On Physical Layer Security over α-η-k-μ Fading for Relay based Vehicular Networks

Sagar Kavaiya*, Dhaval K Patel[†], Yong Liang Guan[‡], Sumei Sun[§], Yoong Choon Chang[¶], Joanne Mun-Yee Lim[‖]
*[†]School of Engineering and Applied Science, Ahmedabad University, India
[‡]School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore
[§]Institute for Infocomm Research, Singapore
[¶]Department of Electrical and Electronic Engineering, Universiti Tunku Abdul Rahman, Malaysia
[‖]School of Engineering, Monash University, Malaysia
Email: *[†]{sagar.k, dhaval.patel}@ahduni.edu.in, [‡]EYLGUAN@ntu.edu.sg,
[§]sunsm@i2r.a-star.edu.sg, [¶]ycchang@utar.edu.my, [‖]Joanne.Lim@monash.edu

***Abstract*—In this paper, we study the secrecy problem for a relay-based vehicular network. We assume that the legitimate transmitter, legitimate receiver, and eavesdropper are equipped with a single antenna. By considering various initial positions of the relay, we obtain the statistical knowledge of the received signal-to-noise ratio over α-η-k-μ fading channel under vehicle mobility. Further, we derive an exact closed form expression for outage probability and secrecy outage probability utilizing the amplify-and-forward relay protocol for a two-lane high way scenario. Monte-Carlo simulations are performed to validate the accuracy of the derived analytical expressions.**

***Index Terms*—Physical layer security, α-η-k-μ fading, secrecy outage probability, eavesdropping, outage probability.**

I. Introduction

Due to the broadcast nature of wireless channels, the confidentiality of the messages is compromised throughout the transmission so that the security and privacy of the messages are vital challenges to handle [1]. The idea of the physical layer security (PLS) is to exploit the physical layer's characteristics to transmit messages in a secure manner [2]. Due to the mobility of the users, the wireless link can be more vulnerable to security threats such as eavesdropping so that it is challenging to provide PLS in vehicular communications [2].

Extensive work has been carried out in open literature, which focuses on the secrecy performance of static users. Shannon has proposed the communication theory for the secrecy system in [3], and the theoretical approach has been covered for the secrecy systems. As the work is limited to the noiseless channels, the secrecy performance of the Gaussian wiretap channel has been carried out in [4]. The detailed analysis for the secrecy capacity and secrecy outage probability (SOP) was carried out over a Rayleigh fading channel in [5]. Furthermore, for the static users, the secrecy performance was also analyzed over the various fading models such as Nakagami-q, κ- μ, and α-μ in [6]–[9]. Securing communication over cognitive radio enabled wireless networks over Nakagami-m channels was analyzed in [10], and the extensive analysis of secrecy outage probability was proposed.

Apart from these works, to improve the security in wireless networks, various relay-based schemes for underlay cognitive radio systems were covered in [11], [12] and authors have shown the usage of cooperative relaying by utilizing the amplify-and-forward, decode-and-forward, and, cooperative jamming. It has been found that emerging communication scenarios (e.g., mobile-to-mobile communication in 5G networks) need to adopt the versatile channel model so that PLS over α-η-k-μ for the static users was analyzed in [13]. To be more realistic, the secrecy problem for vehicular communication without consideration of the relay-based network was handled in [14], and the impact of mobility on PLS is studied in [15]. In practice, infotainment applications in emergency vehicle services need extra security during transmission because it carries sensitive information. Moreover, the broadcasting of essential safety messages can be performed over a secure communication link for that the modeling of the fading channel has to be accurate. Therefore, we carried out this research over recently proposed dynamic fading α-η-κ-μ fading channel, which is suitable and accurate for a vehicular environment. The fading model encounters the amplitude and phase envelope in its probability distribution function (PDF) [16]. To the best of the authors' knowledge, no work is carried out in the previous literature, which considers the impact of mobility on PLS over α-η-κ-μ fading channel with a relay-based highway scenario. The main contributions of our work are as follows:

1) We first obtain the statistical knowledge of received signal-to-noise ratio (SNR) by considering initial positions of the relay under the impact of mobility. Furthermore, we derive an exact closed-form expression of outage probability over α-η-κ-μ fading channel with the amplify-and-forward relay protocol. Moreover, when we assume the velocity as zero with no relay, the derived expressions are reduced as given in [13].
2) To maintain the perfect secrecy in the presence of passive and mobile eavesdropper located in the network, we provide SOP analysis over α-η-κ-μ fading channel. We conclude with the asymptotic analysis of the secrecy outage probability to provide more insights on secrecy performance.

