Performance Evaluation of a Novel Intrusion Detection System in Next Generation Networks

Keshav Sood, *Associate Member, IEEE*, Dinh Duc Nha Nguyen, Mohammad Reza Nosouhi, Neeraj Kumar, *Senior Member, IEEE*, Frank Jiang, Morshed Chowdhury, and Robin Doss, *Senior Member, IEEE*

***Abstract*—The integration of Internet of Things (IoT) with 5G simply creates additional threat landscape and any network infrastructure is more vulnerable. Severe attacks on networks potentially damage organization reputation, customers or tenants lose confidence, and impacts operational and maintenance cost. Intrusion detection systems (IDSs) are an effective approach to mitigate threats. We present a novel IDS mechanism in which the unique Radio Frequency (RF) features of IoT devices are used to create a learning model which is later used to identify the illegitimate devices in the network. Leveraging the Deep Autoencoder (DAE), the existing steady-state feature extraction is generalized. The performance evaluation is conducted using a real data set from different aspects including the mobility of the nodes. The proposed IDS is broken down into pluggable virtual network function (VNF) components and its evaluation is presented for its integration into the 5G network slicing ecosystem from the perspective of the European Telecommunications Standards Institute (ETSI) standards. A Proof of Concept (PoC) is presented using ETSI Open Source NFV Management and Orchestration (OSM-MANO) test bed, deployed on AWS cloud systems, to show how the proposed approach would fit in with a real-life MANO.**

***Index Terms*—5G security, deep learning, Internet of Things (IoT), intrusion detection, physical layer security.**

I. Introduction

5G TECHNOLOGY offers attractive opportunities for Internet of Things (IoT) service providers to offer flexible applications and services in many sectors [1], [2]. However, the wide adoption of 5G-IoTs, also considered as Next Generation Networks (NGNs) has increased the risk of cyber-attacks at an alarming rate [1]. To secure any network, Intrusion Detection Systems (IDSs) have been recognized as a fundamental and effective tool for intruder or anomaly detection [3]. We note that the existing IDSs have some key limitations. To better comprehend this, we divide the existing works (in IDSs) into two categories, a) traffic-based and b) Radio Frequency (RF) signature-based IDSs. Following this, key limitations are discussed. Table I shows the state-of-the-art of existing IDSs (in both categories) in cloud-based networks.

Category 1: The authors in [3] have proposed an approach using autoencoder with an IDS benchmark dataset. The accuracy to detect DDoS attacks is 99.65%, but the approach does not show consistent and highly accurate results to detect other attacks, for example the accuracy to detect Remote to User (R2L) is 7.14%. The work is not evaluated by utilizing a real-world NGN platform to demonstrate the merits of the model in this context. In [4], multi–level information on the monitored devices is collected using some tracing techniques. The data analysis is performed on a dedicated machine on the cloud. However, these techniques only work with the IoT devices that support the TCP/IP protocol stack, i.e., it suffers from the heterogeneity issue in terms of supported protocols. Moreover, the scheme is also not tested on any 5G (NGN) cloud environment to demonstrate how the proposal fits into a real NGN. In [5], a self-taught learning based SVM model is used for anomaly detection. Further, the authors in [6] explore the benefits of a stacked contractive autoencoder and SVM classifier approaches to realize the IDS's performance. The models are compared with the baseline autoencoder models using well known security datasets established two decades ago. The proposals are not feasible nor related to 5G core networks. Further, the trade-off between model training time and accuracy is not explored. Therefore, the proposal is not fully suitable for high speed cloud-based 5G-IoT networks.

Towards NGNs, [7] introduced a two-level Deep Learning based self-adaptive anomaly detection and cyber-defense system for 5G mobile networks in which traffic fluctuations are expected. The authors in [8] proposed a new architecture to detect flooding DDoS attacks at the source's side. The limitation of these works is that the computation is shifted to the control plane that may add additional end-to-end latency. Moreover, the loss precision metric is highly affected when a large variety of attacks are launched, i.e., where the general scale of data changes may impact key performance indicators of machine learning based models. Authors in [9] proposed an

Manuscript received 9 November 2022; revised 16 January 2023 and 31 January 2023; accepted 1 February 2023. Date of publication 7 February 2023; date of current version 9 October 2023. The associate editor coordinating the review of this article and approving it for publication was S. Scott-Hayward. *(Corresponding authors: Keshav Sood; Frank Jiang.)*

Keshav Sood, Dinh Duc Nha Nguyen, Mohammad Reza Nosouhi, Frank Jiang, Morshed Chowdhury, and Robin Doss are with the School of IT, Deakin University, Melbourne, VIC 3125, Australia (e-mail: keshav.sood@deakin.edu.au; nguyendinh@deakin.edu.au; m.nosouhi@deakin.edu.au; frank.jiang@deakin.edu.au; morshed.chowdhury@deakin.edu.au; robin.doss@deakin.edu.au).

Neeraj Kumar is with Thapar University, Patiala 146004, India, also with the School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, India, also with the Department of Electrical and Computer Engineering, Lebanese American University, Beirut 1102 2801, Lebanon, also with the Faculty of Computing and IT, King Abdulaziz University, Jeddah 21589, Saudi Arabia, and also with Chandigarh University, Mohali 140413, India (e-mail: nehra04@gmail.com; neeraj.kumar@thapar.edu; neeraj.kumar@lau.edu.lb).

Digital Object Identifier 10.1109/TNSM.2023.3242270

TABLE I
SUMMARY OF THE KEY EXISTING WORKS IN INTRUSION DETECTION SYSTEM

Year/Ref.	Domain: 5G (✓), Non-5G (X), Others specified	Model Used	Data Set	Edge Network	ETSI-NFV Compatibility	OSM MANO Orchestration: No Evaluation (X) Independent to each slice (✓), Centralized Evaluation (C)
2018, [3]	X	autoencoder	NSL-KDD, KDD Cup '99	X	X	X
2020, [4]	X	Decision Trees, Random Forest, Gradient Boosted Trees, LSTM	Real hardware, Multisensor 6 from AEOTEC a z-wave device	✓	X	X
2019, [23]	X	ANN	NSL-KDD, KDD Cup 99 UNSW-NB15	X	X	X
2020, [6]	X, cloud systems	autoencoder + SVM	NSL-KDD, KDD Cup 99	X	X	X
2018, [5]	X	autoencoder + SVM	NSL-KDD, KDD99	X	X	X
2019, [7]	✓	DNN, LSTM	CTU-13	✓	X	X
2019, [8]	✓	CART	-	X	X	X
2019, [9]	✓	DNN	AWID-CLS-R	X	X	X
2020, [10]	✓	CNN	CIC-IDS2018	X	X	X
2019, [12]	X	CNN	RF Signatures	✓	X	X
2019, [11]	X, IoT	ANN	RF Signatures	X	X	X
Our Scheme	✓ AWS Cloud platform	Autoencoder	RF Signatures	✓	✓	✓

IDS for a 5G and IoT network based on Deep Autoencoders (DAs) and its performance was evaluated using the benchmark Aegean Wi–Fi Intrusion dataset. The authors method was also compared with other recent solutions. The authors in [10] developed a Convolutional Neural Network model (CNN) using NAS (Neural Architecture Search) to detect malicious traffic in 5G networks.

Category 2: In [11], a learning–based authentication mechanism has been proposed based on the uniqueness of Radio Frequency (RF) features. The authors have used a supervised machine learning model to uniquely identify 10,000 different wireless devices and achieved 99% accuracy in their experiments. However, the deployed learning model has not been clearly discussed in the paper. This is a very notable omission since supervised machine learning models usually have poor classification performance in scenarios with many classes. In addition, they have not proposed a defense mechanism against replay attacks to show the effectiveness of the proposal against attacks. In [12], an RF signature-based intrusion detection approach is proposed. The data contains the traces of range of Signal-to-Noise ratio (SNR) to ensure the robustness of the approach using a CNN model. Recently, the authors in [13] determined that the unintentional Electromagnetic Emission (EM) from electronic devices may pose a serious security threat, particularly leading to a side channel attack. Researchers, for this anomaly detection in the RF spectrum (or EM emission filtration) used Savitzky-Golay filter and compared the outcome with a prior emanation profile of these devices to determine rogue devices in a network environment. The comparison of their results based upon temporal-analysis with the existing work has solid results which then becomes the base of the emission security domain. Currently we believe that by using AI methods the work can be further enhanced and applied in the autonomous trust calculation or enhancement in zero trust architecture domain.

We have identified key limitations in both of these categories. Firstly, the existing IDSs are not efficient for intrusion detection in NGNs, for example, Snort is a popular Deep Packet Inspection (DPI) tool that is able to work effectively on transmission rates up to 1 Gbps but it starts to discard packets from 1.5 Gbps [14] while 5G delivers transmission rates up to 10 Gbps. Further, a) the existing works do not fully consider the high level of heterogeneity which adversely impact the security solutions, means the heterogeneity in IoT stands in the way of achieving good security [15], b) the existing works have used decade old data sets which lacks the NGN's features as well as the modern footprint attack style, c) lack of modern 5G traffic features/scenarios, and the training and testing sets have different distributions, d) the existing schemes are not rigorously tested on real NGN (example 5G) test beds using real 5G data sets.

Note that the use of heavy virtualization is evident in almost all sectors including cellular networks. The European organization ETSI is developing requirements and architecture for virtualization for various functions within telecoms networks. From our literature synthesis, we have not identified any existing works with fully tested approaches using ETSI-NFV standards. This evaluation is important to capture the difficulty of deploying novel IDSs into a real-life cloud based next generation architecture to get a sense of realism of solutions in real-life. Hence, we reiterate that a lightweight IDS solution is needed for NGNs, which is a great challenge.

Motivated from these limitations, our proposal fully accounts for and considers these gaps and requirements. We propose a novel RF signature-based IDSs for NGNs using the unique physical layer features of IoT nodes, due to the inconsistencies in Transmitter (Tx) manufacturing process, of legitimate IoT wireless devices to recognize an intruder device. This feature uniqueness is due to the nonideality of Radio Frequency (RF) circuits in the Tx module of IoT wireless

devices. These are considered as inherent RF properties of Tx modules known as *RF signature* of a Tx module in the literature [11], [16], [17], [18]. It is caused by the inconsistencies in Tx manufacturing processes which is almost unavoidable (or at least very expensive to be avoided) [11], [19], [20]. However, this has no negative impact on the performance of a Tx module if it complies with the specifications of the relevant wireless standard, and it will be compensated at the receiver circuit (Rx). We embrace the nonideality of Tx modules and develop a Deep Autoencoder (DAE) model to learn the RF signature of legitimate IoT devices in the network.

