Eavesdropping with Periscopes: Experimental Security Analysis of Highly Directional Millimeter Waves

Daniel Steinmetzer*, Joe Chen†, Jiska Classen*, Edward Knightly† and Matthias Hollick*
*Secure Mobile Networking Lab, TU Darmstadt, Germany, {dsteinmetzer, jclassen, mhollick}@seemoo.tu-darmstadt.de
†Rice Networks Group, Rice University, Houston, USA, {joe.chen, knightly}@rice.edu

***Abstract*—Next generation wireless networks utilizing millimeter waves (mm-waves) achieve extremely high data rates using narrow signal beams. Featuring a high directivity and being susceptible to blockage by objects, mm-waves are often assumed to be hard to intercept. However, small-scale objects within the beam cause reflections, thus enabling eavesdroppers to receive the signal from the outside. In this paper, we practically demonstrate the vast impact that inconspicuous objects might have on mm-wave security. Experiments on our novel mm-wave software defined radio (SDR) testbed highlight that even centimeter-scale reflectors make eavesdropping from outside the signal beam possible. More sophisticated objects increase the signal strength of the reflected signal or allow the attacker to choose its location with more latitude. Modern communication devices with metal surfaces like mobile phones or laptops cause sufficient reflections for eavesdropping as well; signals will bounce off the intended receiver. With our experiments, we demonstrate empirically that reflections enable potential attackers to achieve a received signal strength as high as that of the intended receiver with only a minimal impact on the receiver's performance. For blockages that do not impact the quality of the reception, reflections decrease the secrecy capacity by 32%. When tolerating small signal blockage towards the intended receiver, the attacker overcomes any inherent security of narrow beams and reduces the secrecy capacity to zero.**

I. Introduction

The wide bandwidth available in mm-wave bands such as 60 GHz enables higher data rates compared to legacy bands such as 2.4 and 5 GHz. Because path loss increases quadratically with carrier frequency, high antenna directionalities are required to realize links at WLAN scale distances. Indeed, the IEEE 802.11ad standard specifies beamwidths as small as 3 degrees [1]. Because of the narrow beamwidth, it is often asserted that mm-wave networks are inherently resilient to eavesdropping. It is assumed that eavesdropping would be infeasible if the eavesdropper was forced to locate itself within several degrees of the path between the transmitter and the receiver [2], [3].

In this paper, we show that eavesdroppers can successfully intercept even highly directional transmissions by creating a virtual periscope using a small-scale object as a reflector. Prior measurement studies have established that mm-wave signals reflect off of large scale surfaces such as walls and buildings [4]. However, this would make eavesdropping obvious to the receiver, as a large scale reflector would block the communication. In contrast, we show that a small-scale reflector can enable eavesdropping by simultaneously being sufficiently small to not impede the highly directive communication between the intended transmitter and receiver, and being sufficiently large or having sufficient geometric and material properties to enable the eavesdropper to decode a reflected signal (see Figure 1).

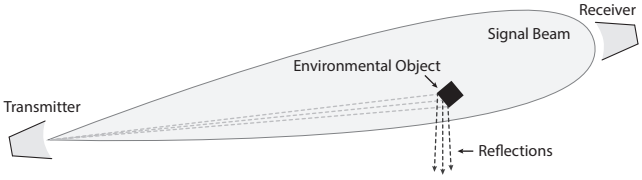


Fig. 1. Small-scale object exploited by an eavesdropper to create a virtual periscope and reflect the signal out of the intended signal beam.

We consider three classes of attackers:

- *Object manipulator.* This attacker tampers with the environment, e.g., by placing or moving small-scale physical objects. By carefully placing/manipulating objects in proximity of the signal beam, the attacker causes reflections and even directs these towards its eavesdropping antennas.
- *Nomadic attacker.* This attacker changes its position, but cannot directly manipulate physical objects within the signal beam. Nomadic attackers do not have to place any additional objects but instead find a favorable location to exploit reflections from the environment.
- *Opportunistic stationary attacker.* This attacker neither moves itself nor an environmental object (possibly to avoid suspicion or because the attacker has only left an eavesdropping 'bug' in a room). Consequently, this attacker must solely rely on high reflections towards its position from environmental objects within the narrow beam of the intended communication.

To develop an understanding of the impact of these attacks, we design and implement a mm-wave SDR-based testbed environment based on the wireless open-access research platform (WARP) [5] and off-the-shelf 60 GHz transceivers. We create a WLAN scenario comprising a transmitter and receiver with highly directional antennas and place a variety of small scale objects between them. For each object, we measure the reflections towards an eavesdropper and the blockage

of the targeted transmission. We vary the shape, size, and material of the object to represent a wide variety of common small-scale objects spanning from coffee cups to cell phones. Such objects could be placed in a particular location by the *object manipulator* or represent those that are common in the environment without object manipulation. We place the eavesdropper in an exhaustive set of locations in order to represent the *nomadic attacker* and also to evaluate the spatial footprint of an *opportunistic stationary attacker*. Exemplary experimental findings are as follows.

First, the *object manipulator* attack can be devastating. If the attacker cannot control the orientation of the small-scale object, a cylindrical object such as a coffee cup sufficiently disperses the reflective signal to enable eavesdropping from an extensive area. On the contrary, if the object manipulator controls both the location and orientation of the small-scale object, we show that a small concave object can be exploited to focus energy towards the eavesdropper. For example, bending a metal reflector leads to a received signal strength at the eavesdropper as high as that at the intended receiver.

Second, for a particular placed object, we explore the *nomadic attack*. Here, the eavesdropper exploits an existing small-scale object and searches an acceptable location to receive reflections. The nomadic eavesdropper seeks to find such a location with minimal change in position to avoid detection. We show that reflections with high signal strength exist, privileged for eavesdropping.

Last, the *opportunistic stationary attacker* has a relatively small footprint when aiming at high signal strength. Consequently, this attack likely needs to compensate for poor signal quality. Besides using expensive antenna apertures this attack might be distributed to be effective, e.g., with eavesdropping elements planted throughout the physical space.

The remainder of this paper is structured as follows. We provide a concise background on mm-wave propagation and outline our system and adversary model in Section II. This is followed by a description of our testbed implementation in Section III. In Section IV, we conduct practical testbed experiments to evaluate our attack scenarios. Section V summarizes related work on mm-wave communication and physical layer security. Finally, we discuss our findings and conclude this paper in Section VI.

