Achievable secrecy rate analysis in mmWave ad hoc networks with multi-array antenna transmission and artificial noise

Ahmed Fathy Darwesh | Abraham O. Fapojuwo

Department of Electrical and Computer Engineering, University of Calgary, AB, Canada

Correspondence
Ahmed Fathy Darwesh, Department of Electrical and Computer Engineering, University of Calgary, AB, Canada.
Email: ahmed.darwesh@ucalgary.ca

Abstract
This paper analyzes the achievable secrecy rate in a millimeter wave (mmWave) ad hoc network with multi-array antenna transmission in the presence of non-colluding and colluding eavesdroppers. By exploiting the tools of stochastic geometry, the average achievable secrecy rate is derived, taking into consideration the impact of blockages, directional beamforming, and Nakagami-\(m\) fading. Moreover, a simple yet effective artificial noise transmission (Tx-AN) technique is applied at the transmitting nodes to enhance the secrecy performance while the channel state information at the desired transmitter is unknown. Numerical and simulation results are presented for the average achievable secrecy rate in the mmWave ad hoc network without and with the Tx-AN technique. For example, at the high transmit power (>20 dBm), the average achievable secrecy rate with the Tx-AN technique is up to three times higher than that obtained when the Tx-AN technique is not used. Furthermore, the results demonstrate the secrecy robustness of the Tx-AN technique against increasing eavesdroppers’ intensity. Finally, the proper power allocation between the message and AN signals that maximizes the average achievable secrecy rate is computed.

1 | INTRODUCTION

1.1 | Background

Millimeter wave (mmWave) will play a crucial role in the next-generation wireless networks (i.e. 5G and 6G networks), as it enables the use of frequency bands above 6 GHz [1]. In this regard, mmWave network offers a huge spectrum that increases the data transfer rate [2]. Moreover, the small wavelength in the mmWave band translates to small antenna size making the use of a large number of antennas practical. However, an mmWave network is plagued with many challenges including high propagation loss, sensitivity to blockages, and penetration loss [3]. Most recent researches are devoted to overcoming these drawbacks [4–6]. The mmWave band is also beneficial for ad hoc networks to achieve a data rate performance better than that of an ad hoc network operating in the microwave bands [7]. Besides, more interference immunity is attained because of the high vulnerability to blockages and use of directional antenna arrays for transmission and reception [8]. The mmWave ad hoc network performance is evaluated using the stochastic geometry framework in [7, 9].

A major concern for the next-generation wireless networks is information security. This concern escalates with the rapid increase of the eavesdroppers’ computational capabilities and use of various eavesdropping strategies. For example, the work [10] reports that massive data transmission needs to be highly secured in an mmWave ad hoc network subject to eavesdroppers with high capabilities. Therefore, the conventional secrecy techniques that assume any limitations on the adversary side are inappropriate to achieve a secure information transmission. Recently, researchers have demonstrated a significant interest in the physical layer security (PLS) to give an additional layer of security [11–14]. Physical layer security is defined as the study of different techniques for improving the security of networks by exploiting the wireless channel characteristics. The PLS techniques are more appropriate to achieve secure transmission due to incurring less computational complexity than the security techniques at the higher protocol layers [15]. Thus, references [16–19] study the PLS in a microwave ad hoc network in the presence of eavesdroppers. Recent works evaluate the secrecy performance for different types of mmWave networks [20–22]. However, a little progress has been made in the PLS of mmWave ad hoc network subject to eavesdroppers [23, 24]. Subsequently,
more work is still needed to analyze and enhance the secrecy performance in mmWave ad hoc networks.

### 1.2 Related work

In [16], the far away nodes from the intended receiver are selected to transmit the artificial noise (AN) to enhance the secrecy performance in an ad hoc network. Furthermore, the tradeoffs between achievable node throughput and the allowable number of eavesdroppers for the non-colluding and colluding eavesdroppers are studied. The effect of the PLS constraints on the throughput of large-scale decentralized wireless networks is introduced in [17]. Moreover, to achieve high security, the secrecy guard zone with AN networks is applied. In [18], the tradeoff between the connection and secrecy outage probabilities for an ad hoc network with multi-antenna transmission is presented. Further, the sectoring or beamforming are combined with the AN to improve the secrecy performance in the wireless ad hoc network. The connection outage probability and the secrecy outage probability for a single-input single-output (SISO) ad hoc network are analyzed in [19], where a hybrid full-/half-duplex receiver technique is utilized to enhance the secrecy transmission. In this technique, the authors divide the receivers in a wireless ad hoc network into full-duplex receivers which transmit jamming signal and receive the desired signal simultaneously, and half-duplex receivers receiving only the desired signals. Note that all the previous works in [16–19] focus on the PLS in ad hoc networks designed for the sub-6 GHz bands.

Based on the mmWave band, the secrecy outage probability achieved via an on-off transmission scheme with AN transmission strategy is analyzed in [25], where the secrecy performance of the mmWave network relies on the destination’s and the eavesdropper’s directions and propagation paths. In [26], expressions for transmitting probability and secrecy outage probability in mmWave systems have been derived with different secure on-off transmission strategies. The analysis includes capacity threshold-based on-off scheme, secrecy guard zone on-off scheme, and hybrid on-off scheme. In [27], the secrecy throughput of the mmWave network is proposed. In addition, three transmission schemes are investigated, namely, maximum ratio transmitting (MRT) beamforming, AN beamforming, and partial MRT (PMRT) beamforming to improve the secrecy performance. This work is extended against randomly located eavesdroppers in [22], in which the secrecy throughput under a secrecy outage probability constraint is maximized. However, both [27] and [22] assume that the instantaneous channel state information (CSI) between the desired user and its transmitter is perfectly known. In [28], a hybrid analog-digital precode design is proposed to enhance the PLS of mmWave multiple-input single-output (MISO) systems with partial channel knowledge. In addition to maximizing the secrecy rate lower bound, a low-complexity AN-aided hybrid precode design is introduced. Based on an iterative fast Fourier transform (FFT), the authors in [29] designed an optimized antenna subset selection that provided low computational complexity and improved secrecy performance. In [30], the PLS of mmWave relaying networks in the presence of multiple eavesdroppers was studied. The first order integral expressions of average achievable secrecy rate of secure connectivity probability and secrecy outage probability have been derived. Also considering security of mmWave relaying networks, the impact of an untrusted amplify-and-forward (AF) relay and eavesdroppers has been investigated in [31]. To achieve secure communication, cooperative jamming by both the transmitter and receiver has been presented. Focusing on the PLS in an mmWave ad hoc network, the authors in [23] evaluated the average secrecy rate in a large-scale mmWave ad hoc network with and without the AN scheme. Moreover, the directional beamforming is used between the transmitters and their corresponding receivers using a single-array antenna at all nodes (i.e. SISO ad hoc network). The most recent work for enhancing the secure communication of an mmWave ad hoc network in the presence of passive non-colluding eavesdroppers has been presented in [32]. In this work, a Sight-based Cooperative Jamming (SCJ) scheme has been investigated to improve the secrecy performance by utilizing the signal attenuation difference between the line of sight (LoS) and non-LoS (NLoS) links of the mmWave signal. The SCJ scheme relies on inserting a group of jamming transmitters in the mmWave ad hoc network to transmit with a certain probability the AN signal that degrades the signal-to-noise ratio (SNR) at the eavesdroppers. Moreover, the secrecy transmission capacity is presented to evaluate the secrecy performance under the SCJ scheme.

Unlike the existing works in [16–19] that study the PLS of microwave ad hoc networks, this paper focuses on the secrecy rate analysis of mmWave ad hoc networks with multi-array antenna transmission, taking into account the impact of blockages, directional beamforming, and Nakagami-\(m\) fading. Furthermore, the AN secrecy techniques in [22, 25, 27, 28] mainly depend on the knowledge of the CSI at the desired transmitter. In contrast, the AN technique applied in this paper to enhance secrecy performance does not require knowledge of the CSI between the desired transmitter-receiver (Tx-Rx) pair. Unlike the previous works which neglect small-scale fading [23] and assumes a single-array antenna for message transmission [23, 32], this paper accounts for both small scale fading and multi-array antenna transmission.

### 1.3 Motivation and contribution

The motivation for this paper is the lack of mmWave network secrecy performance results in the existing literature that consider an mmWave ad hoc network characterized by small-scale fading, multi-array antenna transmission, and the use of AN technique that does not require knowledge of the CSI. Accounting for these three factors, an extensive secrecy rate analysis of an mmWave ad hoc network with multi-array antenna transmission in the presence of non-colluding and colluding eavesdroppers is presented. In addition, a simple yet effective AN transmission technique, which does not require knowledge of the CSI at the desired transmitter, is applied to enhance the secrecy performance.
The main contributions of this paper are summarized as follows:

- A mathematical expression is derived for the average achievable secrecy rate in an mmWave ad hoc network with multi-array antenna transmission, taking into account the effect of blockages, Nakagami-$m$ fading, and directional beamforming in the transmission and reception. Results are derived for the two scenarios of non-colluding and colluding eavesdroppers.
- A multi-array AN transmission (Tx-AN) technique that does not require knowledge of the CSI at the desired transmitter is proposed to enhance the average achievable secrecy rate. Further, our analysis presents the secrecy robustness of the Tx-AN technique against increasing the eavesdroppers’ intensity.
- Approximate average achievable secrecy rate results with and without the Tx-AN technique are derived under a simplified LoS mmWave model. The analytical results provide insights on the effect of the system parameters on the secrecy performance.
- The impact of varying the power allocation between the message and AN signals on the secrecy performance is studied along with a numerical determination of the appropriate AN power fraction that maximizes the average achievable secrecy rate.

**Organization:** The rest of the paper is organized as follows: In Section 2, the system model is presented, including the network model, the mmWave models, and the eavesdroppers’ interception strategies. Analysis of the average achievable secrecy rate is the topic of Section 3. In Section 4, the Tx-AN technique is applied to enhance secrecy performance. Section 5 presents the numerical and simulation results, along with the discussion of the results. The paper is concluded in Section 6.

