Adversarial Obstruction of Millimeter Wave Links

Leonardo Badia
University of Padova, Italy
email: leonardo.badia@unipd.it

Vincenzo Mancuso
IMDEA Networks Institute, Madrid, Spain
email: vincenzo.mancuso@imdea.org

Marco Ajmone Marsan
IMDEA Networks Institute, Madrid, Spain
email: marco.ajmone@imdea.org

***Abstract*—We use a stochastic geometry approach to study an adversarial attack to the physical layer of millimeter wave communications, which is extremely vulnerable to blockage due to obstructions. Previous investigations have applied stochastic geometry to the study of millimeter wave communication scenarios with randomly located obstructions, but in this paper we investigate what happens if some of them are actually due to a malicious attacker. It turns out that, with just few strategically positioned obstructions, an adversary can significantly hinder the millimeter wave link operation and cause extremely high outage probabilities. As expected, scenarios with multiple reflections are more robust against this kind of attack, since they can exploit the diversity of reflected paths, despite their lower quality. Conversely, millimeter wave communications without (or with limited) multipath diversity are shown to be extremely fragile. We also investigate the impact on blockage of different parameters of the obstructions, including their number, shape, and size. Finally, we elaborate the applications of our findings to identify countermeasures against this attack.**

***Index Terms*—Millimeter wave communication; communication system security; adversarial blockage.**

I. Introduction

Millimeter wave (mmwave) technology is expected to revolutionize wireless communications by making bandwidths in the frequency range 30–300 GHz available to users, thus reducing congestion of the microwave spectrum, while at the same time achieving high data rates required for future applications [1].

However, many papers [2], [3] point out the challenges of mmwave communications, due to a less robust physical layer on which communication incurs high risk of outage. This may frequently happen whenever transmitter and receiver operate in non-line-of-sight (non-LoS or nLoS), because mmwave signals suffer from high penetration losses, lower diffraction, and generally low transmit power that may not give adequate signal-to-noise ratio (SNR) at the receiver's side.

Nevertheless, at short distances, mmwave communications may be suitable and outperform standard microwave communications if proper beamforming is employed [4], because of wider bandwidth and reduced interference. What is more, properties such as low penetration would turn into an advantage for dense deployments [5]. Without further discussing these aspects, on which many authors have given valuable contributions, we are interested in exploring the robustness of mmwave communications in realistic communication scenarios, especially with regard to the presence of obstructions.

While several studies consider the impact on blockage of objects randomly and unintentionally placed in the communication region [6], [7], we notice that no previous investigation argued that the fragility in the communication channel due to obstructions may be exploited by an adversary to cause service disruption. At the same time, physical layer security investigations, e.g., about jamming scenarios [8]–[11], are sometimes considering variable positions of the terminals, but the analysis of the placement of an adversary as inherently causing harm does not seem to get much attention, despite being in our opinion a quite simple attack to enact.

For this reason, this paper attempts to fill a gap in the literature by introducing this kind of attack and quantifying its impact on mmwave communications. We present a quantitative analysis based on the frameworks of [4], [12], modified to add the intervention of an adversary, maliciously placing obstacles on the best available path. We analyze multiple scenarios and quantitatively assess the role of different system parameters.

The main conclusion of our study is that adversarial blockage can heavily impact mmwave communications, and may be difficult to counteract. Depending on how many obstacles can be placed by an adversary, the communication quality can be significantly worsened (lower SNRs, higher outage probabilities). While it is understandable that this general property follows the security principles that an all-powerful attacker is always able to disrupt communications, we claim that in the specific scenarios that we consider, it does not really take a significant effort for the attacker to cause impairments to the transmission [13]–[16].

Additionally, we argue that such an attack is relatively easy to perform as long as the adversary is able to gain information on the channel quality over different paths. While this clearly requires some survey of the communication environment, it may be realistic to think of this option being available in indoor or small-distance outdoor scenarios, which are the environment of choice of mmwave communications [17]–[19].

Given that mmwave communications are expected to have a primary option to transmit over a line-of-sight (LoS) path, already placing the first additional obstacle is hurtful, and communications can be destroyed with few strategically placed obstacles. We show how reflection-rich scenarios are naturally more robust to this kind of attack thanks to their intrinsic path diversity [20]. We investigate how the shape of obstructions can play a role; since the attacker is expected to place obstacles so as to cause maximal blockage, elongated items are more harmful.

Finally, we also discuss possible countermeasures for contrasting this kind of attacks. While the actual implementation is left for future research, it is important to point out possible solutions, e.g., based on beamsteering or reconfigurable intelligent surfaces (RISs) [21], [22].

The rest of this paper is organized as follows. In Section II, we review the related literature, and we present our analysis based on stochastic geometry in Section III. Numerical results are extensively collected for a wide range of scenarios in Section IV, and Section V elaborates on the practical consequences of our findings for mmwave scenarios. Finally, Section VI concludes the paper.

II. Related Work

Due to the increasing need to support applications with low latency, high speed, and heavy traffic, as expected for next generation communications, a fertile line of research has emerged about the propagation characteristics of the mmwave spectrum comprising the frequencies at 30–300 GHz [3].

Compared to other wireless technologies, where the higher layers of the protocol stack can be studied with an agnostic attitude towards the underlying physical layer, mmwave communications definitely force some careful cross-layer considerations in the analysis. The reason is that, while other communication media, such as microwaves, can consider, at least as a first approximation, simple free-space, benign propagation models, mmwave must necessarily take into account a number of additional limiting factors [5].

First of all, path loss is more acute in mmwave-bands, since its frequency-dependent part is well known to grow by 6 dB per octave, which usually constrains their use in short-distance communications links. Moreover, in mmwave communications other factors come into play, such as atmospheric attenuation from surrounding gases (usually air, but even worse if rain, fog, or moisture are present) in the transmission medium [20]. Finally, obstructions severely limit communications, unlike what happens for microwave signals, which can be treated as penetrating material artifacts such as walls or interposing items so as to sustain communications even in nLoS conditions. For mmwave communications, it is common to assume that obstructed paths cannot be used, and nLoS communications happen on unobstructed bouncing trajectories [23]. In all actuality, small items can be traversed by mmwave communications, however this usually causes a strong attenuation—a few dB per centimeter—that may make some bounce paths better than LoS [2]. Nevertheless, we will factor these aspects in our model so as to see what is the best path to use in the presence of multiple paths as well as multiple obstructions placed on them.

In light of their expected impact on next generation wireless communications, security aspects of mmwave communications are also very important [24]. However, it seems that the only investigations about physical layer security revolve around standard authentication and privacy procedures when dealing with the control of the physical layer, not the physical reality itself. For example, [14] considers attacks (and possible countermeasures) to the sensing procedures of the mmwave transmitters, with the goal of injecting false measurements. This is a serious problem, especially if some joint sensing and communication procedures are adopted for mmwave scenarios, but pertains more to the area of spoofing signals and requires sensing and processing capability at the attacker's side. The authors of [13] discuss instead possible attacks based on physical layer data against the classifiers of mmwave signals that are based on deep learning techniques. Finally, [15] analyzes physical layer security problems and possible solutions in mmwave communications, and even adopts a stochastic geometry model as we do here, but does not consider blockage as a consequence of an attack, and only secrecy capacity in the case of eavesdropping is investigated. Thus, concerning the physical placement of the obstructions in the transmission scenario, we cannot find any previous reference pointing out possible threats based on this simple, yet effective, attack strategy, thereby making our contribution novel.