II. System and Adversary Model

Our system model consists of three communication parties (1) a transmitter Alice, (2) a receiver Bob, and (3) an eavesdropper Eve. Alice transmits a signal towards Bob that she wants to keep secret from Eve by using a narrow beamwidth. We assume that both antennas of Alice and Bob are perfectly aligned and transmit in the optimal direction. Eve aims at revealing information Alice sends to Bob without obstructing it. She tries to receive reflections from objects in the signal beam. For convenience, we assume that Eve uses the same hardware as Alice and Bob. In terms of transmission, Eve acts passively and is only listening for signals.

In the following, we concisely give mm-wave background, set up a link budget model, describe all adversary models in detail, provide information on the environment we are considering, and discuss our performance metrics.

A. Background on mm-Waves

The carrier frequencies of mm-waves are between 30 and 300 GHz, so their wavelength is less than a centimeter. This leads to different propagation phenomena than those happening in lower frequencies. Without limitation, in the following, we assume a typical carrier frequency of 60 GHz and corresponding wavelength of 5 mm. Signals are subject to high reflections and penetration [4]. Rough surfaces lead to significant scattering effects while diffraction effects become marginal [6]. These propagation effects of mm-waves call for a fundamental rethinking of protocol and system design. The high attenuation of mm-waves is a huge challenge when transmitting over long distances—highly-directional antennas or antenna arrays are required. These provide strong antenna gains by narrowing their transmission beam. The IEEE 802.11ad standard [7] specifies beamforming with antenna arrays to achieve beamwidths of 3°. By using horn antennas with large apertures, similar effects are achievable with just one antenna. Our hardware features beamwidths of 7° at minimum. Outside of the designated beam, the signal strength decreases massively and decoding becomes impossible. The sender and receiver align their beam using a sweeping and a beam refinement protocol [1]. However, beamforming and antenna alignment are still key challenges for mm-wave communication [3]. We next provide a free space path loss (FSPL) model describing the link budget in communication with reflections.

B. Link Budget

The FSPL model is a good approximation for the propagation loss experienced at a certain distance from the transmitter in free space without any environmental obstacles. According to [8], we compute the FSPL as

$$\text{FSPL} = \left(\frac{4\pi df}{c}\right)^2, \tag{1}$$

where f is the carrier frequency of the signal, d the distance to the transmitter, and c the speed of light. Since the FSPL increases with f^2, it is significantly higher for mm-waves compared to legacy frequency bands.

In this work, we consider objects inside the signal beam that cause reflections and blockage. In the FSPL model, we express this by summing in additional reflection gains and blocking losses. The received signal strength over reflections in decibel (dB) is expressed by

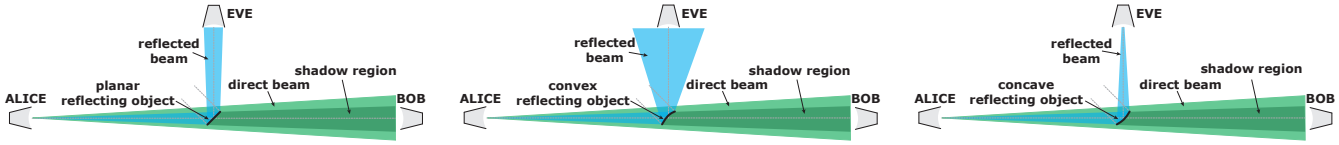
$$P_\text{r}[\text{dB}] = P_\text{tx} + G_\text{tx} - \text{FSPL}_d + G_\text{r} + G_\text{rx}, \tag{2}$$

where P_tx is the transmitted power, G_tx and G_rx are the antenna gains at the transmitter and receiver, FSPL_d denotes the FSPL over a certain distance d, and G_r is the reflection gain. In terms of blockage, the received signal strength is expressed by

$$P_\text{b}[\text{dB}] = P_\text{tx} + G_\text{tx} - \text{FSPL}_d - L_\text{b} + G_\text{rx}, \tag{3}$$

where L_b denotes the blockage loss.

Assuming that all devices have identical hardware and operate at the same beamwidth, which translates into $G_\text{tx} = G_\text{rx}$ and P_tx being constants, the received signal strengths only depend on the reflectivity, blockage and distance between devices. This implies that variations in distance can compensate for bad reflectivity or blockage and vice versa.



(a) planar reflecting object (b) convex reflecting object (c) concave reflecting object

Fig. 2. System model showing the setup of Alice, Bob and Eve with reflections of the signal beam on different shapes of objects.

Practical antennas for mm-waves achieve directivity gains above 20 dB. Objects of different size, shape and orientation may feature different characteristics. Although this model does not incorporate any misalignment of the antennas and reflectors, it provides a basic understanding of the scenarios covered in this work and guides us in specifying the attacker models in the following.

C. Attacker Models

Throughout this paper, we distinguish three attacker models, (1) the object manipulator moving and placing objects to cause reflections towards a fixed eavesdropping position, (2) the nomadic attacker moving itself and exploiting reflections of existing objects in the environment it cannot change, and (3) the opportunistic stationary attacker that can neither move nor manipulate the environment and must try to eavesdrop from its original location.

1) The object manipulator: This model considers Eve to be located at a fixed position outside of the signal beam. From there it is impossible to receive the signal directly. However, Eve tampers with the environment and places arbitrary objects to cause reflections towards her direction. She is able to steer her antenna towards this object to optimally receive reflections of the transmitted signal. By doing so, she aims at obtaining a signal quality sufficient for information decoding. At the same time, Eve tries to remain invisible to Alice and Bob by causing only marginal blockage of the direct signal transmission.

2) The nomadic attacker: In contrast to the previous model, Eve cannot change the environment but tries to exploit existing environmental reflections. She can freely choose a location outside the beam and steer her antenna towards any reflector in the environment. Since she cannot affect the blockage at all, Eve only aims at maximizing her received signal quality by seeking for the optimal eavesdropping location and orientation. Even though using existing objects might be harder, detecting this attack is difficult because nothing in the environment changes from normal operation.

3) The opportunistic stationary attacker: In the final model, Eve can neither manipulate the environment nor move herself to an optimal position. This means that Eve must rely on environmental objects in the hope that the signal will reflect towards her. Like for the nomadic attacker, Eve does not affect blockage, but she can only steer her antenna from a fixed location for best reception. This is the weakest adversary model, but it makes Eve nearly impossible to detect because nothing changes in the environment, including Eve herself.

