Exploiting Multipath Terahertz Communications for Physical Layer Security in Beyond 5G Networks

Vitaly Petrov*, Dmitri Moltchanov*, Josep Miquel Jornet†, Yevgeni Koucheryavy*
*Tampere University, Finland
†University at Buffalo, The State University of New York, USA,
Email: *{vitaly.petrov, dmitri.moltchanov, evgeny.kucheryavy}@tuni.fi, †jmjornet@buffalo.edu

***Abstract*—Terahertz (THz) band communications, capable of achieving the theoretical capacity of up to several terabits-per-second, are one of the attractive enablers for beyond 5G wireless networks. THz systems will use extremely directional narrow beams, allowing not only to extend the communication range but also to partially secure the data already at the physical layer. The reason is that, in most cases, the Attacker has to be located within the transmitter beam in order to eavesdrop the message. However, even the use of very narrow beams results in the considerably large area around the receiver, where the Attacker can capture all the data. In this paper, we study how to decrease the message eavesdropping probability by leveraging the inherent multi-path nature of the THz communications. We particularly propose sharing the data transmission over multiple THz propagation paths currently available between the communicating entities. We show that, at a cost of the slightly reduced link capacity, the message eavesdropping probability in the described scheme decreases significantly even when several Attackers operate in a cooperative manner. The proposed solution can be utilized for the transmission of the sensitive data, as well as to secure the key exchange in THz band networks beyond 5G.**

I. Introduction

Terahertz band (0.3–10 THz) communication is the next frontier of wireless networks, allowing for data exchange at rates of up to several terabits-per-second [1]. The two major advances brought by the use of THz band on top of the fifth-generation (5G)-grade millimeter wave (mmWave) radio are: (i) active harnessing of wide frequency bands above 300 GHz [2]; and (ii) utilization of ultra-massive multiple input multiple output (MIMO) systems with theoretically up to several thousands of antenna elements [3]. These enhanced beyond 5G systems may not only improve the performance in existing use-cases, but also enable novel haptic services, such as data kiosk [4], massive augmented and virtual reality (AR/VR) [5], and tactile Internet [6], among others.

One of the first standards for the communications over the THz band has been released by IEEE in 2017 [7], with several others currently in development [8]. The research community is also making significant progress in designing the miniaturized hardware modules for the prospective THz band radio [9], channel and capacity modeling [10], [11], novel link-layer techniques [12], and enhanced system-level solutions [13], [14]. These efforts promise that commercial THz communications systems will appear in the near future [15].

To alleviate the effects of severe propagation losses, THz band systems are expected to rely upon extremely directional antenna radiation patterns providing noticeable gains at both transmit and receive sides [3]. Furthermore, the THz frequencies are naturally prone to blockage by both stationary and mobile objects in the channel, including building walls, vehicles, furniture, and even human bodies [14], [16]. This leads to complex dynamic multi-path propagation environment between the access point (AP) and the user equipment (UE) with a single line-of-sight (LoS) component and multiple non-line-of-sight (nLoS) reflected and scattered paths [11], [17]. To enable uninterrupted data transmission, the beamsteering mechanism has to be used to continuously select the path, currently characterized by the best signal-to-noise (SNR) ratio.

The use of extremely directional narrow beams brings inherent benefits to the physical layer security of mmWave and THz band communications [18]. The reason is that the Attacker has to physically be within the transmitting beam in order to decode any notable portion of data [19]. It has been particularly shown in [20] and [21] that the use of narrow beams together with the physical layer security-specific encoding allows to substantially decrease the probability of data to be eavesdropped in both LoS and nLoS conditions. Nevertheless, the perfect secrecy can still not be achieved, as the *"eavesdropping zone"* – the area, where the Attacker can successfully eavesdrop the data, is still relatively large [22].

There have been some techniques recently proposed to overcome this issue and reduce the size of the eavesdropping zone by sharing the secret communications with UE among several APs or several distant antenna arrays at a single AP [23]. Particularly, the envisioned distance between several antenna arrays at the THz band radio is shown to be insufficient for a significant spatial diversity of beams [24]. On its turn, as the channel conditions change rapidly [16], [25], the data sharing among several APs notably increases the system complexity by requiring real-time synchronization among several THz APs.

To overcome the abovementioned issues, *we propose and analyze an enhanced method to build a secure THz communications system by utilizing multiple propagation paths between a given AP and UE*. We particularly focus on the *multi-path* approach, where the node consequently transmits the different shares of the sensitive data over different propagation paths currently available towards the receiver (see Fig. 1). The data are encoded in a way that the receiver can decode the message only if it successfully receives *all* the shares. We show that although this scheme slightly reduces the link capacity versus

978-1-7281-1878-9/19/$31.00 ©2019 IEEE

the baseline *single-path* scheme (as the nLoS paths are also used even when the better LoS path is available), the message eavesdropping probability drastically decreases, even when attackers operate in a cooperative manner. To the best of authors' knowledge, this is one of the first studies addressing the security of the THz communications at the physical layer.

The contributions of this work are summarized as follows.

- *A mathematical framework* capable to characterize the message eavesdropping probability, the link capacity, and the secrecy rate of THz communications in typical outdoor urban deployments. The framework is flexible to account for the different number of THz multi-path components used for the data exchange, as well as for various crowd and attackers densities around UE.
- *A comparative analysis* of baseline *single-path* and proposed *multi-path* strategies for secure THz communications within our mathematical framework. The trade-offs between the performance-centric and security-centric metrics of interest are reported for a wide range of system and environment parameters.

The rest of the paper is organized as follows. The system model for our study is introduced in Sec. II. The mathematical framework to characterize the secrecy rate in our system and the trade-off between link capacity and eavesdropping probability is developed in Sec. III. The numerical results illustrating the introduced trade-offs between the secrecy level and the performance are discussed in Sec. IV. The conclusions are outlined in the last section.

II. System Model

In this section, we specify the system model by introducing its individual components. We start describing the deployment of interest, then proceed with the radio part describing propagation, blockage, antenna, and eavesdropping assumptions. Finally, we define the metrics of interest. The main notation used in the paper is summarized in the Table I.

