Toward IoT Node Authentication Mechanism in Next Generation Networks

Dinh Duc Nha Nguyen, Keshav Sood, *Senior Member, IEEE*, Yong Xiang, *Senior Member, IEEE*, Longxiang Gao, *Senior Member, IEEE*, Lianhua Chi, *Senior Member, IEEE*, and Shui Yu, *Fellow, IEEE*

***Abstract*—Although the next generation networks (5G-NGNs) provide a flexible infrastructure to support latency-sensitive and bandwidth-hungry mission-critical Internet of Things (IoT) applications, however, the 5G-IoT integration in NGNs has increased the threat surface. Unfortunately, IoT devices are resource constrained, and the traditional intrusion detection systems (IDS) approaches based on cryptography are not effective on 5G-IoT ecosystems. In this article, we propose an effective 5G-IoT node authentication approach that leverages unique radio frequency (RF) fingerprinting data to train the Deep learning model to detect legitimate and nonlegitimate IoT nodes. Our approach is based on Mahalanobis Distance theory and Chi-square distribution theories. The proposed approach achieves a higher detection accuracy (99.35%) as well as lower training time compared to other existing approaches which is a key benefit of our approach in NGNs. The experiments are conducted using ETSI-open source NFV management and orchestration (OSM-MANO) platform on Amazon Web Services (AWSs) cloud platform to verify how the proposed approach would fit in real-life scenarios. The method can be used as a standalone security system or as a part of multifactor authentication.**

***Index Terms*—5G security, authentication, Internet of Things (IoT), next generation networks, radio frequency (RF) fingerprinting.**

I. Introduction

THE FIFTH-GENERATION mobile networks (5G) offer flexible infrastructure for the rapid deployment of large-scale Internet of Things (IoT) systems. Particularly, 5G becomes a key technology to support flexible smart IoT applications, such as autonomous vehicles, smart cities, Industry 4.0, etc. [1], [2]. Unfortunately, this integration of next generation networks and IoT (NGN-IoT) has substantially expands the threat landscape of large scale for NGN-IoT networks and applications [3], [4], [5]. Note that the IoT devices can be easily exploited as they are resource constrained and cannot perform high computational authentication protocol/s at end-host (IoT device). This means that IoT devices can potentially be an attractive attack surface or platform for adversaries to use these devices as botnets [6]. In such critical scenarios effective, scalable, and lightweight authentication plays a vital role to classify legitimate and nonlegitimate IoT devices in NGNs.

The traditional IoT authentication schemes are primarily based on credential and cryptography approaches. In the credential-based schemes the access control model grants network access to users based on the set credentials, such as user accounts and passwords. Cryptography-based methods, on the other hand, provide encrypted communication channels (using hash technologies). Both types of authentication schemes suffer from critical issues [7], [8]. First, IoT devices are resource constrained and so they cannot support power hungry cryptographic algorithms to run on end-nodes (IoTs) [6]. Adversaries can easily knock down networks, can use IoT devices and turn them into botnets, etc. Moreover, in some leaking credential or certificate-based authentication scenarios, the traditional authentication approaches cannot fully avoid impersonation attacks [9], [10]. In NGNs, networks have unique features which also do not fully support traditional approaches to function at optimum levels. For example, 5G supports real-time applications, which also means that the authentication time to verify legitimate and nonlegitimate nodes should be within the acceptable range, otherwise it introduces high latency in the detection time of nodes legitimacy [4], [11]. This highlights the need of investigating new node authentication mechanism with an ability to quickly and dynamically update the classification models (for node authentication). The existing security solutions based on traffic data analyses are also not suitable and secure for NGNs [12]. It means the authentication based on traffic data analyses is weak to prevent the impersonate attack [13]. Hence, authentication for next-generation IoTs is still a challenging issue.

Recently, physical layer authentication (PLA) has raised the attention of researchers to use physical features of wireless devices for authentication [14], [15], [16] as the radio frequency (RF) features are almost impossible to mimic [17]. PLA technique leverages the nonlinear characteristics of physical devices to generate unique device identifiers. In IoTs, the

Manuscript received 19 April 2022; revised 13 September 2022; accepted 24 March 2023. Date of publication 29 March 2023; date of current version 25 July 2023. This work was supported in part by the Taishan Scholars Program under Grant TSQN202211214. *(Corresponding author: Dinh Duc Nha Nguyen.)*

Dinh Duc Nha Nguyen and Keshav Sood are with the Centre of Cyber Security Research and Innovation, School of IT, Deakin University, Geelong, VIC 3220, Australia (e-mail: nguyendinh@deakin.edu.au; keshav.sood@deakin.edu.au).

Yong Xiang is with the Deakin Blockchain Innovation Lab, School of IT, Deakin University, Geelong, VIC 3220, Australia (e-mail: yong.xiang@deakin.edu.au).

Longxiang Gao is with the Faculty of Computer Science and Technology, Qilu University of Technology (Shandong Academy of Sciences), Jinan 250316, China, and also with the Shandong Computer Science Center (National Supercomputer Center in Jinan), Jinan 250101, China (e-mail: longxiang.gao@deakin.edu.au).

Lianhua Chi is with the Computer Science and Information Technology, La Trobe University, Melbourne, VIC 3086, Australia (e-mail: l.chi@latrobe.edu.au).

Shui Yu is with the Department of School of Software, University of Technology Sydney, Sydney, NSW 2007, Australia (e-mail: shui.yu@uts.edu.au).

Digital Object Identifier 10.1109/JIOT.2023.3262822

PLA uses the wireless RF fingerprints (signatures) to authenticate legitimate IoT devices [17], [18], [19]. Approaches based on RF signatures extracts the traits of wireless devices that occurs during manufacturing of devices (radio circuitry fabrication) due to hardware random imperfections. The key definite reason for using physical flaws or imperfections (as unique features for authentication) is that it is highly difficult to replicate the RF fingerprints by employing other devices [17]. In other words, typically, some domains are more sensitive, and security is critically important in such domains for example in industrial/operational IoT sectors or mission article applications. Here, RF features-based node authentication plays important role over network traffic analysis-based and resource constrained crypto solutions [20], [21].