D. Eavesdropping Topology & Environment

Throughout this paper, we assume reflecting objects to be directly on the center line of the narrow beam between Alice and Bob, which is the optimal case that causes both the highest reflection and blockage. However, a reflector anywhere within the signal beam can be used to perform the attack. As illustrated in Figure 2, Bob receives the signal in the shadow region, blocked by the reflecting object. Eve, outside the direct signal beam, only receives the reflections bouncing off the object. The reflecting object is considered with different characteristics, in particular its reflectivity and blockage. Both vary with different materials and sizes, but also with the structure and shape of the object. We consider planar reflectors (see Figure 2a) for which transmitted and reflected beams have the same width, convex reflector shapes (see Figure 2b) that disperse the signal to different directions, as well as concave reflector shapes (see Figure 2c) that focus the signal towards a certain focal point. In our analysis, we only encounter first-order reflections and do not consider additional reflections on multiple objects.

E. Performance Metrics

To evaluate performance, we measure both the signal strength and bit error rate (BER) in transmission. From the signal strength at Bob and Eve, we determine the effective reflectivity and blockage of an object as

$$r = \max\left(s_{\text{Eve}}\right) \;/\; \max\left(s_{\text{opt}}\right) \tag{4}$$

$$b = 1 - \left(\max\left(s_{\text{Bob}}\right) \;/\; \max\left(s_{\text{opt}}\right)\right) \tag{5}$$

where s_{Bob} and s_{Eve} are the received signal strengths at Bob and Eve in linear scale and s_{opt} the optimal received signal strength from a direct transmission without reflectors. We further utilize the secrecy capacity [9] to express the performance of eavesdropping as

$$c_s = \log_{10}\left(1 + s_{\text{Bob}}\right) - \log_{10}\left(1 + s_{\text{Eve}}\right) \tag{6}$$

and normalize this value to the maximum in optimal transmission. The secrecy capacity represents the advantage in signal quality of Bob over Eve by residing in the beam. Its maximum value of 1 means that Eve is unable to decode anything from the signal. The lowest value of 0 indicates that the signal strength at Eve is at least as high as at Bob which easily facilitates eavesdropping. The effective blockage represents attenuation of the signal by placing the reflector in the beam. The reflectivity is the relative reflected signal strength compared to the signal strength at Bob in unblocked transmission. The secrecy capacity considers both, blockage and reflectivity. The eavesdropper's goal is to lower the secrecy capacity while reducing the effective blockage to stay undetected.

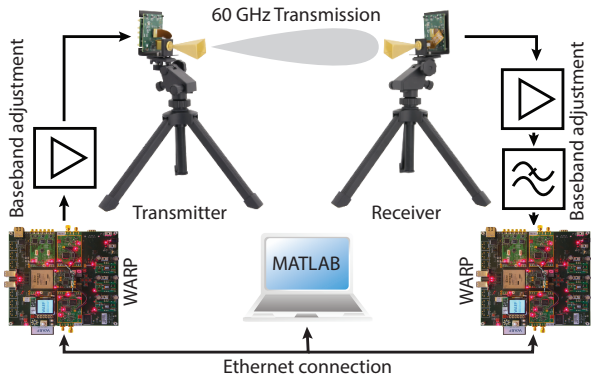


Fig. 3. Hardware setup showing interconnection of WARP and the mm-wave transceivers.

III. Testbed Implementation

Our novel implemented testbed brings the advantages of SDRs to mm-wave applications and enables transmission of arbitrary waveforms over wireless links at 60 GHz. It supports variable data modulation schemes and adjustable frame formats. The hardware is composed of WARP [5], commercial mm-wave transceivers from the Pasternack/VubIQ 60 GHz development system [10], and connecting circuits for signal adjustments as shown in Figure 3 and described in the following.

WARP is a platform for rapid prototyping of wireless communication systems. In combination with the WARPLab firmware, interfacing analog signals from MATLAB becomes possible. We utilize two WARP nodes with extension boards for providing in- and output of analog baseband signals. The nodes are synchronized over Ethernet and controlled from one MATLAB instance.

The Pasternack/VubIQ 60 GHz development system consists of a transmitter and a receiver with exchangeable horn antennas. Throughout this paper, we use the narrowest available beamwidth of 7°. The transceiver boards provide adjustable signal amplifiers, filters, and mixers for up- and down-converting the signal to available channels specified in IEEE 802.11ad. All transceivers are equipped with internal clocks but configured to share a common one for simplicity.

Since the output signals of the WARP do not match the mm-wave transceivers' input specifications and vice versa, we need to adjust the baseband signals. At the transmitter side, we convert the single-ended I/Q output of the WARP to differential I/Q and attenuate the amplitude. At the receiver, we amplify the signal again to get the maximum resolution from the WARP's analog-to-digital converters. Furthermore, we add a low-pass filter to prevent aliasing effects. For these signal adjustments we utilize common differential operational amplifiers ('op-amps') and basic components mounted on custom circuit boards.

Our implementation also incorporates data encoding and decoding. We currently support single-carrier transmission with binary phase-shift-keying (BPSK) or quadrature-amplitude-modulation (QAM). For delay detection and channel equalization, we equip each transmission frame with a pre-known BPSK encoded preamble. For each transmission, we evaluate the BER over all data symbols as well as a signal strength indicator of the received preamble. Throughout this paper, we present our evaluation results using 4-QAM for data encoding. With this modulation, we are able to transmit data with an BER as low as 0.09 over an distance of 2 m.

IV. Testbed Experiments

To demonstrate the practicality of eavesdropping on mm-waves, we conduct five different experiments that show:

1) the feasibility of eavesdropping on reflections,
2) reflector location optimization,
3) freedom-of-space from scattering,
4) focused reflections for improved signal strength, and
5) reflections on common communication devices.

In all these experiments, we mount the transmitter on a rotating table to steer the signal in different directions. This ensures that the signal beam is in at least one orientation optimally aligned to the receiver. We then place the receiving antenna at different locations as seen in Figure 4. Depending on the experiment, we evaluate different distances of Bob in direct line of transmission and different angles of Eve with constant distance to the reflector. Eve's initial orientation is perpendicular to the transmission direction. In every experiment, we conduct 100 iterations and state the 95% confidence intervals for measurements of BER and signal strength. The signal strength is expressed in dB and normalized to the noise floor to be always greater than zero if a signal is received. In the following, we discuss each experiment in detail.

