PASID: Exploiting Indoor mmWave Deployments for Passive Intrusion Detection

Francesco Devoti*, Vincenzo Sciancalepore†, Ilario Filippini* and Xavier Costa-Perez†

*DEIB, Politecnico di Milano, Italy

†NEC Laboratories Europe, Heidelberg, Germany

***Abstract*—As 5G deployments start to roll-out, indoor solutions are increasingly pressed towards delivering a similar user experience. Wi-Fi is the predominant technology of choice indoors and major vendors started addressing this need by incorporating the mmWave band to their products. In the near future, mmWave devices are expected to become pervasive, opening up new business opportunities to exploit their unique properties.**

In this paper, we present a novel *PASsive Intrusion Detection* system, namely PASID, leveraging on already deployed indoor mmWave communication systems. PASID is a software module that runs in off-the-shelf mmWave devices. It automatically models indoor environments in a passive manner by exploiting regular beamforming alignment procedures and detects intruders with a high accuracy. We model this problem analytically and show that for dynamic environments machine learning techniques are a cost-efficient solution to avoid false positives. PASID has been implemented in commercial off-the-shelf devices and deployed in an office environment for validation purposes. Our results show its intruder detection effectiveness ($\sim 99\%$ accuracy) and localization potential (~ 2 meters range) together with its negligible energy increase cost ($\sim 2\%$).

I. Introduction

5G is finally here. Mobile operators around the world are racing toward rolling out commercial 5G services in their networks, and as the 5G momentum continues to build, more commercial networks will come online in the next months and years worldwide. With more than 80% of mobile data traffic originating or terminating indoors, service providers aiming at keeping pace with 5G are increasingly considering the mmWave technology for indoor locations as the solution to bring current WiFi products to the next level. mmWave can elevate user experiences to new heights by bringing multi-Gigabit/s speeds, ultra-low latency experiences, and virtually unlimited capacity to a wide range of devices such as smartphones, tablets, AR/VR (augmented/virtual reality) headsets, and always-connected laptops. Moreover, since most offices have Wi-Fi connectivity for computers and other enterprise devices, mmWave networks can realize the vision of the "mobile office of the future", bringing enhanced performance, convenience, security, and user experiences not possible with today's connectivity solutions.

On the standardization side, the IEEE 802.11ad working group, also known as WiGig, already defined a solution delivering high-speed communication capabilities for devices operating in the mmWave frequency bands. Based on this standard, commercial off-the-shelf products are available today. The future IEEE 802.11ay [1] standard, currently under development, is being designed to provide up to 30Gbit/s of indoor capacity within 30 meters [2].

The high data rates offered by mmWave systems compared to classical sub-6GHz Wi-Fi ones come at the price of much worse propagation properties. Attenuation is very strong at mmWave frequencies and thus, mmWave devices require a larger number of antenna elements so as to provide high spatial processing gains that compensate for experienced pathloss [3]. These multiple antenna elements enable mmWave transmitters to electronically steer the radiation pattern providing spatial diversity to the communication channel [4]. Moreover, strong multi-path features and high obstacle blockage sensitivity make mmWave communications very sensible to propagation environment changes.

In this paper we present the PASID solution (PASsive Intrusion Detection) which takes advantage of the unique properties of mmWave communication channels to, in addition to enable Gigabit/s data rates, perform *indoor intrusion detection* in a *passive* manner, i.e., without requiring an active connection to the potential intruder. In particular, mmWaves can easily pass through common clothing materials and reflect on human bodies. Such reflected waves result in frequency variations that reveal discrepancies from expected power measurements. Thereby, detecting the potential presence of an unexpected person in an indoor environment. In order to do so, a data analytics engine ([5], [6]) can carefully parse the data and capture mmWave channel variations. *Deep neural networks* can then *automatically learn* the reference channel environment of a given mmWave indoor deployment and, if an unexpected channel variation is detected, recognize whether it is due to the presence of an intruder. Furthermore, the directional nature of the mmWave signal enables a *localization* feature by sounding the channel on different directions and determining the *position* of intruders without requiring an active connection.

The contributions of the work presented here are as follows:

c1. Analytical modeling of mmWave channel variation outliers detection by monitoring and analysis of gathered power measurements.

c2. Distribution similarity process comparing regularly obtained channel monitoring measurements against a reference environment without intruders.

c3. Design of a deep neural network that continuously keeps track of real-time channel measurements and triggers an alert message when an intrusion is detected.

c4. Localization of intruders within a given indoor reference channel environment.

c5. Implementation of PASID as a stand-alone software in off-the-shelf mmWave routers and validation in a real office.

The rest of the paper is organized as follows: Section II introduces the analytical modeling of the problem. Section III describes the PASID model we use to build the outlier detection phase and the distribution similarity process. The deep neural network design is then presented in Section IV followed by an overview of the testbed implementation details in Section V. Experimental results are summarized and discussed in Section VI. Section VII discusses the related work on the topic. Finally, Section VIII provides our concluding remarks.

II. PASID MODEL DESIGN

In order to detect channel anomalies within an indoor reference environment, a mmWave channel monitoring phase is required. In particular, power measurements on an established mmWave link must be regularly collected and analyzed to detect unexpected changes. Following the IEEE 802.11ad protocol guidelines, power measurements are regularly performed during the beam training phase, i.e., when two mmWave devices seek for which beam to activate providing the best channel quality.

Hereafter, we provide the main pillars of the beam training procedure as defined by the IEEE 802.11ad standard showing the impact on the passive channel sensing within indoor environments. This allows to analytically formulate the problem and thus, to provide a mathematical preliminary solution in order to successfully detect intruders.

Notation. We denote matrix and vector in **bold** text. $(\cdot)^T$ and $(\cdot)^H$ stand for vector or matrix transposition and Hermitian transposition, respectively. $||\boldsymbol{x}||^2$ denotes the L2-norm of a vector $\boldsymbol{x}$ while $tr(\boldsymbol{x})$ is the trace of the square matrix $\boldsymbol{x}$.

A. The beam training procedure in IEEE 802.11ad

IEEE 802.11ad (and its evolution 802.11ay) covers many relevant aspects to establish and sustain a communication link between mmWave-enabled devices. To provide the required beamforming capabilities, such devices are equipped with electronically steerable antenna arrays controlled by predefined weights vectors included in a codebook that may automatically activate different transmitting and receiving beam patterns. A specific codebook must be selected for transmitting or receiving operations to activate the communication and establish the connection.

The beam pattern activation is performed by means of a complex *Beam Forming Training* phase. During this phase, the so-called initiator transmits Sector Sweep (SSW) frames whereas the responder collects power measurements. As soon as the initiator has probed all available beam patterns by selecting available weights vectors in the codebook, in turn, the responder can start the sector sweep procedure letting the initiator collecting power measurements. This procedure is activated during the association phase being periodically repeated to properly adjust the beam selection during the communication and prevent connection disruptions due to an unexpected signal drop [7]. The entire procedure allows to instantaneously obtain a snapshot of the environment by exploiting the spatial diversity while at the same time considering the best communication path to establish the connection.

