IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 20, 2018, accepted October 16, 2018, date of publication October 30, 2018, date of current version December 3, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2878741

Performance Analysis of Interference and Eavesdropping Immunity in Narrow Beam mmWave Networks

QING XUE[1], PEI ZHOU[1], XUMING FANG[1], (Senior Member, IEEE), AND MING XIAO[2], (Senior Member, IEEE)

[1]Key Laboratory of Information Coding and Transmission, Southwest Jiaotong University, Chengdu 610031, China
[2]Department of Communication Theory, Royal Institute of Technology, 100 44 Stockholm, Sweden

Corresponding author: Xuming Fang (xmfang@swjtu.edu.cn)

The work of Q. Xue, P. Zhou, and X. Fang was supported in part by the NSFC under Grant 61471303, in part by the NSFC-Guangdong Joint Foundation under Grant U1501255, and in part by the EU FP7 QUICK Project under Grant PIRSES-GA-2013-612652. The work of M. Xiao was supported by the EU FP7 QUICK Project under Grant PIRSES-GA-2013-612652.

ABSTRACT Exploiting highly directional antenna arrays to compensate for severe propagation loss is one of the defining features in millimeter-wave (mmWave) communications. With efficient beamforming techniques, mmWave transceivers can form steerable narrow beams. Therefore, different from convenient microwave networks, the signal or interference power in mmWave communications is highly directional and closely related to critical parameters such as interference distance and angles of departure/arrival. The high directivity implies that the co-channel interference among simultaneously active mmWave links can be expected to be significantly smaller than that for omnidirectional links and, meanwhile, the security of mmWave communications may also be enhanced. In this context, will the traditional interference mitigation and physical-layer security techniques still be efficient or necessary in mmWave networks? The answer may be negative in certain conditions. However, there is no detailed analysis on the conditions for this issue. In this paper, we jointly analyze the inter-beam interference and secrecy performance of mmWave communications for their close relation to signal-to-interference-plus-noise ratio. We also derive various performance limits (e.g., interference/eavesdropping distance limit, transmission power limit, offset angle limit, and beamwidth limit) of interference and eavesdropping immunity in mmWave networks. The theoretical and numerical results verify our analysis.

INDEX TERMS Millimeter wave (mmWave), narrow beams, inter-beam interference, physical layer security, eavesdropping, immunity.

I. INTRODUCTION

Millimeter wave (mmWave) communications, operating in about 30-300 GHz bands, have attracted significant research interest recently [1]–[4], since the massive available spectrum can potentially provide multiple Gbps (gigabit per second) data rate [5], [6]. Thanks to the short wavelength of mmWave radio, large-scale directional antenna arrays can be packed into the limited dimensions of mmWave transceivers. With efficient beamforming techniques [7], highly directional beams with substantial array gains can be synthesized to compensate for the severe propagation loss [8] in mmWave networks. In this context, the signal or interference power in mmWave communications is highly directional and closely related to the angles of departure/arrival [9]. Therefore, many technologies introduced in the last decade for interference mitigation in microwave networks (e.g., inter-cell interference coordination and interference alignment) may have limited gains in mmWave networks [3]. Under the new characteristics of mmWave, the efficiency of traditional physical layer security techniques (e.g., artificial noise) should be re-checked as well [10]. The existing research on wireless communications takes great effort on interference suppression/coordination and physical layer security. However, with the emergence and rapid development of the mmWave technology and system, the problems may be rather different. Consequently, the existing interference

suppression/coordination mechanisms or physical layer security techniques may no longer be suitable for mmWave networks and even some of them are redundant.

Different from interference coordination mainly in either the time or frequency domain in microwave networks, spatial or beamspace interference coordination receives more attention in mmWave networks (e.g., [11]–[15]). The high directivity of mmWave links implies that the co-channel interference among simultaneously active links can be expected to be significantly smaller than that for omnidirectional links [16], since the interference from off-boresight directions would be rejected. Hence, adaptive arrays with narrow beams can reduce the impact of interference, meaning that mmWave networks are most likely to be noise-limited rather than interference-limited [17]. Many relevant studies of mmWave communications are based on the hypothesis that the co-channel/inter-beam interference is negligible when the beamwidth is narrow enough, which may not always hold. To the best of our knowledge, there has been no work on giving detailed quantitative analysis on the conditions for this hypothesis. Generally speaking, the amount of interference mainly depends on the location of the interferers relative to the reference receiver (e.g., the relative distance and direction), the antenna radiation patterns, and the transmitted power of the reference receiver and the interferers. In this context, through the analysis of the effects of various parameters on the interference, we show the performance limits of interference immunity (i.e., the received interference power is insufficient to degrade the reference link performance) in mmWave networks. In this study, the *limit* refers to the critical numerical value (i.e., the boundary value) at which the condition of interference/eavesdropping immunity starts to hold. Here, we extend the concept of interference/eavesdropping immunity in the Ultra-wideband (UWB) technology [18] in the time domain to the beamspace. As one of the key parameters for determining interference, the interference range has been analyzed in [16] and [19]. However, the results are not universal, since the adopted antenna pattern is either ideal or does not consider side lobes.

Moreover, the investigation of physical layer security in mmWave networks is a very promising and highly rewarding area [20]. Concerning the peculiar propagation characteristics of mmWave, the secrecy performance of mmWave networks will be quite different from conventional microwave networks, which should be re-evaluated. Specifically, in [10], secrecy performance of noise-limited and artificial noise assisted mmWave cellular networks under a stochastic geometry framework is analyzed. The work of Zhu *et al.* [21] explored the potential of physical layer security in mmWave ad hoc networks and characterized the impact of mmWave channel characteristics, random blockages, and antenna gains on the secrecy performance. In [22], secure transmissions under slow fading channels with multipath propagation in mmWave systems is studied. These studies focus on the security of mmWave networks from different aspects. On the other side, since directional communications with narrow beams in mmWave networks can suppress the interference from neighbors effectively, the received signal-to-noise ratio (SNR) at eavesdroppers may be extremely low such that the eavesdroppers are unable to decode the secret messages. That is, mmWave networks with narrow beams own inherent security and the existing physical layer security techniques may have limited gains in some conditions. In this study, we investigate the performance limits of physical layer eavesdropping immunity (i.e., a secure connection is possible). Note that we analyze the physical layer security from the beamspace aspect, which is quite different from the existing literatures (e.g., [10], [22], [23]).

Different from microwave networks, the transmission distance, transmission power, offset angle of departure/arrival and beamwidth all have impact on the performance of mmWave networks due to the inherent directivity. If one or more of these boundary conditions are not satisfied, the directional communication in mmWave networks will be damaged. Meanwhile, both of the interference-proof and physical layer security could naturally gain the benefit from the directivity. Hence, with the limits, we can determine whether the existing interference suppression/coordination and physical layer security techniques can be simplified or even omitted in mmWave communications. From [23], we can know that, only if the capacity of legitimate receiver greater than the capacity of eavesdropper, the physical layer security can be achieved. Thus, both interference immunity and eavesdropping immunity are closely related to SINR. In this context, we jointly investigate the performance limits of both interference-proof and eavesdropping immunity in this study. Moreover, since the security performance in mmWave networks is determined by the operating beams of the legitimate transmitter/receiver and eavesdroppers (i.e., the inter-beam interference is the basis of physical layer security), we will first consider the interference immunity problem in mmWave networks and then investigate the physical layer eavesdropping immunity problem under different eavesdropping scenarios.

Our main contributions can be summarized as follows:

1) We investigate the inter-beam interference of an mmWave network with multiple simultaneous links in beamspace MU-MIMO and the Device-to-Device (D2D) mode. We also give quantitative analysis of the performance limits of interference immunity in muti-antenna narrow beam mmWave networks.
2) We investigate the various performance limits of physical layer eavesdropping immunity in mmWave networks in beamspace under passive/active eavesdropping scenarios with multiple colluding/non-colluding eavesdroppers.
3) We analyze the impact of the blockage of a potential eavesdropper to the legitimate user signal from physical layer security in mmWave networks with narrow beams.
4) Our study shows that mmWave networks have inherent interference/eavesdropping proof ability when the actual interference/eavesdropping distance is larger than the interference/eavesdropping distance limit, or the actual

transmission power of the interference/eavesdropping link is lower than the transmission power limit, or the actual offset angle of departure/arrival is larger than the offset angle limit, or the operating beamwidth is smaller than the beamwidth limit.

The rest of the paper is organized as follows. In Section II, the system model is introduced. Section III investigates the inter-beam interference issue of mmWave networks and carries out quantitative analysis of interference immunity. In Section IV, the performance limits of eavesdropping immunity in mmWave networks are analyzed. Section V shows some numerical simulations. Conclusions are provided in Section VI.

II. SYSTEM MODELS

We consider a cellular network consisting of an mmWave base station (MBS) and multiple mmWave user equipments (MUEs). Meanwhile, both the MBS and MUEs are equipped with directional antennas, which are favorable to support simultaneous transmissions. By adopting the beamforming training (or beam steering) process, the transmit and receive beam pair set that best matches the simultaneous links can be determined. In this section, we will first describe the inter-beam interference scenario and then present the beamspace eavesdropping scenario for the mmWave network.

Considering that the actual transmission paths of mmWave signals are unpredictable in multiple reflection environment, the operating links in this study are assumed to be line-of-sight (LOS). It should be mentioned that, although the analysis is based on LOS scenario, its core ideas can be extended to Non-LOS (NLOS) scenarios. In fact, most of malicious interference and eavesdropping usually occur in long-distance outdoor transmission scenarios. However, since there may have severe path loss caused by high diffraction loss and multiple reflection effects in these environments, NLOS paths in mmWave communications are generally considered in short-range (e.g., indoor) scenarios [24].

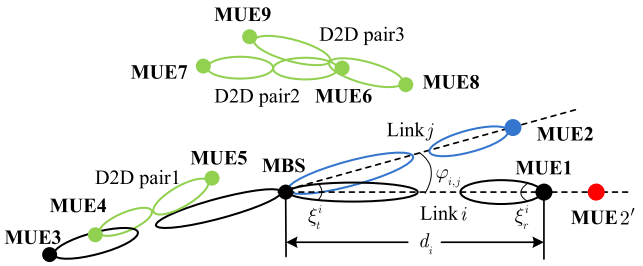


FIGURE 1. System model for mmWave communications with multiple D2D and beamspace MU-MIMO links. In order to make the figure clear, we do not draw side lobes, which is considered in our analysis.

A. INTER-BEAM INTERFERENCE MODEL

As shown in Fig. 1, we assume that the MBS is capable of supporting multiple beams simultaneously and each MUE is operating with a single beam. In order to investigate the inter-beam interference in the mmWave network, we consider two communication modes: (a) The MBS serves multiple MUEs simultaneously with multiple directional beams, i.e., in the downlink beamspace MU-MIMO mode, of which the link set is denoted as $\mathbb{N}_{\mathrm{MIMO}}$; (b) Communications between a pair of MUEs using directional beams, i.e., in the D2D mode, of which the link set is denoted as $\mathbb{N}_{\mathrm{D2D}}$. Meanwhile, we have the simultaneous link set $\mathbb{N} = \mathbb{N}_{\mathrm{MIMO}} + \mathbb{N}_{\mathrm{D2D}}$.