A. Baseline and Setup

Before starting the individual experiments, we analyze the baseline and measure the performance of Bob and Eve without any objects in the beam. These measurements produce s_{opt}, which is needed for the effective reflectivity and blockage calculations via Equations (4) and (5) in subsequent experiments with reflectors. We distribute the antennas for Alice and Bob at a fixed distance of 2 m away from each other. The evaluated objects are placed in the center and optimally oriented to reflect the signal towards Eve, who resides 1 m away, oriented perpendicular to the transmission direction.

In optimal transmission without any objects in the beam, Bob's signal strength peaks at perfect alignment of 0° with 23.9 dB, as shown in Figure 5. Since we are using an antenna with a beamwidth of 7°, the signal strength drops around 3 dB

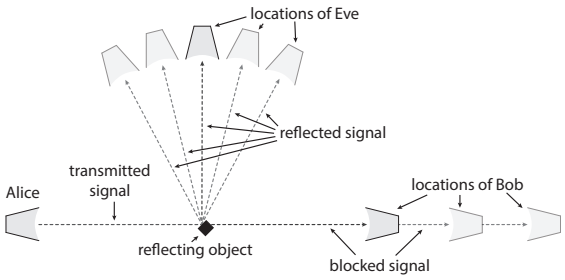


Fig. 4. Experimental setup showing the communication parties and location variations analyzed throughout our evaluation.

at an offset angle of 3.5°. Due to the narrow beamwidth, we measure a signal strength of 0 dB at Eve which is unsurprising since Eve resides outside the beam.

B. Feasibility of Eavesdropping on Reflections

In our first experiment, we evaluate the impact of an object manipulator placing arbitrary objects in the signal beam to cause reflections towards an eavesdropping antenna. Although it is well-known that mm-waves reflect off metallic reflectors and many other materials, we investigate the critical point between reflector size and material and the effective blockage and reflectivity. An optimal reflector maximizes reflectivity for eavesdropping but simultaneously minimizes blockage to avoid being detected. In particular we use a metal block and small metal sheets of different sizes. We further use a block of wood and acrylic glass as reflecting objects. Given the beamwidth of 7°, all objects (except the acrylic glass) are significantly smaller than the beam, which has a width of 12 cm at the distance of 1 m.

The larger metal sheet and the wood block cause high attenuation, while all other objects only marginally block the signal. Apparently, metal causes strong reflections, but their strength highly depends on the reflector's size. Only the smallest 10x10 mm^2 metal sheet results in a low received signal strength at Eve. Even the wood block and acrylic glass, both with plain surfaces, cause considerable reflections. The effective reflectivity r (Equation (4)) and blockage b (Equation (5)) of each object is shown in Figure 6. The metal block has an effective reflectivity of 96 %, which means that the signal quality at Eve is nearly as good as at Bob. However, this reflectivity comes with high blockage of 63 % and might be easily detectable. The smaller metal sheets only block less than 1 % of the signal and still provide a notable effective reflectivity of up to 16 %. With a reflectivity of 47 % and a blockage of 10 %, the acrylic glass is good tradeoff between both characteristics.

All analyzed objects decrease the secrecy capacity c_s (Equation (6)) of the system. The small 25x25 mm^2 metal sheet decreases the secrecy capacity by 32 %. The metal block of size 70x70 mm^2 diminishes the secrecy capacity to 1 %, meaning that Eve's reception is nearly as good as Bob's.

C. Reflector Location Optimization

While the last section revealed the feasibility of eavesdropping on reflections, the question on where to place the reflector is still unanswered. In our second experiment, we aim to determine the optimal reflecting location that diminishes the secrecy capacity of Alice's transmission. We let the object manipulator optimize its performance by varying the relative object location within the beam. To cause the reflections, we use a medium size metal sheet of size 70x70 mm^2. While the reflector and the eavesdropper are at fixed locations separated by 1 m, we set up the receiving antenna for Bob at distances of 1 m, 2 m, and 3 m away from the reflecting object. This results in a communication distance of 2 m, 3 m, and 4 m between Alice and Bob, respectively. The eavesdropping distance is constantly 2 m. By varying only the distance of Bob and not that of Eve, we ensure to maintain the same reflections in all evaluation steps. However, varying this distance affects

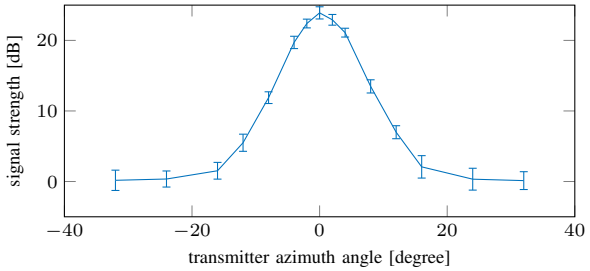


Fig. 5. Received signal strength at Bob in optimal transmission without any object in the path.

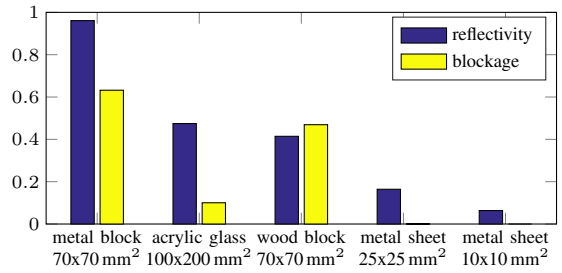


Fig. 6. Reflectivity and blockage characteristics of different objects placed in the transmission.

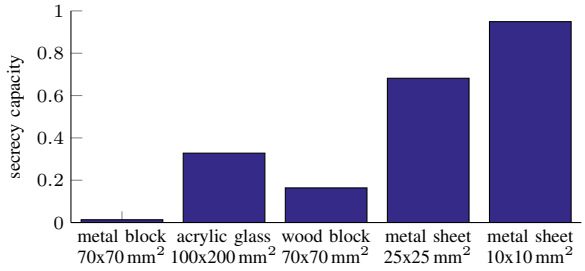


Fig. 7. Achievable secrecy capacity with different objects in the signal beam.

the optimal received signal strength s_{opt} at Bob in direct transmission without blockage. For larger distances between Alice and Bob, the relative eavesdropping distance decreases and we observe different performances.

