G_{D}	5 dB
$\mathrm{G_E}$	1 dB
N_{D}	2
N_{E}	2

where γ_{th} is a secrecy capacity threshold. The integral in (16) has no closed-form form because of Meijer's G-function. With the aid of the results in [36–38], a lower bound on the SOP can be obtained as

$$\begin{aligned} F_{\mathrm{SOPL}} &= \Pr(\gamma_{\mathrm{D}} < \beta\gamma_{\mathrm{E}}) \\ &= \int_0^{\infty} F_{\mathrm{D}}(\beta\gamma_{\mathrm{E}}) f_{\mathrm{E}}(\gamma_{\mathrm{E}}) d\gamma_{\mathrm{E}} \\ &= \frac{1}{\prod_{i=1}^{N} \Gamma(m_i) \prod_{j=1}^{N} \Gamma(m_j)} \times \\ &\quad G_{N+1,N+1}^{N+1,N}\left[\frac{\overline{\gamma_{\mathrm{D}}}}{\beta\overline{\gamma_{\mathrm{E}}}} \frac{\prod_{j=1}^{N} \frac{m_j}{\Omega_j}}{\prod_{i=1}^{N} \frac{m_i}{\Omega_i}}\Big|_{m_1,\ldots,m_N,0}^{1-m_1,\ldots,1-m_N,1}\right] \end{aligned} \tag{18}$$

5 Probability of SPSC

The probability of SPSC means the existence of secrecy capacity,which is a fundamental benchmark in secure communications. It is given as

$$\begin{aligned} F_{\mathrm{SPNC}} &= \Pr(C_{\mathrm{S}}(\gamma_{\mathrm{D}}, \gamma_{\mathrm{E}}) > 0) \\ &= \Pr(\gamma_{\mathrm{D}} > \gamma_{\mathrm{E}}) \\ &= 1 - \int_0^{\infty} F_{\mathrm{D}}(\gamma_{\mathrm{E}}) f_{\mathrm{E}}(\gamma_{\mathrm{E}}) d\gamma_{\mathrm{E}} \end{aligned} \tag{19}$$

and substituting (9) and (10) in (19) gives

$$\begin{aligned} F_{\mathrm{SPNC}} &= 1 - \frac{1}{\prod_{i=1}^{N} \Gamma(m_i) \prod_{j=1}^{N} \Gamma(m_j)} \times \\ &\quad G_{N+1,N+1}^{N+1,N}\left[\frac{\overline{\gamma_{\mathrm{D}}}}{\overline{\gamma_{\mathrm{E}}}} \frac{\prod_{j=1}^{N} \frac{m_j}{\Omega_j}}{\prod_{i=1}^{N} \frac{m_i}{\Omega_i}}\Big|_{m_1,\ldots,m_N,0}^{1-m_1,\ldots,1-m_N,1}\right] \end{aligned} \tag{20}$$

6 Numerical results

In this section, Monte-Carlo simulation results are presented to confirm the analysis in the previous sections. Figure 2 presents the ASC performance versus K for $\overline{\gamma}$ =10 dB. The

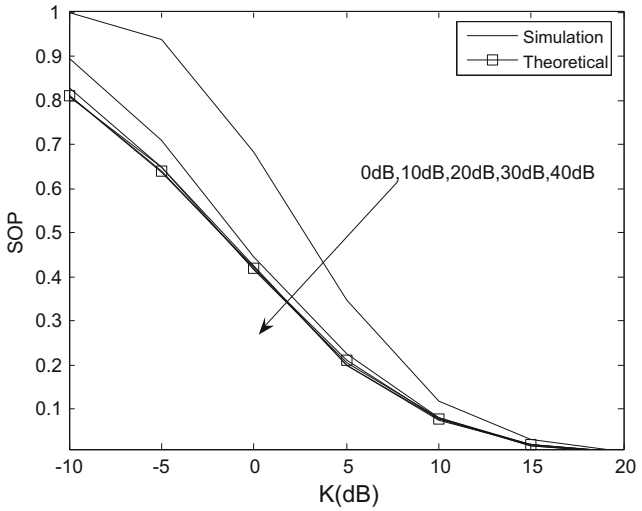

Fig. 6 SOP performance versus K

simulation parameters are given in Table 1. Combinations of m_D and m_E are denoted as (m_D, m_E). Figure 2 shows that the Monte-Carlo simulation results match very well with the analytical results. For a fixed K, the ASC performance is improved with increasing m_D and decreasing m_E. The ASC performance for (2,1) is better than that of (1,1) and (1,2). This is because the fading severity of an N-Nakagami channel is less for a larger m. Further, it is observed that the ASC performance improves as K increases. This is because a higher K means that the S → D channel is better than the S → E channel.