Note that, due to the millimeter waves high frequency, their propagation is strongly influenced by the environment itself, including human bodies, walls and even glass objects, which can seriously hamper the signal propagation [8]. Thus, the presence of an intruder in the environment can change the propagation conditions, although it might not completely obstruct the communication path between a pair of mmWave nodes. Notably, intruders might have a strong influence on the propagation environment that translates into relevant changes in the beam training measurements outcome. Therefore, the power measurements performed by mmWave devices during standard operations can be exploited to build a complete sensing map of the propagation environment and promptly capture unexpected variations. In the next section, we mathematically leverage on those measurements to detect propagation environment changes, and passively sense intrusions in an area.

B. Effects of intrusion on the Beam training Phase

Let us consider a mmWave communication system consisting of multiple mmWave-enabled 802.11ad devices, which can exchange data while periodically performing the beam training phase according to the 802.11ad guidelines. Hereafter, we focus on the effects produced by propagation environment changes onto the received power measured by those devices.

The short wavelength characterizing mmWave propagation translates into a quasi-optical propagation behavior. As a consequence, objects which lie in the propagation environment can provide communication blockages as well as a large number of reflected paths that can sustain the communication, especially in indoor environments. Therefore, mmWave propagation can be assumed to be a multi-path communication and we can describe the communication channel with a geometrical model [9], which takes into account the multi-path profile of the environment as follows:

$$\mathbf{H} = \sum_{l \in \mathcal{L}} \alpha_l \mathbf{a}_{\text{Rx}}(\phi_{\text{Rx},l}) \mathbf{a}_{\text{Tx}}(\phi_{\text{Tx},l})^H, \tag{1}$$

wherein $\mathcal{L}$ is the set of paths constituting the multi-path profile, α_l is the complex gain of the l^{th} path. $\mathbf{a}_{\text{Tx}}$ and $\mathbf{a}_{\text{Rx}}$ are the array steering vectors of the transmitting and receiving device respectively, which account for the physical characteristics of the arrays, while $\phi_{\text{Tx},l}$ and $\phi_{\text{Rx},l}$ are the angle of departure and the angle of arrival of the l^{th} path.

Such devices are provided with a default beam codebook of size P as a set $\mathcal{P} = (\boldsymbol{p_i})$ of weighting vectors. Different weighting vectors identify distinct beam patterns activated by each device. During the beam training phase, each of the weighing vectors in the transmitter and receiver codebooks, namely $\mathcal{P}_{tx}$ and $\mathcal{P}_{rx}$, are sequentially selected and applied to

the steering vector of the devices. We can define the set of available pairs of beams[1] as the following:

$$\mathcal{B} := \{(i,j) | \mathbf{p}_i \in \mathcal{P}_{tx}, \mathbf{p}_j \in \mathcal{P}_{rx}\}. \quad (2)$$

Let us consider the activation of a given couple of transmitting and receiving beams $(i,j) \in B$. Thus, we can describe the overall communication gain provided by (i,j) as follows:

$$g^{ij} = |\mathbf{p}_j^{\mathrm{H}} \mathbf{H} \mathbf{p}_i|^2, \quad (3)$$

wherein $\mathbf{p}_i \in \mathcal{P}_{\mathrm{TX}}$ and $\mathbf{p}_j \in \mathcal{P}_{\mathrm{RX}}$ are respectively the i^{th} and the j^{th} weighting vectors defined in the transmitting and receiving codebooks of the devices.

The received power associated to the beam pair $(i,j) \in \mathcal{B}$ can be derived as a function of the overall communication gain (expressed in dB):

$$\zeta^{ij} = \Omega_{\mathrm{TX}} + G^{ij} + X^{ij}, \quad (4)$$

wherein Ω_{TX} is the transmission power, G^{ij} is the overall communication gain expressed in dB, and X^{ij} is a random variable that takes into account the non-ideality of the communication channel. For the sake of simplifying the system model discussion, we reasonably assume it as normally distributed[2] , i.e., $\mathcal{N}(0, \sigma^{ij})$, where σ^{ij} is the variance calculated as per [10]. As a consequence, given a propagation environment, the power $\boldsymbol{\zeta} = (\zeta^{ij})$ for each beam pair (i,j) has a multivariate normal distribution, i.e., $\boldsymbol{\zeta} \sim \mathcal{N}(\mu, \boldsymbol{\Sigma})$ with mean $\mu \in \mathbb{R}^P$ and covariance matrix $\boldsymbol{\Sigma} \in \mathbb{S}_{++}^P$ being symmetric positive, and exhibits a probability density function as the following

$$p(\boldsymbol{\zeta}, \mu, \boldsymbol{\Sigma}) = \frac{1}{(2\pi)^{P/2} |\boldsymbol{\sigma}|^{1/2}} e^{-\frac{1}{2}(\boldsymbol{\zeta}-\mu)^T \boldsymbol{\Sigma}^{-1} (\boldsymbol{\zeta}-\mu)}, \quad (5)$$

where

$$\boldsymbol{\Sigma} = E[(\boldsymbol{\zeta} - \mu)(\boldsymbol{\zeta} - \mu)^T] = E[\boldsymbol{\zeta}\boldsymbol{\zeta}^T] - \mu\mu^T. \quad (6)$$

It is worth pointing out that the activation of different beam couples provides very different overall communication gains as different weighting vectors $\boldsymbol{p}_i$ are designed to be directional and therefore to emphasize different communication directions. This enables the spatial diversity in the power measurements campaign considering different directions and covering a $360°$-angle from the device perspective.

As mentioned above, devices are periodically performing the beam training phase, wherein beam patterns are sequentially activated to retrieve power measurements so as to select the best beam for sustaining the data transmission. Analytically, per each beam training phase t, we get a sample of the random process ζ^{ij} for each selected beam pair that can be gathered in the matrix $\boldsymbol{\zeta}_t = (\zeta^{ij})$. We consider a set of sequential beam training phases taken in the k^{th} measurement time window $\mathcal{T}_k$ as $\mathcal{S}_k := \{\boldsymbol{\zeta}_t : t \in \mathcal{T}_k\}$.

[1]The activated beam pattern $f(\theta)$ is obtained as a function of the angle θ, $f(\theta) = \boldsymbol{p}_i \boldsymbol{a}(\theta)$. However, to avoid clutter both terms beam and weighting vector are used interchangeably in the rest of the paper.

[2]This is a reasonable assumption in dense multipath scenarios due to the large number of contributions. However, this assumption is relaxed in Section IV where we provide an effective solution for general distributions.

Given the measurement time window $\mathcal{T}_k$ and its size $T_k = |\mathcal{T}_k|$, we can then estimate the expected mean value and variance of the received power distribution per each couple $(i,j) \in \mathcal{B}$ by computing the following two matrices:

$$\mathbf{M}_k = (\hat{\mu}_k^{ij}) = \frac{1}{T_k} \sum_{t \in \mathcal{T}_k} \boldsymbol{\zeta}_t^{(i,j)}, \quad (7)$$

$$\mathbf{D}_k = (\hat{\sigma}_k^{ij}) = \sqrt{\frac{1}{T_k} \sum_{t \in \mathcal{T}_k} (\boldsymbol{\zeta}_t^{(i,j)} - \hat{\mu}_k^{ij})^2}. \quad (8)$$

Note that if the measurement time window is large enough those values well represent the distribution of ζ^{ij} in the standard environmental conditions. i.e. no intrusions are detected.

