INL/CON-17-43878-Revision-0

On Success Probability of Eavesdropping Attack in 802.11ad mmWave WLAN

Arup Bhuyan, Sarankumar Balakrishnan, Zhi Sun, Pu Wang

May 2018

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/CON-17-43878-Revision-0

On Success Probability of Eavesdropping Attack in 802.11ad mmWave WLAN

Arup Bhuyan, Sarankumar Balakrishnan, Zhi Sun, Pu Wang

May 2018

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract C.D.00.01.GL.05.14

On Success Probability of Eavesdropping Attack in 802.11ad mmWave WLAN

Sarankumar Balakrishnan*, Pu Wang†, Arup Bhuyan‡ and Zhi Sun*

*Department of Electrical Engineering, University at Buffalo, Buffalo, NY 14260 USA
†Dept. of Computer Science, University of North Carolina at Charlotte, Charlotte, NC, 28223 USA
‡Idaho National Laboratory (INL), Idaho Falls, ID, 83402 USA
E-mail: {sarankum, zhisun}@buffalo.edu*, Pu.Wang@uncc.edu†, arupjyoti.bhuyan@inl.gov‡

***Abstract*—Next generation wireless communication networks utilizing 60 GHz millimeter wave (mmWave) frequency bands are expected to achieve multi-gigabit throughput with the use of highly directional phased-array antennas. These directional signal beams provide enhanced security to the legitimate networks due to the increased difficulties of eavesdropping. However, there still exists significant possibility of eavesdropping since (i) the reflections of the signal beam from ambient reflectors enables opportunistic stationary eavesdropping attacks; and (ii) carefully designed beam exploration strategy enables active nomadic eavesdropping attack. This paper discusses eavesdropper attack strategies for 802.11ad mmWave systems and provides the first analytical model to characterize the success possibility of eavesdropping in both opportunistic stationary attacks and active nomadic attacks.**

I. Introduction

Millimeter wave communication is considered to be one of the key enabling technology of next generation very high throughput wireless networks. Millimeter wave frequency bands have different propagation characteristics than those at lower microwave frequencies. At mmWave frequencies, the signal experiences high attenuation due to propagation and penetration losses [1]. When compared to microwave frequencies at sub 6GHz band, 60 GHz mmWave frequency bands experiences additional 20 dB signal attenuation due to signal propagation characteristics at 60 GHz. The IEEE 802.11ad standard [2] addresses these challenges by using high gain directional antennas to overcome the signal attenuation at 60 GHz. IEEE 802.11ad leverages the wide bandwidth available at 60GHz frequency band and data-rates of around 7 Gbps are envisioned with the use of beamforming with phased-array antennas to steer around the obstacles.

With the expected proliferation of 802.11ad based mmWave WLAN for high throughput indoor connectivity, security of these wireless networks becomes a critical issue. Contrary to the omni-directional signal transmission in legacy 802.11 based wireless networks operating at 2.4 and 5 GHz microwave band, 60 GHz 802.11ad mmWave networks are characterized by highly directional transmission enabled by beamforming [1]. 802.11ad standard specifies a minimum beamwidth of 3 degrees. Conventionally, it is believed that the very narrow beamwidth offers inherent PHY security against eavesdroppers. However, such optimistic conclusion is based on the assumption that eavesdroppers only rely on line of sight (LOS) link to the legitimate devices and do not have any information of the direction of the beam used by the legitimate devices.

In practice, there still exists significant possibility of eavesdropping in 802.11ad mmWave systems. On the one hand, many millimeter wave indoor experimental measurements have shown that first order reflections from structures in an indoor environment contributes to majority of signal power in NLOS [3]. Thus, in 60 GHz mmWave communication, along with LOS, first order reflections from ambient reflectors play a crucial role in the signal coverage of such systems. As a result, even not in the LOS region of the narrow mmWave beam, it is still possible for eavesdropper to overhear the transmission due to the multiple reflection paths. On the other hand, to establish the highly directional mmWave link, the legitimate transmitter and receiver need to scan all the possible direction sectors to search the optimal beam between themselves [2]. Due to the broadcasting nature of the beam searching procedure, eavesdropper can estimate the LOS region of the beam selected by the legitimate users. Once the eavesdropper moves to the LOS region, the possibility of successful eavesdropping will dramatically increase.

To date, the understanding of the eavesdropping attack in 802.11ad mmWave WLAN system is still limited to experimental results. In [4], a multi-antenna eavesdropping attack strategy is proposed. The ability of the eavesdropper to reliably detect the intentional jamming from the legitimate transmitter is experimentally demonstrated. In [5], an attack on the antenna subset modulation (ASM) technique is developed based on compressive sensing technique. In [6], the impact of reflections on the physical layer security of mmWave systems are experimentally demonstrated. It shows that the eavesdropper can successfully eavesdrop even highly directional signal beams when small-scale reflectors are placed along the direction of the main beam. However, to our best knowledge, no existing work has provided an analytical model to characterize various eavesdropping attacks in 802.11ad mmWave WLANs.