A considerable number of papers, including some previously mentioned ones, discuss the implications of obstructions on mmwave channels, due to randomly located objects along the path or structural blockage of the communication devices, such as the human body holding the communication apparatuses. For example, [25] investigates environmental mobility in vehicular networks, and its implications on the blockage in mmwave communications. Coexistence between different kinds of mmwave communications (terrestrial and satellite) is studied in [26], with an evaluation of their possible mutual interference, which again is meant to happen unintentionally.

The blocking caused by a human body is discussed in [19] and, for instance, other references such as [17] and [18] extend it to the case of pedestrian crowds intercepting the beam, or people traveling along it, respectively. Paper [27] studies mmwave communications for unmanned aerial vehicles (drones) and discusses how the propellers cause structural blockage to the transmitter. Finally, many related papers [4], [6], [7], [12], [28] use stochastic geometry to characterize randomly placed obstructions and obtain closed-form models.

However, in all these papers, obstructions are caused by either randomly placed objects that just happen to cause blockage, or unavoidable structural screening done without any malicious intent. Our approach can be seen as a direct extension of these analytical frameworks, with the added twist that one or more adversaries are also present. It is important to note that such an extension does not really depend on the specific framework and can be applied to a number of theoretical evaluations, as well as practical measurements. We assume that the adversary has full information about the geometry of the environment and the propagation parameters, and exploits it to cause intentional harm to mmwave communications, specifically placing obstacles on the trajectories of the paths that are expected to be chosen by the transmitter.

This attack somehow resembles other physical layer adversarial strategies, such as jamming from different locations [11], [24]. However, it can be enacted even by an attacker with no transmission capability, but just the ability to place obstacles. In reality, it requires a measurement of the channel characteristics and possibly a survey of the area by the attacker, but nothing more complicated than what the transmitter/receiver pair itself performs to estimate the transmission channel [13]. Also, the attack can be difficult to detect as it may exploit items already present in the environment, with just minor displacements to cause maximal blockage of the paths.

III. Model

The physical layer attack that we study in this paper takes place on a mmwave communication link between a transmitter (TX) and a receiver (RC), placed in a three-dimensional walled environment. The TX and the RC are d meters apart, and their positions, as well as the characteristics of the environment, are common knowledge, not just to the legitimate transmitter but also to an attacker that aims to cause intentional link blockage.

In the rest of this paper, we use the term *object* to identify obstructions randomly placed in the environment, and the term *obstacle* to denote the obstructions intentionally positioned by the attacker. The term *obstruction* will be used

TABLE I
LIST OF PARAMETERS AND NOTATIONS

symbol	meaning
k=0, 1, ...	path index, with 0 being LoS
d_k	length of path k
a_k	attenuation on path k
n_k	number of random objects on path k
m_k	number of malicious obstacles on path k
X_k	total length of obstructions along path k
μ_k	fading parameter on path k
W_k	wall attenuation on path k
λ	density of obstructions in the environment
λ_0	density of random objects without the obstacles placed by the attacker
M	number of obstacles placed by the attacker
z	specific attenuation (per unit length) of obstructions
A_O	absorption coefficient
f	carrier frequency
σ	background additive noise term
$P_{\rm tx}$	transmitted power
G	antenna gain
$\gamma, \gamma_{\rm th}$	SNR and SNR threshold
$\ell_0, \ell_{\max}$	average, maximum length of an intercepting chord

when referring to both, as obstacles and objects indeed have the same physical characteristics, they just differ in their placement being intentional or not, respectively.

For ease of readability, in Table I we report all the parameters and notations used in the following.

Depending on the environment characteristics, the mmwave signal can be reflected by walls, so, in addition to the direct (LoS) path, there exist also bounce paths reflecting on the walls. In our analysis, we consider up to 6 paths with single reflections, studied through a quasi-deterministic channel model [29]. The paths are denoted as $k \in \{0, 1, 2, \ldots, 6\}$, with 0 being the LoS path, and the other indices referring to possible reflections (left, right, front, rear, ceiling, and floor).

We also model the non-intentional blockage present in the environment by assuming a random placement of objects, which may represent obstructions on the mmwave paths. To this end, we exploit a stochastic geometry approach for the random object placement, and assess the extent of the attenuation caused by each obstruction based on geometrical considerations. The objects are placed according to a Poisson point process (PPP), whose intensity λ_0 denotes the average number of objects per unit volume.

We consider strongly directional antennas for both transmitter and receiver, with negligible side lobes, aligned with fast beamsteering [30], thus causing the transmission to happen always on the path with lowest attenuation (or best SNR). Thus, all paths but the selected one only see very low transmission power, which we neglect in our model. This selected path does not necessarily correspond to the LoS path, which can be obstructed. At any rate, once the geometric parameters are set (room features and placements of transmitter, receiver, and random obstructions), the beamsteering is deterministic and only depends on the attenuation of each path with an additional average loss due to small scale fading.

However, we assume that an adversary is present, with the ability to place M obstacles to cause intentional malicious blockage on the paths available to the TX-RC pair. To characterize this intentional blockage, we assume the following. First of all, the obstacles placed by the attacker have the exact same shape and characteristics of the random objects present in the environment, the only difference being that instead of being randomly scattered across the room, they are intentionally placed so as to intercept the paths causing maximum blockage. Since the presence of obstacles increases the number of obstructions in the room, in the following we will always consider an actual intensity of obstructions denoted as $\lambda \geq \lambda_0$. Throughout our investigations, we will set λ to a given value, and change M, which can be equivalently seen as placing the non-malicious objects with a rate $\lambda_0 = \lambda - M/V_{\rm room}$, where $V_{\rm room}$ is the volume of the room, or the attacker being able to take some of the objects already existing in the room and move them so as to obstruct the transmission paths.

The transmitter is oblivious to the presence of maliciously placed obstacles, and the attack is hard to detect since the adversarial obstructions are indistinguishable from other objects in the room; scenarios with an increasing number of obstacles look like they have just bad channel conditions, which could even happen in the presence of only random objects [11].

Nevertheless, the transmitter is always able to perform beamsteering and select the best available path accounting for all obstructions, either malicious or not, and, following [4], [6], [12], the SNR at the RC is a function of the small scale fading h and of a random variable $a_{\min} = \min_k a_k$ that represents the attenuation over the best available path chosen by beamsteering, computed on the average fading depth. As a result, the SNR γ can be written as

$$\gamma = \frac{P_{\rm tx} G |h|^2}{\sigma^2 a_{\min}}, \tag{1}$$

where $P_{\rm tx}$ is the transmit power, G is the antenna gain, σ is a noise term. In turn, the attenuation in dB on the kth path is

$$10\log_{10} a_k = 20\log_{10}(4\pi f d_k/c) + A_{\rm O} d_k + W_k + \mu_k + z X_k, \tag{2}$$

where the first term in the summation is the standard expression for free space path loss, with f being the carrier frequency, d_k the length of path k, and c the speed of light. The following term accounts for absorption, with $A_{\rm O}$ being the absorption coefficient. Term W_k represents the wall attenuation, where we note that $W_0 = 0$ because path 0 is the LoS path, and all other paths hit the walls just once. Term μ_k is the inverse of the average fading depth, in dB, so that the channel coefficient is $h 10^{-\mu_k/10}$. Finally, zX_k represents the additional attenuation due to blockage, where z is a proportionality coefficient and X_k is the total obstruction length over path k, obtained by summing over all obstructions.