Let us consider an intrusion event that occurs when a person moves inside the propagation environment. We can draw the following three observations: i) due to the hydrophobic millimeter-wave behavior, the presence of an intruder may completely block some of the paths $l \in \mathcal{L}$ between the transmitter and the receiver, ii) the flat surfaces that characterize most of the fixtures in the environment might act as wave reflectors: the intruder might permanently move them thereby disrupting some existing path while building new communication channels, iii) a moving person acting as an intruder continuously moves around intermittently blocking some of the communication paths. Such changes in the propagation environment translate into a tangible multi-path profile change that reflects the modifications of the received power statistics both in terms of average and variance. In what follows, we develop a mathematical solution to detect such changes.

C. The kernel density value

A density estimate based on a non-parametric kernel estimate function [11], namely a ground truth density is performed in order to accurately detect unexpected data measurements. In this way, measurement values differing from the ground truth density are labelled as outliers. However, when no assumptions are taken about the distribution of the measurements, outlier detection is only feasible by comparing the estimated density of a given measurement value to the average density of its neighbors, namely unsupervised outlier detection method as shown by LOF [12].

We can define the distribution density $q(x_t)$ restricted to a subset of measurement values taken within measurement time window $\mathcal{T}_k$ as the following

$$\tilde{q}(\boldsymbol{\zeta}_t) = \frac{1}{T} \sum_{\boldsymbol{\zeta}_\tau \in \mathcal{S}_k} \frac{1}{h(\boldsymbol{\zeta}_\tau)^P} K\left(\frac{\boldsymbol{\zeta}_t - \boldsymbol{\zeta}_\tau}{h(\boldsymbol{\zeta}_\tau)}\right), \quad (9)$$

where $T = |\mathcal{T}_k|$, $K(\cdot)$ is a kernel function expressed as a multivariate Gaussian function with P dimensions, zero mean and unit standard deviation as follows

$$K(x) = \frac{1}{(2\pi)^P} e^{-\frac{||x||^2}{2}}, \quad (10)$$

where $h(\boldsymbol{\zeta}_\tau)$ is the bandwidth function and can be defined as the following

$$h(\boldsymbol{\zeta}_t) = hd_k(\boldsymbol{\zeta}_t), \quad (11)$$

where $d_k(\boldsymbol{\zeta}_t)$ denotes the distance to the kth nearest neighbor of measurement $\boldsymbol{\zeta}_t$. The bandwidth value h indicates the weight selected for $d_k(\boldsymbol{\zeta}_t)$. On the one side, the larger the bandwidth value h, the more influential are the k nearest neighbors that are further away. On the other side, the smaller the value h, the more we focus on k nearest neighboring measurements. By substituting Eqs. (10)-(11) into Eq. (9), we can derive the density function as the following

$$\tilde{q}(\boldsymbol{\zeta}_t) = \frac{1}{T} \sum_{\boldsymbol{\zeta}_\tau \in \mathcal{T}_k} \frac{1}{2\pi^{\frac{P}{2}} h d_k(\boldsymbol{\zeta}_\tau)^P} e^{-\frac{r_k(\boldsymbol{\zeta}_t, \boldsymbol{\zeta}_\tau)^2}{2h d_k(\boldsymbol{\zeta}_\tau)^2}}, \quad (12)$$

where $r_k(x, y)$ is the reachability distance [13] expressed as $r_k(x, y) = \max(||x-y||^2, d_k(y))$ to prevent the distance from being very small.

Let us now suppose to have two consecutive sets of measurements $\mathcal{S}_k$ and $\mathcal{S}_{k+1}$ respectively taken in $\mathcal{T}_k$ and $\mathcal{T}_{k+1}$, and assume that in $k+1$ an intrusion occurred while in the measurement time window $\mathcal{T}_k$ a sufficient number [3] of samples has been retrieved to have a good estimation of the non-intrusion statistics. Given a beam pair (i, j), it yields that:

$$\boldsymbol{\zeta}_{t \in \mathcal{T}_k} \sim \mathcal{N}(\mu_k, \boldsymbol{\Sigma}_k), \quad \boldsymbol{\zeta}_{\tau \in \mathcal{T}_{k+1}} \sim \mathcal{N}(\mu_{k+1}, \boldsymbol{\Sigma}_{k+1}), \quad (13)$$

where $\boldsymbol{\Sigma}_t$ is the covariance matrix that automatically adjusts to the shape of the measurements set within time window $\mathcal{T}_k$. Using a general Gaussian kernel with such covariance matrix, it yields

$$\tilde{q}(\boldsymbol{\zeta}_t) = \frac{1}{T} \sum_{\boldsymbol{\zeta}_\tau \in \mathcal{T}_k} \frac{1}{2\pi^{\frac{P}{2}} h^P |\boldsymbol{\Sigma}_t|^{1/2}} e^{-\frac{r d_k(\boldsymbol{\zeta}^*_t, \boldsymbol{\zeta}^*_\tau)^2}{2h}}, \quad (14)$$

where $rd_k(\boldsymbol{x}, \boldsymbol{y}) = \max(d_\Sigma(\boldsymbol{x}, \boldsymbol{y})^2, d_k(\boldsymbol{y}))$, $d_\Sigma(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{x}^* - \boldsymbol{y}^*)^T(\boldsymbol{x}^* - \boldsymbol{y}^*)$ and $\boldsymbol{x^*} = (\boldsymbol{\Lambda}^T)^{-1/2}\boldsymbol{V}^T(\boldsymbol{x^*} - \mu)$. Please note that $\boldsymbol{\Lambda} = \text{diag}(\lambda_1, \ldots, \lambda_k)$ is the diagonal matrix of eigenvalues and $\boldsymbol{V} = [v_1, \ldots, v_k]$ is the matrix of corresponding eigenvectors of $\boldsymbol{\Sigma}_t$. We can now derive the density value factor as the following

$$\gamma(\boldsymbol{\zeta}_t) = \frac{\sum_{\boldsymbol{\zeta}_\tau \in \mathcal{T}_k} \frac{\tilde{q}(\boldsymbol{\zeta}_\tau)}{T}}{\tilde{\boldsymbol{\zeta}}_t + c \cdot \sum_{\boldsymbol{\zeta}_\tau \in \mathcal{T}_k} \frac{\tilde{q}(\boldsymbol{\zeta}_\tau)}{T}}. \quad (15)$$

Then, we can consider as outlier for the beam pair $(i, j) \in \mathcal{B}$ any value $\gamma(\boldsymbol{\zeta}_t) \geq \Delta$, where Δ is a detection threshold. This translates the system behavior into true positive event, i.e., $TP = Pr\left(\gamma(\boldsymbol{\zeta}_t) \geq \Delta\right), t \in \mathcal{T}_{k+1}$, and true negative event, i.e., $TN = Pr\left(\gamma(\boldsymbol{\zeta}_t) < \Delta\right), t \in \mathcal{T}_k$.

