Towards Spoofing Resistant Next Generation IoT Networks

Mohammad Reza Nosouhi, Keshav Sood, Marthie Grobler, and Robin Doss, *Senior Member, IEEE*

***Abstract*— The potential vulnerability to wireless spoofing attacks is still a critical concern for Next Generation Internet of Things (NGIoT) networks which may result in catastrophic consequences in mission–critical applications. Conventional solutions may impose additional signal processing, protocol, and latency overheads which are inappropriate for NGIoT networks designed to provide high–speed and low–latency connections for a large number of resource–constrained IoT devices. In this paper, we utilize the uniqueness of beam pattern features in mmWave–enabled devices and propose a scalable security mechanism for the detection of wireless spoofing attacks in NGIoT networks. This uniqueness is proven to exist due to the non–ideal manufacturing of antenna arrays used in mmWave–enabled devices. In our approach, when legitimate mmWave–enabled IoT devices enrol into the network, their unique beam features are learned by a learning model developed at the network server. Then, during data transmission, network base stations (gNBs)/Access Points (APs) measure the beam features from the received RF signals and send them to the network server for the detection of anomalies. We develop our learning model based on Deep Autoencoders (DAEs) that are an effective tool for anomaly detection. Fortunately, the beam feature extraction can be performed using the beam searching mechanism that is already provided in mmWave standards (5G–NR and IEEE 802.11ad). Thus, feature extraction does not introduce any signal processing overheads to the system. Moreover, the proposed mechanism imposes zero computation/communication overhead to the resource—constrained IoT nodes. In our experiments, we reached 98.6% accuracy in the detection of illegitimate devices which confirms the effectiveness of the proposed approach.**

***Index Terms*— 5G–NR, deep learning, Internet of Things (IoT), IoT security, mmWave communication, physical layer security, wireless spoofing attack detection.**

I. Introduction

THE Next Generation Internet of Things (NGIoT) facilitates the development of innovative IoT applications by integrating different technologies into conventional IoT systems. In this regard, millimeter wave (mmWave) wireless communication (offered in 5G–NR and IEEE 802.11ad) is considered as a promising technology to address the energy efficiency and low latency requirements of these bandwidth–hungry applications [1]–[3]. Due to their operation at Super High Frequency (SHF) and Extremely High Frequency (EHF) bands, mmWave systems provide ultra-high speed and reliable communications in relatively short distances. This makes them a suitable communication approach for NGIoT applications that are deployed in populated environments or in application scenarios in which a very high level of network connectivity is needed, e.g., V2X communications in Intelligent Transportation Systems (ITS), real-time surveillance cameras, Industrial IoT applications, high-precision navigation systems, etc. In these applications, the detection of illegitimate network accesses is an open issue since they are potentially vulnerable to wireless spoofing attacks, e.g., Man–in–the–Middle attacks, device impersonation, session hijacking, sinkhole attacks, etc. [4]–[6].

There are several issues that render the conventional security solutions ineffective and/or inefficient to address wireless spoofing attacks in NGIoT networks. (1) The lack of an effective public key infrastructure (PKI) in large–scale IoT networks prevents the employment of public key encryption techniques to perform secure device authentication and the exchange of symmetric shared keys between IoT devices and gNBs/APs [7], [8]. (2) Limited computation and energy resources of IoT devices may make the security solutions inefficient [7], [9]. (3) IoT devices are usually vulnerable to physical attacks (i.e., they might be physically accessed by an attacker to obtain sensitive information, e.g., root keys) [10], [11]. (4) NGIoT mission–critical applications are latency–sensitive, thus, can not tolerate any additional latency overhead introduced by security solutions [6], [12]. (5) Security solutions based on public key cryptography rely on the computational hardness of a mathematical problem (e.g., discrete logarithm) which can be effectively solved by a quantum–enabled attacker in future [8]. (6) For highly dynamic IoT applications, e.g., Internet of Vehicles (IoV), IoT devices may join or leave the network repeatedly and at any time. This results in large authentication overheads for the devices as well as the network gNBs/APs [7], [13].

To address these issues, physical layer security (PLS) is considered as a promising approach to provide lightweight security solutions for IoT networks [7], [14], [15]. In PLS–based security approaches, the provenance of data is checked by extracting and analysing the intrinsic features of Radio Frequency (RF) signals (known as RF signature) that are unique for every wireless IoT device. This feature uniqueness is a result of the non-ideality of RF circuits in the transmitter module (Tx) of wireless IoT devices. It is caused

Manuscript received December 12, 2021; revised March 18, 2022; accepted April 8, 2022. Date of publication April 28, 2022; date of current version May 6, 2022. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. George Loukas. *(Corresponding author: Mohammad Reza Nosouhi.)*

Mohammad Reza Nosouhi, Keshav Sood, and Robin Doss are with the Centre for Cyber Security Research and Innovation, Deakin University, Geelong, VIC 3220, Australia (e-mail: m.nosouhi@deakin.edu.au; keshav.sood@deakin.edu.au; robin.doss@deakin.edu.au).

Marthie Grobler is with CSIRO's Data61, Melbourne, VIC 3008, Australia (e-mail: marthie.grobler@data61.csiro.au).

Digital Object Identifier 10.1109/TIFS.2022.3170276

by the non-ideality of Tx manufacturing processes and is very expensive to avoid making the unique RF features difficult to forge (unlike the software–based characteristics) [16]–[18]. Thus, they could be utilized to ensure data provenance in IoT networks [16], [19].

In this regard, a number of device authentication mechanisms have been proposed based on RF signature (RF fingerprint) of IoT devices [16], [20]–[22], [23]. However, they suffer from at least one of the following practical issues which make them weak/inefficient for practical implementations. (1) They use RF modulation features (e.g., frequency and phase offsets) that are very limited in numbers. Consequently, in large–scale IoT scenarios, the obtained low–dimensional feature space results in poor classification accuracy. (2) The deployed RF features might be data dependent causing them to change when IoT devices send different bit streams. This may degrade the classification performance [16], [24]. (3) In preamble–based approaches, the transmitter needs to include a specific preamble bit stream in the transmitted data to enable the receiver device to accurately extract RF features from the received signal. This results in additional bandwidth overheads and may degrade the performance of IoT applications [16]. (4) The current RF fingerprint mechanisms may suffer from lack of stability in the RF features since a change in environment and/or device parameters (e.g., power supply voltage) may change the RF modulation features [16]. In addition to the mentioned challenges, these approaches may introduce additional signal processing and protocol overheads to gNBs/APs. This is an important issue in IoT networks with a large number of wireless IoT devices [21], [24].

Motivated by this, we propose a lightweight and learning–based security mechanism for the detection of wireless spoofing attacks in 5G mmWave–enabled NGIoT networks. In our system design, we utilize the unique beam pattern features of the legitimate mmWave—enabled IoT wireless devices to recognize an illegitimate device. Since the mmWave communication systems work at frequencies above 6 GHz (24 GHz to 52.6 GHz licensed band for 5G–NR and 60 GHz unlicensed band for IEEE 802.11ad [2], [25]) the wavelength is in the *mm* range (5-12.5 mm). Thus, large–scale array antennas can be fabricated on small physical platforms. It has been proved that the non–ideal manufacturing of theses antenna arrays makes the beam pattern features of an emitted signal unique to the transmitter device [24]. However, authenticating a large number of IoT devices (using a lightweight and learning–based classification model) may result in poor classification accuracy (the scalability issue). For this reason, we propose a Deep Autoencoder (DAE) model that learns the device dependent beam features of legitimate IoT devices to identify illegitimate devices (anomalies). Using this approach, the classification task is performed in a way that is similar to a binary classification problem. DAEs are known as effective Deep Learning–based models to perform anomaly detection tasks [26]. Beside scalability, the significant characteristics of our proposed mechanism are as follows: (1) High–dimensional beam features are utilized to develop the anomaly detection DAE model. Having a high–dimensional feature space improves the reliability and accuracy of the learning–based detection model. (2) The beam features are independent of the transmitted data. Thus, the proposed mechanism is a preamble–less physical layer security mechanism. (3) The unique beam features of a single mmWave–enabled device are stable since they do not depend on variable device parameters (e.g., power supply voltage) [24]. (4) The beam features can be extracted using the beam searching mechanism which is a built–in procedure in mmWave standards (5G–NR and IEEE 802.11ad). Thus, feature extraction does not impose additional protocol and signal processing overheads to the system. (5) No additional hardware/software modules are required at the transmitter side. Thus, it results in zero computation/communication overhead on the resource constrained IoT nodes.

Our experiments confirm the effectiveness of the proposed mechanism in the detection of wireless spoofing attacks. We achieved 98.6% of accuracy for 100 legitimate devices. Our main contributions are as follows:

- We propose a lightweight security solution for the detection of wireless spoofing attacks in 5G mmWave–enabled NGIoT networks. The proposed mechanism is a practical approach that addresses the drawbacks of the current RF fingerprinting security solutions and can be integrated into 5G–NR and IEEE 802.11ad mmWave communication systems with no additional protocol overheads.
- To address the scalability problem of the current RF fingerprinting mechanisms, we propose a scalable DAE model that (regardless of the number of devices) performs the recognition of legitimate devices in the form of a binary classification problem.
- To make the malicious replay efforts unsuccessful, we propose a novel time–based solution that makes it infeasible for an attacker device to reuse the RF signals of legitimate devices (obtained through eavesdropping attempts) and conduct a spoofing attack.

In the reminder of the paper, we review the related work in Section 2 and present the proposed security mechanism in Section 3. Our security analysis and the results of our experiments are provided in Section 4 and 5 respectively. Finally, we conclude the paper in Section 6 by presenting a summary and future work.

II. Related Work

Previous research on the detection of wireless spoofing attacks focus on the utilization of unique characteristics of radio communication channels [21], [27]. These approaches work based on the fact that wireless channel impairments such as path loss, shadowing, and multipath fading make the channel–dependent features location specific. Consequently, RF signals sent from devices at different locations provide features with different values at the receiver (e.g., received signal strength (RSS), channel state information (CSI), channel frequency response (CFR), etc.). In [28], channel states of data packets are used to detect spoofing attacks in dynamic wireless networks. In this work, the interactions between spoofers and a legitimate receiver during the authentication process are formulated as a zero–sum authentication game. Using

reinforcement learning, a player obtains the optimum test threshold in a dynamic environment. In [29], the authors have utilized signal processing and feature recognition techniques to improve the attack detection performance. In this regard, they introduce a novel pre–treatment mechanism based on sparse representation (SR) to reinforce signal characteristics. To further increase the attack detection accuracy, the authors have developed a fuzzy C–mean clustering algorithm to solve the recognition problem.