In [12], X_k is taken as the sum of the average intersection lengths of the mmwave beam with each obstruction; if they are unintentional (just random objects in the room), their average length is derived according to the second Cauchy formula [31]. In short, a randomly placed three dimensional convex object of volume V and total surface S causes an obstruction based on a random intercepted chord that has length $\ell_0 = 4V/S$.

We modify this framework and include maliciously positioned obstacles as well. An intentionally placed obstacle does not intercept the path with a generic chord, but with its diameter, i.e., the chord of maximal length $\ell_{\max}$. For example, in case of spherical objects of radius r, the average

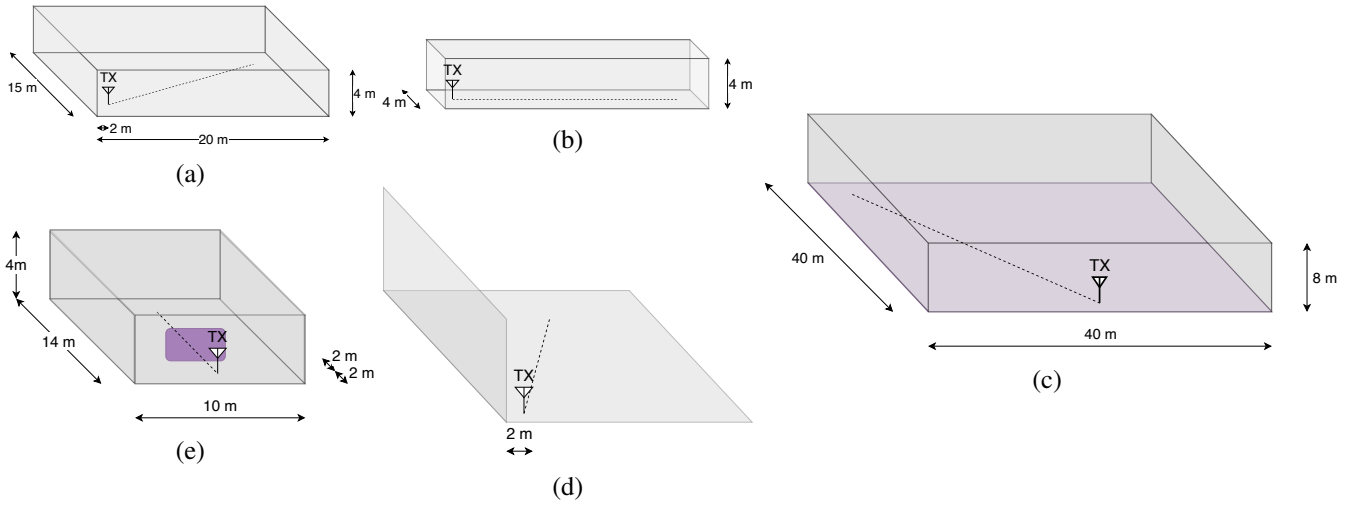

Fig. 1. From top-left, clockwise: (a) a box-shaped reflective room; (b) a corridor; (c) a ballroom/conference hall; (d) an outdoor scenario beside a building; (e) a closed room without LoS. The transmitter is placed at "TX" and the receiver is located along the dashed line, at variable distances.

interception length of a random object is $\ell_0 = \frac{4}{3}r$, while the diameter is $\ell_{\max} = 2r$.

Concerning the adversarial strategy, we assume that the attacker maliciously places the first obstacle on the best path for the transmitter. If $M > 1$, obstacles are subsequently placed according to a greedy policy, that is, one at a time, choosing the path that has lowest attenuation on average after the placement of the previous obstacles. Each obstacle is causing a known blockage $z\ell_{\max}$, so the adversary can update the attenuation terms and assign the next obstacle to the current best path, and repeat until all M obstacles are placed.

At the end of the procedure, the channel attenuation will be determined with analogous computations involving randomly placed objects and malicious obstacles, with the same attenuation per unit distance of the intercepted path (but note that malicious obstacles have a higher interception equal to their diameter). For this operation, the adversary is required to have channel sensing capabilities, which is analogous to what the legitimate transmitter uses to perform beamsteering. Actually, the adversary sensing only requires a much coarser granularity as it simply takes the average of the fast fading term.

As a consequence, we are able to estimate the performance of the mmwave communication through several possible quantitative indicators. In our analysis, we choose the *outage probability*, since for many applications it is more significant or general than other alternatives, such as the expected data rate or the spectral efficiency, and allows us to express the consequences of the high variability in performance induced by blockage [16], [32].

From (1), the outage probability for an SNR threshold $\gamma_{\rm th}$ is derived as

$$P_{\rm out}(\gamma_{\rm th}) = \Pr\left(\frac{|h|^2}{\Psi} \le \Theta\gamma_{\rm th}\right) = \int_0^\infty \left(1 - e^{-\Theta\gamma_{\rm th}x}\right) f_\Psi(x)dx \quad (3)$$

with constant $\Theta = \sigma^2/(GP_{\rm tx})$, where h is Rayleigh distributed and therefore $|h|^2$ is exponentially distributed, and $\Psi = a_{\min}$ is an aleatory average attenuation process, whose randomness depends on the process that models the presence of objects, and which does not depend on the normalized channel fading h, but it depends on the average depth of fading, which is a constant under stationary conditions, see (2). From this, we can derive the outage probability as

$$P_{\rm out}(\gamma_{\rm th}) = 1 - e^{-\sum_k N_k} \sum_i \sum_{n_i=0}^{\infty} \frac{N_i^{n_i}}{n_i!} \exp(-\Theta\gamma_{\rm th}) \cdot \exp\left(10^{\mu_i\left(L_i + z(n_i\ell_0 + m_i\ell_{\max})\right)/10}\right) \prod_{k\neq i} \sum_{n_k=\nu(k,i)}^{\infty} \frac{N_k^{n_k}}{n_k!}, \quad (4)$$

where n_k is the number of objects on the kth path according to the PPP, $N_k = \mathbb{E}[n_k]$, m_k is the number of malicious obstacles on the kth path, and $\nu(k,i)$ is the smallest integer number of objects on the kth path such that the attenuation on the ith path is smaller than on the kth path, i.e.,

$$\nu(k,i) = \max\left\{0, \left\lceil n_i + (m_i - m_k)\frac{\ell_{\max}}{\ell_0} + \frac{20\log_{10}(d_i/d_k) + A_O(d_i - d_k) + W_i - W_k + \mu_i - \mu_k}{z\ell_0} \right\rceil\right\}. \quad (5)$$

IV. Numerical Results

We evaluate these formulas on the 3D (three dimensional) scenarios (a)–(e) shown in Fig. 1, with different numbers of malicious obstacles and link distances. Unless otherwise specified, we use these default parameters. The transmit power is $P_{\rm tx} = 0.1$ W, the carrier frequency is $f = 60$ GHz. Scenarios (a) and (b) use a bandwidth $B_0 = 8.64$ GHz with reference to IEEE 802.11ay [33]. Accordingly, the noise power term is $\sigma^2 = 3.58 \cdot 10^{-11}$ W, which roughly corresponds to the thermal noise at 300 K. Such a bandwidth is too large for scenarios (c), (d), and (e), where the propagation condition is worse (consequently, the data rate is limited); for those, we use a bandwidth $B_0/4 = 2.16$ GHz, as per the IEEE 802.11ad standard [33], and the noise power is then 6 dB lower.