Figure 3 presents the ASC performance versus K with (1,1). The other simulation parameters are $\overline{\gamma}$ =5 dB, 10 dB, 15 dB, 20 dB. The simulation parameters are given in Table 2.This again shows that the Monte-Carlo simulation results match the analytical results. For fixed K, the ASC performance is improved as $\overline{\gamma}$ increases. This is because the S → D channel is better than the S → E channel.

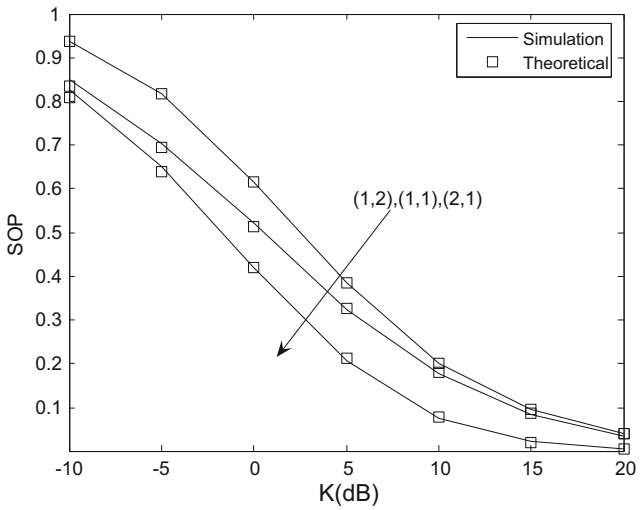

Fig. 7 SOP performance versus K

Table 4 Simulation Parameters

m_D	1	1	2
m_E	2	1	1
G_D	5 dB	5 dB	5 dB
G_E	1 dB	1 dB	1 dB
N_D	2	2	2
N_E	2	2	2

Figure 4 presents the SPSC performance versus K with $\overline{\gamma}$ =10 dB. The simulation parameters are given in Table 1. This confirms the analysis given previously as it matches the Monte-Carlo simulation results. For fixed K, the SPSC performance is improved as m_D increases and m_E decreases. The SPSC performance for (2,1) is best. Further, it is clear that the SPSC performance improves as K increases. This is because the S → D channel is better than the S → E channel.

Figure 5 presents the SPSC performance versus K with $\overline{\gamma}$ =0 dB, 5 dB, 10 dB, 15 dB, 20 dB. The simulation parameters are given in Table 3. This shows that the SPSC performance cannot be improved by increasing $\overline{\gamma}$. This observation matches the results obtained from (21)–(22).

Figure 6 presents the SOP performance versus K with (2,1). The simulation parameters are $\overline{\gamma}$ =0 dB, 10 dB, 20 dB, 30 dB, 40 dB, $G_D = 5$ dB, $G_E = 1$ dB, $N_D = N_E = 2$, and $\gamma_{th} = 0$ dB. This shows that the analytical bound on the SOP cannot be improved by increasing $\overline{\gamma}$. This observation confirms the results obtained from (18)–(20). As $\overline{\gamma}$ increases, the Monte-Carlo simulation results approach the analytical bound on the SOP.

Figure 7 presents the SOP performance versus K with $\overline{\gamma}$ =20 dB,and $\gamma_{th} = 0$ dB. The simulation parameters are given in Table 4. This again shows that the Monte-Carlo simulation results match the analytical results. For fixed K, the SOP performance is improved with increasing m_D and decreasing m_E.

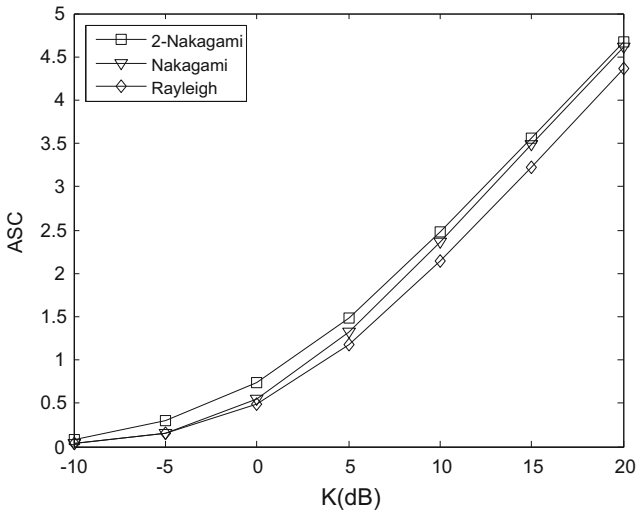

Fig. 8 ASC performance under different channels

Table 5 Simulation Parameters

	2-Nakagami	Nakagami	Rayleigh
m_D	2	2	1
m_E	2	2	1
G_D	5 dB	5 dB	5 dB
G_E	5 dB	5 dB	5 dB
N_D	2	1	1
N_E	2	1	1

The SOP performance of (2,1) is the best. Further, the SOP performance improves as K increases.