The proposed IDS resides in a network slice of 5G network. The network slice has its own independent Management and Orchestration (MANO) unit through which each tenant can manage the security of its own slice [21]. Thus, a RF signature-based DAE model is developed in our proposal, and it is managed by the independent MANO unit of a network slice at the core segment of the 5G-IoT network. This is done with the collaboration of IoT gateway/edge computing devices that have direct radio communication links to the IoT wireless devices and can extract their RF signature.

The contributions of this paper are as follows:-

- We propose a deep learning based novel IDS mechanism which leverages the Radio Frequency features of IoT devices to identify legitimate devices in networks. Using a real data set, the proposal is compared with two recent approaches. We have further evaluated the impact of nodes mobility on the proposed IDS's performance.
- The proposed IDS is broken down into pluggable Virtual Network Function (VNF) components. The high level framework and its evaluation is presented for its integration into the 5G network slicing ecosystem from the perspective of the ETSI standards. The PoC implementation and evaluation, using OSM-MANO, is presented. This is to capture the difficulty of trying to integrate as well as to show the relevant aspects of deployment challenges of the approach in virtualized environments.
- The security analysis of the proposal is presented to validate its effectiveness from the replay attacks which are common in cloud systems. We propose a novel solution that makes the malicious replay efforts unsuccessful. The proposed solution makes it infeasible for a malicious device to reuses the RF signals of legitimate devices (obtained through eavesdropping attempts) to get access to the network.

Recently, RF signature-based security solutions are gaining wide attention since the existing security solutions are power-hungry and take significant power consumption and overhead [22]. Whereas the IoT devices are resource-constrained and do not fully support the onboard security solution implementation, hence it impacts the operation of low latency requirements and power-hungry applications in NGNs. Conversely, PUF solutions consume significantly less energy than expensive cryptography hardware [11]. Hence, NGN-IoTs can significantly benefit from PUF-based IDS as radio frequency signatures of each node are analyzed and stored in gateway or secure server which eventually alleviates the need of traditional key-based security solutions in many scenarios.

II. Background and Related Work

RF signatures-based IDS: Our solution lies in the second category (RF signature-based IDS). Note that we do not advocate that the network based IDSs (category 1) are not effective, rather we have listed both categories and provided common key limitations. This clearly emphasized the gap in both categories. However, the RF signatures-based solutions have certain advantages over network based IDSs. RF signatures are the digital radio fingerprints of any physical device (including IoT) that serves as a unique identifier. The unique physical variations (example mentioned in Section I) occur naturally during semiconductor manufacturing of a device which typically can be used in applications with high security requirements. These RF features are Physically Unclonable Function features (PUF) which are robust (stable over time), unique (means no two PUFs are the same), easy to evaluate (to be feasibly implemented), extremely difficult to replicate (so the PUF cannot be copied) and very difficult or impossible to predict (extremely costly) [22], [24], [25].

5G Network Slicing and ETSI-NFV: In 5G, network slicing is an essential component that can be seen as a network configuration which allows multiple virtualized networks to be created on top of a common physical infrastructure. The virtual networks can be controlled independently by an independent management and orchestration such as Open Source NFV Management and Orchestration (OSM-MANO). Each sub-network (or virtualized sub-network) can be leased to mobile virtual network operators, they can further split the allocated sub-virtual network into more specific sub-networks, eventually to enable distinct end-to-end network services in an independent manner. It significantly reduces the heterogeneous network management complexities. To effectively enable the multiplexing of virtualized and independent logical networks the ETSI-NFV group within ETSI, is developing requirements and architecture for virtualization for various functions within telecoms networks, [26], [27].

Previous Research Works: There are some works (other than presented in Table I) given in [28], [29], [30], [31] in which a signature is defined for every known attack. When a suspicious network or system behavior is detected (for network–based and host–based IDSs, respectively), an alert is triggered if the suspicious behavior is matched with the signature of an attack. This technique is usually an accurate and effective approach for detecting known attacks. However, it is ineffective to detect new attacks since no signature is available for them. In [32], [33], [34], a profile of normal network activities is defined as a reference and any deviation from this normal behavior generates the alert. Although this approach is effective in the detection of new attacks, it may result in high false positive rates [35]. This is a result of the high level of complexity in defining a profile of normal network activities. Thus, in case of selecting a tight threshold, any network activity that

does not completely match the normal profile is regarded an intrusion [35].

Further, in [36], [37], [38], predefined specifications (sets of rules and profiles that determine the normal network behavior) are used by the system to detect any anomaly. Here, the rules and profiles in the specifications are manually defined by a human expert. This results in better performance (lower false positive rates). However, these approaches may not be effective in highly dynamic network environments and is prone to human faults and errors. In addition, it can be a time–consuming process to manually generate the specifications [36]. Finally, there are some hybrid approaches that may utilize some positive features of the signature–based, anomaly–based, and specification–based methods to increase their effectiveness and limit the weaknesses [39], [40].

However, the solutions based on this approach are mostly too complicated with additional computation overheads [35], [40]. Moreover, in some cases, they result in low accurate intrusion detection or high false positive rates which makes the reliability of IDS doubtful [39].

Novelty and Originality: Our work presents an Intrusion Detection System (IDS) in which the unique radio frequency (RF) features of IoT devices are used to create a learning model which we have used to identify the illegitimate devices in the network. We have compared our work with [11] and [41] and the base of our work is [11]. We would like to emphasize that [11] introduces a device authentication mechanism while our work presents an intrusion detection system. Although in both works, the uniqueness of RF features of different Tx modules is utilized, in [11] the introduced model focuses on the identification (recognition) of many legitimate devices (i.e., authentication). However, our model proposes a mechanism to identify an illegitimate device (i.e., an intruder) among legitimate devices. This has led us to develop an anomaly detection model using Deep Auto Encoders (DAEs) while in [11] a classification model (ANN) has been developed. In fact, we have developed an unsupervised model to achieve the anomaly detection target (i.e., a binary classification model that classifies devices to either legitimate or illegitimate classes) while in [11] a model has been developed to recognize the identify of each device (i.e., multi-class classification). Thus, our model suits those scenarios in which the recognition of device identity is not important, but the detection of intruder devices is critical (it can be deployed on top of a traditional authentication mechanism to increase the overall security).

In addition, in our work, we provide an approach for integration of the proposed IDS into standard 5G networks, it is broken down into pluggable virtual network function (VNF) components. In this regard, a framework and its evaluation are presented in the manuscript for IDS integration into the 5G network slicing ecosystem from the perspective of the European Telecommunications Standards Institute (ETSI) standards. To further strengthen the novelty and then the evaluation part, we have used a real data set and again compare our work with [11] and [41]. Additionally, experiments are added to show the impact of the mobility on the performance of the proposed IDS.

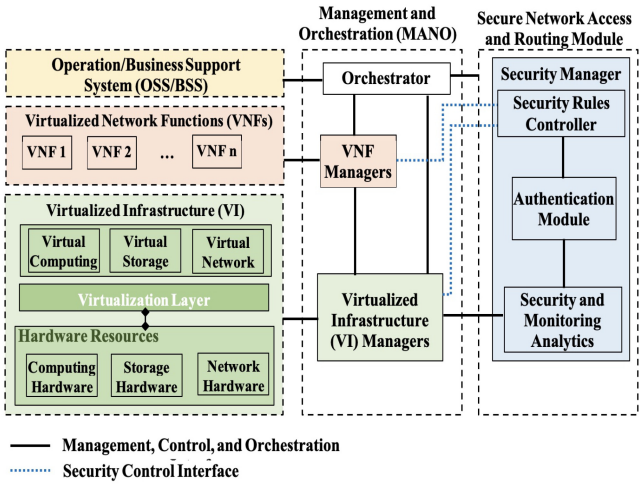

Fig. 1. Integration of the proposed IDS mechanism into the ETSI NFV standard architecture used in 5G networks.

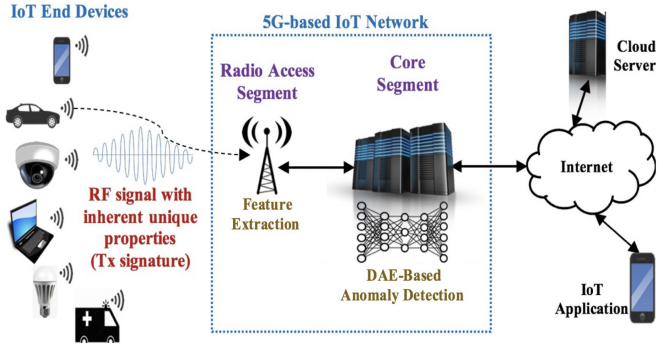

Fig. 2. A high level architecture of the proposed approach.

III. The Proposed IDS Mechanism

We propose that the proposed IDS is a VNF module in ETSI architecture as illustrated in Fig. 1. A high level view of our proposed IDS approach is shown in Fig. 2. We consider that the RF signals with inherent unique properties, also known as Tx signatures, are received by the feature extraction module which resides at RAN segment (or Radio Access Network) of the 5G network. We emphasize that this Tx signature is unclonable. Now, this feature extraction module performs the real-time features extraction (from RF signals) of wireless IoT devices. The extracted features are then used to train a Deep Learning model so that the model learn these unique RF features of the legitimate devices in the network, eventually to distinguish legitimate and non-legitimate IoT node. This is comprehensively discussed in Section III-D. Now, in the following literature, we discuss the feature selection module in detail as well as present the proposed *Feature Extraction (FE)* module. Following this, we introduce our DAE–based *Anomaly Detection (AD)* module for feature analysis and detection of intruder devices. Finally, we present the fundamental framework required to integrate the proposed modules into the standard ETSI framework or architecture of 5G networks.