In this paper, we analyze the success possibility of two types of eavesdropping attacks, including the opportunistic stationary attack and the active nomadic attack. In the opportunistic stationary attack, the eavesdropper can only stay in the random position of the indoor environment. We consider when the LOS path is available and when only NLOS path is available due to reflectors. Stochastic geometry based coverage analysis

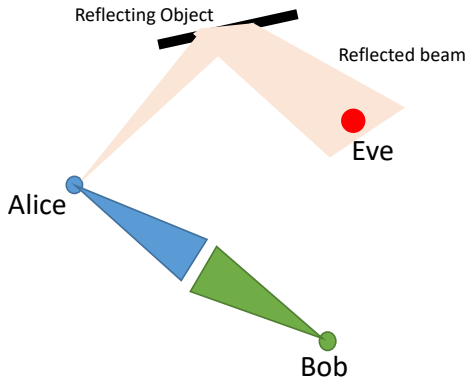

Fig. 1: System model showing Alice, Bob and Eve with reflected signal

is developed for the eavesdropper in the presence of LOS and reflected signal paths. In the active nomadic attack, the eavesdropper can move to any location in the environment to launch the attack. We first develop the LOS region estimation method based on the 802.11ad beam search procedure so that the eavesdropper knows where to move. Then the successful possibility of the active nomadic attack is derived. Finally, we support our analytical model with ray-tracing based numerical simulations of an 802.11ad network in an indoor living room environment.

The remainder of this paper is structured as follows. In section II we introduce the system model and in section III we present two eavesdropper attack strategies for 802.11ad WLAN systems and discuss the probability of successful overhearing of transmission under those strategies. In section IV we discuss simulation results and section V offers conclusion.

II. PHY Layer Security: System Model

We consider a 802.11ad based indoor wireless network with LOS signal path and NLOS signal path facilitated by signal reflections of the macro and micro structures within the indoor environment. Fig 1 shows the system model with Alice and Bob communicating through direct beam and Eve overhearing Alice's transmission through reflected beam. Each node in the network is equipped with an antenna array that can form discrete set of beams. The beams are defined by azimuth angle θ and beamwidth μ. We adopt a sectored antenna model in which the number of sectors employed depends on the beamwidth. In our model we assume the sector width is equal to the beamwidth of the main lobe. The antenna gain is a function of the beamwidth μ.

A. Antenna Gain

As mentioned in our 802.11ad system model, we assume all the nodes are equipped with phased-array antenna for directional beamforming. We use sector antenna model in our analysis [7]. The antenna array gain G is given by

$$G = \begin{cases} g_m^2, & \text{with probability}(\frac{\mu}{2\pi})(\frac{\mu}{2\pi}) \\ g_m g_s, & \text{with probability}(\frac{\mu}{2\pi})(1-\frac{\mu}{2\pi}) \\ g_s g_m, & \text{with probability}(1-\frac{\mu}{2\pi})(\frac{\mu}{2\pi}) \\ g_s^2, & \text{with probability}(1-\frac{\mu}{2\pi})(1-\frac{\mu}{2\pi}) \end{cases} \quad (1)$$

where g_m and g_s are main lobe and side lobe gains respectively. μ is the half-power beamwidth in radians. When the beam pattern of the nodes are aligned maximum directivity gain of $g_m g_m$ is obtained.

The antenna gain pattern in our system model is based on the model specified in [8]. The gain pattern $G(\theta)$ is given by

$$G(\theta) = \begin{cases} g_m = G_0 - 3.01 * (\frac{2\theta}{\mu})^2 & \text{if } 0 \le \theta \le \frac{\theta_{ml}}{2} \\ g_s = -0.411 * \ln(\mu) - 10.6 & \text{if } \frac{\theta_{ml}}{2} < \theta \le \pi \end{cases} \quad (2)$$

where $G_0 = 20 * \log(\frac{1.62}{\sin(\frac{\mu}{2})})$, main lobe angular width $\theta_{ml} = 2.58 * \mu$, and θ is the main lobe direction.

B. Channel Model

We consider a noise-limited 60 GHz mmWave WLAN system and the signal-to-noise ratio (SNR) at a typical receiver is given by

$$SNR = \frac{P_t G_{tx} G_{rx}}{(\frac{4\pi d}{\lambda})^\alpha \sigma^2} \quad (3)$$

where P_t is the transmit power, G_{tx} is the antenna gain of transmitter, G_{rx} is the antenna gain of receiver, d is the distance between the transmitter and the receiver, λ is the wavelength of the signal, α is the path loss exponent and σ^2 is the noise variance.

C. mmWave nodes

The spatial locations of the transmitters, receivers and the eavesdropper are modeled as homogeneous Poisson Point Process (PPP), $\Phi \subset \mathbb{R}^2$, with intensity λ_n in $\mathbb{R}^2$ [9], [10]. The typical transmitter (Alice) is assumed to be located at the origin. Standard path loss model $l(d) = ||d||^{-\alpha}$, where α is path loss exponent, is assumed between any pair of communicating nodes. The locations of the nodes are specified by polar coordinates (d, θ) where θ is measured from the positive x-axis.