Motivated from this, we propose an RF signatures-based effective IoT authentication methodology to authenticate wireless IoT nodes in NG-IoT networks. We use Mahalanobis Distance (MD) and Chi-squared distribution theories in our solution. The idea is inspired from the face detection method in real life. Human face can be distinguished by the size (measurements) of parts of the face such as eyes, mouth, nose, etc. and the correlation of these parts. For example, we consider two features to precisely detect two different faces from each other, these features are 1) length of face from hairline to the bottom of jawline and 2) width of forehead at the widest point for instance. We collect the measurement and calculate the correlation among these. The results of this correlation will be unique to every person, which means we obtain a unique signature of the face/person. Similarly, our solution obtains a unique "face" or (RF signature) of wireless IoT device. We use MD theory to compute this correlation.

The significant contributions of our solution are as follows.

1) We propose an effective node authentication approach for the next generation 5G-IoT network. We leverage MD and Chi-squared distribution theories in our solution to train these models using RF signatures-based features of wireless IoT nodes. To the best of our knowledge, we are among the early ones jointly considered employing RF signatures and these theories in the next-generation IoT networks authentication research domain.
2) We have conducted the experiments under different signal to noise ratio (SNR) conditions and number of devices to show that the proposed method has stable average detection accuracy as well as lower node detection time. The tradeoff between the accuracy and scalability is also examined.
3) We tested the approach on ETSI-5G OSM-MANO platform to: a) show the proposal is aligned with the standard architecture and b) to verify the approach's effectiveness in real time. We use Amazon Web Service (AWS) cloud platform (as virtual infrastructure manager) for deployment and evaluation of our scheme. The comparison of our approach with other recent approaches is shown. The results prove that our solution outperforms these existing methods in terms of training time, resources, and accuracy.

In contrast to the existing works, we have shown that our scheme provides higher detection accuracy (under different SNR scenarios) as well as takes lesser training time to update ML models. From the deployment side of this proposal into real life, we have conducted experiments to prove that our scheme reduces CPU utilization and memory usage of virtual networks resources. In remainder of this article Sections II and III provides the related works and preliminaries, respectively. Section IV provides the proposed scheme and the performance evaluation is discussed in Section V. Section VI concludes this article and discusses some future works. Table I shows abbreviations and Table III lists the notations in the paper.

TABLE I
LIST OF ABBREVIATIONS USED IN THE ARTICLE

Abbreviation	Definition	Abbreviation	Definition
5G-NGNs	The next generation networks	MD	Mahalanobis Distance
ANN	Artificial Neural Network	MSCNN	Multisampling Convolutional Neural Network
AWS	Amazon Web Services	NFV	Network Functions Virtualization
CD	Chi-square Distribution	NG-IoT	The Next Generation Networks & IoT
CDF	Cumulative Distribution Function	NLOS	Non-line-of-sight
CFD	Carrier Frequency Differences	NS	Network Service
CFO	Carrier Frequency Offset	OTs	Operational Technologies sector
CNN	Convolutional Neural Network	PCA	Principal Component Analysis
CSI	Channel State Information	PLA	Physical Layer Authentication
DNN	Dense Neural Network	PDF	Probability Density Function
DWT	Discrete Wavelet Transform	PSD	Power Spectral Density
ETSI	European Telecommunications Standards Institute	RF	Radio Frequency
HOS	Higher Order Statistical	RRC	Root-raised cosine
I/Q	In-phase and Quadrature	RSS	Radio Signal Strength
IDS	Intrusion Detection Systems	SNR	Signal to Noise Ratio
IoT	Internet of Things	SVM	Support Vector Machine
KNN	K-Nearest Neighbor	SYNC	Synchronization
LOS	Line-of-sight	TFED	Time-Frequency-Energy
LSVM	Linear Support Vector Machine	UAV	Unmanned Aerial Vehicle
MANO	Management & Orchestration	VMD	Variational Mode Decomposition

II. RELATED WORK

RF fingerprinting-based authentication approach is a known research domain in wireless networks. Also, the deep learning-based approaches are recently becoming popular to verify node's legitimacy. The deep learning models work on data set which they extract (on-line or off-line) for model training and evaluation. The main aim of feature extraction is to capture the information from RF signals and generate the unique identifier for the device. A number of RF features can be used in the RF fingerprinting techniques, such as: Power Spectral Density (PSD) and normalized PSD, discrete wavelet transform (DWT), power amplifier, magnitude and phase errors, I/Q origin offset, SYNC correlation of the frame, carrier frequency differences (CFDs), phase shift differences (PSD), radio signal strength (RSS), channel state information (CSI), carrier frequency offsets (CFOs), instantaneous phase, amplitude, frequency, etc. [18], [33]. In most of the existing works, the RF features are extracted from the RF transmitter signals. The machine learning models, see Table II, are

TABLE II
SUMMARY OF THE KEY EXISTING WORKS

Year/Ref.	Project aim/overview	Model Used
2018 [22]	Kitsune: reduce the label effort and employ Autoencoder to identify the normal and abnormal patterns.	Autoencoder
2019 [17]	RF-PUF: find an unique sigature based on RF features and ANN algorithm for classification.	ANN
2019 [23]	Classify RF fingerprinting features based on PCA for dimensional reduction and SVM.	PCA + SVM
2019 [24]	Classify ZigBee devices using MSCNN based on region of interest feature.	MSCNN
2019 [25]	Employs the RF fingerprinting (transient signals) and LSVM for classification.	LSVM
2020 [26]	Slora: prevent impersonate attacks using two RF features and classification based on SVM.	SVM
2020 [27]	Detecting and classifying the UAVs based on RF fingerprinting on Wi-Fi and Bluetoot protocols.	KNN
2020 [28]	Improve the performance of fingerprint classification scheme by extracting the region of interest characteristic.	Lightweight CNN
2020 [29]	Modify the classic CNN model of VGG-16 for frequency fingerprint recognition.	CNN
2020 [30]	Improve the recognition performance by extracting the best-performing feature subset and classification by KNN.	KNN
2020 [31]	H2ID: detecting the attack using two stages: anomaly detection and attack classification.	Deep Autoencoder
2021 [32]	Using deep learning to classify waveform domain from the raw sample for the device identifications.	DNN
2021 [13]	Mitigate the noise by using Nelder-Mead simplex-based channel estimator under Rayleigh fading conditions.	MDA/ML

TABLE III
KEY NOTATIONS

Notation	Explanation
D	the Mahalanobis distance
x	RF feature vector
y	vector of mean values of the variables
T	transpose vector
C	the covariance matrix
k	the number of RF features
v_{thr}	cut-off value
γ	the lower incomplete gamma function
Γ	the gamma function
$f(x;k)$	the probability density function
$F(x;k)$	the cumulative distribution Function

used to classify them to determine the device signatures for authentication purposes.

