Towards Physical Layer Security for Internet of Vehicles: Interference Aware Modelling

Abubakar U. Makarfi, *Member, IEEE,* Khaled M. Rabie, *Senior Member, IEEE*, Omprakash Kaiwartya, *Member, IEEE*, Kabita Adhikari, *Member, IEEE*, Galymzhan Nauryzbayev, *Member, IEEE*, Xingwang Li, *Senior Member, IEEE*, Rupak Kharel, *Senior Member, IEEE*.

***Abstract*—The physical layer security (PLS) of wireless networks has witnessed significant attention in next generation communication systems due to its potential towards enabling protection at signal level in dense network environments. The growing trends towards smart mobility via sensor enabled vehicles is transforming today's traffic environment into Internet of Vehicles (IoVs). Enabling PLS for IoVs would be a significant development considering the dense vehicular network environment in the near future. In this context, this paper presents a PLS framework for a vehicular network consisting a legitimate receiver and an eavesdropper, both under the effect of interfering vehicles. The double-Rayleigh fading channel is used to capture the effect of mobility within the communication channel. The performance is analyzed in terms of the average secrecy capacity (ASC) and secrecy outage probability (SOP). We present the standard expressions for the ASC and SOP in alternative forms, to facilitate analysis in terms of the respective moment generating function (MGF) and characteristic function of the joint fading and interferer statistics. Closed-form expressions for the MGFs and characteristic functions were obtained and Monte Carlo simulations were provided to validate the results. Approximate expressions for the ASC and SOP were also provided, for easier analysis and insight into the effect of the network parameters. The results attest that the performance of the considered system was affected by the number of interfering vehicles as well as their distances. It was also demonstrated that the system performance closely correlates with the uncertainty in the eavesdropper's vehicle location.**

***Index Terms*—Double-Rayleigh fading channels, interference modelling, physical layer security, secrecy capacity, secrecy outage probability, vehicular communications.**

I. Introduction

THE emerging concept of Intelligent Transportation Systems (ITS) is envisioned to improve efficiency, reliability, passenger safety as well as enriched infotainment experiences [1], [2]. A key enabler of ITS is the novel paradigm of Internet of Vehicles (IoV), which seeks to enhance the existing capabilities of Vehicular Ad-hoc Networks (VANETs) with the Internet-of-Things (IoT) [1]. Thus, while communication in VANETs involve Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I), communication in IoVs additionally include Vehicle-to-Road Side Units (V2R), Vehicle-to-Infrastructure of Cellular Networks, Vehicle-to-Sensors (V2S), and Vehicle to Personal Devices (V2P), relying on different wireless communication technologies for disseminating information [3]. Hence, we observe a growing trend towards smart mobility via sensor enabled vehicles towards transforming today's traffic environment. As the number of wireless connected devices and vehicles within our transportation systems continue to increase [4], certain technical challenges, with respect to reliable and scalable wireless transmissions for IoV are becoming more apparent [5]. Large amounts of information is generated within the network [1], [5], [6], sometimes up to thousands of times of that by a person. Vehicle density is also highly dynamic over space and time [5], with different urgency requirements for information exchange. These practical realities bring about interference concerns within the shared spectrum and bring forth an even greater need for securing all aspects of the network.

Although there is a growing interest in securing the availability and/or reliability of information exchange in IoV networks through new technologies such as blockchain [7]–[9] or cloud services [10], nevertheless, wireless communication security can be implemented across several layers of the system. Traditionally, one of such approaches, referred to as physical layer security (PLS), employs the inherent characteristics of the propagation channels, such as interference, fading and noise to realize keyless secure transmission through signal design and signal processing approaches [11]. The benefits of employing PLS include less computational complexity compared to computation-based cryptography techniques as well as reduced challenges in distribution and management of secret keys, especially in decentralized systems such as IoT/IoV networks or 5G/beyond 5G heterogenous networks. Furthermore, PLS techniques can be integrated through signal design and resource allocation depending on the prevailing channel conditions [12].

Performance analysis of wireless communication systems over fading channels or in interference-limited networks with respect to PLS have been studied in various literature. For

Manuscript received February 25, 2020; revised April 27, 2020 and June 2, 2020; accepted June 19, 2020. Date of publication xx, 2020.

A. U. Makarfi, K. M. Rabie and R. Kharel are with the Faculty of Science and Engineering, Manchester Metropolitan University, Manchester, UK, M15 6BH (e-mails: {a.makarfi; k.rabie; r.kharel}@mmu.ac.uk).
O. Kaiwartya is with the School of Science and Technology, Nottingham Trent University, UK (e-mail: omprakash. Kaiwartya@ntu.ac.uk).
K. Adhikari is with the School of Engineering, Newcastle University, Newcastle, UK, NE1 7RU (email: kabita.adhikari@ncl.ac.uk)
G. Nauryzbayev is with the School of Engineering and Digital Sciences, Nazarbayev University, Nur-Sultan, 010000, Kazakhstan (email: galymzhan.nauryzbayev@nu.edu.kz).
X. Li is with the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo, China (e-mail: lixingwang@hpu.edu.cn).

instance, the performance of secure cooperative systems over correlated Rayleigh fading channels was studied in [13], while the secrecy outage probability (SOP) over correlated composite Nakagami-m/Gamma fading and the secrecy capacity in the presence of multiple eavesdroppers over Nakagami-m channels were considered in [14] and [15], respectively. Furthermore, the secrecy capacity in generalized fading has been studied over κ-μ shadowed fading channels [16]–[18], over α-μ/κ-μ and κ-μ/α-μ fading channels [19] and over Fisher-Snedecor $\mathcal{F}$ composite fading channel [20]. Meanwhile, the effect of interference on secrecy was observed in a NOMA system in [21], examined for secrecy capacity of a cognitive radio (CR) network in [22] and investigating for the SOP in a Rayleigh faded channel in [23].

With respect to PLS in vehicular communications, a few studies have been conducted in a path-loss non-fading scenario, such as, in [24], where the mobility of nodes were leveraged to improve security in a downlink multiuser network and in [25] for a cooperative decode-and-forward (DF)-based relay network. Several other studies consider various fading models. For example, PLS of vehicular networks was studied in double-Rayleigh and N-Nakagami fading in [26] and [27] respectively, while a relay-assisted mobile network in such fading channels was discussed in [28]. Additionally, secrecy performance for an amplify-and-forward (AF)-based V2I networks under Rayleigh channels was studied in [29], secrecy performance for a DF-based V2V network over double-Rayleigh fading channels in [30], while cooperative AF relaying was investigated for double-Rayleigh fading in [31], [32] and Nakagami-m fading in [33]. The significance of investigating PLS in IoV networks is crucial due to the rapid advancement towards autonomous and connected vehicles as well as to avoid or minimize the associated risk of security compromise and attacks in such networks. It has however been observed that the effect of interference on PLS has received less attention, even though interference is inherent within shared networks [34] and affects the secrecy performance [22], [23]. The issue of interference should be of particular interest in IoV networks because of the large information generated, as well as the requirements of the IEEE 1609.4 standard that institutes specifications suggesting the selection of the least congested channel for data transmission [35]. Additionally, given the random nature of such networks due to uncertain mobility and density of vehicles, the received signal-to-interference-and-noise ratio (SINR) is routinely used as the channel quality measure along with geocasting and other geometry-based localization techniques [36], [37].

Notwithstanding the aforementioned works that studied PLS of wireless networks in different fading channels [13]–[20], [22], [38]–[40] and particularly for vehicular networks in [26]–[33], little attention has been given to the effects of interference in PLS analysis or the effects of eavesdropper uncertainty. In [22], [23], interference was considered on PLS and in [41] the uncertainty of the eavesdropper location was taken into account and shown to affect the PLS analysis. However, [22], [23], [41] were studied for non-vehicular networks and not considered jointly. Moreover, to the best of our knowledge, no previous literature on vehicular communication networks has investigated the PLS considering the joint effects of the three parameters, i.e., fading channel, interference within the shared network and the uncertainty of the eavesdropper location within the shared space. In this paper, the effect of the uncertainty of the eavesdropper location was taken into account, by modelling its distance as a random variable (RV), while the mobile vehicular fading channel was modelled as a double-Rayleigh fading channel, which has been shown from experimental measurements, to be a more appropriate model for the high mobility of nodes in a vehicular network, rather than the more common Rayleigh or Nakagami-m distributions [42], [43].

Motivated by the aforementioned studies and research gap, we investigate the PLS of an IoV network, wherein we consider a legitimate receiver and an eavesdropper, within the shared network, both under the effect of interferer vehicles, thus, examining the dual challenges of interference and security in IoV networks. We summarize the key contributions of this paper as follows:

- New analysis for the combined effect of three random parameters on a vehicular communication channel, i.e., channel fading, interference and eavesdropper uncertainty. To the best of our knowledge, the effect of these three parameters has not been considered jointly for vehicular communication networks.
- The capacity analysis of the system under interference constraints was simplified by expressing the logarithm of the signal-to-interference-and-noise ratio (SINR) in a form that presents the random variables (RVs) as a linear sum in an exponent. This allows easier analysis of the secrecy capacity in the presence of an eavesdropper, in terms of the joint moment generating function (MGF) of the RVs. Closed-form expressions for the MGFs of the joint interference and fading channels were obtained, to facilitate the analysis of various system parameters.
- Novel expressions for the SOP were presented, by obtaining transformations in terms of the characteristic functions of the joint statistics of the RVs. Closed-form expressions for the characteristic function of the joint interference and fading channels were obtained, which are new, to the best of the authors' knowledge.
- We considered a special case of uniformly distributed interfering vehicular nodes in the system. We therefore modelled the density of mobile nodes as a Poisson point process (PPP) and obtained closed-form expressions for the MGF of the joint statistics of the four random system parameters.
- Novel closed-form approximations for the secrecy capacity and high SINR regime analysis for the SOP were derived. The approximate expressions, allow us to gain better insights into the behavior of the considered network scenario.

Throughout the analysis, Monte Carlo simulations are provided to verify the accuracy of the derived expressions. The results show that the performance of the system in terms of both the secrecy capacity and the SOP is impacted by the presence of interfering nodes. The results further demonstrate

the effect of uncertainty in the eavesdropper's location on the analysis.

The remaining of this paper is organized as follows. In Section II, we describe the system under study. Thereafter, in Section III, we derive expressions for efficient computation of the secrecy capacity of the network and derive the MGFs of the SINR in closed-form, while in Section IV, we derive expressions for the SOP of the network as well as the associated closed-form characteristic functions. Finally, in Sections V and VI, we present the results and outline the main conclusions.

Mathematical Functions and Notations: The following notations are used.

Notation	Definition
$\mathbb{E}[\cdot]$	Expectation operator
$\mathrm{G}_{u,v}^{s,t}(x \mid \cdots)$	Meijer's G-function [44, Eq. (9.302)]
$\Gamma(z)$	$=\int_0^\infty t^{z-1}e^{-t}dt$, the gamma function [45, Eq. (8.310)]
$\Gamma(a,b)$	$=\int_b^\infty t^{a-1}e^{-t}dt$, the upper incomplete gamma function [45, Eq. (9.14.1)]
${}_pF_q(\alpha;\beta;z)$	Generalized hypergeometric series [45, Eq. (9.14.1)]
${}_2F_1(\alpha;\beta;\gamma;z)$	Gauss hypergeometric function [45, Eq. (9.111)]
$K_v(z)$	Modified Bessel function of the second kind and v-th order [45, Eq. (8.407)]
$\varphi(-it)$	$=\mathbb{E}\left[e^{-itX}\right]$, the characteristic function of X.
$\mathcal{M}_X(z)$	$=\mathbb{E}\left[e^{-zX}\right]$, the MGF of X.
$\mathcal{M}_{X,Y}(z)$	$=\mathcal{M}_X(z)\mathcal{M}_Y(z)$, the joint MGF of X and Y.
$f(\gamma)$	Probability density function of γ.

II. System Model

Consider a system of nodes operating in a vehicular network as depicted in Fig. 1. We designate three nodes of interest: the information source vehicle (S), the information destination vehicle (D) and a passive eavesdropper[1] vehicle (E). The vehicle S transmits information to the desired vehicle D, while E attempts to receive and decode the confidential information. Furthermore, the presence of other vehicular nodes operating within the same space and frequency band, results in co-channel interference to the received signals of D and E. Moreover, while D and E are known to lie within a certain maximum radius $r_{\max}$ from S, the precise relative distances of the V2V links are unknown during transmission, which is a realistic assumption for a network of this nature [26], [41].