Given such probabilities, the detection threshold value Δ can be optimized so that the system accuracy is maximized. However, since the received power statistics are not known a priori and they are strongly dependent on the specific environment, the detection threshold must be chosen considering different environment settings.

III. Passive Intrusion Detection

While the outlier detection process helps to recognize the next environmental change as described in Section II, we need to identify the current status of our system based on the data collected within a measurement time window $\mathcal{T}_k$ in order to trigger an alert for potential intruders. We define two main system states: i) intrusion detected and ii) no intrusion detected, as shown in Fig. 1.

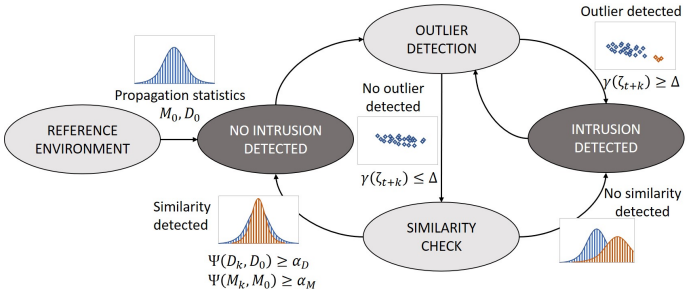


Fig. 1: The state diagram of PASID

Note that the continuous presence of an intruder within the environment may conditionally change the overall power measurements, which may exhibit altered distribution parameters μ and Σ as described in Section II-B. This would result, in turn, in upcoming power measurements distributed according to the new distribution statistics revealing no further outliers. Therefore, our system cannot rely *only* on the outlier detection process to determine the current system state as it might fail while trying to capture diverging behaviors. Instead, we need to introduce a new system state that accounts for such an intermediate state, namely *Similarity check*. This state is entered as soon as no further variation is retrieved, i.e., when no power measurement is marked as an outlier.

If no outliers are detected within an entire measurement time window $\mathcal{T}_k$, the *distribution similarity process* is executed. In particular, this process compares the expected mean values and variances of the received power distribution $\boldsymbol{M}_k$ and $\boldsymbol{D}_k$ within the previous measurement time window $\mathcal{T}_k$ as defined in Eqs. (7)-(8) in Section II-B against the distribution parameters of a reference scenario in $\mathcal{T}_0$. Note that the reference measurements distribution strongly depends on the selected environment and must be taken in advance when the environment is not occupied by any human presence (labelled as reference environment in Fig. 1).

We use the RV-coefficient to quantify the similarity between two matrices [14]. Specifically, we define it between matrices $\boldsymbol{X}$ and $\boldsymbol{Y}$ as the following

$$\Psi(\boldsymbol{X}, \boldsymbol{Y}) = \frac{tr(\Sigma_{XY}\Sigma_{YX})}{\sqrt{tr(\Sigma^2_{XX})tr(\Sigma^2_{YY})}}, \quad (16)$$

where the covariance matrix $\Sigma^2_{XX} = E(\boldsymbol{X}\boldsymbol{X}^T\boldsymbol{X}\boldsymbol{X}^T)$ while $\Sigma_{XY} = E(\boldsymbol{X}\boldsymbol{Y}^T)$. During the distribution similarity process we calculate $\Psi_M(\boldsymbol{M}_k, \boldsymbol{M}_0) \in [0, 1]$ and $\Psi_D(\boldsymbol{D}_k, \boldsymbol{D}_0) \in [0, 1]$. If $\Psi_M \geq \alpha_M$ and $\Psi_D \geq \alpha_D$, we claim that the distribution of measurements in $\mathcal{T}_k$ is similar to the distribution of measurements taken during the reference scenario. This places our system in the "No intrusion detected" state, as shown in Fig. 1. Otherwise, the intrusion state is entered again.

[3] While the sufficient number of samples may change depending on the specific scenario, we consider the minimum number of samples needed to obtain a 95% of confidence level.

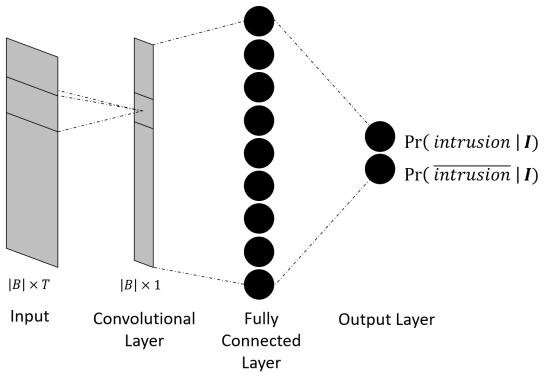


Fig. 2: Overview of the neural network architecture.

A. Discussion on dynamic settings

Different applied settings might result in different system behaviors. In a nutshell, we need to take into account the following aspects while designing our solution: i) a larger measurement time window $\mathcal{T}_k$ might capture better the channel dynamics and properly recognize the outlier but it might return a biased set of distribution statistics ($\boldsymbol{M}_k$ and $\boldsymbol{D}_k$) that might impair the overall similarity process; ii) α_D shall be chosen lower than α_M as the variance is a meaningful feature that better describes the data distribution, iii) the detection threshold value Δ shall be automatically selected as it may lead to reduce the sensitivity of the system to the possible intrusions (when set to high values) while triggering often an alarm (when set to low values) and, iv) we assume the power measurement statistics as normally distributed which makes our analysis tractable, deviations on this assumption would affect our solution effectiveness.

As it can be observed, although the multiple beams exhibit different distributions showing how the spatial diversity affects the mmWave communication channels, they can be reasonably mapped to normal distributions with different variance and mean values based on the selected transmission beam.

The PASID solution described so far effectively works for static scenarios where intruders enter an area without modifying the environment. However, when considering an intruder considerably changing the structure of the indoor environment (e.g., moving furniture or introducing new static objects) the reference environment may significantly change its power measurements distribution leading to a ping-pong effect between the "intrusion detected" and "similarity check" system states. In such a case, even though the room might have no intruders anymore and no outliers are detected, the power measurements distribution within the last measurement interval $\mathcal{T}_k$ may differ from the reference scenario in $\mathcal{T}_0$. To overcome this problem and make our PASID solution able to *dynamically learn* about room structure changes, we introduce in the next section a machine-learning module responsible of updating our reference environment when required.

IV. Learning environmental changes

To make our PASID solution robust to indoor mmWave environment changes we design a machine learning-based solution, which—by means of a training process—is able to *automatically* approximate the system model described in Section III. The advantage of a *self-learning* approach versus a *parametric model-based* solution is multifold: i) the distribution of the power measurements can radically change according to the specific deployment environment, thus the setting parameters have to be properly tuned for each indoor environment to successfully detect intrusions; ii) the indoor environment structure can change (e.g., furniture moved), resulting in a new reference environment that must be identified preventing the system to enter into a deadlock between the non-intrusion and similarity check states; iii) the multivariate Gaussian assumption of the power measurements might not hold if the number of transmission paths is not sufficiently high or in case of non-linearity of the power measurements.