The most regarded solution is proposed by Mirsky et al. [22] known as Kitsune. The proposed solution tries to detect the attack without supervision process. The back end of the mechanism is the Autoencoder algorithm to learn the normal pattern and analyze the abnormal situation. The idea is tested on a Raspberry device to show the effectiveness of the approach. The solution consumes lot of memory and hence not fully suitable for large scale networks. Chatterjee et al. [17] used a neural network (ANN) to find a unique signature based on some RF fingerprinting feature, such as frequency offset and I-Q imbalance. To avoid the effect of channel conditions, the work suggests the RF fingerprinting features need to be compensated and estimated. Tu et al. [23] proposed an idea by combining principal component analysis (PCA) for dimensionality reduction and the support vector machines (SVMs) for classification. They used four RF fingerprint features in their work. Their method can achieve more than 95% detection accuracy. Yu et al. [24] proposed an RF fingerprinting approach to classify ZigBee devices (based on region of interest (ROI) feature) in this work. The work proposes a multisampling convolutional neural network (MSCNN) for both feature extraction and classification. To validate the performance, the experiments are conducted using both Line-of-Sight (LOS) scenarios and non-LOS (NLOS) scenarios. The method reached the highest accuracy at 97% in LOS scenarios.

In contrast to the aforementioned works the study in [25] proposes an RF fingerprinting method based on variational mode decomposition (VMD). It leverages the Bluetooth transient signals and extracts the higher order statistical (HOS) features from the signals. To identify the Bluetooth devices, the work uses the Linear SVM (LSVM) for classification. The work demonstrates that the classification performance has improved compared to time-frequency-energy (TFED) with smaller features and lower SNR levels. The best detection accuracy of the approach is 98.8%. Another popular work in RF fingerprinting technique for IoT devices is SLoRa [26]. The work introduces an authentication approach with RF fingerprinting technique by extracting two RF features, CFO and link signatures. The integration of two characteristics can improve the effectiveness of preventing impersonation attacks. Regarding the classified model, the work chooses SVM and the combination of CFO and link signatures also increases the detection accuracy.

With indoor scenarios, SLoRa has around 97% detection accuracy. SLoRa employs the RF fingerprinting technique for the LoRa communication only. Ezuma et al. [27] used RF fingerprinting on Wi-Fi and Bluetooth protocols. The study investigates the issue of detecting and classifying the unmanned aerial vehicles (UAVs). The work employs RF fingerprinting technique with two stages; Markov models-based naive Bayes to extract the RF signals and then, the *k*-nearest neighbor (KNN) model for classification. To evaluate the method, experiments are conducted in various SNRs with 15 different types of UAVs. The comparisons with five different machine learning models were also studied. The experiments show the highest detection accuracy at 98.13%. Jian et al. [28] used Lightweight convolutional neural network (CNN) model to improve the performance of fingerprint classification scheme. The method uses the ROI for the classification processes. The first step is preprocessing the raw images and extracting the ROI patterns following this the ROI pattern is considered as the intake data for the Neural Network classifiers. The proposed CNN model shows better accuracy and training time.

Further, Zong et al. [29] proposed a method based on CNN. They modified the classic CNN model of VGG-16 for frequency fingerprint recognition. Their solution demonstrates a stable accuracy with the increase of epochs and the accuracy obtained is 99.70%. Li et al. [30] improved the recognition

performance by extracting the best-performing feature subset from the originated features. They used KNN and evaluated the robustness under different SNR settings, and the highest accuracy is 97.86%. In another work Bovenzi et al. [31] proposed H2ID to enhance the effectiveness to detect the attack. The work proposes two stages to identify the attack: the anomaly detection phase employs a lightweight solution relies on the Deep Autoencoder and the second phase, attack classification, uses the openset classification methodology. The key benefit of the method is the efficiency performance for the IoT scenarios and it can be deployed on the resource constraint devices.

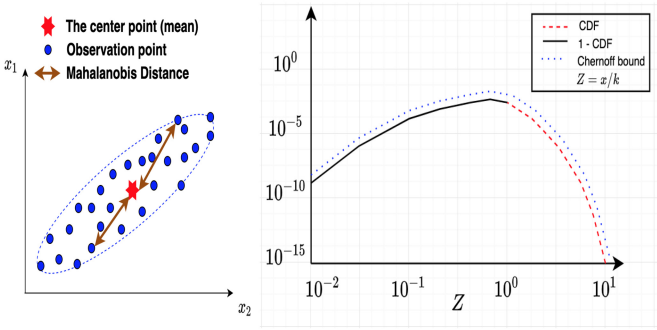
In a recent study, Li and Cetin [32] used the RF fingerprinting idea with a deep learning approach in the waveform domain. They use the images which capture the waveform from the raw sample for the device identifications. They propose the use of dense neural network (DNN) for classification. The method can achieve nearly 99% identification accuracy. In [13], the work is focused on RF fingerprinting with the specific emitter identification (SEI) technique. The proposed solution is effective to mitigate the noise effect in radio operating by using the Nelder-Mead (N-M) simplex-based channel estimator under Rayleigh fading conditions. The work is tested in various scenarios under different SNR values and with the best setting the highest accuracy reported is 95%.

Our Observation: From our literature synthesis, we note that deep learning is widely being used in RF fingerprinting techniques. KNN & SVM are examples of the supervised methods for IoT node classification (legitimate or illegitimate) based on the labeled data [26], [27]. On the other hand, unsupervised methods such as CNN, only need unlabeled data and the algorithm finds the insights from the training set [28], [34]. Unfortunately, in our observation, the RF fingerprinting approaches rely on machine learning theories and still have some limitations [1], [28].

1) The accuracy of a machine learning model depends on the size of the dataset [1], [35], hence it creates a certain challenge with the small to medium size IoT applications/network-scale.
2) Moreover, the time spent on the model training process is another shortcoming of machine learning-based approaches as mobile IoT devices usually join or leave the network frequently which eventually changes the size of the dataset.

This impacts the model training time as well as the node authentication time [3], [4]. This obviously means the increase in the computation time for making and enforcing the authentication decisions and eventually increases the network latency. We emphasize that these aforementioned issues violate the low latency processing requirements of 5G-IoT networks as well as the detection accuracy of authentication systems (trade-off between accuracy and detection time). This has a huge impact on mission critical applications in certain scenarios or certain industrial applications particularly in the operational technologies sector (OTs) (microgrid, smart power plant, etc.).