1) Scenario and Deployment: We model a single communication link between a THz band AP at a height h_A (e.g., at the lamp post or on the wall) and a THz band UE at a height h_U, located d meters apart from the AP. There are two types of objects surrounding the UE: (i) humans, acting as blockers for THz propagation paths and (ii) attackers, eavesdropping all the data that passes through their location (see Fig. 1).

The humans are assumed to follow Poisson point process (PPP) in $\Re^2$ with the density of μ units per square meter. Humans are modeled by cylinders with height h_B and base radius r_B. The attackers are also deployed according to PPP in $\Re^2$ around the UE with the density λ. Both blockers and attackers are modeled to remain stationary during the entire data transmission, which is a realistic assumption, as the THz data frame duration is expected to be very short [2].

2) Propagation Model: The link between the AP and the UE involve N alternative paths that can be used to transmit the data (see Fig. 1). Each of the paths is characterized by its attenuation, zenith of arrival/departure (ZOA/ZOD) and azimuth of arrival/departure (AOA/AOD).

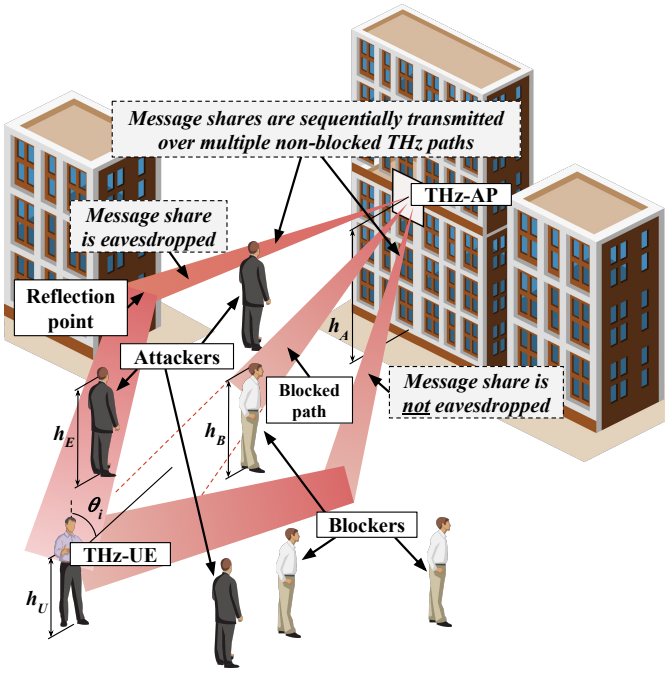


Fig. 1. Secure THz band communications in urban deployments.

The received power $P(x)$ is calculated following the THz band-specific model proposed in [26], while the individual attenuations of the multi-path components and ZOA follow the approximations from [27][1]. Each of the paths suffers from random blockages by humans surrounding the UE. As the THz signal gets significantly attenuated by the human body [15], the data transmission cannot be performed over the path if it is occluded. Thus, at a given time instant, only the currently non-blocked paths are assumed available for the data transmission.

3) Antenna Model: We assume planar antenna arrays at both AP and UE sides with the corresponding antenna gains G_A and G_U. For simplicity, we model the single-lobe cone-shape antenna radiation patterns following [28].

A viable approximation for the angular beam width α of a planar array is provided by $102°/L$, where L is the number of antenna elements in the appropriate plane [29]. Similarly, the linear gain can be approximated as [29]

$$G = \frac{1}{\theta^+ - \theta^-} \int_{\theta^-}^{\theta^+} \frac{\sin(L\pi\cos(\theta)/2)}{\sin(\pi\cos(\theta)/2)} d\theta, \qquad (1)$$

where $\theta^{\pm}$ are the beam angular points.

4) Security and Attackers Model: In this work, we analyze and compare two solutions for secure data transmission over the THz band. In the first solution, termed as *single-path*, the sensitive data gets transmitted as a single message over a single "best" path – the path currently associated with the greatest SNR. We compare the baseline single-path approach with the alternative solution, termed as *multi-path*, where

[1]Out of many available multi-path propagation models for mmWave and THz frequencies (e.g., [11], [17], [24], among others), the model from [27] provides the simplest, analytically-tractable expressions for ZOA and received power share in a random urban outdoor deployment, needed for our analysis.

TABLE I
NOTATION USED IN THE PAPER.

Parameter	Interpretation
h_A, h_U	THz-AP and THz-UE heights
λ	Spatial density of eavedroppers
μ	Spatial density of blockers
h_B, r_B	Blockers height and radius
h_E	Eavesdroppers height
L_A, L_U	Number of THz-AP and THz-UE antenna elements
G_A, G_U	THz-AP and THz-UE gains
α	Beamwidth of the THz-AP antenna radiation pattern
K	Attenuation caused by reflection
N	Total number of paths available at the UE
M	Number of paths used in *Multi-path* scheme, $M \leq N$
x	2D distance between THz-AP and THz-UE
d	3D distance between THz-AP and THz-UE
θ_i	Zenith of arrival angle of cluster i
$P_{S,i}$	Received power share of cluster i
P_i	Received power of cluster i
N_0	Johnson-Nyquist noise
$C(x)$	Shannon rate at distance x
$C_S(x)$	Secrecy rate at distance x
$l_{E,i}, w_{E,i}$	Length and width of eavesdropping zone of cluster i
$l_{B,i}, w_{B,i}$	Length and width of blockage zone of cluster i
$p_{B,i}$	Blockage probability of cluster i
$p_{E,i}$	Eavesdropping probability of cluster i
$q_{N,i}$	Probability of having i out of N clusters blocked
$v_{N,i}$	Eavesdropping probability with i out of N clusters blocked
p_E	Eavesdropping probability

the message containing the sensitive data gets split over M, $M \leq N$, strongest paths. The secure encoding is used so that the message can be decoded only if all the shares are received [20].

The role of attackers is to compromise the secrecy of the THz band communications. In this work, we assume passive attackers, who eavesdrop all the messages passing around them but do not block the signal or modify any data. We also assume that all the attackers operate in a cooperative manner, that is, the message share is assumed eavesdropped if it is captured by at least a single attacker. The attackers successfully eavesdrop the message if they capture all of the message shares.