Thus, in PASID we adopt a Deep Convolutional Neural Network Classifier architecture as depicted in Fig. 2. For each time interval k, the set of power measurements $\mathcal{S}_k$ taken within measurement time window $\mathcal{T}_k$ is organized as a matrix $\boldsymbol{I}_k \in \mathbb{R}^{B\times T}$ such that columns of $\boldsymbol{I}_k$ contain the measurements vector $\boldsymbol{\zeta}_t$ at the time $t \in \mathcal{T}$, whereas rows represent the temporal evolution of each element of $\boldsymbol{\zeta}_t$ within the measurement time window $\mathcal{T}_k$. The convolutional layer has a kernel with $T \times 1$ size and it is used to reduce the dimensionality of the input layer. Given the dimensions of the kernel, we can write the output of the convolutional layer as the following:

$$\boldsymbol{f}_k = y\left(\boldsymbol{I}_k \cdot \boldsymbol{w}\right), \tag{17}$$

wherein $\boldsymbol{f}_k = (f_k^{(i,j)})$ is relative to each beam couple $(i,j) \in \mathcal{B}$, $y(\cdot)$ is the *relu* activation function and $\boldsymbol{w}$ is the set of weights of the convolutional layer.

The idea behind is to exploit the convolutional layer to find an ad-hoc weighting vector $\boldsymbol{w}$, which is able to translate the temporal evolution of $\boldsymbol{\zeta}_t$ into a lower dimensional feature space that represents the intrusion phenomena and, at the same time, keeps separated the contributions of each couple $(i,j) \in \mathcal{B}$. The output of the convolutional layer is a vector with $B \times 1$ size. This vector is fed into a deep fully connected neural network comprising a 9-neurons layer followed by a 2-neurons output layer with *relu* and *softmax* activation functions, respectively. Such layers carry out the classification process. Additionally, the output neurons provide a score, which represents the conditioned probabilities $Pr(\text{intrusion}|\boldsymbol{I}_k)$ and $Pr(\overline{\text{intrusion}}|\boldsymbol{I}_k)$ by means of the softmax activation function. Therefore, the output neuron that maximizes the score represents the chosen output class inferred by PASID.

A key feature of the presented neural network is that, if the training set is provided with a sufficiently different number of indoor scenarios, the convolutional layer can potentially learn to extract features which are relevant to detect intrusion events independently on the environment itself. The variety of the training data affects also the classification part of the network that is able to generalize the classification process. This translates into a system which tends to be more *portable*:

Fig. 3: Deployed testbed in an office environment.

the higher variety of examples in the training set, the shorter the initial adaptation to the specific area of interest. Clearly, the perfect portability is an ideal condition, which might depend on the complexity of the faced scenario.

V. Testbed Implementation

We envision our solution as a standalone software component running on top of off-the-shelf mmWave devices, including (but not limited to) commercial routers, smart TVs, connected bulbs or plugs. While an optimal planning in the device placement process might be required to provide a full area coverage, we leave this design challenge out of the scope of the paper due to space concerns. However, we developed and deployed PASID into into an office testbed to check its feasibility in real indoor scenarios.

A. Testbed equipment and setup

We assume our testbed composed of four off-the-shelf 802.11ad-compliant Tp-Link Talon AD7200 devices that offer quasi-full spatial coverage of the considered area. Those devices are equipped with a 32-elements antenna array. Transmitting and receiving beam patterns are defined in two different codebooks consisting of 36 transmitting sector patterns and one quasi-omnidirectional receiving sector pattern, respectively. The default device firmware does not include an easy access to the beam training and received power values, therefore we use the LEDE-ad7200 firmware [15] on such devices that allows us to retrieve all needed information. Such a firmware provides several user space interfaces, which allows to interact with the *wil6210* firmware module that fully controls the IEEE 802.11ad interface. It provides access to the power measurements performed during the beam training phase, such as measured Received Signal Strength Indicator (RSSI) and SNR per each activated beam pattern.

We deploy the 4 mmWave devices in a $4m \times 8m$ office environment used as the testbed location. We consider two different device deployment setups. In the first setup, we install our devices under the ceiling of the office to investigate on the PASID performance when an intruder does not obstruct the Line-of-Sight (LOS) path. The latter, instead, includes mmWave devices placed on the desks and on the room lockers. This setup is LOS-blockage-prone as the LOS is established at

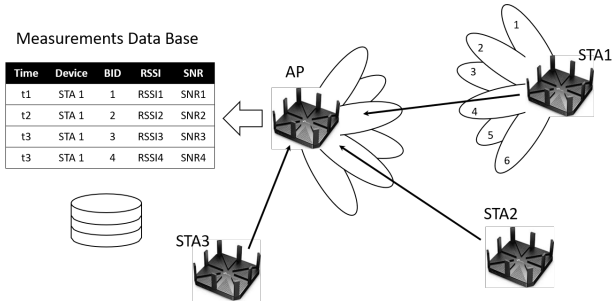


Fig. 4: Measurement process considering 1 AP and 3 STAs.

human body level and might be considered as a very common deployment for offices and private houses.

Fig. 3 shows the latter experimental setup with different devices distributed in the office. Devices are labeled according to their running configurations, i.e., Access Point (AP) or Stations (STAs). During our measurement campaigns, we emulate an intruder irruption inside the area of interest by considering a real human body, which is moving inside the office as well as a fictitious human phantom by means of water filled barrels that accurately emulate the field perturbation caused by a human body at 60-GHz-irradiation, as indicated in [16]. Additionally, we divide the floor walkable area in 52 reference squares, each with $50cm \times 50cm$ size to keep track of the actual intruder position in the room.

B. PASID execution

We build our reference scenario by choosing only one reference device (i.e., the AP in our testbed) and running PASID on top. In particular, as shown in Fig. 4, we set one device as an AP whereas the other three devices as stations (STA). STAs periodically perform the beam training phase with the AP to maintain or establish a new connection. While running the beam training process between AP and STA1, each transmission beam pattern is iteratively activated and power measurements are collected into a database that stores information about the STA ID, the beam ID, the measured RSSI, SNR values and the measurement time. This process is automatically repeated for each STA such that the AP is provided with an overall picture of the environment channels condition from different viewpoints. While PASID is only executed on a single reference device, it can be additionally run on each STA so as to provide a further enriched system view of the environment at the expense of some additional overhead to transmit this data to the AP.

Once the reference scenario without human bodies has been created, and the neural network of PASID is updated with the training weight set (as described in Section VI), the detection system is automatically activated as described in Fig. 1 of Section III. Measurements are periodically retrieved when the beam training process is executed such that the neural network can accurately parse current channel conditions and trigger an alarm when an intrusion is detected. We refer the reader to Section VI for more information on the setting parameters used in our experiments.

VI. Experimental results

The measurement collection is performed in an office environment as described in Section V. We consider three different office furniture setups by placing a locker in different positions inside the office. The presence of the locker aims to emulate a change in the office environment that should not trigger an intrusion alarm. Devices are configured to have one as AP and all the others as STAs. In other words, we establish 3 different mmWave links between each pair of AP and STA.