The upcoming sections of the paper are as follows: Section II describes the system model. In Section III, derivation of the received SNR over the various initial position of the legitimate receiver is carried out. In Section IV, secrecy performance over α-η-κ-μ fading channel is evaluated. Section V describes the numerical results followed by conclusion.

II. System Model

In this section, we consider a cognitive radio network consisting of one legitimate transmitter and one legitimate receiver in the presence of one eavesdropper. Each user contains the single antenna [11].

978-1-7281-8895-9/20/$31.00 © 2020 IEEE

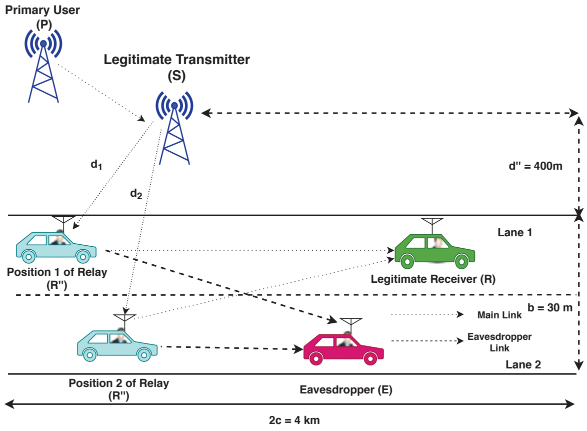

Figure 1: Highway vehicular network model

A. Network Model

The road traffic scenario with dense traffic on a two-lane highway as a cognitive vehicular model is shown in Fig. (1). S denotes the legitimate static transmitter. The road length is $2c$ and width is b. The network model illustrates the location of the relay under two cases. The distance between the nearer edge of the road and legitimate transmitter is d'', and the road width is considered as b.

B. Channel Model

Consider the highway vehicular scenario suggested in Fig. (1). The relay vehicle (R'') equipped with a single antenna, based on its initial positions from the legitimate transmitter is shown. The relay vehicle is allowed to receive information after the resource allocation has been provided in a cognitive radio-based network. Here, vehicle (E) performs the role of a passive eavesdropper, which is a part of a network. The channel state information is considered to be perfect. The channel model of α-η-κ-μ is considered as follows [16]:

$$f_R(r) = \frac{\alpha r^{\alpha\mu-1} \sum_{k=0}^{\infty} \frac{k! c_k L_k^{\mu-1}(2r^\alpha)}{(\mu)_k}}{2^\mu \Gamma(\mu) \exp\left(\frac{r^\alpha}{2}\right)}, \tag{1}$$

where R denotes envelope, α indicates non-linearity parameter of the medium, k is the ratio of total power of dominant components to the scattered total power. Moreover $\Gamma(\cdot)$ is the Gamma function [17, Eq. (8.310.1)]. $(\cdot)_k$ is the Pochhammer symbol [17, Eq.(6.1.22)], $L(\cdot)_k^{\mu-1}$ is the Lagrangian polynomial [17, Eq. (8.970.1)]. Furthermore, c_k is computed with the recursive equation defined in [16, Eq. (15)].

C. Signal Model

In this section, we define the signal model received at relay nodes and legitimate receiver in the presence of a mobile eavesdropper. The signal is transmitted through the legitimate transmitter (S) to a legitimate receiver (R) through the relay nodes (R”). At the first instant, the signal received by node (R”) is

$$y(t) = h_{SR''}(t)x(t) + n_{R''}(t), \tag{2}$$

where $h_{SR''}$ is a channel coefficient vector under the effect of mobility between the relay node and legitimate transmitter, x is the transmitted symbol, n is the complex hardware additive white Gaussian noise. At the same time, t denotes the time constraint, which implies the channel is time-varying or the received signal varies concerning the mobility of the vehicle. The channel gain h is given as:

$$h_{SR''}(t) = \frac{g_x}{\sqrt{1 + d_x^\zeta(t)}} \tag{3}$$

where g_x represents the channel gain following the α-η-κ-μ fading, ζ denotes the path loss component given in [18]. Since the vehicles are moving, d_x represents the distribution of the distance d given in [19]. Further, the received signal after amplifying and forwarding at the legitimate transmitter is given as:

$$\begin{aligned} y'(t) &= h_{R''R}(t)y(t) + n_R(t) \\ &= h_{R''R}(t)(h_{SR''}(t)x(t) + n_{R''}(t)) + n_R(t) \end{aligned} \tag{4}$$

where $h_{R''R}$ is channel coefficient vector under the effect of mobility between relay node and legitimate receiver.

III. Statistical Knowledge of Received Signal to Noise Ratio under Mobility

In order to evaluate the secrecy performance, the received SNR under the vehicle mobility can be derived for α-η-κ-μ fading by calculating the CDFs, for which, the general formula is given as:

$$F_Z(z) = \int_0^\infty \int_{-\infty}^{yz} f_{XY}(x, y) dx dy \tag{5}$$

where, for each case, $f_X(x)$ and $f_Y(y)$ is replaced by the independent distribution of fading channel and distance respectively.

1) Case 1: Relay is nearer to legitimate transmitter (Position 1) : The PDF of distance between SU and PU is defined as [19, Eq. (11.1)]. By substituting ([19, Eq. (11.1)]) and (1) in the (5), the CDF is obtained for the $case1$, which is further differentiated to obtain the PDF as (8).

2) Case 2: Relay is at far distance from legitimate transmitter (Position 2) : The PDF of distance for this case d is given as [19, Eq. 11.2]. By substituting ([19, Eq. 11.2]) and (1) in the (5), the CDF is obtained for the $case2$, which is further differentiated to obtain the PDF as (9). To solve the initial integrals we first convert it into a hyperbolic function to discover the appropriate identity in the second integral term which is defined as [17, Eq. (2.741.1)]. The obtained solutions are the CDF of the received SNR under the impact of mobility which further differentiated to calculate the PDFs. Furthermore, as the integral does not converge without a conditions, we opt the conditional expression by considering the $z < 1$. The CDFs are obtained from this methods are consisting of the impact of mobility with the fading conditions.

For proof, refer Appendix A ■

IV. Secrecy Performance over α-η-κ-μ Fading Channels

A. Analysis of the Outage Probability

Outage is stated as the probability that the received instantaneous SNR γ falls below a threshold γ_{th}. In this section, we derive the outage probability with respect to the various initial positions of relay node. The general formula to derive an outage probability is given as:

$$P_{out} = Pr(0 \leq \gamma \leq \gamma_{th}), \tag{6}$$

$$P_{out} = \int_0^{\gamma_{th}} f_\gamma(\gamma) dz, \tag{7}$$

$$p_\gamma(\gamma)_{case1} = \frac{\left(\frac{\gamma\mu}{\overline{\gamma}}\right)^{d(\mu-1)} exp\left(\frac{-\gamma}{\overline{\gamma}\times(1-(\alpha))}\right) \times F_1(\kappa, 1/2ab; \frac{\mu\times det(\alpha)d}{(1-det(\alpha+2d))})}{(1-det(\mu))^d} \tag{8}$$

$$p_\gamma(\gamma)_{case2} = \frac{\left(\frac{\gamma\mu}{\overline{\gamma}}\right)^{d(\mu-1)} exp\left(\frac{-\gamma}{\overline{\gamma}\times(1-(\alpha))}\right) \times \beta(i,j,k,l)}{(1-det(\alpha))^d} \tag{9}$$

$$P_{out}^{case1} = 1 - e^{ab/z_{th}} \sum_{z=1}^{T_k} \sum_{n=0}^{\alpha} \Gamma(e^{z-1} + z) + (\alpha^3/2e^{-d} + \eta^2)C_k + D_k \tag{10}$$

$$P_{out}^{case2} = 1 - e^{ab/z_{th}} \sum_{n=1}^{T_k} \sum_{n=0}^{\alpha} \Gamma(e^{\mu-1} + z^n) + (\psi^3/2e^{-d} + \eta^2)F_k + E_k \tag{11}$$