Overall, in the existing works there are still some concerns related to the utilization of computational resources, training data size as well as the stable detection accuracy. Further, none of the existing works clarifies how valid their proposed approach is on any 5G testbed. Key metrics of evaluation such as model training time, node authentication time, the utilization of resources etc., are missed out. This evaluation is vital to get insights to know deployment challenges when we deploy the schemes in real next generation network platforms. Also they do not show the tradeoff between the accuracy and model training time with respect to (w.r.t.) frequent change in network scale. We note that these metrics are critical for any NG-IoT authentication system performance. In this article, we propose a framework to tackle these issues and our scheme is aligned with standard ETSI-NFV architecture for 5G networks. Additionally, the method can effectively work in small-to large-scale 5G-based IoT networks. To the best of our knowledge, we are the early ones propose to use MD correlation theory using RF signatures for 5G-IoT node authentication.



(a) (b)

Fig. 1. (a) MD. (b) Chi-squared random variable with 10 degrees of freedom has a Chernoff bound for the CDF and tail (1-CDF) ($k = 10$).

III. Preliminaries

A. Mahalanobis Distance

MD is the distance between two points in multivariate space. It is a measurement of the distance between a variable x and a distribution computed using a mean and a covariance matrix. As a result, MD is thought to have a multivariate normal distribution. Pattern recognition researchers frequently use this theory to compare the data distributions of train and test samples. Furthermore, the covariance matrix aids in determining the shape of the data spread in feature space. The zone of persistent MD around the central point, as shown in Fig. 1(a), forms an ellipse in 2-D space (assuming 2 variables are measured). When we employ many variables, the area is turned into an ellipsoid or hyperellipsoid. In comparison to the Euclidean distance, if the dimensionality of variables is interconnected, MD can eliminate misleading information. It accomplishes this by first converting the dimensions into uncorrelated variables, then, transforming their variance to a constant value and calculating the Euclidean distance.

B. Chi-Square Distribution

In the case of independent variables, the Chi-square distribution (CD) provides a continuous distribution of the total of squared random variables. It gives the confidence intervals

covering the variance and standard deviation of a point in relation to a normal distribution. It is also used to assess how well sampling data conforms to the actual population. According to (8), the MD is a sub-branch of the CD with k degrees of freedom (k being the number of dimensions of the dataset). Although it is true that in real time, variables do not always adhere to the premise of normalcy. In such circumstances, converting the MD to Chi-square p-values (probability of witnessing a test statistic) recodes it to a 0-1 scale. Because MD has no upper limit, this rescaling may be useful for analysis. In general, the p-value indicates the likelihood of encountering an MD value that is as big or higher than the actual MD value; p values near to 0 reflect high MD values and hence are significantly different (valid nodes) to the optimum combination of new variables. p-values near to one indicate poor MD (illegitimate nodes) and are thus very comparable to the optimal mix of new IoT nodes (sometimes called predictor variables). Mathematically, the Chi-squared Distribution (also χ^2-distribution) is the distribution of a total of the squares of k. Suppose $x_1, x_2, \ldots, x_k$ are independent variables, so the total of their squares as

$$Q = \sum_{i=1}^{k} {x_i}^2 \tag{1}$$

the CD with k is denoted as

$$Q \sim \chi^2(k) \text{ or } Q \sim \chi_k^2. \tag{2}$$

A Chi-squared distribution is the same as squaring a Gaussian distribution if the degree of freedom is 1. When a result, as the sample/test size grows, the test distribution approaches a normal distribution. The extreme values of the Chi-squared distribution and the normal distribution have a link in this scenario. It causes the normal distribution/Chi-squared distribution to have a low probability, especially with tiny p values. The following is the definition of the probability density function:

$$f(x; k) = \frac{x^{\frac{k}{2}-1} e^{-\frac{x}{2}}}{2^{\frac{k}{2}} \Gamma\left(\frac{k}{2}\right)}, x > 0. \tag{3}$$

The cumulative distribution function (CDF) of CD is denoted as

$$F(x; k) = \frac{\gamma\left(\frac{k}{2}, \frac{x}{2}\right)}{\Gamma\left(\frac{k}{2}\right)} \tag{4}$$

where $\gamma(s, t)$ is the lower incomplete gamma function and $P(s, t)$ is the regularized gamma function.

This function has the following simple form when $k = 2$:

$$F(x; 2) = 1 - e^{\frac{-x}{2}}. \tag{5}$$

This can be readily calculated by combining $f(x; 2) = (1/2)e^{(-x/2)}$ directly. The integer recurrence of the gamma function helps to calculate $F(x; k)$ for other small, even k. Letting $z \equiv (x/k)$, Chernoff bounds on the lower and upper tails of the CDF may be acquired. The Chernoff bound sets exponentially declining constraints on sums of independent

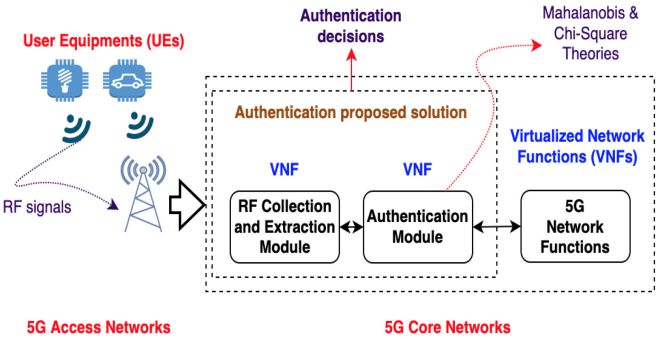


Fig. 2. High-level architecture of the proposed approach.

random variables' tail distributions. In other words, it presents the shape of the CDF. For the cases when $0 < z < 1$ (This includes all examples in which this CDF would be less than 50 percent)

$$F(zk; k) \leq \left(ze^{(1-z)}\right)^{\frac{k}{2}}. \tag{6}$$

The tail bound for the cases when $z > 1$, similarly, is [see Fig. 1(b)]

$$1 - F(zk; k) \leq \left(ze^{(1-z)}\right)^{\frac{k}{2}}. \tag{7}$$

IV. Proposed Framework

In this section, the high-level framework of our proposed scheme is shown in Fig. 2. The framework consists of two separate modules that are deployed at the core segment of the 5G network in form of virtualized network functions (VNFs). These modules being VNFS, can therefore easily be integrated into the standard architecture of ETSI NFV. The first module is RF Collection and Extraction that has a responsibility to leverage the RF feature data of devices and transfer that data to the next module. Our module works with receivers (gateways or base stations) at the 5G Access Networks to extract raw RF signals from IoT transmitters into RF feature data. In the proposed approach, the RF features of every device that connects to the network are extracted by the first contact point of the devices (examples access points or gateways). These RF features are sent to the backend server where they are applied to our proposed Mahalanobis model for the detection of any anomalies. The RF features are extracted from the IoT nodes' RF signals during its normal communications. The backend server (authentication module in our case) performs anomaly detection for many devices. We assume that the feature extraction that takes place in our module is aligned with the processes explained in [17] and [18].