[1]In this context, a passive eavesdropper is a node that only gathers information on the network, but makes no attempt to actively disrupt, tamper or inject any information into the network. Examples of such attacks may include ID disclosure, snooping and session hijacking. See [3] and the references therein for details of such attacks.

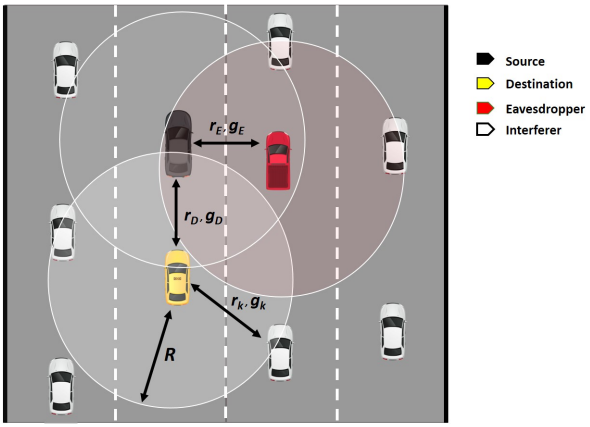

Figure 1: A schematic representation of the system model for the vehicular network under study. R is the maximum distance of interfering nodes. r_D is the source to destination distance. r_E is the source to eavesdropper distance.

The received signals at D and E are respectively represented as

$$y_D = h_D x + \sum_{k=1}^{K} h_{D_k} x_k + w_D, \tag{1}$$

$$y_E = h_E x + \sum_{l=1}^{L} h_{E_l} x_l + w_E, \tag{2}$$

where K and L denote the number of interference nodes at D and E, respectively. x, x_k and x_l are the transmitted signals by S, the k-th interferer and the l-th interferer, with powers P_s, P_k and P_l, respectively. The terms w_D and w_E indicate the additive white Gaussian noise (AWGN) at D and E, respectively. Without loss of generality, we denote the power spectral density of the AWGN as N_0 and equal at both links. The terms $h_i = \sqrt{g_i r_i^{-\beta}}$, $i \in \{D, E\}$, is the channel coefficient from S to the receiving vehicles D and E, where r_i is the V2V link distance, β is the path-loss exponent and g_i is the channel gain following double-Rayleigh fading [26]. As far as the interferers are concerned, $h_{i_j} = \sqrt{g_{i_j} r_{i_j}^{-\beta}}$, $i \in \{D, E\}$, $j \in \{k, l\}$ are the channel coefficients between the j-th interferer at a distance r_{i_j} from the receiving node, and g_{i_j} is the j-th interferer channel gain.

Based on (1) and (2), the instantaneous SINRs at D and E are respectively given by

$$\gamma_D = \frac{P_s \mid h_D \mid^2}{\sum_{k=1}^{K} P_k \mid h_{D_k} \mid^2 + N_0}, \tag{3}$$

and

$$\gamma_E = \frac{P_s \mid h_E \mid^2}{\sum_{l=1}^{L} P_l \mid h_{E_l} \mid^2 + N_0}. \tag{4}$$

III. Secrecy Capacity Analysis

In this section, we derive analytical expressions for the average secrecy capacity (ASC) of the system. The maximum achievable secrecy capacity is defined by [46]

$$C_s = \max\{C_D - C_E, 0\}, \tag{5}$$

where $C_D = \log_2(1+\gamma_D)$ and $C_E = \log_2(1+\gamma_E)$ are the instantaneous capacities of the main and eavesdropping links, respectively. The secrecy capacity in (5) can therefore be expressed as [46]

$$C_s = \begin{cases} \log_2(1+\gamma_D) - \log_2(1+\gamma_E), & \gamma_D > \gamma_E, \\ 0, & \gamma_D \leq \gamma_E. \end{cases} \quad (6)$$

The ASC for the system $\overline{C}_s$ is given by [47]

$$\begin{aligned} \overline{C}_s &= \mathbb{E}\left[C_s(\gamma_D, \gamma_E)\right] \\ &= \mathbb{E}\left[\log_2(1+\gamma_D)\right] - \mathbb{E}\left[\log_2(1+\gamma_E)\right] \\ &= \int_0^\infty \log_2(1+\gamma_D) f(\gamma_D) \mathrm{d}\gamma_D \\ &\quad - \int_0^\infty \log_2(1+\gamma_E) f(\gamma_E) \mathrm{d}\gamma_E, \end{aligned} \quad (7)$$

where $f(\gamma_D)$ and $f(\gamma_E)$ are the probability density functions (PDFs) of γ_D and γ_E, respectively. It is worth noting at this point that the average in (7) is with respect to γ_D and γ_E. However, assuming each SINR term has M RVs, then we would in turn require at least M-fold numerical integrations to average out the RVs $\{g_D, g_{D_1} \ldots g_{D_K}, g_E, g_{E_1} \ldots g_{E_K}, r_D, r_E, r_{D_1} \ldots r_{D_k}$ and $r_{E_1} \ldots r_{E_k}\}$ contained within each SINR term. Therefore, obtaining the exact solution of $f(\gamma_D)$ and $f(\gamma_E)$ would be at least arduous, if not impossible. However, the computational complexity of the task is greatly reduced by adopting the MGF approach, as mentioned earlier.

We commence by expressing the logarithmic function in (6) in an alternate form. Recalling the identity [48, Eq. (6)]

$$\ln(1+x) = \int_0^\infty \frac{1}{s}\left(1 - e^{-xs}\right) e^{-s} \mathrm{d}s, \quad (8)$$

and by substituting $x = \gamma_D$ in (8), we can express the instantaneous capacity of the main link as

$$C_D = \frac{1}{\ln(2)} \int_0^\infty \frac{1}{s}\left(1 - e^{-s\frac{P_s|h_D|^2}{\sum_{k=1}^K P_k |h_{D_k}|^2 + N_0}}\right) e^{-s} \mathrm{d}s. \quad (9)$$

After some algebraic manipulations and substituting $s = z\left(\sum_{k=1}^K P_k \mid h_{D_k}\mid^2 + N_0\right)$, we obtain an expression in the desired form with the RVs appearing only in the exponent. Thus,

$$\begin{aligned} C_D = \frac{1}{\ln(2)} \int_0^\infty \frac{1}{z} e^{-zN_0} \Bigg(& e^{-z\sum_{k=1}^K P_k |h_{D_k}|^2} \\ & - e^{-zP_s|h_D|^2} e^{-z\sum_{k=1}^K P_k |h_{D_k}|^2} \Bigg) \mathrm{d}z, \end{aligned} \quad (10)$$

and after taking the expectation, we obtain the average capacity of the main link as

$$\begin{aligned} \overline{C}_D &= \mathbb{E}\left[\log_2\left(1 + \frac{P_s \mid h_D\mid^2}{\sum_{k=1}^K P_k \mid h_{D_k}\mid^2 + N_0}\right)\right] \\ &= \frac{1}{\ln(2)} \int_0^\infty \frac{1}{z} e^{-zN_0} \left(\mathcal{M}_{\phi_D}(z) - \mathcal{M}_{\chi_D, \phi_D}(z)\right) \mathrm{d}z, \end{aligned} \quad (11)$$

where $\mathcal{M}_{\phi_D}(z) = \mathbb{E}\left[e^{-z\sum_{k=1}^K P_k g_{D_k} r_{D_k}^{-\beta}}\right]$ is the MGF of the cumulative interference at D and $\mathcal{M}_{\chi_D, \phi_D}(z) = \mathbb{E}\left[e^{-z\left(P_s g_D r_D^{-\beta} + \sum_{k=1}^K P_k g_{D_k} r_{D_k}^{-\beta}\right)}\right]$ is the joint MGF of the legitimate link and cumulative interference at D. Using similar analysis, the average capacity of the eavesdropper link can be represented as

$$\overline{C}_E = \frac{1}{\ln(2)} \int_0^\infty \frac{1}{z} e^{-zN_0} \left(\mathcal{M}_{\phi_E}(z) - \mathcal{M}_{\chi_E, \phi_E}(z)\right) \mathrm{d}z, \quad (12)$$

where $\mathcal{M}_{\phi_E}(z)$ is the MGF of the cumulative interference at E and $\mathcal{M}_{\chi_E, \phi_E}(z)$ is the joint MGF of the eavesdropper link and cumulative interference at E.

From (6), (11) and (12), the alternate form for the ASC in (7) can be expressed as

$$\begin{aligned} \overline{C}_s = & \frac{1}{\ln(2)} \int_0^\infty \frac{1}{z} e^{-zN_0} \left(\mathcal{M}_{\phi_D}(z) - \mathcal{M}_{\chi_D, \phi_D}(z)\right) \mathrm{d}z \\ & - \frac{1}{\ln(2)} \int_0^\infty \frac{1}{z} e^{-zN_0} \left(\mathcal{M}_{\phi_E}(z) - \mathcal{M}_{\chi_E, \phi_E}(z)\right) \mathrm{d}z. \end{aligned} \quad (13)$$

From (13), we observe that the integrals are symmetrical and differ mainly in the relative locations of S, D and E. Therefore, this signifies the importance of taking into account the node locations in the analysis. It is worth noting that, by definition of the ASC in (6), a zero ASC exists once the second term in (13), exceeds the value of the first term i.e. the secrecy of the system is not guaranteed. In what follows, we compute the MGFs presented in (13).

A. Computation of Moment Generating Functions

1) The MGF $\mathcal{M}_{\phi_D}(z)$: The MGF of the cumulative interference at D is given by $\mathcal{M}_{\phi_D}(z) = \mathbb{E}\left[e^{-z\sum_{k=1}^K P_k g_{D_k} r_{D_k}^{-\beta}}\right]$, defined by

$$\begin{aligned} \mathcal{M}_{\phi_D}(z) &= \mathbb{E}\left[e^{-z\sum_{k=1}^K P_k g_{D_k} r_{D_k}^{-\beta}}\right] \\ &= \prod_{k=1}^K \mathbb{E}\left[e^{-zP_k g_{D_k} r_{D_k}^{-\beta}}\right] \\ &= \prod_{k=1}^K \int_g \int_r e^{-zP_k g_{D_k} r_{D_k}^{-\beta}} f_{r_{D_k}}(r) f_{g_{D_k}}(g) \mathrm{d}r_{D_k} \mathrm{d}g_{D_k}, \end{aligned} \quad (14)$$

where $f_{g_{D_k}}(g)$ and $f_{r_{D_k}}(r)$ are the PDFs of the channel gain g_{D_k} and interferer distance r_{D_k}, respectively.

$$\mathcal{M}_{\psi}\left(z\right)=\frac{4}{3(1+zR^{-\beta})^{2}}{}_{2}F_{1}\left(2,\frac{1}{2},\frac{5}{2},\frac{zR^{-\beta}-1}{zR^{-\beta}+1}\right)-\frac{(2z)^{\frac{2}{\beta}}\,\Gamma\left(1+\frac{1}{\beta}\right)^{2}\Gamma\left(1-\frac{2}{\beta}\right)}{R^{2}}+\frac{2\pi\beta z}{R^{\beta}}\left[\frac{{}_{3}F_{2}\left(\frac{3}{2},\frac{3}{2},\frac{1}{2}-\frac{1}{\beta};\frac{1}{2},\frac{3}{2}-\frac{1}{\beta};z^{2}R^{-2\beta}\right)}{4\left(\beta-2\right)}-\frac{z\,{}_{3}F_{2}\left(2,2,1-\frac{1}{\beta};\frac{3}{2},2-\frac{1}{\beta};z^{2}R^{-2\beta}\right)}{\pi\left(\beta-1\right)R^{\beta}}\right]. \quad (18)$$

Let us start by defining a special case of the MGF in (14) with only the RVs, given by

$$\begin{aligned}\mathcal{M}_{\psi}\left(z\right)&=\mathbb{E}\left[e^{-zg_{D_k}r_{D_k}^{-\beta}}\right]\\&=\int_{g_{D_k}}\int_{r_{D_k}}e^{-zg_{D_k}r_{D_k}^{-\beta}}f_{r_{D_k}}(r)f_{g_{D_k}}(g)\mathrm{d}r_{D_k}\mathrm{d}g_{D_k},\end{aligned} \quad (15)$$

where g_{D_k} follows a double-Rayleigh distribution. A double-Rayleigh RV is by definition the product of two independent Rayleigh RVs. Thus, we can obtain the PDF of the double-Rayleigh channel from the generalized n-Rayleigh distribution [49, Eq. (8)] for $n=2$ as

$$f\left(g\right)=\mathrm{G}_{0,2}^{2,0}\left(\frac{1}{4}g^{2}\middle|\begin{matrix}-\\\frac{1}{2},\frac{1}{2}\end{matrix}\right). \quad (16)$$

The interferer node distances, r_{D_k}, are assumed to be uniformly distributed within a circular region, with interference radius R around the receiver, with a PDF given by [50]

$$f\left(r\right)=\begin{cases}\frac{2r_{D_k}}{R^{2}}, & 0<r_{D_k}\leq R,\\0, & \text{otherwise.}\end{cases} \quad (17)$$

Using (16) and (17), the MGF in (15) can be expressed as in (18), shown on the top of the page.