5) Metric of Interest: We concentrate on characterizing the trade-off between eavesdropping probability, p_E, and link capacity at the air interface, $C(x)$ between AP and UE located at two-dimensional (2D) distance x. The former is defined as the probability that a field of attackers are capable of overhearing the ongoing transmission.

For the single-path scheme, the link capacity is assumed to equal the Shannon rate of the path with the greatest SNR out of all currently available non-blocked paths. For the multi-path scheme, the link capacity is defined as a Shannon rate over M currently non-blocked paths used for the data exchange, i.e.,

$$C(x) = \frac{B}{M} \sum_{i=1}^{M} \log_2 \left(1 + S_i(x)\right), \tag{2}$$

where S_i $i = 1, 2, \ldots, M$ are the SNR values at the distance x over over the path i. Finally, we also characterize the secrecy rate, $C_S(x)$, defined as the rate of data not eavesdropped by the attackers.

III. Secrecy and Performance Analysis

In this section, we develop a model for assessing the trade-off between eavesdropping probability and achieved data rate. We first characterize blockage and eavesdropping probabilities for individual paths and then proceed with metrics of interest.

A. Eavesdropping Zones for THz Multipath Propagation

In order to eavesdrop the message, the attacker has to be physically located within the transmitting beam. Therefore, the size of the eavesdropping zone – the ground-level 2D zone around the UE, where the attacker has to stay in order to still be within the transmitting beam – can be calculated from the deployment parameters, as detailed in this subsection. For the first-order analysis, we approximate the eavesdropping zone for the path i with a rectangle $l_{E,i} \times w_{E,i}$, where $w_{E,i}$ is determined by the actual width (in meters) of the AP beam around UE, while $l_{E,i}$ is defined by the AP beam elevation around UE and the eavesdroppers height, see Fig. 2.

For the antenna model, discussed in Section II, the width of the eavesdropping zone for the LoS path, $w_{E,1}$, can be estimated as follows, see Fig. 2(a),

$$w_{E,1} = d \tan(\alpha/2), \tag{3}$$

where d is the three-dimensional (3D) distance between the AP and UE and α is the AP beamwidth.

Then, the length of the eavesdropping zone for the LoS case, $l_{E,1}$ is derived from the scenario geometry as

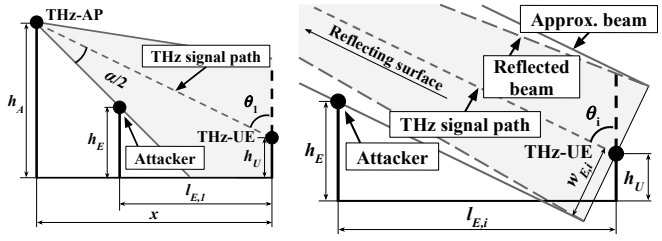
$$l_{E,1} = x - (h_A - h_E) \tan(\theta_1 - \alpha/2), \tag{4}$$

where x is 2D distance between the AP and the UE nodes, h_A is the AP height, h_E is the eavesdropper height, and θ_1 is the line-of-sight zenith angle of arrival.

The model in [27] does not provide the exact number of reflections and scatterings for a given path. We construct an approximation assuming one reflection and no scattering for the nLoS path. This approximation upper bounds the size of the eavesdropping zone. *In practice, the zone can be smaller as there can be more than one reflection on the nLoS path.*

The spatial density of the received power from the nLoS path is inversely proportional to the width of the beam going over this path. Therefore, the eavesdropping zone width for nLoS path can be calculated as

$$w_{E,i} = d \tan(\alpha/2) \sqrt{P_{S,1}/(P_{S,i}K)}, \tag{5}$$



(a) LoS path, $i = 1$ (b) nLoS path, $i > 1$

Fig. 2. Projections of the eavesdropping zones for LoS and nLoS cases.

where $P_{S,1}$ is the LoS power share, $P_{S,i}$ is the random variable (RV) representing the power share of the i-s nLoS path. Here, K is the additional attenuation caused by the reflection from the object. K is at least 10 dB for the typical materials [14].

Consequently, the approximate length of the eavesdropping zone, $l_{E,i}$ can be derived as follows, see Fig. 2(b),

$$l_{E,i} = (h_E - h_U)\tan(\theta_i) + w_{E,i}/\cos(\theta_i), \tag{6}$$

where h_U is the UE height and θ_i is an RV representing the current ZOA for the selected path.

For the PPP field of attackers, we derive the eavesdropping probability for the path i, $p_{E,i}$, as the probability that at least a single attacker is located in the corresponding zone as, i.e,

$$p_{E,i} = 1 - e^{-\lambda w_{E,i} l_{E,i}},\ i = 1,2,\ldots,N. \tag{7}$$

B. Blockage Zones for THz Multipath Propagation

Let $p_{B,i}$ be the probability that the i-th communication path between AP and UE is blocked and consider blockage of LoS path, $p_{B,1}$, first. For a certain 2D distance x between AP and UE, we observe that there is always the so-called *LoS blockage zone* as shown in Fig. 3. Using geometric arguments, the width and length of the LoS blockage zone are

$$w_{B,1} = 2r_B,\ l_{B,1} = \left(x\frac{h_B - h_U}{h_A - h_U} + r_B\right), \tag{8}$$

where r_B is the radius of the human blocker.

Using the void probability for the PPP of blockers, we have

$$p_{B,1} = 1 - e^{-2\mu r_B\left[x\frac{h_B - h_U}{h_A - h_U} + r_B\right]}. \tag{9}$$

Let $\theta_i(x)$, $i = 2,3,\ldots,N$, be the RVs denoting ZOA. Consider now the blockage probability for the i-th path, $p_{B,i}$, $i = 2,3,\ldots$. As shown in [27], ZOA of the path i can be approximated by Laplace distribution with the probability density function (pdf)

$$f_{\theta_i}(y;x) = \frac{1}{2b_i(x)} e^{-\frac{|y - a_i(x)|}{b_i(x)}},\ y \in [0;\pi),\ i = 2,3,\ldots, \tag{10}$$

where y is the corresponding ZOA value and $a^{(i)}(x)$, $b^{(i)}(x)$, $i = 2,3,\ldots,N$, are the parameters.