Let P_t^i be the transmitted power of link i ($i \in \mathbb{N}$); d_i be the distance between the transmitter and receiver of link i ($i \in \mathbb{N}$); ξ_t^i and ξ_r^i be the transmitting and receiving beamwidth (i.e., the angle between the half-power points of the main lobe) of link i ($i \in \mathbb{N}$), respectively; $\varphi_{i,j}$ ($0 \le |\varphi_{i,j}| \le \pi$) be the offset angle of link j relative to link i ($i, j \in \mathbb{N}_{\mathrm{MIMO}}$). Here, there are three interference scenarios between link i and link j:

1) $i, j \in \mathbb{N}_{\mathrm{MIMO}}$: If $\varphi_{i,j} < \frac{\xi_t^i + \xi_t^j}{2}$, the interference is mainly caused by the main lobes of link i and link j. Otherwise, the interference is caused by side lobes. Typically, when $\varphi_{i,j} = 0$ (e.g., when MUE2 is located at the position of MUE2' shown in Fig. 1), whether MUE1 will be interfered by link j and the magnitude of the interference depends on P_t^j and d_i.
2) $i, j \in \mathbb{N}_{\mathrm{D2D}}$: As D2D pair2 and pair3 shown in Fig. 1, when the operating state of MUE6 and MUE9 is different, the two links may interfere with each other. For example, if MUE6 is the transmitter of link i and MUE9 is the receiver of link j, MUE9 may receive some interference signals from MUE6.
3) $i \in \mathbb{N}_{\mathrm{MIMO}}$, $j \in \mathbb{N}_{\mathrm{D2D}}$: As the link of MBS-MUE3 and D2D pair1 shown in Fig. 1, when MUE5 is the transmitter of link j, the two links may interfere with each other.

In this context, the inter-beam interference mainly depends on the relative direction and distance between the interferers and the reference receiver, the beam patterns, and the transmitted power of the reference receiver and the interferers. Furthermore, the interference scenario of link i ($\forall i \in \mathbb{N}$) can be summed up as a combination of the above three scenarios.

Although only the beamspace MU-MIMO and D2D mode are described here, the interference model shows the worst-case scenario and it can be seen as an abstract description of a general scene, in order to obtain the performance limits of interference immunity in mmWave networks. For instance, the transmission of a network node operating simultaneously with multiple beams can be analogous to the beamspace MIMO mode and the general point-to-point communication can be analogous to the D2D mode.

B. PHYSICAL LAYER EAVESDROPPING MODEL

Taking link i ($i \in \mathbb{N}$) as a legitimate link, we describe the beamspace eavesdropping scenarios according to the mmWave network. It consists of three communication parties, i.e., the typical transmitter Alice, the legitimate receiver Bob, and multiple malicious eavesdroppers (e.g., Eve), as depicted in Fig. 2. We assume that the operating beams of Alice and Bob are perfectly aligned to keep secret from the potential eavesdroppers.

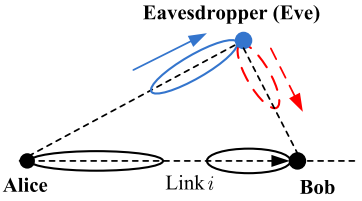


FIGURE 2. MmWave communication with potential eavesdropping. Note that Eve works only with the receiving beam in passive scenario or with both the transmitting and receiving beams in active scenario.

To evaluate the secrecy performance of link i, we distinguish two eavesdropping scenarios:

1) Passive Eavesdropping: The potential eavesdroppers (e.g., Eve) act passively without any active attacks to deteriorate link i. Eve in this scenario only needs single beam for listening signals.
2) Active Eavesdropping: Eve sends some interference signals (e.g., artificial noise) to Bob with a transmitting beam while eavesdropping the secret messages from Alice with a receiving beam. That is, we consider beamspace active eavesdropping in the mmWave network rather than that in time/frequency domain in microwave networks.

In addition, we consider both non-colluding and colluding eavesdroppers in the above two scenarios. In the non-colluding case, the eavesdroppers individually overhear link i without centralized processing. In the colluding case, the eavesdroppers can exchange and combine their received signals at a central data processing unit, thus improving their ability to decode the secret messages [23]. Generally, active eavesdropping with colluding eavesdroppers is the worst-case scenario for physical layer security.

To simplify illustration, we summarize the main notations used throughout the paper in Table 1.

TABLE 1. List of main notations.

Symbol	Definition
$\mathbb{N}$	The set of the simultaneous links in the mmWave network
$\mathbb{N}_{\mathrm{MIMO}}$	Beamspace MU-MIMO link set ($\mathbb{N}_{\mathrm{MIMO}} \subseteq \mathbb{N}$)
$\mathbb{N}_{\mathrm{D2D}}$	D2D link set ($\mathbb{N}_{\mathrm{D2D}} \subseteq \mathbb{N}$)
P_t^i	Transmission power of link i ($i \in \mathbb{N}$)
$G_{t,\max}^i$	Maximum transmitting antenna gain of link i ($i \in \mathbb{N}$)
$G_{r,\max}^i$	Maximum receiving antenna gain of link i ($i \in \mathbb{N}$)
d_i	Length of link i ($i \in \mathbb{N}$)
$d_{i,j}$	Distance between RX i and TX j ($i, j \in \mathbb{N}$)
$\varphi_{i,j}$	Offset angle of link j relative to link i ($i, j \in \mathbb{N}_{\mathrm{MIMO}}$)
ϑ_1^j	Offset angle of transmitting beam j relative to the boresight direction of RX i and TX j ($i, j \in \mathbb{N}$)
ϑ_2^j	Offset angle of receiving beam i relative to the boresight direction of RX i and TX j ($i, j \in \mathbb{N}$)
ξ_t^i	Transmitting beamwidth of link i ($i \in \mathbb{N}$)
ξ_r^i	Receiving beamwidth of link i ($i \in \mathbb{N}$)
$\mathbb{Q}_E$	Potential eavesdropper set in the mmWave network
d_e	Passive eavesdropping distance of eavesdropper e ($e \in \mathbb{Q}_E$)
ϕ_e	Angle between the boresight directions of link i and the eavesdropping link related to eavesdropper e ($e \in \mathbb{Q}_E$)
σ_i^2	Noise power of link i ($i \in \mathbb{N}$)
$d_{e,A}$	Distances between eavesdropper e and Alice in active eavesdropping scenario
$d_{e,B}$	Distances between eavesdropper e and Bob in active eavesdropping scenario
$d_{e,x}$	Distances between eavesdropper e and x ($x \in \mathbb{Q}_E \backslash e$) in active eavesdropping scenario
ϕ_1^e	Offset angle of the receiving beam of eavesdropper e relative to the legitimate link
ϕ_2^e	Offset angle of the transmitting beam of eavesdropper e relative to the legitimate link
α_e	Shadowing angle of eavesdropper e

III. INTERFERENCE IMMUNITY ANALYSIS

In what follows, for the mmWave network with narrow beams, we will investigate the performance limits of interference immunity by analyzing the impact of various parameters on inter-beam interference.

According to Friis transmission formula, the received power of link i in free-space transmission can be determined by [4]

$$P_r^i = P_t^i \cdot G_t^i \cdot G_r^i \cdot \left(\frac{\lambda}{4\pi d_i^{n/2}}\right)^2, \tag{1}$$

where G_t^i and G_r^i are the antenna gains of the transmitter and receiver, respectively, λ is the operating wavelength, and n is the pathloss exponent and $n = 2$ in free space. By making channel measurements and then finding a suitable value of n, this formula in (1) can be also used to approximately describe the power of the received signal in non-free-space propagation as well [4]. In addition, we approximate the actual antenna pattern by the sinc antenna pattern model [9]. That is, the normalized array gain can be approximated as

$$g(\vartheta) = \frac{\sin^2(N\pi\vartheta)}{(N\pi\vartheta)^2}, \tag{2}$$

where N is the number of antenna elements and ϑ is the azimuthal beam angle. In general, we have $N \gg 1$ in mmWave networks. Meanwhile, the transmitting and receiving beams for each link are assumed to be aligned by adopting beamforming training (or beam steering) mechanism. Hence, we have $P_r^i = P_t^i G_{t,\max}^i G_{r,\max}^i \left(\frac{\lambda}{4\pi d_i^{n/2}}\right)^2$, where $G_{t,\max}^i$ and $G_{r,\max}^i$ are the maximum transmitting and receiving antenna gains of link i, respectively.

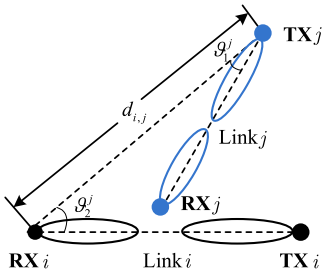


FIGURE 3. Illustration of concurrent directional beams.

As illustrated in Fig. 3, denoting $d_{i,j}$ as the distance between link i's receiver (RX i) and link j's transmitter (TX j),

ϑ_1^j ($0 \le \left|\vartheta_1^j\right| \le \pi$) and ϑ_2^j ($0 \le \left|\vartheta_2^j\right| \le \pi$) as the offset angles of the operating beams of TX j and RX i relative to the boresight direction of RX i and TX j (i.e., the offset angles of departure and arrival considering interference), respectively, the received interference power of link i is given by

$$P_I^i = \sum_{j\in\mathbb{N}\backslash i} P_t^j \cdot G_t^j\left(\vartheta_1^j\right) \cdot G_r^i\left(\vartheta_2^j\right) \cdot \left(\frac{\lambda}{4\pi d_{i,j}^{n/2}}\right)^2 = \sum_{j\in\mathbb{N}\backslash i} P_t^j G_{t,\max}^j g\left(\vartheta_1^j\right) G_{r,\max}^i g\left(\vartheta_2^j\right) \left(\frac{\lambda}{4\pi d_{i,j}^{n/2}}\right)^2. \tag{3}$$

Note that Fig. 3 shows the general relationship between link i and j. If TX i and TX j are the same transmitter (e.g., the MBS in Fig. 1) that operate with different beams, then $i, j \in \mathbb{N}_{\text{MIMO}}$; otherwise, $i, j \in \mathbb{N}_{\text{D2D}}$, or one of them in $\mathbb{N}_{\text{MIMO}}$ and the other in $\mathbb{N}_{\text{D2D}}$.

Denoting σ_i^2 as the thermal noise power, then, $\text{SINR}_i = \frac{P_r^i}{\sigma_i^2 + P_I^i}$. Considering that we mainly focus on the analysis of the influence of inter-beam interference, for simplifying analysis, similar to [16], we do not consider thermal noise here. Therefore, the received signal-to-interference ratio (SIR) of link i can be evaluated as

$$\text{SIR}_i = \frac{P_r^i}{P_I^i} = \frac{P_t^i \cdot G_{t,\max}^i \cdot d_i^{-n}}{\sum_{j\in\mathbb{N}\backslash i} P_t^j \cdot G_{t,\max}^j \cdot g\left(\vartheta_1^j\right) \cdot g\left(\vartheta_2^j\right) \cdot d_{i,j}^{-n}}. \tag{4}$$

It can be seen from (2)-(3) that P_I^i is mainly related to $d_{i,j}$, P_t^j, ϑ_1^j, ϑ_2^j, N_t^j, N_r^i, and $\mathbb{N}$, hereafter called interference parameters, where N_t^j and N_r^i are the number of antennas at TXj and RX i, respectively. Since ξ_t^j and ξ_r^i depend mainly on N_t^j and N_r^i, respectively (i.e., the larger the number of antennas, the narrower the beam), the impact of beamwidth on link performance can be reflected by the size of antenna array in this study. As given in [9], we have $\xi_t^j \doteq 1/N_t^j$ and $\xi_r^i \doteq 1/N_r^i$.