D. Obstacles and reflectors

The indoor environment is randomly populated with obstacles and reflectors modeled as homogeneous PPP in $\mathbb{R}^3$. Obstacles are those objects that have zero reflection coefficient, i.e they do not reflect signals whereas reflectors reflect signals and have reflection coefficient ρ. We assume that the signals are completely reflected by the reflector. In our analysis, we ignore signal penetration and diffraction. The centers of obstacles and reflectors X_i form a homogeneous PPP Φ_0 with density λ_0. Both the obstacles and reflectors are assumed to have random length, width and height. The length $L_i \in \{l_{min}, l_{max}\}$, width $W_i \in \{w_{min}, w_{max}\}$ and height $H_i \in \{h_{min}, h_{max}\}$ of the obstacles and reflectors are assumed to be i.i.d distributed with

probability density functions (PDF) defined by $f_L(l)$, $f_W(w)$ and $f_H(h)$ respectively. The orientation of the obstacles and reflectors Θ_i are uniformly distributed between $[0, 2\pi)$. Thus the objects (obstacles and reflectors) are defined by quintuple $\{X_i, L_i, W_i, H_i, \Theta_i\}$.

E. Distribution of distance to first obstacle

From [9], we know that the total number of blockages N between a transmitter and receiver is a Poisson random variable with mean $\beta r_0 + p$ where $\beta = \frac{2\lambda_0(E[W]+E[L])}{\pi}$ and $p = \lambda_0 E[L]E[W]$, i.e $\mathbb{E}(N) = \beta r_0 + p$. Here r_0 is the distance between the transmitter and the first obstacle. Therefore the CDF of r_0, $F_{R_0}(r_0)$ is given by

$$\begin{aligned} F_{R_0}(r_0) &= P(R_0 \leq r_0) \\ &= 1 - P(R_0 \geq r_0) \\ &= 1 - e^{-(\beta r_0 + p)}. \end{aligned} \tag{4}$$

Let $f_{R_0}(r_0)$ be the pdf of the distance r_0. For distance $r_0 > 0$, the pdf $f_{R_0}(r_0)$ can be obtained by differentiating (4) with respect to r_0 as

$$f_{R_0}(r_0) = \beta e^{-(\beta r_0 + p)}. \tag{5}$$

III. PHY Layer Security: Eavesdropper Attacker Model

In this section, we discuss PHY layer attacker strategies for Eve to overhear Alice's transmission. We discuss two eavesdropping attacker model for Eve: 1) opportunistic stationary attack and 2) active nomadic attack. Accordingly, we discuss the probability of Eve successfully overhearing Alice's transmission under opportunistic stationary attack strategy and active nomadic attack strategy. For our analysis, we follow the geometry based blockage model specified in [11], [12]. SNR_{Eve} denotes the signal-to-noise ratio obtained at the eavesdropper due to LOS or reflected signal. T denotes the SNR threshold at which Eve can successfully overhear the signal from the transmitter Alice. Therefore, the coverage probability of the eavesdropper Eve is defined by $P(SNR_{Eve} \geq T)$. Due to the random distributions of the objects in the indoor environment under consideration, the eavesdropper could be covered by either direct LOS signal from the transmitter or through the reflections from the reflecting objects in the indoor environment. Accordingly P_{LOS} and P_{ref} define the coverage probability of Eve due to LOS and reflected signals respectively.

A. Opportunistic Stationary Attacker

In this attacker strategy, depending on Eve's random location, Eve could overhear Alice's transmission either through LOS signal or through reflections from the reflectors. In this mode of attack, Eve doesn't move its position. She stays in her random location and her success of overhearing Alice's transmission heavily depends on the availability of LOS or reflections. Initially Eve uses omni-directional antenna and performs a sector sweep to continuously scan the environment for the best possible DMG-beacon reception from Alice. Eve upon deciding on the best sector from Alice transmission based on RSSI measurements, switches her antenna from omni-directional to directional antenna and steers her antenna to the sector with highest received signal power. The sector Eve chooses to overhear transmission from Alice could be a sector in the direction of LOS or could be towards a strongest reflected signal. Eve periodically performs the beam searching procedure and updates her best sector to overhear transmission from Alice.