The atmospheric absorption is $A_{\rm O} = 0.15$ dB/m, the attenuation coefficient of obstructions is $z = 100$ dB/m, consistent with human bodies [34], the total antenna gain is $G = 30$ dB, the outage threshold $\gamma_{\rm th}$ is set to 5 dB. The wall reflection attenuation terms W_k depend on polarization and incidence angle on each wall, according to Fresnel law,

assuming a reflection between air and wall, whose refraction indices are 1.0 and 1.5, respectively [12]. This gives different values for each wall, depending on the geometry of the scenario.

We consider spherical objects of radius $r = 0.1$ m, which is roughly the size of a human head. We assume that obstruction locations are distributed according to maliciously placed obstacles superposed to a PPP of randomly scattered objects, with resulting overall density $\lambda = 1$ m^{-3}. This implies that, if only random objects are present, a path of 10 m is intercepted on average by 0.314 obstructions, with a 73% probability of no obstruction, which can be seen as a mild blockage. If malicious obstacles are present, the actual intensity of the PPP is lower, because we always keep the same number of obstructions in the room, but some of them are maliciously placed.

With reference to Fig. 1 for a visual display, the considered scenarios are as follows. All numerical values are in meters.
Scenario (a): a box-shaped room of size $20 \times 15 \times 4$. The transmitter is in position $(2, 2, 1)$. The receiver is placed at variable distance d on the dashed line towards $(18, 13, 1)$. Distances are from $d_{\min}$=6 to $d_{\max}$=18. All reflections are accounted for (6 in total).
Scenario (b): a corridor-like environment, i.e., a $50 \times 4 \times 4$ room, with one side much longer than the others. The transmitter is located at $(2, 2, 1)$, and the receiver is aligned on the main length so its position is $(2, 2 + d, 1)$, where d is the distance, that goes from $d_{\min}$=6 to $d_{\max} = 42$; since the corridor is meant not to have walls on the short sides, there are no reflections on the left and the right.
Scenario (c): a hotel ballroom used as a conference hall. The room size is $40 \times 40 \times 8$. The transmitter is placed on a raised stage located at $(20, 2, 2.5)$. The receiver is in the audience, at height 0.8 and located at an angle of $\pi/3$. Distances are from $d_{\min}$=10 to $d_{\max}$=34. It is assumed that the floor is covered with carpet, and therefore the ground reflection is neglected. All other reflections are present, even though the room is very big so they are generally much longer than the LoS path (especially for short transmitter-receiver distance).
Scenario (d): this is meant to represent an outdoor scenario, where a tall building is present to the left of the transmitter. The environment is $30 \times 30 \times 4$, but only three paths are included: LoS, and reflections on the wall to the left, and the ground. There is no ceiling, no right wall, and no walls to the front and back either. The transmitter is at $(2, 2, 1)$. The receiver is directed to an angle of $\pi/4$, at distances from $d_{\min}$=6 to $d_{\max}$=30. In this specific scenario, the intensity of the PPP describing obstruction locations is decreased to 0.333 m^{-3}, for better consistency with an outdoor environment, giving roughly 90% probability of non-obstructed path at $d = 10$.
Scenario (e): this is an indoor environment, with no LoS path due to a structural obstruction. The size is $10 \times 14 \times 4$, the transmitter is at $(5, 2, 1)$ and the receiver is aligned along the long side of the room, so its coordinates are $(5, 2+d, 1)$, with distance $d \in [d_{\min}, d_{\max}]$=[3, 12]. A structural obstruction is present between transmitter and receiver, e.g., a thick wall from $(4, 4)$ to $(6, 4)$, of height 2. Because of this obstruction, the LoS is blocked, and so are the reflections on the ground and the walls to the front and the back of the transmitter. Still, communication is possible thanks to the reflections on the left and right walls, and on the ceiling.

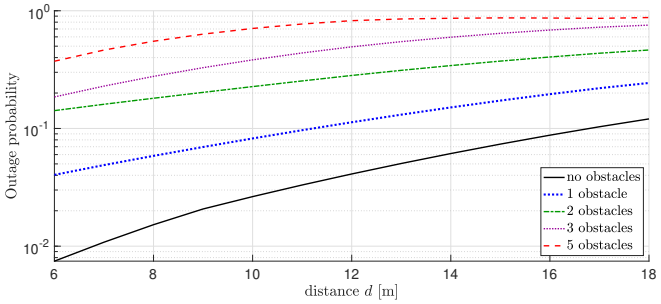

Fig. 2. Scenario (a) – room: Outage probability vs. distance, for different numbers of malicious obstacles.

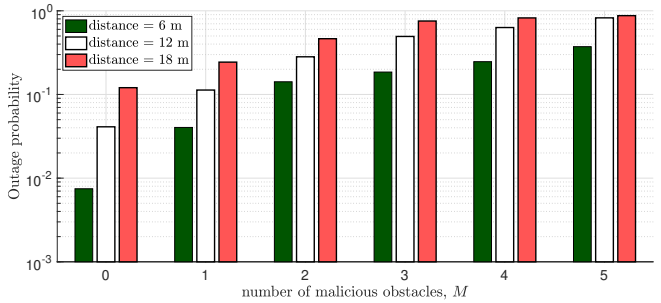

Fig. 3. Scenario (a) – room: Outage probability vs. number of malicious obstacles, for different distances.

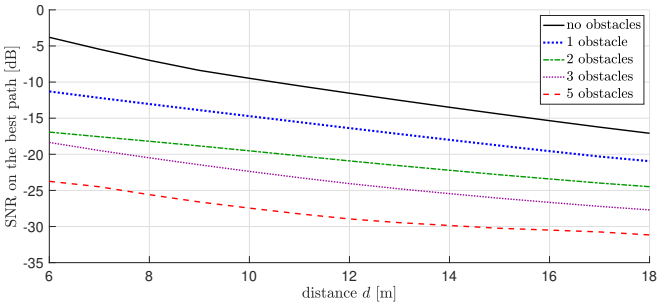

Fig. 4. Scenario (a) – room: Received SNR on the best path vs. distance, for different numbers of malicious obstacles.

A. *Scenarios (a) and (b)*

In Figs. 2–3 we show the results for scenario (a), specifically the outage probability versus the distance, for a variable number of obstacles, and the other way around (number of obstacles as the independent variable for some values of the distance), respectively. The results are more general and other metrics can be plotted as well, for example Fig. 4 reports the average received SNR, which can actually be computed for all the scenarios, following (1), but it gives essentially the same insight as the outage probability. It can be seen that the presence of malicious obstacles significantly harms the communication, causing frequent outages. Yet, this is the only scenario where the communication still survives to some extent even by adding 3 malicious obstacles, which happens thanks to the higher multipath diversity. For the other scenarios, fewer obstacles are needed to cause complete outages.