Assuming that link i has interference immunity (i.e., the received interference is insufficient to degrade the performance of link i and, thus, link i will be accurate even without interference mitigation) when $\text{SIR}_i > \eta$, where η is a given threshold. Here, we define the *limit* of an interference parameter as its maximum or minimum value for interference immunity, which can be obtained if $\text{SIR}_i = \eta$ holds. Hence, let

$$\frac{P_t^i \cdot G_{t,\max}^i \cdot d_i^{-n}}{P_t^j \cdot G_{t,\max}^j \cdot g\left(\vartheta_1^j\right) \cdot g\left(\vartheta_2^j\right) \cdot d_{i,j}^{-n} + P_{I;j}} = \eta, \tag{5}$$

the limits of interference parameters of link j ($\forall j \in \mathbb{N}\backslash i$) can be derived as the following propositions, where

$$P_{I;j} = \sum_{k\in\mathbb{N}\backslash i,j} P_t^k \cdot G_{t,\max}^k \cdot g\left(\vartheta_1^k\right) \cdot g\left(\vartheta_2^k\right) \cdot d_{i,k}^{-n}. \tag{6}$$

Definition 1 (Interference Distance Limit): The interference distance limit is the minimum value of the interference distance for inter-beam interference immunity, i.e., $d_{i,j_0} = \min d_{i,j}$ for $\text{SIR}_i > \eta$.

Proposition 1: Consider an mmWave network with multiple simultaneous links in beamspace MU-MIMO and the D2D mode, of which the links' set is denoted by $\mathbb{N}$. For a typical link i and an interference link j ($\forall j \in \mathbb{N}\backslash i$), according to Definition 1, the limit of interference distance $d_{i,j}$ is given by

$$d_{i,j_0} = \left(\frac{P_t^j \cdot G_{t,\max}^j \cdot g\left(\vartheta_1^j\right) \cdot g\left(\vartheta_2^j\right)}{\frac{P_t^i \cdot G_{t,\max}^i \cdot d_i^{-n}}{\eta} - P_{I;j}}\right)^{1/n}. \tag{7}$$

Proof: Since $d_{i,j_0} = \min d_{i,j}$ for $\text{SIR}_i > \eta$, let $\text{SIR}_i = \eta$ and assuming all other parameters except $d_{i,j}$ in (5) are known quantities, we obtain the interference distance limit d_{i,j_0} shown in (7). ■

Definition 2 (Transmission Power Limit): The transmission power limit is the maximum transmission power of TX j for interference immunity, i.e., $P_t^{j_0} = \max P_t^j$ for $\text{SIR}_i > \eta$.

Proposition 2: Consider the mmWave network described in Proposition 1. For typical link i and interference link j, according to Definition 2, the limit of TX j's transmission power P_t^j is given by

$$P_t^{j_0} = \frac{\frac{P_t^i \cdot G_{t,\max}^i \cdot d_i^{-n}}{\eta} - P_{I;j}}{G_{t,\max}^j \cdot g\left(\vartheta_1^j\right) \cdot g\left(\vartheta_2^j\right) \cdot d_{i,j}^{-n}}. \tag{8}$$

Proof: Since $P_t^{j_0} = \max P_t^j$ for $\text{SIR}_i > \eta$, assuming all other parameters except P_t^j in (5) are known quantities, we obtain the transmission power limit $P_t^{j_0}$ shown in (8). ■

Definition 3 (Offset Angle Limit): The offset angle limit is the minimum offset angle of departure/arrival for $\text{SIR}_i > \eta$.

Proposition 3: Consider the mmWave network described in Proposition 1. For the typical link i and the interference link j, according to Definition 3, the limit of the offset angle of departure and arrival (i.e., ϑ_1^j and ϑ_2^j) are, respectively,

$$\vartheta_1^{j_0} \Leftarrow \frac{\sin^2\left(N_t^j \pi \vartheta_1^{j_0}\right)}{\left(N_t^j \pi \vartheta_1^{j_0}\right)^2} = \frac{\frac{P_t^i \cdot G_{t,\max}^i \cdot d_i^{-n}}{\eta} - P_{I;j}}{P_t^j \cdot G_{t,\max}^j \cdot g\left(\vartheta_2^j\right) \cdot d_{i,j}^{-n}}, \tag{9}$$

and

$$\vartheta_2^{j_0} \Leftarrow \frac{\sin^2\left(N_r^i \pi \vartheta_2^{j_0}\right)}{\left(N_r^i \pi \vartheta_2^{j_0}\right)^2} = \frac{\frac{P_t^i \cdot G_{t,\max}^i \cdot d_i^{-n}}{\eta} - P_{I;j}}{P_t^j \cdot G_{t,\max}^j \cdot g\left(\vartheta_1^j\right) \cdot d_{i,j}^{-n}}. \tag{10}$$

Proof: Since $\vartheta_1^{j_0} = \min \vartheta_1^j$ for $\text{SIR}_i > \eta$, assuming all other parameters except ϑ_1^j in (5) are known quantities, we obtain $\vartheta_1^{j_0}$ shown in (9). Similarly, we obtain $\vartheta_2^{j_0}$ shown in (10). ■

Definition 4 (Beamwidth Limit): The beamwidth limit is the maximum operating beamwidth for interference immunity, i.e., $\xi_t^{j_0} = \max \xi_t^j$ or $\xi_r^{i_0} = \max \xi_r^i$ for $\text{SIR}_i > \eta$.

Proposition 4: Consider the mmWave network described in Proposition 1. For the typical link i and the interference link j, according to Definition 4, the limit of the operating beamwidth of TX j and RX i (i.e., ξ_t^j and ξ_r^i) are, respectively, $\xi_t^{j_0} \doteq 1/N_t^{j_0}$ and $\xi_r^{i_0} \doteq 1/N_r^{i_0}$, where

$$N_t^{j_0} \Leftarrow \frac{\sin^2\left(N_t^{j_0}\pi\vartheta_1^j\right)}{\left(N_t^{j_0}\pi\vartheta_1^j\right)^2} = \frac{\frac{P_t^i\cdot G_{t,\max}^i\cdot d_i^{-n}}{\eta} - P_{I:j}}{P_t^j\cdot G_{t,\max}^j\cdot g\left(\vartheta_2^j\right)\cdot d_{i,j}^{-n}}, \quad (11)$$

and

$$N_r^{i_0} \Leftarrow \frac{\sin^2\left(N_r^{i_0}\pi\vartheta_2^j\right)}{\left(N_r^{i_0}\pi\vartheta_2^j\right)^2} = \frac{\frac{P_t^i\cdot G_{t,\max}^i\cdot d_i^{-n}}{\eta} - P_{I:j}}{P_t^j\cdot G_{t,\max}^j\cdot g\left(\vartheta_1^j\right)\cdot d_{i,j}^{-n}}. \quad (12)$$

Proof: Combining (2) with (5) and assuming all other parameters except N_t^j are known quantities, we obtain $N_t^{j_0}$ shown in (11). Further, as we approximate the actual antenna pattern by the sinc antenna pattern model, i.e., $\xi_t^j \doteq 1/N_t^j$, we obtain $\xi_t^{j_0} \doteq 1/N_t^{j_0}$. Similarly, we can obtain $\xi_r^{i_0}$. ■

In particular, for link $i, j \in \mathbb{N}_{\text{MIMO}}$, we have $d_{i,j} = d_i$, $\vartheta_1^j = \varphi_{i,j}$, $\vartheta_2^j = 0$ (i.e., $g\left(\vartheta_2^j\right) = 1$), and $G_{t,\max}^j = G_{t,\max}^i$ in general, hence, when $P_{I:j} = 0$, the interference limits are, respectively,

$$P_t^{j_0} = \frac{P_t^i}{\eta\cdot g\left(\varphi_{i,j}\right)}, \quad (13)$$

$$\varphi_{i,j_0} \Leftarrow \frac{\sin^2\left(N_t^j\pi\varphi_{i,j_0}\right)}{\left(N_t^j\pi\varphi_{i,j_0}\right)^2} = \frac{P_t^i}{\eta\cdot P_t^j}, \quad (14)$$

$$\xi_t^{j_0} \doteq 1/N_t^{j_0} \Leftarrow N_t^{j_0} \Leftarrow \frac{\sin^2\left(N_t^{j_0}\pi\varphi_{i,j}\right)}{\left(N_t^{j_0}\pi\varphi_{i,j}\right)^2} = \frac{P_t^i}{\eta\cdot P_t^j}. \quad (15)$$

Thus, when $\xi_r^i < \xi_r^{i_0}$ ($i \in \mathbb{N}$), $d_{i,j} > d_{i,j_0}$, $P_t^j < P_t^{j_0}$, $\vartheta_1^j > \vartheta_1^{j_0}$, $\vartheta_2^j > \vartheta_2^{j_0}$, or $\xi_t^j < \xi_t^{j_0}$ ($\forall j \in \mathbb{N}\backslash i$), interference mitigation techniques for link i may have limited gains and could be simplified in the mmWave network.

IV. PHYSICAL LAYER EAVESDROPPING IMMUNITY ANALYSIS

In this section, we analyze the physical layer eavesdropping immunity limits of the mmWave network under the two different beamspace eavesdropping scenarios depicted in Fig. 2, where the set of the potential eavesdroppers is denoted by $\mathbb{Q}_E$.

In the following, we utilize the secrecy rate to evaluate the secrecy performance of the legitimate link (e.g., link i) as [23]

$$R_i = \max\left\{\log_2(1+\text{SINR}_B) - \log_2(1+\text{SINR}_E), 0\right\}, \quad (16)$$

where SINR_B and SINR_E are the received SINR at the legitimate receiver (e.g., Bob) and the eavesdroppers (e.g., Eve), respectively. Generally, when $R_i > 0$, a secure connection is possible [25]. Therefore, let $R_i = 0$, i.e., $\frac{\text{SINR}_B}{\text{SINR}_E} = 1$, the eavesdropping limits can be derived. Similar to the interference parameter limits, the eavesdropping limits here are defined as the critical values of the parameters related to physical eavesdropping (hereafter called eavesdropping parameters) for beamspace eavesdropping immunity (i.e., secure connection), which can be obtained if $R_i = 0$ holds.

A. PASSIVE EAVESDROPPING

Since the eavesdroppers do not take any active attacks to deteriorate link i in this scenario, the SINR at Bob and eavesdropper e ($e \in \mathbb{Q}_E$) are respectively reduced to

$$\text{SNR}_B = \frac{P_t^i\cdot G_{t,\max}^i\cdot G_{r,\max}^i\cdot\left(\frac{\lambda}{4\pi d_i^{n/2}}\right)^2}{\sigma_i^2}, \quad (17)$$

$$\text{SNR}_e = \frac{P_r^e}{\sigma_e^2} = \frac{P_t^i G_{t,\max}^i g\left(\phi_e\right) G_{r,\max}^e\left(\frac{\lambda}{4\pi d_e^{n/2}}\right)^2}{\sigma_e^2}, \quad (18)$$

where ϕ_e ($0 \le |\phi_e| \le \pi$) is the angle between the boresight directions of the eavesdropping link and link i; d_e is the distance between Alice and e; σ_e^2 is the noise variance at e.