**Notations:** In this paper, bold lower-case letters $\mathbf{x}$ and bold upper-case letters $\mathbf{X}$ are used to denote vectors and matrices, respectively, $||\mathbf{x}||^2$ is the squared Euclidean norm of the vector $\mathbf{x}$, $\mathbf{I}_N$ denotes the identity matrix of a size $N$, $|\mathbf{A}|$ denotes the determinant of a matrix $\mathbf{A}$, and $[\mathbf{a}]^\dagger$ indicates $\max\{\mathbf{a}, 0\}$. The expectation of a random variable $\mathbf{x}$ is denoted by $\mathbb{E}[\mathbf{x}]$, the Laplace transform of $y$ is defined by $\mathbb{E}[e^{-\lambda \mathbf{y}}]$, $\mathcal{F}_1(a, b_1, b_2; \mathbf{c} \mid \mathbf{x}, y)$ is the Gauss hypergeometric function, $\mathcal{F}_1(a, b_1, b_2; \mathbf{c} \mid \mathbf{x}, y)$ denotes the Appell hypergeometric function of two variables $\mathbf{x}$ and $\mathbf{y}$, and the notations $T_r$, $R$, and $e$ respectively denote the transmitting node, the legitimate receiver, and the eavesdropper. In addition, the index “o” denotes the desired transmitter (Alice) and a number of transmitters (interferers) randomly distributed in the service area. The locations of the interferers are modeled as a homogeneous Poisson point process (PPP) $\Phi_B$ with intensity $\lambda_B$. Each transmitter has its corresponding receiver located at a fixed distance $r_e$. Based on Slivnyak’s theorem [34], Alice is assumed to be located at the origin, for convenience. Each transmitting node is assumed to transmit the message signal using a multi-array antenna, comprising $N_T$ single-array antennas where each single-array antenna provides a single directive beam. The total transmit power of all the $N_T$ array antennas is fixed at $P_T$. A single-array antenna is applied at Bob and at each receiver. A link is formed between each single-array antenna of a transmitting node and the single-array antenna of a receiving node. The CSI between each single-array antenna of a given transmitter and the single-array antenna of a receiver is assumed to be unknown so that the transmit power per single-array antenna will be $P_I = P_T/N_T$. The system also comprises a set of eavesdroppers whose locations are modeled by an independent homogeneous PPP $\Phi_e$ with intensity $\lambda_e$. Each eavesdropper employs a single-array antenna for the interception. Eavesdroppers are commonly assumed to possess strong processing capabilities and can collaborate with each other to cancel the interference [35, 36]. The assumed network topology is shown in Figure 1.

## 2  SYSTEM MODEL

### 2.1 Network model

An mmWave ad hoc network is considered in which the Tx-Rx pairs are characterized by the Poisson bipolar model [33]. In this model, the transmitting nodes comprise the desired transmitter (Alice) and a number of transmitters (interferers) randomly distributed in the service area. The locations of the interferers are modeled as a homogeneous Poisson point process (PPP) $\Phi_B$ with intensity $\lambda_B$. Each transmitter has its corresponding receiver located at a fixed distance $r_e$. Based on Slivnyak’s theorem [34], Alice is assumed to be located at the origin, for convenience. Each transmitting node is assumed to transmit the message signal using a multi-array antenna, comprising $N_T$ single-array antennas where each single-array antenna provides a single directive beam. The total transmit power of all the $N_T$ array antennas is fixed at $P_T$. A single-array antenna is applied at Bob and at each receiver. A link is formed between each single-array antenna of a transmitting node and the single-array antenna of a receiving node. The CSI between each single-array antenna of a given transmitter and the single-array antenna of a receiver is assumed to be unknown so that the transmit power per single-array antenna will be $P_I = P_T/N_T$. The system also comprises a set of eavesdroppers whose locations are modeled by an independent homogeneous PPP $\Phi_e$ with intensity $\lambda_e$. Each eavesdropper employs a single-array antenna for the interception. Eavesdroppers are commonly assumed to possess strong processing capabilities and can collaborate with each other to cancel the interference [35, 36]. The assumed network topology is shown in Figure 1.

#### 2.2 MmWave model

##### 2.2.1 Blockage and path loss models

For each link, the blockage model in [9] is adopted, where obstacles divide an incident mmWave signal path into two paths: LoS path and NLoS path with path loss exponent $\alpha_L$ and $\alpha_N$, respectively. The probability of a communication link being LoS is $\xi_L(r) = e^{-\alpha_L r}$, where $r$ is the path length and $\alpha_L$ is a constant that depends on the density of the buildings and their average width and length. By the fact that a link is either LoS or NLoS, $\xi_N(r) = 1 - \xi_L(r)$ is the probability of a communication link being NLoS. Then, the path loss at a distance $r$ from the transmitter can be expressed as [23, 37]

$$L(r) = \xi \left( \max(\xi, r) \right)^{-\alpha}, \quad \text{w.p. } \xi_L(r),$$

where $j \in [L, N]$, $\xi$ is the reference distance that makes the path loss model suitable at a small distance and at large intensity of the transmitters and eavesdroppers [38], and $\xi$ is the path loss intercept constant which depends on the operating frequency $f_r$, normally calculated by $(c/4\pi f_r)^2$ [23] where $c$ is the speed of light. Furthermore, based on the lowest mmWave path loss exponents, the commonly used mmWave operating frequencies are 28 GHz, 38 GHz, 60 GHz and 73 GHz [39, 40].

##### 2.2.2 Small-scale fading

For each link, the small-scale fading amplitude $b$ is modeled by Nakagami-$m$ random variable where the shape parameter $m$ is
represented by $m_L$ and $m_N$ for LoS and NLoS links, respectively [4]. Subsequently, the channel fading power gain is modeled as a gamma distributed random variable, $b^2 \sim \Gamma(m_j, 1/m_j)$ and $j \in \{L, N\}$. Note that the Rayleigh fading model is not suitable for the mmWave bands, especially when directional beamforming is applied. The reason is the absence of large amount of scattering at the mmWave bands, but which exists at the microwave bands [2, 41]. The independent Nakagami-$m$ fading is more general and analytically tractable, hence it is adopted in most of the recent studies on mmWave networks [20, 21, 41].

### TABLE 1

| Notation | Parameter       | Formula                                |
|----------|-----------------|----------------------------------------|
| $\tilde{\theta}$ | Beamwidth     | $2\pi / \sqrt{n}$                     |
| $G_M$    | Main-lobe gain  | $n$                                    |
| $G_\mu$  | Side-lobe gain  | $1 / (\sin^2(3\pi / 2\sqrt{n}))$      |

2.2.3 | Directional beamforming

To overcome the high propagation loss at the mmWave bands, all transmitting and receiving nodes including the eavesdroppers use directional beamforming. The sectored model is applied to analyze the beam pattern by using the uniform planar array (UPA) antenna for each array [42]. In this model, the beamwidth $\tilde{\theta}$, main-lobe gain $G_M$ and side-lobe gain $G_\mu$ are each a function of $n$, the number of antenna elements per single-array antenna, as shown in Table 1. Note that $n$ becomes $n_T$, $n_A$ and $n_e$, denoting the number of antenna elements per single-array antenna for message signal transmission, artificial noise signal transmission, and signal interception by an eavesdropper, respectively.
Recall the assumption of no prior knowledge of the CSI of the links between each Tx-Rx pair. Hence, the blind transmit and receive beamforming (TR-BF) discovery mechanism in [43] is utilized by each Tx-Rx pair to accurately determine the antenna direction with respect to each other. Subsequently, the maximum gain $G_i^c, G_j^c$ can be achieved between Alice and Bob while the effective antenna gain seen by Bob from each interferer $i \in \Phi_B$ can be written as [21]

$$G_i = \begin{cases} 
G_i^T G_i^R, & \text{w.p. } \beta_{MM} = \frac{\Theta (2\pi)^2}{(2\pi)^2}, \\
G_i^T G_i^R, & \text{w.p. } \beta_{M\mu} = \frac{\Theta (2\pi)^2}{(2\pi)^2}, \\
G_i^T G_i^R, & \text{w.p. } \beta_{\mu M} = \frac{(2\pi-\Theta)}{(2\pi)^2}, \\
G_i^T G_i^R, & \text{w.p. } \beta_{\mu\mu} = \frac{(2\pi-\Theta)(2\pi-\Theta)}{(2\pi)^2}, 
\end{cases} \quad (2)$$

where $\beta_{ilm} = \{M, \mu\}$ and $\mu \in \{M, \mu\}$ denotes the probability that the effective antenna gain $G_i^c, G_j^c$ occurs. Here, $\Theta$ and $\Theta$ are the beamwidth of the transmitting node and Bob, respectively.

Similarly, the effective antenna gain seen by each eavesdropper $e \in \Phi$, from Alice or interferer $i \in \Phi_B$ can be written as follows:

$$G_i = \begin{cases} 
G_i^T G_i^R, & \text{w.p. } \kappa_{MM} = \frac{\Theta (2\pi)^2}{(2\pi)^2}, \\
G_i^T G_j^R, & \text{w.p. } \kappa_{M\mu} = \frac{\Theta (2\pi)^2}{(2\pi)^2}, \\
G_i^T G_i^R, & \text{w.p. } \kappa_{\mu M} = \frac{(2\pi-\Theta)}{(2\pi)^2}, \\
G_i^T G_j^R, & \text{w.p. } \kappa_{\mu\mu} = \frac{(2\pi-\Theta)(2\pi-\Theta)}{(2\pi)^2}, 
\end{cases} \quad (3)$$

where $\kappa_{elm} = \{M, \mu\}$ and $\mu \in \{M, \mu\}$ denotes the probability that the effective antenna gain $G_i^c, G_j^c$ occurs, and $\Theta$ is the beamwidth of the eavesdropper $e \in \Phi_e$.

### 2.3 Simplified LoS MmWave model

The simplified LoS mmWave model is convenient to analyze the dense mmWave networks, where the density of the network topology is analogous to the blockage density. In this model, an equivalent LoS ball with fixed radius $R_{L}$ is used to simplify the LoS region [4, 44]. Subsequently, the step function is used to identify the probability of LoS communication link as follows:

$$\xi_{L}(r) = \begin{cases} 
1 & \text{for } r < R_{L}, \\
0 & \text{otherwise}. \quad (4)
\end{cases}$$

### 2.4 Passive eavesdroppers interception strategies

The passive eavesdropping attack is the most common attack against the wireless networks where no active eavesdropping actions are used to corrupt the received SNR at the desired receiver. In this work, two different passive eavesdroppers’ strategies are considered to intercept Alice’s message signal.