The Authentication Module uses the MD and CD theories to validate the node's legitimacy. In our method, we employ the MD over other distance measure algorithms since the MD provides a better performance in classification [36], [37], [38]. The background of these theories is discussed in the previous section. Fig. 3 gives a high-level view of the workflow of the theoretical model used in our proposed method.

Now, if a new node enters the network (red dot outside the MD region, shown in Fig. 3, the MD calculates the distance

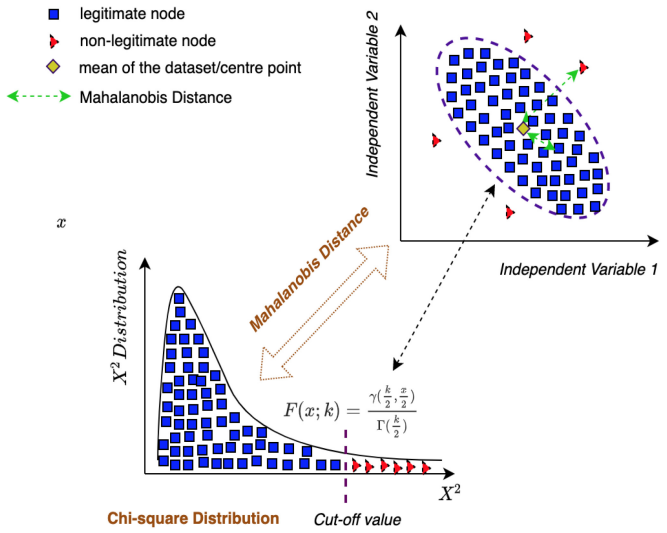


Fig. 3. Detect legitimate node by MD and Chi-squared Distribution.

between a new node and the mean of the data set (from the centred point shown as an orange squared box). The formula to compute MD is as follows.

$$D = \sqrt{(x-y)^T.C^{-1}.(x-y)}. \tag{8}$$

In this case $(x-y)$ is the vector's distance from the mean. This is then partitioned by the covariance matrix. This is exactly a multidimensional variant of the regular standardisation $(z = (x-\mu)/\sigma)$ (where μ shows the mean and σ represents the standard deviation). The absolute value of z reflects the difference in raw score x and mean. In other words, $z = (x$ vector$)-($mean vector$)/($covariance matrix$)$. The equation shows that distance has an inverse relation with covariance. Furthermore, the covariance illustrates the relationship between the variables in the dataset. As a result, if the correlation is found, the distance is much reduced, and vice versa. Note that the MD advances the well-known Euclidean distance formula, which is $d(x,y) = \sqrt{(x,y)}$ between vectors x and y. Because these two formulas are showing two alternative realizations of a vector X of random variables, x and y are random vectors. Knowing that x and y are realizations of the same multivariate random variable, the MD computes the deviation between them. It is important to note that: 1) the mismatch of any realization x with itself should be equal to zero; 2) the dissimilarity should be a symmetric function of the realizations and should reflect the existence of a random process; and 3) MD takes into account the covariance matrix C of the multivariate random variable.

From (5), the cut-off value (refer to Fig 3 is determined by the CDF which separates the rejection region (illegitimate nodes) and the sampling distribution (legitimate nodes). A node is confirmed as legitimate if its MD to the mean of the dataset is less than the cut-off value. There are a number of measure algorithms but the MD has a higher performance in classification tasks [36], [37], [38]. In contrast to other RF fingerprinting approaches which apply machine learning algorithms for the classification process, our proposed framework does the same job with MD and CD theory, however, significantly increases the efficiency of the classification process in terms of detection time, training time, CPU and memory usages.

Authentication Module can categorize the transmitter devices into the legitimate and nonlegitimate node with a cut-off value by using MD and CD theories. Now, we discuss the mathematical model of the Authentication Module in the proposed method.

Assume $\mathbf{X}$ is a set of observation $X^k = \{x_1, x_2, \ldots, x_n\}$ where k is a number of features. We have u is the mean of the observation data. In this case, we have MD

$$D = \sqrt{(x-u)^T.C^{-1}.(x-u)} \tag{9}$$

where T is the transpose vector and C is the inverse covariance matrix of the number of features. From the above equation, we have

$$D_i = \sqrt{(x_i-u)^T.C^{-1}.(x_i-u)} = f_D(x_i) \tag{10}$$

With the k number of features used in the proposed solution, we have the CD denoted as $\chi^2_k(D_i)$. If the k is a positive integer, so we can calculate the Gamma function as follows

$$\Gamma\left(\frac{k}{2}\right) = \left(\frac{k}{2}-1\right)! \tag{11}$$

In case the $k/2$ is a complex numbers with a positive real part, we compute the Gamma function as

$$\Gamma\left(\frac{k}{2}\right) = \int_0^\infty x^{\frac{k}{2}-1} e^{-x}\, dx, \qquad \Re(z) > 0. \tag{12}$$

Now, assume γ is the incomplete gamma function, we have

$$\gamma(s,x) = \int_0^x t^{s-1}\, e^{-t}\, dt. \tag{13}$$

From (4), the $\gamma([k/2];[x/2])$ can be computed as

$$\gamma\left(\frac{k}{2};\frac{x}{2}\right) = \int_0^{\frac{x}{2}} t^{\frac{k}{2}-1}\, e^{-t}\, dt. \tag{14}$$

Hence, we have the CDF used in this case as $F(x;k)$. The CDF, which divides the exclusion zone (illegitimate nodes) and the legitimate nodes (see Fig. 3), determines the cut-off value. If a node's MD to the mean of the dataset is less than the cut-off value, the node is considered as legitimate. Algorithm 1 shows the high-level workflow of the proposed method.

V. Performance Evaluation

In this section, we evaluate our method by conducting experiments under various scenarios. We use the Wireless Waveform Generator toolbox of MATLAB to generate a dataset. We use 450 testing devices, and we have slightly modified the frequency, amplitude, and phase of every device to stimulate the nonideality of RF characteristics. Each device outputs 100 RF signal data. Table IV describes the RF features we utilized in our experiments (along with their mean and standard deviation values). For exact reproducibility of our work, the processed dataset is available via the link provided in the footnote.[1] We show our results in Fig. 4 and Table V.