1) NON-COLLUDING EAVESDROPPERS

In this case, each eavesdropper acts individually so that link i is secure if the condition $\frac{\text{SNR}_B}{\max\limits_{e\in\mathbb{Q}_E}\text{SNR}_e} > 1$ holds. Assuming that eavesdropper x ($x \in \mathbb{Q}_E$) is the most malicious eavesdropper, i.e., $\text{SNR}_x = \max\limits_{e\in\mathbb{Q}_E}\text{SNR}_e$, we can derive the eavesdropping limits according to

$$\frac{\text{SNR}_B}{\text{SNR}_x} = \frac{G_{r,\max}^i\cdot d_i^{-n}\cdot\sigma_x^2}{g\left(\phi_x\right)\cdot G_{r,\max}^x\cdot d_x^{-n}\cdot\sigma_i^2} = 1. \quad (19)$$

Proposition 5: Consider a legitimate link i in an mmWave network under passive eavesdropping scenario with multiple non-colluding eavesdroppers in beamspace. Denoting $\mathbb{Q}_E$ as the set of the potential eavesdroppers, if $\text{SNR}_x = \max\limits_{e\in\mathbb{Q}_E}\text{SNR}_e$, i.e., eavesdropper x is the most malicious eavesdropper in $\mathbb{Q}_E$, the limits of eavesdropping parameters (i.e., d_x, ϕ_x, and ξ_t^i) are, respectively,

$$d_{x_0} = \left(\frac{g\left(\phi_x\right)\cdot G_{r,\max}^x\cdot\sigma_i^2}{G_{r,\max}^i\cdot\sigma_x^2}\right)^{1/n}\cdot d_i, \quad (20)$$

$$\phi_{x_0} \Leftarrow \frac{\sin^2\left(N_t^i\pi\phi_{x_0}\right)}{\left(N_t^i\pi\phi_{x_0}\right)^2} = \frac{G_{r,\max}^i\cdot\sigma_x^2\cdot d_x^n}{G_{r,\max}^x\cdot\sigma_i^2\cdot d_i^n}, \quad (21)$$

$$\xi_t^{i_0} \doteq \frac{1}{N_t^{i_0}} \Leftarrow N_t^{i_0} \Leftarrow \frac{\sin^2\left(N_t^{i_0}\pi\phi_x\right)}{\left(N_t^{i_0}\pi\phi_x\right)^2} = \frac{G_{r,\max}^i\sigma_x^2 d_x^n}{G_{r,\max}^x\sigma_i^2 d_i^n}. \quad (22)$$

Proof: For passive eavesdropping scenario with non-colluding eavesdroppers, the secrecy performance of the legitimate link i depends on the most malicious eavesdropper in $\mathbb{Q}_E$, e.g., eavesdropper x, which satisfies $\text{SNR}_x = \max\limits_{e\in\mathbb{Q}_E}\text{SNR}_e$. Thus, the critical condition of eavesdropping

immunity for this case is $\frac{\mathrm{SNR}_B}{\mathrm{SNR}_x} = 1$. Assuming all other parameters except d_x in (19) are known quantities, we obtain the eavesdropping distance limit d_{x_0} shown in (20). Similarly, we obtain the offset angle limit ϕ_{x_0} and the beamwidth limit $\xi_t^{i_0}$ shown in (21) and (22), respectively. ■

Hence, when $d_x > d_{x_0}$, $\phi_x > \phi_{x_0}$ or $\xi_t^i < \xi_t^{i_0}$, physical layer security and conventional encryption techniques for link i may be simplified in the mmWave network.

2) COLLUDING EAVESDROPPERS

Since the colluding eavesdroppers may gather their received information and send it to a central processor, we have $\mathrm{SNR}_E = \frac{\sum_{e\in\mathbb{Q}_E} P_r^e}{W_E}$ in this case [25], where W_E is the noise power. Note that the effect of signal phase is not considered here. Thus, the critical condition for a secure connection would be

$$\frac{\mathrm{SNR}_B}{\mathrm{SNR}_E} = \frac{G_{r,\max}^i \cdot d_i^{-n}}{\sigma_i^2} \cdot \frac{W_E}{\sum\limits_{e\in\mathbb{Q}_E} g\left(\phi_e\right) G_{r,\max}^e d_e^{-n}} = 1. \tag{23}$$

Specifically, the secrecy performance of link i is related to N_t^i, d_e, ϕ_e and $\mathbb{Q}_E$.

Proposition 6: Consider a legitimate link i in an mmWave network under passive eavesdropping scenario in beamspace with multiple colluding eavesdroppers of which the set is denoted by $\mathbb{Q}_E$. For eavesdropper e ($\forall e \in \mathbb{Q}_E$), the limits of eavesdropping parameters (i.e., d_x, ϕ_x, and ξ_t^i) are, respectively,

$$d_{e_0} = \left(\frac{g\left(\phi_e\right) \cdot G_{r,\max}^e}{\frac{G_{r,\max}^i \cdot W_E}{d_i^n \cdot \sigma_i^2} - \sum\limits_{x\in\mathbb{Q}_E\backslash e} \frac{g(\phi_x)\cdot G_{r,\max}^x}{d_x^n}} \right)^{1/n}, \tag{24}$$

$$\phi_{e_0} \Leftarrow \frac{\sin^2\left(N_t^i \pi \phi_{e_0}\right)}{\left(N_t^i \pi \phi_{e_0}\right)^2} = \frac{\frac{G_{r,\max}^i W_E}{d_i^n \sigma_i^2} - \sum\limits_{x\in\mathbb{Q}_E\backslash e} \frac{g(\phi_x) G_{r,\max}^x}{d_x^n}}{G_{r,\max}^e d_e^{-n}}, \tag{25}$$

$$\xi_t^{i_0} \doteq 1/N_t^{i_0}, \tag{26}$$

where

$$N_t^{i_0} \Leftarrow \frac{\sin^2\left(N_t^{i_0} \pi \phi_e\right)}{\left(N_t^{i_0} \pi \phi_e\right)^2} = \frac{\frac{G_{r,\max}^i W_E}{d_i^n \sigma_i^2} - \sum\limits_{x\in\mathbb{Q}_E\backslash e} \frac{g(\phi_x) G_{r,\max}^x}{d_x^n}}{G_{r,\max}^e d_e^{-n}}. \tag{27}$$

Proof: The critical condition for a secure connection is given in (23) for the passive eavesdropping scenario with colluding eavesdroppers. For each eavesdropper e ($e \in \mathbb{Q}_E$), assuming all other parameters except d_e in (23) are known quantities, we obtain the eavesdropping distance limit d_{e_0} shown in (24). Similarly, we obtain the offset angle limit ϕ_{e_0} and the beamwidth limit $\xi_t^{i_0}$ shown in (25) and (26), respectively. ■

In the case of colluding eavesdroppers, link i is secure if $\xi_t^i < \xi_t^{i_0}$, $d_e > d_{e_0}$ or $\phi_e > \phi_{e_0}$ for $\forall e \in \mathbb{Q}_E$.

B. ACTIVE EAVESDROPPING

Since eavesdroppers send interference signals while listening to the secret messages in this scenario, they will not only deteriorate the legitimate link, but also interfere with each other. Hence, the inter-beam interference should be taken into consideration. In this context, we have

$$\mathrm{SINR}_B = \frac{P_t^i \cdot G_{t,\max}^i \cdot G_{r,\max}^i \cdot \left(\frac{\lambda}{4\pi d_i^{n/2}}\right)^2}{\sum\limits_{e\in\mathbb{Q}_E} P_t^e G_{t,\max}^e G_{r,\max}^i g\left(\phi_2^e\right) \left(\frac{\lambda}{4\pi d_{e,B}^{n/2}}\right)^2 + \sigma_i^2}, \tag{28}$$

$$\mathrm{SINR}_e = \frac{P_t^i \cdot G_{t,\max}^i \cdot g\left(\phi_1^e\right) \cdot G_{r,\max}^e \cdot \left(\frac{\lambda}{4\pi d_{e,A}^{n/2}}\right)^2}{P_I^e + \sigma_e^2}, \tag{29}$$

where $P_I^e = \sum\limits_{x\in\mathbb{Q}_E\backslash e} P_t^x \cdot G_t^x\left(\phi_t^{x,e}\right) \cdot G_r^e\left(\phi_r^{x,e}\right) \cdot \left(\frac{\lambda}{4\pi d_{e,x}^{n/2}}\right)^2$ is the interference power of eavesdropper e; $d_{e,A}$, $d_{e,B}$ and $d_{e,x}$ are the distances between eavesdropper e and Alice, e and Bob, e and x ($x \in \mathbb{Q}_E\backslash e$), respectively; ϕ_1^e ($0 \le \left|\phi_1^e\right| \le \pi$) and ϕ_2^e ($0 \le \left|\phi_2^e\right| \le \pi$) are the offset angles of the receiving and transmitting beam of e relative to the boresight direction of link i, respectively; $\phi_t^{x,e}$ ($0 \le \left|\phi_t^{x,e}\right| \le \pi$) and $\phi_r^{x,e}$ ($0 \le \left|\phi_r^{x,e}\right| \le \pi$) are the offset angles of x's transmitting beam and e's receiving beam relative to the boresight direction of e and x, respectively.

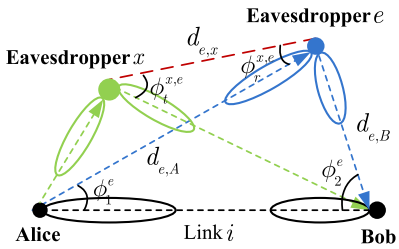


FIGURE 4. Illustration of the beam position relation between the legitimate link *i* and two active eavesdroppers *e* and *x*.

As illustrated in Fig. 4, according to the sine theorem and cosine theorem, respectively, we can obtain that

$$\frac{d_{e,A}}{\sin\phi_2^e} = \frac{d_{e,B}}{\sin\phi_1^e} = \frac{d_i}{\sin\left(\pi - \left|\phi_1^e\right| - \left|\phi_2^e\right|\right)}, \tag{30}$$

and

$$d_{e,x}^2 = d_{e,A}^2 + d_{x,A}^2 - 2d_{e,A}d_{x,A}\cos\left(\phi_1^e - \phi_1^x\right). \tag{31}$$

1) NON-COLLUDING EAVESDROPPERS

In this case, assuming that eavesdropper e ($e \in \mathbb{Q}_E$) is the most malicious eavesdropper, i.e., $\mathrm{SINR}_e = \max\limits_{x\in\mathbb{Q}_E} \mathrm{SINR}_x$,

we can derive the eavesdropping limits of e when the condition $\frac{\mathrm{SINR}_B}{\mathrm{SINR}_e}=1$ holds, i.e.,

$$A_1\cdot d_{e,A}^{n}-B_1\cdot g\left(\phi_1^e\right)=C_1\cdot P_t^e\cdot g\left(\phi_1^e\right)\cdot g\left(\phi_2^e\right)\cdot d_{e,B}^{-n}, \tag{32}$$

where $A_1=\frac{G_{r,\max}^{i}\cdot d_i^{-n}}{G_{r,\max}^{e}}\left(P_I^e+\sigma_e^2\right)$, $B_1=\sum\limits_{x\in\mathbb{Q}_E\setminus e}P_t^x\cdot G_{t,\max}^{x}\cdot G_{r,\max}^{i}\cdot g\left(\phi_2^x\right)\cdot\left(\frac{\lambda}{4\pi d_{x,B}^{n/2}}\right)^2+\sigma_i^2$, and $C_1=G_{t,\max}^{e}\cdot G_{r,\max}^{i}\cdot\left(\frac{\lambda}{4\pi}\right)^2$.