#### 2.4.1 Non-colluding eavesdroppers

In this strategy, one of the eavesdroppers in $\Phi$, intercepts Alice’s message signal independently based on different criteria, and without co-ordination with the other eavesdroppers in the network. In this paper, the eavesdropper (Eve) that has the smallest path loss to Alice is assumed to intercept Alice’s transmission because the path loss has a significant effect on the mmWave signal’s propagation. Recall from Section 2.2.1 that each link can be a LoS or NLoS path. Hence, by applying the thinning theorem [45], the eavesdroppers in $\Phi$ can then be divided into two independent PPPs: LoS eavesdroppers process $\Phi_L$ (i.e. eavesdroppers that have LoS link with Alice) and NLoS eavesdroppers process $\Phi_N$ (i.e. eavesdroppers that have NLoS link with Alice). Due to Eve being the eavesdropper with the smallest path loss to Alice, then Eve is either the nearest eavesdropper in $\Phi_L$ to Alice or the nearest one in $\Phi_N$ to Alice. The probability density function (pdf) of the distance between Alice and Eve given that Alice is intercepted by an LoS or NLoS eavesdropper in $\Phi_i$, $i \in \{L, N\}$ can be formulated as [4]

$$f_j(z) = \frac{T_j P_j(z)}{D_j} \exp \left( -2\pi \lambda, \int_{0}^{z} (1 - \xi_{j}(v)) dv \right), \quad z > 0, \quad (5)$$

where $j \in \{L, N\}$, $\Xi_{L} = z^{a_{L}} / a_{L}$, $\Xi_{N} = z^{a_{N}} / a_{N}$, $T_j = 1 \cdot \exp \left( -2\pi \lambda, \int_{0}^{\infty} \xi_{j}(v) dv \right)$ is the probability that Alice is intercepted by at least one eavesdropper in $\Phi_i$, $i \in \{L, N\}$, and $D_j$ is the probability that Alice is intercepted by an eavesdropper in $\Phi_i$, $i \in \{L, N\}$, given by [4]

$$D_j = T_j \int_{0}^{\infty} \exp \left( -2\pi \lambda, \int_{0}^{z} (1 - \xi_{j}(v)) dv \right) P_j(z) dz, \quad (6)$$

and $P_j(z)$ is the conditional pdf of the distance from the nearest eavesdropper in $\Phi_i$, $j \in \{L, N\}$ to Alice given that Alice is intercepted by at least one eavesdropper in $\Phi_i$, expressed as [4]

$$P_j(z) = 2\pi \lambda, z^{a_{j}} / a_{j} \exp \left( -2\pi \lambda, \int_{0}^{z} \xi_{j}(v) dv \right) / T_j, \quad z > 0. \quad (7)$$

The plot of (5) can be seen in Figures 2 and 3 for different values of the eavesdroppers’ intensity. The figures a a decrease in the mean value of $f_L(z)$ and $f_N(z)$ when the eavesdroppers’ intensity increases, meaning Eve becomes closer to Alice in the presence of dense eavesdroppers.

**Corollary 1.** Under the simplified LoS mmWave model, $f_j(z)$ can be approximated by

$$\tilde{f}_L(z) = z \exp \left( -2\pi \lambda, z^{a_{L}} / a_{L} \right), \quad z > 0. \quad (8)$$
Colluding eavesdroppers

The average achievable secrecy rate in the presence of colluding eavesdroppers can be calculated by [46]:

\[ C_S \triangleq \left[ C_R - C_E \right]^+, \]

where \( C_R \) and \( C_E \) are the average achievable rates at Bob and Eve, respectively, and \([g]^+ = \max\{g, 0\}\).

Firstly, the signal-to-interference-plus-noise ratio (SINR) at Bob \( E_{\text{R}} \) must be determined to compute its average achievable rate, \( C_{\text{R}} \). Aside from the useful signal obtained by Bob from Alice, it receives unwanted signals from interferers in \( \Phi_{\text{B}} \) and the sum is then also added to the thermal noise power, \( \sigma^2 \). Hence, the SINR received at Bob can be formulated as

\[ E_{\text{R}} = \frac{P_i |\mathbf{h}_i|^2 G^i M L(r_i)}{\sum_{j \in \Phi_{\text{B}}} P_i |\mathbf{h}_j|^2 G L(r_{j}) + \sigma^2}. \]

where \( \mathbf{h}_i = [h_{i1}, h_{i2}, \ldots, h_{iN_{\text{F}}}] \) is the \( 1 \times N_{\text{F}} \) vector of the independent Nakagami-\( m \) random variables with amplitude \( h_{i,k} \) for the link \( k \) between the transmitter antenna array \( i \) and receiver antenna array, where \( k = 1, 2, \ldots, N_{\text{F}} \). Clearly, \( |\mathbf{h}_i|^2 \) is an \( N_{\text{F}} \)-dimensional multivariate gamma distributed random variables, \( \mathbf{h}_{\text{R}} \) stands for the \( 1 \times N_{\text{F}} \) vector of independent Nakagami-\( m \) random variables between interferer \( i \in \Phi_{\text{B}} \) and Bob, and \( r_{\text{IR}} \) is the distance between interferer \( i \) and Bob.

Lemma 1. The average achievable rate at Bob is given by

\[ C_R = E[\log_2(1 + E_{\text{R}})], \]

\[ = \log_2(\tau) \int_0^\infty \frac{1}{x} \left(1 - \sum_{j \in \Phi_{\text{N}}} \xi_j(r_j)\right) \left(1 + \frac{x}{\tau} L(r_j)\right)^{-\tau} \Psi(x)e^{-x\sigma^2} \, dx, \]
where
\[
\Psi(x) = \sum_{j\in\{L,N\}} \exp \left( -2\pi\lambda_B \int_0^\infty \zeta_j(v) \right)
\times \left( 1 - \sum_{l,u\in\{M,M^,\}} \beta_{lu} (1 + \chi \varphi_j L(v)^{-\tau_j}) du \right).
\]
(12)

The function \(\Psi(x)\) denotes the Laplace transform of the aggregate interference at Bob, \(\tilde{\rho}_j = \frac{1}{m_j} P_t G^j L_0^j G^M_{iu} \), \(\rho_j = \frac{1}{m_j} P_t G^j L_0^j G^M_{iu} \), \(\tau_j = N_\gamma m_j \), and \(m_j\) is Nakagami fading shape parameter for the \(j\)th type of link, \(j \in \{L,N\}\).

Proof. See Appendix A.1.

Remark 1. From Lemma 1, the narrower the directive beams between Alice and Bob are, the higher the antenna gain and, hence, the higher the received message signal. In addition, low antenna gain at the interferers is achieved. The effect of high message received signal and low interference is high received SINR which, consequently, results in high average achievable rate at Bob. Further, increasing the interferers’ intensity \(\lambda_B\) leads to a reduction in \(\Psi(x)\) from (12) with a negative effect on the average achievable rate at Bob.

Remark 2. Lemma 1 involves two integrals one of which is inside the exponential function hence derivation of a closed-form expression for the average achievable rate is formidable and resort is made to numerical computation. An approximate result for \(C_R\) is obtained by using the simplified LoS mmWave model in (4).

Corollary 2. Under the simplified LoS mmWave model, \(C_R\) can be approximated by
\[
C_R \approx \log_2(1 + \xi_E) = \log_2(1 + \xi_E) \int_0^\infty \frac{1}{x} (1 - Y(x)) e^{-2\sigma^2 x} dx,
\]
(13)

where
\[
\tilde{\Psi}(x) = \exp \left( -2\pi\lambda_B \left[ \frac{R^2}{2} - \sum_{l,u\in\{M,M^,\}} \beta_{lu} \right]
\times \left( \frac{R^2}{2} \mathcal{F}_1 \left( \frac{\alpha_j}{\alpha_j L_j}; \frac{\alpha_j - 2}{\alpha_j}; -\chi \varphi_j \xi \tau_j \alpha_j \right)
\times \left( \frac{\alpha_j}{\alpha_j L_j}; \frac{\alpha_j - 2}{\alpha_j}; -\chi \varphi_j \xi \tau_j \alpha_j \right) \right) \right).
\]
(14)

Remark 3. Corollary 2 shows that the approximate average achievable rate at Bob is impacted by the LoS parameters such as the LoS path loss exponent \(\alpha_L\), LoS Nakagami fading shape parameter \(m_L\), and LoS ball radius \(R_L\). As seen in (14), \(\tilde{\Psi}(x)\) is a decreasing function of \(R_L\), which produces a reduction in the approximate average rate at Bob in (13), since larger LoS region results in higher interference.

Remark 4. The approximate result is still not in a closed form. But the numerical calculation is simpler because it involves only one integral and the integral inside the exponential function no longer exists.

As a prelude to calculating \(C_E\), the average achievable rate at Eve, first the SNR at Eve \(\xi_E\) is determined as:
\[
\xi_E = \frac{P_t ||h_E||^2 G_L(r_E)}{\sigma_k^2},
\]
(15)

where \(h_E\) is the \(1 \times N_\gamma\) vector of independent Nakagami-\(m\) random variables between Alice and Eve, \(r_E\) is the distance between Alice and Eve, and \(\sigma_k^2\) is the thermal noise power at Eve.

Lemma 2. The average achievable rate at Eve can be determined as
\[
C_E = \mathbb{E} [\log_2(1 + \xi_E)] = \log_2(1 + \xi_E) \int_0^\infty \frac{1}{x} (1 - Y(x)) e^{-2\sigma^2 x} dx,
\]
(16)

where
\[
Y(x) = \sum_{j\in\{L,N\}} D_j
\times \sum_{l,u\in\{M,M^,\}} \chi \varphi_j \xi \int_0^\infty (1 + \chi \varphi_j L(v)^{-\tau_j} f_j(v)) dv.
\]
(17)

The function \(Y(x)\) is the Laplace transform of the intercepted message signal by Eve and \(\varphi_j = \frac{1}{m_j} P_t G^j L_0^j G^M_{iu}\).

Proof. See Appendix A.2.