We define the event $C_{Eve} : SNR_{Eve} \geq T$ as the event when the received SNR of Eve is above a certain threshold to successfully receive the signal. Accordingly, the probability that Eve will be able to successfully receive the signal is given by

$$P(C_{Eve}) = P(SNR_{Eve} \geq T). \tag{6}$$

We further define two events LOS_{Eve} and Ref_{Eve} as the events when the eavesdropper is covered by a LOS signal from the legitimate transmitter Alice and by reflections from the reflectors present in the environment respectively. Since the contributions of second-order and higher-order reflections to the total received signal power are negligible in mmWave systems, in our system model we only consider first-order reflections. We further make assumptions that the reflected signal is fully reflected by the obstacle with reflection co-efficient ρ. We also ignore refraction and diffraction of signals in our system model. By taking in to account the possibility of Eve being covered by either LOS from Alice or by reflections from the environment, the coverage probability of Eve is given by

$$\begin{aligned} P(C_{Eve}) = P(SNR_{Eve} \geq T | LOS_{Eve}) P(LOS_{Eve}) + \\ P(SNR_{Eve} \geq T | Ref_{Eve}) P(Ref_{Eve}). \end{aligned} \tag{7}$$

Here the first term is the coverage probability when Eve is covered by LOS from Alice and the second term is the probability of Eve being covered by a reflected signal.

It has been shown in [9], the total number of obstacles N between two nodes separated by distance r_0 is a Poisson random variable with mean $\beta r_0 + p$, where $\beta = \frac{2\lambda_0(E[W]+E[L])}{\pi}$ and $p = \lambda_0 E[L]E[W]$. The probability that there exist a LOS link between Alice and Eve with distance r_0, i.e there are no obstacles between them is

$$P(LOS_{Eve}) = P(N = 0) = e^{-(\beta r_0 + p)}. \tag{8}$$

Note that (8) does not take height of the object X_i in to account. In our model the object height $H_i \in [h_{min}, h_{max}]$ are modeled with pdf $f_H(h)$. Let H_{tx} and H_{Rx} denote the height at which the transmitter and receiver antennas are located. The height H_i of the obstacle is independent of X_i, L_i, W_i, θ_i. The effective number of obstacles $\hat{N}$ that block the direct LOS between the nodes separated by distance r_0 can be determined by using Thinning theorem [13]. The effective number of obstacles $\hat{N}$ is a Poisson random variable with $\mathbb{E}[\hat{N}] = \eta \mathbb{E}[N]$ where $\mathbb{E}[N] = \frac{2\lambda(\mathbb{E}[L]+\mathbb{E}[W])}{\pi} r_0$ and

$$\eta = 1 - \int_0^1 \int_{h_{min}}^{sH_{rx}+(1-s)H_{tx}} f_H(h) dh ds. \tag{9}$$

Therefore the probability Eve will be in LOS with respect to

Alice is given by

$$P(LOS_{Eve}) = e^{-\eta(\beta r_0 + p)}. \quad (10)$$

The conditional probability $P(SNR_{Eve} \geq T | LOS_{Eve})$ will be 1 as long as Eve's direction θ_{Eve} is within the beamwidth μ of Alice direction (i.e Eve is in the sector of Alice's transmission) and the distance of Eve from Alice, denoted as r_0 is within the threshold distance d_0 which satisfies the SNR threshold T requirements of Eve. Therefore under the event that Eve is in the direction of Alice's transmission and within the SNR threshold distance, the probability Eve will be successfully able to overhear Alice's signal under LOS condition is

$$P_{LOS} = e^{-\eta(\beta r_0 + p)}. \quad (11)$$

It is well known that in an indoor environment such as living room with windows, television, and other commonly present objects made of metals and glass surfaces reflect mmWave well. The reflected signal strength depends on the shape, size and material properties of the reflector. The work in [6] presents experimental results for reflection of mmWave signals by objects present in the living room scenario. Such reflections from the ambient reflector in the environment could potentially enable the eavesdropper to overhear Alice's transmission even when LOS from Alice is not available to Eve. The probability of Eve overhearing transmissions from Alice from a reflected path is given by

$$P(SNR_{Eve} \geq T | Ref_{Eve}) P(Ref_{Eve}). \quad (12)$$

The event Eve being covered by a reflected beam depends on the distance of the first reflector from Alice d_r and the orientation of the reflector ϕ. The distribution of the distance of the first reflector from Alice is shown in section II-E. The probability density function of the orientation of the reflector $f_\Phi(\phi)$ is assumed to be uniformly distributed between $[0, \pi]$. Let Eve is at a distance of d_{Eve} from the reflector. For a signal reflected by a reflector with reflection coefficient ρ, the received SNR at Eve is given by

$$SNR_{Eve} = \frac{P_t G_{tx} G_{rx}}{(\frac{4\pi d_{Eve}}{\lambda})^\alpha \rho \sigma^2}. \quad (13)$$

As long as Eve is inside the beamwidth of the reflected signal and the distance of Eve from the reflector d_{Eve} is within the threshold distance $d_0 = (\frac{p_t G_{tx} G_{rx}}{(\frac{4\pi}{\lambda})^\alpha \rho \sigma^2 T})^{1/\alpha}$ where T is SNR threshold, $P(SNR_{Eve} \geq T | Ref_{Eve})$ is 1. Here G_{tx} is the transmitter gain from Alice, G_{rx} is the gain of Eve's antenna. Now conditioned on the distance d_r of the first reflector from Alice and the orientation of the reflector ϕ, it can be readily shown that the probability of Eve being covered by a reflected signal is

$$P_{ref} = \int_0^\pi \int_0^\infty e^{-\eta\beta d_{Eve}} \eta\beta e^{-\eta(\beta r + p)} \frac{1}{\pi} dr d\alpha \quad (14)$$

where η is given by (9).