An attack detection approach has been proposed in [30] that works based on the extraction and analysis of channel fingerprints in a slow time–varying fading channel. In [31], a machine learning–based mechanism has been proposed to detect spoofing attacks in wireless sensor networks (WSNs) based on the RSS parameter. The main idea behind the proposed mechanism is based on the fact that due to shadowing, slow variations occur in the average RSS. The significant characteristic of the proposed algorithm is that it is optimized for scenarios where the legitimate node and the attacker are located at a very close physical distance from each other which is the worst–case attack scenario. Another RSS–based mechanism has been proposed in [32] for the detection of identity attacks in IEEE wifi–based ad hoc networks. In the proposed distributed mechanism, each wireless node utilizes the channel characteristics and obtains the distance parameters to detect malicious identities in its own radio range.

The attack detection mechanism introduced in [33] works based on the analysis of time series of physical layer features in a network of wearable devices. The novel idea of this work is based on the fact that body movement makes the RSS behavior of off–body devices different from on–body devices. This diversity in feature dynamics is used to distinguish legitimate devices from malicious attackers. To find the optimum model for the prediction of RSS time series, the autoregression (AR) and long short term memory (LSTM) learning models have been used and a comparison based on the obtained results has been presented [33].

A number of RF fingerprinting mechanisms have been proposed in the literature for the detection of wireless spoofing attacks. In one of the most recent studies, Huan *et al*. [20] propose a novel mechanism to perform node identification and spoofing attack detection in WSNs. In this approach, the inherent (device dependent) clock skews of wireless nodes are utilized to identify the legitimate wireless nodes in the network. Two variations of this approach are proposed in the paper, i.e., centralized and distributed, to be used in single–hop and multi–hop WSNs, respectively. In [16], a learning—based mechanism has been proposed to authenticate IoT devices based on the uniqueness of RF features. The authors have used a supervising machine learning model to identify 10000 different wireless devices and achieved the high accuracy of 99% in their experiments. However, the deployed learning model has not been clearly discussed in the paper. This is very important since supervised machine learning models usually have poor classification performance in the scenarios with a large number of classes. In addition, they have not proposed a defence mechanism against replay attacks.

Since the mmWave wireless networks have been recently emerged (e.g., IEEE 802.11ad and 5G-NR), the detection of wireless spoofing attacks in these networks has not been thoroughly investigated so far. As far as we know, three research works have been published in this field so far. In the first work [34], the authors introduced a virtual channel model to enable spoofing detection in mm–Wave massive MIMO networks. In the proposed approach, the Euclidean distance of virtual channels are used to establish a binary hypothesis test. Moreover, a novel solution has been proposed based on Neyman–Pearson testing to find the optimum threshold for the Euclidean distance between channel matrices. However, their approach is based on the assumption that successive message transmissions are occurred within the coherence time of the communication channel. This can make the solution ineffective for applications with low message exchange rate. The second work is a novel learning–based mechanism proposed by Wang *et al.* [27] for the detection of spoofing attacks in IEEE 802.11ad networks. In this work, it is proposed to utilize signal to noise ratio (SNR) traces obtained at the receiver during the sector level sweep (SLS) process to distinguish malicious signals from legitimate transmissions. Regarding the learning model, backpropagation and forward propagation neural networks have been proposed to provide effective performance with small sample learning and allow for quick model construction. However, scalability and device mobility are two main concerns that have not been discussed in this work.

Another interesting research in the field of device fingerprinting in mmWave wireless networks is presented in [24]. Findings from this paper forms the basis of our work, specifically the uniqueness of beam patterns. As far as we know, the uniqueness of beam features in mmWave wireless networks is introduced in [24] for the first time. The authors used several off-the-shelf mmWave devices to show that the identification of these devices using their beam features is feasible. They achieved 99% identification accuracy. They also proposed a multiple access point architecture to utilize the spatial features of device beam patterns since their findings show that a signal replay attack is feasible with high success rate in scenarios with a single access point. They have shown that the success rate of a replay attack is significantly reduced when using the proposed multiple access point architecture. In the following, we describe the main characteristics that distinguish our work from [24].

As pioneering work, the target of [24] is to show the feasibility of device identification using beam patterns, i.e., to identify each individual mmWave-enabled device using its unique beam features (i.e., device authentication). In this regard, they have performed their experiments with a small number of devices (12 devices). However, further research efforts are required to develop a classification model that can classify a large number of devices using the proposed technique (i.e., the scalability property). Our work, however, focuses on the recognition of intruder devices from legitimate devices whose beam features have been already learned by the DAE model. In other words, we do not employ a classification model to identify specific devices (with specific access rights). Instead,

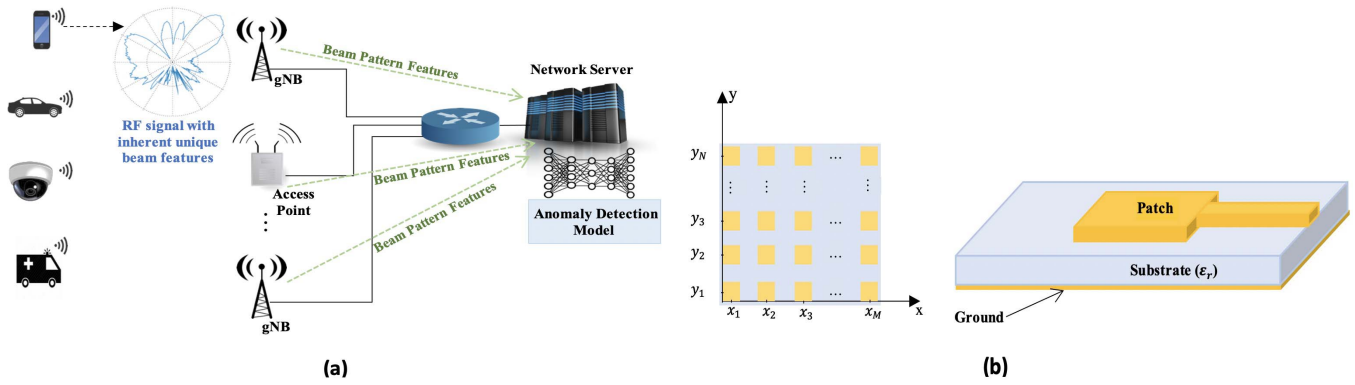

Fig. 1. (a) The proposed system architecture. (b) Basic geometry of an array antenna and a single antenna element.

we utilize the anomaly detection capabilities of DAE-based models for the accurate detection of intruder devices among a larger number of legitimate devices (100 devices).

Moreover, in [24], to prevent signal replay attacks, the authors have proposed a multiple gNB/AP architecture that uses the spatial features of beam patterns to address replay attacks. In the proposed solution, the deployment position of gNBs/APs is critical because the beam features obtained by them will be very similar if they are placed too close to each other (i.e., no additional knowledge is obtained) [24]. However, in our work, the security solution proposed in Section 4.3 works in scenarios with a single gNB/AP as well.

Motivated by this, we propose a DAE–based anomaly detection model that does not suffer from the scalability issue. This is because using a DAE–based model, we solve the attack detection problem in the form of a binary classification problem (i.e., legitimate or spoofer). Thus, increasing the number of IoT devices does not change the required output classes of the learning model. Furthermore, our approach addresses the device mobility issue by performing the learning (training) phase at different locations of the IoT devices such that the beam features are extracted from different orientation angles.

III. The Proposed Security Mechanism

In this section we present the proposed data provenance approach for the detection of wireless spoofing attacks in NGIoT networks. We first describe the system model and discuss the uniqueness of beam pattern features for every device. Then, we explain the feature extraction process and present the proposed DAE–based learning model for anomaly detection.

A. System Model

We consider a 5G–based IoT network with mmWave–enabled IoT devices (see Fig. 1–a). Each IoT device is equipped with a uniform rectangular planar array (URPA) antenna. The number of antenna elements along the x and y directions are M and N, respectively (Fig. 1–b). The feature extraction process is done at the gNB/AP which has established a direct wireless communication link to the IoT device based on either 5G–NR or IEEE 802.11ad protocols. This process is performed during the beam searching phase that is a built–in procedure of the mentioned protocols. We assume the network gNBs/APs are trusted entities that have been connected to a network server (through secure connections) that is responsible for developing and running the learning-based anomaly detection model. Thus, any wireless spoofing attack in the network is detected by the network server.

The proposed mechanism consists of a learning phase which is a one–time procedure and is performed when IoT devices are enrolled into the network. In this phase, the beam pattern features of each individual IoT device are extracted by the network gNBs/APs and sent to the network server where a dataset of the received features is created which is used to train the learning–based anomaly detection model. In case of mobile IoT devices, we assume the learning phase is performed at different locations of the IoT devices such that the beam features are extracted from different orientation angles.

After the learning phase is completed, (during the normal data transmission phase) the trained model at the network server applies the beam features (extracted from the RF signals of IoT devices) to the anomaly detection model to ensure data provenance in the network. If a feature vector is extracted from a signal transmitted by an illegitimate device, the learning model will detect it as an anomaly (since it has not learned it before).