Remark 5. Based on Figures 2 and 3, an increase in \(\lambda\), produces a decrease in the mean value of \(j_f(v)\) resulting in a reduction in \(Y(x)\) from (17), which increases the average achievable rate at Eve according to (16).

Corollary 3. Based on the simplified LoS mmWave model, \(C_E\) simplifies to:
\[
C_E \approx \log_2(1 + \xi_E) \int_0^\infty \frac{1}{x} (1 - \tilde{Y}(x)) e^{-2\sigma^2 x} dx,
\]
(18)

where
\[
\tilde{Y}(x) = \sum_{l,u\in\{M,M^,\}} \chi \varphi_j \xi \int_0^\infty (1 + \chi \varphi_j L(v)^{-\tau_j} f_L(v)) dv.
\]
(19)
Remark 6. From (19), the approximate average achievable rate at Eve is only affected by the LoS links between Alice and the eavesdroppers in $\Phi_e$ due to $D_L = 1$, while the NLoS links can be neglected (i.e. $D_N = 0$). Moreover, when $\lambda_e$ increases, the mean value of $f_r(e)$ decreases resulting in higher achievable rate.

Finally, by substituting (11) and (16) in (9), the exact average achievable secrecy rate of an mmWave ad hoc network with message transmission via a multi-array antenna in the presence of non-colluding eavesdroppers can be determined. Moreover, by substituting (13) and (18) in (9), the approximate average achievable secrecy rate is obtained.

### 3.2 Colluding eavesdroppers

Unlike the previous section on non-colluding eavesdroppers where only one eavesdropper Eve with the smallest path loss to Alice is assumed to intercept Alice’s signal, in this section all the eavesdroppers in $\Phi_e$ can intercept Alice’s signal and transmit the intercepted signal along with their background noise $\sigma_e^2$ to the Main-Eve where the signals are combined. However, the average achievable rate at Bob $C_{PB}$ remains the same as (11) in Lemma 1, because only the eavesdroppers’ interception strategy has changed. Therefore, the SNRs collected at the Main-Eve will be

$$\xi_e = \sum_{r \in \Phi_e} P_j |h_{ej}|^2 G_{L}(r_e) \sigma_e^2,$$

where $h_{ej}$ is the $1 \times N_T$ vector of independent Nakagami-$m$ random variables between Alice and the eavesdropper $e \in \Phi_e$, and $r_e$ is the distance between Alice and the eavesdropper $e$.

**Lemma 3.** The average achievable rate at the Main-Eve can be calculated by:

$$C_{E} = E[\log_2(1 + \xi_e)] = \log_2(e) \int_0^\infty \frac{1}{x} (1 - Y^e(x)) e^{-\alpha x^2} dx,$$

where

$$Y^e(x) = \sum_{j \in [L,N]} \exp\left( -2\pi \lambda_e \int_0^\infty \xi_j(v) \right) \times \left( 1 - \frac{\kappa_l(1 + \Phi L(x))^0}{\alpha_l} \right)^0, \ (22)$$

where $Y^e(x)$ is the Laplace transform of the combined message signal at the Main-Eve.

**Proof.** The proof follows the same manner as done to obtain (12) in Lemma 1. Hence, the proof is omitted here. \qed

**Remark 7.** In the case of colluding eavesdroppers, there exists a significant effect of the eavesdroppers’ intensity on the average achievable rate at the Main-Eve because $Y^e(x)$ is a decreasing function of $\lambda_e$, as shown in (22) thus increasing $C_{E}$, based on (21).

**Corollary 4.** The average achievable rate at the Main-Eve in Lemma 3 can be determined by applying the simplified LoS mmWave model. In this case, $C_{E}$ becomes:

$$C_{E} \approx \log_2(e) \int_0^\infty \frac{1}{x} (1 - \hat{Y}^e(x)) e^{-\alpha x^2} dx,$$

where

$$\hat{Y}^e(x) = \exp\left( -2\pi \lambda_e \left[ \frac{R^2_e}{2} - \sum_{l, e \in [M, \mu]} \kappa_{le} \right. \right. \times \left. \left. \left( \frac{R^2_e}{2} - \tau_l \right)^2 \alpha_{le} \left( \frac{2 - \alpha_{le}}{\alpha_{le}} \right) \right) \! \! \left( -\kappa_{le} \epsilon R^2_e \! \! \right) \! \! \left( -\kappa_{le} \epsilon R^2_e \! \! \right) \right). \ (24)$$

**Remark 8.** The approximate achievable rate at the Main-Eve is still impacted by the eavesdroppers’ intensity, as seen in (24). However, based on the simplified LoS mmWave model, an eavesdropper affects the average achievable rate at the Main-Eve if and only if its distance from Alice is less than the LoS radius $R_L$. Otherwise, the eavesdropper lies inside the NLoS region and its impact can be neglected.

Now, the average achievable secrecy rate in the presence of colluding eavesdroppers can be calculated as

$$C_{S} = \left[ C_{R} - C_{E} \right]^+. \ (25)$$

Substituting (11) and (21) in (25), the exact average achievable secrecy rate of an mmWave ad hoc network with message transmission via a multi-array antenna in the presence of colluding eavesdroppers can be determined. Similarly, the approximate average achievable secrecy rate can be obtained by substituting (13) and (23) in (25).

**Remark 9.** The exact average achievable secrecy rate (based on LoS and NLoS mmWave model) and the approximate average achievable secrecy rate (based on LoS mmWave model) are close to each other, regardless of whether the eavesdroppers are colluding or non-colluding. The reason is that the received signal from the NLoS paths is small compared to that from the LoS paths so that received signal based on the composite LoS and NLoS mmWave model is approximately the same as the received signal based on the LoS model.
In this section, the effect of adding AN into the transmission on the average achievable secrecy rate is analyzed. The purpose of an AN transmission is to reduce the illegitimate channels’ capacity between the eavesdroppers and Alice and thus attain a reasonable secrecy performance, even if the eavesdroppers have a better channel than that seen by Bob [47]. Consequently, AN transmission via a multi-array antenna at the transmitting nodes, referred to as Tx-AN technique in this paper, is used to enhance the average achievable secrecy rate of an mmWave ad hoc network in the presence of non-colluding and colluding eavesdroppers. In this technique, the total transmit power is divided into message signal transmit power $P_T^d = (1 - \eta)P_T$ and AN signal transmit power $P_T^a = \eta P_T$ assigned for message signal and AN signal transmission, respectively, where $\eta$ is the AN power fraction. Moreover, the total transmit array antenna $N_T$ is split into the message signal transmit array antennas and AN signal transmit array antennas denoted by $N_x$ and $N_a$, respectively, where $N_T = N_x + N_a$. Furthermore, the main lobe beam of the AN array antenna of each transmitting node is not directed to its corresponding receiver to ensure that each legitimate receiver never receives the transmitted AN from its intended transmitter. The implementation of the Tx-AN technique in an mmWave ad hoc network in the presence of eavesdroppers is Figure 4.

Although the Tx-AN technique is simple and easy to implement practically as illustrated above, it exhibits a significant improvement in the average achievable secrecy rate in the presence of non-colluding and colluding eavesdroppers. Recall that the Tx-AN technique does not require the knowledge of the CSI between Alice and Bob, and neither the knowledge of the CSI between Alice and the eavesdroppers.
4.1 With Tx-AN technique in the presence of non-colluding eavesdroppers

With the Tx-AN technique, the average achievable secrecy rate of an mmWave ad hoc network in the presence of non-colluding eavesdroppers can be calculated as

$$\hat{C}_S \triangleq \left[ \hat{C}_R - \hat{C}_E \right]^+,$$  \hspace{1cm} (26)

where $\hat{C}_R$ and $\hat{C}_E$ are the average achievable rates at Bob and Eve, respectively, with the Tx-AN technique implemented at each transmitter.

First, the SINR at Bob $\hat{C}_R$ must be characterized assuming the Tx-AN technique is implemented at each transmitter to obtain $\hat{C}_R$. Alice and each interferer transmit message signal at power $P_i^M = P_i^M / N_i$ per array, main lobe gain $G_M^j$ with beamwidth $\phi$, and side lobe gain $G_S^j$. Additionally, Alice and each interferer transmit AN signals at power $P_i^A = P_i^A / N_i$ per array, main lobe gain $G_M^A$ with beamwidth $\phi$, and side lobe gain $G_S^A$. As noted earlier, the AN of a transmitter is not directed to its corresponding receiver so that Bob never receives the AN signal transmitted by Alice [48]. Hence, the SINR at Bob can be calculated:

$$\hat{C}_R = \frac{P_i^M \| h_i \|^2 G_M^j G_M^R L(r_i) - \sum_{j \in \Phi_B \setminus \{i\}} P_i^M \| h_i \|^2 G_M^j G_M^R L(r_i) + \sigma^2}{\sum_{j \in \Phi_B \setminus \{i\}} P_i^M \| h_i \|^2 G_M^j G_M^R L(r_i) + \sigma^2},$$  \hspace{1cm} (27)

where $h_i^R$ and $h_i^A$ are the $1 \times N_i$ and $1 \times N_i$ vectors of independent Nakagami-$m$ random variables of the message signal and AN signal channels, respectively, between interferer $i \in \Phi_B$ and Bob. Here, $G_M^j$ and $G_M^A$ are the effective gains of the message and AN array antennas, respectively, seen by Bob from the transmitting interferer $i$. However, Bob cannot simultaneously receive the main lobe of the interference and the main lobe of the AN signals which are transmitted by the same interferer $i \in \Phi_B$. The reason is that the main lobe of the interference and that of the AN signals are always pointing in a different direction by design. In other words, these two events are mutually exclusive with probability $\Pr(\{G_M^j \cap G_M^A\}) = 0$. Hence, the total effective antenna gain $\hat{C}_S = G_M^j + G_M^A$ seen by Bob from the interferer $i \in \Phi_B$ can be written as follows:

$$\hat{C}_S = \left\{ \begin{array}{ll}
G_M^j + G_M^A, & \text{w.p. } \delta_{M,MM} = \frac{\phi \pi}{(2\pi)^2}, \\
G_M^j + G_M^A, & \text{w.p. } \delta_{MM,MM} = \frac{\phi \pi (2\pi - \phi)}{(2\pi)^2}, \\
G_M^j + G_M^A, & \text{w.p. } \delta_{MM,MM} = \frac{\phi \pi (2\pi - \phi)}{(2\pi)^2}, \\
G_M^j + G_M^A, & \text{w.p. } \delta_{MM,MM} = \frac{\phi \pi (2\pi - \phi)}{(2\pi)^2}, \\
G_M^j + G_M^A, & \text{w.p. } \delta_{MM,MM} = \frac{\phi \pi (2\pi - \phi)}{(2\pi)^2}, \\
\end{array} \right. $$ \hspace{1cm} (28)

where $\delta_{M,MM}$, $\delta_{MM,MM}$, and $\delta_{MM,MM}$ denote the probability that the effective antenna gains $G_M^j G_M^R$ and $G_M^A G_M^R$ occur simultaneously.