B. Active Nomadic Attacker

Before proceeding to describe the active nomadic attack by the eavesdropper, we briefly discuss the 802.11ad beamforming training protocol. IEEE 802.11ad enables the access to the medium in Beacon Intervals (BIs). A BI consists of Beacon Header Interval (BHI) and Data Transmission Interval (DTI). The BHI consist of the following three sub-intervals: Beacon Transmission Interval (BTI), Association Beamforming Training (A-BFT) and Announcement Transmission Interval (ATI).

Since 802.11ad devices use directional antenna for communication, to determine the appropriate transmit and receive direction which are referred to as sectors, 802.11ad protocol introduces beamforming training between pair of nodes. The beamforming training process in IEEE 802.11ad is explained as follows: During the BTI interval, one of the node acts as a transmitter and sends directional multi-gigabit (DMG) beacons over different antenna sectors and the other node listens to these beacons with an omni-directional antenna. The receiving node chooses the sector with highest received power as the sector for transmission from transmitter node to receiver node. During the A-BFT period, the nodes interchange their role as transmitter and receiver and performs a similar beamforming training process to find the best sector in the reverse direction. In this way, a pair of node finds the best sector for transmission and reception.

To perform an active LOS attack, Eve must know the sectors and also the ground truth direction of these sectors used by Alice and Bob for communication. We assume that Eve has the capability to employ mmWave localization algorithm to localize the positions of nodes. Eve, from a random position, listens to the beamforming training beacons from Bob during the A-BFT period and determines the sector direction of Bob from Eve. The beacons during the A-BFT period from Bob also has feedback information about the best sector to use from Alice to Bob found during the beamforming training process between Alice and Bob in the BTI period. Eve by virtue of listening to these beacons from Bob has the knowledge of sector used for Alice to Bob direction and also the direction of Bob from Eve. Eve equipped with the sector direction, performs location (distance) estimate of Bob and moves to the location of Bob. Eve then steers its antenna to the sector used by Alice to communicate with Bob and overhears the communication.

In order to analyze the success probability of Eve overhearing the transmission from Alice under the active nomadic attack model, we consider a marked, homogeneous Poisson Point Process (H-PPP) with intensity λ_m. H-PPP, $\Phi = \{l, m\}$ models the location of the transmitter and receiver pair and their associated marks. l represents the location of the transmitter. The marks $m = (\theta, \epsilon)$ are i.i.d, where θ denotes the beam direction of Eve towards Alice and ϵ denotes the beam direction error. The marks represent Eve's location through θ and distance R_0. R_0 is the distance between Alice and Eve after Eve moves to Bob's location. The gain pattern $G(\theta)$ which is a function of beam direction θ is assumed to be symmetric about the

boresight of the antenna. Therefore under symmetric gain pattern assumption, it is sufficient to consider absolute beam direction error $|\epsilon|$ and $G(\theta) = G(\epsilon)$. We model the beam direction error ϵ as a random variable with distribution $f_{|\epsilon|}$ and hence the antenna gain of Eve towards Alice is also a random variable with distribution $f_{G_r}(g)$. Under perfect localization of Bob, the beam direction of Eve would be aligned towards Alice. However, the error in estimating the location of Bob introduces error in the direction of Eve's beam towards Alice. In our model, we assume the beam direction θ to be uniformly distributed in $[-\pi, \pi]$ and the distribution of error in beam direction $f_{|\epsilon|}$ of Eve towards Alice is assumed to be half-normal distribution and the distribution of gain of Eve is $f_{G_r}(g) = F_{|\epsilon|}(\mu/2)\delta(g - g_m) + (1 - F_{|\epsilon|}(\mu/2))\delta(g - g_s)$ [14]. Here $g1$ and $g2$ are main lobe and side lobe gains.

1) Success Probability: Here, we discuss the success probability of Eve overhearing Alice's transmission under the active nomadic attack model. As discussed before, Eve estimates the location of Bob through localization procedure and moves to Bob's location. We analyze the success probability of Eve conditioned on the beam direction error $|\epsilon|$ arising due to the uncertainty in the location estimate of Bob. The success probability of Eve is given as

$$\begin{aligned} P_{success} &= P\{SNR_{Eve} \geq T\} \\ &= P\left\{ \frac{P_t G_t G_r(\epsilon)}{(\frac{4\pi R_0}{\lambda})^\alpha \sigma^2} \geq T \right\} \\ &= P\left\{ R_0 \leq \left(\frac{P_t G_t G_r(\epsilon)}{T(\frac{4\pi}{\lambda})^\alpha \sigma^2} \right)^{1/\alpha} \right\}. \end{aligned} \tag{15}$$