We see that the secrecy performance of link i mainly depends on N_t^i, N_r^i $d_{e,A}$, $d_{e,B}$, P_t^e, ϕ_1^e and ϕ_2^e.

Proposition 7: Consider a legitimate link i in an mmWave network under active eavesdropping scenario with multiple non-colluding eavesdroppers in beamspace. Denoting $\mathbb{Q}_E$ as the set of the potential eavesdroppers, if $\mathrm{SINR}_e=\max\limits_{x\in\mathbb{Q}_E}\mathrm{SINR}_x$, i.e., eavesdropper e is the most malicious eavesdropper in $\mathbb{Q}_E$, the limits of eavesdropping parameters (i.e., P_t^e, ϕ_1^e, ϕ_2^e, ξ_t^i, ξ_r^i, $d_{e,A}$, and $d_{e,B}$) are, respectively,

$$P_t^{e_0}=\frac{A_1\cdot d_{e,A}^{n}-B_1\cdot g\left(\phi_1^e\right)}{C_1\cdot g\left(\phi_1^e\right)\cdot g\left(\phi_2^e\right)\cdot d_{e,B}^{-n}}, \tag{33}$$

$$\phi_1^{e_0}\Leftarrow\frac{\sin^2\left(N_t^i\pi\phi_1^{e_0}\right)}{\left(N_t^i\pi\phi_1^{e_0}\right)^2}=\frac{A_1\cdot d_{e,A}^{n}}{C_1\cdot P_t^e\cdot g\left(\phi_2^e\right)\cdot d_{e,B}^{-n}+B_1}, \tag{34}$$

$$\phi_2^{e_0}\Leftarrow\frac{\sin^2\left(N_r^i\pi\phi_2^{e_0}\right)}{\left(N_r^i\pi\phi_2^{e_0}\right)^2}=\frac{A_1\cdot d_{e,A}^{n}-B_1\cdot g\left(\phi_1^e\right)}{C_1\cdot P_t^e\cdot g\left(\phi_1^e\right)\cdot d_{e,B}^{-n}}, \tag{35}$$

$$\xi_t^{i_0}\doteq\frac{1}{N_t^{i_0}}\Leftarrow\frac{\sin^2\left(N_t^{i_0}\pi\phi_1^e\right)}{\left(N_t^{i_0}\pi\phi_1^e\right)^2}=\frac{A_1 d_{e,A}^{n}}{C_1P_t^e g\left(\phi_2^e\right)d_{e,B}^{-n}+B_1}, \tag{36}$$

$$\xi_r^{i_0}\doteq\frac{1}{N_r^{i_0}}\Leftarrow\frac{\sin^2\left(N_r^{i_0}\pi\phi_2^e\right)}{\left(N_r^{i_0}\pi\phi_2^e\right)^2}=\frac{A_1\cdot d_{e,A}^{n}-B_1\cdot g\left(\phi_1^e\right)}{C_1\cdot P_t^e\cdot g\left(\phi_1^e\right)\cdot d_{e,B}^{-n}}, \tag{37}$$

and when $\Delta=b_1^2-4a_1\,c_1\geq 0$,

$$d_{e_0,A}=\left(\frac{-b_1+\sqrt{\Delta}}{2a_1}\right)^{1/n}, \tag{38}$$

$$d_{e_0,B}=\frac{\sin\phi_1^e}{\sin\phi_2^e}d_{e_0,A}, \tag{39}$$

where $a_1=A_1$, $b_1=-B_1\cdot g\left(\phi_1^e\right)$ and $c_1=-C_1\cdot P_t^e\cdot g\left(\phi_1^e\right)\cdot g\left(\phi_2^e\right)\cdot\frac{\sin^n\phi_2^e}{\sin^n\phi_1^e}$.

Proof: Since the secrecy performance of link i depends on the most malicious eavesdropper (e.g., e) in $\mathbb{Q}_E$ for non-colluding eavesdroppers, the critical condition of eavesdropping immunity here is $\frac{\mathrm{SINR}_B}{\mathrm{SINR}_e}=1$. Assuming all other parameters except P_t^e in (32) are known quantities, we obtain the transmission power limit $P_t^{e_0}$ shown in (33). Similarly, we obtain the offset angle limits $\phi_1^{e_0}$ and $\phi_2^{e_0}$ and the beamwidth limits $\xi_t^{i_0}$ and $\xi_r^{i_0}$ shown in (34)-(37), respectively. Moreover, substituting (30) into (32), we have a quadratic equation with one unknown about $d_{e,A}^n$ as

$$A_1\left(d_{e,A}^{n}\right)^2-B_1g\left(\phi_1^e\right)d_{e,A}^{n}-C_1P_t^e g\left(\phi_1^e\right)g\left(\phi_2^e\right)\frac{\sin^n\phi_2^e}{\sin^n\phi_1^e}=0. \tag{40}$$

Let $a_1=A_1$, $b_1=-B_1\cdot g\left(\phi_1^e\right)$ and $c_1=-C_1\cdot P_t^e\cdot g\left(\phi_1^e\right)\cdot g\left(\phi_2^e\right)\cdot\frac{\sin^n\phi_2^e}{\sin^n\phi_1^e}$, we obtain the eavesdropping distance limit $d_{e_0,A}$ shown in (38) if $\Delta=b_1^2-4a_1\,c_1\geq 0$. Then, according to (30), we obtain the eavesdropping distance limit $d_{e_0,B}$ shown in (39). ■

2) COLLUDING EAVESDROPPERS

Active eavesdropping with colluding eavesdroppers represents the worst-case scenario from the secure communication viewpoint, while it is the best-case scenario from the eavesdropper design viewpoint.

In this case, the eavesdroppers are assumed to have strong ability, and they may cooperate with each other to cancel the inter-beam interference [21], [26]. Then, the SINR expression formulated in (29) reduces to SNR. Thus, we have

$$\mathrm{SNR}_E=\frac{\sum\limits_{e\in\mathbb{Q}_E}P_t^iG_{t,\max}^{i}g\left(\phi_1^e\right)G_{r,\max}^{e}\left(\frac{\lambda}{4\pi d_{e,A}^{n/2}}\right)^2}{W_E}. \tag{41}$$

Let $\frac{\mathrm{SINR}_B}{\mathrm{SNR}_E}=1$, i.e.,

$$G_{r,\max}^{e}g\left(\phi_1^e\right)d_{e,A}^{-n}+C_2=\frac{A_2}{P_t^e g\left(\phi_2^e\right)d_{e,B}^{-n}C_1+B_1}, \tag{42}$$

we can obtain the following results shown in Proposition 8, where $A_2=G_{r,\max}^{i}\cdot d_i^{-n}\cdot W_E$ and $C_2=\sum\limits_{x\in\mathbb{Q}_E\setminus e}g\left(\phi_1^x\right)\cdot G_{r,\max}^{x}\cdot d_{x,A}^{-n}$.

Proposition 8: Consider a legitimate link i in an mmWave network under active eavesdropping scenario with multiple colluding eavesdroppers in beamspace, where $\mathbb{Q}_E$ denotes the set of the potential eavesdroppers. When the condition $\frac{\mathrm{SINR}_B}{\mathrm{SNR}_E}=1$ holds, we can derive the limits of eavesdropping parameters (i.e., P_t^e, ϕ_1^e, ϕ_2^e, ξ_t^i, ξ_r^i, $d_{e,A}$, and $d_{e,B}$) of eavesdropper e ($\forall e\in\mathbb{Q}_E$) as, respectively,

$$P_t^{e_0}=\frac{\frac{A_2}{G_{r,\max}^{e}\cdot g\left(\phi_1^e\right)\cdot d_{e,A}^{-n}+C_2}-B_1}{g\left(\phi_2^e\right)\cdot d_{e,B}^{-n}\cdot C_1}, \tag{43}$$

$$\phi_1^{e_0}\Leftarrow\frac{\sin^2\left(N_t^i\pi\phi_1^{e_0}\right)}{\left(N_t^i\pi\phi_1^{e_0}\right)^2}=\frac{\frac{A_2}{P_t^e\cdot g\left(\phi_2^e\right)\cdot d_{e,B}^{-n}\cdot C_1+B_1}-C_2}{G_{r,\max}^{e}\cdot d_{e,A}^{-n}}, \tag{44}$$

$$\phi_2^{e_0}\Leftarrow\frac{\sin^2\left(N_r^i\pi\phi_2^{e_0}\right)}{\left(N_r^i\pi\phi_2^{e_0}\right)^2}=\frac{\frac{A_2}{G_{r,\max}^{e}\cdot g\left(\phi_1^e\right)\cdot d_{e,A}^{-n}+C_2}-B_1}{C_1\cdot P_t^e\cdot d_{e,B}^{-n}}, \tag{45}$$

$$\xi_t^{i_0}\doteq\frac{1}{N_t^{i_0}}\Leftarrow\frac{\sin^2\left(N_t^{i_0}\pi\phi_1^e\right)}{\left(N_t^{i_0}\pi\phi_1^e\right)^2}=\frac{\frac{A_2}{P_t^e\cdot g\left(\phi_2^e\right)\cdot d_{e,B}^{-n}\cdot C_1+B_1}-C_2}{G_{r,\max}^{e}\cdot d_{e,A}^{-n}}, \tag{46}$$

$$\xi_r^{i_0} \doteq \frac{1}{N_r^{i_0}} \Leftarrow \frac{\sin^2\left(N_r^{i_0}\pi\phi_2^e\right)}{\left(N_r^{i_0}\pi\phi_2^e\right)^2} = \frac{\frac{A_2}{G_{r,\max}^e \cdot g\left(\phi_1^e\right)\cdot d_{e,A}^{-n}+C_2} - B_1}{C_1 \cdot P_t^e \cdot d_{e,B}^{-n}}, \tag{47}$$

and when $\Delta = b_2^2 - 4a_2\, c_2 \geq 0$,

$$d_{e_0,A} = \left(\frac{-b_2+\sqrt{\Delta}}{2a_2}\right)^{1/n}, \tag{48}$$

$$d_{e_0,B} = \frac{\sin\phi_1^e}{\sin\phi_2^e} d_{e_0,A}, \tag{49}$$

where $a_2 = (B_1\, C_2 - A_2)\frac{\sin^n\phi_1^e}{\sin^n\phi_2^e}$, $b_2 = B_1 \cdot G_{r,\max}^e \cdot g\left(\phi_1^e\right)\frac{\sin^n\phi_1^e}{\sin^n\phi_2^e} + C_1\, C_2 \cdot P_t^e \cdot g\left(\phi_2^e\right)$, and $c_2 = C_1 \cdot G_{r,\max}^e \cdot g\left(\phi_1^e\right)\cdot P_t^e \cdot g\left(\phi_2^e\right)$.