We also evaluate scenario (b), which represents a long and narrow corridor. Its results are shown in Figs. 5–6. In the absence of adversaries, this scenario works akin to (a), and even slightly better. This is because there are fewer reflected paths, but they are similar to the LoS path, so they offer good diversity. Note that, in light of the peculiar geometry,

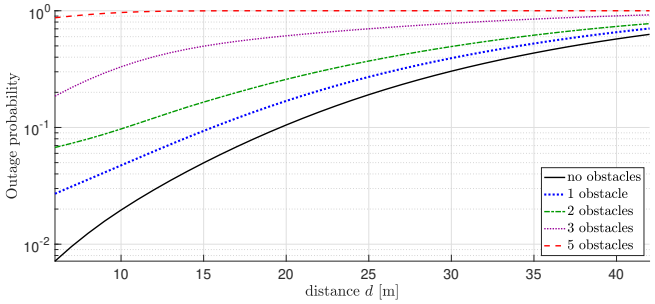

Fig. 5. Scenario (b) – corridor: Outage probability vs. distance, for different numbers of malicious obstacles.

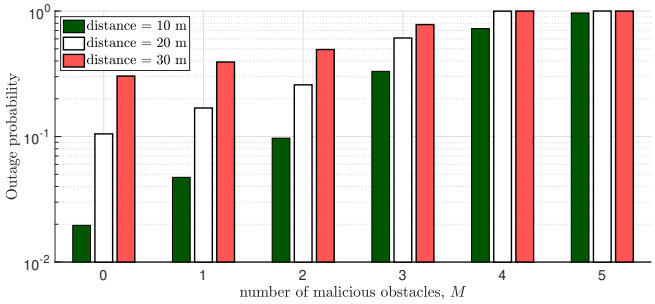

Fig. 6. Scenario (b) – corridor: Outage probability vs. number of malicious obstacles, for different distances.

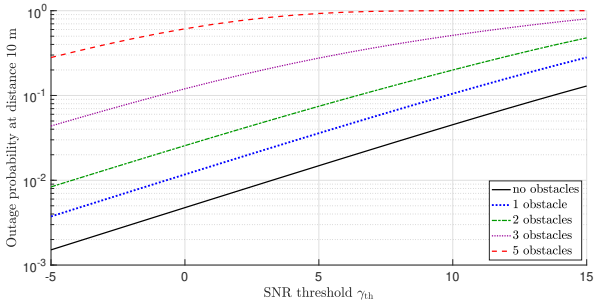

Fig. 7. Scenario (b) – corridor: Outage probability at 10 m, vs. SNR threshold γ_{th}, for a variable number of malicious obstacles.

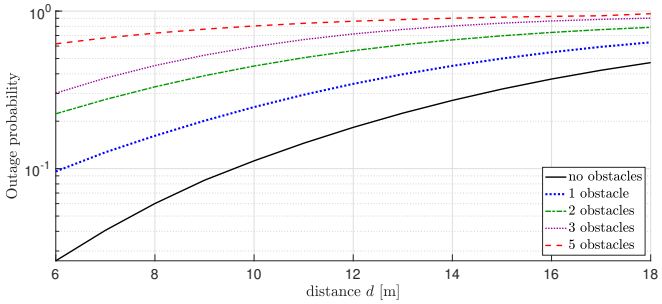

Fig. 8. Scenario (a) – room, higher obstruction density $\lambda = 3$ m^{-3}: Outage probability vs. distance, for a variable number of malicious obstacles.

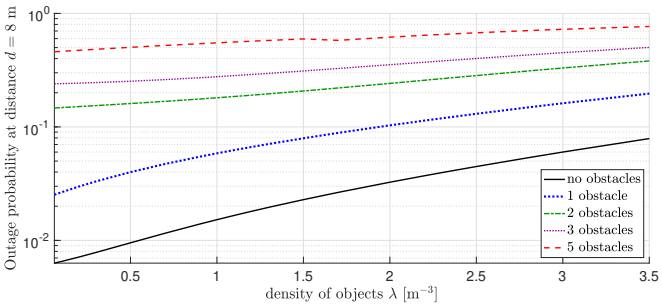

Fig. 9. Scenario (a) – room: Outage probability at 8 m, vs. variable obstruction density λ, for a variable number of malicious obstacles.

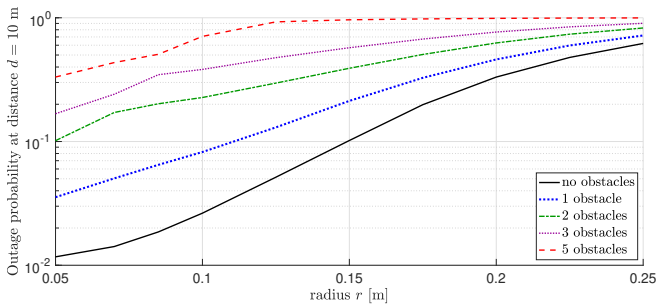

Fig. 10. Scenario (a) – room: Outage probability at $d = 10$ m vs. object radius, for variable number of malicious obstacles.

much longer distances are also considered. However, since on aggregate there are fewer paths, in this scenario it takes fewer malicious obstacles for the adversary to destroy the communication compared to the room in scenario (a).

As another side investigation, we show the outage probability at a distance of 10 meters vs. the SNR threshold γ_{th} in Fig. 7. This result can be plotted for the other scenarios as well (for scenario (a), in particular, it offers the same insight).

To sum up, though scenarios (a) and (b) can be used for mmwave transmissions, adversarial obstructions are harmful and destroy communication with 4-5 malicious obstacles.

B. Varying obstruction parameters

Additional results can be considered to explore the impact of object density. We can look at a more densely populated version of scenario (a) in Fig. 8, where again the outage probability vs. distance is displayed, for different numbers of malicious obstructions. Here, the density of objects is increased to $\lambda = 3$ m^{-3}, so the probability of unobstructed path at 10 m in the absence of malicious obstacles is just 39%. The presence of so many obstacles implies a limitation on the communication range. At the same time, the task of the adversary is made easier, especially on longer distances, by the higher number of randomly located objects. One can also expect that the attack is easier to implement on such a dense scenario, as blockage is already strong and the adversary has a larger number of physical items among which to choose those that are displaced to cause blockage.

In Fig. 9, we consider the density of objects in the environment as the independent variable. The implication is that the opponent is less sensitive to the obstruction density, since it causes harm by specifically placing them in the most damaging way. Yet, lower densities would make the actions of the adversary more evident.

We next present investigations pertaining to the size and shape of obstructions, all performed on scenario (a), even though the results are consistent across all scenarios. In the first evaluation reported in Fig. 10, we show how the outage probability at 10 m changes depending on the radius of the obstructions. We recall that this applies to both randomly located objects and also maliciously placed obstacles. Also, in this case all the obstructions are of spherical shape. It is shown that the outage probability is highly sensitive to the size of the items, and larger obstructions can cause outage with higher probability. This is true for the randomly placed objects and even more so for the malicious obstacles. The

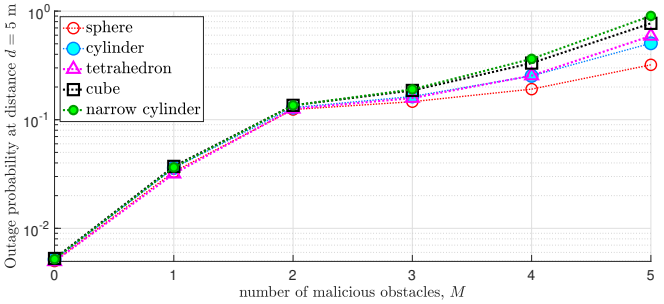

Fig. 11. Scenario (a) – room: Outage probability at $d = 10$ m vs. number of malicious obstacles, for different object shapes.