A. Neural network training

The measurement collection is performed by keeping active the 802.11ad interface of the devices and forcing the beam training phase running within a period of 10 minutes, thereby collecting about 3800 measurements (about 1260 per STA). We repeat such a measurement process 2 times per each considered office furniture relocation: at the first stage no human bodies are placed in the office, while on the second time humans are walking inside the office. Given that the devices do not allow to synchronize the beam training process executions, the number of training phases involving different stations is slightly different. Thus, depending on the number of STAs involved in the experiment we create the feature vector $\boldsymbol{Z}_t$ as follows:

$$\boldsymbol{Z}_t = [\zeta_t^1, \zeta_t^2, \ldots, \zeta_t^N] \tag{18}$$

wherein ζ_t^d indicates that the beam training phase is performed by the d^{th} STA, and N indicates the total number of connected STAs. Since the t-th SLS phase involves only a specific STA d, we fill the subset of features in $\boldsymbol{Z}_t$ corresponding to d with the new data, while the remaining features are taken from the vector $\boldsymbol{Z}_{t-1}$.

Subsequent vectors $\boldsymbol{Z}_t$ belonging to the measurement time window $\mathcal{T}_k$ are then organized in the matrix I_k as described in Section IV. To train the network we generated several matrices I_k with overlapping measurement time windows $\mathcal{T}_k$, being each interval shifted by $\delta_t = 10$ measurements so that two consecutive matrices are expressed as $I_k = [\boldsymbol{Z}_k, \ldots, \boldsymbol{Z}_{k+\delta}]$ and $I_k = [\boldsymbol{Z}_{k+\delta}, \ldots, \boldsymbol{Z}_{k+\delta+T}]$ and I_{k+1}. Moreover, we performed data augmentation by reversing the time dimension of the matrices I to double the dataset. We then labeled each matrix I_k with the corresponding class, i.e. "intrusion" or "non-intrusion", depending respectively on the presence or absence of humans in the office. This leads to a dataset consisting of about 22800 matrices I with a balanced mix of intrusion and non-intrusion classes. We divided the dataset in training, validation and testing sets, which are constituted by the 52.5%, 22.5% and 25% of the entire dataset respectively, and we normalized the dataset as follows:

$$\boldsymbol{Z}_{t_{\text{NORM}}} = \frac{\boldsymbol{Z}_t - \boldsymbol{\mu}_Z}{\boldsymbol{\sigma}_Z}, \tag{19}$$

where $\boldsymbol{\mu}_Z$ and $\boldsymbol{\sigma}_Z$ are respectively the average value and variance of the vector $\boldsymbol{Z}$ considering all the measurements in the training set. We train our neural network with a batch size of 1000, 30 epochs, a learning rate of 0.0001 and using the good-performing *Adam* optimizer as indicated in [17].

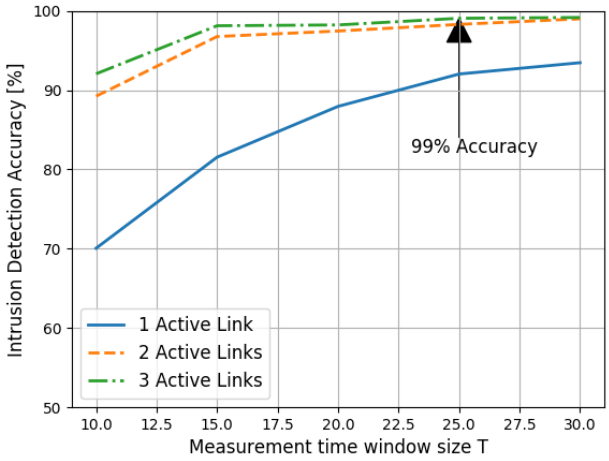


Fig. 5: Average intrusion detection accuracy in the office with different number of connected devices and different sizes of the measurement time window T (where $T = 1$ is about 0.5s).

B. Intrusion detection performance

Fig. 5 shows the average intrusion detection performance achieved by PASID by means of the classification accuracy metrics considering different numbers of connected STAs and different sizes for the measurements time window T. From obtained results we can observe the following: on the one hand, as the number of connected STAs grows, the intrusion detection accuracy performance increases because, by adding different locations of transmitting devices, we increase the information provided to PASID for the mmWave environment modeling. On the other hand, increasing the measurement time window size T also increases the intrusion detection accuracy performance since a larger temporal sample set provides a better overview on the different measurement statistics.

Fig. 6 shows the intrusion detection accuracy performance achieved with an intruder standing *still* in different zones of the monitored area modeled with a human phantom. The results correspond to the worst-case of having a *single* link with $T = 20$. As it can be observed, depending on the position within the office the accuracy varies depending on the reflections in the environment with a range varying from 82 to 98%. Considering a real case with a moving intruder or having more than a single link will result in improved accuracy ranges getting to 99% on average, as shown in Fig.5.

As discussed in Section V, we might allow STAs collaborating with the AP to enrich the overall PASID's channel overview at the expense of some communication overhead. We considered this scenario by adding data available on each STA to vector $\hat{\boldsymbol{Z}}$. Fig. 7 provides the confusion matrix for a scenario with 3 STAs connected. In this case, PASID achieves an outstanding accuracy of 99.67% for $T = 30$.

Finally, as 802.11ad devices are not required to re-train the beams in case of sufficient RSSI, we evaluate the energy consumption of the devices i) when they are connected, ii) when they are forced to trigger the beam training phase and iii)

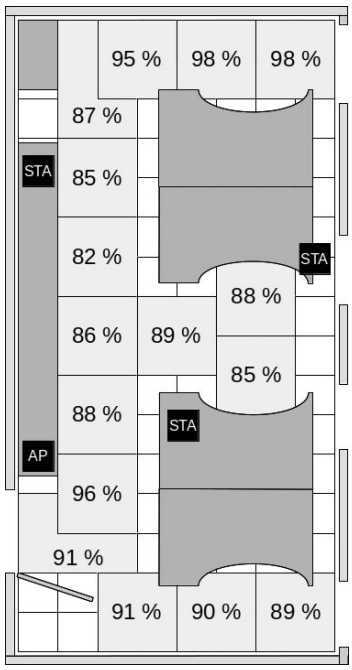


Fig. 6: Intrusion detection accuracy in different zones of the area of interest.

when PASID is executed. To do so, we connect the devices' power supply to a smart plug that records the measured energy consumption when the device 802.11ad interface is powered off, when its active (but no training phase is performed), when devices are forced to perform the training phase and, when PASID is activated.

Results are reported in Table I where the column PASID indicates the activation of the algorithm (for the AP) while it indicates when the stations are collaborating with the AP by sharing their measurements (for the STA).