where $f_\gamma(\gamma)$ is a respective PDF of the received SNR for *case* 1 and *case* 2 . Therefore, by substituting (8) and (9) in 7, we can obtain the outage probability for *case* 1 and *case* 2 respectively as:

$$P_{out}^{case1} = \int_0^{\gamma_{th}} p_\gamma(\gamma)_{case1} d\gamma \tag{12}$$

$$P_{out}^{case2} = \int_0^{\gamma_{th}} p_\gamma(\gamma)_{case2} d\gamma \tag{13}$$

The above integrals are solved with the aid of identities given in [17, Eq. (6.711.1)]. The outage probabilities for *case* 1 and *case* 2 is given as (11). where, $A_k = \left(\frac{\alpha}{\Gamma(\mu)}\right)$, $B_k = \left(\frac{\Gamma(d)}{\Gamma(\kappa)}\right)$, $C_k = \frac{z}{2ab\mu}$, $D_k = \frac{1-det(\alpha)}{4d}$, $E_k = \frac{2}{\Gamma(\kappa)}$, $F_k = \left(\frac{\Gamma(d'')L}{\Gamma(\alpha)}\right)$. Note that k $\in R, E$.

B. Analysis of the Secrecy Outage Probability

In this section, we analyze the secrecy outage probability at the passive eavesdropper side because the aim is to observe the capability of eavesdropper to intrude. However, the legitimate transmitter does not have the CSI information of eavesdropper's channel and hence it has no choice to encode data under a constant code rate R_s.

The instantaneous secrecy capacity is given by [10]

$$C_s(\gamma_E, \gamma_R) = max\left\{ln(1+\gamma_E) - ln(1+\gamma_R), 0\right\} \tag{14}$$

where γ_E and γ_R are the received SNR at eavesdropper and legitimate receiver respectively.

$$Pr\left\{C_s(\gamma_R, \gamma_E) \leq R_s\right\} \tag{15}$$

For the cognitive network the transmitter power at S can be expressed as

$$P_s = min\left(P_{max}, \frac{I_p}{X}\right), \tag{16}$$

where X is a channel gain between primary transmitter and legitimate transmitter, I_P is the interference power, P_{max} is the maximum transmitted power. Here, this channel is considered as perfect hence to obtain the average outage. Using (16) the SOP of can be expressed as :

$$\begin{aligned} P_{sop} = &\underbrace{Pr\left\{C_s(\gamma_R, \gamma_E) \leq R_s, P_s = P_{max}\right\}}_{I_1} \\ &+ \underbrace{Pr\left\{C_s(\gamma_R, \gamma_E) \leq R_s, P_s = \frac{I_p}{X}\right\}}_{I_2}, \end{aligned} \tag{17}$$

The above formula is used to derive the SOP for both the cases, the integral is divided into several sub-integral under certain equality such as when $P_s = P_{max}$, the term I_1 is given by

$$\begin{aligned} I_1 &= Pr\left\{C_s(\gamma_R, \gamma_E) \leq R_s, P_s = P_{max}\right\} \\ &= Pr\left\{Z_R \leq \theta Z_E + \frac{\theta-1}{\alpha}\right\} Pr\left\{x \leq \frac{I_P}{P_{max}}\right\} \end{aligned}$$

$$= \underbrace{\int_0^\infty F_{Z_R}\left(\theta z + \frac{\theta-1}{\alpha}\right) f_{Z_E}(z) dz}_{I_{11}} Pr\left\{x \leq \frac{I_P}{P_{max}}\right\}$$

where F_{Z_R} and f_{Z_E} are respective CDFs and PDFs for the desired cases, $\theta = e^{R_s}$, $Pr\left\{x \leq \frac{I_P}{P_{max}}\right\}$ is given as 1/ $\Gamma(m)$ as per [10]. The derivation of I_{11} can be given as :

$$I_{11} = \int_0^\infty F_{Z_R}\left(\theta z + \frac{\theta-1}{\alpha}\right) f_{Z_E}(z) dz \tag{18}$$