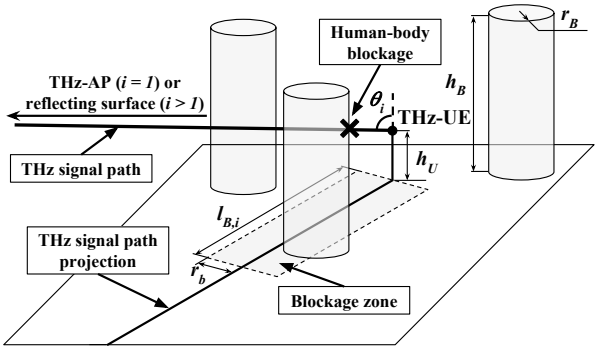


Fig. 3. Blockage zone geometry for LoS and nLoS cases.

Following [27], $a_i(x)$ is independent of the path number i and depends on the separation distance x only: $a_i(x) = a_j(x)$, $\forall i,j = 2,3,\ldots,N$. Furthermore, the mean of ZOA for all the paths coincides with the ZOA of the LoS path. In the contrary, $b_i(x)$ is independent of the distance and depends on the path index i only.

Similarly to the LoS path, for any given ZOA value y_i of the path i, $i = 2,3,\ldots,N$, we define *path i blockage zone*. Using geometric arguments, see Fig. 3, for path i we have [30].

$$p_{B,i}(y;x) = 1 - e^{-2\lambda_B r_B(\tan y_i(h_B - h_U) + r_B)}. \tag{11}$$

Accounting for pdf of θ_i we get

$$p_{B,i}(x) = \int_0^\pi f_{\theta_i}(y;x) p_{B,i}(y;x)dy, \tag{12}$$

that can be evaluated numerically.

C. Clusters Capacity

Having characterized the blockage probabilities of individual clusters of AP to UE link, we now proceed deriving the capacity of individual clusters. Below, we first characterize the received power and then provide the sought capacity.

The fraction of power from the cluster over the i-th path, $P_{S,i}$, $i = 1,2,\ldots$, follows Log-normal distribution with pdf

$$f_{P_{S,i}}(y;x) = \frac{1}{y d_i\sqrt{2\pi}} e^{-\frac{(\ln y - c_i)^2}{2d_i^2}},\ i = 1,2,\ldots,N, \tag{13}$$

where c_i, d_i, $i = 2,3,\ldots$, are parameters. Both c_i and d_i are independent of x and depend on the path index i only [27].

The received power from every cluster is calculated as

$$P_i(x) = P_{S,i} 10^{(P_T + G_A + G_U - T(x))/10},\ i = 1,2,\ldots,N, \tag{14}$$

where P_T is transmit power and T is the path loss, G_A and G_U are the AP transmit and UE receive antenna array gains. Substituting the path loss at low THz frequencies we have

$$P_i(x) = P_{S,i} 10^{\frac{P_T + G_A + G_U - 20\log_{10} f_c - 20\log_{10} x - 10kx/\ln(10) - 147.55}{10}}, \tag{15}$$

where f_c is the frequency, and k is the absorption coefficient.

Accounting for (13) the received power over a path i is

$$f_{P_i}(y;x) = f_{P_{S,i}}(y/A(x);x), \tag{16}$$

where $A(x) = 10^{\frac{P_T + G_A + G_U - 20\log_{10} f_c - 20\log_{10} x - 10kx/\ln(10) - 147.55}{10}}$.

Having obtained the received power over the path i, the Shannon rate for the path i can be written as

$$C_i(x) = B\log_2(1 + P_i(x)/N_0),\ i = 1,2,\ldots,N, \tag{17}$$

where N_0 is the Johnson-Nyquist noise over the bandwidth B.

Note that $C_i(x)$ are all non-linear functions of RVs P_i, $i = 1,2,\ldots,N$. Following [31], pdf of a RV Y, $w(y)$, expressed as function $y = \phi(x)$ of another RV X with pdf $f(x)$ is

$$w(y) = \sum_{\forall j} f(\psi_j(y))|\psi_j'(y)|, \tag{18}$$

where $x = \psi_j(y) = \phi^{-1}(x)$ is the inverse functions.

$$C(x)=\prod_{j=1}^{3}(1-p_{B,j})\frac{1}{3}[C_1(x)+C_2(x)+C_3(x)]+p_{B,3}\prod_{j=1}^{2}(1-p_{B,j})\frac{1}{2}[C_1(x)+C_2(x)]+p_{B,1}\prod_{j=2}^{3}(1-p_{B,j})\frac{1}{2}[C_2(x)+C_3(x)]$$
$$+p_{B,2}\prod_{j=1,3}(1-p_{B,j})\frac{1}{2}[C_1(x)+C_3(x)]+(1-p_{B,1})\prod_{j=2}^{3}p_{B,j}C_1(x)+(1-p_{B,3})\prod_{j=1}^{2}p_{B,j}C_3(x)+(1-p_{B,2})\prod_{j=1,3}p_{B,j}C_2(x). \quad (24)$$

The inverse branch of interest of the Shannon rate function and its derivative are given by

$$\psi(y)=N_0(2^{y/B}-1),\ \psi'(y)=N_0\log(2)2^{y/B}/B, \quad (19)$$

leading to rate pdf in the following form

$$f_{C_i}(y;x)=\frac{A(x)\log(2)2^{\frac{y}{B}}}{B(2^{\frac{y}{B}}-1)d_i\sqrt{2\pi}}e^{-\frac{(\ln\frac{N_0(2^{y/B}-1)}{A(x)}-c_i)^2}{2d_i^2}},\ i=1,2,.. \quad (20)$$

D. Capacity and Eavesdropping Probability

We now proceed deriving the capacity and eavesdropping probabilities of THz communications for both single-path and multi-path transmission schemes.

1) Shannon capacity: Recall that in the single-path transmission scheme AP and UE always operate using the path having the highest received power. Sorting the paths in descending order of their means, we get the following approximation for Shannon capacity of the single-path scheme

$$C(x)=\sum_{i=1}^{M}\left[\prod_{j=1}^{i-1}p_{B,j}\right](1-p_{B,i})C_i(x). \quad (21)$$

Observe that in (21) the rate is expressed as a sum of weighted components. To obtain the pdf of $C(x)$ one may use the convolution of individual components $C_i(x)$ directly in RV domain or, alternatively, using Laplace transform. However, recalling the property of the mean value, we have

$$E[C(x)]=\sum_{i=1}^{M}\left[\prod_{j=1}^{i-1}p_{B,j}\right](1-p_{B,i})\int_0^{\infty}f_{C_i}(y;x)ydy, \quad (22)$$

that can be evaluated numerically.