Proof: The proof is presented in Appendix A. ∎

Therefore, using (54) in (14), we obtain the desired MGF of interferer statistics at D as

$$\begin{aligned}\mathcal{M}_{\phi_D}\left(z\right)&=\prod_{k=1}^{K}\mathcal{M}_{\psi}\left(zP_k\right)\\&=\left\{\mathcal{M}_{\psi}\left(zP_K\right)\right\}^{K},\end{aligned} \quad (19)$$

where the final step in (19) was obtained by assuming identical transmit powers for interferer nodes, such that $P_1=P_2=\cdots=P_k=P_K$.

2) The Joint MGF $\mathcal{M}_{\chi_D,\phi_D}(z)$: The joint MGF $\mathcal{M}_{\chi_D,\phi_D}(z)$ is given by

$$\begin{aligned}\mathcal{M}_{\chi_D,\phi_D}\left(z\right)&=\mathbb{E}\left[e^{-z\left(P_sg_Dr_D^{-\beta}+\sum_{k=1}^{K}P_kg_{D_k}r_{D_k}^{-\beta}\right)}\right]\\&=\mathbb{E}\left[e^{-zP_sg_Dr_D^{-\beta}}e^{-z\sum_{k=1}^{K}P_kg_{D_k}r_{D_k}^{-\beta}}\right]\\&=\mathcal{M}_{\chi_D}\left(z\right)\mathcal{M}_{\phi_D}\left(z\right),\end{aligned} \quad (20)$$

where $\mathcal{M}_{\phi_D}(z)$ is given by the expression (19) and $\mathcal{M}_{\chi_D}(z)$ is the MGF of statistics at D. It is worthwhile noting that the system considered assumes that the location of D is known by S. Consequently, r_D is not random and the MGF is conditioned only on the statistics of the channel. Thus, the expected value for the first MGF in (20) can be given by

$$\begin{aligned}\mathcal{M}_{\chi_D}\left(z\right)&=\mathbb{E}\left[\exp\left(-zP_sg_Dr_D^{-\beta}\right)\right]\\&=\int_{0}^{\infty}e^{-zP_sg_Dr_D^{-\beta}}\mathrm{G}_{0,2}^{2,0}\left(\frac{1}{4}g_D^{2}\middle|\begin{matrix}-\\\frac{1}{2},\frac{1}{2}\end{matrix}\right)\mathrm{d}g_D.\end{aligned} \quad (21)$$

To proceed, we express (21) in a more tractable form, by re-writing the Meijer G-function in an alternate form. Thus, upon invoking [45, Eq. (9.34.3)], we get

$$\mathrm{G}_{0,2}^{2,0}\left(\frac{1}{4}g^{2}\middle|\begin{matrix}-\\\frac{1}{2},\frac{1}{2}\end{matrix}\right)=gK_0\left(g\right). \quad (22)$$

Using (22) and [45, Eq. (6.621.3)] along with some basic algebraic manipulations, we can straightforwardly obtain the desired result as

$$\mathcal{M}_{\chi_D}\left(z\right)=\frac{4}{3(1+zP_sr_D^{-\beta})^{2}}{}_{2}F_{1}\left(2,\frac{1}{2},\frac{5}{2},\frac{zP_sr_D^{-\beta}-1}{zP_sr_D^{-\beta}+1}\right). \quad (23)$$

Hence, we obtain $\mathcal{M}_{\chi_D,\phi_D}(z)$ by substituting (18), (19) and (23) in (20).

3) The MGF $\mathcal{M}_{\phi_E}(z)$: The MGF of the cumulative interference at E is given by $\mathcal{M}_{\phi_E}\left(z\right)=\mathbb{E}\left[e^{-z\sum_{l=1}^{L}P_lg_{E_l}r_{E_l}^{-\beta}}\right]$. From the definition of the MGF, it can be observed that the computation of $\mathcal{M}_{\phi_E}(z)$ follows similar analysis to the interference at D. For the sake of brevity, the analysis will not be repeated here. Thus, using (18), and assuming $P_1=P_2=\cdots=P_l=P_L$, it is easy to show that the desired MGF is

$$\mathcal{M}_{\phi_E}\left(z\right)=\left\{\mathcal{M}_{\psi}\left(zP_L\right)\right\}^{L}. \quad (24)$$

4) The Joint MGF $\mathcal{M}_{\chi_E,\phi_E}(z)$: The joint MGF $\mathcal{M}_{\chi_E,\phi_E}(z)$ can be obtained through similar analysis presented in Sec. III-A2. Therefore, from (20), $\mathcal{M}_{\chi_E,\phi_E}(z)=\mathcal{M}_{\chi_E}(z)\,\mathcal{M}_{\phi_E}(z)$, where $\mathcal{M}_{\phi_E}(z)$ is given by (24). For the system under consideration, the exact location of E is unknown, but lies at a maximum distance $r_{\max}$ from S. Using the PDFs in (16) and (17), we obtain

$$\begin{aligned}\mathcal{M}_{\chi_E}\left(z\right)&=\mathbb{E}\left[\exp\left(-zP_sg_Er_E^{-\beta}\right)\right]\\&=\int_{0}^{\infty}\int_{0}^{r_{\max}}e^{-zP_sg_Er_E^{-\beta}}\frac{2r_E}{r_{\max}^{2}}\mathrm{G}_{0,2}^{2,0}\left(\frac{1}{4}g_E^{2}\middle|\begin{matrix}-\\\frac{1}{2},\frac{1}{2}\end{matrix}\right)\mathrm{d}r_E\mathrm{d}g_E.\end{aligned} \quad (25)$$

Comparing (25) and (14) shows that both expressions are similar with maximum distance $R=r_{\max}$ and source power

$$\overline{C}_s = \frac{1}{\ln(2)} \int_0^{\infty} \frac{1}{z} e^{-zN_0} \left\{ \frac{4}{3(1+zP_K R^{-\beta})^2} {}_2F_1\left(2, \frac{1}{2}, \frac{5}{2}, \frac{zP_K R^{-\beta}-1}{zP_K R^{-\beta}+1}\right) - \frac{\Gamma\left(1+\frac{1}{\beta}\right)^2 \Gamma\left(1-\frac{2}{\beta}\right)}{R^2 (2zP_K)^{-\frac{2}{\beta}}} + \frac{2\pi\beta z P_K}{R^{\beta}} \right.$$
$$\times \left[\frac{{}_3F_2\left(\frac{3}{2}, \frac{3}{2}, \frac{1}{2}-\frac{1}{\beta}; \frac{1}{2}, \frac{3}{2}-\frac{1}{\beta}; (zP_K)^2 R^{-2\beta}\right)}{4(\beta-2)} - \frac{{}_3F_2\left(2, 2, 1-\frac{1}{\beta}; \frac{3}{2}, 2-\frac{1}{\beta}; (zP_K)^2 R^{-2\beta}\right)}{\pi(\beta-1) R^{\beta} (zP_K)^{-1}} \right] \Bigg\}^K \Bigg\{ \Bigg(\frac{4}{3(1+zP_s r_{\max}^{-\beta})^2}$$
$$\times {}_2F_1\left(2, \frac{1}{2}, \frac{5}{2}, \frac{zP_s r_{\max}^{-\beta}-1}{zP_s r_{\max}^{-\beta}+1}\right) - \frac{(2zP_s)^{\frac{2}{\beta}} \Gamma\left(1+\frac{1}{\beta}\right)^2 \Gamma\left(1-\frac{2}{\beta}\right)}{r_{\max}^2} + \frac{2\pi\beta z P_s}{r_{\max}^{\beta}} \left[\frac{{}_3F_2\left(\frac{3}{2}, \frac{3}{2}, \frac{1}{2}-\frac{1}{\beta}; \frac{1}{2}, \frac{3}{2}-\frac{1}{\beta}; (zP_s)^2 r_{\max}^{-2\beta}\right)}{4(\beta-2)} \right.$$
$$\left. \left. - \frac{zP_s \, {}_3F_2\left(2, 2, 1-\frac{1}{\beta}; \frac{3}{2}, 2-\frac{1}{\beta}; (zP_s)^2 r_{\max}^{-2\beta}\right)}{\pi(\beta-1) R^{\beta}} \right] \Bigg) - \frac{4}{3(1+zP_s r_D^{-\beta})^2} {}_2F_1\left(2, \frac{1}{2}, \frac{5}{2}, \frac{zP_s r_D^{-\beta}-1}{zP_s r_D^{-\beta}+1}\right) \Bigg\} \mathrm{d}z \quad (28)$$

P_s. Thus, using (18), $\mathcal{M}_{\chi_E}(z) = \mathcal{M}_{\psi}(zP_s|r_{\max})$. We obtain from (18) and (24) the following

$$\mathcal{M}_{\chi_E,\phi_E}(z) = \mathcal{M}_{\chi_E}(z)\,\mathcal{M}_{\phi_E}(z) = \mathcal{M}_{\psi}(zP_s|r_{\max})\left\{\mathcal{M}_{\psi}(zP_L)\right\}^L. \quad (26)$$

Therefore, by substituting the relevant MGFs from (18), (20), (23), (24) and (26) in (13), we obtain the ASC.

For the special case when the number of interference nodes is equal at both D and E,[2] then ASC can be given as

$$\begin{aligned}
\overline{C}_s =& \frac{1}{\ln(2)} \int_0^{\infty} \frac{1}{z} e^{-zN_0} \left\{\mathcal{M}_{\phi_D}(z) - \mathcal{M}_{\chi_D,\phi_D}(z)\right\} \mathrm{d}z \\
& - \frac{1}{\ln(2)} \int_0^{\infty} \frac{1}{z} e^{-zN_0} \left\{\mathcal{M}_{\phi_E}(z) - \mathcal{M}_{\chi_E,\phi_E}(z)\right\} \mathrm{d}z \\
\overset{(a)}{=}& \frac{1}{\ln(2)} \int_0^{\infty} \frac{1}{z} e^{-zN_0} \left\{\mathcal{M}_{\chi_E,\phi_E}(z) - \mathcal{M}_{\chi_D,\phi_D}(z)\right\} \mathrm{d}z \\
=& \int_0^{\infty} \frac{e^{-zN_0}}{z\ln(2)} \left\{\mathcal{M}_{\chi_E}(z)\,\mathcal{M}_{\phi_E}(z) - \mathcal{M}_{\chi_D}(z)\,\mathcal{M}_{\phi_D}(z)\right\} \mathrm{d}z \\
=& \int_0^{\infty} \frac{e^{-zN_0}}{z\ln(2)} \left\{\mathcal{M}_{\psi}(zP_K)\right\}^K \\
& \times \left[\mathcal{M}_{\psi}(zP_s|r_{\max}) - \mathcal{M}_{\chi_D}(z)\right] \mathrm{d}z, \quad (27)
\end{aligned}$$

where (a) in (27) was obtained due to the fact that $K = L$, $P_K = P_L$ and thus, $\mathcal{M}_{\phi_D}(z) = \mathcal{M}_{\phi_E}(z)$ from (19) and (24). Therefore, the ASC reduces to (28), shown at the top of this page.