Proof: For active eavesdropping with colluding eavesdroppers, we assume that the eavesdroppers have strong ability to cancel the inter-beam interference by cooperating with each other. Then, the SINR expression in this case reduces to SNR according to (41). Meanwhile, the critical condition of eavesdropping immunity here is $\frac{\mathrm{SINR}_B}{\mathrm{SNR}_E} = 1$ which can be converted into (42). Assuming all other parameters except P_t^e in (42) are known quantities, we obtain the transmission power limit $P_t^{e_0}$ shown in (43). Similarly, we obtain the offset angle limits $\phi_1^{e_0}$ and $\phi_2^{e_0}$ and the beamwidth limits $\xi_t^{i_0}$ and $\xi_r^{i_0}$ shown in (44)-(47), respectively. Moreover, substituting (30) into (42), we have a quadratic equation with one unknown about $d_{e,A}^n$ as

$$a_2\left(d_{e,A}^n\right)^2 + b_2 d_{e,A}^n + c_2 = 0, \tag{50}$$

where the coefficients of the equation are shown in Proposition 8. Hence, we obtain the eavesdropping distance limit $d_{e_0,A}$ shown in (48) if $\Delta = b_2^2 - 4a_2\, c_2 \geq 0$. Then, according to (30), we obtain the eavesdropping distance limit $d_{e_0,B}$ shown in (49). ■

Therefore, if $\xi_t^i < \xi_t^{i_0}, \xi_r^i < \xi_t^{i_0}, d_{e,A} > d_{e_0,A}, d_{e,B} > d_{e_0,B}$, $P_t^e < P_t^{e_0}$, $\phi_1^e > \phi_1^{e_0}$ or $\phi_2^e > \phi_2^{e_0}$ for $\forall e \in \mathbb{Q}_E$, link i has eavesdropping immunity.

C. IMPACT OF EAVESDROPPER BLOCKAGE TO PHYSICAL LAYER SECURITY

In order to better achieve eavesdropping, some eavesdroppers in mmWave networks may trace and align their best eavesdropping direction through beamforming training if they have no the knowledge of the legitimate link (e.g., the exact location of the legitimate transceiver). Hence, they may unconsciously enter the coverage area of the transmitting beam of the legitimate link (e.g., link i) to overhear the secret messages, as shown in Fig. 5. Since mmWave radios have limited ability to diffract around obstacles, it is likely to cause signal shadowing that results in link blockage in this scenario. However, the shadow may alter the legitimate on eavesdropping. That is, once the eavesdropper or interference is detected, the original link will be greatly affected, and thus the blockage will play a vigilant role in enhancing security. This scenario is similar to that in quantum communications [27].

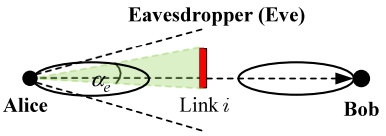


FIGURE 5. Illustration of the impact of the blockage from a potential eavesdropper (e.g., Eve) corresponding to a legitimate link (e.g., link *i* between Alice and Bob) in mmWave networks.

In this subsection, we analyze the impact of the blockage of eavesdropper e ($e \in \mathbb{Q}_E$, e.g., Eve shown in Fig. 5) on the secrecy performance of link i in a two-dimensional mode. The analysis is also applicable to the three-dimensional mode.

Denoting α_e as the shadowing angle of eavesdropper e corresponding to link i, the SINR of Bob in active eavesdropping scenarios can be estimated as

$$\mathrm{SINR}_B = \frac{\left(1-\frac{\alpha_e}{\xi_t^i}\right)\cdot P_t^i \cdot G_{t,\max}^i \cdot G_{r,\max}^i \cdot \left(\frac{\lambda}{4\pi d_i^{n/2}}\right)^2}{P_I^{i,e} + \sigma_i^2}, \tag{51}$$

where $P_I^{i,e} = P_t^e G_{t,\max}^e G_{r,\max}^i g\left(\phi_2^e\right)\left(\frac{\lambda}{4\pi d_{e,B}^{n/2}}\right)^2$ is the interference power of Bob received from Eve. Note that we have $P_I^{i,e} = 0$ in passive eavesdropping scenarios.

We assume that link i will be blocked if $\mathrm{SINR}_B < \gamma$, where γ is a given threshold for blockage events. When letting $\mathrm{SINR}_B = \gamma$, we can obtain the beamwidth limit of link i's transmitting beam for eavesdropping immunity.

Proposition 9: Consider a legitimate link i in an mmWave network with a potential eavesdropper e in active eavesdropping scenarios, where e is in the coverage area of the transmitting beam of link i. When the condition $\mathrm{SINR}_B < \gamma$ holds, we can derive the beamwidth limit $\xi_t^{i_0}$ as

$$\xi_t^{i_0} = \frac{\alpha_e}{1 - \frac{\gamma\cdot\left(P_I^{i,e}+\sigma_i^2\right)}{P_t^i\cdot G_{t,\max}^i\cdot G_{r,\max}^i\cdot\left(\frac{\lambda}{4\pi d_i^{n/2}}\right)^2}}. \tag{52}$$

Proof: Since $\xi_t^{i_0} = \max \xi_t^i$ for $\mathrm{SINR}_B < \gamma$, assuming all other parameters except ξ_t^i in (49) are known quantities, we obtain $\xi_t^{i_0}$ shown in (50). ■

Moreover, letting $P_I^{i,e} = 0$ in (50), we can get $\xi_t^{i_0}$ in passive eavesdropping scenarios.

Hence, when $\xi_t^i < \xi_t^{i_0}$, eavesdropper e with shadowing angle α_e will block link i, which makes it impossible to eavesdrop on the secret messages since the legitimate transmitter (e.g., Alice) will stop transmitting when the blockage event occurs. Compared with conventional microwave networks, this is an inherent property of physical layer security in mmWave networks.

V. NUMERICAL RESULTS

In what follows, we will present numerical simulation of the interference/eavesdropping immunity limits obtained by theoretical analysis in the mmWave network. In the following, we consider free space transmissions, i.e., the pathloss exponent n equals to 2 [4]. Meanwhile, to simplify simulation, we assume that $G^i_{t,\max} = G^j_{t,\max}$ $(\forall i, j \in \mathbb{N})$, $G^e_{r,\max} = G^i_{r,\max}$ and $\sigma_e^2 = \sigma_i^2$ $(\forall e \in \mathbb{Q}_E)$. It should be mentioned that the simulation results may be different with different parameter settings, but the curves with different parameters are consistent with the theoretical analysis.

A. INTER-BEAM INTERFERENCE LIMITS

In this subsection, assuming that $P_{I:j} = 0$ (i.e., there is only one interference link), we show the inter-beam interference limits of link j relative to link i, i.e., d_{i,j_0}, $P_t^{j_0}$, $\vartheta_1^{j_0}$, $\vartheta_2^{j_0}$, $\xi_t^{j_0}$, and $\xi_r^{i_0}$, changing with SINR threshold η. Here, link i is a reference link and link j is one of the potential interference links. In mmWave networks, when the transmitting beam of link j and the receiving beam of link i are in exactly the same or opposite direction, there are four typical inter-beam interference cases related to ϑ_1^j and ϑ_2^j, as illustrated in Fig. 6. Meanwhile, the main lobe of TX j acts as the main interfering signals in case (a), and the side lobes may be interfering signals in the other cases. Some simulation results in this study will be analyzed on the basis of these cases.

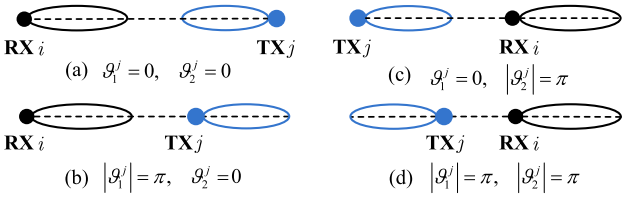


FIGURE 6. Four typical cases of inter-beam interference in mmWave networks.

Supposing $P_t^j = P_t^i$ $(i, j \in \mathbb{N}, j \neq i)$, when η and ϑ_1^j (or ϑ_2^j) are fixed, d_{i,j_0} generally decreases with increasing ϑ_2^j (or ϑ_1^j). For example, as given in Fig. 7(a), when $\eta = 20dB$ and $\vartheta_1^j = 0°$, we have $d_{i,j_0} = 1000m$ when $\vartheta_2^j = 0°$, while $d_{i,j_0} \approx 103m$ when $\vartheta_2^j = 15°$. Since the sinc antenna pattern is adopted to approximate the actual antenna pattern in this study, the normalized array gain fluctuates slightly with the increase of the azimuthal beam angle in side lobes, so that d_{i,j_0} is smaller when $\vartheta_2^j = 12°$ than that when $\vartheta_2^j = 15°$ here. Moreover, the value of d_{i,j_0} varies with η in the interference cases shown in Fig. 6(b)-(d) is given in Fig. 7(b). We see that $d_{i,j_0} \approx 0m$, meaning that link i has inherent interference immunity in these cases even if RX i and TX j are very close to each other.

As shown in Fig. 8(a), given that $d_{i,j} = d_i$ $(i, j \in \mathbb{N}, j \neq i)$, when η and ϑ_1^j are fixed, $P_t^{j_0}$ generally increases with increasing ϑ_2^j. Here, the roles of ϑ_1^j and ϑ_2^j are interchangeable. In particular, for the interference case with

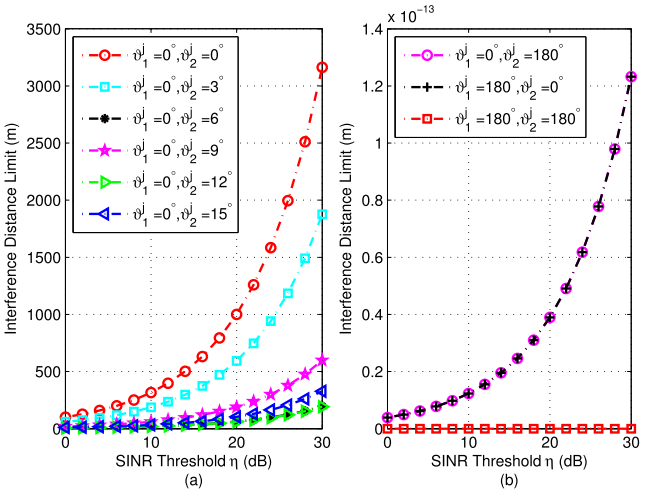


FIGURE 7. The interference distance limit d_{i,j_0} changes versus SINR threshold η with different ϑ_1^j and ϑ_2^j settings, given that $d_i = 100m$ and $N_t^j = N_r^i = 32$.

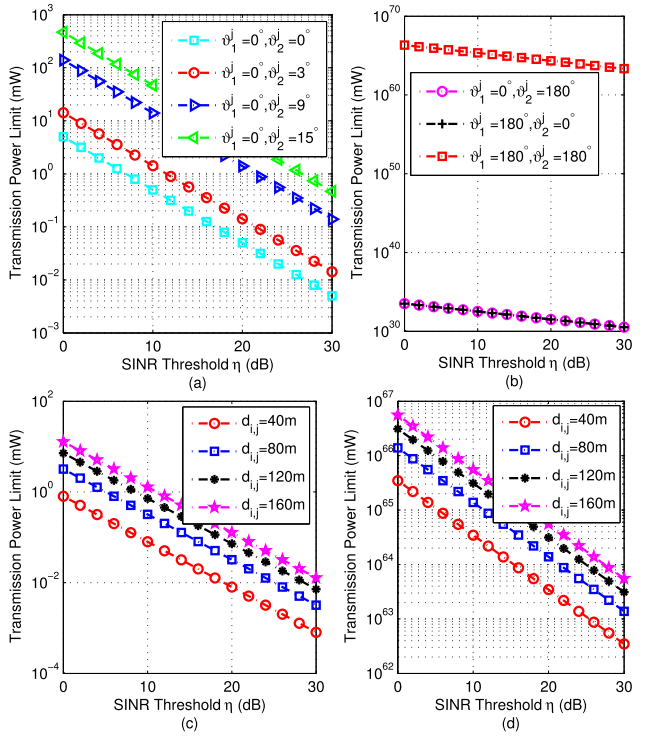


FIGURE 8. Given that $d_i = 100m$, $P_t^i = 5mW$ and $N_t^j = N_r^i = 32$, the transmission power limit $P_t^{j_0}$ changes versus SINR threshold η with different parameter settings: (a)-(b) $d_{i,j} = d_i$, (c) $\vartheta_1^j = \vartheta_2^j = 0°$, and (d) $|\vartheta_1^j| = |\vartheta_2^j| = \pi$.