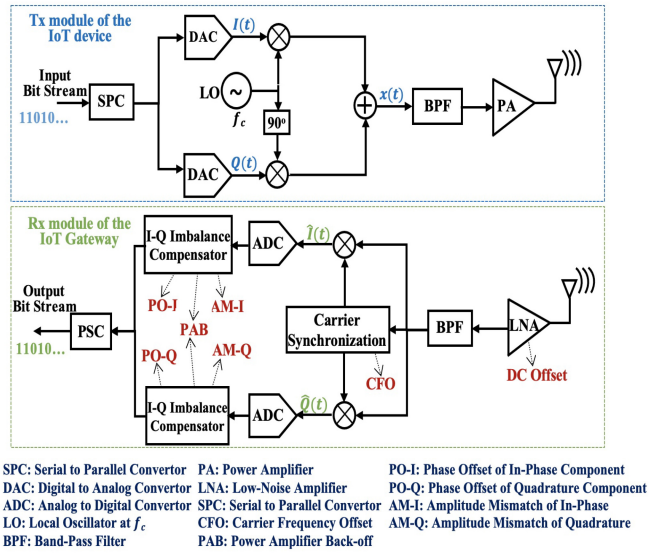

Fig. 3. The feature extraction procedure.

A. Feature Extraction (FE) Module

A high level feature extraction process is shown in Fig. 3. This module performs the real–time features extraction of wireless IoT devices from their received RF signals. Generally, two different techniques for RF feature extraction have been used in the previous research works in the field of RF fingerprinting. These are (1) transient signal analysis and (2) steady–state feature extraction, in which the RF features are extracted from the transient and steady–state parts of the received signal, respectively. The transient segment of a signal starts immediately after the transmitter is powered on and lasts for a very short period of time (e.g., in the range of μ *sec*). This is actually the period during which the output of hardware components of the transmitter (e.g., modulator, power amplifier, etc.) make the transition to their steady–state level. After this period, the transmitter is ready to send the data which is the start of steady–state segment of the RF signal. Although feature extraction from the transient part of the signal results in high identification accuracy (due to the high level of uniqueness in the extracted features) as well as a high level of security, it needs the received signal to be sampled at very high rates [11]. Moreover, in this approach, the beginning and end points of the transient segment should be accurately identified. These requirements make the required hardware for feature extraction complicated and expensive.

The steady–state feature extraction approach does not suffer from these issues. However, it is dependent on the data being sent. In fact, in different data transmissions (with different data) the extracted features may slightly change. This degrades the overall performance in terms of accuracy. To address this issue, the wireless device needs to send (predefined) preamble signals along with the data to enable the detection module at the receiver side to identify the device. In fact, in this method, the features are extracted and analyzed based on the knowledge of the preamble signal sent by the device. In other words, the extracted features are compared with a precalculated set of features that are expected to be extracted from the signal of a specific device.

However, this technique (sending preamble signals) causes two issues. First, it may result in security vulnerabilities since a wireless device might be impersonated through conducting a replay attack. In addition, it needs some changes in the Tx module to perform the preamble transmission at specific times. Moreover, each standard wireless transmission protocol has its own form of preamble signal which results in implementations of the feature extraction module. This prevents the authentication solution to be independent of the transmission protocol at physical layer. As a result, the preamble–based solutions are inefficient for large scale IoT networks with heterogeneous resource–constraint IoT devices. To address this issue, we can remove the need of preamble transmission by deploying a learning–based detection model (instead of a deterministic model) and train it with a sufficient number of feature sets resulted from sending different bit streams. In fact, the detection model learns the possible sets of features (as many as required to achieve an acceptable detection accuracy) based on different data streams transmitted by the wireless device. This makes the detection performance independent of the data that is being transmitted.

In conclusion, we have adopted a steady–state feature extraction approach in which the need of preamble transmission has been eliminated (by deploying a Deep Learning–based anomaly detection method). To perceive the feature extraction procedure, we have considered an IoT device (equipped with a digital radio transmission system) that is transmitting data to a wireless IoT gateway, as shown in Fig. 2. At the Tx side (considering a QAM modulation/demodulation system), the flow of input data is first applied to a serial to parallel converter (SPC). Then, two separate Digital to Analog Converters (DACs) receive the two parallel bit streams to form the in–phase ($I(t)$) and quadrature ($Q(t)$) components of the modulating signal. These components modulate the two relevant carrier signals that have same frequency but out of phase with each other by 90° (i.e., $Sin2\pi f_c t$ and $Cos2\pi f_c t$). The modulated signals are then added together to create $x(t)$ which is filtered, amplified, and transmitted. The orthogonality of the two carrier signals enables the demodulator circuit (at the receiver (Rx) side) to easily separate them and obtain the I and Q components. So far, the wireless IoT device just performs its normal (routine) procedures in sending the data to the IoT gateway, i.e., it does not need to collaborate with the gateway's Rx module for the fulfilment of feature extraction process (e.g., transmitting a preamble signal).

At the Rx side, DC Offset is the first feature that can be extracted by means of the capacitor coupled Low Noise Amplifier (LNA). Then, using the local carrier synchronization unit, the Carrier Frequency Offset (CFO) feature of the Tx local oscillator can be measured [42]. This unit adjusts the frequency of local oscillator (applied to the mixers) based on the frequency of the received signal. This is done to compensate the effect of CFO in the receiver circuit. Note that in this case, we need to have a very accurate reference clock to be able to measure CFO with the required resolution.

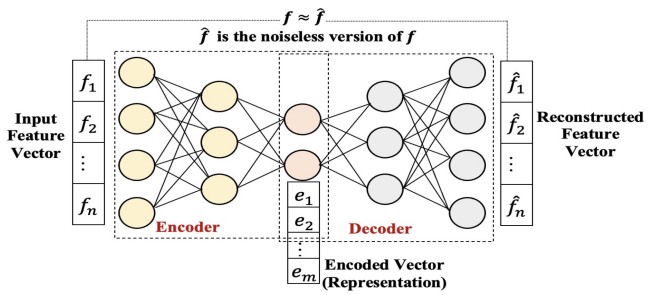

Fig. 4. General Architecture of a Deep Autoencoder.

In the next stage, using the I–Q imbalance compensator unit, the phase offset and amplitude mismatch in the in–phase and quadrature components of the baseband signal can be obtained. These features are unique for every transmitter and can be effectively used in device identification [11], [20]. Power Amplifier Back–off (PAB) is another feature that can be extracted at this stage. It is caused when the power amplifier in the Tx module is driven with a voltage that is high enough to saturate the output (i.e., the amplifier enters the non–linear region of its operation). This feature can be obtained through I–Q baseband imbalance measurements.

We reiterate that 1. Carrier Frequency Offset (CFO) is one of many non-ideal conditions, invoked due to channel noise conditions, which impacts the baseband receiver design. This primarily occurs when the local oscillator signal for down-conversion in the receiver does not synchronize with the carrier signal contained in the received signal as a results the frequency of the received signal deviates. As per the IEEE 802.11 WLAN standards the oscillator precision tolerance is specified to be less than ± 20 ppm. 2. I-Q Features (In-Phase and Quadrature) are from the angle modulation which is decomposed into two amplitude modulations typically I-component (in-phase) and Q-component (quadrature signal). These high-frequency carrier signals is amplitude-modulated by a relatively low-frequency function, which normally conveying some information. In general there is a constant phase difference, ϕ, between any two carriers, so I-component means $\phi(t) = 0$, whereas Q-component means $\phi(t) = \frac{\pi}{2}$.

Finally, the measured features (in the form of a vector) are applied to the DAE–based AD module (described in the next section) for the real–time detection of anomaly.

B. Anomaly Detection (AD) Module

The target of deploying this module is to find out that (with high probability) the RF features (extracted by the FE module) are associated with either a legitimate IoT device or an intruder. This is done through developing a Deep Learning model which is trained to learn the unique RF features of the legitimate devices in the network. General architecture of DAE is shown in Fig. 4. Since in 5G networks, each network slice has its own security manager (operated by its own tenant), as proposed in [21], an AD module serves a single network slice. It learns the features of all the IoT devices that are taking 5G network service from the relevant tenant as shown in Fig. 5. This makes our approach compatible to the standard architecture of 5G networks.

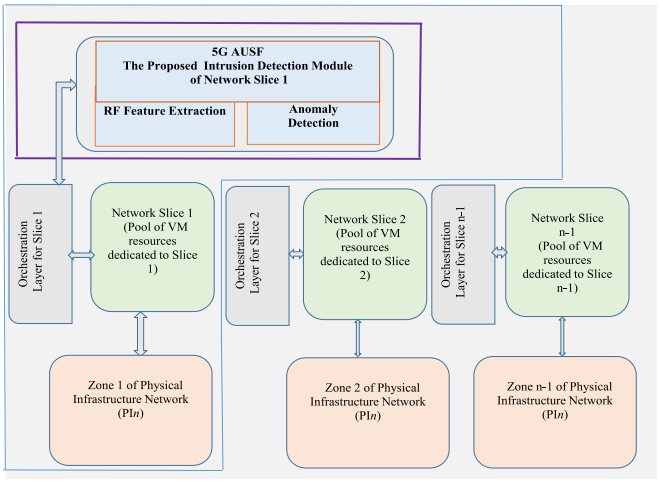

Fig. 5. A high-level framework of the proposed slice-specific node authentication strategy in virtualized environments.

The other benefit of deploying a learning model is that it eliminates the need of preambles (i.e., predefined fixed bit streams) in the received RF signals. As discussed in Section III-A, in the steady–state RF fingerprinting mechanisms, the wireless device needs to send a preamble before sending the data. This enabled the detection module (at the receiver side) to compare the RF features (after extraction from the received signal) with the expected (precalculated) values. This is indeed a significant advantage of our method because the wireless IoT devices do not need to collaborate with the intrusion detection module, i.e., they just follow their own routine procedures. Thus, no hardware/software change or update is required at the IoT devices. In addition, deploying a learning–based detection module makes the system resilient against the changes in RF features of individual devices. These changes may occur due to several reasons such as change of environmental parameters (e.g., temperature), channel conditions, battery voltage, etc. All these changes can be considered during the model training phase to increase the detection accuracy.

In the design of AD module, we have deployed a Deep Autoencoder (DAE) as the core of our learning model. DAEs are a type of Artificial Neural Networks (ANN) that are known as an effective approach to perform anomaly detection in an unsupervised manner. The main idea behind DAEs is that they train a network of neurons to remove noise from the input data vectors. In fact, the weight and bias parameters of the neurons are calculated in such a way that a reconstructed version of the input vectors is obtained at the output in which noise has been removed, as seen in Fig. 4. This enables them to recognize the original (normal) data vectors even if they have been contaminated by different sets of random noise values. To do this, a DAE employs two separate networks of neurons, i.e., an encoder and a decoder. The encoder part performs the dimensionality reduction process while the decoder

is used to reconstruct the input vector from the encoded vector. In fact, during the training phase, the reconstructed vector is repeatedly compared with the input vector to minimize the error (dissimilarity) between them. In other words, a DAE learns the optimum values for the weights and biases of neurons such that the error is minimized. The number of neurons at the output layer of the decoder network is always equal to the number of neurons at the input layer of the encoder because the reconstructed vector should have the same dimension as the input vector. In the following literature, we have presented the mathematical model of the AD module.