B. Beam Pattern Features

In this subsection, we discuss the uniqueness of beam pattern features for each mmWave–enabled IoT device. Considering the URPA antenna array discussed in the previous subsection (which is the most common type of array antenna used in mmWave applications), the antenna beam pattern of the array antenna is represented by

$$AP(\theta, \phi) = EP(\theta, \phi).AF(\theta, \phi) \quad (1)$$

where $EP(.)$ is the element pattern which represents the radiation pattern of a single element. $EP(.)$ is considered equal for all the elements of the antenna if the array size is large [35], [36]. θ and ϕ are the azimuth and elevation angles, respectively. $AF(.)$ is the array factor that is obtained

by applying the complex weight parameters $w_{mn} = \alpha_{mn} e^{j\beta_{mn}}$ (antenna elements excitation) to the following steering vector $S(\theta, \phi)$:

$$S(\theta, \phi) = S_x^T(\theta, \phi).S_y(\theta, \phi), \tag{2}$$

The steering vector is used to perform beam steering which is done to dynamically change the direction of the main lobe of a radiation pattern in real time without making any change in the antenna elements. In (2), $S_x(.)$ and $S_y(.)$ are the steering vectors on the x and y directions, respectively, that are given by the following equations [36]:

$$\begin{aligned} S_x(\theta, \phi) = [1 \; & e^{j\frac{2\pi}{\lambda}x_1 sin(\theta)cos(\phi)} \; e^{j\frac{2\pi}{\lambda}x_2 sin(\theta)cos(\phi)} \; \dots \\ & \dots \; e^{j\frac{2\pi}{\lambda}x_M sin(\theta)cos(\phi)}]^T, \\ S_y(\theta, \phi) = [1 \; & e^{j\frac{2\pi}{\lambda}y_1 sin(\theta)sin(\phi)} \; e^{j\frac{2\pi}{\lambda}y_2 sin(\theta)sin(\phi)} \; \dots \\ & \dots \; e^{j\frac{2\pi}{\lambda}y_N sin(\theta)sin(\phi)}]^T \end{aligned}$$

In these equations, λ is the carrier wavelength and (x_m, y_n) is the coordinates of the antenna elements, for $m = 1, 2, \dots, M$ and $n = 1, 2, \dots, N$ (see Fig. 1–b). After applying the excitation weights w_{mn} on (2), the array factor $AF(.)$ is obtained as:

$$AF(\theta, \phi) = \sum_{m=1}^{M} \sum_{n=1}^{N} \alpha_{mn} e^{j\beta_{mn}} e^{j\frac{2\pi}{\lambda} sin(\theta)(x_m cos(\phi) + y_n sin(\phi))}$$

Assuming $x_{m+1} - x_m = d_x \; \forall m \in \{1, 2, \dots, M-1\}$ and $y_{n+1} - y_n = d_y \; \forall n \in \{1, 2, \dots, N-1\}$, we have

$$AF(\theta, \phi) = \sum_{m=1}^{M} \sum_{n=1}^{N} \alpha_{mn} e^{j\beta_{mn}} e^{j\frac{2\pi}{\lambda} sin(\theta)(md_x cos(\phi) + nd_y sin(\phi))} \tag{3}$$

From equations (1) and (3), it is concluded that the array factor (and the beam pattern of the array antenna, consequently) depends on a number of device dependant parameters. Firstly, the non–ideality of the phase shifter units used to generate β_{mn} creates unique excitation phase shifts in each device. In fact, low resolution phase shifters that are typically deployed to generate the phase shifts make the generated β_{mn} phase shifts unique for every device [24]. For example, the passive 3–bit phase shifter proposed in [37] results in a phase error of 10.4° at 57–67 GHz. This indeed creates a unique RF signature for every mmWave–enabled device considering a large number of antenna elements (M and N).

Secondly, the beam pattern is a function of the dimensional parameters that are implemented through non-ideal fabrication processes during the manufacturing. Specifically, $EP(.)$ is a function of the width and length of the element's patch as well as the thickness of the substrate [24], [38]. For example, the resonance frequency of the antenna patch is represented by

$$f_c = \frac{C}{2L_e(L, W, h)\sqrt{\epsilon_e(\epsilon_r, W, h)}}, \tag{4}$$

where C is the speed of light in vacuum. L_e and ϵ_e are effective length and effective dielectric parameter that are a function of dimensional parameters of the antenna elements (L and W are length and width of the patch, respectively, and $h \ll \lambda$ is thickness of the substrate) [39], [40]. In particular, with the higher frequencies (smaller wavelengths) used in mmWave circuits, the dimensional parameters of the antenna array need to be smaller (e.g., the dimensions of patch, substrate, and microstrip line). Thus, the fabrication of antenna arrays should be performed using extremely accurate instruments and procedures which is very expensive. Thus, the variations in dimensional parameters result in final antenna arrays with unique dimensional features. Note that these variations do not degrade performance of the Tx module since they are effectively compensated at the receiver circuit (Rx) (see [24] for more detail).

The third source of beam feature uniqueness in mmWave array antennas is the relative permittivity (ϵ_r) of the substrate material used in each antenna element. As Fig 1–b shows, the basic geometry of an antenna element consists of a substrate material that supports the metallic patch over a ground plane. The main function of the substrate is to concentrate the electromagnetic fields beneath the patch [38]. According to Equation (4), the relative permittivity (ϵ_r) of the substrate material is an important parameter with a significant impact on the resonance frequency. Thus, the unwanted and unavoidable variations in ϵ_r of the substrate material used in the antenna fabrication process acts as a sources of beam feature uniqueness. In [24], LTCC Ferro A6–S [41] has been deployed in the experiments which is a popular substrate used for mmWave antenna. This substrate has a relative permittivity of 5.9 with 7% error which results in the final ϵ_r of 5.9 ± 0.2 [41].

Therefore, the discussed variations in the parameters of antenna arrays created during the fabrication process generate unique device dependent beam pattern features that can be recognized using a learning–based model to identify illegitimate wireless IoT devices that attempt to perform a wireless spoofing attack. Fortunately, unlike most of the RF modulation features deployed in the current RF fingerprint mechanisms, the discussed antenna array features do not change over time (e.g., by a change in power supply voltage). This provides a high level of stability for our proposed security approach.

C. Feature Extraction

In this subsection, we discuss the extraction of beam features from the mmWave signals received by the network gNBs/APs. In this regard, we focus on the of 5G–NR and show that the beam features can be measured based on the Sounding Reference Signals (SRSs) that are transmitted by mmWave–enabled mobile devices during the beam management procedure defined in the 5G–NR standard protocol. For IEEE 802.11ad, the measurement of beam features has been discussed in [24].

1) Beam Searching: Unlike the conventional cellular technologies, in 5G–NR, the network base stations (called gNBs in 5G) are equipped with large–scale antenna arrays to cover each of the three 120° sectors. In fact, the beam–based cell sector coverage is deployed to increase bandwidth efficiency, system capacity, and throughput [42]. In other words, every mobile device connects to a gNB through a single beam only that is determined through a set of beam management phases. Note that these different beams can be transmitted at the same time using the same frequency. This creates a significant increase in

the system capacity and throughput. In the following, we first provide a brief explanation of the beam management phases in 5G–NR. Then, we show how the beam features can be measured based on the standard SRS signals.

2) Beam Management: In 5G–NR, a set of beam management operations are performed to effectively provide both initial access (for idle mobile devices) and beam tracking procedures (for already connected mobile devices). Unlike LTE, in 5G–NR, the signalling (control) procedures are performed using the beam–based approach. In LTE, these procedures are carried out using omnidirectional signals, i.e., the (small scale) beamforming and directional transmissions are provided for data plane transmissions only [43]. The 5G–NR beam management framework consists of four different operations [42], [44]:

A) *Beam sweeping* which is a technique for sequential transmission of a set of beams such that they cover (sweep) a spatial area. These beams called Synchronization Signal Blocks (SSBs) and are formed/steered using the predefined direction codebooks (identified by specific beamforming vectors) that cover the whole space in both azimuth and elevation directions.

B) *Beam measurement* that is performed to evaluate quality of the received signal at the gNB or mobile devices (for uplink and downlink communications). For the initial access procedure (when a mobile device is in the idle mode), the mmWave–based measurement is done by the mobile device based on the received SSB bursts (In 5G–NR, uplink signals are not used for initial access [42]). However, in the beam tracking procedure, the operation of beam measurement is different for uplink and downlink paths. In the downlink path, the beam measurement is done by the mobile device based on the received synchronization and reference signals (SSB blocks and CSI–RSs) transmitted by the gNB. The CSI–RSs (Channel State Information Reference Signal) are reference signals that are used in the beam tracking phase only (for the connected devices). In the uplink path, the measurements are done by the gNB based on the SRSs transmitted by the mobile device. In our proposed security mechanism, the beam feature can be measured by gNBs using the received SRS beams.

C) *Beam determination* is the selection of the beam with the highest quality based on the measurements done in the previous step. It is done by either the gNBs or by the mobile device to determine the best uplink and downlink beams, respectively. The determined beams are used for the subsequent transmissions until another beam with higher quality is detected (this may happen due to device movements and changes of channel conditions).

D) *Beam reporting* which is used by the mobile device to send beam quality information to the network.

The periodic repetition of the above–mentioned operations enables the mobile devices and gNBs to collaboratively choose/update the best transmitter and receiver beam pairs over the lifetime of their communication.

3) Measurement of Beam Features: As explained in the previous subsection, beam measurement is an important built–in operation of the standard 5G–NR beam management procedure. We take advantage of this operation to generate the beam features required in both training and anomaly detection phases of the proposed security mechanism. In this regard, the antenna pattern $AP_j(\theta, \phi)$ for the jth received beam ($j = 1, 2, \ldots, J$) which is measured by the gNB during the periodic beam management procedure is labelled with the ID of the associated device and sent to the network server through the secure backhaul link. As we discussed in the previous subsection, the measurement of $AP_j(\theta, \phi)$ is carried out by the gNB based on the received uplink SRS beams. Note that the measurement of beam features should be performed during the beam tracking phase. This is because in 5G–NR, no uplink beam is used during the initial access phase (it is the gNB that starts the beam sweeping procedure). In fact, for the sake of simplicity and to take advantage of the standard functionality of 5G–NR beam management, our security mechanism ignores the initial access phase and starts to work (measuring the beam features of the mobile devices) once their connection with the gNB is established (the initial access phase is completed). However, this has no negative effect on the performance of the proposed security mechanism since no sensitive data is transferred during the initial access phase. In other words, if an illegitimate device can successfully initiate a connection with the gNB, it will be immediately recognized as a illegitimate device once it sends the SRS beams.