By just considering shadowing effects, we would expect Bob's signal strength s_{Bob} to decrease similar to s_{opt} and the effective blockage to be constant. In the line-of-sight (LOS) setting, Bob always resides in the shadow region. However, as seen in Figure 8, the blockage decreases with Bob's distance. This effect must be caused by diffraction, which still occurs in mm-waves around small obstacles [11], [12]. Diffraction, by implication, assists the eavesdropper in remaining invisible by lowering the effective blockage. Furthermore, the effective reflectivity increases with Bob's distance. The reflected signal does not change, but, since s_{opt} decreases, the relation of Eve's over Bob's signal strength becomes greater.

Since the effective reflectivity increases more than the blockage decreases, the secrecy capacity decreases with Bob's distance. In this particular experiment, we observe the secrecy capacity to decrease by 81 % when moving Bob's antenna from 1 m to 3 m away. The optimal position for placing the reflecting

object is, obviously, close to Alice. By placing an object there, Eve not only increases the reflected signal strength but also can be less afraid of blocking too much of the beam.

D. Obtaining Freedom-of-Space from Scattering

In this experiment, we analyze the freedom-of-space that a nomadic attacker has in choosing its location for a fixed reflector and whether scattering helps the opportunistic stationary attacker. The more locations from which Eve can successfully eavesdrop as an attacker, the more likely an opportunistic stationary attacker can be successful despite not moving itself nor altering the environment. We setup this experiment as the first one (Subsection IV-B), but instead of placing Eve only perpendicular to the beam directions, we move her on a circle around the reflecting object. Figure 9 shows the reflected signal strength with different reflectors over varying eavesdropping angles. With the metal block of 70x70 mm^2 placed as reflector, we observe a strongly decreasing signal strength when moving away from the optimal position of 90°. With an offset of 7°, the signal strength already drops by around 10 dB. Round objects like a porcelain cup and a metal shielded cup reflect much weaker than the planar metal sheet. However, they feature a nearly constant signal strength over a wide range of eavesdropping positions; they scatter the signal to multiple directions.

The secrecy capacities shown in Figure 10 support that attackers residing not in the optimal reflection direction might improve their performance with round reflectors. In this particular scenario, we observe that the round metal reflector provides better reflections than the planar one at an offset angle of approximately 10°. The attacker benefits from this when only the coarse beam direction is known, or in the case of being limited in movements as the opportunistic stationary attacker is.

E. Focusing the Reflected Signal Beam

To analyze if reflectors can bundle the signal power towards the attacker, we use a planar, concave, and convex metal sheet of size 100x200 mm^2 as reflecting object. In contrast to the previous experiments, we use larger reflectors, because they are easier to bend to the correct curvature. Figure 11 shows the signal strength at Eve with these objects over the transmitter's azimuth angle. With the insights from the previous experiment, it is obvious that the convex reflector provides a low signal strength. However, slight deformations of only a few millimeters are sufficient to optimally focus the beam for our evaluation setup where Alice and Eve are are both 1 m away from the reflector. Doing so, we obtain an increase in signal strength of 1.5 dB compared to the planar reflector. Since we do not vary the size of the object, the blockage remains constant, but as depicted in Figure 12, the effective reflectivity varies. Concave reflectors bundle the reflected signal towards a focal point at which very high signal strengths are achievable. Object manipulators as well as nomadic attackers can exploit this to obtain better eavesdropping performance. However, they only benefit from focusing the signal beam when residing exactly at the focal point, which makes it unfavorable for the opportunistic stationary attacker. Even small misalignments in position and orientation lead to massive losses in signal strength.

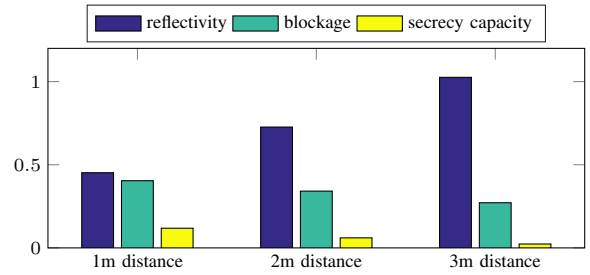


Fig. 8. Effective reflectivity, blockage and secrecy capacity for Alice and Eve at fixed positions and Bob with varying distance. An increasing distance of Bob leads to higher reflectivity and lower blockage and secrecy capacity.

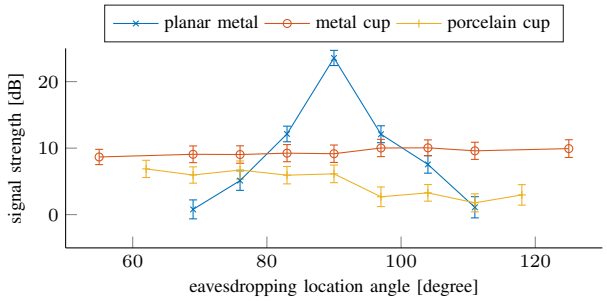


Fig. 9. Effective reflectivity in dependency of the eavesdropper's locations.

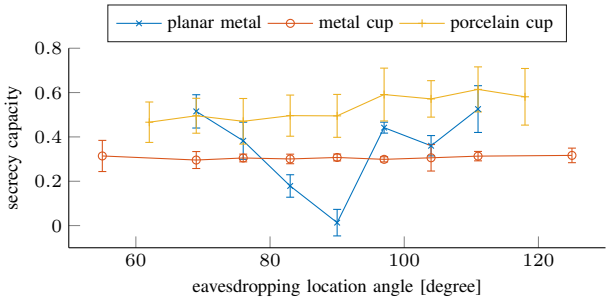


Fig. 10. Secrecy capacity's dependency on the eavesdropper's location.

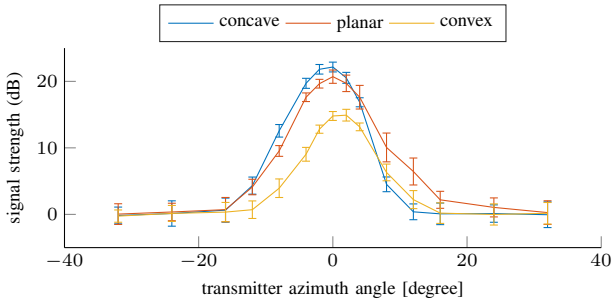


Fig. 11. Signal strength of the eavesdropped signal with bended reflectors.