C. Mathematical Analysis

Consider $\mathbf{F} \in \mathbf{\Omega}$ as the set of training vectors $\mathbf{f}^i = \{f_1, f_2, \ldots, f_n\}$ where $\mathbf{\Omega}$ is the whole space of *n*–dimensional feature vectors. If $\lambda_{\boldsymbol{\alpha}_e} : \mathcal{R}^n \rightarrow \mathcal{R}^m$ and $\lambda_{\boldsymbol{\alpha}_d} : \mathcal{R}^m \rightarrow \mathcal{R}^n$ are the encoding and decoding functions, respectively, we have

$$\mathbf{e}^i = \lambda_{\boldsymbol{\alpha}_e}\left(\mathbf{f}^i\right) \tag{1}$$

$$\hat{\mathbf{f}}^i = \lambda_{\boldsymbol{\alpha}_d}\left(\mathbf{e}^i\right) = \lambda_{\boldsymbol{\alpha}_d} \circ \lambda_{\boldsymbol{\alpha}_e}\left(\mathbf{f}^i\right), \tag{2}$$

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 $\mathbf{E} \in \mathbf{\Omega_e}$ shows the set of encoded vectors where $\mathbf{\Omega_e}$ is an *m*–dimensional feature spaces ($m < n$). $\boldsymbol{\alpha}_e$ and $\boldsymbol{\alpha}_d$ are parameters of the encoder and decoder functions, respectively [43].

Now, assume there is an unknown probability distribution γ defined over $\mathbf{\Omega}$. Given ϵ 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 $\boldsymbol{\alpha}_e$ and $\boldsymbol{\alpha}_d$ such that the expected value of the dissimilarity function ϵ is minimized, i.e.,

$$\begin{aligned} &\min_{(\boldsymbol{\alpha}_e, \boldsymbol{\alpha}_d)} \mathbb{E}_{\left(\mathbf{f}^i, \hat{\mathbf{f}}^i\right) \sim \gamma}\left(\epsilon\left(\mathbf{f}^i, \hat{\mathbf{f}}^i\right)\right) \\ &= \min_{(\boldsymbol{\alpha}_e, \boldsymbol{\alpha}_d)} \mathbb{E}(\epsilon(\mathbf{f}_i, \lambda_{\boldsymbol{\alpha}_d} \circ \lambda_{\boldsymbol{\alpha}_e}(\mathbf{f}_i))) \end{aligned} \tag{3}$$

Because the probability distribution γ 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.,

$$\min_{(\boldsymbol{\alpha}_e, \boldsymbol{\alpha}_d)} \epsilon\left(\mathbf{f}^i, \hat{\mathbf{f}}^i\right) = \min_{(\boldsymbol{\alpha}_e, \boldsymbol{\alpha}_d)} \sum_{j=1}^{n} \epsilon\left(f_j, \lambda_{\boldsymbol{\alpha}_d} \circ \lambda_{\boldsymbol{\alpha}_e}\left(f_j\right)\right) \tag{4}$$

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 $\lambda_{\boldsymbol{\alpha}_e}$, $\lambda_{\boldsymbol{\alpha}_d}$, and the dissimilarity function ϵ. Moreover, applying additional constraints such as regularization can change the type of autoencoder [44]. For example, if MSE is selected as the dissimilarity function, for the autoencoder problem we have

$$\begin{aligned} \min_{(\boldsymbol{\alpha}_e, \boldsymbol{\alpha}_d)} \epsilon\left(\mathbf{f}^i, \hat{\mathbf{f}}^i\right) &= \min_{(\boldsymbol{\alpha}_e, \boldsymbol{\alpha}_d)} \frac{1}{n} \sum_{j=1}^{n} \left(f_j - \hat{f}^j\right)^2 \\ &= \min_{(\boldsymbol{\alpha}_e, \boldsymbol{\alpha}_d)} \frac{1}{n} \sum_{j=1}^{n} \left(f_j - \lambda_{\boldsymbol{\alpha}_d} \circ \lambda_{\boldsymbol{\alpha}_e}\left(f_j\right)\right)^2 \end{aligned} \tag{5}$$

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 [45]. 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 [46].

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

$$\boldsymbol{\alpha}_e^{(k+1)} = \boldsymbol{\alpha}_e^{(k)} - \eta^{(k)} \nabla_{\boldsymbol{\alpha}_e} \epsilon_i\left(\boldsymbol{\alpha}_e^{(k)}\right) \tag{6}$$

$$\boldsymbol{\alpha}_d^{(k+1)} \quad \boldsymbol{\alpha}_d^{(k)} - \eta^{(k)} \nabla_{\boldsymbol{\alpha}_d} \epsilon_i\left(\boldsymbol{\alpha}_d^{(k)}\right) \tag{7}$$

where $\nabla_{\boldsymbol{\alpha}_e} \epsilon_i(\boldsymbol{\alpha}_e^{(k)})$ and $\nabla_{\boldsymbol{\alpha}_d} \epsilon_i(\boldsymbol{\alpha}_d^{(k)})$ are the gradients taken using $\boldsymbol{\alpha}_e$ and $\boldsymbol{\alpha}_d$, respectively (considering a training sample $\mathbf{f}^i$). η 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 η results in faster training but at the risk of missing the optimum values (loss in accuracy). On the other hand, a smaller η makes the convergence of algorithm slower. When the optimization problem is solved, parameters $\boldsymbol{\alpha}_e$ and $\boldsymbol{\alpha}_d$ are obtained. This means that the autoencoder model has been built and vectors $\hat{\mathbf{f}}^i = \lambda_{\boldsymbol{\alpha}_d} \circ \lambda_{\boldsymbol{\alpha}_e}(\mathbf{f}_j)$ can be obtained as the reconstructed vectors [45].

D. Integration With 5G Networks

We consider 5G-IoT as use case of NGNs. In 5G, virtually isolated slices of the network are allocated to Mobile Virtual Network Operators (MVNOs). We assume that every slice is managed by its own orchestration module, this is in line to the existing research work shown in [15], [21]. Regarding security, the slice's orchestration module coordinates the 5G

Algorithm 1 The Proposed Mechanism

Inputs: d_i (address of the ith legitimate IoT device)
n (number of features)
e_{thr} (error threshold)
Output: $R \in \{$"*Authorized Access*", "*Unauthorized Access*"$\}$
1: $\mathbf{f}(d_i, t)$ =*FE_VNF*(d_i)
2: $\hat{\mathbf{f}}^i$ =*AD_VNF*$(\mathbf{f}(d_i, t))$
3: $error = \Delta(\mathbf{f}(d_i, t), \hat{\mathbf{f}}^i) = \frac{1}{n}\sum_{j=1}^{n}(f_j(d_i, t) - \hat{f}_j^i)^2$
4: **if** $error \leq e_{thr}$:
return "*Authorized Access*"
else:
return "*Unauthorized Access*"

Authentication Server Function (AUSF) IoT node authentication module (our IDS mechanism) as shown in Fig. 5. In this approach, each part/module of the our IDS mechanism is performed through invoking one or multiple Virtual Network Functions (VNFs for RF feature extraction and Anomaly detection). These VNFs are managed and customised by the slice's orchestration manager. Using this approach, our proposal not only receives (automatically) the benefits of the standard ETSI framework/architecture of 5G networks, but also it becomes a practical solution due to the following key reasons.

- Network slices are virtually isolated and might be managed by different entities. Thus, considering the differences in security policies of different tenants, it is wise decision to perform any field–based IDS mechanism using a per–slice method.
- The tenant of a slice is the appropriate entity that can make necessary interactions with end users to collect and store the hardware features of users' IoT devices (when they join the network for the first time) to train and update the learning model used in the AD module.
- Regarding the application domain, the proposed approach enables the network provider to offer the authentication service to IoT applications and cloud–based services (e.g., in the form of a multi factor authentication mechanism). Moreover, it is much easier to manage and handle the device authentication requests (received from IoT applications with different security requirements) using a slice–based approach.
- In terms of scalability, this approach offers a high level of efficiency because the task of authenticating a huge number of IoT devices is shared between individual learning models (in a distributed way) that are run by different slices. As a result, the learning model used in the AD module does not need to learn the features of all the IoT devices in the network. This makes the models more agile and efficient in terms of processing, storage, and power overheads. This is indeed a significant advantage for an IDS solution in large–scale 5G–based IoT networks.

Therefore, whenever an IoT device needs to be authenticated, the slice's orchestration layer/manger performs the IDS mechanism by invoking the relevant VNFs. In this regards, it first invokes *FE_VNF()* that extracts and returns the real–time RF features of the device, as seen in Algorithm 1. As explained in Section III-A, this is done through the associated IoT gateway/edge device that has established a direct wireless link to the device. Upon receiving the real–time extracted features, the security manger invokes the *AD_VNF()* which performs the anomaly detection procedure explained in Section III-B and III-C. In addition to *FE_VNF()* and *AD_VNF()*, a number of other VNFs should be defined to handle the other procedures of our approach. For example, *FE_ND_VNF()* is invoked when a new device is joining to the network. Note that the feature extraction process done in such cases is more comprehensive than what is done by *FE_VNF()*. In fact, the RF features of a new device should be extracted and learned in different ways, e.g., using different bit streams, levels of transmission power, etc. As discussed in Section III-A, this is done to make the AD module (1) a preamble–less detection method and (2) resilient to unavoidable situations regarding the possible changes in the condition of communication channel, environment, level of transmission power, etc.

Overall, some other key benefits of our proposal are: (1) Interestingly, it does not require any additional hardware at the Tx side. Thus, it results in no (zero) computation/communication overhead on the resource–constrained IoT nodes. In fact, the computation load required to perform the intrusion detection procedure is completely transferred to the IoT gateway/edge computing devices and deep learning server. (2) It works with any Tx module/wireless protocol at the physical layer. It is also independent of the protocols that are related to upper layers. Thus, the heterogeneity issue of 5G–based IoT systems does not degrade its performance. (3) It is well suited for slice–isolated 5G–based IoT networks and can be effectively integrated into the standard architecture of 5G networks as shown in Fig. 1. (4) It enables network providers to offer the authentication service to IoT applications and cloud–based services (e.g., in the form of a multi–factor authentication mechanism).