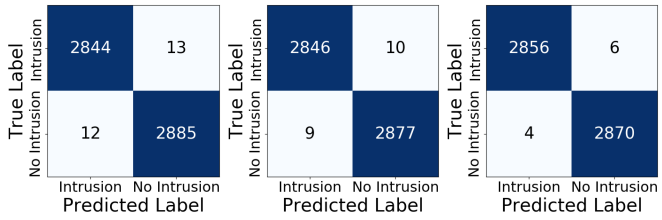
TABLE I: Power consumption measured for the different mmWave devices interface states

	Idle	**Active**	**Beam Training**	**PASID**
AP	6.8 [W]	7.8 [W]	7.8 [W]	8.0 [W]
STA	6.8 [W]	7.4 [W]	7.4 [W]	7.5 [W]

From the results, it is worth noting that the activation of the beam training phase does not significantly affect the devices' power consumption, while the activation of PASID is slightly increasing the overall devices consumption by $\sim 2\%$.

C. Intruder Localization

Given the directional nature of the mmWave communication, we can further exploit the measurements taken during the beam training phase to sense the propagation environment towards specific directions. Specifically, we can map, alongside the intrusion detection, the changes sensed by the different beams onto the (potential) location of the intruder inside the area of interest (i.e., within the office). To validate our idea, we use PASID implementing a variation of the neural network-based solution. We place the human phantom in each



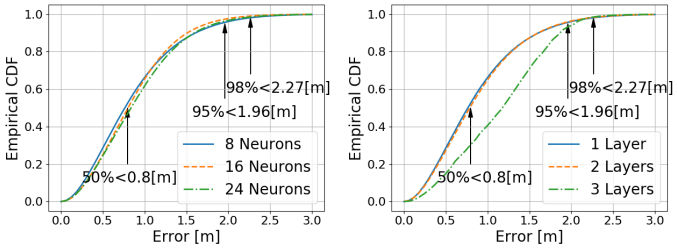
(a) $T = 10$ (b) $T = 20$ (c) $T = 30$

Fig. 7: Confusion matrices with STAs collaborating to PASID data gathering.

of the reference squares on the floor of the area of interest[4] and we collect 20 minutes of measurements per each reference square to gather in total about 7600 measurements per each position. Measurements are associated with the position, i.e. coordinates, of the corresponding reference square in the area of interest, which becomes the desired output of the neural network. To enrich the information during this process, we consider both the measurements taken by the AP and by the STAs in the feature vector $\boldsymbol{Z}$. We divide the dataset in training, validation and testing sets, with 52.5%, 22.5% and 25% of the entire set, respectively. Data is then normalized as described in Eq. (19).

In this case, we neglect the temporal evolution of $\boldsymbol{Z}$, conversely, we assume that an intrusion occurred, hence we aim at mapping $\boldsymbol{Z}$ onto the location of the intruder in the office. Therefore, we adopt a different neural network architecture with respect to the one described in Section IV. We consider a deep neural network with an input layer with the dimensionality of the vector $\boldsymbol{f}$, followed by N L-neurons hidden layers and a 2-neurons output layer. As activation functions, we select *tanh* for the hidden layer and *linear* for the output one. We train our neural network with a batch size of 1000, 100 epochs, a learning rate of 0.0001 and using the good-performing *Adam* optimizer [17]. Fig. 8a shows the intruder localization performance with 1 hidden layer network with different number of neurons, while Fig. 8b is showing the localization performance achieved by keeping the hidden layer size at 8-neurons and changing the depth of the network.

Our results show that we can achieve a localization accuracy



(a) Different neurons (b) Different layers

Fig. 8: Cumulative Distribution Function of the intruder localization error.

[4]We refer the reader to Section V for a detailed description of the human phantom and the reference squares.

slightly above 2 meters in 98% of the cases, and that increasing the complexity of the network does not help to improve localization performances. Therefore, a low complexity architecture, which can fit in the limited hardware of COTS devices is sufficient to effectively exploit directional power measurements to estimate intruders locations.

VII. Related work

Recently, Wi-Fi based environmental sensing and signal human interaction has attracted much attention due to the ability to detect propagation environment changes caused by humans, which may perturb the monitored areas, without requiring any active connection with devices carried by the intruder [18].

Authors in [19] exploit the variance of the RSSI of the signal measured between an AP and a STA together with a maximum likelihood estimator to detect the presence of an intruder in an indoor environment. Results highlight some weakness of the signal RSSI in realistic environments as a feature to detect intrusion due to its high instability. Differently, in [20] RSSI is extracted by Zigbee sensors. The measurements from different sensors enable to track RSSI variation from distinct point of views, which are combined by means of a K-neighborhood clustering to perform intrusion detection. The localization and tracking problem exploiting RSSI values obtained from WSN nodes was reformulated based on an inverse source problem in [21]. Additionally, another work exploiting power measurements to detect the presence of entities inside an area of interest is Radio Tomografic Imaging [22], [23], wherein the RSSI measured by several sensor is exploited to produce a signal attenuation map of the monitored area, which can produce high quality detection and localization at the expense of a relatively high number of sensors.

RSSI was first utilized in WLAN-based human detection as it is easy to obtain. However, it suffers from a severe multipath effect in indoor scenario as it is usually provided by a coarse-grained measurement by devices, therefore the research community moved its attention to the exploitation of Channel State Information (CSI) information to better sense the environment. Differently from RSSI, which is just capturing the received power, CSI is able to provide the channel state at the level of each pair of receiver and transmitter antenna and per each sub-carrier. However, differently from RSSI measurements the extraction of CSI measurements from COTS devices requires some firmware modifications [24].

Authors in [25] present an 802.11n-based human activity monitoring system that leverages on the predictable fluctuation of the received CSI. Specifically, they developed techniques for indoor respiration detection and movement direction estimation using commodity devices. A Passive Intrusion Detection system based on CSI amplitude variation is proposed in [26], however it is still built on the 802.11n technology. Similar to our work, CSI information is collected to train a SVM classifier aiming to distinguish between static and dynamic scenarios and triggers an alarm in case of dynamic scenarios.

In [27], authors use the CSI variance as a feature for an intrusion detection system. Specifically, the measured variance provides the observations, which are used by a 2-state Hidden Markov Model to trigger an alarm. CSI variance is explored also in [28], wherein a device-free passive motion detection based on the earth mover distance algorithm is proposed. Another application of 802.11n-based CSI is proposed in [29] for a device-Free Crowd Counting application, which relies on the percentage of non-zero elements of the CSI matrix to count the number of humans in the monitored area. An additional proposal on the CSI-based WI-Fi indoor localization is investigated by the authors of [6] that explored the meaningful features of a Deep Neural Network to perform precise CSI-based passive indoor localization. Finally, CSI information together with communication directionality are exploited by authors in [30] to perform accurate 3D localization of connected devices.

Differently from the above-mentioned state-of-the-art works, we leverage on the directional properties of 802.11ad-compliant devices to sense the surrounding environment by means of directional RSSI measurements. The spatial diversity allows us to overcome the need of CSI information to achieve remarkable performance. Therefore, it can be implemented in 802.11ad COTS devices without relevant modifications of the firmware. To the best of our knowledge, this work is the first implementation of a passive intrusion detection system running on commercial 802.11ad devices.