By substituting (8) in (18), the general expression is obtained as follows which further utilised to calculate I_1 as:

$$I_{11} = \int_0^\infty F_{\gamma_R}\left(\theta\gamma + \frac{\theta-1}{\alpha}\right) \times p_\gamma(\gamma)_{case1} d\gamma \tag{19}$$

Further for the derivation of I_2, the general formula is given as per [10]. When the $P_S = \frac{I_P}{X}$, by using (15), we can obtain

$$I_2 = \int_{I_p/P_{Max}}^\infty H(x) f_X(x) dx, \tag{20}$$

where, $H(x)$ is the PDF of fading channel as per (1) and $f_X(x)$ can be replaced as PDF of received SNR for *case* 1 and *case* 2. Hence the final expression of the SOP is the summation of the derivation I_1 and I_2 as per (17) which is provided as P_{SOP}^{Case1} and P_{SOP}^{Case2} in Appendix section.

C. Asymptotic Analysis of Secrecy Outage Probability

In this section, we obtain the asymptotic analysis to gain more insight on secrecy performance. The SNR at the eavesdropper side can affect the complete secrecy performance hence, from (18) and (20) by considering the SNR $\overline{\gamma_E} = \overline{\gamma} \to \infty$, we have :

$$\overline{C}_s \approx \frac{\alpha_E \alpha_R}{2^{\mu_{R''}+\mu_R+2}\Gamma(\mu_R)\Gamma(\mu_{R''})} \sum_{k=0}^{\infty} \frac{k! c_{k,R''}}{(\mu_E)_k} \sum_{l=0}^{\infty} \frac{l! c_{l,R}}{(\mu_R)_l} T_0,$$

,

where, T_0 is $(J_1 - J_2)$. Provided that the P_{max} is constant at 1W throughout the transmission, the variation in the I_p

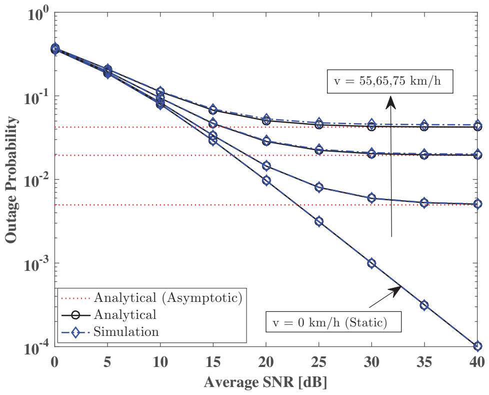

Figure 2: Outage probability against received SNR for case 1 (μ = 1, d' = 100m, $\overline{\gamma}$ = 2 dB at Eve, c =2 km, b = 30m, α = 1, κ = 1)

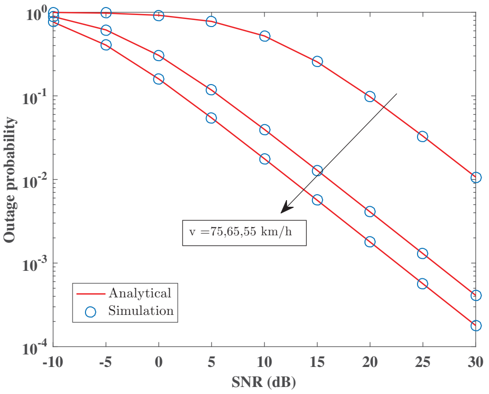

Figure 3: Outage probability against received SNR for case 2 (μ = 1, d' = 100m, $\overline{\gamma}$ = 2 dB at Eve, c =2 km, b = 30m, α = 1, κ = 1

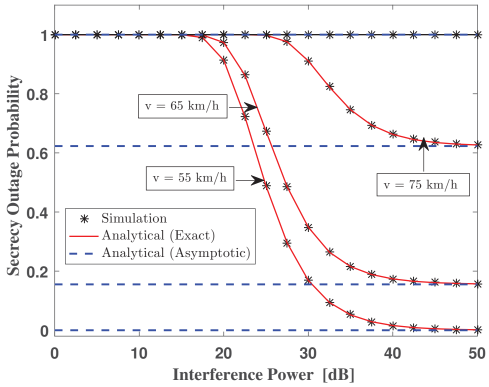

Figure 4: Secrecy outage probability against interference power for case 1 (μ = 1, d' = 100m, $\overline{\gamma}$ = 2 dB at Eve, c =2 km, b = 30m, α = 1, κ = 1)