E. Alignment of This Proposal With Current Industry Standards (3GPP and GSMA-IoT SAFE)

The proposed research work shown in this paper is in the domain of IDSs. A high level framework is presented and the integration of the proposed novelty into the 5G network slicing is discussed. The focus of this work is on the deep learning model used which is based on the RF feature extraction (of wireless IoT node). It is arguable to prove that the work shown here is aligned with the recent industry standards such as 3GPP and GSMA-IoT SAFE. We emphasize that the proposed work aligned with the 3GPP (3rd Generation Partnership Project) standards which defines the mobile telecommunication technologies.[1] 3GPP gives guidelines for global standard designs for interfaces of 5G networks. There are six different working groups (WG) (within security) in 3GPP called the Technical Specification Group Service and System Aspects (TSG SA). The principal aim of 3GPP TSG SA WG3 (SA3) is to define the requirements and specify the architectures and protocols for security and privacy in 3GPP systems. SA3 defines the architectures and protocols for security systems for IoT and

[1]https://www.3gpp.org/specifications-groups

vertical industries while SA5 is responsible for management, orchestration, network slicing, etc.

We emphasize that the proposed architecture and its functioning is aligned with both (SA3 and SA5) the SA working groups. The approach delivers a physical security solution for IoT devices in 5G networks. The proposed IDS scheme leverages the physical RF (radio frequency) signatures/characteristics of wireless IoT nodes as the unique and unclonable identifiers which are used for the authentication processes to grant access rights to legitimate devices and prevent cyber security attacks such as impersonate or replay attacks. Further, we note that the working group SA5 studies network slicing which is a critical element of 5G networking since it enables vertical IoT industries to effectively and flexibly utilize 5G networks and services. The concept of network slicing allows a single network to a network where logical partitions are created to support various types of services depending on customers' needs. Therefore, the network slicing instances are commissioned and decommissioned frequently; this life-cycle raises a challenge for authentication processes. The proposed approach, which concentrates on authorizing IoT devices, overcomes the issue by separating authentication actions with the network slicing life-cycle while ensuring the access control. Furthermore, the architecture can easily be integrated with other 5G Core Access components such as AMF (Access and Mobility Management Function). The AMF handles the connection and mobility management tasks in 5G networks. It means our proposal must ensures the authentication of legitimate devices under roaming scenarios. The proposed approach assists the AMF abilities by authorizing mobility devices and informing AMF and SMF (Session Management Function) as the proposed approach resides or part of each network slice (see Fig. 5). We believe that the proposed approach is consistent with 3GPP 5G standards.

The proposed approach also aligns with GSMA-IoT SAFE (GSMA IoT Security Guidelines),[2] (IoT SIM Applet For Secure End-2-End Communication) standards. The IoT SAFE provides the IoT end-to-end security solution by leveraging SIM as a *Root of Trust*. In the IoT SAFE, a SIM is embedded with a digital certificate to support TLS/(D)TLS protocol for establishing secure communication channels between devices and cloud servers. We note that both the SIM and IoT devices are resource constraints, thus the IoT devices are vulnerable to cyber-attacks. Adversaries can attack the devices and steal digital certificates. Moreover, TLS certificates technology also has weaknesses due to certificate store poisoning or Certificate Authorities attacking scenarios. Our approach can be considered as the multi-authentication solution to the IoT applications. It maintains the end-to-end security as well as improves the *'Root of Trust'* of the IoT SAFE standards.

It does not only secure the communication between the IoT devices and cloud servers but also authorizes the IoT devices in the sessions. For instance, in case a hacker can attack an IoT device and gain access to the digital certificate stored on that device, they might pass the TLS security protocol, but they face the security gate of the proposed approach. In the proposed approach, the physical RF characteristics are extracted for authentication solutions. It is almost impossible to mimic the hardware properties to perform impersonate attacks. As a result, the integration between IoT SAFE and the proposed approach enhances the end-to-end, chip-to-cloud security solution as the needs of enterprises. Moreover, the authentication process of the proposed approach does not interfere with any abilities of the IoT SAFE. The security captures the physical features of IoT devices from the receiver side and executes the authorization. So, the actions do not cause any conflicts or impacts to the IoT SAFE procedures. Overall conceptually we again emphasize that the proposed approach aligns with both the 3GPP as well as the GSMA-IoT SAFE security design guidelines.

[2]https://www.gsma.com/iot/iot-safe/

IV. Performance Evaluation

In this section, we have evaluated the performance of our scheme in the detection of illegitimate wireless IoT devices in the network. We have firstly presented the setups of our experiments and discussed the method we have used to create the dataset of device features for the training of AD module. Then, we have presented the results of our experiments.

A. Setup

For our experiments we use Intel Core i5, 2.3GHz CPU with 8GB of RAM. We used the Wireless Waveform Generator toolbox of MATLAB to generate RF signals based on random bit streams of data. This has enabled us to create a dataset in which the RF features of 100 wireless devices have been collected. For every device, we have slightly changed the frequency, phase, and DC parameters of the waveform generator to model the nonideality of RF circuits in the Tx modules. In addition, we have changed the signal to noise ratio (SNR) parameter to consider the effects of channel situation in our dataset. Regarding the input data, we have created a file of size 1 MB consisted of pseudo–random bits (generated by the *random* module of Python) and applied the file to the wireless waveform generator module to generate the RF signals for each device. This makes the AD module independent of the input bit stream, i.e., it learns the features of a device from a variety of RF signals generated based on a sufficient number of random input bit streams. As we have discussed in Section III-B, this eliminates the need of preambles in the input bit streams which is an advantage of our proposal. Moreover, changing the SNR parameter enables the AD module to learn the features under different channel circumstances.

Our target is to train the AD module as much as possible and in a variety of situations in terms of the input bit stream, channel circumstance, environmental situation, etc. We have performed the experiments at 2.4GHz and based on the QAM–16 modulation. Finally, using the generated signals, we have obtained five RF features for each device as CFO, PO–I, PO–Q, AM–I, and AM–Q (as discussed in Section III-A) in different iterations based on the applied pseudo–random bit streams. Table II shows these features and their mean and standard deviation values. In the second part of the experiments,

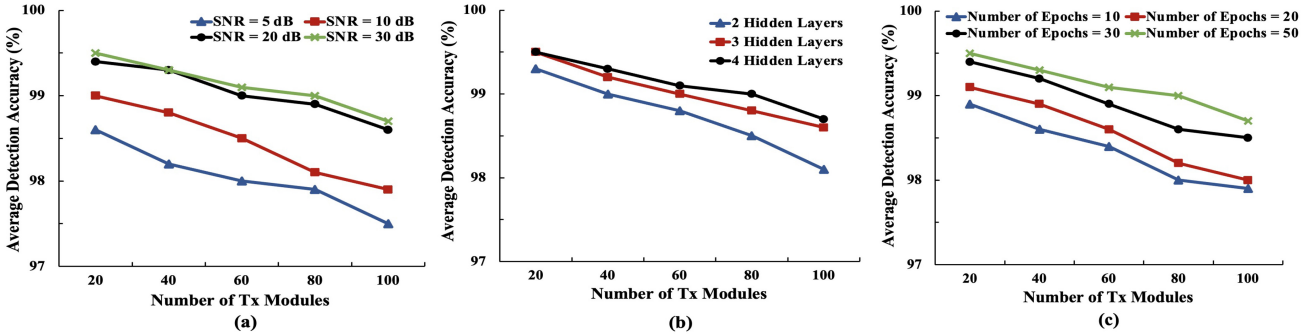

Fig. 6. Average detection accuracy of the proposed AD module for different number of wireless devices and different values of (a) SNR, (b) number of hidden layers, and (c) number of epochs.

TABLE II
RF FEATURES USED IN OUR EXPERIMENTS

Feature	Mean	Standard Deviation
Carrier Frequency Offset (CFO)	2.4 GHz	48 kHz (20 ppm)
Phase Offset (In-Phase) (PO-I)	0°	10°
Phase Offset (Quadrature) (PO-Q)	0°	10°
Amplitude Mismatch (In-Phase)(AM-I)	0 dB	3 dB
Amplitude Mismatch (Quadrature) (AM-Q)	0 dB	3 dB

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

B. Results

In our experiments, we have increased the number of devices from 20 to 100 (with the step of 20) to see the effect of detection performance of our proposal. We have expected the detection accuracy to be considerably degraded in the scenarios with a larger number of devices because in such cases, (intuitively) the feature vectors of distinct devices may become closer to each other. This makes sense in traditional supervised machine learning models (e.g., SVM) in which their classification performance is notably decreased in high dimensional classification scenarios. However, in our case, the amount of reduction in the detection accuracy was not significant. This is indeed a unique attribute of deep autoencoders that has made them as an effective learning model for the fulfillment of anomaly detection tasks. As seen in Fig. 6(a), increasing the number of devices from 20 to 100 results in a 1% reduction in the detection accuracy (approximately) for each level of SNR. In addition, we have noticed that a higher level of SNR improves the detection performance. This is because an RF signal is less distorted in a less noisy channel than a very noisy channel which results in only small changes in the RF features extracted from the received noisy signal. Consequently, the extracted feature vector is more similar to the vectors that the AD module has learned during the training phase. However, this behaviour is seen in low levels of SNR only, i.e., if SNR is high enough (say greater than 20 dB), any increase in the SNR does not result in a significant improvement of accuracy.

We have also examined different architectures of the DAE model in our experiments. We have implemented the DAE model using three different numbers of the hidden layers. As seen in Fig. 6(b), by increasing the number of hidden layers the detection accuracy increases as well. This is because each layer provides a deeper level of knowledge for the model. However, we did not record any significant difference in the accuracy for the scenarios in which three and four hidden layers have been implemented. Since deploying more hidden layers results in a longer training time for the model as seen in Fig. 7(c), the optimum selection for the number of hidden layers in our experiments is three. Regarding the effect of number of epochs on the detection accuracy, the experiments have confirmed that the DAE model performs better if a higher number of epochs is used during the training phase as seen in Fig. 6(c). This is due to the fact that by applying a higher number of epochs may result in overfitting of the model. To avoid overfitting, in our DAE model implementation, we have enabled the *EarlyStopping()* feature of the keras library in Python. Using this feature, the training procedure will be automatically stopped as soon as the model becomes overfitted. This can be checked through the metric of validation loss.