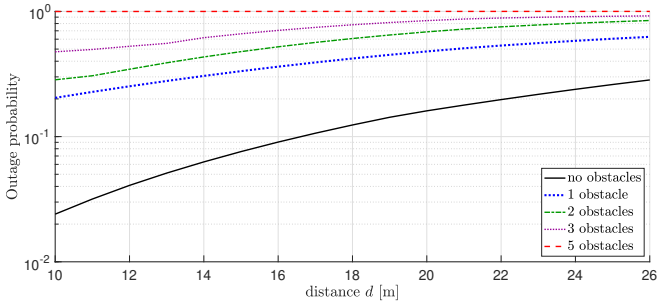

Fig. 12. Scenario (c) – ballroom: Outage probability vs. distance, for variable number of malicious obstacles.

reason is that all obstructions intercepting a path cause attenuation that increases with r. For small values of r, the plots for $M \geq 2$ (all characterized by high outage probabilities, anyways) exhibit border effects, such as angular points in the curve, because the granularity of the placement becomes more evident. The angular points reflect the transitions between different behaviors being more convenient for the attackers. When r is small, it is to place multiple obstacles on the same path; as r becomes larger, there is a transition to the points where it becomes better to block one more path.

Fig. 11 investigates the impact of the shape of the objects. We show the outage probability at 5 m distance, for a variable number of objects having five possible shapes, including (i) the already examined sphere (here with radius $r = 0.15$) and other four, all with volume identical to (i): (ii) a cylinder with base radius r, whose height must then be $\frac{4}{3}r$; (iii) a regular tetrahedron, whose side must be $(16\pi/3)^{1/3}r$ for its volume to be the same as (i); (iv) a cube, whose side is then $(16\pi/3)^{1/3}r$; and finally (v) a "narrow cylinder", i.e., with twice the height as (ii), i.e., $\frac{8}{3}r$, and lower base radius $r/\sqrt{2}$.

The figure shows that the case of spherical objects is actually best for the transmitter, while other shapes start with basically the same outage probability when only random objects are causing obstruction, but make for a worse propagation when the number M of malicious obstacles grows. The reason is that, when an attacker places an item to cause obstruction of a path, it does so by putting it along the diameter to cause the most attenuation. Hence, more elongated items such as the narrow and longer cylinder (v) cause worse obstructions. This also highlights the distinct contributions within the adversarial action. Indeed, the attacker tries to (i) block the LoS and (ii) place obstacles along the diameter for maximal obstruction. The role of (i) is dominant when few obstacles are placed, while (ii) is relevant only when the main paths are blocked.

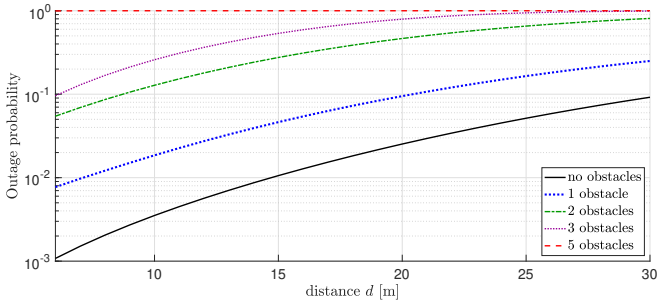

Fig. 13. Scenario (d) – outdoor: Outage probability vs. distance, for variable number of malicious obstacles.

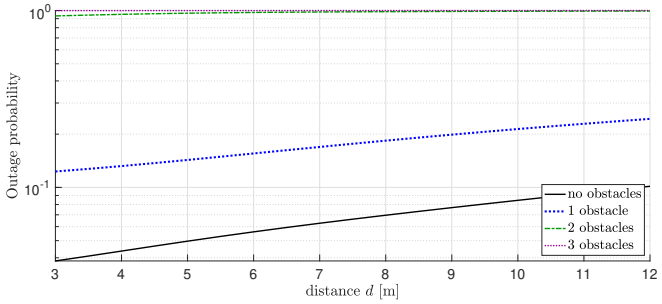

Fig. 14. Scenario (e) – without LoS: Outage probability vs. distance, for variable number of malicious obstacles.

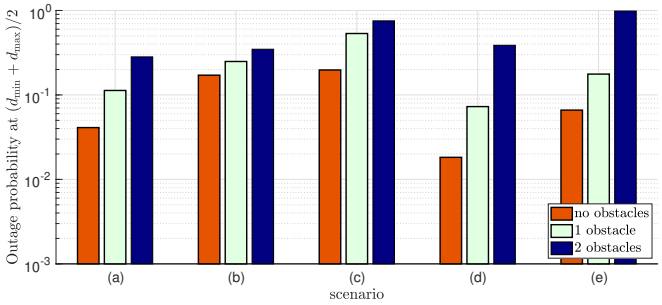

Fig. 15. Outage probability of all the scenarios at intermediate distances, for $M = 0, 1, 2$ malicious obstacles.

C. Scenarios (c), (d), and (e)

We now investigate the other scenarios. The results for scenario (c), the ballroom, are displayed in Fig. 12. This scenario is performing worse than the previous ones. Despite the presence of a good LoS, and the use of a narrower band (so the noise term is lower) the reflected paths are all very long and/or highly attenuated.

Scenarios (d) and (e), whose results are in Figs. 13–14, exhibit even higher vulnerability to malicious attacks. Actually, for the outdoor scenario, in unblocked LoS conditions, the transmission is good and the receiver is rarely in outage, but this is also due to the lower density of obstructions. However, fewer reflections can be exploited by the transmitter, so it is relatively easy for an adversary to block the available paths. Scenario (e) is the most fragile, because it has few paths available and none of them is LoS. Hence, the adversary can already cause considerable damage with 1 obstacle and entirely destroy communication with just 2 obstacles. As a general conclusion, these scenarios where fewer reflections are present, can be extremely fragile to an attacker placing obstacles on their few available paths.

For a final summary, one can look at Fig. 15 that draws a comparison of the five scenarios, showing the impact of

even few obstacles on the outage probability at intermediate distances. Specifically, the receiver is considered to be located at $d = (d_{\min} + d_{\max})/2$; which keeps into account the different size of the environment. The impact of geometry is clear, as scenario (b) is shown to be the most robust to the presence of few malicious obstacles (albeit (a) is better if more obstacles are deployed), thanks to the existence of bounce paths that are weaker but similar in length to the LoS path. Scenario (d) is performing well (due to the lower density of objects) only if the LoS path is undisturbed, while (c) and (e), which are already underperforming without adversarial blockage, definitely fall apart even with one or two malicious obstacles.

V. Discussion

In light of these results, we examine possible consequences on both sides, namely, the attacker's, i.e., how practical it is to implement adversarial blockage, and the legitimate transmitter's, that is, what countermeasures are possible.

A. Implementation of the attack

Our findings highlight that a small number of carefully placed obstacles is sufficient to disrupt mmwave communications. While the actual consequences of blockage depend on the considered scenario, already one obstacle placed across the LoS path, when present, is considerably harming the communication, and few more obstructions annihilate it.