In order to evaluate the success probability $P_{success}$, the distribution of R_0 must be known. The distribution of the distance to the closest visible transmitter R_0 is derived in [9] and is given as

$$f_{R_0}(x) = 2\pi\lambda x e^{-(\beta x + p + 2\pi\lambda \frac{e^{-p}}{\beta^2}[1-(\beta x+1)e^{-\beta x}])} \tag{16}$$

The CDF of R_0 is

$$F_{R_0}(x) = 1 - e^{-2\pi\lambda \frac{e^{-p}}{\beta^2}[1-(\beta x+1)e^{-\beta x}]} \tag{17}$$

Therefore, under the active nomadic attack model with distance of Eve from Alice R_0, SNR threshold T, Eve's beam direction error distribution f_ϵ due to localization error, the success probability of Eve overhearing Alice's transmission is given as

$$P_{success} = \int_0^\infty F_{R_0}(x) f_{G_r}(g_r) dg_r \tag{18}$$

where $x = \left(\frac{P_t G_t G_r(\epsilon)}{T(\frac{4\pi}{\lambda})^\alpha \sigma^2} \right)^{1/\alpha}$.

IV. Simulation Results

In this section we evaluate different Eavesdropper attack strategy based on the analytical model discussed in Section III. We used Matlab to perform simulation studies of the Eavesdropper attacker models presented in Section III. We consider a simulation area of $10m \times 10m$ depicting an indoor living room. Our system model consists of Alice and Bob which are legitimate node pairs communicating and an eavesdropper Eve. Alice and Bob uses 802.11ad based mmWave narrow beam communications for communicating with each other. Eve tries to overhear transmissions from Alice using LOS if available or through reflections from environmental reflectors. It is assumed that Alice and Bob completes beam searching procedure as per 802.11ad protocol and their beams are perfectly aligned. We also assume that Eve has the same capability as that of Alice and Bob and uses 802.11ad protocol. Locations of Alice, Bob and Eve are randomly chosen following a 2D homogeneous PPP model. The obstacles and reflectors are randomly dropped following the PPP model discussed in section II. The dimensions of the obstacles and reflectors are chosen to depict furnitures, fixtures and objects found in a common indoor living room scenario. A list of common parameters used for the simulations are shown in Table 1. The reflection loss ρ due to reflectors present in the environment was set at 7 dB unless otherwise specified. The antenna gain pattern of Alice, Bob and Eve are as shown in Section II-A. We perform numerical simulations for opportunistic stationary attack strategy and active nomadic attack strategy.

TABLE I: Common parameters used in the simulation.

Parameters	Indoor
Carrier Frequency (GHz)	60
Bandwidth (MHz)	2310
Path Loss α	2
Object Density λ_0	$0.08/m^2$
Uniform obst. height H (m)	[0,1]
Uniform obst. width W (m)	[0,1]
Uniform obst. length L (m)	[0,1]
Transmit Power P_t (dBm)	20
Height of Tx antenna (m)	1.5
Height of Rx antenna (m)	1

A. Opportunistic Stationary Attacker

In this simulation, the location of Alice is fixed at the origin and the location of Bob and Eve are randomly chosen based on the PPP model. The orientation of the beam of Alice is towards the direction of Bob.

Fig. 2 shows the coverage probability of Eve for varying distance from Alice. Fig. 2 shows coverage probability of Eve for the following scenarios: 1) Eve is in LOS with respect to Alice, 2) Eve is covered by either a LOS signal or by reflected signal and 3) Eve is only covered by a reflected signal. Fig. 2 also shows coverage probability of Eve for different obstacle dimensions denoted as Dim A and Dim B. The length L, width W and height H of obstacle dimensions denoted by A are drawn uniformly from $[0, 1]$ and dimensions denoted by B are drawn uniformly from $[0, 2]$. The reflection loss for reflectors are fixed at 7 dB. From the Fig.2, we see that the coverage probability due to LOS signal decreases rapidly with

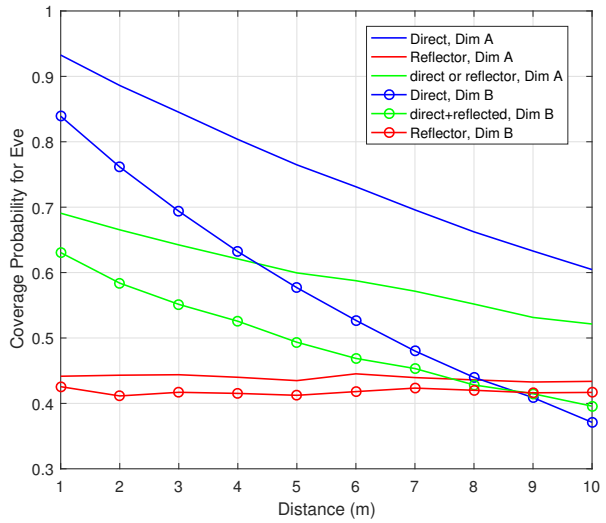

Fig. 2: Coverage probability for Eve for different obstacle dimension sets A and B.