Estimating capacity for the multi-path scheme, where a number of paths are simultaneously used for communications, is a more involved process. Considering the case of $M=2$ and concentrate on estimating the capacity, we have

$$C(x)=(1-p_{B,1})(1-p_{B,2})\frac{1}{2}[C_1(x)+C_2(x)]+$$
$$+(1-p_{B,1})p_{B,2}C_1(x)+p_{B,1}(1-p_{B,2})C_2(x). \quad (23)$$

For $M=3$, we have (24). One may obtain similar expressions for any $M>3$. However, for large values of M, e.g., $M=20$, the calculations become unmanageable. In this case, we propose to rely upon the following approximation. Recall, that $M\le N$ and the mean ZOA of path i, $i=2,3,\ldots,N$ coincides with the LoS ZOA. This implies that $p_{B,i}\approx p_{B,j}=p_B$, $\forall i,j=1,2,\ldots,N$. Although we still need to distinguish between the paths, the probability of choosing any combination of paths is independent of their indexes. Thus, the probability of having i out of M paths non-blocked, $q_{M,i}$, follows a Binomial probability mass function

$$q_{M,i}=\binom{M}{i}(1-p_B)^i p_B^{M-i},\ i=1,2,\ldots,M. \quad (25)$$

Using this approximation, we have for $M=2$

$$C(x)=q_{2,1}\frac{C_1(x)}{2}+q_{2,1}\frac{C_2(x)}{2}+q_{2,2}\left(\frac{C_1(x)}{2}+\frac{C_2(x)}{2}\right). \quad (26)$$

Similarly, for $M=3$ we arrive at

$$C(x)=\frac{1}{3}q_{3,1}\sum_{i=1}^{3}C_i(x)+\frac{1}{3}q_{3,2}\Big[\frac{1}{2}(C_1(x)+C_2(x))+\frac{1}{2}(C_2(x)$$
$$+C_3(x))+\frac{1}{2}(C_1(x)+C_3(x))\Big]+\frac{1}{3}q_{3,3}\sum_{i=1}^{3}C_i(x). \quad (27)$$

Now, consider the contribution of an arbitrarily chosen path i to the achieved capacity. Observe that when j paths are non-blocked and LoS path is one of them, the share of time it is used for transmission is $1/j$. The overall number of combinations how to choose j out of M paths is $\binom{M}{j}$, while the number of times path i appears in these combinations is $\binom{M-1}{j-1}$. Summing up over all possible numbers of non-blocked paths with corresponding Binomial probabilities, we get the following expression for the capacity of the multi-path scheme

$$C(x)=\sum_{i=1}^{M}\sum_{j=1}^{M}q_{M,j}\frac{\binom{M-1}{j-1}}{\binom{M}{j}}\frac{1}{j}C_i(x)=\frac{1-p_B^M}{M}\sum_{i=1}^{M}C_i(x). \quad (28)$$

Similarly to the single-path model, the capacity expression takes the form of weighted sum of rates. The mean value of the rate at the distance x is thus immediately given by

$$E[C(x)]=\frac{1-p_B^M}{M}\sum_{i=1}^{M}\int_0^{\infty}f_{C_i}(y;x)ydy. \quad (29)$$

2) Eavesdropping Probability: To estimate the eavesdropping probability we need to take into account the eavesdropping zone for LoS path is different from the rest of the paths. Furthermore, recall that we are interested in eavesdropping probability conditioned on at least one path non-blocked at UE. The latter probability is given by $1-\prod_{i=1}^{M}p_{B,i}$.

Observe that the probability that the path i is currently in use is $(1-p_{B,i})\prod_{j=1}^{i-1}p_{B,j}$. Thus, the probability that path i is currently in use and eavesdropped is $(1-p_{B,i})p_{E,i}\prod_{j=1}^{i-1}p_{B,j}$. Summing over non-blocked paths we get

$$p_E=\frac{\sum_{i=1}^{M}\left((1-p_{B,i})p_{E,i}\prod_{j=1}^{i-1}p_{B,j}\right)}{1-\prod_{i=1}^{M}p_{B,i}}, \quad (30)$$

where $p_{E,i}$ is eavesdropping probability for the path i.

Similarly to the capacity calculations, the eavesdropping probability for the described multi-path scheme can be estimated differentiating between the blockage probabilities for different paths, $p_{B,i}$, $i = 1,2,\ldots,M$. Let $v_{M,i}$ be the probability that i paths are currently non-blocked, and there is at least one eavesdropper in all the zones for all the paths in use. Let $v_{M,0}$ be the probability that there are no non-blocked paths. Then

$$\begin{aligned} &v_{1,0} = p_{B,1},\, v_{1,1} = (1-p_{B,1})p_{E,1},\\ &v_{2,0} = p_{B,1}p_{B,2},\, v_{2,1} = v_{1,1}p_{B,2} + v_{1,0}(1-p_{B,2})p_{E,2},\\ &\ldots, \end{aligned} \tag{31}$$

leading to the following recursion

$$v_{M,i} = v_{M-1,i-1}(1-p_{B,M})p_{E,M} + v_{M-1,i}p_{B,M}. \tag{32}$$

Finally, the eavesdropping probability is derived as

$$p_E = \frac{\sum_{i=1}^{M} v_{M,i}}{1-\prod_{i=1}^{M} p_{B,i}}, \tag{33}$$

while the secrecy rate $C_S(x)$ is given by $C_S(x) = (1-p_E)C(x)$.