F. Reflections on Common Communication Devices

Even normal communication devices—which will be equipped with mm-wave hardware in the near future—cause reflections towards potential eavesdroppers. These devices are

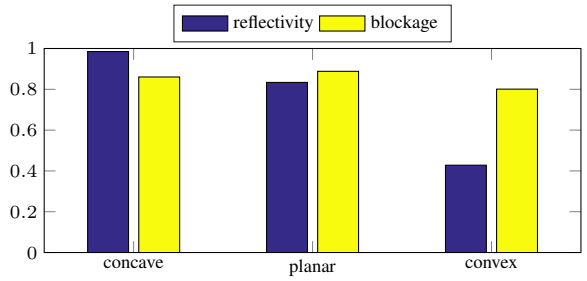


Fig. 12. Blockage and reflectivity of object with different bendings.

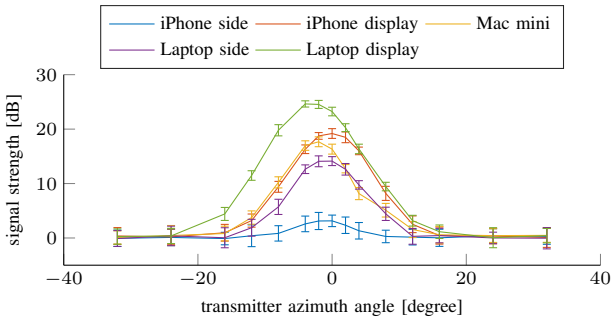


Fig. 13. Reflected signal strength from common communication devices.

typically made of materials with high reflectivity. Both nomadic attackers and opportunistic stationary attackers can take advantage of these reflections despite not being able to place their own reflectors. To analyze how strong these reflections are in practice, we place several communication devices in our evaluation setup. In particular, we use an iPhone 6, a laptop, and a Mac mini with different orientations. Again, we place the devices at a distance of 1 m away from the transmitter and receive the reflected signal at 1 m distance perpendicular to the transmission direction. As shown in Figure 13, the signal reflected at a laptop display achieves the highest possible strength of 24 dB. This is as high as we observed in direct transmission without reflectors. The side of the laptop, the iPhone display, and the Mac Mini also achieve reflected signal strengths between 14 and 19 dB. Only the side of an iPhone is too small and curved to cause significant reflections towards the eavesdropping antenna; the signal strength remains below 4 dB. These results imply that reflections can be caused by not only specifically placed reflectors but also inconspicuous everyday devices. In a typical communication scenario where one device transmits to another, the signals reflected on the surface of the receiver can enable a nomadic attacker as well as the opportunistic stationary attacker to eavesdrop without changing the environment at all.

G. Summary

In our practical evaluation with testbed experiments, we show with simple objects that eavesdropping on reflected mm-wave transmissions is possible and enables attackers to reside outside the designated signal beam. We further show, that varying the reflector position affects the eavesdropping performance and that small scale diffraction helps to be undetectable. By bending objects, we outline that concave surfaces scatter the signal and increase the freedom-of-space at cost of signal strength and that convex surfaces focus the beam and increase the signal strength at certain positions. Finally, we demonstrate that not only additional reflectors but also the intended recipient's devices can cause significant reflections of mm-waves. A summary of all evaluated objects along with their measurement results is provided in Table I.

V. Related Work

Eavesdropping on traditional wireless communication systems is typically assumed as always feasible. Signals are transmitted omni-directionally, thus that attackers only have to reside in range to eavesdrop. For mm-wave communication, the eavesdropping requirements change. The highly directional communication links are commonly seen as more resilient against eavesdropping. To constitute the fundamental differences, we summarize related work on (1) signal propagation and wireless channels characteristics of mm-waves, (2) ray-tracing approaches for mm-waves propagation, as well as (3) incipient stages of physical layer security in mm-waves in the following subsections.

A. Propagation & Channel Characteristics

Early measurements of the 60 GHz channel characteristics were taken in the 1990s [13] and revealed that the limiting weather effects and atmospheric absorptions are negligible for short distances [14]. However, it took some time to discover the benefits for local wireless communication [15], [16] and final standardization within IEEE 802.11ad [7] in 2012. Several works analyzed how mm-wave signals reflect on building materials and indoor structures [17]–[19]. Their findings imply that reflections should not be neglected in indoor environments and also enable communication via indirect line-of-sight paths. [20] determined the blockage of certain objects and humans in the signal beam. Diffraction turns out to be much less relevant than in legacy communication systems [6], but still occurs on small objects [11], [12]. Polarization of signals is considered in [21] and turns out to be important due to low multi-path effects. The work in [22] analyzes MAC layer considerations of mm-wave propagation effects. Complete statistical channel models for typical indoor environments have been established in [6], [23] that enable precise simulations for common wireless applications but do not incorporate special effects such as small-scale reflections.

B. Ray-tracing mm-Waves

Since mm-waves propagation has a quasi-optical nature [24], ray-tracing becomes feasible for analyzing the signal paths. Ray-tracing, typically applied for light-waves and image generation in computer graphics, models reflections and attenuation based on approximate solutions to Maxwell's equations and thereby predicts the received signal strength at a certain position in a given environment. In [25], ray-tracing for mm-waves is verified by comparing real-world measurements in a meeting room to a 3D model. Yet, due to the small wavelength, slight position offsets lead to different results, and the resulting channel predictions have deficits in the time domain. Ray-tracing has also been proposed for lower

TABLE I. SUMMARY OF ALL EVALUATED OBJECTS REFLECTING THE SIGNAL TOWARDS AN EAVESDROPPING ANTENNA OUTSIDE THE SIGNAL BEAM.