Clearly, the attacker must be able to identify the best paths, so an underlying requirement is the knowledge of the propagation scenario. This is not hard to acquire for a sufficiently equipped terminal. The requirements to estimate the channel quality along multiple reflected paths are akin, if not easier, to those that the legitimate receiver must have to properly exploit path diversity [35]. Indeed, the malicious attacker just needs to identify the best paths, without performing proper beamforming and decoding the received signals through any combining. Moreover, low-cost solutions for channel estimation exist [36], [37], which have been shown to be robust to hardware impairments or imperfect channel state information even for a legitimate receiver. So, the situation is definitely in favor of an attacker that does not need to decode the actual signal, but just to estimate where to place an obstruction.

Another objection to this attack concerns the physical placement of obstacles. Since we consider three-dimensional scenarios, and sometimes the considered reflections hit the ceiling, it may seem that placing an obstacle along the path would require a suspended positioning, which is however not that unreasonable in indoor scenarios [23]. In reality, the model itself does not specify where the objects are actually placed along the path, so it can be at any height as long as it intercepts the trajectory, all that matters is that maximal obstruction is caused. While the model is directionally homogeneous for the necessary requirements of a theoretical analysis, it does not seem particularly hard to place obstacles with the only requirement that they are anywhere along the best paths.

Finally, the malicious placement of obstacles can be extremely inconspicuous, as we did not consider special objects causing stronger blockage than those normally present in the room. We can even regard the adversarial action as the simple re-location of existing items in the most harmful way for the transmitter. Such a malicious intent is hard to prove, as the result is the same that would happen under an unlucky placement of obstructions according to the PPP [3], [4].

B. Countermeasures

A first option to consider to counter the attack is to move the transmitter or the receiver to go around the blockage [25], [38]. In our investigation, we focused on a static placement of nodes, which may be the most immediate application, at least for indoor scenarios. If the legitimate transmitter/receiver pair change their positions, they will force the adversary to change the placement of the obstacles, at the risk of being more easily discovered. Yet, it is expected it would also cause misalignments, handovers, and repeated training, with possibly huge overhead. It is plausible that the drawbacks of this defensive strategy are stronger than the advantages and it appears as an unlikely candidate for a systematic application.

An important conclusion that can be drawn from our results is that the resilience to adversarial blockage is strongly correlated to the number of available paths with low attenuation between the transmitter and the receiver. Thus, the problem can be mitigated if multiple reflections are exploited thanks to beamsteering [30], since the selection of the best path among all reflections already outperforms the strategy of only using the LoS path in many cases, and even more so when the communication is under attack by such a malicious opponent that will first of all attempt to block the direct path.

A solution to adversarial blocking may be the use of multiple transmitters and/or receivers from different locations, in the fashion of coordinated multipoint (CoMP). This has been shown to successfully counteract intentional jamming [10] or random non-intentional blockage in mmwave communications, e.g., by people intercepting the beams [21]. Thus, one may think of a similar approach against malicious blockage by an adversary. Such a solution is possible if multiple locations are available and interconnected so as to transmit (or receive) the same content. It does not require particular signal processing capabilities, as long as a selection mechanism for the best available locations for the transmitter/receiver pair is available. Performance-wise, this is expected to scale down the impact of the attacker by roughly $L_{\mathrm{T}} \times L_{\mathrm{R}}$ times, where L_{T} and L_{R} are the numbers of transmit and receive locations, respectively. For example, if the same communication can take place between L_{T} transmit and L_{R} receive locations, instead of just placing an obstacle on the strongest path (usually the LoS), the attacker must block all the strongest paths between each pair, possibly sparing some if one obstacle can block two paths at once.

Even more so, RISs that would artificially create multiple reflections [28], [39], together with the option of exerting some geometric control over them, appear as the most promising candidate to give protection against adversarial blockage. However, the actual implementation of RISs is still open and many solutions have been proposed to realize them. Thus, we believe that, while our investigation gives a strong support to the implementation of such technologies, it also prompts more efforts for a better characterization of which RIS-based technology is most suitable to counteract an attacker.

The options to introduce RIS-aided communications at reduced cost and size need to be weighted also against the ease of implementing an attack against them. For example, a point-like RIS would surely assist the communication but

it ultimately just represents one more reflected path with low attenuation, that is rather easy to block if its position is known or discovered. It may be more interesting to evaluate a linear or planar RIS, whose effective reflection point can be changed with appropriate beamforming [22]. Also, RISs themselves may present further security breeches, which is another aspect to consider; in other words, they can make the system more robust, but also more exploitable if not properly safeguarded. Most of the literature focuses on how a secure RIS can improve the secrecy of a communication, but there are few investigations (a notable exception being [40]) about the impact of malicious attacks against the RIS itself.

Nevertheless, these aspects highlight smart reflective surfaces as one of the most promising fields for future research, not just for mere performance improvements but to obtain a viable application of mmwave communications in reality.

VI. Conclusions

We leveraged existing models based on stochastic geometry for randomly located obstructions to derive the outage probability in mmwave communications, based on the cumulative attenuation caused by multiple objects. We extended them to the case of a malicious adversary placing obstacles with the intent to obstruct the best paths. This led us to identifying this kind of blockage attack as a serious security threat for mmwave communications, which is apparently overlooked by the present literature [24]. Such a malicious blockage can be enacted with relatively low effort, but potentially leads to communication disruption especially when the environment does not have many reflected paths.

This issue can also be addressed from the perspective of game theory [8], [9], [38], surely as a way to analytically frame the detection of an attack, and possibly mitigating it, either from a static perspective or involving the time scale of the obstacle placement (which is not obvious). The adoption of precise countermeasures, of which RISs probably represent the most important candidate [22], [39], is also possible. All of these appear as promising directions for future work.

We believe that our investigation gives a strong justification for these lines of research, not just as a promising addition to the state of the art, but also as a concrete necessity to implement robust and operational systems.

Acknowledgments

This work has been supported by the RESTART Program, financed by the Italian government with the resources of the Italian Recovery, Transformation and Resilience Plan – Mission 4, Component 2, Investment 1.3, theme 14 "Telecommunications of the future," and by the Project AEON-CPS (TSI-063000-2021-38), funded by the Ministry of Economic Affairs and Digital Transformation and the European Union NextGeneration-EU in the framework of the Spanish Recovery, Transformation and Resilience Plan.

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] H. Xu, V. Kukshya, and T. S. Rappaport, "Spatial and temporal characteristics of 60-GHz indoor channels," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 3, pp. 620–630, Mar. 2002.

[3] T. S. Rappaport, F. Gutierrez, 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. 2012.

[4] M. Di Renzo, "Stochastic geometry modeling and analysis of multi-tier millimeter wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5038–5057, Sep. 2015.

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

[6] S. M. Azimi-Abarghouyi, B. Makki, M. Nasiri-Kenari, and T. Svensson, "Stochastic geometry modeling and analysis of finite millimeter wave wireless networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1378–1393, Feb. 2018.

[7] T. Bai and R. W. Heath, "Coverage and rate analysis for millimeter-wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1100–1114, Feb. 2014.

[8] G. Perin, A. Buratto, N. Anselmi, S. Wagle, and L. Badia, "Adversarial jamming and catching games over AWGN channels with mobile players," in *Proc. WiMob*, 2021, pp. 319–324.