Observe that differentiating between cluster blockage probabilities, only recurrent expression can be provided. Assuming that $p_{B,i} \approx p_{B,j} = p_B$, $\forall i,j = 1,2,\ldots,N$, and differentiating between eavesdropping probability of LoS cluster and other clusters, $p_{E,1} = p_{E,L}$, $p_{E,i} = p_{E,nL}$, $i = 2,3,\ldots,N$, a simple approximation can be provided. Particularly, in this case the probability that i out of M clusters are currently non-blocked is provided in (25). For any i non-blocked clusters, the probability that LoS cluster blocked is $\frac{M-1}{M}\frac{M-2}{M-1} \times \cdots \times \frac{M-i}{M-i+1} = \frac{M-i}{M}$. Alternatively, LoS cluster is non-blocked is just i/M. Combining these results one arrives at the following approximation

$$p_E = \frac{\sum_{i=1}^{M} q_{M,i}\left(\frac{M-i}{M}p_{E,nL}^{i} + \frac{i}{M}p_{E,L}p_{E,nL}^{i-1}\right)}{1-\prod_{i=1}^{M} p_{B,i}}. \tag{34}$$

IV. Numerical Assessment

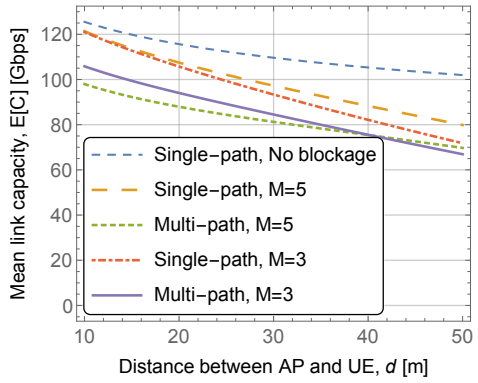
In this section, we characterize the trade-off between the achieved capacity and eavesdropping probability for the single-path and multi-path schemes as a function of system parameters. The system parameters are summarized in Table II.

1) The link capacity: We start characterizing the link capacity (Shannon rate) for both single-path and multi-path schemes as a function of system parameters illustrated in Fig. 4. Particularly, Fig. 4(a) shows the link capacity as a function of the distance between AP and UE for both schemes and the different number of paths maintained at UE, $M = 3$ and $M = 5$. An upper capacity bound for the baseline single-path scheme without blockers, i.e., $\mu = 0$, is also highlighted. Expectedly, in the presence of blockers, the capacity of both schemes get severely compromised. Furthermore, as one may observe, the difference between the single-path and the multi-path schemes is only noticeable up to approximately 40–50 m of the separation distance between AP and UE. For $d > 50$ m, the LoS path is characterized by high blockage probability, so the dominating effect of this path becomes less profound.

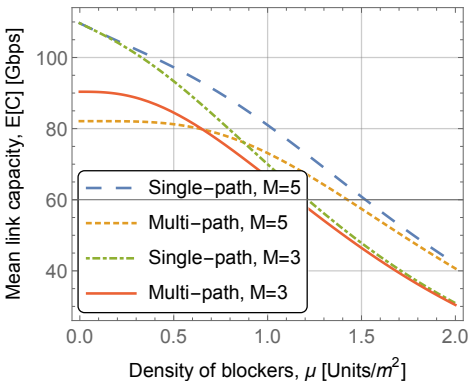
TABLE II
Default system parameters.

Parameter	Value
Carrier frequency, f_c	300 GHz
Bandwidth, B	5 GHz
Transmit power, P_T	0 dBm
AP height, h_A	5 m
UE height, h_U	1.5 m
Blockers height, h_B	1.7 m
Blockers radius, r_B	0.3 m
Eavesdroppers height, h_E	1.7 m
Default spatial blockers density, μ	0.5 bl./m^2
Default spatial eavesdroppers density, λ	0.01 eav./m^2
AOA, ZOA, power share	Parameterized following [27]
AP antenna array elements, L_A	{512, 1024, 2048}
UE antenna array	128×128 elements ($L_U = 128$)

The inherent multi-path diversity of terahertz communications plays a critical role in achieved link capacity. Particularly, as evident from Fig. 4(a), allowing UE to use more paths result in better performance for the single-path scheme for all the considered values of d. Furthermore, the difference increases with the distance as the probability of using LoS path decreases due to the blockage. This behavior is also valid for the multi-path scheme and for large distances between AP and UE, i.e., starting from $d \approx 40$ m. For smaller values of

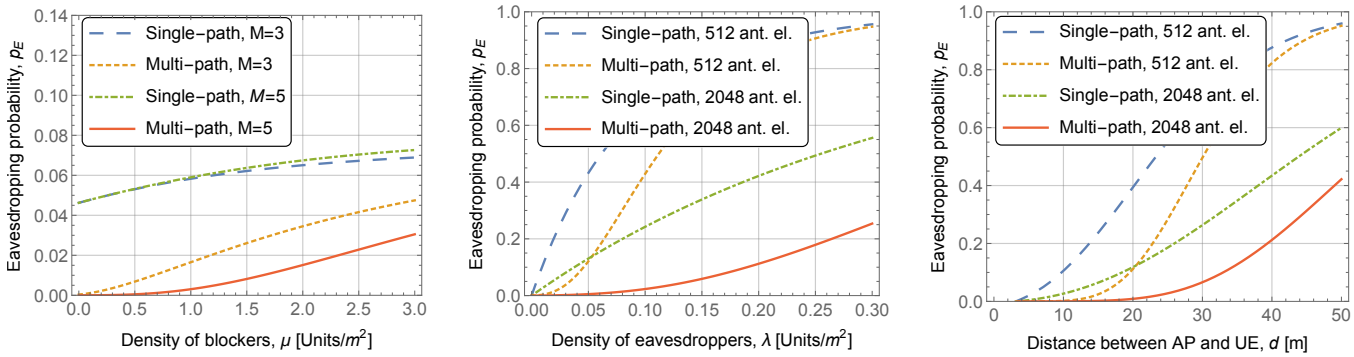


(a) $L_A = 1024$, $\mu = 0.5$



(b) $L_A = 1024$, $d = 30$ m

Fig. 4. THz communications capacity for *Single-path* and *Multi-path* schemes.