Thus, considering a specific mobile device, the network server receives a set of J different beam features measured from J consecutive beams transmitted by the device, i.e., $BF = [AP_1(\theta_1, \phi_1), AP_2(\theta_2, \phi_2), \ldots, AP_J(\theta_J, \phi_J)]^T$. As you see, the size of the feature vector BF can be increased by selecting a large J, i.e., by increasing the number of device's consecutive beams that are used for feature measurement. This improves the accuracy of the DAE learning model used for the detection of anomalies. Moreover, each feature measurement is a function of the azimuth and elevation angles (i.e., θ_j and ϕ_j). If the device is considered to be stationary, the azimuth and elevation angles do not change at different beam transmissions. Thus, we have $\theta_1 = \theta_2 = \ldots = \theta_J$ and $\phi_1 = \phi_2 = \ldots = \phi_J$ in the vector of beam features. In this case, assuming the DAE–based anomaly detection model has been trained using the beam features obtained at the same angles, the model can effectively recognize the feature vector as either normal or anomaly. However, for mobile devices, the angles may change at each beam transmission. In this case, the collected feature vector may have too much distance from the vectors used in the training of the DAE model. This would result in the degradation of the DAE's detection accuracy. To address this issue, the training dataset should be created based on the beam features measured at different azimuth and elevation angles. This has a significant impact on the performance of the proposed security approach because if the dataset misses the feature vectors collected at specific angles, it may later ruin the effect of beam feature uniqueness that is the foundation of this approach. Therefore, having a comprehensive and large training dataset is critical for the DAE model to provide the maximum attack detection accuracy in mobile scenarios. This can be achieved by defining specific procedures for beam feature collection at

different spatial positions when mobile devices enrol into the network.

Note that according to equation (3), the beam features are a function of frequency (or wavelength, equivalently). Thus, any changes in frequency may result in new beam features that are different than the features learned by the DAE anomaly detection model. However, this does not create an issue for the proposed scheme because mmWave communication systems work in Time Division Duplexing (TDD) mode [43]. This is because firstly, they use MaMIMO technology to increase the communication speed and capacity. To perform MaMIMO operation, the status of downlink channel should be estimated using the state information of uplink channel. This can be done only when the uplink and downlink channels are reciprocal which is occurred in TDD mode only [45]. Secondly, the spectrum available for mmWave communication is unpaired which allows the communication in TDD mode only [43]. Working in TDD mode enables the mmWave communications of different devices to be occurred at the same frequency. Therefore, considering a gNB/AP that works at a specific frequency band, the beam features of devices do not change during the communications. However, if the gNB/AP supports multiple frequency bands, the beam features of legitimate devices must be learned by the DAE model at each frequency band separately. This allows the DAE model to recognize the legitimate devices in case of any change in frequency.

4) Anomaly Detection Model: In this subsection, we present the DAE–based learning model used for the detection of feature anomalies. During the one–time training phase, the DAE model is trained to learn the unique beam features of the legitimate IoT devices in the network. Then, the model is able to find out that the received beam features are associated with either a legitimate IoT device or an intruder.

Regardless of the proven effectiveness of DAE-based models in performing anomaly detection tasks, deploying a DAE model makes our security solution scalable. This is indeed an important characteristic since the proposed solution attempts to secure the large scale NGIoT networks. In fact, in the proposed approach, the attack detection problem is solved in the form of a binary classification problem instead of a multiclass classification problem that its accuracy heavily depends on the number of devices (classes). However, the current (learning–based) RF fingerprinting solutions take advantage of machine/deep learning models to solve a multiclass classification problem. This reduces their accuracy in networks with a large number of IoT devices. For example, the results presented in [24] have been obtained in a network with 12 IoT devices which are not guaranteed to be the same when the solution is deployed in a large scale IoT network. Thus, scalability is a critical issue in RF fingerprinting mechanisms that indeed needs further investigation. Moreover, to train a DAE model, (unlike the conventional machine learning model) the training dataset does not need to include any data of the illegitimate devices. In other words, the DAE model just learns the legitimate data and then can effectively recognize any illegitimate data pattern at its inputs. In the following we explain the architecture of a DAE model to make these characteristic more evident.

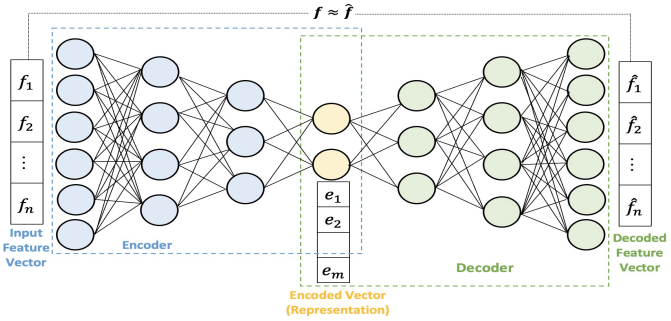

Fig. 2. Architecture of the deep autoencoder model.

DAEs are a type of Artificial Neural Networks (ANN) that have proven abilities and effectiveness in performing anomaly detection tasks using an unsupervised manner. The main idea of DAE models is that they deploy a network of neurons and train it in such a way that it removes noise from the input training data vectors. In fact, during the training of the model, the weight and bias parameters of the neurons are computed in such a way that a reconstructed version of every input vector is obtained at the output in which noise has been removed (see Fig. 2). This enables DAEs to identify the original (normal) data vectors even if they have been contaminated by different sets of random noise values. To do this, a DAE uses two networks of neurons that are called encoder and decoder. The encoder network performs the dimensionality reduction process while the decoder network is used to reconstruct the input vector from the encoded vector. During the DAE training, the weights and bias parameters are repeatedly updated such that the dissimilarity (error) between the reconstructed and input vectors is minimized, i.e., a DAE learns the optimum values for the weights and biases of neurons that result in the maximum similarity between the input and reconstructed vectors. The number of neurons at the output layer is always equal to the number of neurons at the input layer. This is because the reconstructed and input vectors should have the same dimensionality. In the following, we present the mathematical model of the DAE–based anomaly detection model.

Assume $\mathbf{F} \in \boldsymbol{\Psi}$ is the set of training vectors $\mathbf{f}^i = \{f_1, f_2, \ldots, f_n\}$ where $\boldsymbol{\Psi}$ is an n–dimensional feature spaces. If $g_\alpha : \mathcal{R}^n \rightarrow \mathcal{R}^m$ and $g'_\beta : \mathcal{R}^m \rightarrow \mathcal{R}^n$ are the encoding and decoding functions, respectively, we have

$$\mathbf{e}^i = g_\alpha(\mathbf{f}^i)$$
$$\hat{\mathbf{f}}^i = g'_\beta(\mathbf{e}^i) = g'_\beta \circ g_\alpha(\mathbf{f}^i),$$

where $\mathbf{e}^i = \{e_1, e_2, \ldots, e_m\}$ and $\hat{\mathbf{f}}^i = \{\hat{f}_1, \hat{f}_2, \ldots, \hat{f}_n\}$ are the representation (encoded) and reconstructed (decoded) vectors, respectively, associated with the input vector $\mathbf{f}^i$. Note that $\mathbf{E} \in \boldsymbol{\theta}$ shows the set of encoded vectors where $\boldsymbol{\theta}$ is an m–dimensional feature spaces ($m < n$). $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are parameters of the encoder and decoder functions, respectively.

Now, assume there is an unknown probability distribution ρ defined over $\boldsymbol{\Psi}$. Given Δ as a dissimilarity (error) function (such as Mean–Absolute Error (MAE), Mean–Squared Error

(MSE), Euclidean Distance, etc.), the relevant *autoencoder problem* is to find $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ such that the expected value of the dissimilarity function Δ is minimized, i.e.

$$\min_{(\boldsymbol{\alpha},\boldsymbol{\beta})} Exp_{(\mathbf{f}^i,\hat{\mathbf{f}}^i)\sim\rho}(\Delta(\mathbf{f}^i,\hat{\mathbf{f}}^i)) = \min_{(\boldsymbol{\alpha},\boldsymbol{\beta})} Exp(\Delta(\mathbf{f}_i, g'_\theta \circ g_\psi(\mathbf{f}_i)))$$

Because the probability distribution ρ is unknown, it is not feasible to obtain the expected value of the dissimilarity function. Thus, we limit the autoencoder problem to the space of the training vectors, i.e.

$$\min_{(\boldsymbol{\alpha},\boldsymbol{\beta})} \Delta(\mathbf{f}^i,\hat{\mathbf{f}}^i) = \min_{(\boldsymbol{\alpha},\boldsymbol{\beta})} \sum_{j=1}^{n} \Delta(f_j, g'_\theta \circ g_\psi(f_j))$$

The above autoencoder problem is solved for every $\mathbf{f}^i$ and $\hat{\mathbf{f}}^i$ in $\mathbf{F}$ and $\hat{\mathbf{F}}$ (respectively), i.e., all the vectors in the training dataset are learnt. Different types of autoencoders can be derived from this general model depending on the choice of functions f_α, f'_β, and the dissimilarity function Δ. Moreover, applying additional constraints such as regularization can change the type of autoencoder. For example, if MSE is selected as the dissimilarity function, for the autoencoder problem we have

$$\min_{(\boldsymbol{\alpha},\boldsymbol{\beta})} \frac{1}{n}\sum_{j=1}^{n}(f_j - \hat{f}^j)^2 = \min_{(\boldsymbol{\alpha},\boldsymbol{\beta})} \frac{1}{n}\sum_{j=1}^{n}(f_j - g'_\theta \circ g_\psi(f_j))^2$$

To solve the above autoencoder problem, gradient–based optimization approach is a popular and effective method to choose. There exists several versions of gradient–based optimization algorithms. For example, in Batch Gradient Descent (BGD), the gradients of all samples are calculated at first. Then, based on the obtained gradients, the neural network parameters are updated. However, it is used in offline training applications in which the whole set of the training dataset is available. However, in online (real–time) applications, training samples may become available after the model is employed. On the other hand, Stochastic Gradient Descent (SGD) can be used in online training applications. Each time, it updates the parameters using an instant training sample [34], [35]. In other words, in BGD, all the training samples must be learnt before a single update is done on the network parameters. However, in SGD, one or a subset of the training samples can be learnt in order to update the network parameters. This makes SGD an efficient optimization algorithm. Specifically, in high–dimensional optimization problems, SGD performs very efficient in terms of speed and computational overhead.