B. The MGF for a Poisson Point Process

In this subsection, we consider the special case when we have no restriction on the likely distance of an interfering mobile node. The interferer effect can be modelled by a Poisson process, when we assume that the spatial locations of the vehicular nodes are uniformly distributed [51]. In this case, the interferer radius $R \to \infty$ as well as the number of interferer nodes at D, $K \to \infty$. We can then define the average interferers per unit area $\lambda = \frac{K}{\pi R^2}$ (interferers/m^2), such that $0 < \lambda < \infty$. Then, from (14) and (53), the MGF for the cumulative interference can be represented as

$$\begin{aligned}
\mathcal{M}(z|g_D) &= \lim_{\substack{K\to\infty, R\to\infty \\ \lambda = K/\pi R^2}} \prod_{k=1}^{K} \int_0^{R} e^{-zP_K g_D r_D^{-\beta}} f_{r_D}(r)\mathrm{d}r_D \\
&= e^{-\lambda\pi (zP_K g_D)^{\frac{2}{\beta}} \Gamma\left(1-\frac{2}{\beta}\right)}, \quad (29)
\end{aligned}$$

Proof: The proof is presented in Appendix B. ■

It can be observed that (29) corresponds to the Poisson MGF with interferer density, λ. From (29), we employ (22) to average out the MGF $\mathcal{M}_{\psi}^{p}(z) = \int_0^{\infty} e^{-\lambda\pi (zP_K g_D)^{\frac{2}{\beta}} \Gamma\left(1-\frac{2}{\beta}\right)} g_D K_0(g_D)\,\mathrm{d}g_D$. For path-loss exponent $\beta = 4$, we can straightforwardly obtain a closed-form solution for the MGF using [52, Eq. (2.16.8.8)]. After some algebraic manipulations, we obtain (30) at the top of the next page, where $\rho = \lambda\left(zP_K\pi^3\right)^{\frac{1}{2}}$.

C. Approximate Secrecy Capacity

In this section, we present an approximate solution to the ASC computed in (28) in order to provide a more direct solution. From (6), it can be seen that the secrecy capacity is defined as a logarithmic function. Thus, we can define an approximate solution to (28) by invoking Jensen's inequality[3] [53, pp. 453] and applying to the expressions for the instantaneous capacities of the main and eavesdropping links. Therefore, the average capacity at D is

$$\mathbb{E}\left[\log_2(1+\gamma_D)\right] \leq \log_2\left(1+\mathbb{E}\left[\gamma_D\right]\right)$$

[2]This assumption is plausible, because for uniformly distributed interference nodes, the number of interference nodes at D and E may remain the same, while retaining their independence.

[3]Jensen's inequality asserts that, if $f(x)$ is a convex function, then $\mathbb{E}\left[f(X)\right] \geq f\left(\mathbb{E}\left[X\right]\right)$, provided that the expectations exist and are finite.

$$\mathcal{M}_{\psi}^{p}(z) = {}_2F_3\left(1,1;\frac{1}{4},\frac{1}{2},\frac{3}{4};\frac{\rho^4}{64}\right) - \rho 2^{\frac{1}{2}}\Gamma\left(\frac{5}{4}\right)^2 {}_1F_2\left(\frac{5}{4};\frac{1}{2},\frac{3}{4};\frac{\rho^4}{64}\right) + \frac{\rho^2\pi}{4}{}_1F_2\left(\frac{3}{2};\frac{3}{4},\frac{5}{4};\frac{\rho^4}{64}\right) - \frac{\rho^3 2^{\frac{1}{2}}}{3}\Gamma\left(\frac{7}{4}\right)^2 {}_1F_2\left(\frac{7}{4};\frac{5}{4},\frac{3}{2};\frac{\rho^4}{64}\right) \quad (30)$$

$$= \log_2\left(1 + \mathbb{E}\left[\frac{P_s g_D r_D^{-\beta}}{\sum_{k=1}^{K} P_k g_{D_k} r_{D_k}^{-\beta} + N_0}\right]\right), \quad (31)$$

where γ_D is defined in (3) and the expectation term on the second line can be represented as $\mathbb{E}\left[P_s g_D r_D^{-\beta}\right] \times \mathbb{E}\left[\frac{1}{\sum_{k=1}^{K} P_k g_{D_k} r_{D_k}^{-\beta} + N_0}\right]$. By using (22), the first expectation can be obtained as

$$\mathbb{E}\left[P_s g_D r_D^{-\beta}\right] = P_s r_D^{-\beta} \int_0^{\infty} g_D g_D K_0(g_D)\, \mathrm{d}g_D \overset{(b)}{=} \frac{\pi P_s r_D^{-\beta}}{2}, \quad (32)$$

where (b) in (32) was obtained with the aid of [45, Eq. (6.521.10)]. The second expectation can be obtained as

$$\mathbb{E}\left[\frac{1}{\sum_{k=1}^{K} P_k g_{D_k} r_{D_k}^{-\beta} + N_0}\right] \overset{(c)}{=} \mathbb{E}\left[\int_0^{\infty} e^{-z\left(\sum_{k=1}^{K} P_k g_{D_k} r_{D_k}^{-\beta} + N_0\right)} \mathrm{d}z\right] \overset{(d)}{\geq} \int_0^{\infty} e^{-z\left(\mathbb{E}\left[\sum_{k=1}^{K} P_k g_{D_k} r_{D_k}^{-\beta} + N_0\right]\right)} \mathrm{d}z, \quad (33)$$

where (c) in (33) was obtained with the help of [45, Eq. (8.312.2)] and (d) was obtained by invoking Jensen's inequality. Next, the expectation in (33) can be obtained for the independent RVs. The expectation $\mathbb{E}[g_{D_k}]$ is derived using similar steps as (32), while $\mathbb{E}\left[r_{D_k}^{-\beta}\right]$ is obtained using the PDF in (17) and the monotonicity of the expectation operator[4]. Therefore, we obtain the approximation as

$$\mathbb{E}[r_{D_k}] = \int_0^{R} \frac{2r_{D_k}}{R} r_{D_k}\mathrm{d}r_{D_k} = \frac{2R}{3}. \quad (34)$$

Thus, (31) resolves to the approximate expression for the average capacity at D as

$$\overline{C}_D^{\text{aprx}} = \log_2\left(1 + \frac{\pi P_s r_D^{-\beta}}{2\left(N_0 + \frac{K\pi P_K}{2}\left(\frac{3}{2R}\right)^{\beta}\right)}\right). \quad (35)$$

Using similar analysis to the derivation of (35) while considering the uncertainty of the eavesdropper location with maximum radius, $r_{\max}$, we obtain a bounded expression for the average capacity at E as

$$\overline{C}_E^{\text{aprx}} = \log_2\left(1 + \frac{\pi P_s r_{\max}^{-\beta}}{\left(\frac{2}{3}\right)^{\beta}\left(N_0 + \frac{L\pi P_L}{2}\left(\frac{3}{2R}\right)^{\beta}\right)}\right). \quad (36)$$

From (6), (35) and (36), we obtain the desired closed-form approximate expression as

$$\overline{C}_s^{\text{aprx}} = \log_2\left(1 + \frac{\pi P_s r_D^{-\beta}}{2\left(N_0 + \frac{K\pi P_K}{2}\left(\frac{3}{2R}\right)^{\beta}\right)}\right) - \log_2\left(1 + \frac{\pi P_s r_{\max}^{-\beta}}{\left(\frac{2}{3}\right)^{\beta}\left(N_0 + \frac{L\pi P_L}{2}\left(\frac{3}{2R}\right)^{\beta}\right)}\right). \quad (37)$$

It is worth noting that, in addition to the fact that (37) is in closed-form with elementary functions, the expression also lends itself much easier to analysis as compared to (28). From observation of (37), it can be seen that the interferer affects both the eavesdropper and the destination receiver. The accuracy of the approximate ASC expression is discussed in Sec. V.

IV. Secrecy Outage Probability

In this section, we derive expressions for the SOP. The SOP can be defined as the probability that the secrecy capacity falls below a target secrecy rate [39]. This can be represented as

$$P_o = \Pr[C_s < R_s], \quad (38)$$

where R_s is the pre-determined target secrecy rate. From (6) and (38) we obtain

$$\begin{aligned} P_o &= \Pr\left[\log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right) < R_s\right] \\ &= \Pr\left[\frac{1+\gamma_D}{1+\gamma_E} < 2^{R_s}\right] \\ &= \Pr[\gamma_D < \nu - 1 + \nu\gamma_E] \\ &\overset{(e)}{=} \Pr\left[\frac{P_s \mid h_D \mid^2}{\sum_{k=1}^{K} P_k \mid h_{D_k} \mid^2 + N_0} < \nu - 1 + \nu\left(\frac{P_s \mid h_E \mid^2}{\sum_{l=1}^{L} P_l \mid h_{E_l} \mid^2 + N_0}\right)\right], \end{aligned} \quad (39)$$

where $\nu = 2^{R_s}$ and (e) follows from substituting (3) and (4). After some algebraic manipulations, we can express (39) as

[4]monotonicity depicts that if the RVs $X \leq Y$, then $\mathbb{E}[X] \leq \mathbb{E}[Y]$.

$$P_o = \Pr\left[X < \left(\nu - 1 + \frac{\nu W P_s r_E^{-\beta}}{T}\right)\frac{Y}{P_s r_D^{-\beta}}\right]$$
$$= \Pr\left[X < \frac{\nu Y}{c} - \frac{Y}{c} + \frac{\nu Y W P_s r_E^{-\beta}}{T P_s r_D^{-\beta}}\right]$$
$$\overset{(f)}{=} \Pr\left[X < Y\frac{(\nu-1)}{c} + \nu W c_r\right], \quad (40)$$

where $c = P_s r_D^{-\beta}$ and $c_r = \left(\frac{r_D}{r_E}\right)^{\beta}$, while the RVs $W = g_E$, $X = g_D$, $Y = \sum_{k=1}^{K} P_k g_{D_k} r_{D_k}^{-\beta} + N_0$ and $T = \sum_{l=1}^{L} P_l g_{E_l} r_{E_l}^{-\beta} + N_0$. Assuming the special case, where the number of interference nodes $K = L$, then line (f) in (40) follows from the fact that the average cumulative interference at both D and E, $\mathcal{M}_{\phi_D}(z) = \mathcal{M}_{\phi_E}(z)$ as shown in Sec. III-A.

Since X follows a double-Rayleigh distribution given in (16), using the PDF representation in (22), we can express P_o as the CDF of X given by

$$P_o = 1 - \Theta K_1(\Theta), \quad (41)$$

where $\Theta = Y\frac{(\nu-1)}{c} + \nu W c_r$.

To obtain the average SOP, we express the Bessel function term in a more tractable form. Using [45, Eq. (8.432.5)] and utilizing the fact that $s\Gamma(s) = \Gamma(1+s)$, we get

$$\overline{P}_o = \mathbb{E}\left[1 - \int_0^{\infty} \frac{\cos(\Theta t)}{(t^2+1)^{\frac{3}{2}}}\mathrm{d}t\right]$$
$$\overset{(g)}{=} 1 - \int_0^{\infty} \frac{1}{(t^2+1)^{\frac{3}{2}}}\mathbb{E}\Big[\underbrace{\cos\left(\frac{(\nu-1)}{c}Yt\right)\cos(\nu W c_r t)}_{\mathcal{J}_1}$$
$$\underbrace{- \sin\left(\frac{(\nu-1)}{c}Yt\right)\sin(\nu W c_r t)}_{\mathcal{J}_2}\Big]\mathrm{d}t, \quad (42)$$

where (g) was obtained by invoking [45, Eq. (1.313.5)].