(a) $L_A = 1024$, $d = 10$, $\lambda = 0.01$ (b) $\mu = 0.5$, $d = 10$, $M = 5$ (c) $\mu = 0.5$, $\lambda = 0.01$, $M = 5$

Fig. 5. THz communications eavesdropping probability for *Single-path* and *Multi-path* schemes.

d the effect is reversed. The main reason here is again the dependence of the paths blockage zones sizes on d. When d is small, the probability that all the paths are non-blocked is high for both $M = 3$ and $M = 5$ implying that the contribution of the LoS path to the overall capacity is higher for $M = 3$. As d increases, blockage probability for the LoS path increases, thus, reducing the role of this path for the link capacity.

Consider now the effect of spatial blockers density, μ, on the Shannon rate illustrated in Fig. 4(b). Logically, for the small values of μ, the link capacity of baseline schemes coincide, as the LoS path is used almost all the time. For larger values of μ, the rate starts to deviate drastically, as the probability of simultaneously blocking 3 paths becomes much smaller than the corresponding probability for $M = 5$. Furthermore, the difference between the link capacities for the considered schemes decreases with the growth of the blockers density and the values almost coincide for $\mu = 1.5$ units/m^2. Similarly to Fig. 4(a), we observe that for the small values of μ, the multi-path scheme with $M = 3$ outperforms the one with $M = 5$.

2) The eavesdropping probability: We now proceed with studying the eavesdropping probability for a wide range of system parameters illustrated in Fig. 5. Particularly, Fig. 5(a) shows the eavesdropping probability for both schemes as a function of the spatial density of blockers, μ. As one may observe, for a wide range of μ, the multi-path scheme provides substantial performance gains at the slight decrease in achieved system capacity, as illustrated in Fig. 4(b) for both $M = 3$ and $M = 5$. Specifically, for $\mu = 1.5$ and $M = 5$ the loss in capacity is only $2-3$ Gbps, while the difference in the eavesdropping probability is over 600%: decreasing from approximately 0.06 for the single-path scheme to less than 0.01 for the multi-path scheme. It is also logical to observe that the greater number of the available paths, M, leads to the lower eavesdropping probability for both schemes.

Let us now study the behavior of both schemes as a function of the spatial density of eavesdroppers, λ, as shown in Fig. 5(b) for the two values of the number of antenna elements at the AP, $L_A = 512$ and $L_A = 2048$. One of the critical trends here is that the increase in L_A leads to better performance for both the single-path and multi-path schemes. The underlying reason is that the system with the higher value of L_A leads to the smaller size of the eavesdropping zone and, thus, lower values of the individual eavesdropping probabilities for a given path. For $L_A = 2048$, the gains are observed across the entire range of the density of eavesdroppers, while for $L_A = 512$ both curves converge already at $\lambda \approx 0.03$ units/m^2. The eavesdropping probability for the single-path and the multi-path schemes is shown in Fig. 5(c) as a function of the 2D distance between the AP and the UE, d, for two values of L_A. For $L_A = 2048$ the noticeable gains are observed across the entire range of d, while for $L_A = 512$ the curves converge at $d \approx 50$ m.

3) The secrecy rate: Finally, we study the secrecy rate, C_S, presented in Fig. 6 as a function of the density of blockers. The secrecy rate metric here combines the previous two (C and p_E), thus, allowing to compare the two schemes within a single plot. As observed from Fig. 6, the multi-path scheme achieves considerably greater secrecy rate over a wide range of system parameters. The gain varies from approximately 4 Gbps for the low density of eavesdroppers, $\lambda = 0.03$, to more than 10 Gbps for $\lambda = 0.1$. Similar conclusions are observed for the secrecy rate as a function of other system parameters, such as distance and the number of antenna elements, L_A.

In summary, the multi-path scheme achieves notable gains over the single-path in both the eavesdropping probability and the secrecy rate at a cost of a slightly decreased link capacity.

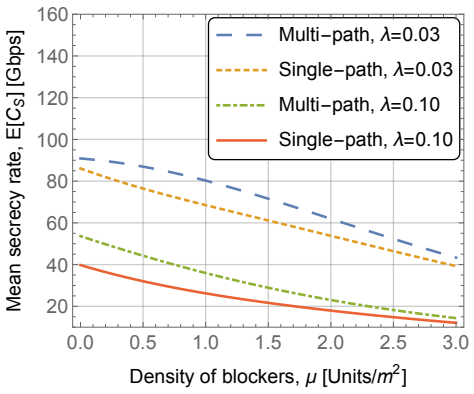


Fig. 6. Secrecy rate for *Single-path* and *Multi-path* schemes, $d = 15$ m, $M = 5$.

V. Conclusions

Secure data transmission is one of the critical requirements for the wireless systems beyond 5G. The prospective use of THz band provides additional tools for securing communications already at the physical layer. In this paper, we have investigated how the security of data transmissions can be leveraged by exploiting the multi-path propagation of THz communications. We have developed a mathematical framework capturing the inherent trade-offs between the eavesdropping probability and the capacity of a THz link in a typical urban scenario with various crowd and attackers densities, and the different number of multi-path components. With the proper parameterization, our framework can be further applied to the analysis of other THz-specific deployments, such as indoor office, house, etc.

We have also shown that sharing the message across all the currently non-blocked propagation paths between AP and UE with the proposed *multi-path* scheme drastically decreases the eavesdropping probability and increases the secrecy rate of THz communications at the expense of slightly reduced link capacity. With the slightly degraded capacity and the overheads of beam realignment procedure and additional coding, brought by the *multi-path* scheme, the proposed solution can be utilized selectively, e.g., to improve the security of sensitive communications (online banking, cryptocurrency transactions, etc.), as well as to secure the exchange of the session encryption keys. The baseline *single-path* scheme can be applied to all other non-sensitive communications. The presented study may serve as one of the building blocks towards secure and robust wireless communications over the THz band as an integral part of beyond 5G networks.

Acknowledgements

The authors would like to thank the anonymous reviewers of IEEE INFOCOM 2019 UBTCN Workshop for their helpful and constructive comments that greatly contributed to improving the final version of the paper. J. M. Jornet acknowledges the support from NSF Grant CNS-1730148.

References

[1] K. Huang and Z. Wang, "Terahertz terabit wireless communication," *IEEE Microwave Magazine*, vol. 12, no. 4, pp. 108–116, June 2011.

[2] I. F. Akyildiz, J. M. Jornet, and C. Han, "Teranets: Ultra-broadband communication networks in the terahertz band," *IEEE Wireless Communications*, vol. 21, no. 4, pp. 130–135, August 2014.