Since we build the autoencoder for an online (real–time) application with a huge number of data points, we solve the autoencoder problem using the SGD approach. Therefore, we have

$$\boldsymbol{\alpha}^{(k+1)} = \boldsymbol{\alpha}^{(k)} - \epsilon^{(k)}\nabla_{\boldsymbol{\alpha}}\Delta_i(\boldsymbol{\alpha}^{(k)})$$
$$\boldsymbol{\beta}^{(k+1)} = \boldsymbol{\beta}^{(k)} - \epsilon^{(k)}\nabla_{\boldsymbol{\beta}}\Delta_i(\boldsymbol{\beta}^{(k)})$$

where $\nabla_{\boldsymbol{\alpha}}\Delta_i(\boldsymbol{\alpha}^{(k)})$ and $\nabla_{\boldsymbol{\beta}}\Delta_i(\boldsymbol{\beta}^{(k)})$ are the gradients taken using $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, respectively (considering a training sample $\mathbf{f}^i$). ϵ is the learning rate that is used to adjust the speed of convergence. It determines the size of steps that are taken to reach the optimum parameters. Using larger values for ϵ results in faster training but at the risk of missing the optimum values (loss in accuracy). On the other hand, a smaller ϵ makes the convergence of algorithm slower. When the optimization problem is solved, parameters $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are obtained. This means that the autoencoder model has been built and vectors $\hat{\mathbf{f}}^i = g'_\theta \circ g_\psi(\mathbf{f}_j)$ can be obtained as the reconstructed vectors.

Algorithm 1 The Detection Mechanism

Inputs: $\mathbf{x}_i$ (The RF signal claiming to be from the ith legitimate IoT device)
d_i (address of the ith legitimate IoT device)
J (number of features)
e_{thr} (error threshold)
Output: $R \in$ {"*Authorized Access*", "*Spoofing Device Detected*"}
1: $\mathbf{f}(\mathbf{x}_i, t) = Beam\ Measurement(\mathbf{x}_i)$
2: $\hat{\mathbf{f}}^j = DAE(\mathbf{f}(\mathbf{x}_i, t))$
3: $error = \Delta(\mathbf{f}(\mathbf{x}_i, t), \hat{\mathbf{f}}^j) = \frac{1}{n}\sum_{j=1}^{n}(f_j(\mathbf{x}_i, t) - \hat{f}_j^i)^2$
4: **if** $error \leq e_{thr}$:
return "*Authorized Access*"
else:
return "*Spoofing Device Detected*"

D. Complexity Analysis

In this subsection, we analyze the computational complexity of the proposed anomaly detection model. We firstly emphasize that the proposed scheme imposes zero computation and communication overhead to the IoT devices. This is because the scheme does not rely on the cooperation of IoT devices and their beam features (i.e., RF signature) are extracted from the RF signals transmitted for their normal communications. Instead, the main computation burden of the scheme is carried by the backend server that runs the DAE–based anomaly detection algorithm. Assume the DAE model consists of L layers where layer 1 and L are the input and output layers, respectively. Consider the DAE model as a fully connected network of neurons (see Fig. 2), i.e., the worst-case scenario in terms of computational complexity. We refer to the size of ith layer as $n^{(i)}$ ($i \in \{1, 2, \ldots, L\}$) which is the number of neurons in that layer. In this case, we have $n^{(1)} = n^{(L)} = n$, where n is the size of feature vectors. The output of ith layer is written as

$$y^{(i)} = [y_1^{(i)} \quad y_2^{(i)} \quad \ldots \quad y_{n^{(i)}}^{(i)}],$$

where, $y_j^{(i)} = g(\sum_{k=1}^{n^{(i-1)}} w_{jk}^{(i)} y_k^{(i-1)})$ in which $w_{jk}^{(i)}$ is the weight of jth neuron in layer i applied to $y_k^{(i-1)}$, and g is the activation function deployed in layer i. Therefore, the number of multiplications and additions required to compute $y^{(L)}$ (the final output of the DAE network) are obtained as follows.

At each layer i ($i \in \{2, 3, \ldots, L\}$), $n^{(i)}$ output values must be computed (i.e., $y_1^{(i)}, y_2^{(i)}, \ldots, y_{n^{(i)})}^{(i))}$). The computation of each value $y_j^{(i)}$ requires $n^{(i-1)}$ multiplications and $(n^{(i-1)} - 1)$ additions. Thus, the total number of required multiplications and additions are $N_M = \sum_{i=2}^{L} n^{(i)} n^{(i-1)}$ and $N_A = \sum_{i=2}^{L} n^{(i)}(n^{(i-1)} - 1)$, respectively.

To further simplify N_M and N_A, we assume that the encoder and decoder networks of the DAE model have the same number of layers (see Fig. 2) and the size of each layer in the encoder/decoder network is a half/double the size of the previous layer (these assumptions are usually considered in DAE implementations). In this case, for N_M, we have

$$N_M = 2[(\frac{n}{2} \times n) + (\frac{n}{4} \times \frac{n}{2}) + \ldots + (\frac{n}{2^{L/2-1}} \times \frac{n}{2^{L/2-2}})] = 2n^2 \sum_{i=1}^{L/4-1} \frac{1}{2^{2i-1}},$$

where, n is the size of feature vectors. Similarly, for N_A, we have $N_A = 2[n^2 \sum_{i=1}^{L/4-1} \frac{1}{2^{2i-1}} - n \sum_{i=1}^{L/2-1} \frac{1}{2^i}]$. For a specific DAE network, the n and L parameters are fixed. Thus, regardless of the number of IoT devices or network intruders, N_M and N_A can be accurately computed. Since n is typically a limited number (e.g., 128), N_M and N_A will be small enough to be handled by currently used servers (considering their enormous computational capabilities). For example, assume a backend server with a single Intel Core i7-8086K processor that performs 2×10^{11} instructions per second at 5.0 GHz [46]. If $n = 128$, and five instructions are required for each multiplication/addition operation (on average), the server can perform 1.2×10^6 anomaly detection computations in a second (approximately).

IV. Security Analysis

In this section, we analyze the security aspects of the proposed mechanism. We first discuss the immunity of the proposed approach against physical/hardware attacks and highlight the challenges that an attacker needs to address to bypass the proposed security mechanism in order to conduct a relay–based spoofing attack. The related attack model is also presented. Finally, we introduce a delay–based supplementary technique to make the relay–based spoofing attempts unsuccessful.

A. Attacker Challenges

Because 1) in the proposed security mechanism, IoT devices do not require to store any encryption key in their memory, and 2) it is infeasible to forge device–dependant beam features, the proposed security mechanism is resilient against physical/hardware attacks such as invasive, semi–invasive or side–channel attacks [47]. In other words, an attacker receives no benefit from physical access to a sample IoT device and investigation of its hardware. However, it might be vulnerable to relay–based spoofing attacks in which the attacker intercepts the signal transmitted by a wireless device (via eavesdropping on its communications in the network) and then relays the signal (usually with some delay) to the intended destination to impersonate the device [16], [47]. Due to the unique 5G characteristics and the special properties of beam features, there are several challenges that make a relay–based spoofing attempt very challenging for the attacker. In this regard, we identified the following critical challenges that the attacker needs to address them before conducting such an attack.

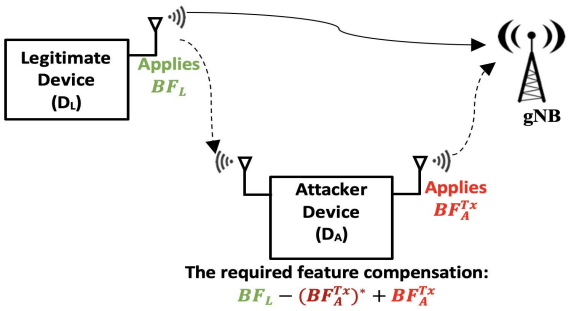

Fig. 3. A sample replay attack scenario. Each antenna applies its own signature into the signal during the transmission. The attacker device must perform some expensive compensation operations on the relayed signal in order to remove the effect of its own signature on the original beam features.

Challenge 1: In 5G–NR, massive MIMO technology is used to beamform RF signals to different directions (devices). It has been shown that deploying MaMIMO makes the 5G–NR robust against passive eavesdropping attempts [45]. The reason is that beamforming a signal towards a (legitimate) destination device makes the signal to noise ratio (SNR) at the legitimate device several orders of magnitude larger than SNR at the eavesdropper. To address this challenge, the attacker device needs to be physically placed very close to the legitimate device such that the communication channels to the device and the eavesdropper are highly correlated [45].

Challenge 2: When an attacker device relays a legitimate signal towards a gNB, it automatically (undeliberately) introduces its own antenna array signature into the relayed signal. This makes the beam features of the relayed signal different than the features that the DAE-based anomaly detection model has learned during the training phase. To address this challenge, the attacker needs to carefully design and use an array antenna such that in the final relayed signal, the signature of the attacker device is compensated (see Fig. 3). However, such designs and implementations need extensive knowledge and effort which makes the attack very expensive. Moreover, the designed hardware can be deployed to impersonate a single IoT device only. This prevents the attacker to conduct a large–scale attack.

Challenge 3: In IoT networks with stationary devices, the anomaly detection model has learned the beam features of the legitimate devices based on specific azimuth and elevation angles. Thus, if the attacker device is not placed on the direct communication path between the legitimate device and the gNB, the beam features of its relayed signal will be different that the beam features that the gNB has already measured (and learned). This enables the model to recognize the relayed signal as a spoofing attack. This is because according to equations (1) and (3), in addition to the device–dependency property, the measured beam features depend on the azimuth and elevation angles associated with the communication path between the transmitter and receiver antennas. In other words, the gNB has measured (and learned) $BF_{leg} = [AP^1_{leg}(\theta^1_{leg}, \phi^1_{leg}), AP^2_{leg}(\theta^2_{leg}, \phi^2_{leg}), \ldots, AP^J_{leg}(\theta^J_{leg}, \phi^J_{leg})]^T$ during the training phase while it measures $BF_{att} = [AP^1_{att}(\theta^1_{att}, \phi^1_{att}), AP^2_{att}(\theta^2_{leg}, \phi^2_{att}), \ldots, AP^J_{att}(\theta^J_{leg}, \phi^J_{att})]^T$ from the relayed

signal, where $(\theta_{leg}^{j}, \phi_{leg}^{j}) \neq (\theta_{att}^{j}, \phi_{leg}^{j})$ for $j = 1, 2, \ldots, J$. To overcome this challenge, the attacker device has to be placed on the direct communication path between the legitimate device and the gNB such that both the attacker device and the gNB experience the same azimuth and vertical angles.