[1]https://github.com/ndducnha/mahalanobis_dataset

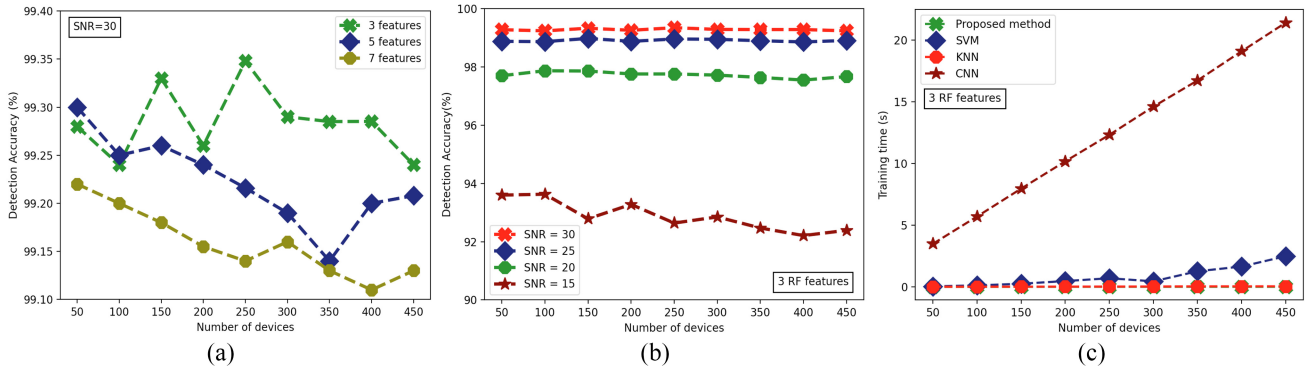


Fig. 4. (a) Average detection accuracy of our scheme at different number of features. (b) Average detection accuracy of our scheme at different number of devices and different values of SNR. (c) Comparison of the proposed method with different machine learning models.

Algorithm 1 Workflow of the Proposed Framework

RF Collection and Extraction Phase

Inputs: *raw data* (RF raw signals)
k (number of features)
x_i (address of the ith legitimate IoT nodes)
n (number of IoT nodes)

Outputs: dataset: $dataset_{k\times i}$

Authentication Phase

Inputs: $dataset_{k\times i}$
The mean: $m = \sum_{j=1}^{n} x_i/n$
Cut-off value: $v_{thr} = \frac{\gamma(\frac{k}{2},\frac{x}{2})}{\Gamma(\frac{k}{2})}$
Mahalanobis Distance: $md_i = (\sqrt{(x-m)^T.C(m)^{-1}.(x-m)})$

if $md_i <= v_{thr}$:
$authentication$ = **TRUE**
else:
$authentication$ = **FALSE**

Outputs: *authentication*

TABLE IV
RF FEATURES USED IN OUR EXPERIMENTS

No.	Features	Mean	Standard Deviation
1	Carrier Frequency Offset(CFO)	2.4 GHz	48 kHz
2	Amplitude Mismatch (In-Phase)	0 dB	3 dB
3	Amplitude Mismatch (Quadrature)	0 dB	3 dB
4	Phase Offset (In-Phase)	0^o	10^o
5	Phase Offset (Quadrature)	0^o	10^o
6	Clock skew	0 ns	40 ns
7	DC offset	0 V	1 V

First, we determine the performance of our mechanism w.r.t. varying IoT node numbers and SNR values. As it is seen in Fig. 4(a) that the best detection accuracy, 99.35%, we obtain is with three features. It can seen that increasing the number of features (from 3 to 7) does not result in a substantial loss in accuracy. To examine the impact of changing SNR on our approach's performance, we gradually raised the number of devices from 50 to 450 to determine detection accuracy at different SNR values (from 15 to 30 dB). We employed three features in this test: 1) CFO; 2) Amplitude Mismatch; and 3) Phase Offset.The results of the testing are shown in Fig. 4(b). The detection accuracy is consistent. As the SNR increases, the detection accuracy increases as well.This is an inevitable result, given that the SNR measures the effect of noise signals on the original signals. We also compute the training time of our solution based on MD and CD theories with other machine learning models and we note that our approach is better than the existing ones [see Fig. 4(c)].

TABLE V
COMPARISON OF OUR METHOD WITH THE EXISTING APPROACHES

Reference and ML Model	MDA/ML [13]	CNN [24]	SVM [26]	KNN [27]	LSVM [25]	Proposed method
Highest detection accuracy (%)	95%	97%	97%	98.13%	98.8%	99.35%

Further, Table V shows a comparison of our scheme with the recent works. We note that our method has the highest detection accuracy at 99.35%. With the CNN [24] and the SVM [26] mechanisms, the detection accuracy is 97%. The MDA/ML [13] has the lowest detection accuracy in this comparison. KNN [27] and LSVM [25] have the accuracy of 98.13% and 98.8%, respectively. In general, we show that our method outperforms other recent works.

Other than the accuracy versus IoT node numbers, we also considered training time as a measure to evaluate the success of our method in order to calculate the node authentication time of the proposed methodology. In the same scenario (3 RF features, dataset with SNR = 30), we compare the training time of our solution at various transmitter counts with RF fingerprinting approaches based on machine learning (we used three features: 1) CFO; 2) Amplitude Mismatch; and 3) Phase Offset). The classified models we use in these experiments are SVM, KNN, and CNN. The result is shown in Fig. 4(c). It demonstrates that our methodology outperforms the other machine learning-based methodologies. This makes sense since machine learning methods take a long processing time for classification [28], but our method with straightforward distance computations is faster. The metric is important in the next generation 5G-IoT environment where the IoT devices might be added or removed to/from the network frequently. Therefore, the classified models have to be