$\vartheta_1^j = \vartheta_2^j = 0°$, link j with low transmission power P_t^j may cause interference to link i. For example, when $\eta = 20dB$, we have $P_t^{j_0} = 0.05mW$. However, for the interference case with $|\vartheta_1^j| = |\vartheta_2^j| = \pi$, link i is subject to interference only when P_t^j is very large, e.g., $P_t^{j_0} = 2.16 \times 10^{64} mW$

when $\eta = 20dB$, as seen in Fig. 8(b). Considering that power spectral density is regulated by spectrum management organizations (e.g., Federal Communications Commission), such a large transmission power is not allowed in an actual communication system. Thus, we generally have $P_t^j < P_t^{j0}$ in this case as well as in the cases shown in Fig. 6(b)-(c), i.e., link i has inherent interference immunity here. Further, Fig. 8(c) and (d) show P_t^{j0} changes versus η with different $d_{i,j}$ in the two cases, respectively. We see that P_t^{j0} increases with increasing $d_{i,j}$ when η, ϑ_1^j, and ϑ_2^j are fixed.

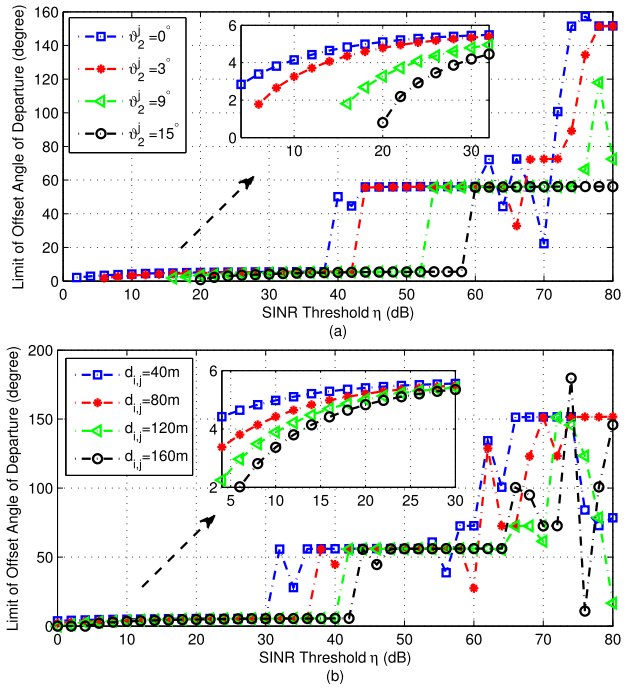


FIGURE 9. The limit of offset angle of departure $\vartheta_1^{j_0}$ changes versus SINR threshold η with different parameter settings: (a) $d_{i,j} = d_i$, (b) $\vartheta_2^j = 0°$, given that $d_i = 100m$ and $N_t^j = N_r^j = 32$.

Supposing $P_t^j = P_t^i$ $(i, j \in \mathbb{N}, j \neq i)$, Fig. 9(a) shows ϑ_1^{j0} changes versus η with different values of ϑ_2^j when $d_{i,j} = d_i$. In General, ϑ_1^{j0} increases with increasing η if ϑ_2^j is fixed. Moreover, as shown in Fig. 9(b), if ϑ_2^j is fixed (e.g., $\vartheta_2^j = 0°$), ϑ_1^{j0} generally increases with decreasing $d_{i,j}$. Note that the fluctuation of each curve is mainly caused by the fluctuation of the approximated side lobe gain in the sinc antenna pattern model. Similarly, we can get the changing trend of ϑ_2^{j0} versus η with different parameter settings.

Moreover, supposing $\vartheta_1^j = 0°$, the beamwidth limit ξ_r^{i0} changes versus η with different parameter settings is given in Fig. 10, where the change trend of ξ_r^{i0} with different values of ϑ_2^j is shown in Fig. 10(a) and that with different values of $d_{i,j}$ is shown in Fig. 10(b). Clearly, the larger the value of ϑ_2^j or $d_{i,j}$, the greater the value of ξ_r^{i0}. Similarly, we can get the changing trend of ξ_t^{j0} versus η with different parameter settings. When $\xi_r^i < \xi_r^{i0}$ or $\xi_t^j < \xi_t^{j0}$, the existing interference suppression/coordination techniques may be simplified or

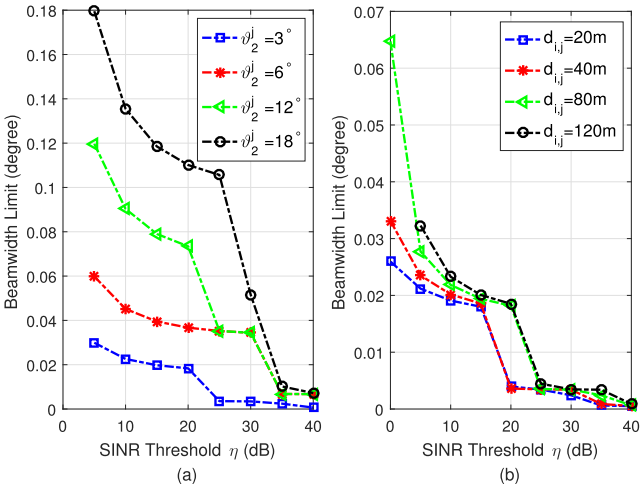


FIGURE 10. Given that $d_i = 100m$ and $\vartheta_1^j = 0°$, the beamwidth limit ξ_r^{i0} changes versus SINR threshold η with different parameter settings: (a) $d_{i,j} = d_i$, (b) $\vartheta_2^j = 3°$.

even omitted in mmWave systems. Further, the larger the beamwidth limit, the smaller the size of antenna array, and the less the design cost.

B. PHYSICAL EAVESDROPPING LIMITS

In this subsection, we present some numerical simulation results of the beamspace eavesdropping immunity limits of link j relative to link i in the passive eavesdropping scenario with multiple colluding/non-colluding eavesdroppers. Here, link i is the legitimate link and link j is one of the potential eavesdropping links.

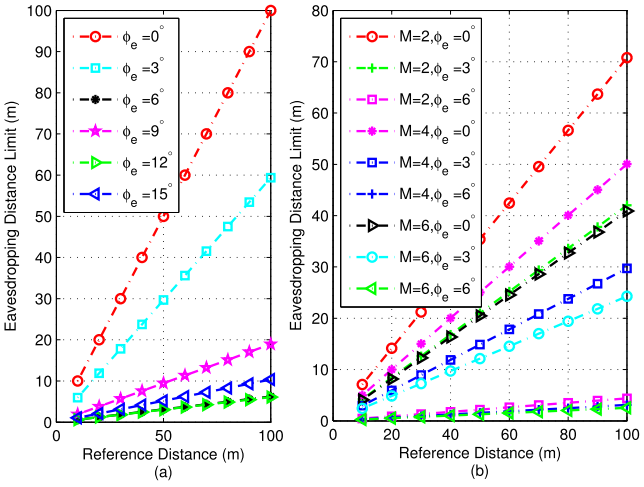


FIGURE 11. The eavesdropping distance limit d_{e_0} changes versus the reference distance d_i in passive eavesdropping scenario: (a) Non-colluding eavesdroppers, (b) Colluding eavesdroppers, given that $N_t^i = 32$, $d_x = d_i$ and $\phi_x = 6°$ for $\forall x \in \mathbb{Q}_E \backslash e$.

Assuming that eavesdropper e $(e \in \mathbb{Q}_E)$ is the most malicious eavesdropper in the passive eavesdropping scenario with non-colluding eavesdroppers, its eavesdropping distance limit d_{e_0} changing versus the reference distance d_i with different values of ϕ_e is given in Fig. 11(a). we see that d_{e_0} generally decreases with increasing ϕ_e for a fixed value

of d_i. Since we adopt the sinc antenna pattern in this study, there may be some special cases in simulations, e.g., the curve with $\phi_e = 15°$ is above that with $\phi_e = 6°$. Meanwhile, for the passive eavesdropping scenario with colluding eavesdroppers, the changing trend of d_{e_0} under different parameter settings is shown in Fig. 11(b), where M is the number of eavesdroppers in $\mathbb{Q}_E$. To simplify simulation, we assume that $d_x = d_i$ and $\phi_x = 6°$ for $\forall x \in \mathbb{Q}_E \backslash e$. We see that, for a fixed ϕ_e, the larger the value of M, the smaller the value of d_{e_0}. For example, when $d_i = 100m$ and $\phi_e = 3°$, we have $d_{e_0} = 42m$ if $M = 2$, while $d_{e_0} = 24m$ if $M = 6$. That is, the greater the number of colluding eavesdroppers, the stronger the eavesdropping capability, which is bad from the secure communication viewpoint. Furthermore, some simulation results of the offset angle limit ϕ_{e_0} changing versus d_e under different parameter settings in the passive eavesdropping scenario with non-colluding eavesdroppers and that with colluding eavesdroppers are given in Fig. 12. We see that ϕ_{e_0} decreases with increasing d_e for a fixed d_i, meaning that the larger the eavesdropping distance, the smaller the offset angle limit, then the stronger the ability to prevent eavesdropping for the legitimate link.

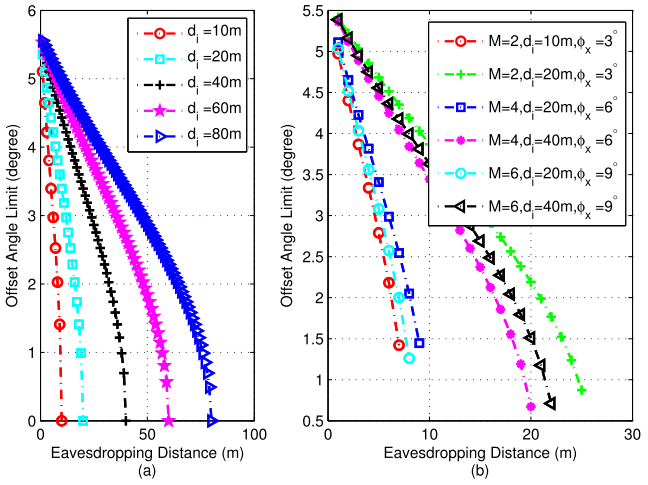


FIGURE 12. The offset angle limit ϕ_{e_0} changes versus eavesdropping distance d_e in passive eavesdropping scenario: (a) Non-colluding eavesdroppers, (b) Colluding eavesdroppers, given that $N_t^i = 32$, $d_x = 20m$ for $\forall x \in \mathbb{Q}_E \backslash e$.

Moreover, similar to the results in Fig. 10, the larger the eavesdropping distance d_e or the offset angle ϕ_e, the greater the eavesdropping beamwidth limit and, then, the smaller the limit of the size of antenna array. Further, according to the theoretical analysis given in Eq. (33)-(39) and Eq. (42)–(48), we can get the corresponding numerical results of the eavesdropping immunity limits (i.e., $P_t^{e_0}$, $\phi_1^{e_0}$, $\phi_2^{e_0}$, $\xi_t^{i_0}$, $\xi_r^{i_0}$, $d_{e_0,A}$, and $d_{e_0,B}$, for $e \in \mathbb{Q}_E$) under the active eavesdropping scenario with multiple colluding/non-colluding eavesdroppers. However, considering that the inter-beam interference environment is very complex and the reasonable parameter setting is very difficult in this scenario, we do not give the corresponding simulation results here.