We have also used three different activation functions in our implementations, i.e., *Sigmoid*, *Tanh*, and *ReLu*. The best results were obtained using the Tanh activation function as shown in Fig. 7(a). In Fig. 7(b), we have noticed the effect of encoding dimension on the detection accuracy. The encoding dimension is defined as the size of the encoded (representation) vector. Note that the accuracy reduces for lower encoding dimensions because in these cases, too much compression is done on the input vectors which makes the decoding procedure more difficult, eventually less accurate. Moreover, for a fixed number of encoding dimension, (as discussed before) increasing the number of hidden layers results in a more accurate detection. We have also trained the DAE model using different batch sizes on the training data. As we have expected, the training time is significantly affected by a change in the batch size. The reason is that the DAE model learns all the data available in a batch (and updates the parameters of neurons) before the next batch is learned. Thus, a small batch size increases the number of times that model learns and updates its parameters

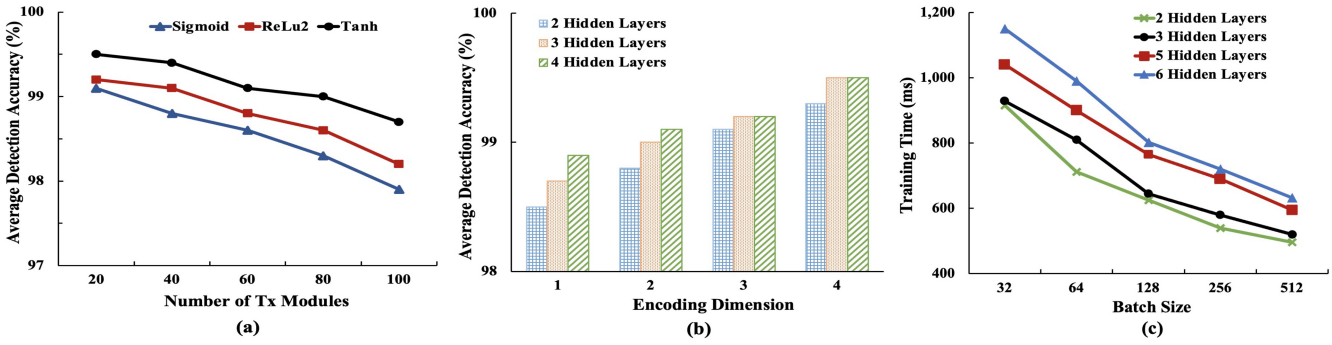

Fig. 7. (a) The effect of three different activation functions on the average detection accuracy. (b) Reducing the encoding dimension degrades the performance in terms of the average detection accuracy. (c) Training time of the DAE model employed in the AD module. Employing a higher number of hidden layers results in more time taken for the training phase. However, selecting a larger batch size shortens the training phase.

TABLE III
COMPARISON OF OUR APPROACH WITH [11] AND [41]

Method	Accuracy	F–Score	Recall	Precision
[11]	90.72%	94.96%	95.10%	94.42%
[41]	86.84%	85.42%	85.42%	79.05%
Our Approach	92.2%	95.94%	94.81%	97.10%

which results in much longer training phase. Fig. 7(c) shows the result. Moreover, as we have discussed before, employing a higher number of hidden layers has the disadvantage of having longer training time.

Finally, it is arguable that the standard deviations of certain features in the Tx devices are taken very high (example 3dB for amplitude mismatch as shown in Table II). This means such high deviations make intrusion detection easy. However, in real scenarios such huge variations are not practical. To investigate the impact of this critical and valid argument, we have further evaluated the performance of DAE based proposed IDS. As shown in Fig. 8 we have determined the detection accuracy of DAE w.r.t number of nodes at different standards deviation values. As standard deviation decreases so thus the detection accuracy of the DAE model decreases. However, interestingly the DAE model has still shown better result as the drop in the accuracy is not much significant. However, to build confidence in our scheme, we have further validated our approach. To gain a deeper understanding and trust in our approach we have used real-world data set and compare our approach with existing works closely relevant to our work.

C. Comparison Using Real Data Set

In this sub-section, we have evaluated our proposed method, and compared this with two recent approaches, using real dataset.[3] We present a comparison of our proposal with two recent approaches, which presents the average values of accuracy, F-Score, Recall, and Precision metrics as shown in Table III. The dataset is collected by the Institute for the Wireless Internet of Things (WIOT) [47]. The transmitter is set up to produce and transfer Wi-Fi signals from 20 National

[3]https://repository.library.northeastern.edu/collections/neu:gm80kf51n

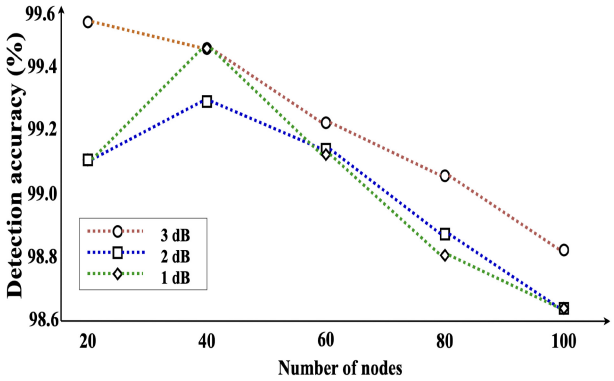

Fig. 8. The detection accuracy vs. number of nodes w.r.t varying standard deviation.

Instruments Software Defined Radios running Gnuradio. At the receiver side, other Gnuradios are employed to collect the I/Q signal values. Researchers collected one transmission at one time using one receiver. The collected data (raw IQ samples) was stored in three different WiFi demodulation process stages: (i) raw IQ samples before applying FFT operation, (ii) raw IQ after applying FFT operation and (iii) the equalized IQ samples. Following this the authors analysed the data to comprehend the impact of each stage on RF fingerprinting accuracy. We have used this dataset with the "Arena Wireless Different Antennas," Day 1 setup [48]. The transmission parameters are similar to IEEE 802.11 a/g (Wi-Fi with 2.432 GHz and 20 MS/s) using BPSK modulation. The antenna type is Ettus VERT2450. In our experiment, we reprocessed the I/Q raw data into the real values and we employed 100,000 data entries from each device. It means that the matrix of our dataset is 20 X 100,000.

From our experiments as shown in Table III we confirm that the highest detection accuracy is around 92.2% at 20 devices. Firstly, we emphasize that the work in [11] and [41] have formulated the research problem as a classification problem and used ANN and CNN, respectively, for authentication. As we have mentioned, [11] is the base of our work and this is a very solid work in the field of node authentication using RF fingerprinting. The findings of this work have created the base of our work. Their approach was simulated using a neural

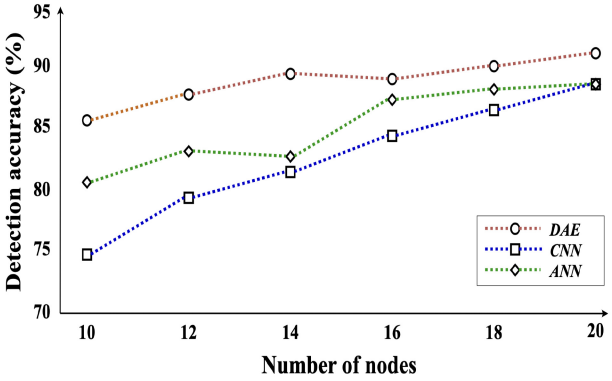

Fig. 9. The detection accuracy of DAE (proposed), ANN [11] and (CNN) [41], using real-data set.

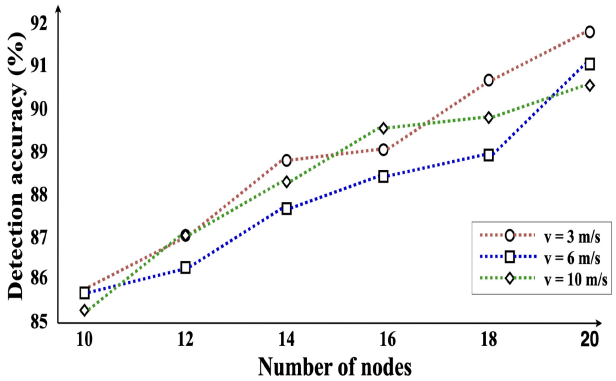

Fig. 10. The impact of mobility of nodes on the performance of the proposed IDS.

network toolbox in MATLAB. They have proved the feasibility of the approach using two software-defined radio (SDRs) devices. Our work uses the similar approach, using a real data set (of 20 devices), but with a focus on detecting an illegitimate node rather than an authentication of the node. We use DAE's anomaly detection capabilities for the accurate detection of intruder devices among large number of legitimate devices.

We further reiterate that in [11] and [41] the authors used ANN and CNN, respectively. Note that the authentication is one-class classification, whereas the traditional classification approaches aim to clearly distinguish two or more classes with the training set containing objects from all the classes. So, the training dataset has only legitimate devices and it shows poor performance for one-class classification. Therefore, in our results the accuracy (legitimate and non-legitimate) drops. In contrast, our approach uses the threshold value (using DAE) to determine if the device is legitimate or not, therefore our approach is better in terms of authentication as well (not only the IDS). We have conducted another experiment to compare the ANN and CNN models performance with DAE using a real-data set. From Fig. 9, we note that DAE gives better results.

D. Impact of Mobility

Now we have also investigated the impact of mobility on the performance of the proposed IDS. We applied the Doppler shift formula to generate the shift in pitch of a node as it travels. This is to understand the relation between the impact on wireless signal w.r.t the velocity of the node/s. To calculate the Doppler shift we firstly specified how fast the transmitter and/or receiver is moving. As in our proposed approach the gateway is immobile, hence the offset is calculated by the velocity of the node in order to compute the actual frequency received by the gateway. We have pre-processed the real dataset with different velocity before feeding it to the proposed framework to simulate how the mobility impacts on the ability of the access control system.

Our evaluation results are shown in Fig. 10. In this Figure we note the degradation in the accuracy at higher node velocity however the model improves as we increase the number of nodes, this is because of the behaviour of neural networks or say the model becomes well generalised with enough number of samples. Hence the proposed IDSs can well handle the impact of node mobility on its detection accuracy at a large number of nodes. Further comparison of this aspect with the models used in [11] and [41] is also shown in Fig. 9. We emphasize that the proposed model works better than the existing schemes in mobility scenarios as seen in this figure that DAE still shows better results.