Therefore, the security properties of our proposed mechanism combined with the unique characteristics of the massive MIMO technology create the above–mentioned challenges for the attacker. However, in this paper, we assume a powerful attacker who is able to address these challenges and proceed with the attack. In this regard, we propose a delay–based supplementary technique to fully address the issue. Before we explain this solution, we present the attack model in the next subsection.

B. Attack Model

The target of the attacker device D_A is to gain access to the network by taking advantage of the authentication signals transmitted by a legitimate device D_L. To do this, D_A attempts to intercept and relay D_L signals that are sent during the network authentication procedure. We assume our proposed security mechanism is used by the network to ensure the provenance of the authentication messages received from wireless devices. Regarding the network architecture, we consider all the assumptions that we made in Section III.A. In addition, we assume that the network server authenticates the devices in the network. It is supposed that the server does not respond to duplicate authentication requests (that belong to the same device ID) and accepts only the first requests.

We assume D_A has been equipped with a mmWave–enabled transceiver and has the knowledge of communication channel between D_L and the gNB. Moreover, D_A can be placed in a position close enough to D_L such that it can effectively eavesdrop its communications. This position is assumed to be on the communication path between D_L and the gNB, thus, the discussed azimuth and elevation angles do not change during the signal relay. We assume the DAE–based model has been trained with the beam features of D_L and other legitimate devices. Thus, it effectively distinguishes the legitimate beam features from illegitimates.

C. Delay–Based Supplementary Technique

To fully address the relay–based attacks, we propose a delay—based technique using which the network service schedules the transmission of authentication responses to the network IoT devices who have submitted a network access request. This is done in such a way that the signal relay attempts made by D_A become ineffective and are not considered by the network.

To better explain this, assume D_A (that is eavesdropping on the communications of D_L) is able to successfully identify the Authentication Request ($AReq$) messages of D_L. To start conducting the attack, D_A submits its own $AReq$ message immediately after it detects D_L's $AReq$ message (with the minimum time gap between the two authentication procedures). Note that D_A has to submit its request with an ID different than D_L's ID. This is because the server does not respond to duplicate authentication requests. Assume the D_L and D_A's requests are the only unhandled $AReq$ messages in the network. The network server then replies to D_L by sending the Authentication Response ($ARes$) message to it which includes a random number r_1. In fact, it asks D_L to send r_1 back to the network. At the same time, it starts a timer initialized with a short and predefined period of time τ. However, when the network server receives the $AReq$ message of D_A, it does not send an $ARes$ message to it until the timer is up. Upon receiving the $ARes$ message, D_L transmits a reply signal (with r_1 in it) which is processed by the gNB to extract its beam features. This signal is targeted by D_A to be intercepted and relayed to the gNB. However, D_A has not received any $ARes$ message from the network yet, thus, it can not relay the signal immediately. In other words, the eavesdropped signal must be delayed by D_A until the relevant $ARes$ message is received which includes the random number r_2. This is an infeasible task for D_A to perform if τ is large enough (e.g., >1 msec). In fact, creating delay in the transmission of a radio signal without making changes on the signal features is infeasible. The current passive delay line solutions work mostly based on either coaxial/optical fibre cables [48] or electro–acoustic devices [49], [50]. However, when delays in the millisecond (or larger) ranges are required, these solutions are impractical. For example, considering the speed of light in a coaxial/optical fibre cable, 200 metres of the cable is required to delay the signal by 1 microsecond.

Therefore, the selection of τ in the millisecond range prevents the attacker to deploy the required delay line. On the other hand, adopting a large τ may negatively affect the performance of the IoT application. In this regard, if we consider $\tau = 1$ msec, the server will be able to authenticate 1000 devices per second (regardless of other delays caused by signal propagation, processing, software running, etc.). Moreover, in this case, the created delay is smaller than the latency requirements of most of the latency critical IoT applications [51].

V. Performance Evaluation

In this section, we present the results of our experiments and discuss the feasibility of the proposed security mechanism. We first explain the setups of our experiments and discuss the method used to create the dataset of device features for the training of the DAE module. Then, we present the results of our experiments.

A. Experimental Setup

To perform our experiments, we used 5G Toolbox, Antenna Array Designer App, and Phased Array System Toolbox of MATLAB [52] to generate and customize mmWave waveforms to use as training data. The 5G Toolbox provides standard–compliant functions for the modelling and verification of the 5G communications systems that work based on 3GPP 5G–NR Release 15 [53]. In this toolbox, we used several components from the Phased Array System Toolbox to perform beamforming functions on the generated waveforms. In addition, we used the Antenna Array Designer App for the

TABLE I
PARAMETERS OF THE EXPERIMENTS

Parameter	Value
Frequency range	FR2–n257 (26.5–29.5 GHz)
Center Frequency	28 GHz
Synchronization signal block (SSB) pattern	Case D (for FR2)
Tx array size	6 x 6
Tx azimuthal sweep limits	[-60, 60]
Tx elevation sweep limits	[0, 90]
Rx array size	32 x 32
Rx azimuthal sweep limits	[-180, 180]
Rx elevation sweep limits	[-90, 0]
SNR	10, 20, 30 dB

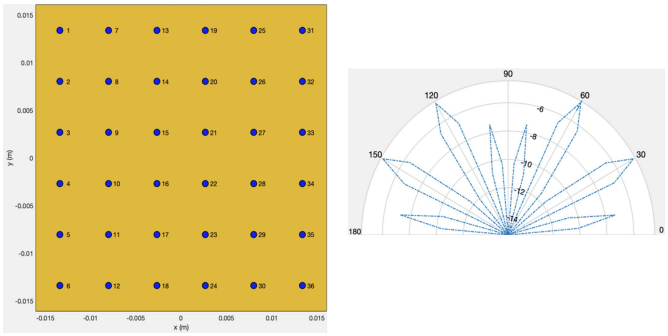

Fig. 4. The geometry and pattern of the 32 × 32 array antenna used in the experiments.

custom design of antenna arrays (see Fig. 4). We used the Additive White Gaussian Noise model (AWGN) for the communication channel between IoT devices and the gNB. The AWGN model is widely used in wireless channel modelling to imitate the effect of background noise added to the signal in the communication channel. We changed the signal to noise ratio (SNR) from 10 dB to 30 dB to consider the effect of channel situation in our dataset. In fact, changing the SNR parameter enables the DAE model to learn the beam features under different channel circumstances. Finally, a complete 5G–NR transceiver was implemented in which the receiver extracts beam features of the received signal using the standard beam measurement function defined in 3GPP 5G–NR Release 15 [53]. This enabled us to create a dataset of the beam features of 100 mmWave enabled devices. For every device, we slightly changed the antenna array parameters to model the non-ideality of antenna arrays. Furthermore, we created a vector of device locations which included 10 different locations and used it in the dataset generation process. Table I summarizes the parameters used in our experiments.

In the second part of the experiments, we used the obtained dataset to develop a DAE model in TensorFlow 2.0 and keras libraries of Python. We used 70% of the dataset for the training of the DAE model and the rest were used for the validation and test procedures (10% and 20%, respectively). We performed the experiments by changing parameters such as number of hidden layers, activation function, and number of epochs to see the effect on the detection accuracy.

B. Results

We performed the experiments by increasing the number of devices from 20 to 100 (with the step of 20) to evaluate the scalability property of the proposed detection mechanism. We noticed that the detection accuracy does not experience any notable degradation when the number of devices increases. This is indeed a significant advantage of the proposed mechanism that is a result of deploying a DAE–based detection model. In the RF fingerprinting mechanisms that work based on traditional supervised machine learning models (e.g., SVM), the classification accuracy can be considerably degraded when the number of devices increases. This is because in such cases, (intuitively) the feature vectors of distinct devices become closer to each other in high dimensional classification scenarios.

We repeated the experiments using three different SNR values. To do this, we generated three different training datasets, each one obtained based on a specific SNR. Moreover, changing the location of mobiles devices in each iteration automatically applies the effect of a range of SNRs on each dataset. We noticed that the detection accuracy improves when a higher level of SNR is applied on the wireless channel (see Fig. 5–a). In fact, at a higher SNR, the resolution of the extracted features increases during the beam measurement operation since the signal is less distorted in a less noisy channel than a very noisy channel which. This makes the feature vectors more identifiable by the DAE module. However, at SNRs greater than 20 dB we did not notice any significant improvement in the detection accuracy. Fig. 5–b illustrates the detection accuracy when SNR of the illegitimate device changes from 10 to 40 dB. As the figure shows, the system offers more accurate performance if the training phase is carried out at a higher level of SNR. In fact, in such cases, the spoofer device must increase the transmission power to the level at which the DAE model has learned the beam features of the legitimate devices. However, going beyond that level does not result in any considerable benefit for the spoofer device.

We also changed the number of locations at which the beam features of the legitimate devices were extracted during the training phase. We started from 2 training locations that resulted in poor detection performance (see Fig. 5–c). As we discussed in Section III, to offer the best performance, the DAE model must learn the beam features from different locations and orientation angles. We observed significant improvement in the detection accuracy when we used the training datasets obtained using 5 and 10 training locations. Thus, it is critical to employ a special training mechanism to measure the beam features at different locations during the enrolment of devices.