Analyzed Object	Size	Section	Effective Reflectivity	Effective Blockage	Secrecy Capacity	Impacts
metal block	70x70 mm^2	IV-B, IV-D	0.96	0.63	0.01	very good reflections but also high blockage
wood block	70x70 mm^2	IV-B	0.41	0.46	0.16	medium reflections and high blockage
acrylic glass	100x200 mm^2	IV-B	0.47	0.10	0.33	good tradeoff between reflections and blockage
metal sheet	25x25 mm^2	IV-B	0.16	0.00	0.68	no blockage but still some reflections
metal sheet	10x10 mm^2	IV-B	0.06	0.00	0.95	too small for significant reflections
metal sheet	70x70 mm^2	IV-C	0.45	0.40	0.12	medium reflections and significant blockage
metal cup	cup size	IV-D	0.20	0.62	0.30	scattering to all directions
porcelain cup	cup size	IV-D	0.14	0.48	0.46	poor reflections but still scatters
metal sheet	100x200 mm^2	IV-E	0.83	0.80	0.00	good reflections but very high blockage
convex metal sheet	100x200 mm^2	IV-E	0.42	0.89	0.00	good scattering but very high blockage
concave metal sheet	100x200 mm^2	IV-E	0.98	0.86	0.00	focuses the reflections but very high blockage
iPhone display	n/a	IV-F	0.58	—	—	good reflections
iPhone side	n/a	IV-F	0.09	—	—	poor reflections due to non-optimal surface
laptop display	n/a	IV-F	1.00	—	—	perfect reflections
laptop side	n/a	IV-F	0.32	—	—	low reflections on non-solid surface
Mac mini	n/a	IV-F	0.49	—	—	acceptable reflections

radio frequency indoor [26] and outdoor [27] propagation. However, ray-tracing typically does not model diffraction and interference, which makes it inaccurate for shadow regions behind small-scale objects and multi-antenna systems. To the best of our knowledge, no accurate ray-tracing models for small-scale objects in mm-waves exist, which makes analyzing the eavesdropping scenario with ray-tracing methods inappropriate.

C. Physical Layer Security in mm-Waves

Physical layer security aims to secure communication system based on signal propagation phenomena. One possibility in this area is to extract symmetric keys from random channel observations to encrypt the transmitted data on higher layers. In [28], keys are extracted from a mm-wave channel impulse response. Their experiments show that moving objects and people in the environment cause significant changes in the channel measurements, which increase the quality of extracted keys. Another method that applies mm-waves for physical layer security is based on jamming or artificial interferences. For lower frequencies, jamming schemes that specifically distort eavesdroppers are well known [29], [30]. A similar approach in the mm-wave band uses a technique called antenna subset modulation [31]. By utilizing only a random selection of antennas in an array, the constellation in sidelobes blurs. While the intended receiver in the desired direction is unaffected by this, possible eavesdroppers are distorted and prevented from decoding. However, an antenna subset is a relatively small keyspace that might be revealed by known-plaintext attacks as already shown against physical layer security mechanisms in lower frequency [32]. In general, applying artificial interferences on mm-waves might have less impact on aligned antennas. Directional antennas are less affected by jammers to those they are not aligned to. Novel mechanisms to protect mm-wave communication on the physical layer based on the special propagation characteristics are necessary [3]; existing security schemes cannot be simply applied to mm-waves.

VI. DISCUSSION AND CONCLUSION

Although millimeter wave communication systems are often marketed as intrinsically secure against eavesdropping from outside the signal beam, our practical work demonstrates that this is not true. We introduce three distinct attacker models against mm-wave communication systems, and design and implement a mm-wave SDR testbed platform to practically evaluate the attack performance.

Attackers of the object manipulator class can tamper with the environment by placing objects in the signal beam to cause reflections towards a fixed eavesdropping antenna. Using this method, they can achieve good reflections with low blockage. Our experiments show that it is possible to place objects in such a way that reflections facilitate eavesdropping: objects as small as 25x25 mm^2 decrease the secrecy capacity by 32 % with zero effective blockage. Sophisticated object structures can focus the signal beam towards a certain eavesdropper. For a fixed object size, the blockage remains nearly independent from the object's shape and orientation, but the effective reflectivity towards a certain eavesdropping position varies.

Nomadic attackers fall into a significantly weaker attacker class; they cannot actively manipulate the environment. Yet, they can also achieve a very good eavesdropping performance by exploiting reflections at the intended recipient of the communication. Our results show that device-incident reflections of common communication devices, such as a desktop and notebook computer or a mobile phone, are sufficient to enable eavesdropping: essentially the mm-wave recipient becomes the traitor to itself. For example, an iPhone display can yield a very high reflectivity of 58 %. In such a scenario, the attacker only has to find a good eavesdropping location, point its antenna toward the receiver, and then eavesdrops on the reflected signals that bounce off of the intended receiver.

The opportunistic stationary attacker is less powerful; it must eavesdrop from a given location without being able to manipulate objects. Our results show that round objects, such as a coffee cup, disperse the signal into multiple directions,

thus facilitating attacks from opportunistic attackers. In most cases, however, we found the signal to be too weak for effective eavesdropping if the attacker was off by a few degree from the optimal angle of reflection. More powerful opportunistic eavesdroppers, such as multiple cooperative eavesdroppers launching a distributed attack, might be able to make opportunistic eavesdropping practical, though.

Our findings prove that even highly directional mm-wave transmissions are not intrinsically secure against attackers outside the beam. This motivates the design and implementation of novel physical layer security mechanisms that exploit the special propagation characteristics and high directionality of mm-waves to secure wireless communication systems. Future work should come up with possible countermeasures to prevent against such low level eavesdropping attacks.

ACKNOWLEDGMENT

This work was supported by the German Federal Ministry of Education and Research (BMBF) within EC SPRIDE, by the German Research Foundation (DFG) within the project CROSSING and the Hessian LOEWE excellence initiative within CASED. This research was also supported by Cisco Systems, Intel, the Keck Foundation, and by NSF grants CNS-1444056, CNS-1126478 and CNS-1012831.

REFERENCES

[1] T. Nitsche, C. Cordeiro, A. B. Flores, E. W. Knightly, E. Perahia, and J. C. Widmer, "IEEE 802.11ad: directional 60 GHz communication for multi-Gigabit-per-second Wi-Fi," *IEEE Communications Magazine*, vol. 52, no. 12, pp. 132–141, 2014.

[2] L. E. Frenzel, "Millimeter Waves Will Expand the Wireless Future," *Electronic Design*, no. 04/2013, pp. 30–36, 2013.

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

[4] T. S. Rappaport, R. W. Heath Jr, R. C. Daniels, and J. N. Murdock, *Millimeter Wave Wireless Communications*. Prentice Hall, Sep. 2014.

[5] WARP Project. [Online]. Available: http://warpproject.org

[6] A. Maltsev, R. Maslennikov, A. Sevastyanov, A. Lomayev, A. Khoryaev, A. Davydov, and V. Ssorin, "Characteristics of indoor millimeter-wave channel at 60 GHz in application to perspective WLAN system," in *European Conf. on Antennas and Propagation (EuCAP)*. IEEE, 2010.