To evaluate $\mathcal{J}_1$ in (42), we note that the RVs Y and W are independent. Hence, the expectation of the second cosine term in $\mathcal{J}_1$ can be obtained with the aid of [45, Eq. (6.699.4)] and the PDF form in (22), to get

$$\mathcal{J}_1 = \mathbb{E}\left[\cos\left(\frac{(\nu-1)}{c}Yt\right)\cos(\nu W c_r t)\right]$$
$$= \mathbb{E}\left[\cos\left(\frac{(\nu-1)}{c}Yt\right)\right]\int_0^{\infty}\cos(\nu g_E c_r t)\, g_E K_0(g_E)\,\mathrm{d}g_E$$
$$= \mathbb{E}\left[\cos\left(\frac{(\nu-1)}{c}Yt\right)\right]{}_2F_1\left(1,1,\frac{1}{2},-(\nu c_r t)^2\right). \quad (43)$$

To evaluate the expectation of the first term in (43), we re-express the cosine function in a more tractable form by invoking [45, Eq. (1.311.3)]. Thus,

$$\mathcal{J}_1 = c_f \mathbb{E}\left[\frac{1}{2}\left\{e^{-i\frac{(\nu-1)}{c}Yt} + e^{i\frac{(\nu-1)}{c}Yt}\right\}\right]$$
$$= \frac{c_f}{2}\mathbb{E}\left[e^{-\frac{it(\nu-1)}{c}\left(\sum_{k=1}^{K} P_k g_k r_k^{-\beta} + N_0\right)} + e^{\frac{it(\nu-1)}{c}\left(\sum_{k=1}^{K} P_k g_k r_k^{-\beta} + N_0\right)}\right]$$
$$= \frac{c_f}{2}\left[\varphi(-it)\, e^{-itc_\nu N_0} + \varphi(it)\, e^{itc_\nu N_0}\right], \quad (44)$$

where $c_f = {}_2F_1\left(1,1,\frac{1}{2},-(\nu c_r t)^2\right)$, $c_\nu = \frac{(\nu-1)}{c}$ and the characteristic function $\varphi(-it) = \mathbb{E}\left[e^{-\frac{it(\nu-1)}{c}\sum_{k=1}^{K} P_k g_k r_k^{-\beta}}\right]$ is computed in Appendix C.

The term $\mathcal{J}_2$ in (42) can be obtained using [45, Eq. (6.699.3)] and the PDF form in (22). The expectation of the second sine term in $\mathcal{J}_2$ can be obtained as

$$\mathbb{E}[\sin(\nu W c_r t)] = \int_0^{\infty}\sin(\nu g_E c_r t)\, g_E K_0(g_E)\,\mathrm{d}g_E$$
$$= 2\nu c_r t\,\Gamma\left(\frac{3}{2}\right)\Gamma\left(\frac{3}{2}\right){}_2F_1\left(\frac{3}{2},\frac{3}{2};\frac{3}{2};-(\nu c_r t)^2\right)$$
$$\overset{(h)}{=} \frac{\pi\nu c_r t}{2\left(1+(\nu c_r t)^2\right)^{\frac{3}{2}}}, \quad (45)$$

where (h) in (45) was obtained using [45, Eq. (9.121.1)] and the identities $s\Gamma(s) = \Gamma(1+s)$ and $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$. From (45) and [45, Eq. (1.311.1)], we can express $\mathcal{J}_2$ in the form

$$\mathcal{J}_2 = \frac{c_g}{2i}\mathbb{E}\left[e^{i\frac{(\nu-1)}{c}Yt} - e^{-i\frac{(\nu-1)}{c}Yt}\right]$$
$$= \frac{c_g}{2i}\mathbb{E}\left[e^{\frac{it(\nu-1)}{c}\left(\sum_{k=1}^{K} P_k g_k r_k^{-\beta} + N_0\right)} - e^{-\frac{it(\nu-1)}{c}\left(\sum_{k=1}^{K} P_k g_k r_k^{-\beta} + N_0\right)}\right]$$
$$= \frac{c_g}{2i}\left[\varphi(it)\, e^{itc_\nu N_0} - \varphi(-it)\, e^{-itc_\nu N_0}\right], \quad (46)$$

where $c_g = \frac{\pi\nu c_r t}{2\left(1+(\nu c_r t)^2\right)^{\frac{3}{2}}}$, while $\varphi(-it)$ and $\varphi(it)$ are given in (47) and (48), respectively, shown at the top of the next page.

Proof: The proof is presented in Appendix C. ∎

Using (42), (44), (46), (47) and (48), the average SOP of the system reduces to (49), shown at the top of the next page.

A. High SINR Secrecy Outage Probability Approximation

In this section, we present an approximate solution to the SOP computed in (49). From (39), in the high SINR regime, the SOP is

$$P_o = \Pr\left[\frac{1+\gamma_D}{1+\gamma_E} < 2^{R_s}\right]$$
$$\overset{(k)}{\approx} \Pr[\gamma_D < \nu\gamma_E]$$
$$\overset{(l)}{\approx} \Pr\left[X < \frac{\nu g_E r_E^{-\beta}\left(\sum_{k=1}^{K} P_k g_{D_k} r_{D_k}^{-\beta} + N_0\right)}{r_D^{-\beta}\left(\sum_{l=1}^{L} P_l g_{E_l} r_{E_l}^{-\beta} + N_0\right)}\right], \quad (50)$$

where $X = g_D$, $\nu = 2^{R_s}$, while γ_D and γ_E are defined in (3) and (4) respectively. The line (k) in (50) follows from the approximation,[5] $\frac{1+x}{1+y} \simeq \frac{x}{y}$ [31].

[5]This approximation is commonly used in the literature for such analysis (see [31], [32] and the references therein). The approximation becomes more accurate as x and y become larger.

$$\varphi(-it)=\left[\frac{2}{\beta}\left(\frac{itc_\nu P_K}{R^\beta}\right)^{\frac{2}{\beta}}\left\{4^{\frac{1}{\beta}}\Gamma\left(1+\frac{1}{\beta}\right)^2\Gamma\left(-\frac{2}{\beta}\right)+\left(\frac{\pi\left(itc_\nu P_K R^{-\beta}\right)^{\frac{\beta-2}{\beta}}}{2(\beta-2)\left(R^{2\beta}-(itc_\nu P_K)^2\right)}\right)\left[2(\beta-1)R^{2\beta}\right.\right.$$
$$\times\,{}_2F_1\left(-\frac{1}{2},\frac{1}{2}-\frac{1}{\beta},\frac{3}{2}-\frac{1}{\beta},-\left[\frac{(tc_\nu P_K)}{R^\beta}\right]^2\right)-\left((\beta-2)R^{2\beta}+2(itc_\nu P_K)^2\right){}_2F_1\left(\frac{1}{2},\frac{1}{2}-\frac{1}{\beta},\frac{3}{2}-\frac{1}{\beta},-\left[\frac{(tc_\nu P_K)}{R^\beta}\right]^2\right)\Bigg]$$
$$\left.\left.+\frac{\beta}{2}\left(itc_\nu P_K R^{-\beta}\right)^{-\frac{2}{\beta}}{}_3F_2\left(1,1,-\frac{1}{\beta};\frac{1}{2},1-\frac{1}{\beta};-\left[\frac{(tc_\nu P_K)}{R^\beta}\right]^2\right)\right\}\right]^K \tag{47}$$

$$\varphi(it)=\left[\frac{2}{\beta}\left(-\frac{itc_\nu P_K}{R^\beta}\right)^{\frac{2}{\beta}}\left\{4^{\frac{1}{\beta}}\Gamma\left(1+\frac{1}{\beta}\right)^2\Gamma\left(-\frac{2}{\beta}\right)+\left(\frac{\pi\left(-itc_\nu P_K R^{-\beta}\right)^{\frac{\beta-2}{\beta}}}{2(\beta-2)\left(R^{2\beta}+(tc_\nu P_K)^2\right)}\right)\left[2(\beta-1)R^{2\beta}\right.\right.$$
$$\times\,{}_2F_1\left(-\frac{1}{2},\frac{1}{2}-\frac{1}{\beta},\frac{3}{2}-\frac{1}{\beta},-\left[\frac{(tc_\nu P_K)}{R^\beta}\right]^2\right)-\left((\beta-2)R^{2\beta}-2(tc_\nu P_K)^2\right){}_2F_1\left(\frac{1}{2},\frac{1}{2}-\frac{1}{\beta},\frac{3}{2}-\frac{1}{\beta},-\left[\frac{(tc_\nu P_K)}{R^\beta}\right]^2\right)\Bigg]$$
$$\left.\left.+\frac{\beta}{2}\left(-itc_\nu P_K R^{-\beta}\right)^{-\frac{2}{\beta}}{}_3F_2\left(1,1,-\frac{1}{\beta};\frac{1}{2},1-\frac{1}{\beta};-\left[\frac{(tc_\nu P_K)}{R^\beta}\right]^2\right)\right\}\right]^K \tag{48}$$

$$\overline{P}_o=1-\int_0^\infty\frac{1}{(t^2+1)^{\frac{3}{2}}}\left\{\frac{1}{2}{}_2F_1\left(1,1,\frac{1}{2},-\left(\nu t\left(\frac{r_D}{r_E}\right)^\beta\right)^2\right)\left[\varphi(-it)\exp\left(-it\frac{(\nu-1)}{P_s r_D^{-\beta}}N_0\right)+\varphi(it)\exp\left(it\frac{(\nu-1)}{P_s r_D^{-\beta}}N_0\right)\right]\right.$$
$$\left.-\frac{\pi\nu t\left(\frac{r_D}{r_E}\right)^\beta}{4i\left(1+\left(\nu t\left(\frac{r_D}{r_E}\right)^\beta\right)^2\right)^{\frac{3}{2}}}\left[\varphi(it)\exp\left(it\frac{(\nu-1)}{P_s r_D^{-\beta}}N_0\right)-\varphi(-it)\exp\left(-it\frac{(\nu-1)}{P_s r_D^{-\beta}}N_0\right)\right]\right\}\mathrm{d}t \tag{49}$$

Given X follows a double-Rayleigh distribution, then the approximate SOP can be expressed using (41). Thus, we obtain

$$\begin{aligned}\overline{P}_o^{\text{aprx}}&\overset{(m)}{=}\mathbb{E}\left[1-\nu g_E c_r K_1(\nu g_E c_r)\right]\\&=1-\int_0^\infty\nu g_E^2 c_r K_0(g_E)K_1(\nu g_E c_r)\,\mathrm{d}g_E\\&\overset{(n)}{=}1-\frac{1-(\nu c_r)^2+(\nu c_r)^2\ln\left((\nu c_r)^2\right)}{\left((\nu c_r)^2-1\right)^2},\end{aligned}\tag{51}$$

where $c_r=\left(\frac{r_D}{r_E}\right)^\beta$. Line (m) in (51) was obtained by observing that the summation terms cancel out in (l) of (50), while (n) was obtained by invoking [45, Eq. (6.576.4)] After simplification, we obtain a closed-form approximate SOP expression as

$$\overline{P}_o^{\text{aprx}}=\frac{(\nu c_r)^2\left((\nu c_r)^2-\ln\left((\nu c_r)^2\right)-1\right)}{\left((\nu c_r)^2-1\right)^2}.\tag{52}$$

Comparing (49) and (52), it can be observed that, at high SINR regimes, the average SOP can be simplified and expressed in elementary functions, independently of the interference terms. Thus, this approximation lends itself to secrecy analysis based on the relative locations of the vehicular nodes only and allows for better insight into the performance of the system. The term c_r therefore, which is a ratio between the distances of interest, is an important metric for the SOP.

V. Numerical Results and Discussions

In this section, we present and discuss some results from the mathematical expressions derived in the paper. We then investigate the effect of key parameters on the ASC of the system. Monte Carlo simulations were conducted on MATLAB software package with at least 10^5 iterations, while numerical expressions were plotted on Mathematica package. However, most common mathematical packages can be used to plot the expressions. Unless otherwise stated, we have assumed source power $P_s=10$ W, interferer transmit power $P_K=10$ W, source to destination (S-to-D) distance $r_D=4$ m, maximum eavesdropper distance $r_{\max}=10$ m, maximum interferer distance $R=20$ m and path-loss exponent $\beta=2.7$.

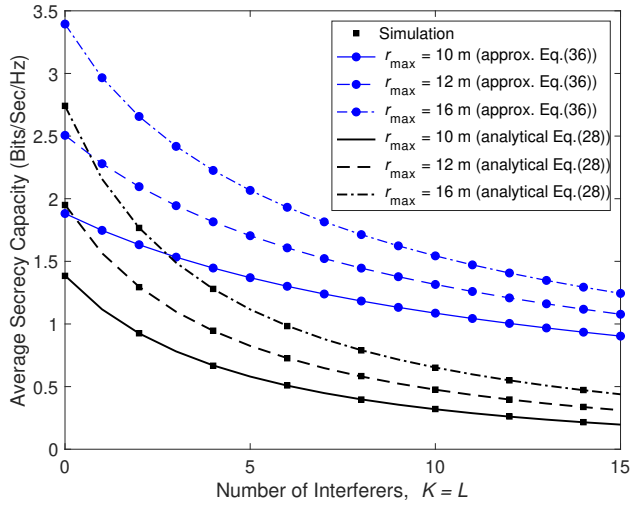

Figure 2: ASC versus number of interferers $K = L$, with varied maximum eavesdropper radius $r_{\max}$.