Figure 8 presents the ASC performance under different channels with $\overline{\gamma}$ =5 dB. The simulation parameters are given in Table 5. For fixed K, the ASC performance under 2-Nakagami channels is the best. This is because the fading severity of 2-Nakagami channels is larger than Nakagami and Rayleigh channels. Further, the ASC performance improves as K increases. This is because the S → D channel is better than the S → E channel.

7 Conclusion

In this paper, the secrecy performance of the mobile vehicular networks over N-Nakagami fading channels has been investigated. Exact closed-form expressions for the probability of strictly positive secrecy capacity (SPSC), secrecy outage probability (SOP), and average secrecy capacity (ASC) were derived and verified via Monte-Carlo simulations. The simulation results showed that the m, N, G_D, and G_E had a significant effect on the secrecy performance.

Acknowledgements This work was supported by the National Natural Science Foundation of China (No. U1806201, 61671261, 61304222, 61402246, 61771271, 61802217), Shandong Province Natural Science Foundation (No. ZR2017BF023), Shandong Province Postdoctoral Innovation Project (No. 201703032), Open Fund Project of Fujian Provincial Key Laboratory of Information Processing and Intelligent Control (Minjiang University) (No. MJUKF-IPIC201806), the Opening Foundation of Key Laboratory of Opto-technology and Intelligent Control(Lanzhou Jiaotong University), Ministry of Education (Grant No. KFKT2018-2),State Key Laboratory of Millimeter Waves (No. K201824),the University Science and Technology Planning Project of Shandong Province (No. J17KA058), the Doctoral Found of QUST (No. 0100229029),China Postdoctoral Science Foundation (No. 2017 M612223), Project of Shandong Province Higher Educational Science and Technology Program (No. J18KA315).

References

1. Liu X, Liu YX, Xiong NN, Zhang N, Liu AF, Shen H, Huang CQ (2018) Construction of large-scale low-cost delivery infrastructure using vehicular networks. IEEE Acc 6:21482–21497
2. Hou XM, Fu, Zhang Q, Liu D (2017) Dynamic coordination process based on predictive graph in Mobile cloud environment. J Liaocheng Univ (Natural Sci Edit) 30(4):96–100
3. Ahmed E, Gharavi H (2018) Cooperative vehicular networking: a survey. IEEE Trans Intell Trans Syst 19(3):996–1014
4. Li JQ (2018) Solving reverse logistic problem in prefabricate system by a discrete artificial bee Colony algorithm. J Liaocheng Univ (Natural Sci Ed) 31(2):102–110
5. Yu X, Chu Y, Jiang F, Guo Y, Gong DW (2018) SVMs classification based two-side cross domain collaborative filtering by inferring intrinsic user and item features. Knowl-Based Syst 141:80–91
6. Tian QY (2017) Various alternatives for optimization of open-pit-mine integrated Fleet haulage dispatching. J Liaocheng Univ (Natural Sci Edit) 30(3):88–92
7. Qiao J, He YJ, Shen XM (2018) Improving video streaming quality in 5G enabled vehicular networks. IEEE Wirel Commun 25(2): 133–139
8. Dong P, Zheng T, Yu S, Zhang HK, Yan XY (2017) Enhancing vehicular communication using 5G-enabled smart collaborative networking. IEEE Wirel Commun 24(6):72–79
9. Wymeersch H, Seco-Granados G, Destino G, Dardari D, Tufvesson F (2017) 5G mmWave positioning for vehicular networks. IEEE Wirel Commun 24(6):80–86
10. Huang XM, Yu R, Kang JW, He YJ, Zhang Y (2017) Exploring Mobile edge computing for 5G-enabled software defined vehicular networks. IEEE Wirel Commun 24(6):55–63
11. Bernardinia C, Asgharb MR, Crispocd B (2017) Security and privacy in vehicular communications: challenges and opportunities. Veh Commun 4(10):13–28
12. Manvi SS, Tangade S (2017) A survey on authentication schemes in VANETs for secured communication. Veh Commun 4(9):19–30
13. Lin ME (2016) Computer network attack modeling method based on attack graph. J Liaocheng Univ (Natural Sci Edit) 29(3):100–104
14. Lai CZ, Zhou HB, Cheng N, Shen XS (2017) Secure group communications in vehicular networks: a software-defined network-enabled architecture and solution. IEEE Veh Technol Mag 12(4):40–49
15. Jo HJ, Kim IS, Lee DH (2018) Reliable cooperative authentication for vehicular networks. IEEE Trans Intell Trans Syst 19(4):1065–1079
16. Liu X (2013) Probability of strictly positive secrecy capacity of the Rician-Rician fading channel. IEEE Wireless Commun Lett 2(1): 50–53
17. Liu X (2013) Outage probability of secrecy capacity over correlated log-normal fading channels. IEEE Commun Lett 17(2):289–292
18. Liu X (2014) Strictly positive secrecy capacity of log-normal fading channel with multiple eavesdroppers. In: IEEE International Conference on Communications (ICC), Sydney, pp 775–779
19. Lei H, Gao C, Guo Y, Pan G (2015) On physical layer security over generalized gamma fading channels. IEEE Commun Lett 19(7): 1257–1260
20. Lei H, Gao C, Ansari IS, Guo Y, Pan G, Qaraqe KA (2016) On physical layer security over SIMO generalized-K fading channels. IEEE Trans Vehic Tech 65(9):7780–7785
21. Zou Y, Wang X, Shen W (2013) Optimal relay selection for physical-layer security in cooperative wireless networks. IEEE J Select Areas Commun 31(10):2099–2111
22. Zou Y, Champagne B, Zhu WP, Hanzo L (2015) Relay-selection improves the security-reliability trade-off in cognitive radio systems. IEEE Trans Commun 63(1):215–228
23. Pan G, Tang C, Zhang X, Li T, Weng Y (2016) Physical-layer security over non-small-scale fading channels. IEEE Trans Vehic Tech 65(3):1326–1339
24. Cao Y, Zhao N, Richard Yu F, Jin M, Chen Y, Tang J, Leung VCM (2018) Optimization or Alignment: Secure Primary Transmission