**Lemma 4.** The exact average achievable rate at Bob when the Tx-AN technique is implemented at the transmitters, $\hat{C}_R$, can be determined by

$$\hat{C}_R = \mathbb{E}[\log_2(1 + \hat{C}_R)] = \log_2(e) \int_0^\infty \frac{1}{\lambda} \left( 1 - \sum_{j \in \{l, N\}} \xi_j(r_j) \right) \left( 1 + \exp(-\hat{C}_R) \right) \psi(x) e^{-\lambda x} dx,$$  \hspace{1cm} (29)

where

$$\psi(x) = \sum_{j \in \{l, N\}} \exp\left( -2\pi \lambda B \int_0^\infty \xi_j(r_j) \left( 1 - \sum_{l \in \Omega} \delta_{M,MM} \right) \left( 1 + x \rho_j^L \right)^{-1/j} \right) \rho_j^L(x) e^{-\lambda L x} dx,$$  \hspace{1cm} (30)

The function $\psi(x)$ denotes the Laplace transform of the interference plus AN signals at Bob, $\rho_j^L = \frac{1}{m_j} P_i^M G_M^j G_M^R$, $\rho_j^A = \frac{1}{m_j} P_i^M G_M^A G_M^R$, $\rho_j^A = \frac{1}{m_j} P_i^A G_M^j G_M^R$, $\rho_j^A = \frac{1}{m_j} P_i^A G_M^A G_M^R$, and the set of all possible values of $(l, n, q)$.

**Proof.** See Appendix A.3.

**Remark 10.** With the Tx-AN technique, the average achievable rate at Bob increases as the power fraction $\eta$ increases. Besides, the width of the directive beams for the message and AN signals, which affects directly the values of $\rho_j^L$ and $\rho_j^A$, dominates also the average achievable rate. The directivity of the transmit and receive beams can be designed based on the number of antenna elements per array, as seen in Table 1.

**Corollary 5.** When a simplified LoS mmWave model is used, the results in Lemma 4 can be approximated as follows:

$$\hat{C}_R = \log_2(e) \int_0^\infty \frac{1}{\lambda} \left( 1 - \left( 1 + x \hat{C}_R \right)^{-1/j} \right) \hat{\psi}(x) e^{-\lambda x} dx,$$  \hspace{1cm} (31)

where

$$\hat{\psi} = \exp\left( -2\pi \lambda B \left[ \frac{R^2_L}{2} - \sum_{l, n \in \{M, \mu\}} \delta_{M,MM} \left( \frac{R^2_L}{2} \right) \right] F_1 \left( \frac{2}{\alpha_L}, \frac{2}{\alpha_L}, \frac{2}{\alpha_L}; \frac{2}{\alpha_L}, \frac{2}{\alpha_L}; -\infty \rho_j^L \alpha L \right) - \frac{\ell^2}{2} \right) F_1 \left( \frac{2}{\alpha_L}, \frac{2}{\alpha_L}, \frac{2}{\alpha_L}; \frac{2}{\alpha_L}, \frac{2}{\alpha_L}; -\infty \rho_j^L \ell \alpha L \right).$$  \hspace{1cm} (32)
Next, with the Tx-AN technique, the received SNR at Eve becomes the received signal-to-AN-ratio, SANC, denoted by $\hat{\xi}_E$ calculated as

$$
\hat{\xi}_E = \frac{P_j^{|\mathbf{h}_E|^2}G^j_{\mu}L(r_E)}{I_{IE} + I_{IE} + \sigma^2_n},
$$

(33)

where $I_{IE} = P_j^{|\mathbf{h}_E|^2}G^j_{\mu}L(r_E)$ is the received AN power at Eve from Alice and $I_{IE} = \sum_{l \in \Phi_B}P_j^{|\mathbf{h}_E|^2}G^j_{\mu}L(r_E)$ is the received AN at Eve from the interferers in $\Phi_B$. Here, $\mathbf{h}_E$ and $\mathbf{h}_E$ are the $1 \times N_I$ and $1 \times N_A$ vectors of independent Nakagami-\(m\) random variables of the message signal and AN signal channels, respectively, between Alice and Eve. $\mathbf{h}_E$ is the $1 \times N_A$ vector of independent Nakagami-\(m\) random variables of the AN signal channel between the interferer $i \in \Phi_B$ and Eve. $G_{\mu}^j$ is the effective antenna gain seen by Eve from interferer $i \in \Phi_B$ which can be obtained from (3) by replacing $G_{M}^j$, $G_{A}^j$, and $\phi$ with $G_{M}^j$, $G_{A}^j$, and $\phi$, respectively, with probability $\omega_{lu,lu,\mu} \in \{ M, \mu \}$ that the effective antenna gain $G_{\mu}^j$ occurs. Here, $G_{E}^j$ and $G_{A}^j$ are respectively the message and AN effective antenna gains seen by Eve from Alice. Recall that for each transmitter, the main lobe of the AN array and message array are pointing in different directions. Hence, Eve cannot receive simultaneously the main lobe of the message and AN signals, that is, $P(G_{A}^j \cap G_{M}^j) = 0$. The total effective antenna gain $\tilde{G}_E = G_{E}^j + G_{A}^j$ seen by Eve from Alice can be written as follows:

$$
\tilde{G}_E = \left\{ \begin{array}{ll}
G_{M}^j + G_{\mu}^j & \text{w.p.} \quad \gamma_{M,\mu,\mu} = \frac{\phi}{(2\pi)^2}, \\
G_{M}^j + G_{\mu}^j & \text{w.p.} \quad \gamma_{M,\mu} = \frac{\phi (2\pi - \phi)}{(2\pi)^2}, \\
G_{\mu}^j + G_{M}^j & \text{w.p.} \quad \gamma_{M,\mu} = \frac{\phi (2\pi - \phi)}{(2\pi)^2}, \\
G_{\mu}^j + G_{\mu}^j & \text{w.p.} \quad \gamma_{M,\mu} = \frac{\phi (2\pi - \phi)}{(2\pi)^2}, \\
G_{\mu}^j + G_{\mu}^j & \text{w.p.} \quad \gamma_{M,\mu} = \frac{\phi (2\pi - \phi)}{(2\pi)^2}, \\
G_{\mu}^j + G_{\mu}^j & \text{w.p.} \quad \gamma_{M,\mu} = \frac{\phi (2\pi - \phi)}{(2\pi)^2}, \\
\end{array} \right.
$$

(34)

where $\gamma_{\mu,\mu} \in \{ \mu, \mu \}$ denotes the probability that the effective antenna gains $G_{\mu}^j G_{\mu}$ and $G_{\mu}^j G_{\mu}$ occur simultaneously.

**Lemma 5.** The exact average achievable rate at Eve with the Tx-AN technique implemented at Alice and all the interferers can be calculated by

$$
\hat{C}_E = \log_2(e) \int_0^\infty \frac{1}{\lambda_E} \left( u_1(\lambda_E) - u_2(\lambda_E) \right) v_3(\lambda_E) e^{-\lambda_E} d\lambda_E,
$$

(35)

where

$$
u_1(\lambda) = \sum_{j \in \{L, N\}} D_j
$$

$$\times \sum_{l, u \in \{M, \mu\}} \omega_{lu} \int_0^\infty \left( 1 + x \varphi^{\lambda} \right)^{-\lambda} f_j(x) dx,
$$

(36)

$$
u_2(\lambda) = \sum_{j \in \{L, N\}} D_j \int_0^\infty \sum_{l, u \in \{M, \mu\}} \gamma_{\mu,\mu} \left( 1 + x \varphi^{\lambda} \right)^{-\lambda} f_j(x) dx,
$$

(37)

$$
u_3(\lambda) = \sum_{j \in \{L, N\}} \exp \left( -2\pi \lambda_E \int_0^\infty \zeta_j(x) \left( 1 - \sum_{l, u \in \{M, \mu\}} \omega_{lu} \right) \left( 1 + x \varphi^{\lambda} \right)^{-\lambda} f_j(x) dx \right).$$

(38)

The functions $u_1(\lambda), u_2(\lambda)$, and $u_3(\lambda)$ are the Laplace transform of the received AN signal at Eve from Alice, the received message plus AN signals at Eve from Alice, and the received AN signal at Eve from the interferers in $\Phi_B$, respectively, $\varphi_j = \frac{1}{m_j} P_j G_{\mu} \varphi_{\mu}$, $\varphi_j = \frac{1}{m_j} P_j G_{\mu} \varphi_{\mu}$, $\varphi^{\lambda} = \frac{1}{m_j} P_j G_{\mu} \varphi_{\mu}$, $D_j$ is given by (6), and $m_j$ is Nakagami fading shape parameter for the $j^{th}$ type of link, $j \in \{L, N\}$.

**Proof.** See Appendix A.4.

**Remark 11.** From Remark 5, an increase in the eavesdroppers’ intensity results in an increased achievable rate at Eve. However, with the Tx-AN technique implemented at the transmitting nodes, the average achievable rate at Eve exhibits a small increase as $\lambda_E$ increases. Recall that an increase in $\lambda_E$ decreases the mean value of $f_j(x)$, as seen in Figs. 2 and 3. The reason is that the increase of $\lambda_E$ affects both $u_1(\lambda)$ and $v_2(\lambda)$ simultaneously, as seen in (36) and (37). Therefore, the increase of $\lambda_E$ has a small impact on the average achievable rate at Eve from (35). Moreover, a dense network with high interferers’ intensity reduces the value of $u_1(\lambda)$, as shown in (38), which decreases the average achievable rate at Eve.