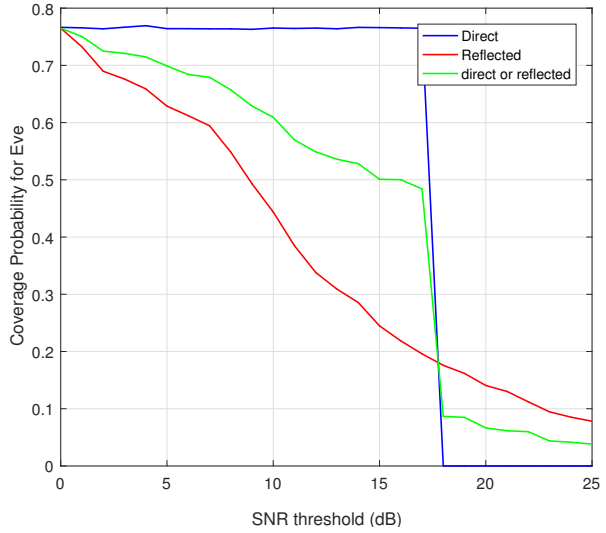

Fig. 3: Coverage probability for Eve for different SNR threshold T.

distance. As the obstacle size increases, the coverage probability of Eve decreases significantly. The coverage probability due to reflected beam remains almost constant with respect to distance of Eve from Alice. When the obstacle size increases (here set B) and at longer distance of Eve from Alice, the reflected signal coverage probability is higher than the LOS coverage probability. This is due to, with increasing distance and increasing obstacle size the probability of LOS signal decreases and Eve is more likely to be covered by the reflected signal.

Fig. 3 shows the coverage probability of Eve with respect to varying SNR threshold level. Here we fix the distance of

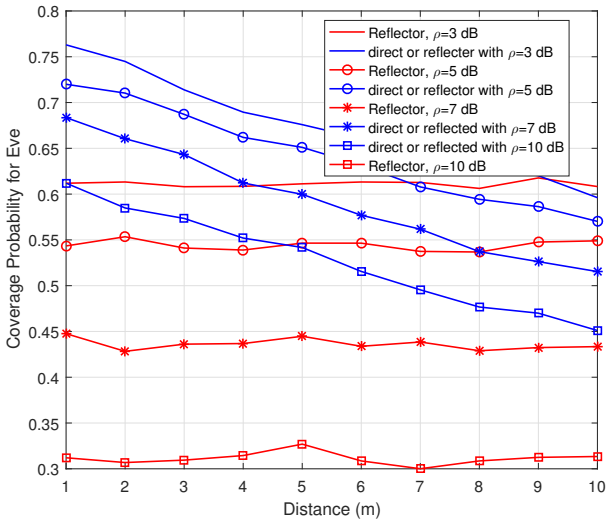

Fig. 4: Coverage probability for Eve for different reflection loss ρ.

Eve from Alice at $5m$. It can be seen, for a fixed distance of Eve from Alice, as long as the SNR threshold is satisfied the coverage probability due to LOS signal is almost constant, but the coverage probability due to reflected signal decreases rapidly. When the received LOS signal is below the SNR threshold, the coverage probability due to LOS drops to zero. At higher SNR thresholds, the contributions of reflections becomes more evident.

In Fig. 4, we show the coverage probability of Eve for two cases: 1) when Eve is covered by either a direct beam or a reflected beam. 2) when Eve is covered only by a reflected beam. We show the coverage probability for different reflection losses ρ depicting the scenario of different reflection materials found in the indoor environment. From the Fig.4, we see that Eve has significant coverage probability with reflector with ρ of 3 dB and 5 dB. For a reflection loss of 10 dB, the coverage probability of Eve significantly reduces. It shows that commonly found objects in the indoor environment with low reflection loss can significantly aid in eavesdropping even in the absence of LOS to Alice.

B. Active Nomadic Attacker

To evaluate the success probability of Eve overhearing Alice transmission to Bob under active nomadic attack, the distance between Alice and Eve is fixed at $5m$ and all the other parameters are fixed as shown in Table I. Simulations were carried out for various beamwidths of $\mu = 20°, 30°$ and $60°$. The beam orientation error $|\epsilon|$ for Eve is uniform on $[0, \frac{\mu}{2}]$. Success probability for each SNR threshold is an average of 10,000 simulation runs. From Fig. 5 we see that, the probability of success for Eve to overhear Alice transmission decreases as the beamwidth used by Alice and Eve increases. This is due to the fact that the antenna gain decreases with increasing beamwidth of the antenna. Fig. 5 also shows the comparison