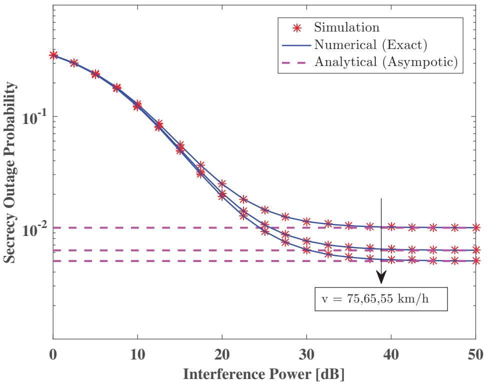

Figure 5: Secrecy outage probability against interference power for case 2 (μ = 1, d' = 100m, $\overline{\gamma}$ = 2 dB at Eve, c =2 km, b = 30m, α = 1, κ = 0

affects the SOP which can be defined as the intermediate term J_1 for the *case* 1 is given as:

$$J_1 = \int_0^\infty v^{\frac{\alpha_E\mu_E}{2}-1} e^{\left(\frac{-v^{\frac{\alpha_E}{2}}}{2}\right)} L_k^{\mu_E-1} \times \left(2v^{\frac{\alpha_E}{2}}\right) \times \int_v^\infty \ln(u) \times u^{\frac{\alpha_R\mu_R}{2}-1} e^{\left(\frac{-u^{\frac{\alpha_R}{2}}}{2}\right)} L_l^{\mu_R-1} \left(2u^{\frac{\alpha_R}{2}}\right) dudv \tag{21}$$

The intermediate term J_2 for the *case* 1 is given as:

$$J_2 = \int_0^\infty \ln(v) \times v^{\frac{\alpha_E\mu_E}{2}-1} e^{\left(\frac{-v^{\frac{\alpha_E}{2}}}{2}\right)} L_k^{\mu_E-1} \times \left(2v^{\frac{\alpha_E}{2}}\right) \times \int_v^\infty u^{\frac{\alpha_R\mu_R}{2}-1} e^{\left(\frac{-u^{\frac{\alpha_R}{2}}}{2}\right)} \times L_l^{\mu_R-1} \left(2u^{\frac{\alpha_R}{2}}\right) dudv \tag{22}$$

Since both J_1 and J_2 consist of infinite integral terms, it is replaced by the appropriate identities provided in [17, Eq. (6.711.1),(6.711.2)]. Similarly, for the case 2, the term J_1 and J_2 can be evaluated. Note that, to evaluate the asymptotic performance of the secrecy outage probability under both the cases, the consideration of the SNR values at the eavesdropper side should be very high. Since the analysis is carried out for the eavesdropper side we focus on the velocity of the eavesdropper rather than the legitimate receiver because the aim is to get over the capability of the eavesdropping.

V. Numerical Results

This section presents the simulation results carried out to validate the accuracy of derived analytical expressions of outage probability and secrecy outage probability. We generate the samples of α-η-κ-μ fading channel as per [20]. For simulations R_s = 0.1 bits/s/Hz and P_{max} = 1W are considered. By considering the highway scenario of two lane, the analytical expression derived in Section III for outage probability states that the conditions for outage is depends on the vehicle velocity as well as the SNR at the relay node. Furthermore, we consider the fixed velocity in order to obtain the behavior of the outage probability under all cases. By looking on the behavior the secrecy outage probability for all cases, it can be seen that for certain fix interference power in cognitive radio systems and fix velocity the secrecy outage is depended on the fading parameter between the relay node and legitimate receiver. The results are obtained for best possible values of α, κ and μ.