Substituting (29) and (35) in (26), the exact average achievable secrecy rate of an mmWave ad hoc network with the Tx-AN technique implemented at the transmitters in the presence of non-colluding eavesdroppers can be determined. Note that (26) is solved numerically as done in (9) and (25).

**Remark 12.** A special case may occur when Eve is very close to Bob or Eve is at the same angle as Bob. This special case, albeit occurring with small probability, creates a problem in that the eavesdropper will not receive the AN, and hence the benefit of AN in enhancing the secrecy performance cannot be realized.

**Corollary 6.** The expressions in (36) and (37) can be simplified in the same manner as done to obtain (19) in Corollary 3. Also, (38) can be approximated similarly as done to obtain (14) in Corollary 2. Therefore, the approximate average achievable rate at Eve can be determined.
Remark 13. The approximate average achievable rate at Eve is based on the nearest LoS eavesdroppers (i.e. \(f_j(v)\)) compared to the exact average achievable rate which relies on \(f_j(v), j \in \{L, N\}\), as seen in (36) and (37). Moreover, Eve receives AN signals only from the LoS interferers in \(\Phi_B\) which has a better effect on the approximate average achievable rate.

4.2 With Tx-AN technique in the presence of colluding eavesdroppers

The exact average achievable secrecy rate of mmWave ad hoc network with the Tx-AN technique in the presence of colluding eavesdroppers can be calculated as

\[
\hat{C}_S^E \triangleq \left[\hat{C}_R^E - \hat{C}_E^E\right]^+, \tag{39}
\]

where \(\hat{C}_R^E\) and \(\hat{C}_E^E\) are the average achievable rates at Bob and the Main-Eve, respectively, with applying the Tx-AN technique.

To simplify the analysis in this section, the Tx-AN technique is implemented by Alice only. Hence, the SINR at Bob can be calculated as

\[
\hat{\xi}_R = \frac{P_1^a \|h_{M}^c\|^2 G_{M}^{R} L(r_{B})}{\sum_{\nu \in \Phi_B^c} P_1 \|h_{\nu}^c\|^2 G_{\nu}^{R} L(r_{B}) + \sigma^2}, \tag{40}
\]

Recall that the AN transmitted by Alice is not received by Bob. Subsequently, \(\hat{C}_R^E\) can be obtained by

\[
\hat{C}_R^E = \mathbb{E}[\log_2 (1 + \hat{\xi}_R)],
\]

\[
= \log_2 (e) \int_0^{\infty} \frac{1}{x} \left(1 - \sum_{j \in [L,N]} \xi_j (r_B)\right) \times \left(1 + \chi \xi_j (r_B) \right)^{-\tau_j} \Psi(x) e^{-x \sigma^2} dx, \tag{41}
\]

where \(\Psi(x)\) is the Laplace transform of the aggregate interference at Bob which is determined in (12). However, based on the eavesdroppers’ intercepted message signals, AN signals and the background noise \(\sigma_j^2\), the SANR at the Main-Eve can be calculated by

\[
\hat{\xi}_E = \sum_{\nu \in \Phi} P_1^a \|h_{\nu}^c\|^2 G_{\nu}^{R} L(r_{E}) + \sigma_j^2, \tag{42}
\]

where \(h_{\nu}^c\) and \(h_{\nu}^m\) are the \(1 \times N_3\) and \(1 \times N_3\) vectors of independent Nakagami-\(m\) random variables of the message and AN signal channels, respectively, between Alice and eavesdropper \(\nu \in \Phi_v\).

**Lemma 6.** The exact average achievable rate at the Main-Eve when the Tx-AN technique is implemented by Alice is given by:

\[
\hat{C}_E^E = \mathbb{E}[\log_2 (1 + \hat{\xi}_E)],
\]

\[
= \log_2 (e) \int_0^{\infty} \frac{1}{x} \left(\psi_1 (x) - \psi_2 (x)\right) e^{-x \sigma^2} dx, \tag{43}
\]

where

\[
\psi_1 (x) = \sum_{j \in [L,N]} \exp \left(-2 \pi \lambda_j \int_0^{\infty} \xi_j (r) \right) \times \left(1 - \sum_{l_a \in [M]} \frac{\omega_{l_a} (1 + \chi \xi_j (r) \right)^{-\tau_j} \vartheta (l_a) e^{-x \sigma^2} dx, \tag{44}
\]

\[
\psi_2 (x) = \sum_{j \in [L,N]} \exp \left(-2 \pi \lambda_j \int_0^{\infty} \xi_j (r) \left(1 - \sum_{l_a \in [M]} \vartheta (l_a) (1 + \chi \xi_j (r) \right)^{-\tau_j} \vartheta (l_a) e^{-x \sigma^2} dx, \tag{45}
\]

The functions \(\psi_1 (x)\) and \(\psi_2 (x)\) are the Laplace transform of the received AN signal (from Alice) and the received message plus AN signal at the eavesdroppers in \(\Phi_v\), respectively.

**Proof.** The proof of (44) and (45) follows the same manner as was done to obtain (12) in Lemma 1 and (30) in Lemma 4, respectively.

Remark 14. In general, when the intensity of the colluding eavesdroppers increases, the average achievable rate at the Main-Eve increases, as seen in Remark 5. However, from (44) and (45), the increase of \(\lambda_j\) decreases \(\psi_1 (x)\) and \(\psi_2 (x)\) simultaneously that results in a small effect, as seen in (43). Consequently, the increase in \(\lambda_j\) has a negligible effect on the average achievable rate at the Main-Eve under the Tx-AN technique. This manifests the secrecy robustness of the Tx-AN technique against the most dangerous eavesdropping scenario (i.e. colluding eavesdropping).

Finally, substituting (41) and (43) in (39), the exact average achievable secrecy rate of an mmWave ad hoc network with the Tx-AN technique implemented only by Alice in the presence of colluding eavesdroppers can be determined.

**Corollary 7.** Applying the simplified LoS mmWave model, (44) and (45) are approximated in the same manner as used to determine (14) in Corollary 2 and (32) in Corollary 5, respectively. Subsequently, the approximated average achievable rate at the Main-Eve can be obtained.

**Remark 15.** The approximate average achievable rate at the Main-Eve is close to the exact average achievable rate due to neglecting the NLoS eavesdropper which has a small impact on the SANR collected at the Main-Eve.
TABLE 2  Summary of values of system parameters

| Parameter | Value |
|-----------|-------|
| $f_c$, $\sigma^2$, $\alpha_L$, $\alpha_N$, $\eta$ | 73 GHz, $-71$ dBm, 2.1, 3.4, 0.25 [39] |
| $m_L$, $m_N$, $\epsilon$, $\tau_0$, $\varpi$ | 3, 2, 1 m, 15 m, 1/141.4 m$^{-1}$ [4] |
| $\lambda_B$, $\lambda_E$, $N_B$, $N_A$ | 50/km$^2$, 50/km$^2$, 3, 3 arrays [21] |
| $R_L$, $\sigma_L$, $\sigma_N$, $\Lambda$ | 200 m, 16, 16, 16 elements per array [42] |

5  NUMERICAL RESULTS AND DISCUSSION

The usefulness of the analytical results derived in Section 3 and Section 4 is demonstrated in this section. The analytical results are computed numerically using the Mathematica tool [49], and are validated by Monte Carlo simulations with 10,000 iterations. Unless otherwise stated, the assumed parameter values are provided in Table 2 and are referenced from [4, 21, 39, 42].

Figure 5 plots the average achievable secrecy rate for an mmWave ad hoc network in the presence of non-colluding and colluding eavesdroppers versus the total transmit power. Initially when the total transmit power increases from 5 to 20 dBm, it is seen from Figure 5 that the average achievable secrecy rate increases because the mmWave network tends to be noise-limited. Conversely, when the total transmit power increases beyond 20 dBm, the average achievable secrecy rate curve deteriorates with increasing total transmit power due to the network becoming interference-limited. Figure 6 studies the impact of eavesdroppers’ intensity on the average achievable secrecy rate, when the mmWave ad hoc network is interference limited at a total transmit power of 30 dBm. Figure 6 reveals that the increase in $\lambda$ produces improvement in the received message signal at the eavesdroppers that decreases the average achievable secrecy rate according to (9) and (25). In both Figures 5 and 6, the average achievable secrecy rate in the presence of colluding eavesdroppers is worse than that of non-colluding eavesdroppers, as expected. Similarly, the average achievable secrecy rate at a low interferers’ intensity $\lambda_B = 0.00005$/km$^2$ is better than that at high intensity $\lambda_B = 0.0001$/km$^2$.

Figure 7 plots the average achievable secrecy rate with and without Tx-AN technique ($\lambda_B = 0.00005$/km$^2$) with and without Tx-AN technique versus the total transmit power in the presence of colluding eavesdroppers for different $n_A$, the number of antenna elements per antenna array for AN transmission. It is observed that the average achievable secrecy rate is improved by using the Tx-AN technique at high total transmit...
power ($> 20$ dBm) because the mmWave ad hoc network tends to be interference limited. The Tx-AN increases the AN of the interferers at the eavesdroppers thus decreasing the achievable rate thereby providing improved average achievable secrecy rate. For example, the results show that using the Tx-AN technique with a total transmit power of $35$ dBm and $n_A = 16$ achieves a $53\%$ improvement in the average achievable secrecy rate when the Tx-AN technique is not utilized. Furthermore, this percentage improvement can be increased by increasing both $P_T$ and $n_A$. Also from Figure 7, applying the AN at low transmit power shows negligible improvement because the mmWave ad hoc network tends to be noise limited. Consequently, the AN transmit power which is subtracted from the total power is not effective and the message transmit power is reduced at the same time. Figure 7 further shows that better average achievable secrecy rate is achieved with increasing $n_A$ due to the higher AN main lobe gain attained based on the direct proportionality between the main lobe gain and number of antenna elements, as shown in Table 1. Figure 8 studies the achieved secrecy performance when a small number of antenna elements per antenna array is used. The figure proves that the Tx-AN technique still works for the smaller number of antenna elements per antenna array. Further, Figures 7 and 8 show a slight decrease in the secrecy performance at high total transmit power when the Tx-AN technique is used. The reason is that high total transmit power results in high interference signal and high AN signal in the network, which leads to a slight degradation in the SINR at Bob (recall that the eavesdroppers only can cancel the interference signal).