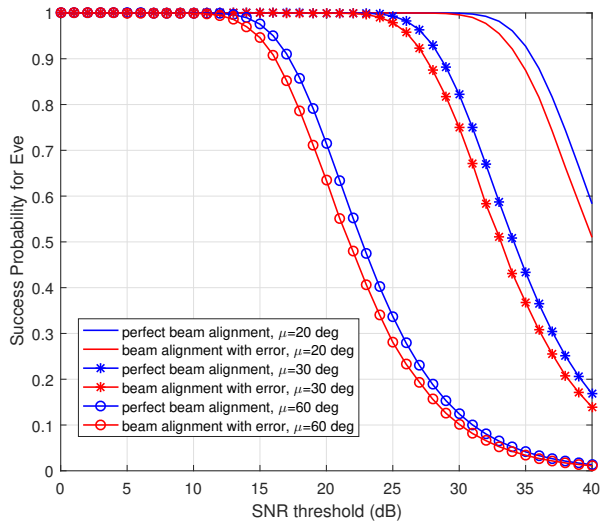

Fig. 5: Success probability for Eve under active nomadic attack.

between perfect beam orientation between Eve and Alice (i.e. no beam orientation error due to localization uncertainty) and beam orientation error due to location uncertainty for each of the beamwidths considered. It is seen that, since in our simulation studies we set beam orientation error due to location uncertainty to be within the main lobe beamwidth ($|\epsilon| \in [0, \frac{\mu}{2}]$), we see marginal degradation in the success probability of Eve. Fig. 5 shows that with the knowledge of the active transmission sector of Alice and by using narrow beamwidth antenna with high gain, Eve has higher probability of success in overhearing Alice's transmission under active nomadic attack.

V. Conclusions

It is often assumed in mmWave communication systems that because of its quasi-optical propagation characteristics, it is practically infeasible for an eavesdropper to overhear the transmission from outside the direction of the main beam. However, the presence of reflectors in the environment can significantly aid in eavesdropping through the reflected signal. Moreover, active nomadic attack based on the knowledge of 802.11ad protocol can further increase the successful eavesdropping possibility. In this work, we presented eavesdropping attack strategy for 802.11ad mmWave WLAN systems and evaluated the probability of successful overhearing of the transmission from Alice. From our simulation studies, we show that the success probability of eavesdropping can be significant due to the presence of reflectors in the environment and the active eavesdropping attack.

References

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

[2] E. Perahia, C. Cordeiro, M. Park, and L. L. Yang, "Ieee 802.11 ad: Defining the next generation multi-gbps wi-fi," in *Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE*. IEEE, 2010, pp. 1–5.

[3] F. Fuschini, S. Häfner, M. Zoli, R. Müller, E. Vitucci, D. Dupleich, M. Barbiroli, J. Luo, E. Schulz, V. Degli-Esposti *et al.*, "Analysis of in-room mm-wave propagation: Directional channel measurements and ray tracing simulations," *Journal of Infrared, Millimeter, and Terahertz Waves*, vol. 38, no. 6, pp. 727–744, 2017.

[4] D. Steinmetzer, M. Schulz, and M. Hollick, "Lockpicking physical layer key exchange: Weak adversary models invite the thief," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2015, p. 1.

[5] C. Rusu, N. González-Prelcic, and R. W. Heath, "An attack on antenna subset modulation for millimeter wave communication," in *Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference on*. IEEE, 2015, pp. 2914–2918.

[6] D. Steinmetzer, J. Chen, J. Classen, E. Knightly, and M. Hollick, "Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves," in *Communications and Network Security (CNS), 2015 IEEE Conference on*. IEEE, 2015, pp. 335–343.

[7] T. Bai and R. W. Heath, "Coverage and rate analysis for millimeter-wave cellular networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 1100–1114, 2015.

[8] I. Toyoda and T. Seki, "Antenna model and its application to system design in the millimeter-wave wireless personal area networks standard," *NTT Tech. Rev*, vol. 9, pp. 1–5, 2011.

[9] T. Bai, R. Vaze, and R. W. Heath, "Analysis of blockage effects on urban cellular networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 5070–5083, 2014.

[10] ——, "Using random shape theory to model blockage in random cellular networks," in *Signal Processing and Communications (SPCOM), 2012 International Conference on*. IEEE, 2012, pp. 1–5.

[11] N. A. Muhammad, P. Wang, Y. Li, and B. Vucetic, "Analytical model for outdoor millimeter wave channels using geometry-based stochastic approach," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 912–926, 2017.

[12] C. Tatino, I. Malanchini, D. Aziz, and D. Yuan, "Beam based stochastic model of the coverage probability in 5g millimeter wave systems," *arXiv preprint arXiv:1704.07079*, 2017.

[13] B. François and B. Bartłomiej, "Stochastic geometry and wireless networks. volume i. theory," *NoW PublishersBreda*, 2009.

[14] J. Wildman, P. H. J. Nardelli, M. Latva-aho, and S. Weber, "On the joint impact of beamwidth and orientation error on throughput in directional wireless poisson networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 12, pp. 7072–7085, 2014.