We implemented the DAE-based anomaly detection model using three different activation functions, i.e., *Sigmoid*, *Tanh*, and *ReLu*. The best results were obtained using the *Tanh* activation function (see Fig. 6–a). Moreover, we performed the experiments using three different numbers of the hidden layers. As we expected, increasing the number of hidden layers results in improvement of the detection accuracy (see Fig. 6–b). Indeed, every additional layer enables the model to obtain a deeper level of knowledge about the training data. However, having more hidden layers in the model results in longer training times. As Fig.6–b shows, there is no considerable increase in the detection accuracy when the number of hidden

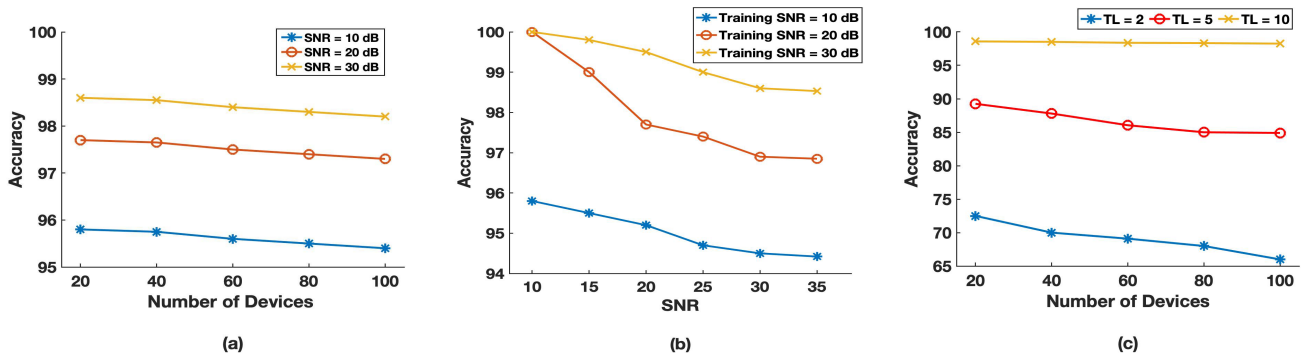

Fig. 5. (a) and (b) The effect of SNR on the detection accuracy.(c) Increasing the number of training locations improves the detection accuracy.

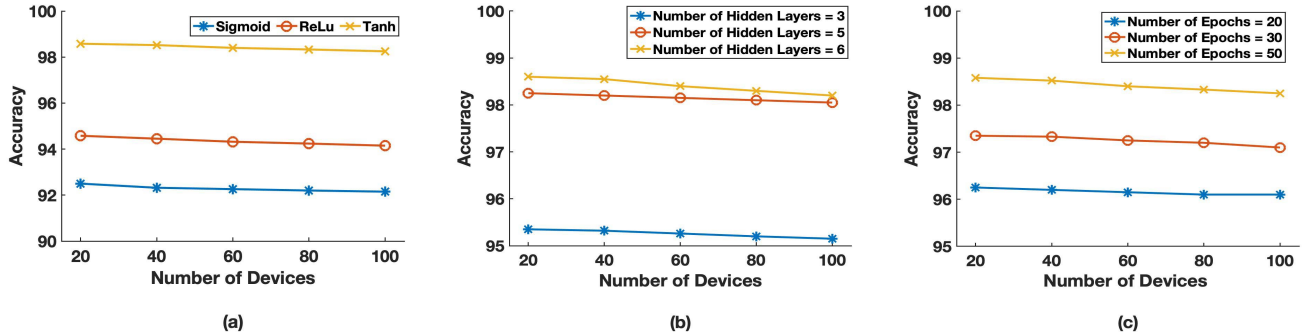

Fig. 6. (a) The effect of activation function on the detection accuracy. (b) Average detection accuracy for different number of devices and different values of number of hidden layers. (c) The effect of number of epochs on the detection accuracy.

layers increases from 5 to 6. Thus, in our experiments, the optimum selection for the number of hidden layers is 5.

Our experiments showed that if (during the training phase) a higher number of epochs is applied, the DAE model offers better performance (see Fig. 6–c). In fact, applying a higher number of epochs provides more chance for the model to deeply learn the training data. However, this may result in the model overfitting. To address the overfitting problem, we enabled the *EarlyStopping()* feature of the keras library in our Python code. Enabling this feature causes the termination of model training loop once the model becomes overfitted. This is checked by monitoring the metric of validation loss at the end of every epoch to find if it is no longer decreasing. Moreover, any change in the batch size affects the training time. This is because during the training phase, the model learns all the data that is available in a batch (and updates the parameters of neurons) before the next batch is learned. As a result, applying a small batch size increases the number of times that model learns and updates its parameters which results in much longer training times. Furthermore, the effect of encoding dimension on the detection accuracy was investigated. The encoding dimension is considered as the size of the encoded (representation) vector (see Fig. 2). We noticed that for lower encoding dimensions, the detection accuracy reduces. The reason is that for lower encoding dimensions, (intuitively) the input vector experiences too much compression. This makes the decoding procedure more difficult/less accurate and results in a higher level of dissimilarity between the output (decoded) and input vectors. In addition, increasing the number of hidden layers provides more accurate detections (considering a fixed value of the encoding dimension).

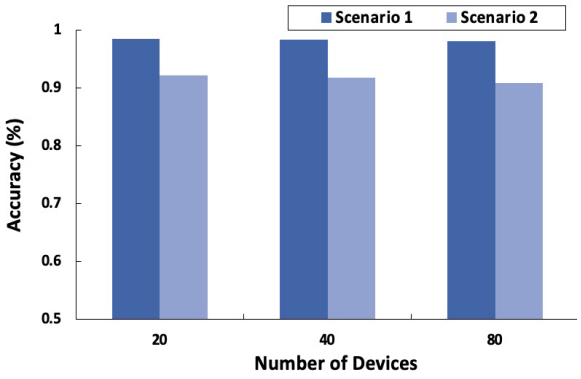

Fig. 7. The effect of antenna array size on detection accuracy. In scenario 1, 6×6 antenna arrays were used but in scenario 2, 4×4 antenna arrays were deployed.

We also changed the size of array antenna in the deployed devices and the gNB to investigate the effect of antenna array size on the level of uniqueness in beam features. In this regard, we decreased the size of antenna array from 6×6 (scenario 1) to 4×4 (scenario 2) for the deployed devices, and from 32×32 (scenario 1) to 16×16 (scenario 2) for the gNB. As Fig. 7 shows, smaller detection accuracies were reduced in scenario 2. Intuitively, the reason is that with a smaller number of antenna elements, the number of sources for beam

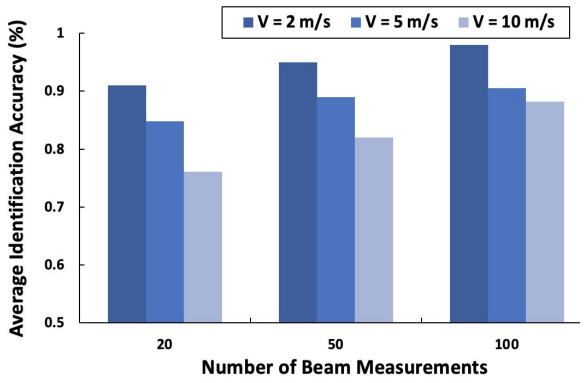

Fig. 8. Average identification accuracy for mobile devices with different average velocities.

feature uniqueness reduces, e.g., phase shifter units used for each antenna element, dimensional tolerances exist during the antenna fabrication process, or relative permittivity (ϵ_r) of the substrate material used in each antenna element. This makes the beam features of devices less distinguishable which results in less accurate detection of an illegitimate device.

C. The Effect of Mobility

To evaluate the effect of mobility on the identification accuracy, we implemented the random waypoint mobility model (RWP) [54] in MATLAB and used it for the mobile devices to measure their beam features in the mobility scenario. In the RWP model, the trajectory of a device is modelled by a series of connected lines (segments) that are called transitions. In every transition, the device moves from the endpoint of the previous transition towards the (randomly selected) destination point (endpoint) of the current transition with a randomly chosen velocity. Then, the device pauses for some random time before the next transition starts. Regarding the communication channel, we used the Rician fading channel model from the Communications Toolbox of MATLAB to consider the effect of multipath fading, scattering, Doppler shift, etc. on the performance of the detection scheme. These unwanted phenomena occur due to the dynamic environment between the mobile devices and the fixed gNB/AP.

We trained the DAE model using the dataset obtained based on the exploited mobility and fading channel models and computed the average identification accuracy. Fig. 8 shows the results for the three training datasets generated using different average velocities at SNR = 30 dB. We observed a degradation in the identification accuracy when a larger average velocity was applied. The reason is that the beam angles change more rapidly when a device moves faster which makes the beam features more different than what the DAE model has learned. However, as the figure indicates, training the model with a larger number of beam measurements improves the model ability to identify a device. As a result, the deployment of a special training mechanism (for the measurement of beam features at different azimuth and elevation angles during the enrolment of devices) can effectively address the mobility issue.

VI. Summary and Future Work

In this paper, a lightweight mechanism is proposed for the detection of wireless spoofing attacks in mmWave-enabled IoT networks. In the proposed mechanism, the device–dependant beam features of legitimate devices are learned by a DAE–based learning model during a training phase. Then, the identity of any connecting IoT device can be validated using the developed learning model, i.e., an illegitimate device can be detected as an anomaly since the RF features extracted from its received signal has not been learned by the model before. The main characteristics of the proposed mechanism is that it offers scalability and causes zero computation/communication overhead to the resource—constrained IoT devices. Moreover, we proposed a delay–based solution to make the malicious replay efforts unsuccessful. The results of our experiments prove the effectiveness of the proposed approach. As a future work direction, the effectiveness of different Machine/Deep Learning models can be investigated to utilize the uniqueness of mmWave beam features in the development of a scalable device authentication mechanism for NGIoT networks. In addition, we intend to employ real IoT devices equipped with mmWave communication interfaces (as these devices will become more accessible) and generate a real dataset to train the learning model.

References

[1] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020.
[2] X. Lu, V. Petrov, D. Moltchanov, S. Andreev, T. Mahmoodi, and M. Dohler, "5G-U: Conceptualizing integrated utilization of licensed and unlicensed spectrum for future IoT," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 92–98, Jul. 2019.
[3] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018.
[4] A. Jurcut, T. Niculcea, P. Ranaweera, and N.-A. Le-Khac, "Security considerations for Internet of Things: A survey," *Social Netw. Comput. Sci.*, vol. 1, no. 4, pp. 1–19, Jul. 2020.
[5] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019.
[6] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?" *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 41–49, Sep. 2018.
[7] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.
[8] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.
[9] J. Tang, H. Wen, K. Zeng, R.-F. Liao, F. Pan, and L. Hu, "Light-weight physical layer enhanced security schemes for 5G wireless networks," *IEEE Netw.*, vol. 33, no. 5, pp. 126–133, Sep. 2019.
[10] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)*, Feb. 2017, pp. 32–37.
[11] T. Alladi, V. Chamola, B. Sikdar, and K. R. Choo, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 17–25, Mar. 2020.
[12] W. Wang, P. Xu, D. Liu, L. T. Yang, and Z. Yan, "Lightweighted secure searching over public-key ciphertexts for edge-cloud-assisted industrial IoT devices," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4221–4230, Jun. 2020.
[13] K. M. Alam, M. Saini, and A. E. Saddik, "Toward social internet of vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, 2015.