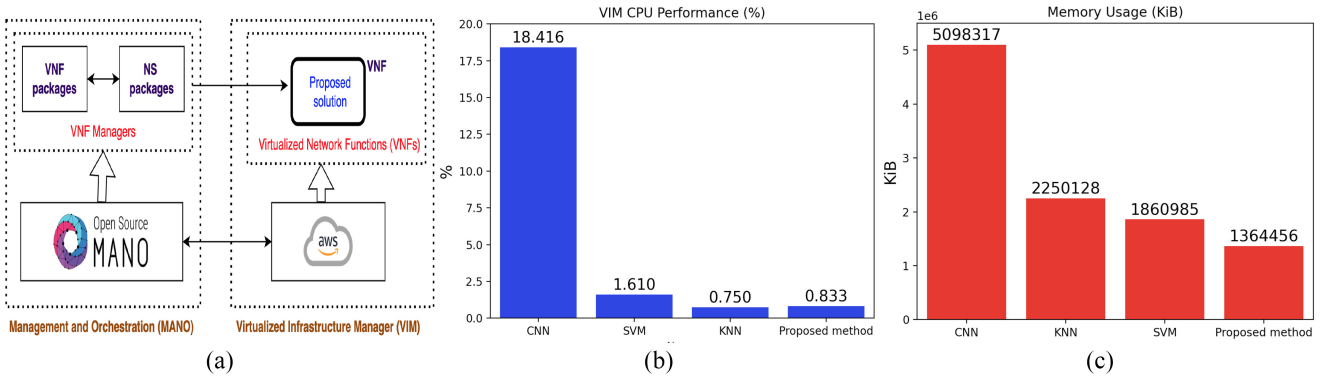


Fig. 5. (a) High level of the standard 5G ETSI-MANO architecture used in the experiments. (b) VNF CPU utilization of the proposed method compared to different machine learning models. (c) Memory usage of the proposed method compared to different machine learning models.

retrained regularly. The lower training time benefits to reduce IoT node authentication time in large scale mobile networks.

To get insights on the performance of the approach in real-life 5G platform, we use OSM-MANO for our evaluation. The proposed idea is integrated in the form of VNFs as shown in Fig. 5(a). The results are shown in Fig. 5. The classification module is implemented as a VNF, known by Authentication VNF, on AWSs platform. The Authentication VNF module is deployed by the network service (NS) manager on open source Mano (OSM). OSM version 10 has been installed on an Amazon Elastic Compute Cloud (Amazon EC2). The EC2 has 8 GB of RAM and 4 virtual CPUs (Intel Xeon processors). The OSM links to the AWS-represented virtualized infrastructure (VI). In 5G, the system is compliant with the ETSI-NFV architecture. The OSM deploys a VNF having 16 GB of RAM and 8 vCPU (Intel Xeon processors). Python 3.6.9, Keras 2.8.0 and Tensorflow version 1.14.0 are used in these VNFs.

We have conducted experiments to evaluate the CPU Utilization as well as memory usage to show the effectiveness of our method while we actually deploy the method in real-time. We use 450 devices at SNR = 30 to evaluate the CPU and memory resources of our solution as well as to conduct comparison with other three classification models: 1) SVM; 2) KNN; and 3) CNN. Fig. 5 shows the results of both CPU Utilization and memory usages. We note that the detection accuracy is 99.35% (the proposed method), 91.38% (SVM), 93.31% (KNN), and 98.4% (CNN). For memory usage, our method has the lowest memory usages. In terms of CPU utilization metric, both our solution and KNN use less CPU than other models. Although the CPU metric of our approach is higher than the KNN but it is not significant (0.833% and 0.75%), we note that our approach achieves higher detection accuracy but utilizes lower CPU and memory resources. We also ran additional tests to examine classification metrics, the results of which are reported in Table VI. These metrics demonstrate the efficacy of our solution.

TABLE VI
CLASSIFICATION METRICS OF THE PROPOSED METHOD AT SNR = 30 AND THE NUMBER OF DEVICES ARE 450

Metric	Proposed method	SVM	KNN	CNN
Accuracy score	99.35%	91.38%	93.31%	98.4%
F1-score	99.67%	95.46%	96.53%	98.42%
Precision	99.36%	99.69%	96.21%	98.40%
Recall	99.99%	91.58%	96.86%	98.46%

VI. CONCLUSION AND FUTURE WORK

In this article, a framework, and the performance evaluation of a novel approach of intrusion detection systems (IDSs) based on RF fingerprinting features of wireless IoT nodes is shown. The selected RF features are then used to train the deep learning model using MD and CD theories. The proposal is integrated into ETSI-NFV standard 5G architecture. The proof-of-concept of its deployment and its performance evaluation is conducted. The proposal has clear advantages over the existing solutions since they are dependent on data type and data size related issues. Our approach not only achieves the highest accuracy for detection but also outperforms other machine learning-based in RF fingerprinting. While the results are encouraging, the study will be extended to rigorously analyze the impact of environmental changes on the used features. Some interesting research directions for the future work are listed below. First, we need to evaluate the robustness of the approach under conditions of interfering channels and other channel distortions. Furthermore, while the MATLAB-simulated dataset is utilized in many RF experiments and the outcomes are promising, in future the proposed approach should be evaluated using any real dataset. In this work, due to time and space limitations we have provided limited discussion on the processing overhead. It is true that model training is CPU/GPU intensive operation, IoT devices are not supposed to do that. In future, we can assume a scenario where a model is trained according to the deployed devices, while only the testing process is run on the device itself (to identify and authenticate the peer node). The testing process is well recognized to be less resource intensive and easily deployable on any platform.

Finally, from a data science aspect a fundamental and interesting future work, form this version, would be to investigate why the two statistics (MD and Chi-Square) allow high accuracy without resorting to machine learning algorithms. What they capture in contrast to previous work is worth investigating. Besides, another key direction is to study quantum computing or serverless computing to analyze the end-to-end

delay [39]. Furthermore, the proposed method can be tested with Edge/Fog computing which brings the back-end services near to the end-user and this can reduce the latency.

REFERENCES

[1] K. Sood, K. K. Karmakar, V. Varadharajen, N. Kumar, Y. Xiang, and S. Yu, "Plug-in over plug-in evaluation in heterogeneous 5G enabled networks and beyond," *IEEE Netw.*, vol. 35, no. 2, pp. 34–39, Mar./Apr. 2021.

[2] M. Alshaikhli, T. Elfouly, O. Elharrouss, A. Mohamed, and N. Ottakath, "Evolution of Internet of Things from blockchain to IOTA: A survey," *IEEE Access*, vol. 10, pp. 844–866, 2022.

[3] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020.

[4] K. Sood, S. Yu, D. D. N. Nguyen, Y. Xiang, B. Feng, and X. Zhang, "A tutorial on next generation heterogeneous IoT networks and node authentication," *IEEE Internet Things Mag.*, vol. 4, no. 4, pp. 120–126, Dec. 2021.

[5] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1657–1681, 3rd Quart., 2017.