[3] I. F. Akyildiz and J. M. Jornet, "Realizing ultra-massive MIMO (1024×1024) communication in the (0.06–10) terahertz band," *Nano Communication Networks*, vol. 8, pp. 46–54, June 2016.

[4] D. He *et al.*, "Stochastic channel modeling for kiosk applications in the terahertz band," *IEEE Transactions on Terahertz Science and Technology*, vol. 7, no. 5, pp. 502–513, September 2017.

[5] K. Sakaguchi *et al.*, "Where, when, and how mmWave is used in 5G and beyond," *IEICE Transactions on Electronics*, vol. E100.C, no. 10, pp. 790–808, October 2017.

[6] M. Simsek, A. Aijaz, M. Dohler, J. Sachs, and G. Fettweis, "5G-enabled tactile internet," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 460–473, March 2016.

[7] "IEEE Standard for High Data Rate Wireless Multi-Media Networks – Amendment 2: 100 Gb/s Wireless Switched Point-to-Point Physical Layer," IEEE Std 802.15.3d-2017, Specification, 2017.

[8] T. Kurner and S. Rey, "IEEE 802.15.3d and other activities related to THz communications. Where to go next?" in *Towards Terahertz Communications Workshop*, March 2018.

[9] Q. J. Gu, "Thz interconnect: The last centimeter communication," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 206–215, April 2015.

[10] V. Petrov, M. Komarov, D. Moltchanov, J. M. Jornet, and Y. Koucheryavy, "Interference analysis of EHF/THF communications systems with blocking and directional antennas," in *Proc. of IEEE Global Communications Conference (GLOBECOM)*, December 2016.

[11] C. Han, A. O. Bicen, and I. F. Akyildiz, "Multi-ray channel modeling and wideband characterization for wireless communications in the terahertz band," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2402–2412, May 2015.

[12] C. Han and I. F. Akyildiz, "Distance-aware bandwidth-adaptive resource allocation for wireless systems in the terahertz band," *IEEE Transactions on Terahertz Science and Tech.*, vol. 6, no. 4, pp. 541–553, July 2016.

[13] V. Petrov, D. Moltchanov, and Y. Koucheryavy, "Applicability assessment of terahertz information showers for next-generation wireless networks," in *Proc. of IEEE International Conference on Communications (ICC)*, May 2016.

[14] V. Petrov, J. Kokkoniemi, D. Moltchanov, J. Lehtomaki, Y. Koucheryavy, and M. Juntti, "Last meter indoor terahertz wireless access: Performance insights and implementation roadmap," *IEEE Communications Magazine*, vol. 56, no. 6, pp. 158–165, June 2018.

[15] I. F. Akyildiz, J. M. Jornet, and C. Han, "Terahertz band: Next frontier for wireless communications," *Physical Communication*, vol. 12, pp. 16 – 32, September 2014.

[16] J. Kokkoniemi, J. Lehtomaki, K. Umebayashi, and M. Juntti, "Frequency and time domain channel models for nanonetworks in terahertz band," *IEEE Transactions on Antennas and Propagation*, vol. 63, no. 2, pp. 678–691, February 2015.

[17] S. Priebe, M. Jacob, and T. Kurner, "AoA, AoD and ToA characteristics of scattered multipath clusters for THz indoor channel modeling," in *Proc. of the 11th European Wireless Conference*, April 2011, pp. 1–9.

[18] B. Li, H. Gao, and X. Jing, "Mapping millimeter wave propagation to 5G physical layer: A brief review and look forward," in *Proc. of ISCIT*, September 2016, pp. 695–699.

[19] Y. Zhu, L. Wang, K. Wong, and R. W. Heath, "Physical layer security in large-scale millimeter wave ad hoc networks," in *Proc. of IEEE Global Communications Conference (GLOBECOM)*, December 2016.

[20] Y. Wu *et al.*, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, April 2018.

[21] K. Xiao, S. Zhang, and Y. He, "On the secrecy capacity of 5G new radio networks," *Wireless Communications and Mobile Computing*, May 2018.

[22] J. Ma *et al.*, "Security and eavesdropping in terahertz wireless links," *Nature*, 2018.

[23] M. Karmoose *et al.*, "Leveraging mm-wave communication for security," *CoRR*, vol. abs/1803.08188, March 2018.

[24] S. Priebe *et al.*, "Channel and propagation measurements at 300 GHz," *IEEE Transactions on Antennas and Propagation*, vol. 59, no. 5, pp. 1688–1698, May 2011.

[25] V. Petrov, M. A. Lema, M. Gapeyenko, K. Antonakoglou, D. Moltchanov, F. Sardis, A. Samuylov, S. Andreev, Y. Koucheryavy, and M. Dohler, "Achieving end-to-end reliability of mission-critical traffic in softwarized 5G networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, pp. 485–501, March 2018.

[26] J. M. Jornet and I. F. Akyildiz, "Channel modeling and capacity analysis for electromagnetic wireless nanonetworks in the terahertz band," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3211–3221, October 2011.

[27] M. Gapeyenko, V. Petrov, D. Moltchanov, S. Andreev, Y. Koucheryavy, M. Valkama, M. R. Akdeniz, and N. Himayat, "An analytical representation of the 3GPP 3D channel model parameters for mmWave bands," in *Proc. of 2nd Workshop Millim.-Wave Netw. Sens. Syst., ACM MobiCom*, October 2018.

[28] V. Petrov, M. Komarov, D. Moltchanov, J. M. Jornet, and Y. Koucheryavy, "Interference and SINR in millimeter wave and terahertz communication systems with blocking and directional antennas," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1791–1808, March 2017.

[29] A. B. Constantine *et al.*, "Antenna theory: analysis and design," *Microstrip Antennas (third edition), John Wiley & Sons*, 2005.

[30] M. Gapeyenko, V. Petrov, D. Moltchanov, S. Andreev, N. Himayat, and Y. Koucheryavy, "Flexible and reliable UAV-assisted backhaul operation in 5G mmWave cellular networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 11, pp. 2486–2496, November 2018.

[31] S. Ross, *Introduction to probability models*. Academic Press, 2010.