[14] D. Wang *et al.*, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1878–1911, 2nd Quart., 2019.
[15] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.
[16] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT security through authentication of wireless nodes using *in-situ* machine learning," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 388–398, Feb. 2019.
[17] M. Andraud, H.-G. Stratigopoulos, and E. Simeu, "One-shot non-intrusive calibration against process variations for analog/RF circuits," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 11, pp. 2022–2035, Nov. 2016.
[18] S. Sen, "Context-aware energy-efficient communication for IoT sensor nodes," in *Proc. 53rd ACM/EDAC/IEEE Design Automat. Conf. (DAC)*, Jun. 2016, pp. 1–6.
[19] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless physical-layer identification: Modeling and validation," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2091–2106, Sep. 2016.
[20] X. Huan, K. S. Kim, and J. Zhang, "NISA: Node identification and spoofing attack detection based on clock features and radio information for wireless sensor networks," *IEEE Trans. Commun.*, vol. 69, no. 7, pp. 4691–4703, Jul. 2021.
[21] G. Baldini and G. Steri, "A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1761–1789, 3rd Quart., 2017.
[22] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, "Deep learning for RF device fingerprinting in cognitive communication networks," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 1, pp. 160–167, Feb. 2018.
[23] T. J. Bihl, K. W. Bauer, and M. A. Temple, "Feature selection for RF fingerprinting with multiple discriminant analysis and using ZigBee device emissions," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1862–1874, Aug. 2016.
[24] S. Balakrishnan, S. Gupta, A. Bhuyan, P. Wang, D. Koutsonikolas, and Z. Sun, "Physical layer identification based on spatial–temporal beam features for millimeter-wave wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1831–1845, 2020.
[25] S.-Y. Lien, S.-L. Shieh, Y. Huang, B. Su, Y.-L. Hsu, and H.-Y. Wei, "5G new radio: Waveform, frame structure, multiple access, and initial access," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 64–71, Jun. 2017.
[26] Z. Zhang, P. Cui, and W. Zhu, "Deep learning on graphs: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 34, no. 1, pp. 249–270, Jan. 2022.
[27] N. Wang, L. Jiao, P. Wang, W. Li, and K. Zeng, "Machine learning-based spoofing attack detection in mmWave 60 GHz IEEE 802.11ad networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Jul. 2020, pp. 2579–2588.
[28] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.
[29] N. Wang, W. Li, T. Jiang, and S. Lv, "Physical layer spoofing detection based on sparse signal processing and fuzzy recognition," *IET Signal Process.*, vol. 11, no. 5, pp. 640–646, Jul. 2017.
[30] S. Liu, "MAC spoofing attack detection based on physical layer characteristics in wireless networks," in *Proc. IEEE Int. Conf. Comput. Electromagn. (ICCEM)*, Mar. 2019, pp. 1–3.
[31] E. M. D. L. Pinto, R. Lachowski, M. E. Pellenz, M. C. Penna, and R. D. Souza, "A machine learning approach for detecting spoofing attacks in wireless sensor networks," in *Proc. IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, May 2018, pp. 752–758.
[32] M. Faisal, S. Abbas, and H. Ur Rahman, "Identity attack detection system for 802.11-based ad hoc networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, pp. 1–16, Dec. 2018.
[33] W. Yan, S. Hylamia, T. Voigt, and C. Rohner, "PHY-IDS: A physical-layer spoofing attack detection system for wearable devices," in *Proc. 6th ACM Workshop Wearable Syst. Appl.*, 2020, pp. 1–6.
[34] N. Wang, J. Tang, and K. Zeng, "Spoofing attack detection in mm-wave and massive MIMO 5G communication," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 1–5.
[35] W. Tan, S. D. Assimonis, M. Matthaiou, Y. Han, X. Li, and S. Jin, "Analysis of different planar antenna arrays for mmWave massive MIMO systems," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Jun. 2017, pp. 1–5.
[36] J. Chen, "When does asymptotic orthogonality exist for very large arrays?" in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 4146–4150.
[37] J. Elkind, E. Goldberger, and E. Socher, "57–67-GHz highly compact bidirectional 3-bit phase shifter in 28-nm CMOS," *IEEE Microw. Wireless Compon. Lett.*, vol. 28, no. 11, pp. 1017–1019, Nov. 2018.
[38] N. Sharma and V. Sharma, "A design of microstrip patch antenna using hybrid fractal slot for wideband applications," *Ain Shams Eng. J.*, vol. 9, no. 4, pp. 2491–2497, Dec. 2018.
[39] A. Ghosh, V. Kumar, G. Sen, and S. Das, "Gain enhancement of triple-band patch antenna by using triple-band artificial magnetic conductor," *IET Microw., Antennas Propag.*, vol. 12, no. 8, pp. 1400–1406, 2018.
[40] M. Abbasi Layegh, C. Ghobadi, and J. Nourinia, "The optimization design of a novel slotted microstrip patch antenna with multi-bands using adaptive network-based fuzzy inference system," *Technologies*, vol. 5, no. 4, p. 75, Nov. 2017. [Online]. Available: https://www.mdpi.com/2227-7080/5/4/75
[41] *Ferro A6–S High Frequency LTCC System, Ferro Electronic Materials*. Accessed: May 21, 2021. [Online]. Available: https://ostec-materials.ru/upload/iblock/0bb/0bb9ac1ff67ce748dfb231486fb13f5e.pdf
[42] M. Giordani *et al.*, "A tutorial on beam management for 3GPP NR at mmWave frequencies," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 173–196, 1st Quart., 2018.
[43] T. Inoue, "5G standards progress and challenges," in *Proc. IEEE Radio Wireless Symp. (RWS)*, Jan. 2017, pp. 1–4.
[44] *Study on New Radio (NR) Access Technology—Physical Layer Aspects—Release 14, TR 38.802*. Accessed: 13th Feb. 2021. Accessed: Feb. 13, 2021. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/38_series/38.802/
[45] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.
[46] *Intel Core I7-8086K Processor*. Accessed: Mar. 7, 2022. [Online]. Available: https://www.intel.com.au/content/www/au/en/products/sku/148263/intel-core-i78086k-processor-12m-cache-up-to-5-00-ghz/specifications.html
[47] U. Ruhrmair and M. van Dijk, "PUFs in security protocols: Attack models and security evaluations," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 286–300.
[48] J. Wang *et al.*, "Subwavelength grating enabled on-chip ultra-compact optical true time delay line," *Sci. Rep.*, vol. 6, no. 1, pp. 1–10, Sep. 2016.
[49] R. Lu, T. Manzameque, Y. Yang, and S. Gong, "S0-mode lithium niobate acoustic delay lines with 1 dB insertion loss," in *Proc. IEEE Int. Ultrason. Symp. (IUS)*, Oct. 2018, pp. 1–9.
[50] T. Manzaneque, R. Lu, Y. Yang, and S. Gong, "Low-loss and wideband acoustic delay lines," *IEEE Trans. Microw. Theory Techn.*, vol. 67, no. 4, pp. 1379–1391, Apr. 2019.
[51] P. Schulz *et al.*, "Latency critical IoT applications in 5G: Perspective on the design of radio interface and network architecture," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 70–78, Feb. 2017.
[52] *MATLAB Products and Services*. Accessed: Jan. 21, 2021. [Online]. Available: https://au.mathworks.com/products.html
[53] *3GPP 5G–NR, Release 15*. Accessed: Jan. 21, 2021. [Online]. Available: https://www.3gpp.org/release-15
[54] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*. Boston, MA, USA: Springer, 1996, pp. 153–181.

Mohammad Reza Nosouhi received the master's degree in telecommunications engineering from the Isfahan University of Technology, Isfahan, Iran, in 2007, and the Ph.D. degree from the University of Technology Sydney, Ultimo, NSW, Australia, in 2020. He has more than ten years of industry experience in ICT field. He is currently working as a Research Fellow with the Centre for Cyber Security Research and Innovation (CSRI), Deakin University, Australia. His research interests are post-quantum cryptography, next generation authentication systems, applied cryptography, and blockchain systems.

Keshav Sood is currently a Lecturer with the Centre for Cyber Security Research and Innovation, School of IT, Deakin University, Melbourne, Australia. Previously, he worked as a Research Fellow with the Advanced Cyber Security Engineering Research Centre (ACSRC), The University of Newcastle, NSW, Australia.

Marthie Grobler received the Ph.D. degree from the University of Johannesburg, South Africa. She currently holds a position as a Principal Research Scientist with CSIRO's Data61, Melbourne, Australia, where she drives the research group's work on human centric cybersecurity. She is passonate about making cybersecurity more accessible for people in the pathway of the fourth industrial revolution. From applying governance models in the digital space to teaching children in rural areas about technology, she works towards a thorough and effective approach to maximise cybersecurity knowledge and practical application.

Robin Doss (Senior Member, IEEE) received the B.Eng. degree in electronics and communications from the University of Madras, India, in 1999, and the M.Eng. and Ph.D. degrees from RMIT University, Australia, in 2000 and 2004, respectively. He is currently the Director of the Centre for Cyber Security Research and Innovation (CSRI), Deakin University, Australia. In addition, he leads the "Development of Next Generation Authentication Technologies" theme within the National Cyber Security Cooperative Research Centre (CSCRC). He has an extensive research publication portfolio. His research program has been funded by the Australian Research Council (ARC), Government Agencies, such as the Defence Signals Directorate (DSD), Department of Industry, Innovation and Science (DIIS), and industry partners. His research interests include the broad areas of system security, protocol design, and security analysis, with a focus on smart, cyber-physical, and critical infrastructures. He is a member of the Research Council of the Oceania Cyber Security Centre (OCSC) and the Executive Council of the IoT Alliance Australia (IoTAA). In 2019, he was a recipient of the Cyber Security Researcher of the Year Award from the Australian Information Security Association (AISA).