Finally, it could be arguable that whether the proposed system is secure and feasible or not. Therefore, in the following section we have discussed the effectiveness of our IDS from a certain attack.

V. Security Analysis

Now we discussed the security aspects of our proposal and have presented an effective approach for the prevention of replay attacks. We emphasize that our IDS is immune against physical/hardware and host–based attacks. Then, we have investigated the potential vulnerability of our IDS against replay attacks. Finally, we present an effective solution to protect it against this kind of attacks.

Interestingly, our IDS is not vulnerable against physical/hardware attacks (e.g., invasive, semi–invasive or side–channel attacks, [49], [50]) that need physical access to the devices, or software–based attacks (e.g., malware–based or API attacks). This is because (1) it is infeasible (extremely hard if not impossible) to forge RF signatures with multiple features and (2) in our IDS no digital signature is recorded in wireless IoT devices. However, it may suffer from replay attacks [11], [50] in which the attacker (after eavesdropping on a network communication) intercepts the transmitted data, and then maliciously re–sends it (usually with some delay) to mislead the receiver. In our IDS, if a malicious device intercepts the signal of a legitimate IoT device (that is sent in response to the network authentication request) and re–sends it as its own response, the AD module may detect no anomaly. This is because in this case, the feature extraction procedure is done on a signal originated from a legitimate device (i.e., the learning model has already learned its RF signature). Thus, the attacker may be authenticated into the network.

To conduct a successful replay attack, the attacker needs to neutralize an inherent security property of our IDS that is

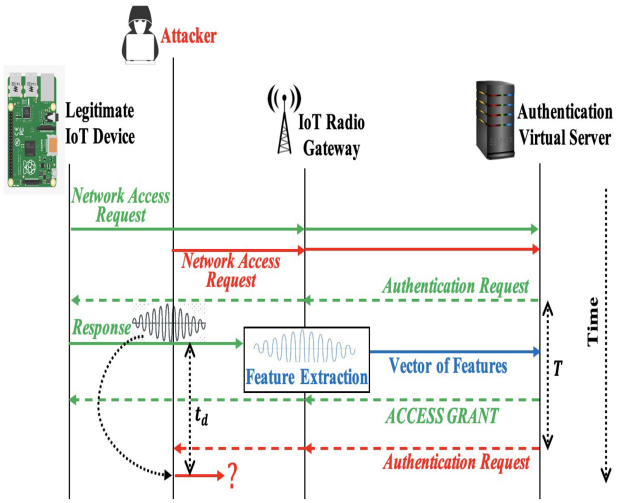

Fig. 11. The proposed delay–based solution to address replay attacks.

to eliminate the changes (on the legitimate signal) caused by the RF signature of the attacker's device. In fact, when the attacker device replays the legitimate signal, it automatically applies its own RF signature on the reused signal. The reason is that the signal has to pass through different RF circuits in the Tx module of the malicious device (e.g., filter, power amplifier, antenna, etc.) which affect both frequency and phase features of the signal. Therefore, the RF signature of the legitimate device is corrupted. This results in the detection of an anomaly in the AD module. However, one may argue that the attacker could design an accurate (and expensive) Tx module in such a way that the changes on the legitimate RF signature are minimized. Although this makes it more difficult and expensive to perform the attack, we have proposed an effective delay–based solution to effectively make the replay attack efforts unsuccessful.

A. Delay–Based Solution

To address the issue of replay attacks, we have proposed a delay–based mechanism in which the authentication service handler of the network (i.e., the slice's orchestration manager) intentionally delays the transmission of authentication requests to the IoT devices who have submitted a network access request, as this can be seen in Fig. 11. To better understand this, consider a malicious device D_M who is eavesdropping on the communications of a legitimate IoT device D_L. Assume that D_M can successfully identified the of D_L which is a Network Access Request (NAR) message. To start conducting the attack, D_M submits its own NAR immediately after it detects D_L's NAR message (to minimize the time gap between the two authentication procedures). Upon receiving the NAR message of D_L, the server replies to D_L immediately (assuming this is the only unanswered NAR message in the network) by sending the Authentication Request (AR) message to D_L asking the device to reply back. It also invokes the *FE_VNF()* function to perform the feature extraction procedure at the IoT gateway/edge computing device. At the same time, it invokes a timer initialized with a short and predefined period of time T.

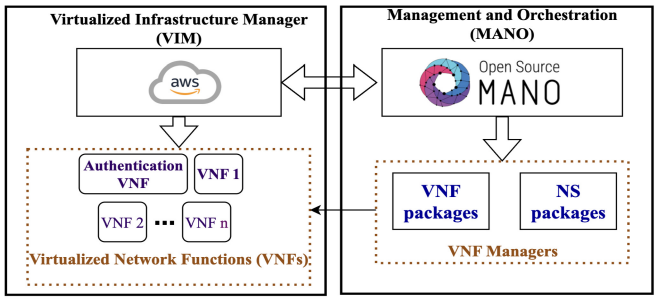

Fig. 12. Structural diagram of the integration of our proposal with ETSI-MANO architecture.

However, when the server receives the NAR message of D_M, it does not reply to it until the timer is up. Upon receiving the AR message, D_L transmits the reply signal which is processed by the FE module to extract its features. This signal is targeted by D_M to be intercepted and re–transmitted to the server. However, D_M has not received any AR message from the network yet, thus, it can not re–transmit the signal immediately. In other words, the eavesdropped signal must be delayed by D_M until the relevant AR message is received. This is an infeasible task for D_M to perform if T is large enough (e.g., 1 msec). The reason is that delaying the transmission of an RF signal without making changes on the amplitude, frequency, and phase features of the signal is infeasible. The current solutions for the implementation of passive delay lines work mostly based on either coaxial/optical fibre cables or electro–acoustic devices [51] (note that active delay lines do not work for the attacker in this attack scenario since they definitely change the RF features of the signal). However, these solutions are not practical when the required delay should be in the millisecond (or larger) ranges. Thus, adopting T in the millisecond range prevents the attacker to deploy an appropriate passive delay line. On the other hand, selecting a large value for T may result in performance degradation of the IoT application in terms of latency. For example, considering $T = 1$ msec, the server can authenticate 1000 devices per second (regardless of other delays caused by signal propagation, processing, software running, etc.) and the created delay is much smaller than the latency requirements of most of the latency critical IoT applications [52].

VI. PoC: Integration of the Proposed IDS Mechanisms With ETSI-NFV Architecture and Performance Evaluation

In this subsection, we have given a proof of concept using ETSI OSM-MANO test bed to show how the proposed approach would fit in with a real-life MANO. This is to capture the difficulties of deploying the VNFs involved in process and give a sense of realism to the solution. We reiterate that this contribution presents relevant aspects of deployment of the approach and evaluation results show its performance, as below. Fig. 12 shows the structural diagram of our proposal using ETSI-VNF architecture in which we use OSM MANO for the deployment of our scheme as pluggable VNF module. We use Amazon Cloud Service (AWS) cloud platform for

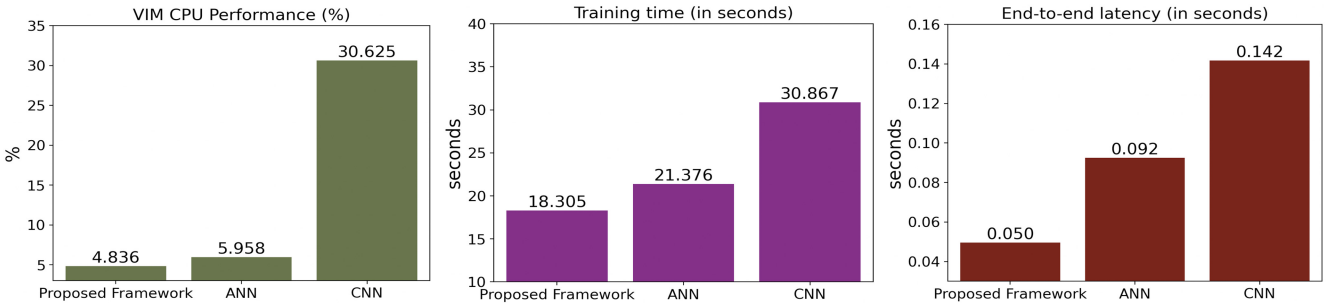

Fig. 13. (a) The proposed schemes impact on a) CPU Utilization, b) Model training time, and c) End-to-end delay. These key metrics are compared with other models used in the existing works [11] (ANN) and [41] (CNN), respectively. Our results showing better performance.

the deployment and conducting evaluation of our proposal. The Open-Source MANO version 10 is setup on an Amazon Elastic Compute Cloud (Amazon EC2). The EC2 features 8GB of memory and 4 vCPU Intel Xeon processors. The OSM connects to the Virtualized Infrastructure Manager (VIM) which is in our experiments is the AWS. The system is aligned with ETSI-NFV architecture in 5G. The VNF uses Python 3.8.3 and Tensorflow version 2.8.0. We use 200 devices (100 legitimate and 100 non-legitimate), Epochs are 100, batch size is 128.

Fig. 13(a) illustrates the impact of our proposal on CPU utilization. In comparison to CNN our proposal consumes significantly lesser processing resources. With ANN the difference in CPU consumption is not that significant but at the same time we achieve very high accuracy as shown in Table III. Further, from Fig. 13(b) we see that our approach takes lesser training time to train model, it means the approach is suitable in scenarios where nodes enter and leave network frequently. It also means the authentication time is lesser which is an advantage in high-speed low latency next generation networks. The same is evident in Fig. 13(c). More importantly the scheme is highly beneficial for any cloud system or in any network where heavy use of virtualization is seen, means an effective utilization of resources and operational costs will be reduced without much compromising with accuracy.

Now since the target systems are resource-constrained, it is vital to have a quantitative understanding of estimating the power consumption estimation of the hardware implemented in our method. The scheme we propose does not rely on the cooperation of IoT nodes as RF signatures of each node are stored and analyzed in a secure server running the DAE-based anomaly detection algorithm (see Fig. 5). Given the main computation is on the VNFs involved, we evaluated their power consumption to better understand sustainable computation.