Fig. (2) shows the OP performance when the relay node is nearer to the legitimate transmitter. As we can observe, under the specific fading parameter and fix velocity of 55, 65 and 75 km/h respectively, the OP performance is degraded with the increased velocity but the variation in the degradation is low which implies that if the relay node is near to the legitimate transmitter, to procure the secure transmission at higher velocities, the SNR requirement is low. Fig. (3) shows the OP performance when the relay node is at far distance the legitimate transmitter. As we can observe, under the specific fading parameter and fix velocity of 55, 65 and 75 km/h respectively, the OP performance is degraded with the increased velocity but the variation in the degradation is high which implies that if the relay node is at far distance the legitimate transmitter, to procure the secure transmission at higher velocities, the SNR requirement is high. Fig. (4) shows the SOP performance when the relay node is nearer to the legitimate transmitter. As we can observe, under the specific fading parameter and fix velocity of 55, 65 and 75 km/h respectively, the SOP performance is degraded with the increased velocity which implies that, to procure the secure transmission at higher velocities the SNR or secrecy rate should be higher. However, the secrecy performance is depended on the chosen fading parameters. In this case we have obtained the results for best possible fading parameters. Fig. (5) shows the SOP performance when the relay node is at far distance to the legitimate transmitter. As we can observe, under the specific fading parameter and fix velocity of 55, 65 and 75 km/h respectively, the SOP performance is degraded with the increased velocity but the variation in the degradation is high compare to the case 1.

VI. Conclusions

In this paper, we have investigated the secrecy outage probability and outage probability to secure communications over α-η-κ-μ for vehicular communications in which various relay position such as near to the legitimate transmitter and far from the transmitter are being considered. We observe that under the impact of velocity, it is better to have the relay at nearer to the legitimate transmitter under the dynamic fading conditions. Performance is degraded under the high velocities of the vehicle. The exact closed form expressions for outage and secrecy outage have been derived. We have also observed the joint impact of fading parameters and relay positions on the outage and secrecy outage probability. However, for the some values of low fading parameter with the impact of high velocity, greater than 0.6 can results in the worst performance. We also observe the impact of mobility on outage with respect to asymptotic conditions under the perfect channel estimation.

Appendix A
Derivation of Distribution of Received SNR

Since both the distributions are independent from each other and by substituting ([19, Eq. (11.1)]) and (1) in (5) we have,

$$F_Z(z)^{case1} = \int_0^\infty \int_{-\infty}^{yz} \frac{\alpha r^{\alpha\mu-1} \sum_{k=0}^{\infty} \frac{k! c_k L_k^{\mu-1}(2r^\alpha)}{(\mu)_k}}{2^\mu \Gamma(\mu) \exp\left(\frac{r^\alpha}{2}\right)}$$
$$\frac{d}{4ab}\left[\pi + 2arcsin\left(\frac{2(y^2-(b-h)^2)}{y^2}\right) - 1\right] drdy \quad (23)$$

At first integrating the inner integral with respect to dr and from [17] the integral in (23) is further given by considering the appropriate identities as:

$$F_Z(z)^{case1} = \frac{z^2}{ab}\frac{1}{\Gamma(\mu)}\left(\frac{1}{det(\alpha)}\right)^m \times$$
$$\int_0^\infty yArcsin\left(2y^2 - \frac{(b-h)^2}{y^2}\right) \times \frac{k! c_k L_k^{\mu-1}(2r^\alpha)}{d} dy \quad (24)$$

Using [17], we first obtained CDF which is further simplified in PDF given as (8). Similar process is carried out to obtain the PDF for $case$ 2 as (9). Where, $\beta = F_1(\kappa, 1/2ab; \frac{\mu \times det(\alpha)d}{(1-det(\alpha+2d))})$, $F_1 = \left[\{0.5,\mu,\alpha\},\{1.5,d\},yz^2\right]$. Similarly substituting (1) and (6)in (25), PDF for $case$ 2 can be expressed as (20). Where, $i = \frac{z}{2ab\kappa}$, $j = \frac{1-det(\alpha)}{4d}$, $k = \frac{2z}{2d^2+1}$, $l = \frac{1-det(\alpha)}{\mu}$ and $\beta(i,j,k,l)$ is the polynomial function given in [17]. Furthermore, the SOP expression from the integral for $case$ 1 is provided as:

$$P_{SOP}^{Case1} = \frac{\alpha_E 2^{-(\mu_E+\mu_R+2)} \overline{\gamma_R}^{\frac{-\alpha_B \mu_R}{2}}}{\Gamma(\mu_E)\Gamma(\mu_R)\overline{\gamma_E}^{\frac{\alpha_E \mu_E}{2}}} \sum_{n=0}^{\infty} \frac{n! c_{n,E}}{(\mu_E)_n} \sum_{s=0}^{n} T_1$$