VIII. Conclusions

mmWave deployments will become pervasive in indoor environments to address the increasing future users' data rates needs. In this paper, we analyze a mmWave technology solution that exploits its unique propagation properties to *passively detect intruders* indoors. The solution has been modeled analytically and the main limitations of traditional approaches identified.

Based on this, the machine learning-based solution PASID is presented that, given a specific indoor space, i) automatically models the propagation environment and ii) passively detects if an intruder enters the area, i.e. without requiring/enforcing any active communication. To evaluate its feasibility in practice PASID has been deployed in 4 off-the-shelf mmWave devices in a $32m^2$ office. Our results show that PASID achieves an intruder detection effectiveness of $\sim 99\%$ and localizes targets within a $\sim$ 2 meters range at a negligible energy cost ($\sim 2\%$).

References

[1] IEEE P802.11ay, "Enhanced throughput for operation in license-exempt bands above 45 GHz," IEEE 802.11 Working Group, Mar. 2019.

[2] Y. Ghasempour, C. R. C. M. da Silva, C. Cordeiro, and E. W. Knightly, "IEEE 802.11ay: Next-generation 60 GHz communication for 100 Gb/s Wi-Fi," *IEEE Communications Magazine*, vol. 55, no. 12, Dec. 2017.

[3] K. Haneda, J. Jrvelinen, A. Karttunen, M. Kyr, and J. Putkonen, "A statistical spatio-temporal radio channel model for large indoor environments at 60 and 70 GHz," *IEEE Transactions on Antennas and Propagation*, vol. 63, no. 6, pp. 2694–2704, Jun. 2015.

[4] T. S. Rappaport, Y. Xing, G. R. MacCartney, A. F. Molisch, E. Mellios, and J. Zhang, "Overview of millimeter wave communications for fifth-generation (5G) wireless networkswith a focus on propagation models," *IEEE Transactions on Antennas and Propagation*, vol. 65, no. 12, Dec. 2017.

[5] H. Huang, Y. Song, J. Yang, G. Gui, and F. Adachi, "Deep-learning-based millimeter-wave massive MIMO for hybrid precoding," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, Mar. 2019.

[6] S. Liu, R. Y. Chang, and F. Chien, "Analysis and visualization of deep neural networks in device-free Wi-Fi indoor localization," *IEEE Access*, vol. 7, pp. 69 379–69 392, May 2019.

[7] Y. Yang, H. S. Ghadikolaei, C. Fischione, M. Petrova, and K. W. Sung, "Reducing initial cell-search latency in mmWave networks," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, Apr. 2018.

[8] C. Slezak, V. Semkin, S. Andreev, Y. Koucheryavy, and S. Rangan, "Empirical effects of dynamic human-body blockage in 60 GHz communications," *IEEE Communications Magazine*, vol. 56, no. 12, Dec. 2018.

[9] D. De Donno, J. P. Beltrán, D. Giustiniano, and J. Widmer, "Hybrid analog-digital beam training for mmwave systems with low-resolution RF phase shifters," in *IEEE International Conference on Communications Workshops (ICC)*, May 2016.

[10] H. Yang, M. H. Herben, and P. F. Smulders, "Indoor radio channel fading analysis via deterministic simulations at 60 GHz," in *IEEE 3rd International Symposium on Wireless Communication Systems*, Sep. 2006.

[11] S. Hawkins, H. He, G. Williams, and R. Baxter, "Outlier detection using replicator neural networks," in *Proceedings of the 4th Int. Conf. on Data Warehousing and Knowledge Discovery (DaWaK02)*, Sep. 2002.

[12] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "LOF: identifying density-based local outliers," in *ACM sigmod record*, vol. 29, no. 2, May 2000.

[13] E. Cohen, E. Halperin, H. Kaplan, and U. Zwick, "Reachability and distance queries via 2-hop labels," in *Proceedings of the Thirteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, ser. SODA '02. Society for Industrial and Applied Mathematics, Jan. 2002.

[14] Herve Abdi, "Congruence coefficient, RV-coefficient and mantel coefficient," In Neil Salkind (Ed.), Encyclopedia of Research Design., Jan. 2010.

[15] D. Steinmetzer, D. Wegemer, and M. Hollick. (2017) Talon tools: The framework for practical IEEE 802.11ad research. [Online]. Available: https://seemoo.de/talon-tools

[16] C. Gustafson and F. Tufvesson, "Characterization of 60 GHz shadowing by human bodies and simple phantoms," in *6th European Conference on Antennas and Propagation (EUCAP)*, Mar. 2012.

[17] S. Vani and T. V. M. Rao, "An experimental approach towards the performance assessment of various optimizers on convolutional neural network," in *3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, Oct. 2019.

[18] M. Youssef, M. Mah, and A. Agrawala, "Challenges: device-free passive localization for wireless environments," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*. ACM, Sep. 2007.

[19] M. Moussa and M. Youssef, "Smart devices for smart environments: Device-free passive detection in real environments," in *IEEE International Conference on Pervasive Computing and Communications*, Mar. 2009.

[20] J. Yang, Y. Ge, H. Xiong, Y. Chen, and H. Liu, "Performing joint learning for passive intrusion detection in pervasive wireless environments," in *Proceedings IEEE INFOCOM*, Mar. 2010.

[21] F. Viani, P. Rocca, M. Benedetti, G. Oliveri, and A. Massa, "Electromagnetic passive localization and tracking of moving targets in a WSN-infrastructured environment," *Inverse Problems*, vol. 26, no. 7, Jul. 2010.

[22] Q. Wang, H. Yiitler, R. Jntti, and X. Huang, "Localizing multiple objects using radio tomographic imaging technology," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 5, May 2016.

[23] J. Wilson and N. Patwari, "Radio tomographic imaging with wireless networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 5, pp. 621–632, May 2010.

[24] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Tool release: Gathering 802.11 n traces with channel state information," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 1, Jan. 2011.

[25] D. Zhang, H. Wang, and D. Wu, "Toward centimeter-scale human activity sensing with wi-fi signals," *Computer*, vol. 50, no. 1, Jan. 2017.

[26] T. Wang, D. Yang, S. Zhang, Y. Wu, and S. Xu, "Wi-Alarm: Low-cost passive intrusion detection using WiFi," *Sensors*, vol. 19, no. 10, May 2019.

[27] J. Lv, D. Man, W. Yang, X. Du, and M. Yu, "Robust WLAN-based indoor intrusion detection using PHY layer information," *IEEE Access*, vol. 6, Dec. 2017.

[28] W. Liu, X. Gao, L. Wang, and D. Wang, "BFP: Behavior-free passive motion detection using PHY information," *Wireless Personal Communications*, vol. 83, no. 2, Feb. 2015.

[29] W. Xi, J. Zhao, X.-Y. Li, K. Zhao, S. Tang, X. Liu, and Z. Jiang, "Electronic frog eye: Counting crowd using WiFi," in *IEEE INFOCOM*, Apr. 2014.

[30] I. Pefkianakis and K.-H. Kim, "Accurate 3D localization for 60 GHz networks," in *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*, Nov. 2018.