[7] IEEE 802.11 WG, "IEEE 802.11ad Wireless LAN MAC and PHY Specifications Amendment 3: Enhancements for Very High Throughput in the 60 GHz Band," 2012.

[8] J. C. Whitaker, *The Electronics Handbook, Second Edition*. CRC Press, Apr. 2005.

[9] J. Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels," *IEEE Int. Symp. on Information Theory*, 2006.

[10] Pasternack Enterprises. Pasternack 60 GHz Transmit/Receive (Tx/Rx) Development System (PEM003-KIT). [Online]. Available: http://www.pasternack.com/60-ghz-development-systems-category.aspx

[11] M. Jacob, S. Priebe, R. Dickhoff, T. Kleine-Ostmann, T. Schrader, and T. Kürner, "Diffraction in mm and Sub-mm Wave Indoor Propagation Channels," *IEEE Trans. on Microwave Theory and Techniques*, vol. 60, no. 3, pp. 833–844, 2012.

[12] T. Kleine-Ostmann, M. Jacob, S. Priebe, R. Dickhoff, T. Schrader, and T. Kürner, "Diffraction measurements at 60 GHz and 300 GHz for modeling of future THz communication systems," *Int. Conf. on Infrared, Millimeter, and Terahertz Waves (IRMMW-THz)*, 2012.

[13] P. F. M. Smulders and A. G. Wagemans, "Wideband indoor radio propagation measurements at 58 GHz," *Electronics Letters*, vol. 28, no. 13, pp. 1270–1272, 1992.

[14] T. Manabe, Y. Miura, and T. Ihara, "Effects of antenna directivity on indoor multipath propagation characteristics at 60 GHz," *IEEE Int. Symp. on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 1995.

[15] P. Smulders, "Exploiting the 60 GHz band for local wireless multimedia access: prospects and future directions," *IEEE Communications Magazine*, vol. 40, no. 1, pp. 140–147, 2002.

[16] E. Perahia, C. Cordeiro, M. Park, and L. L. Yang, "IEEE 802.11 ad: Defining the next generation multi-Gbps Wi-Fi," in *IEEE Consumer Communications and Networking Conf. (CCNC)*, 2010.

[17] B. Langen, G. Lober, and W. Herzig, "Reflection and transmission behaviour of building materials at 60 GHz," *IEEE Int. Sym. on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 1994.

[18] J. Ahmadi-Shokouh, S. Noghanian, E. Hossain, M. Ostadrahimi, and J. Dietrich, "Reflection Coefficient Measurement for House Flooring Materials at 57-64 GHz." *IEEE Global Communications Conf. (GLOBECOM)*, 2009.

[19] K. Sato, T. Manabe, T. Ihara, H. Saito, S. Ito, T. Tanaka, K. Sugai, N. Ohmi, Y. Murakami, M. Shibayama, Y. Konishi, and T. Kimura, "Measurements of reflection and transmission characteristics of interior structures of office building in the 60-GHz band," *IEEE Transactions on Antennas and Propagation*, vol. 45, no. 12, pp. 1783–1792, 1997.

[20] S. Singh, F. Ziliotto, U. Madhow, E. Belding, and M. Rodwell, "Blockage and directivity in 60 GHz wireless personal area networks: from cross-layer model to multihop MAC design," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 8, pp. 1400–1413, 2009.

[21] A. Maltsev, E. Perahia, R. Maslennikov, A. Sevastyanov, A. Lomayev, and A. Khoryaev, "Impact of Polarization Characteristics on 60-GHz Indoor Radio Communication Systems," *IEEE Antennas and Wireless Propagation Letters*, vol. 9, pp. 413–416, 2010.

[22] S. Sur, V. Venkateswaran, X. Zhang, and P. Ramanathan, "60 GHz Indoor Networking through Flexible Beams: A Link-Level Profiling," *to appear in ACM Conf. of the Special Interest Group for the Computer Systems Performance Evaluation Community (SIGMETRICS)*, 2015.

[23] J. Schönthier, "WP3-study the 60 GHz channel and its modelling."

[24] A. Maltsev, R. Maslennikov, A. Sevastyanov, A. Khoryaev, and A. Lomayev, "Experimental investigations of 60 GHz WLAN systems in office environment," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 8, pp. 1488–1499, 2009.

[25] W. K. M. Peter, W. Keusgen, and R. Felbecker, "Measurement and Ray-Tracing Simulation of the 60 GHz Indoor Broadband Channel: Model Accuracy and Parameterization," in *European Conf. on Antennas and Propagation (EuCAP)*. IET, 2007, pp. 1–8.

[26] S. Y. Seidel and T. S. Rappaport, "A ray tracing technique to predict path loss and delay spread inside buildings," in *IEEE Global Telecommunications Conf (GLOBECOM)*, pp. 649–653.

[27] T. C. Becker, D. J. Cichon, and W. Wiesbeck, "Computation-time efficient determination of 3D propagation paths in rural area," *IEEE Antennas and Propagation Society Int. Symp. (APSURSI)*, vol. 1, pp. 502–505, 1995.

[28] M. A. Forman and D. Young, "The generation of shared cryptographic keys through half duplex channel impulse response estimation at 60 GHz," in *Int. Conf. on Electromagnetics in Advanced Applications (ICEAA)*. IEEE, 2010, pp. 627–630.

[29] W. Shen, P. Ning, X. He, and H. Dai, "Ally Friendly Jamming: How to Jam Your Enemy and Maintain Your Own Wireless Connectivity at the Same Time," in *IEEE Symp. on Security and Privacy (S&P)*.

[30] N. Anand, S.-J. Lee, and E. W. Knightly, "STROBE: Actively securing wireless communications using Zero-Forcing Beamforming," in *IEEE Conf. on Computer Communications (INFOCOM)*, 2012, pp. 720–728.

[31] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna Subset Modulation for Secure Millimeter-Wave Wireless Communication," *IEEE Transactions on Communications (TCOM)*, vol. 61, no. 8, pp. 3231–3245, 2013.

[32] M. Schulz, A. Loch, and M. Hollick, "Practical Known-Plaintext Attacks against Physical Layer Security in Wireless MIMO Systems," in *Proc. of Network and Distributed System Security Symposium (NDSS)*, 2014.