where, $T_1 = \frac{\beta(i,j,k,l)}{s!\overline{\gamma_E}^{\frac{\alpha_E}{2}}}$. Similarly, the SOP expression from the integral for $case$ 2 is provided as:

$$P_{SOP}^{Case2} = A_k B_k \sum_{n=1}^{\infty} \lambda_k^n z^\mu \frac{e^{z/cb}(1/ab)}{d^2} +$$
$$C_k D_k \sum_{n=1}^{\infty} \lambda_k^n \frac{e^{z/cb}(1/cb)}{d^2} + \eta\sqrt{\alpha} \quad (25)$$

References

[1] A. D. Wyner, “The wire-tap channel,” *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2013.

[3] C. E. Shannon, “Communication theory of secrecy systems,” *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[4] S. Leung-Yan-Cheong and M. Hellman, “The gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[5] J. Barros and M. R. D. Rodrigues, “Secrecy capacity of wireless channels,” in *Proc. IEEE International Symposium on Information Theory*, July 2006, pp. 356–360.

[6] N. Bhargav, S. L. Cotton, and D. E. Simmons, “Secrecy capacity analysis over κ μ fading channels: Theory and applications,” *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3011–3024, 2016.

[7] J. M. Romero-Jerez and F. J. Lopez-Martinez, “A new framework for the performance analysis of wireless communications under Hoyt (Nakagami-q) fading,” *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1693–1702, 2017.

[8] F. Jameel, S. Wyne, and I. Krikidis, “Secrecy outage for wireless sensor networks,” *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1565–1568, 2017.

[9] H. Lei, C. Gao, I. S. Ansari, Y. Guo, G. Pan, and K. A. Qaraqe, “On physical-layer security over simo generalized-k fading channels,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7780–7785, 2016.

[10] H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. Qaraqe, “Secrecy outage performance for SIMO underlay cognitive radio systems with generalized selection combining over Nakagami-m channels,” *IEEE Trans. Veh. Technol*, vol. 65, no. 12, pp. 10 126–10 132, Dec 2016.

[11] H. Lei, H. Zhang, I. S. Ansari, Z. Ren, G. Pan, K. A. Qaraqe, and M.-S. Alouini, “On secrecy outage of relay selection in underlay cognitive radio networks over nakagami-m fading channels,” *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 4, pp. 614–627, 2017.

[12] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Trans. Signal Process*, vol. 58, no. 3, pp. 1875–1888, 2009.

[13] A. Mathur, Y. Ai, M. R. Bhatnagar, M. Cheffena, and T. Ohtsuki, “On physical layer security of α-η-κ-μ fading channels,” *IEEE Commun. Lett.*, vol. 22, no. 10, pp. 2168–2171, 2018.

[14] Y. Ai, M. Cheffena, A. Mathur, and H. Lei, “On physical layer security of double Rayleigh fading channels for vehicular communications,” *IEEE Commun Lett.*, vol. 7, no. 6, pp. 1038–1041, Dec 2018.

[15] J. Tang, M. Dabaghchian, K. Zeng, and H. Wen, “Impact of mobility on physical layer security over wireless fading channels,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 7849–7864, 2018.

[16] M. D. Yacoub, “The α-η-κ-μ fading model,” *IEEE Trans. Antennas Propag.*, vol. 64, no. 8, pp. 3597–3610, 2016.

[17] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2014.

[18] J. Karedal, N. Czink, A. Paier, F. Tufvesson, and A. F. Molisch, “Path loss modeling for vehicle-to-vehicle communications,” *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 323–328, 2011.

[19] S. Zhu, C. Guo, C. Feng, and X. Liu, “Performance analysis of cooperative spectrum sensing in cognitive vehicular networks with dense traffic,” in *Proc. VTC Spring*, 2016, pp. 1–6.

[20] V. M. Rennó, R. A. de Souza, and M. D. Yacoub, “On the generation of α-η-κ-μ samples with applications,” in *Proc. of Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2017, pp. 1–5.