[9] A. Garnaev, A. P. Petropulu, W. Trappe, and H. V. Poor, "A jamming game with rival-type uncertainty," *IEEE Trans. Wireless Commun.*, vol. 19, no. 8, pp. 5359–5372, Aug. 2020.

[10] J. Zhu, Z. Wang, Q. Li, H. Chen, and N. Ansari, "Mitigating intended jamming in mmWave MIMO by hybrid beamforming," *IEEE Wireless Commun. Lett.*, vol. 8, no. 6, pp. 1617–1620, Jun. 2019.

[11] V. Vadori, M. Scalabrin, A. V. Guglielmi, and L. Badia, "Jamming in underwater sensor networks as a bayesian zero-sum game with position uncertainty," in *Proc. IEEE Globecom*, 2015.

[12] A. A. Abdelnabi, V. Mancuso, and M. Ajmone Marsan, "Outage of millimeter wave links with randomly located obstructions," *IEEE Access*, vol. 8, pp. 139 404–139 421, 2020.

[13] B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, "Channel-aware adversarial attacks against deep learning-based wireless signal classifiers," *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 3868–3880, Jun. 2022.

[14] Z. Sun, S. Balakrishnan, L. Su, A. Bhuyan, P. Wang, and C. Qiao, "Who is in control? Practical physical layer attack and defense for mmWave-based sensing in autonomous vehicles," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3199–3214, 2021.

[15] 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.

[16] I. K. Jain, R. Kumar, and S. S. Panwar, "The impact of mobile blockers on millimeter wave cellular systems," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 4, pp. 854–868, Apr. 2019.

[17] G. R. MacCartney, T. S. Rappaport, and S. Rangan, "Rapid fading due to human blockage in pedestrian crowds at 5G millimeter-wave frequencies," in *Proc. IEEE Globecom*, 2017.

[18] J. Huang, C.-X. Wang, H. Chang, J. Sun, and X. Gao, "Multi-frequency multi-scenario millimeter wave MIMO channel measurements and modeling for B5G wireless communication systems," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 9, pp. 2010–2025, Sep. 2020.

[19] M. Peter, M. Wisotzki, M. Raceala-Motoc, W. Keusgen, R. Felbecker, M. Jacob, S. Priebe, and T. Kürner, "Analyzing human body shadowing at 60 GHz: Systematic wideband MIMO measurements and modeling approaches," in *Proc. IEEE EUCAP*, 2012, pp. 468–472.

[20] Y. Niu, Y. Li, D. Jin, L. Su, and A. V. Vasilakos, "A survey of millimeter wave communications (mmWave) for 5G: opportunities and challenges," *Wirel. Netw.*, vol. 21, no. 8, pp. 2657–2676, 2015.

[21] G. R. MacCartney and T. S. Rappaport, "Millimeter-wave base station diversity for 5G coordinated multipoint (CoMP) applications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3395–3410, Jul. 2019.

[22] J. C. B. Garcia, A. Sibille, and M. Kamoun, "Reconfigurable intelligent surfaces: Bridging the gap between scattering and reflection," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2538–2547, Nov. 2020.

[23] L. Feng, H. Yang, R. Q. Hu, and J. Wang, "mmWave and VLC-based indoor channel models in 5G wireless networks," *IEEE Wireless Commun.*, vol. 25, no. 5, pp. 70–77, May 2018.

[24] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, May 2019.

[25] M. Hussain, M. Scalabrin, M. Rossi, and N. Michelusi, "Mobility and blockage-aware communications in millimeter-wave vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13 072–13 086, Nov. 2020.

[26] F. Guidolin, M. Nekovee, L. Badia, and M. Zorzi, "A study on the coexistence of fixed satellite service and cellular networks in a mmWave scenario," in *Proc. IEEE ICC*, 2015, pp. 2444–2449.

[27] J. Bao, D. Sprinz, and H. Li, "Blockage of millimeter wave communications on rotor UAVs: Demonstration and mitigation," in *Proc. IEEE MILCOM*, 2017, pp. 768–774.

[28] Y. Zhu, G. Zheng, and K.-K. Wong, "Stochastic geometry analysis of large intelligent surface-assisted millimeter wave networks," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1749–1762, Aug. 2020.

[29] R. J. Weiler, M. Peter, W. Keusgen, A. Maltsev, I. Karls, A. Pudeyev, I. Bolotin, I. Siaud, and A.-M. Ulmer-Moll, "Quasi-deterministic millimeter-wave channel models in MiWEBA," *EURASIP J. Wirel. Commun. Netw.*, vol. 2016, no. 1, pp. 1–16, Mar. 2016.

[30] R. Bonjour, M. Singleton, S. A. Gebrewold, Y. Salamin, F. C. Abrecht, B. Baeuerle, A. Josten, P. Leuchtmann, C. Hafner, and J. Leuthold, "Ultra-fast millimeter wave beam steering," *IEEE J. Quantum Electron.*, vol. 52, no. 1, pp. 1–8, Jan. 2015.

[31] K. Rizk, J.-F. Wagen, and F. Gardiol, "Two-dimensional ray-tracing modeling for propagation prediction in microcellular environments," *IEEE Trans. Veh. Technol.*, vol. 46, no. 2, pp. 508–518, Feb. 1997.

[32] H. Jung and I.-H. Lee, "Outage analysis of millimeter-wave wireless backhaul in the presence of blockage," *IEEE Commun. Lett.*, vol. 20, no. 11, pp. 2268–2271, Nov. 2016.

[33] Y. Ghasempour, C. R. Da Silva, C. Cordeiro, and E. W. Knightly, "IEEE 802.11ay: Next-generation 60 GHz communication for 100 Gb/s Wi-Fi," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 186–192, Dec. 2017.

[34] M. Vallejo, J. Recas, P. G. Del Valle, and J. L. Ayala, "Accurate human tissue characterization for energy-efficient wireless on-body communications," *Sensors*, vol. 13, no. 6, pp. 7546–7569, 2013.

[35] H.-L. Chiang, W. Rave, T. Kadur, and G. Fettweis, "Hybrid beamforming based on implicit channel state information for millimeter wave links," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 2, pp. 326–339, May 2018.

[36] G. Medina, A. S. Jida, S. Pulipali, R. Talwar, T. Y. Al-Naffouri, A. Madanayake, M. E. Eltayeb *et al.*, "Millimeter-wave antenna array diagnosis with partial channel state information," in *Proc. IEEE ICC*, 2021.

[37] N. Maletic, J. Gutiérrez-Teran, and E. Grass, "Beamforming mmWave MIMO: Impact of nonideal hardware and channel state information," in *Proc. IEEE TELFOR*, 2018.

[38] L. Badia and A. Bedin, "Blockage-peeking game of mobile strategic nodes in millimeter wave communications," in *Proc. IEEE MedComNet*, 2022.

[39] W. Mei, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface-aided wireless networks: From single-reflection to multireflection design and optimization," *Proc. IEEE*, vol. 110, no. 9, pp. 1380–1400, Sep. 2022.

[40] Y. Wang, H. Lu, D. Zhao, Y. Deng, and A. Nallanathan, "Wireless communication in the presence of illegal reconfigurable intelligent surface: Signal leakage and interference attack," *IEEE Wireless Commun.*, vol. 29, no. 3, pp. 131–138, Jun. 2022.