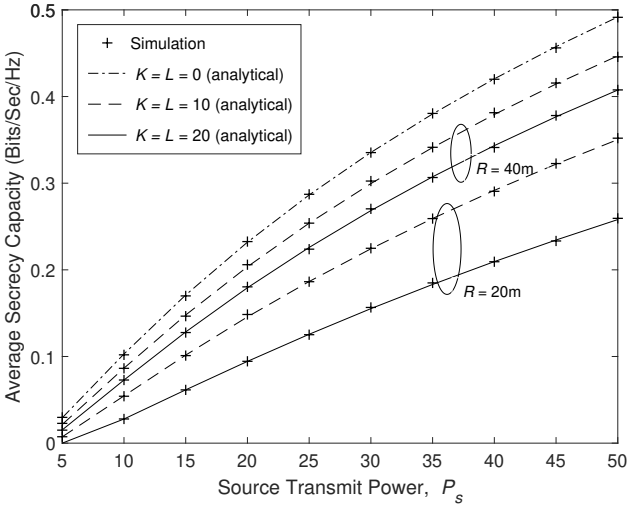

Figure 4: ASC versus source transmit power P_s for varied interferer numbers $K = L$ and maximum interferer distances R.

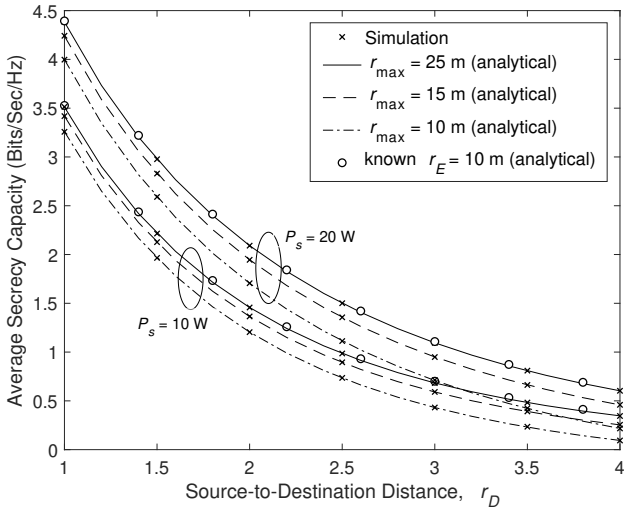

Figure 3: ASC versus source to destination (S-to-D) link for varied source transmit power P_s and known eavesdropper distance r_E.

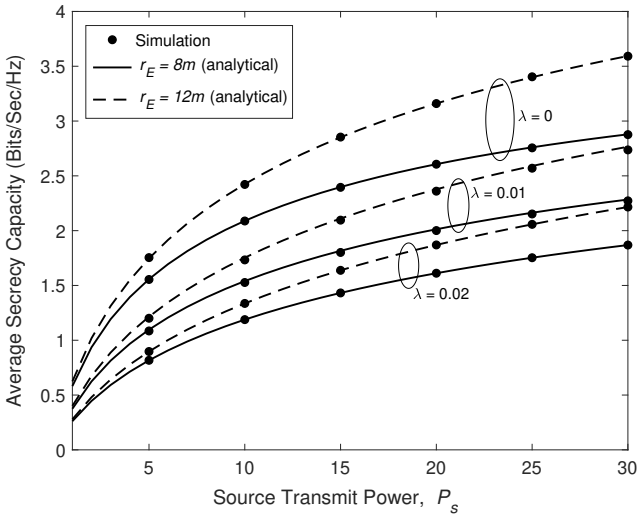

Figure 5: ASC versus source transmit power P_s for varied interferer density λ[interferers/m^2] and source to eavesdropper distances r_E.

A. Average Secrecy Capacity

In this subsection, we examine the ASC of the proposed system. In Fig. 2, we present a plot of the ASC against the number of interfering sources in the network, for both the approximate and exact analytical expressions. The approximate curves were plotted from the expression derived in Eq. (37), while the exact analytical curves were obtained from the expression derived in Eq. (28). We observe that the approximations converge towards the exact analytical solution with increased presence of interfering vehicles. However, given the disparity, the exact solutions are preferable for more precise analysis, while the approximations are valid in analyzing the effect of the various network parameters, due to the similar trends with easier mathematical tractability. It can be further observed from the results that the number of active interfering nodes have a negative impact on the ASC, with the ASC rapidly decreasing with interference. Moreover, this impact can be effective at various eavesdropper distances from the node, as seen when $r_{\max}$ is increased. It should be noted that the parameter $r_{\max}$ is a proxy for the uncertainty of E's location. In a practical scenario, a vehicle is more likely to know the location of D in which it establishes communication with, as against a passive eavesdropper whose presence may not be known. Therefore, we assume both D and E are always within the radius $r_{\max}$, while the interferer nodes are restricted by a larger outer radius of R. The increased secrecy observed when $r_{\max}$ increases indicates that when E is more likely to be closer to S-to-D V2V link, then the secrecy is compromised, and vice versa. The next figure will further demonstrate the importance of $r_{\max}$ and the relative distances of the nodes to the ASC.

Fig. 3 shows a plot of the ASC against the S-to-D distance r_D, with different values of P_s and $r_{\max}$. We assume $R =$ 40m and 5 interfering nodes. First, we observe that the ASC decreases as D moves away from S, which is expected because

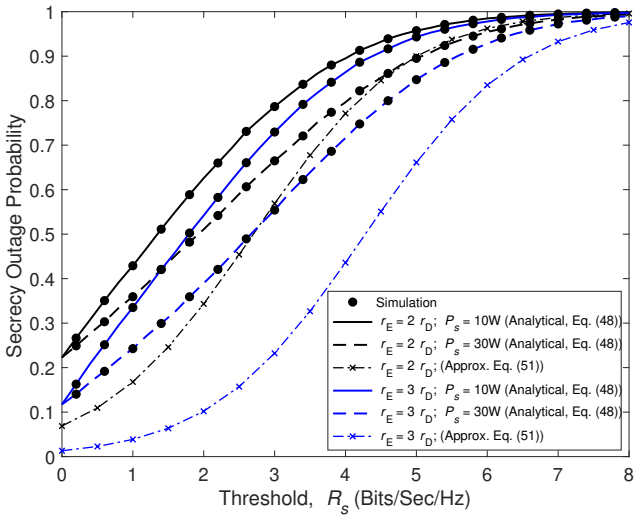

Figure 6: SOP versus Threshold R_s for varied eavesdropper distances r_E and source transmit power P_s.

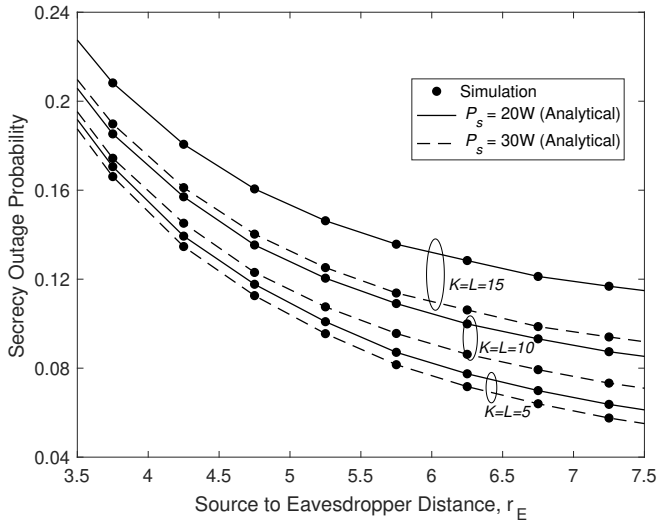

Figure 7: SOP versus source to eavesdropper (S-to-E) link for varied source transmit power P_s.

the SINR at D is also decreasing. Next, we see the effect of increasing the maximum range of E. At the different P_s values, we observe that increasing $r_{\max}$ improves the ASC because this means the likely radius of finding E is extended. However, as $r_{\max}$ is reduced, the ASC rapidly decreases and reaches zero approximately when $r_{\max} = 2r_D$. This shows the significance of the relative locations of S, D and E. To further demonstrate this, we assume a known location for E and use this distance r_E to illustrate the significance of our result with respect to interferer impact on secrecy. We assume $r_E = 10$m and plot the exact ASC for the V2V network, through simulations. From Fig. 3, it can be observed that the ASC for known r_E is much superior to the case when E's location is uncertain. In fact, from our analysis, it is clear that the ASC at $r_E = 10$m is equivalent to the ASC when $r_{\max} = 25$m within the region studied. This therefore signifies the importance of taking into account the uncertainty of the location of E, especially for the security analysis of passive eavesdroppers, when the eavesdropper is unlikely to give away its position by transmissions.

In Fig. 4, we present the ASC with respect to P_s for different number of interfering nodes K and maximum interferer range R. As expected, the ASC increases monotonically with increased P_s. Furthermore, within the region investigated, the ASC is highest without any interfering nodes and degrades with more active interfering nodes, as already demonstrated in the previous figure. Additionally, it can be observed that for the same number of interferers, increasing R, improves the ASC of the system. Given that both S and E are affected by the interference in the network, then an increased radius of interferers, reduces the density of interfering nodes, which in turn improves the ASC.

In Fig. 5, we examine the effect of interference for the case when the number of vehicular nodes are random (unknown). In practice, this is a more realistic scenario albeit the complexity of the analysis is increased due to the addition of another RV. For this case, we model a Poisson point process with the interferer (vehicle) density parameter λ representing interferers per unit area. The figure depicts a plot of the ASC against the source transmit power, with different values of interference density λ and source to eavesdropper (S-to-E) distance r_E. We assume path-loss exponent $\beta = 4$, fixed eavesdropper distances $r_E = 8$m and 12m, as well as interferer densities $\lambda = 0.01$ and 0.02 interferer/m^2. The analytical ASC was obtained using (27) along with (30) for the first MGF term and (23) for the third MGF term. For fixed r_E, the second MGF is obtained using (23), while substituting $r_D = r_E$, such that $\mathcal{M}_{\chi_E}(z) = \frac{4}{3(1+zP_s r_E^{-\beta})^2} {}_2F_1\left(2, \frac{1}{2}, \frac{5}{2}, \frac{zP_s r_E^{-\beta}-1}{zP_s r_E^{-\beta}+1}\right)$. Considering Fig. 5, we can observe that the case with no interference (i.e. $\lambda = 0$) provides the highest ASC rate, as expected. As the interferer density increases, at fixed values of r_E and P_s, we observe that the ASC rate decreases due to the effect of interference. Additionally, we consider a known and fixed r_E in order to determine the effect of increasing the relative distances of S-to-D link compared to S-to-E link. It can be observed that the ASC increases when r_E is increased and this effect is more pronounced when P_s is greater. For instance, at $\lambda = 0$, when P_s increases from 5W to 30W, the ASC increases by as much as 0.7 bits/s/Hz between values for $r_E = 2r_D = 8$m and $r_E = 3r_D = 12$m. In fact, increasing P_s (or equivalently increasing SIR) results in better ASC at all values of r_E and λ.

B. Average Secrecy Outage Probability

In this subsection, we present results for the average SOP of the system from both the approximate and exact analytical expressions. The approximate curves were plotted from the approximate high SINR bounds derived in Eq. (52), while the exact analytical curves were obtained from the expression derived in Eq. (49). In Fig. 6, the SOP is plotted against the threshold values of the secrecy rate, R_s, for different values of the source power and eavesdropper distance. Specific values employed are $r_D = 4$m, $K = L = 1$ and $R = 10$m. From

the plot, we observe that the approximate expressions provide a lower bound for the exact expressions and are tighter at higher SINR (i.e. $P_s = 30$W) with $r_E = 2r_D = 8$m. This indicates that for high SINR regimes, the effect of the network parameters can be closely monitored using the more tractable approximate expressions. We further observe that the SOP increases steadily as the threshold rate increases. Similarly, the outage probability increases when the eavesdropper is closer to the source as well as when the source power decreases, i.e. lower SINR. Thus, the secrecy threshold rate needs to be selected while taking into consideration the effects of possible eavesdropper location in the network and SINR rates, in order to minimize the outage.