[6] P. Gope, O. Millwood, and B. Sikdar, "A scalable protocol level approach to prevent machine learning attacks on physically unclonable function based authentication mechanisms for Internet of Medical Things," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 1971–1980, Mar. 2022.

[7] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[8] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1686–1721, 3rd Quart., 2020.

[9] B. Bera, A. K. Das, S. Garg, M. J. Piran, and M. S. Hossain, "Access control protocol for battlefield surveillance in drone-assisted IoT environment," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2708–2721, Feb. 2022.

[10] A. K. Das, B. Bera, M. Wazid, S. S. Jamal, and Y. Park, "On the security of a secure and lightweight authentication scheme for next generation IoT infrastructure," *IEEE Access*, vol. 9, pp. 71856–71867, 2021.

[11] T. Alladi, V. Venkatesh, V. Chamola, and N. Chaturvedi, "Drone-MAP: A novel authentication scheme for drone-assisted 5G networks," in *Proc. IEEE INFOCOM IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2021, pp. 1–6.

[12] N. Miguélez-Gómez and E. A. Rojas-Nastrucci, "Antenna additively manufactured engineered fingerprinting for physical-layer security enhancement for wireless communications," *IEEE Open J. Antennas Propag.*, vol. 3, pp. 637–651, 2022.

[13] M. Fadul, D. Reising, T. D. Loveless, and A. Ofoli, "Nelder-Mead simplex channel estimation for the RF-DNA fingerprinting of OFDM transmitters under Rayleigh fading conditions," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2381–2396, 2021.

[14] N. Xie, H. Tan, L. Huang, and A. X. Liu, "Physical-layer authentication in wirelessly powered communication networks," *IEEE/ACM Trans. Netw.*, vol. 29, no. 4, pp. 1827–1840, Aug. 2021.

[15] Y. Wang, J. Jin, Y. Li, and C. Choi, "A reliable physical layer authentication algorithm for massive IoT systems," *IEEE Access*, vol. 8, pp. 80684–80690, 2020.

[16] N. Zhang et al., "Physical-layer authentication for Internet of Things via WFRFT-based Gaussian tag embedding," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 9001–9010, Sep. 2020.

[17] 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.

[18] N. Soltanieh, Y. Norouzi, Y. Yang, and N. C. Karmakar, "A review of radio frequency fingerprinting techniques," *IEEE J. Radio Freq. Identification*, vol. 4, no. 3, pp. 222–233, Sep. 2020.

[19] H. Thapliyal and S. P. Mohanty, "Physical unclonable function (PUF)-based sustainable cybersecurity," *IEEE Consum. Electron. Mag.*, vol. 10, no. 4, pp. 79–80, Jul. 2021.

[20] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10250–10276, Oct. 2020.

[21] K. Huang, L.-X. Yang, X. Yang, Y. Xiang, and Y. Y. Tang, "A low-cost distributed denial-of-service attack architecture," *IEEE Access*, vol. 8, pp. 42111–42119, 2020.

[22] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for Online network intrusion detection," 2018, *arXiv:1802.09089*.

[23] Y. Tu, Z. Zhang, Y. Li, C. Wang, and Y. Xiao, "Research on the Internet of Things device recognition based on RF-fingerprinting," *IEEE Access*, vol. 7, pp. 37426–37431, 2019.

[24] J. Yu, A. Hu, G. Li, and L. Peng, "A robust RF fingerprinting approach using multisampling convolutional neural network," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6786–6799, Aug. 2019.

[25] A. Aghnaiya, A. M. Ali, and A. Kara, "Variational mode decomposition-based radio frequency fingerprinting of Bluetooth devices," *IEEE Access*, vol. 7, pp. 144054–144058, 2019.

[26] X. Wang, L. Kong, Z. Wu, L. Cheng, C. Xu, and G. Chen, "SLoRa: Towards secure LoRa communications with fine-grained physical layer features," in *Proc. 18th Conf. Embedded Netw. Sensor Syst.*, 2020, pp. 258–270.

[27] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, and I. Guvenc, "Detection and classification of UAVs using RF fingerprints in the presence of Wi-Fi and Bluetooth interference," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 60–76, 2020.

[28] W. Jian, Y. Zhou, and H. Liu, "Lightweight convolutional neural network based on singularity ROI for fingerprint classification," *IEEE Access*, vol. 8, pp. 54554–54563, 2020.

[29] L. Zong, C. Xu, and H. Yuan, "A RF fingerprint recognition method based on deeply convolutional neural network," in *Proc. IEEE 5th Inf. Technol. Mechatron. Eng. Conf. (ITOEC)*, 2020, pp. 1778–1781.

[30] Y. Li, Y. Lin, Z. Dou, and Y. Chen, "Research on RF fingerprint feature selection method," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, 2020, pp. 1–5.

[31] G. Bovenzi, G. Aceto, D. Ciuonzo, V. Persico, and A. Pescapé, "A hierarchical hybrid intrusion detection approach in IoT scenarios," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2020, pp. 1–7.

[32] B. Li and E. Cetin, "Waveform domain deep learning approach for RF fingerprinting," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, 2021, pp. 1–5.

[33] X. Guo, Z. Zhang, and J. Chang, "Survey of mobile device authentication methods based on RF fingerprint," in *Proc. IEEE INFOCOM IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2019, pp. 1–6.

[34] M. K. M. Fadul, D. R. Reising, and M. Sartipi, "Identification of OFDM-based radios under Rayleigh fading using RF-DNA and deep learning," *IEEE Access*, vol. 9, pp. 17100–17113, 2021.

[35] X.-Y. Liu and X. Wang, "Real-time indoor localization for smartphones using tensor-generative adversarial nets," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 32, no. 8, pp. 3433–3443, Aug. 2021.

[36] L. Yang, Y. Li, J. Wang, and N. N. Xiong, "FSLM: An intelligent few-shot learning model based on siamese networks for IoT technology," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9717–9729, Jun. 2021.

[37] L. Friedman and O. V. Komogortsev, "Assessment of the effectiveness of seven biometric feature normalization techniques," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2528–2536, Oct. 2019.

[38] D. Das and C. S. G. Lee, "A two-stage approach to few-shot learning for image recognition," *IEEE Trans. Image Process.*, vol. 29, pp. 3336–3350, 2020.

[39] S. S. Gill et al., "AI for next generation computing: Emerging trends and future directions," *Internet Things*, vol. 19, Aug. 2022, Art. no. 100514.