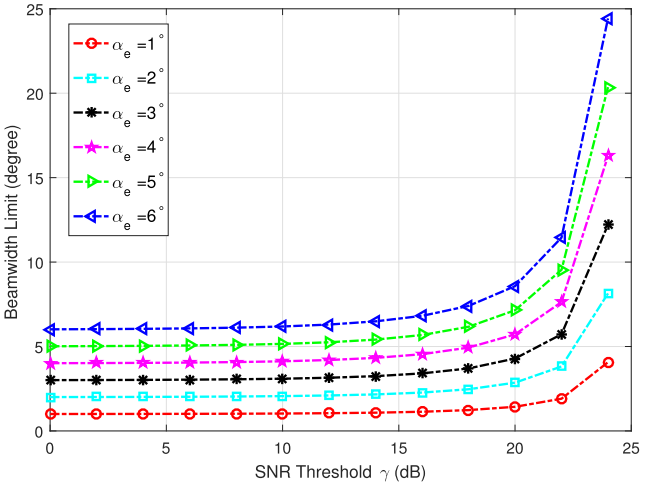


FIGURE 13. The beamwidth limit $\xi_t^{i_0}$ changes versus SNR threshold γ, given that $d_i = 100m$ and $P_t^i = 5mW$.

In order to evaluate the impact of the blockage of eavesdropper e on the secrecy performance of link i, we assume that $G_{t,\max}^i = G_{r,\max}^i = 40$dBi and set σ_i^2 [dB] $= -174$ [dBm/Hz] $+ 10\log_{10}(B) + NF$, where $NF = 6$dB is noise figure and $B = 1.5$GHz is the operating bandwidth. Furthermore, we consider the mmWave network operating in 60GHz band with $\lambda = 5mm$. In this context, the beamwidth limit $\xi_t^{i_0}$ in passive eavesdropping scenarios changes versus SNR threshold γ is given in Fig. 13. We see that $\xi_t^{i_0}$ increases with increasing γ for a fixed α_e. Meanwhile, when γ is fixed, the larger the value of α_e, the larger the value of $\xi_t^{i_0}$. For example, when $\gamma = 20$dB, we have $\xi_t^{i_0} = 1.4°$ when $\alpha_e = 1°$, while $\xi_t^{i_0} = 7.1°$ when $\alpha_e = 5°$. Eavesdropper e with shadowing angle α_e will block link i if $\xi_t^i < \xi_t^{i_0}$, meaning that link i has inherent eavesdropping immunity in this scenario. In addition, the impact of eavesdropper's blockage on physical layer security in mmWave networks under active eavesdropping scenarios is similar to that under passive eavesdropping scenarios.

VI. CONCLUSIONS

Thanks to directional transmissions with narrow beams, the inter-beam interference can be suppressed from neighbors effectively in mmWave networks. Thus, the efficiency of traditional interference coordination mechanisms and physical layer security techniques should be re-checked. However, there has been no work on giving the detailed analysis. In this context, we investigated the various performance limits of interference and physical layer eavesdropping immunity in mmWave networks by quantitative analysis. For each interference/eavesdropping link, when the actual interference/eavesdropping distance is greater than the interference/eavesdropping distance limit, the actual transmission power is lower than the transmission power limit, the actual offset angle is larger than the offset angle limit, or the actual beamwidth is smaller than the beamwidth limit, we found

that the mmWave network has interference/eavesdropping immunity. Moreover, some of the existing techniques for interference coordination and physical layer security may be simplified or even unnecessary in mmWave systems in certain conditions, and thus the corresponding design and implementation cost of wireless systems can also be reduced.

ACKNOWLEDGMENT

Q. Xue is currently with the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China.

REFERENCES

[1] Z. Pi and F. Khan, "An introduction to millimeter-wave mobile broadband systems," *IEEE Commun. Mag.*, vol. 49, no. 6, pp. 101–107, Jun. 2011.

[2] T. S. Rappaport *et al.*, "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, May 2013.

[3] S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter-wave cellular wireless networks: Potentials and challenges," *Proc. IEEE*, vol. 102, no. 3, pp. 366–385, Mar. 2014.

[4] M. Xiao *et al.*, "Millimeter wave communications for future mobile networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 9, pp. 1909–1935, Sep. 2017.

[5] K. Zheng, L. Zhao, J. Mei, M. Dohler, W. Xiang, and Y. Peng, "10 Gb/s hetsnets with millimeter-wave communications: Access and networking—Challenges and protocols," *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 222–231, Jan. 2015.

[6] P. Wang, Y. Li, L. Song, and B. Vucetic, "Multi-gigabit millimeter wave wireless communications for 5G: From fixed access to cellular networks," *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 168–178, Jan. 2015.

[7] S. Kutty and D. Sen, "Beamforming for millimeter wave communications: An inclusive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 949–973, 2nd Quart., 2016.

[8] M. Marcus and B. Pattan, "Millimeter wave propagation: Spectrum management implications," *IEEE Microw. Mag.*, vol. 6, no. 2, pp. 54–62, Jun. 2005.

[9] X. Yu, J. Zhang, M. Haenggi, and K. B. Letaief, "Coverage analysis for millimeter wave networks: The impact of directional antenna arrays," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 7, pp. 1498–1512, Jul. 2017.

[10] C. Wang and H.-M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5569–5585, Aug. 2016.

[11] Q. Xue, X. Fang, M. Xiao, and L. Yan, "Multiuser millimeter wave communications with nonorthogonal beams," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 5675–5688, Jul. 2017.

[12] Q. Xue, X. Fang, and C.-X. Wang, "Beamspace SU-MIMO for future millimeter wave wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 7, pp. 1564–1575, Jul. 2017.

[13] Q. Xue, X. Fang, and M. Xiao, "Beam management for millimeter wave beamspace MU-MIMO systems," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Oct. 2017, pp. 1–6.

[14] L. You, X. Gao, G. Y. Li, X.-G. Xia, and N. Ma, "BDMA for millimeter-wave/terahertz massive MIMO transmission with per-beam synchronization," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 7, pp. 1550–1563, Jul. 2017.

[15] X. Xiong, X. Wang, X. Gao, and X. You, "Beam-domain channel estimation for FDD massive MIMO systems with optimal thresholds," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4669–4682, Jul. 2017.

[16] S. Singh, R. Mudumbai, and U. Madhow, "Interference analysis for highly directional 60-GHz mesh networks: The case for rethinking medium access control," *IEEE/ACM Trans. Netw.*, vol. 19, no. 5, pp. 1513–1527, Oct. 2011.

[17] T. S. Rappaport, F. Gutierrez, Jr., E. Ben-Dor, J. N. Murdock, Y. Qiao, and J. I. Tamir, "Broadband millimeter-wave propagation measurements and models using adaptive-beam antennas for outdoor urban cellular communications," *IEEE Trans. Antennas Propag.*, vol. 61, no. 4, pp. 1850–1859, Apr. 2013.

[18] T. K. K. Tsang and M. N. El-Gamal, "Ultra-wideband (UWB) communications systems: An overview," in *Proc. IEEE 3rd Int. IEEE-NEWCAS Conf.*, Quebec City, Canada, Jun. 2005, pp. 381–386.

[19] H. Shokri-Ghadikolaei and C. Fischione, "The transitional behavior of interference in millimeter wave networks and its impact on medium access control," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 723–740, Feb. 2016.

[20] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[21] Y. Zhu, L. Wang, K. K. Wong, and R. W. Heath, Jr., "Secure communications in millimeter wave ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3205–3217, May 2017.

[22] Y. Ju, H. M. Wang, T. X. Zheng, and Q. Yin, "Secure transmissions in millimeter wave systems," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2114–2127, May 2017.

[23] P. C. Pinto, J. Barros, and M. Z. Win, "Wireless physical-layer security: The case of colluding eavesdroppers," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, South Korea, Jul. 2009, pp. 2442–2446.

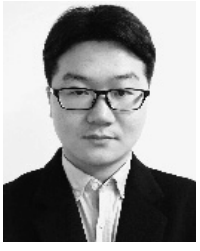
[24] A. Maltsev *et al.*, "Characteristics of indoor millimeter-wave channel at 60 GHz in application to perspective WLAN system," in *Proc. 4th Eur. Conf. Antennas Propag.*, Apr. 2010, pp. 1–5.

[25] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.

[26] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, Jun. 2014.

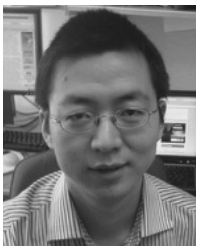
[27] M. Niemiec and A. R. Pach, "Management of security in quantum cryptography," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 36–41, Aug. 2013.

QING XUE received the B.E. degree in communication engineering from the University of Jinan, Jinan, China, in 2011, and the Ph.D. degree in information and communication engineering from Southwest Jiaotong University, Chengdu, China, in 2018. She joined the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China, in 2018, where she is currently a Lecturer. Her research interests include millimeter-wave wireless communications and radio resource management.



PEI ZHOU received the B.E. degree in communication engineering from Southwest Jiaotong University, Chengdu, China, in 2015, where he is currently pursuing the Ph.D. degree with the Key Laboratory of Information Coding and Transmission, School of Information Science and Technology. His research interests include 5G cellular networks, millimeter-wave wireless networks, radio resource management, and machine learning.

XUMING FANG received the B.E. degree in electrical engineering, the M.E. degree in computer engineering, and the Ph.D. degree in communication engineering from Southwest Jiaotong University, Chengdu, China, in 1984, 1989, and 1999, respectively. He was a Faculty Member with the Department of Electrical Engineering, Tongji University, Shanghai, China, in 1984. In 1985, he joined the School of Information Science and Technology, Southwest Jiaotong University, where he has been a Professor since 2001 and the Chair of the Department of Communication Engineering since 2006. He held visiting positions with the Institute of Railway Technology, Technical University of Berlin, Berlin, Germany, in 1998 and 1999, and also with the Center for Advanced Telecommunication Systems and Services, The University of Texas at Dallas, Richardson, in 2000 and 2001. He has, to his credit, around 260 high-quality research papers in journals and conference publications. He has authored or co-authored five books or textbooks. His research interests include wireless broadband access control, radio resource management, multihop relay networks, and broadband wireless access for high-speed railway. He is the Chair of the IEEE Vehicular Technology Society of Chengdu Chapter and an Editor of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.



MING XIAO received the bachelor's and master's degrees in engineering from the University of Electronic Science and Technology of China, Chengdu, in 1997 and 2002, respectively, and the Ph.D. degree from the Chalmers University of Technology, Sweden, in 2007. From 1997 to 1999, he was a Network and Software Engineer with ChinaTelecom. From 2000 to 2002, he also held a position with the Sichuan Communications Administration. Since 2007, he has been with the Department of Information Science and Engineering, School of Electrical Engineering and Computer Science, Royal Institute of Technology, Sweden, where he is currently an Associate Professor. He has been an Associate Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS since 2012 and the IEEE WIRELESS COMMUNICATIONS LETTERS from 2012 to 2016, and has been a Senior Editor of the IEEE COMMUNICATIONS LETTERS since 2015. He was the Lead Guest Editor of the IEEE JSAC Special issue on ''Millimeter Wave Communications for Future Mobile Networks'' in 2017.