In Fig. 7, we study the SOP as a function of the S-to-E distance, for different values of the source power and interference. While varying r_E, we normalized the S-to-D distance, such that $r_D = 1$m. As expected, the SOP is observed to monotonically decrease as r_E increases. This indicates that the increased relative distance between the nodes improves the secrecy and thereby reduces the possibility of outage. Additionally, we observe that increased interference or reduced source power, increases the probability of secrecy outage.

VI. Conclusions

In this paper, we examined the impact of interference on the PLS of a wireless vehicular communication network, by analyzing the ASC and SOP of the system. Due to the nature of the network and statistics of the SINR, we reduced the complexity of the solution by expressing the ASC in terms of the MGF of the RVs representing the joint fading and random distances of interfering nodes, and eavesdropper node. Similarly, we expressed the SOP in terms of the characteristic function of the joint interferer statistics RVs. Thereafter, we found closed-form expressions for the various MGFs and characteristic functions, which were then used to analyze the performance of the system in terms of the considered performance metrics. The results demonstrated the effect of some key system parameters such as the distances of the V2V nodes and eavesdropper node, as well as the number and distances of interfering nodes. The results showed the importance of the analysis with respect to considering uncertainty of the eavesdropper location. Particularly, the maximum range of E, indicates the level of uncertainty on E's location and reducing this radius reduces the ASC, while assuming a known eavesdropper location significantly improves the ASC. The results also showed that for both the ASC and SOP, the presence of interfering nodes reduce the achievable secrecy of the system, thereby further highlighting the importance of our analysis.

Appendix A
Proof of Eq. (18)

Upon invoking [45, Eq. (2.33.10)] along with some mathematical manipulations (for $\beta > 2$),[6] the inner integral in (14) resolves to

$$\int_0^R e^{-zg_D r_D^{-\beta}} \frac{2r_D}{R^2} \mathrm{d}r_D = \frac{R^2 e^{-zg_D R^{-\beta}} - (zg_D)^{\frac{2}{\beta}} \Gamma\left(1-\frac{2}{\beta}, zg_D R^{-\beta}\right)}{R^2}, \quad (53)$$

thus, (15) becomes

$$\begin{aligned}\mathcal{M}_\psi(z) =& \int_0^\infty \mathrm{G}_{0,2}^{2,0}\left(\frac{1}{4}g_D^2 \middle| \begin{matrix} - \\ \frac{1}{2},\frac{1}{2} \end{matrix}\right) \times \frac{R^2 e^{-zg_D R^{-\beta}} - (zg_D)^{\frac{2}{\beta}} \Gamma\left(1-\frac{2}{\beta}, zg_D R^{-\beta}\right)}{R^2} \mathrm{d}g_D \\ =& \int_0^\infty \mathrm{G}_{0,2}^{2,0}\left(\frac{1}{4}g_D^2 \middle| \begin{matrix} - \\ \frac{1}{2},\frac{1}{2} \end{matrix}\right) \frac{(zg_D)^{\frac{2}{\beta}} \Gamma\left(1-\frac{2}{\beta}, zg_D R^{-\beta}\right)}{R^2} \\ & - \int_0^\infty \mathrm{G}_{0,2}^{2,0}\left(\frac{1}{4}g_D^2 \middle| \begin{matrix} - \\ \frac{1}{2},\frac{1}{2} \end{matrix}\right) e^{-zg_D R^{-\beta}} \mathrm{d}g_D, \quad (54)\end{aligned}$$

which after several manipulations can be expressed as in (18). It is worth noting that, using [45, Eq. (6.621.3)], the second integral term in (54) reduces to the first term in (18), while using [52, Eq. (2.16.61.1)] and the Bessel representation of the PDF in (22), we can express the first integral in (54) as the last 3 terms in (18).

This completes the proof.

Appendix B
Proof of Eq. (29)

From (14) and (53), the MGF for the cumulative interference can be represented as

$$\begin{aligned}\mathcal{M}(z|g_D) =& \lim_{\substack{K\to\infty, R\to\infty \\ \lambda = K/\pi R^2}} \prod_{k=1}^{K} \int_0^R e^{-zg_D r_D^{-\beta}} f_{r_D}(r) \mathrm{d}r_D \\ =& \lim_{\substack{K\to\infty, \\ R\to\infty \\ \lambda = K/\pi R^2}} \left[e^{-zg_D R^{-\beta}} - \frac{(zg_D)^{\frac{2}{\beta}} \Gamma\left(1-\frac{2}{\beta}, zg_D R^{-\beta}\right)}{R^2} \right]^K. \end{aligned} \quad (55)$$

By using [54, Eq. (4.2.23)] and the fact that $\Gamma(s) = \Gamma(s,0)$, then (55) becomes

$$\begin{aligned}\mathcal{M}(z|g_D) =& \lim_{K\to\infty} \left[1 - \frac{\lambda\pi}{K}(zg_D)^{\frac{2}{\beta}} \Gamma\left(1-\frac{2}{\beta}, 0\right)\right]^K \\ =& \exp\left(-\lambda\pi (zg_D)^{\frac{2}{\beta}} \Gamma\left(1-\frac{2}{\beta}\right)\right), \end{aligned} \quad (56)$$

where the final line in (56) was obtained by invoking [45, Eq. (1.211.4)].

This completes the proof.

[6] For $\beta > 2$, only the free-space model ($\beta = 2$) is excluded. Hence, this constraint is acceptable for our purpose.

APPENDIX C
PROOF OF EQS. (47) AND (48)

The characteristic functions are defined in (44) and (46). We first evaluate $\varphi(-it)$, thus

$$\begin{aligned}\varphi(-it) &= \mathbb{E}\left[e^{-itc_\nu \sum_{k=1}^{K} P_k g_k r_k^{-\beta}}\right] \\ &= \int_0^{\infty}\int_0^{R} e^{-itc_\nu \sum_{k=1}^{K} P_k g_k r_k^{-\beta}} \frac{2r_k}{R^2} g_k K_0(g_k)\,\mathrm{d}g_k \mathrm{d}r_k \\ &\overset{(j)}{=} \prod_{0}^{K}\int_0^{\infty}\left(-\frac{itc_\nu P_k g_k}{R^\beta}\right)^{\frac{2}{\beta}} \\ &\quad \times \Gamma\left(-\frac{2}{\beta}, -\frac{itc_\nu P_k g_k}{R^\beta}\right) g_k K_0(g_k)\,\mathrm{d}g_k, \quad (57)\end{aligned}$$

where (j) in (57) was obtained using [45, Eq. (2.33.10)]. By invoking [52, Eq. (2.16.61.1)] along with some algebraic manipulations, $\varphi(-it)$ can be evaluated as in (47).

The term $\varphi(it) = \mathbb{E}\left[e^{itc_\nu \sum_{k=1}^{K} P_k g_k r_k^{-\beta}}\right]$ can be evaluated using similar analysis to the derivation of (47). Thus, using [52, Eq. (2.16.61.1)] along with some algebraic manipulations, a closed-form expression for $\varphi(it)$ can be obtained as in (48).

This completes the proof.

REFERENCES

[1] C. Chen, J. Hu, T. Qiu, M. Atiquzzaman, and Z. Ren, "CVCG: Cooperative V2V-Aided Transmission Scheme Based on Coalitional Game for Popular Content Distribution in Vehicular Ad-Hoc Networks," *IEEE Trans. Mobile Comput.*, vol. 18, no. 12, pp. 2811–2828, Dec. 2019.

[2] T. Qiu, R. Qiao, and D. O. Wu, "EABS: An Event-Aware Backpressure Scheduling Scheme for Emergency Internet of Things," *IEEE Trans. Mobile Comput.*, vol. 17, no. 1, pp. 72–84, Jan. 2018.

[3] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Vehicular Communications*, vol. 20, p. 100182, 2019.

[4] L. Farhan, R. Kharel, O. Kaiwartya, M. Hammoudeh, and B. Adebisi, "Towards green computing for Internet of things: Energy oriented path and message scheduling approach," *Sustainable Cities and Society*, vol. 38, pp. 195 – 204, 2018.

[5] Y. Ni, L. Cai, J. He, A. Vinel, Y. Li, H. Mosavat-Jahromi, and J. Pan, "Toward reliable and scalable internet of vehicles: Performance analysis and resource management," *Proc. IEEE*, vol. 108, no. 2, pp. 324–340, Feb. 2020.

[6] J. Hu, C. Chen, T. Qiu, M. Atiquzzaman, and Q. Pei, "Elastic and Inelastic Content Distribution based on Clonal Selection in VANETs," in *IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[7] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Netw.*, vol. 32, no. 3, pp. 78–83, May 2018.

[8] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.

[9] W. Dong, Y. Li, R. Hou, X. Lv, H. Li, and B. Sun, "A Blockchain-based Hierarchical Reputation Management Scheme in Vehicular Network," in *IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[10] A. Kaci and A. Rachedi, "Mc-Track: A Cloud based data oriented vehicular tracking system with adaptive security," in *IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[11] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[12] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Commun.*, vol. 14, no. 12, pp. 1–14, Dec. 2017.

[13] Y. Y. Zu and K. Xiao, "Outage performance of secure cooperative systems over correlated rayleigh fading channels," in *2016 25th Wireless and Optical Commun. Conf. (WOCC)*, May 2016, pp. 1–5.

[14] G. C. Alexandropoulos and K. P. Peppas, "Secrecy outage analysis over correlated composite Nakagami-m /Gamma fading channels," *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 77–80, Jan. 2018.

[15] M. Z. I. Sarkar, T. Ratnarajah, and M. Sellathurai, "Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppers," in *Asilomar Conf. Sig. Sys. Comput.*, Nov. 2009, pp. 829–833.

[16] M. Srinivasan and S. Kalyani, "Secrecy capacity of κ-μ shadowed fading channels," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1728–1731, Aug. 2018.

[17] J. Sun, X. Li, M. Huang, Y. Ding, J. Jin, and G. Pan, "Performance analysis of physical layer security over κ-μ shadowed fading channels," *IET Commun.*, vol. 12, no. 8, pp. 970–975, 2018.

[18] J. Sun, H. Bie, X. Li, J. Zhang, G. Pan, and K. M. Rabie, "Secrecy Performance Analysis of SIMO Systems Over Correlated κ-μ Shadowed Fading Channels," *IEEE Access*, vol. 7, pp. 86 090–86 101, 2019.

[19] N. Bhargav and S. L. Cotton, "Secrecy capacity analysis for α-μ /κ-μ and κ-μ / α-μ fading scenarios," in *2016 IEEE 27th Annual Int. Symp. Personal, Indoor, and Mobile Radio Commun. (PIMRC)*, Sep. 2016, pp. 1–6.

[20] O. S. Badarneh, P. C. Sofotasios, S. Muhaidat, S. L. Cotton, K. Rabie, and N. Al-Dhahir, "On the Secrecy Capacity of Fisher-Snedecor F Fading Channels," in *2018 14th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2018, pp. 102–107.

[21] G. Anjos, D. Castanheira, A. Silva, and A. Gameiro, "Securing Non-Orthogonal Multiple Access Systems Against Simultaneous Eavesdropping Attacks Coming from Inside and Outside of the Network," in *2019 IEEE 30th Annual Int. Symp. Personal, Indoor, and Mobile Radio Commun. (PIMRC*, 2019, pp. 1–7.

[22] Z. Shu, Y. Yang, Y. Qian, and R. Q. Hu, "Impact of interference on secrecy capacity in a cognitive radio network," in *Proc. IEEE Global Commun. (GLOBECOM)*, Dec. 2011, pp. 1–6.

[23] D. S. Karas, A. A. Boulogeorgos, G. K. Karagiannidis, and A. Nallanathan, "Physical layer security in the presence of interference," *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 802–805, Dec. 2017.