Figure 9 presents the effects of changing the eavesdroppers’ intensity on the average achievable secrecy rate with and without Tx-AN technique in the presence of non-colluding and colluding eavesdroppers at $P_T = 30$ dBm and $\lambda_e = 0.00005$ km$^{-2}$. The figure shows the average achievable secrecy rate decreases with increasing $\lambda_e$. The degradation happens due to the increase in the received interference signal at Bob. The combined effect of the interferers’ and eavesdroppers’ intensities on the average achievable secrecy rate is shown in Figure 12. The figure shows the average achievable secrecy rate decreases when both the interferers’ intensity and eavesdroppers’ intensity increase. Nevertheless, the average achievable secrecy rate with the Tx-AN technique is still higher than that obtained when the Tx-AN technique is not used.

Finally, Figure 13 shows the optimal value of AN power fraction, denoted by $\eta^*$, which maximizes the average achievable secrecy rate as a function of the total transmit power for an mmWave ad hoc network with the Tx-AN technique in the presence of non-colluding and colluding eavesdroppers. It is seen from Figure 13 that the value of $\eta^*$ increases with increasing total transmit power $P_T$. The reason is that the eavesdroppers receive increasing message.
signal power with increasing value of $P_T$. Now, increasing the value of $\eta^*$ is the counter-action for increasing the AN signal power at the eavesdroppers to maximize the average achievable secrecy rate. However, the curves are saturated at $\eta^* \geq 0.5$ because the AN signal power becomes greater than the message signal power, which has a negative impact on the average achievable secrecy rate. Further, if there is power control when the value of $P_T$ is dynamic, then it follows that the power allocation fraction must also be adaptive to $P_T$, to achieve improved secrecy performance.

6 | CONCLUSION

In this paper, the analysis of the average achievable secrecy rate in an mmWave ad hoc network with multi-array antenna transmission in the presence of non-colluding and colluding eavesdroppers is presented, taking into consideration the blockages, directional beamforming, and Nakagami-$m$ fading. Moreover, the analysis demonstrates the reduction in the average achievable secrecy rate due to increasing the intensities of the transmitting nodes and eavesdroppers. Furthermore, it is recommended to use the Tx-AN technique to improve the average achievable secrecy rate in an interference-limited mmWave ad hoc network. Besides, the Tx-AN technique shows high secrecy robustness of the average achievable rate against the eavesdroppers’ intensity. However, without the Tx-AN technique, the average achievable secrecy rate faces a fast deterioration with increasing intensity of the eavesdroppers. Finally, based on the system model parameters, the appropriate AN power fraction should be chosen to maximize the average secrecy rate. In the future, this work can be extended to mmWave ad hoc networks with multi-array antenna transmission and reception.
**FIGURE 12** Average achievable secrecy rate versus $\lambda_B$ and $\lambda_e$ with and without Tx-AN technique ($P_T = 30$ dBm)

**FIGURE 13** AN power fraction for maximum average achievable secrecy rate $\eta^*$ versus $P_T$ ($\lambda_B = \lambda_e = 0.00005/\text{km}^2$)

**ORCID**

Ahmed Fathy Darwesh
https://orcid.org/0000-0003-1313-8810

**REFERENCES**

1. Fellers, R.: Millimeter waves and their applications. Elecrr. Eng. 75(10), 914–917 (1956)

2. Rappaport, T.S., et al.: Millimeter wave mobile communications for 5G cellular: It will work! IEEE access 1, 335–349 (2013)

3. Rangan, S., et al.: Millimeter wave cellular wireless networks: Potentials and challenges. Proc. IEEE 102, 366–385 (2014)

4. Bai, T., Heath, R.W.: Coverage and rate analysis for millimeter-wave cellular networks. IEEE Trans. Wireless Commun. 14(2), 1100–1114 (2014)

5. Ghosh, A., et al.: Millimeter-wave enhanced local area systems: A high-data-rate approach for future wireless networks. IEEE J. Sel. Areas Commun. 32(6), 1152–1163 (2014)

6. Roh, W., et al.: Millimeter-wave beamforming as an enabling technology for 5G cellular communications: Theoretical feasibility and prototype results. IEEE Commun. Mag. 52(2), 106–113 (2014)

7. Thornburg, A., Heath, R.W.: Ergodic rate of millimeter wave ad hoc networks. IEEE Trans. Wireless Commun. 17(2), 914–926 (2017)

8. Bai, T., et al.: Analysis of blockage effects on urban cellular networks. IEEE Trans. Wireless Commun. 13(9), 5070–5083 (2014)

9. Thornburg, A., et al.: Performance analysis of outdoor mmwave ad hoc networks. IEEE Trans. Signal Process. 64(15), 4065–4079 (2016)

10. Zhou, L., Haas, Z.J.: Securing ad hoc networks. IEEE Netw. 13(6), 24–30 (1999)

11. Mazin, A., et al.: Secure key management for 5g physical layer security. In: 2017 IEEE 18th Wireless and Microwave Technology Conference (WAMICON), pp. 1–5. IEEE, Piscataway (2017)

12. Wu, Y., et al.: A survey of physical layer security techniques for 5G wireless networks and challenges ahead. IEEE J. Sel. Areas Commun. 36(4), 679–695 (2018)

13. Ebrahimi, N., et al.: A novel physical layer security technique using master-slave full duplex communication. In: 2019 IEEE MTT-S International Microwave Symposium (IMS), pp. 1096–1099. IEEE, Piscataway (2019)

14. Li, L., et al.: Deep learning based physical layer security of d2d underlay cellular network. China Commun. 17(2), 93–106 (2020)
15. Wyner, A.D.: The wire-tap channel. Bell Syst. Tech. J. 54(8), 1355–1387 (1975)
16. Vasudevan, S., et al.: Security-capacity trade-off in large wireless networks using keyless secrecy. In: Proceedings of the Eleventh ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 21–30. ACM, New York (2010)
17. Zhou, X., et al.: On the throughput cost of physical layer security in decentralized wireless networks. IEEE Trans. Wireless Commun. 10(8), 2764–2775 (2011)
18. Zhang, X., et al.: Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks. IEEE Trans. Inf. Forensics Secur. 8(11), 1802–1814 (2013)
19. Zheng, T.X., et al.: Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy. IEEE Trans. Wireless Commun. 16(6), 3827–3839 (2017)
20. Wang, C., Wang, H.M.: Physical layer security in millimeter wave cellular networks. IEEE Trans. Wireless Commun. 15(8), 5569–5585 (2016)
21. Vuppala, S., et al.: On the physical layer security analysis of hybrid millimeter wave networks. IEEE Trans. Commun. 66(3), 1139–1152 (2017)
22. Ju, Y., et al.: Safeguarding millimeter wave communications against randomly located eavesdroppers. IEEE Trans. Wireless Commun. 17(4), 2675–2689 (2018)
23. Zhu, Y., et al.: Secure communications in millimeter wave ad hoc networks. IEEE Trans. Wireless Commun. 16(5), 3205–3217 (2017)
24. Zhu, Y., et al.: Physical layer security in large-scale millimeter wave ad hoc networks. In: 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE, Piscataway (2016)
25. Ju, Y., et al.: Secure transmission with artificial noise in millimeter wave systems. In: 2016 IEEE Wireless Communications and Networking Conference, pp. 1–6. IEEE, Piscataway (2016)
26. Yang, W., et al.: Secure on-off transmission in mmwave systems with randomly distributed eavesdroppers. IEEE Access 7, 32681–32692 (2019)
27. Ju, Y., et al.: Secure transmissions in millimeter wave systems. IEEE Trans. Commun. 65(5), 2114–2127 (2017)
28. Ramadan, Y.R., Mirm, H.: Artificial noise aided hybrid precoding design for secure mmwave mimo systems with partial channel knowledge. IEEE Signal Process Lett. 24(11), 1729–1733 (2017)
29. Chen, C., et al.: An iterative FFT-based antenna subset modulation for secure millimeter wave communications. In: 2017 International Conference on Computing, Networking and Communications (ICNC), pp. 454–459. IEEE, Piscataway (2017)
30. Ma, R., et al.: Secure communication in millimeter wave relaying networks. IEEE Access 7, 31218–31232 (2019)
31. Ragheb, M., Hemami, S.M.S.: Secure communication for millimeter-wave systems with randomly located non-colluding eavesdroppers. In: 2020 28th Iranian Conference on Electrical Engineering (ICEE), pp. 1–6. IEEE, Piscataway (2020)
32. Zhang, Y., et al.: Secure millimeter-wave ad hoc communications using physical layer security. arXiv preprint, arXiv:200901988 (2020)
33. Baccelli, F., et al.: Stochastic geometry and wireless networks: Volume II applications. Found. Trends Netw. 4(1–2), 1–312 (2010)
34. Haenggi, M., et al.: Interference in large wireless networks. Found. Trends Netw. 3(2), 127–248 (2009)
35. Geraci, G., et al.: Secrecy rates in broadcast channels with confidential messages and external eavesdroppers. IEEE Trans. Wireless Commun. 13(5), 2931–2943 (2014)
36. Geraci, G., et al.: Physical layer security in downlink multi-antenna cellular networks. IEEE Trans. Commun. 62(6), 2006–2021 (2014)
37. Rappaport, T.S., et al.: Wideband millimeter-wave propagation measurements and channel models for future wireless communication system design. IEEE Trans. Commun. 63(9), 3029–3056 (2015)
38. Baccelli, F., et al.: An aloha protocol for multihop mobile wireless networks. IEEE Trans. Inf. Theory 52(2), 421–436 (2006)
39. Deng, S., et al.: 28 GHz and 73 GHz millimeter-wave indoor propagation measurements and path loss models. In: 2015 IEEE International Conference on Communication Workshop (ICCW), pp. 1244–1250. IEEE, Piscataway (2015)
40. Rappaport, T.S., et al.: 38 GHz and 60 GHz angle-dependent propagation for cellular & peer-to-peer wireless communications. In: 2012 IEEE International Conference on Communications (ICC), pp. 4568–4573. IEEE, Piscataway (2012)
41. Andrews, J.G., et al.: Heath, R.W.: Modeling and analyzing millimeter wave cellular systems. IEEE Trans. Commun. 65(1), 403–430 (2016)
42. Venugopal, K., et al.: Interference in finite-sized highly dense millimeter wave networks. In: 2015 Information Theory and Applications Workshop (ITA), pp. 175–180. IEEE, Piscataway (2015)
43. Ramanathan, R., et al.: Ad hoc networking with directional antennas: a complete system solution. IEEE J. Sel. Areas Commun. 23(3), 496–506 (2005)
44. Park, J., et al.: Tractable resource management with uplink decoupled millimeter-wave overlay in ultra-dense cellular networks. IEEE Trans. Wireless Commun. 15(6), 4362–4379 (2016)
45. Haenggi, M., et al.: Stochastic geometry and random graphs for the analysis and design of wireless networks. IEEE J. Sel. Areas Commun. 27(7), 1029–1046 (2009)
46. Geraci, G., et al.: Secrecy sum-rates for multi-user mimo regularized channel inversion precoding. IEEE Trans. Commun. 60(11), 3472–3482 (2012)
47. Goel, S., Negi, R.: Secret communication in presence of colluding eavesdroppers. In: 2005 IEEE Military Communications Conference, vol. 3, pp. 1501–1506. IEEE, Piscataway (2005)
48. Yang, N., et al.: Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun. Mag. 53(4), 20–27 (2015)
49. Di Renzo, M.: Stochastic geometry modeling and analysis of multi-tier millimeter wave cellular networks. IEEE Trans. Wireless Commun. 14(9), 5038–5057 (2015)
50. Hamdi, K.A.: Capacity of MRC on correlated Rician fading channels. IEEE Trans. Commun. 56(5), 708–711 (2008)
51. Vere-Jones, D.: Alpha-permanents and their applications to multivariate gamma, negative binomial and ordinary binomial distributions. New Zealand J. Math. 26, 125–149 (1997)
52. Marcus, M.: Multivariate gamma distributions. Electron. Commun. Probab. 19, 1–10 (2014)