Assisted by Secondary Networks. IEEE J Sel Areas in Comm (JSAC) 36(4):905–917
25. Zhao N, Yu FR, Li M, Yan Q, Leung VCM (2016) Physical layer security issues in interference- alignment-based wireless networks. IEEE Commun Mag 54(8):162–168
26. Zhao N, Cao Y, Yu R, Chen Y, Jin M, Leung VCM (2018) Artificial Noise Assisted Secure Interference Networks with Wireless Power Transfer. IEEE Trans Vehic Tech
27. Salo J, El-Sallabi HM, Vainikainen P (2006) The distribution of the product of independent Rayleigh random variables. IEEE Trans Antennas Prop 54(2):639–643
28. Karagiannidis GK, Sagias NC, Mathiopoulos PT (2007) N*Nakagami: a novel stochastic model for cascaded fading channels. IEEE Trans Commun 55(8):1453–1458
29. Xu L, Yu X, Wang H, X Wang, J Wang (2018) Secrecy performance of mobile image transmission networks. 11th EAI International Conference on Mobile Multimedia Communications
30. Xu L, Wang J, Liu Y, Shi W, Gulliver TA (2018) Outage performance for IDF relaying Mobile cooperative networks. Netw Appl 23(6):1496–1501
31. Xu LW, Zhang H, Wang JJ, Gulliver TA (2017) Joint TAS/SC and power allocation for IAF relaying D2D cooperative networks. Wirel Netw 23(7):2135–2143
32. Xu LW, Wang JJ, Zhang H, Gulliver TA (2017) Performance analysis of IAF relaying mobile D2D cooperative networks. J Frankl Inst 354(2):902–916
33. Ilhan H, Uysal M, Altunbas I (2009) Cooperative diversity for intervehicular communication: performance analysis and optimization. IEEE Trans Vehic Tech 58(7):3301–3310
34. Bloch M, Barros J, Rodrigues MR, McLaughlin SW (2008) Wireless information-theoretic security. IEEE Trans Vehic Tech 54(6):2515–2534
35. The Wolfram Functions Site. http://functions.wolfram.com/HypergeometricFunctions/MeijerG/21/02/04/
36. Lei H, Ansari IS, Pan G, Alomair B, Alouini MS (2017) Secrecy capacity analysis over α−μ fading channels. IEEE Commun Lett 21(6):1445–1448
37. Yang Q, Wang H (2015) Toward trustworthy vehicular social networks. IEEE Commun Mag 53(8):42–47
38. Yang Q, Lim A, Li S, Fang J, Agrawal P (2010) ACAR: Adaptive connectivity aware routing for vehicular ad hoc networks in city scenarios. Mobile Netw Appl 15(1):36–60