[24] X. Wang, "Moving relays in downlink multiuser networks - a physical-layer security perspective," in *IEEE Veh. Technol. Conf. (VTC Spring)*, 2018, pp. 1–5.

[25] E. M. Ghourab, M. Azab, M. F. Feteiha, and H. El-Sayed, "A Novel Approach to Enhance the Physical Layer Channel Security of Wireless Cooperative Vehicular Communication Using Decode-and-Forward Best Relaying Selection," *Wireless Commun. Mobile Comput.*, pp. 1–15, May 2018.

[26] Y. Ai, M. Cheffena, A. Mathur, and H. Lei, "On Physical Layer Security of Double Rayleigh Fading Channels for Vehicular Communications," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 1038–1041, Dec. 2018.

[27] L. Xu, X.-H. Yu, H.-P. Wang, X. Dong, Y. Liu, W. Lin, X. Wang, and J. Wang, "Physical layer security performance of mobile vehicular networks," *Mobile Netw. Appl.*, pp. 1–7, 2019.

[28] I. Dey, R. Nagraj, G. G. Messier, and S. Magierowski, "Performance analysis of relay-assisted mobile-to-mobile communication in double or cascaded Rayleigh fading," in *IEEE Pacific Rim Conf. Commun. Comput. Sign. Process.*, Aug. 2011, pp. 631–636.

[29] L. Sun, P. Ren, and Q. Du, "Distributed source-relay selection scheme for vehicular relaying networks under eavesdropping attacks," *EURASIP J. Wireless Commun. Netw.*, vol. 2014, no. 1, p. 109, Jul 2014.

[30] J. Zhang and G. Pan, "Secrecy outage analysis with kth best relay selection in dual-hop inter-vehicle communication systems," *AEU - Int J. Electron. Commun.*, vol. 71, pp. 139–144, 2017.

[31] A. Pandey and S. Yadav, "Physical Layer Security in Cooperative AF Relaying Networks With Direct Links Over Mixed Rayleigh and Double-Rayleigh Fading Channels," *IEEE Trans. Veh. Tech.*, vol. 67, no. 11, pp. 10 615–10 630, Nov. 2018.

[32] ——, "Performance evaluation of amplify and forward relaying cooperative vehicular networks under physical layer security," *Trans. Emerging Telecommun. Technol.*, vol. 29, no. 12, p. e3534, Oct. 2018.

[33] ——, "Physical layer security in cooperative amplify-and-forward relay networks over mixed Nakagami-m and double Nakagami-m fading channels: Performance evaluation and optimisation," *IET Commun.*, vol. 14, no. 1, pp. 95–104, 2020.

[34] L. Farhan, O. Kaiwartya, L. Alzubaidi, W. Gheth, E. Dimla, and R. Kharel, "Toward Interference Aware IoT Framework: Energy and Geo-Location-Based-Modeling," *IEEE Access*, vol. 7, pp. 56 617–56 630, 2019.

[35] R. Kasana, S. Kumar, O. Kaiwartya, R. Kharel, J. Lloret, N. Aslam, and T. Wang, "Fuzzy-based channel selection for location oriented services in multichannel VCPS environments," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4642–4651, Dec 2018.
[36] O. Kaiwartya, Y. Cao, J. Lloret, S. Kumar, N. Aslam, R. Kharel, A. H. Abdullah, and R. R. Shah, "Geometry-Based Localization for GPS Outage in Vehicular Cyber Physical Systems," *IEEE Trans. Veh. Tech.*, vol. 67, no. 5, pp. 3800–3812, May 2018.
[37] S. Kumar, U. Dohare, K. Kumar, D. Prasad, K. N. Qureshi, and R. Kharel, "Cybersecurity measures for geocasting in vehicular cyber physical system environments," *IEEE Internet Things J.*, pp. 1–1, 2019.
[38] A. Salem, K. M. Rabie, K. A. Hamdi, E. Alsusa, and A. M. Tonello, "Physical layer security of cooperative relaying power-line communication systems," in *2016 Int. Symp. Power Line Commun, and its Applications (ISPLC)*, Mar. 2016, pp. 185–189.
[39] A. Salem, K. A. Hamdi, and E. Alsusa, "Physical Layer Security Over Correlated Log-Normal Cooperative Power Line Communication Channels," *IEEE Access*, vol. 5, pp. 13 909–13 921, 2017.
[40] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical Layer Security With RF Energy Harvesting in AF Multi-Antenna Relaying Networks," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3025–3038, Jul. 2016.
[41] D. S. Karas, A. A. Boulogeorgos, and G. K. Karagiannidis, "Physical layer security with uncertainty on the location of the eavesdropper," *IEEE Wireless Commun. Lett.*, vol. 5, no. 5, pp. 540–543, Oct. 2016.
[42] A. S. Akki and F. Haber, "A statistical model of mobile-to-mobile land communication channel," *IEEE Trans. Veh. Tech.*, vol. 35, no. 1, pp. 2–7, Feb. 1986.
[43] V. Erceg, S. J. Fortune, J. Ling, A. J. Rustako, and R. A. Valenzuela, "Comparisons of a computer-based propagation prediction tool with experimental data collected in urban microcellular environments," *IEEE J. Sel. Areas Commun.*, vol. 15, no. 4, pp. 677–684, May 1997.
[44] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals, and Series: More Special Functions*, Gordon and Breach Sci. Publ., New York, 1990, vol. 3.
[45] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. Califonia: Academic Press, 7th ed., 2007.
[46] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[47] O. S. Badarneh, P. C. Sofotasios, S. Muhaidat, S. L. Cotton, K. Rabie, and N. Al-Dhahir, "On the secrecy capacity of Fisher-Snedecor $\mathcal{F}$ fading channels," in *14th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2018, pp. 102–107.
[48] K. A. Hamdi, "Capacity of MRC on correlated Rician fading channels," *IEEE Trans. Commun.*, vol. 56, no. 5, pp. 708–711, May 2008.
[49] J. Salo, H. M. El-Sallabi, and P. Vainikainen, "The distribution of the product of independent Rayleigh random variables," *IEEE Trans. Antennas Propag.*, vol. 54, no. 2, pp. 639–643, Feb. 2006.
[50] Y. Shobowale and K. Hamdi, "A unified model for interference analysis in unlicensed frequency bands," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 4004–4013, Aug. 2009.
[51] D. J. Daley, *An Introduction to the Theory of Point Processes : Volume II: General Theory and Structure*, 2nd ed., ser. Probability and Its Applications. New York, NY: Springer New York, 2008.
[52] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals, and Series: Special Functions*, Gordon and Breach Sci. Publ., New York, 1986, vol. 2.
[53] S. Ross, *A First Course in Probability*, 7th ed. Pearson Education, Inc., New Jersey, 2006.
[54] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, ninth dover printing, tenth gpo printing ed. New York: Dover, 1964.

Abubakar U. Makarfi (M'12–SM'20) received the B.Eng. degree (with first-class honors) in electrical and electronic engineering in 2001 and the M.Tech. degree in telecommunications and electronics engineering in 2005. He then received his Ph.D. in electrical and electronic engineering (wireless communications) from the University of Manchester in 2013. He has previously worked in several capacities as an engineer with the Nigerian Navy and the National Space Agency in Nigeria. He is currently a post-doctoral research associate with Manchester Metropolitan University, UK.

Khaled M. Rabie (M'15–SM'20) received the M.Sc. and Ph.D. degrees in electrical and electronic engineering from The University of Manchester, in 2011 and 2015, respectively. He is currently a Lecturer with the Department of Engineering, Manchester Metropolitan University (MMU), U.K. He has worked as a part of several large-scale industrial projects and has published over 90 articles in prestigious journals and international conferences (mostly IEEE). He serves regularly on the Technical Program Committee (TPC) of several major IEEE conferences, such as GLOBECOM, ICC, and VTC. He was a recipient of the Best Student Paper Award from the IEEE ISPLC, TX, USA, in 2015. He serves as an Associate Editor for IEEE Access, an Area Editor for Physical Communication, and an Executive Editor for the Transactions on Emerging Telecommunications Technologies journal. He is also a Fellow of the U.K. Higher Education Academy (FHEA).

Omprakash Kaiwartya (M'14) is currently working as a Lecturer at the School of Science & Technology, Nottingham Trent University (NTU), UK. Previously, He was a Research Associate at the Northumbria University, Newcastle, UK, in 2017 and a Postdoctoral Research Fellow at the Universiti Teknologi Malaysia (UTM) in 2016. He received his Ph.D. degree in Computer Science from Jawaharlal Nehru University, New Delhi, India, in 2015. His research interest focuses on IoT centric future technologies for diverse domain areas focusing on Transport, Healthcare, and Industrial Production. His recent scientific contributions are in Internet of connected Vehicles (IoV), Electronic Vehicles Charging Management (EV), Internet of Healthcare Things (IoHT), and Smart use case implementations of Sensor Networks. He is Associate Editor of reputed SCI Journals including IET Intelligent Transport Systems, EURASIP Journal on Wireless Communication and Networking, Ad-Hoc & Sensor Wireless Networks, IEEE Access, and Transactions on Internet and Information Systems. He is also Guest Editor of many recent special issues in reputed journals including IEEE Internet of Things Journal, IEEE Access, MDPI Sensors, and MDPI Electronics.

Kabita Adhikari (M'14) received her Ph.D degree from Newcastle University, Newcastle upon Tyne, U.K. in 2019. She received her M.Sc. degree from Northumbria University, Newcastle upon Tyne, U.K. in 2007 and her B.Eng. degree from the Institute of Engineering, Pulchowk Campus, Nepal in 2004. She is currently a lecturer in Signal Processing and Control at the School of Engineering, Newcastle University. Her research interests include integration of the conventional mathematical and signal processing methods with leading edge machine learning techniques for the application in healthcare, communications, control and robotic technologies.

Galymzhan Nauryzbayev (M'16) received the B.Sc. (Hons.) degree and M.Sc. (Hons.) degree in Radio Engineering, Electronics and Telecommunications from Almaty University of Power Engineering and Telecommunication, Almaty, Kazakhstan, in June 2009 and June 2011, respectively. In 2016, he obtained a Ph.D. degree in Wireless Communications from the University of Manchester, UK. He is currently an Assistant Professor at Nazarbayev University (Nur-Sultan, Kazakhstan). His research interest is in the area of wireless communication systems, with particular focus on multi-user MIMO systems, cognitive radio, signal processing, energy harvesting, visible light communications, NOMA, interference mitigation, etc. Dr Nauryzbayev served as a Technical Program Committee member on numerous IEEE flagship conferences.

Xingwang Li (M'15–SM'20) received the B.Sc. degree from Henan Polytechnic University, in 2007, the M.Sc. degree from the University of Electronic Science and Technology of China, in 2010, and the Ph.D. degree from the Beijing University of Posts and Telecommunications, in 2015. From 2010 to 2012, he was working with Comba Telecom Ltd., Guangzhou, China, as an Engineer. From 2017 to 2018, he was a Visiting Scholar with Queen's University Belfast, Belfast, U.K. He is currently an Associate Professor with the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo, China. His research interests include MIMO communication, cooperative communication, hardware constrained communication, non-orthogonal multiple access, physical layer security, unmanned aerial vehicles, and the Internet-of-Things. He is currently an Editor on the Editorial Board of IEEE ACCESS, Computer Communications, Physical Communication, and KSII Transactions on Internet and Information Systems. He is also a Lead Guest Editor of the special issue on Recent Advances in Physical Layer Technologies for 5G-Enabled Internet of Things of Wireless Communications and Mobile Computing. He has served as many TPC/Co-Chair, such as IEEE GLOBECOM, IEEE/CIC ICCC, IEEE WCNC, IEEE VTC, and IEEE/IET CSNDSP.

Rupak Kharel (M'09–SM'18) received the Ph.D. degree in secure communication systems from Northumbria University, U.K., in 2011. He is currently a Reader (Associate Professor) within the Department of Computing and Mathematics, Manchester Metropolitan University. His research interests include various use cases and the challenges of the IoT and cyber physical systems including Internet of Vehicles (IoV), cyber security, physical layer security, 5G and beyond systems. He is a Principal Investigator of multiple government and industry funded research projects. Rupak is a Senior member of the IEEE, member of the IET and a Fellow of the Higher Education Academy (FHEA), U.K.