**APPENDIX A**

A.1 | Proof of Lemma 1

The average rate at Bob can be calculated by using Theorem 1 in [23] as follows

\[
R = E\left[\log_2(1 + \frac{\chi}{R})\right],
\]

\[
\overset{(\text{step})}{\equiv} E\left[\log_2(\rho) \int_0^\infty \frac{1}{x} \left(1 - \frac{\chi}{\rho}e^{-x}\right)e^{-x}dx\right],
\]

\[
(A1)
\]

where step (a) is obtained by applying Lemma 1 in [50], and by using (10) and rearranging terms, \(R\) can be written as

\[
R = \log_2(\rho) E\left[\int_0^\infty \frac{1}{x} \left(1 - e^{-\chi x}\right)e^{-x/(\rho + x^2)}dx\right].
\]

\[
(A2)
\]
where $U = P_l||h||^2G_M^TG_M^kL(r)$ is the message signal and $I_R = \sum_{j \in \Phi_B} P_j||h_j||^2G_jL(r_j)$ is the aggregate interference signal power at Bob. Clearly, $U$ and $I_R$ are independent, then,

$$C_R = \log_2(e) \int_0^\infty \frac{1}{x} \left(1 - E[||h||^2 e^{-x}]\right) \times E[||h||^2G_M^kL(r)] e^{-x\sigma^2} dx.$$  \hspace{1cm} (A3)

From [31, 52], the Laplace transform of an $n$-dimensional multivariate gamma distributed random variables $Z$ can be formulated as

$$\mathcal{L}_Z(t) = E[e^{zt}] = \frac{1}{|\mathbf{I}_N + \mathbf{A}_N t|},$$  \hspace{1cm} (A4)

where $\mathbf{A}$ is an $N \times N$ diagonal matrix with entries $1/\nu$, and $\nu (\geq 0)$ is the shape parameter of the gamma random variable. Then, $E[||h||^2 e^{-x}]$ is the Laplace transform of an $N_T$-dimensional multivariate gamma distributed random variables $||h||^2$. Therefore,

$$E[||h||^2 e^{-x}] = \mathbf{I}_{N_j} + Q \times P_l G_M^kG_M^kL(r) e^{-x}$$  \hspace{1cm} (A5)

where $Q$ is an $N_T \times N_T$ diagonal matrix with entries $1/k$, and $k (\geq 0)$ is the shape parameter. Step (a) is obtained by rearranging terms and step (b) follows the law of total expectation based on the LoS and NLoS conditions.

Let $\Psi(x) = E[||h||^2G_M^kL(r)] e^{-x}$ be Laplace transform of the aggregate interference. Then, by using the thinning theorem which divides the interferers into two independent PPPs (i.e. $\Phi'_B$ and $\Phi'_B$), and applying the Laplace Functional of PPP [45]

$$\Psi(x) = \sum_{j \in \{L,N\}} \int_0^\infty \exp\left(-2\pi \lambda_B \int_0^r \xi_j(v) dv\right) \times \left(1 - E[||h||^2G_M^kL(r)] e^{-x\sigma^2}\right) dx$$

where step (a) is obtained by applying the Laplace transform of $n$-dimensional multivariate gamma distributed random variables. Next, by applying the law of total expectation based on the effective antenna gain distribution in (2), (12) results. Finally, by substituting (A5) and (A6) in (A3), (11) is obtained.

### A.2 Proof of Lemma 2

The average rate at Eve can be calculated as follows

$$C_E = E[\log_2(1 + \xi_E)]$$

$$= \log_2(e) \int_0^\infty \frac{1}{x} \left(1 - e^{-x}\right) e^{-x\sigma^2} dx.$$  \hspace{1cm} (A7)

where $V = P_l||h||^2G_jL(r_E)$ is the intercepted message signal power at Eve. Then,

$$C_E = \log_2(e) \int_0^\infty \frac{1}{x} \left(1 - E[||h||^2G_jL(r_E)] e^{-x\sigma^2}\right) e^{-x\sigma^2} dx.$$  \hspace{1cm} (A8)

Let $Y(x) = E[||h||^2G_jL(r_E)] e^{-x\sigma^2}$ be the Laplace transform of the intercepted message signal, hence, by applying the thinning theorem (i.e. $\Phi'_E$ and $\Phi'_E$), and with using the pdf of the distance between Alice and Eve given that Alice is intercepted by an LoS or NLoS eavesdropper [see (5)], $Y(x)$ can be given as

$$Y(x) = \sum_{j \in \{L,N\}} D_j \int_0^\infty E[||h||^2|G_jL(o)] e^{-x\sigma^2} f_j(v) dv$$

where $D_j$ is the probability that Alice is intercepted by an eavesdropper experiencing a link of type $j \in \{L,N\}$ [see (6)]. Step (a) is achieved by applying the Laplace transform of $n$-dimensional multivariate gamma distributed random variables. Finally, by applying the law of total expectation based on the gain distribution in (3), the result in (17) is derived.

### A.3 Proof of Lemma 4

By following the same steps provided in Appendix A.1:

$$\Psi(x) = E[||h||^2G_jL(r_E)] e^{-x\sigma^2}$$

$$+ P_j||h||^2G_jL(r_E)$$  \hspace{1cm} (A10)
Then, by using the thinning theorem, and applying the Laplace Functional of PPP, \( \psi(x) \) will be

\[
\psi(x) = \sum_{j \in L_N} \exp\left(-2\pi \lambda_B \int_0^{\infty} \xi_j(v) \left(1 - \exp\left(-x \sum_{\langle l,u,q \rangle \in \Omega} \delta_{luq} \right)\right) dv\right) E_{[|b_j|^2]} \left[ e^{-x \left( |b_j|^2 + \frac{1}{2} |b_j|^2 \right) G^T_j L(r_j)} \right] dv,
\]

\[
= \sum_{j \in L_N} \exp\left(-2\pi \lambda_B \int_0^{\infty} \xi_j(v) \left(1 - \exp\left(-x \sum_{\langle l,u,q \rangle \in \Omega} \delta_{luq} \right)\right) dv\right) E_{[|b_j|^2]} \left[ e^{-x \left( |b_j|^2 + \frac{1}{2} |b_j|^2 \right) G^T_j L(r_j)} \right] dv,
\]

\[
= \sum_{j \in L_N} \exp\left(-2\pi \lambda_B \int_0^{\infty} \xi_j(v) \left(1 - \exp\left(-x \sum_{\langle l,u,q \rangle \in \Omega} \delta_{luq} \right)\right) dv\right) E_{[|b_j|^2]} \left[ e^{-x \left( |b_j|^2 + \frac{1}{2} |b_j|^2 \right) G^T_j L(r_j)} \right] dv,
\]

where \( \xi_j(v) \) is the received message signal power at Eve and \( I_E = P^T_i |b_i|^2 G^T_i L(r_i) \) is the received AN power at Eve from Alice and \( I_{E_j} = \sum_{i \in \Phi \setminus \{i\}} P^T_i |b_i|^2 G^T_i L(r_i) \) is the received AN at Eve from the interferers in \( \Phi_B \). Due to \( \hat{P} \) and \( I_E \) are dependent and are independent of \( I_{E_j} \), we have:

\[
\overline{C}_E = \log_2(e) \int_0^{\infty} \frac{1}{x} \left( E_{[|b_i|^2]} G^T_j r_i \left[ e^{-x r_i} \right] \right) \Psi_2(v) dv,
\]

where \( \Psi_2(v) \) is proved using the same approach as (17) in Appendix A.2 by replacing \( P^T_i, |b_i|^2 \) and \( G^T_j \) with \( P^T_i, |b_i|^2 \) and \( G^T_j \), respectively, then (36) is obtained.

Then, by applying the thinning theorem in \( \Psi_2(v) \), and using the pdf of the distance between Alice and Eve given that Alice is intercepted by an LoS or NLoS eavesdropper, \( \Psi_2(v) \) can be written as

\[
\Psi_2(v) = \sum_{j \in L_N} D_j \int_0^{\infty} \int_0^{\infty} \int_0^{\infty} \Psi_1(v) dv,
\]

where \( D_j \) is the received AN at \( r_j \) and \( \Psi_1(v) \) is the pdf of the distance between Alice and Eve given that Alice is intercepted by an LoS or NLoS eavesdropper. Finally, by following the same procedure for deriving (12) in Appendix A.1, (38) is obtained.