In existing literature, researchers have mainly discussed two methods to compute the power consumption: direct measurements and estimation approach [53]. In our work, using the same data set, we have adopted a similar approach proposed by [54] to estimate the power consumption analysis. The power consumption is calculated as:

$$P = t_r \times (c_i \times P_c \times c_u + m_i \times P_m) \tag{8}$$

where P is the power consumption (in kWh), t_r is the actual running time (hours), c_i the number of running cores, m_i the memory available (gigabytes), c_u is the processor usage factor ranging from 0 to 1, P_c denotes the power consumption of a computer core, while P_m denotes the power drawn by the memory (watt).

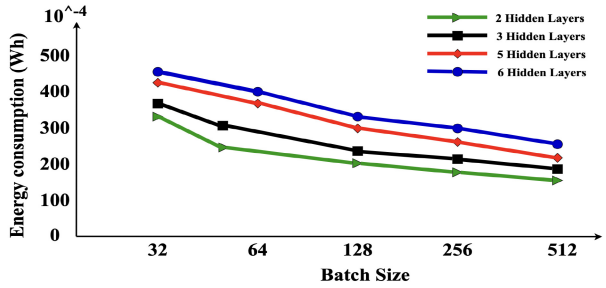

Fig. 14. The power consumption of the proposed framework.

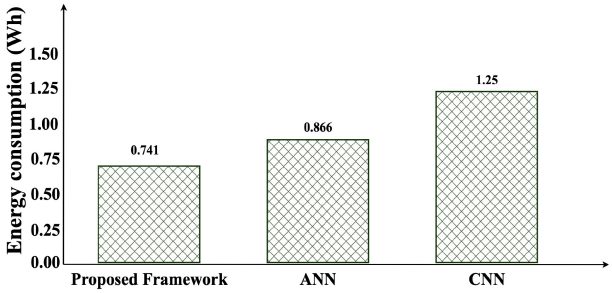

Fig. 15. The comparisons on power consumption between the proposed schemes and other machine learning algorithms.

We used a benchmark tool[4] with our system configuration (Intel Core i5, 2.3GHz with 4 cores) with 8GB memory usage and recorded the actual running time in the experiments. Fig. 14 shows the energy consumption of the AD module in the framework under various batch sizes and hidden layers settings. As expected, the large batch size costs less energy because the training time is faster. The DAE model learns the data in a batch, and adjusts the parameters of the neurons before the next batch is learnt. A small batch size increases the training time as the model learns and updates its parameters more frequently. Furthermore, comparisons between the proposed method and other machine learning algorithms (ANN [11] and (CNN) [41]) have been conducted, see Fig. 15. The results show that our method is energy efficient.

[4]http://calculator.green-algorithms.org/

VII. Summary and Future Work

We have proposed a novel IDS mechanism to detect malicious IoT nodes in 5G virtualized networks. An anomaly detection module using the deep autoencoder model is developed to learn the unique RF features of all the wireless legitimate IoT devices in a network (in the training phase). Then, the identity of any connecting IoT device in the network can be validated using the developed learning model. In fact, it identifies an illegitimate device as an anomaly since the RF features extracted from its received signal has not been learned by the model before. We have also proposed a framework for the integration of our IDS into the 5G standard ETSI-NFV architecture to show how our IDS run and coordinated by the orchestration layer of a network slice. Further, we have validated that the proposal is secure from certain attacks, i.e., replay attacks. This we have demonstrated by mounting an attack and by proposing a novel delay–based solution that makes the malicious replay efforts unsuccessful. The results are showing the feasibility and effectiveness of the proposed approach. In future, the feasibility of utilizing RF features in the frequency domain can be investigated to compare the results with the scenarios in which the RF feature are analyzed in the time domain. Another interesting research direction for the future work is to utilize the unique RF features of wireless IoT device for the development of a secure data provenance mechanism to maximize trustworthiness in 5G–base IoT networks. Finally, we agree that security proof of the model we have provided is limited to a certain attack, however, analysing the complete security of the approach itself against variety of attacks will form a completely new and interesting project. The first step would be to rigorously analyse the potential threats and vulnerabilities against the proposed approach following which the security proof is required.

Acknowledgment

The authors are thankful to the Editor and anonymous reviewers for the insightful comments which have improved the quality of this work. The authors thank Dr. Guy Wood-Bradley for his careful reading and suggestions on this manuscript.

References

[1] 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.

[2] 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.

[3] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 2, no. 1, pp. 41–50, Feb. 2018.

[4] R. Gassais, N. Ezzati-Jivan, J. M. Fernandez, D. Aloise, and M. R. Dagenais, "Multi-level host-based intrusion detection system for Internet of Things," *J. Cloud Comput.*, vol. 9, no. 1, pp. 1–16, 2020.

[5] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep learning approach combining sparse autoencoder with SVM for network intrusion detection," *IEEE Access*, vol. 6, pp. 52843–52856, 2018.

[6] W. Wang, X. Du, D. Shan, R. Qin, and N. Wang, "Cloud intrusion detection method based on stacked contractive auto-encoder and support vector machine," *IEEE Trans. Cloud Comput.*, vol. 10, no. 3, pp. 1634–1646, Jul.–Sep. 2022.

[7] L. F. Maimó, A. H. Celdrán, M. G. Pérez, F. J. G. Clemente, and G. M. Pérez, "Dynamic management of a deep learning-based anomaly detection system for 5G networks," *J. Ambient Intell. Humanized Comput.*, vol. 10, pp. 3083–3097, Aug. 2019.

[8] M. Antonio et al., "Traffic-flow analysis for source-side DDoS recognition on 5G environments," *J. Netw. Comput. Appl.*, vol. 136, pp. 114–131, Jun. 2019.

[9] S. Rezvy, Y. Luo, M. Petridis, A. Lasebae, and T. Zebin, "An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks," in *Proc. 53rd Annu. Conf. Inf. Sci. Syst. (CISS)*, 2019, pp. 1–6.

[10] J. Lam and R. Abbas, "Machine learning based anomaly detection for 5G networks," 2020, *arXiv:2003.03474*.

[11] 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.

[12] J. Bassey, D. Adesina, X. Li, L. Qian, A. Aved, and T. Kroecker, "Intrusion detection for IoT devices based on RF fingerprinting using deep learning," in *Proc. 4th Int. Conf. Fog Mobile Edge Comput. (FMEC)*, 2019, pp. 98–104.

[13] M. F. Bari, M. R. Chowdhury, B. Chatterjee, and S. Sen, "Detection of rogue devices using unintended near and far-field emanations with spectral and temporal signatures," in *IEEE/MTT-S Int. Microw. Symp. Tech. Dig.*, 2022, pp. 591–594.

[14] L. F. Maimó, F. J. G. Clemente, M. G. Pérez, and G. M. Pérez, "On the performance of a deep learning-based anomaly detection system for 5G networks," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Computed, Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, 2017, pp. 1–8.

[15] 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.

[16] R. P. F. Hoefel, "IEEE 802.11ax: A study on techniques to mitigate the frequency offset in the uplink multi-user MIMO," in *Proc. 8th IEEE Latin-Amer. Conf. Commun. (LATINCOM)*, 2016, pp. 1–6.

[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] D. Banerjee, B. Muldrey, S. Sen, X. Wang, and A. Chatterjee, "Self-learning MIMO-RF receiver systems: Process resilient real-time adaptation to channel conditions for low power operation," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, 2014, pp. 710–717.

[19] S. Sen, V. Natarajan, S. Devarakond, and A. Chatterjee, "Process-variation tolerant channel-adaptive virtually zero-margin low-power wireless receiver systems," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 33, no. 12, pp. 1764–1777, Dec. 2014.

[20] 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.

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

[22] L. Bai, L. Zhu, J. Liu, J. Choi, and W. Zhang, "Physical layer authentication in wireless communication networks: A survey," *J. Commun. Inf. Netw.*, vol. 5, no. 3, pp. 237–264, 2020.

[23] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019.

[24] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.

[25] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 282–310, 1st Quart., 2021.

[26] S. Wijethilaka and M. Liyanage, "Survey on network slicing for Internet of Things realization in 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 957–994, 2nd Quart., 2021.

[27] "ETSI." Accessed: Feb. 15, 2022. [Online]. Available: https://www.etsi.org/technologies/nfv/nfv
[28] C. Liu, J. Yang, R. Chen, Y. Zhang, and J. Zeng, "Research on immunity-based intrusion detection technology for the Internet of Things," in *Proc. 7th Int. Conf. Nat. Comput.*, vol. 1, 2011, pp. 212–216.
[29] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6LoWPAN based Internet of Things," in *Proc. IEEE 9th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)* 2013, pp. 600–607.
[30] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. A. Spirito, "An IDS framework for Internet of Things empowered by 6LoWPAN," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2013, pp. 1337–1340.
[31] D. Oh, D. Kim, and W. W. Ro, "A malicious pattern detection engine for embedded security systems in the Internet of Things," *Sensors*, vol. 14, no. 12, pp. 24188–24211, 2014.
[32] P. Pongle and G. Chavan, "Real time intrusion and wormhole attack detection in Internet of Things," *Int. J. Comput. Appl.*, vol. 121, no. 9, pp. 1–9, 2015.
[33] N. K. Thanigaivelan, E. Nigussie, R. K. Kanth, S. Virtanen, and J. Isoaho, "Distributed internal anomaly detection system for Internet-of-Things," in *Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, 2016, pp. 319–320.
[34] T.-H. Lee, C.-H. Wen, L.-H. Chang, H.-S. Chiang, and M.-C. Hsieh, "A lightweight intrusion detection scheme based on energy consumption analysis in 6LowPAN," in *Advanced Technologies, Embedded and Multimedia for Human-centric Computing: HumanCom and EMC 2013*. Dordrecht, The Netherlands: Springer, 2014, pp. 1205–1213.
[35] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, Apr. 2017.
[36] J. P. Amaral, L. M. Oliveira, J. J. P. C. Rodrigues, G. Han, and L. Shu, "Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2014, pp. 1796–1801.
[37] S. Misra, P. V. Krishna, H. Agarwal, A. Saxena, and M. S. Obaidat, "A learning automata based solution for preventing distributed denial of service in Internet of Things," in *Proc. Int. Conf. Internet Things 4th Int. Conf. Cyber, Phys. Social Comput.*, 2011, pp. 114–122.
[38] A. Le, J. Loo, Y. Luo, and A. Lasebae, "Specification-based IDS for securing RPL from topology attacks," in *Proc. IFIP Wireless Days (WD)*, 2011, pp. 1–3.
[39] J. Krimmling and S. Peter, "Integration and evaluation of intrusion detection for CoAP in smart city applications," in *Proc. IEEE Conf. Commun. Netw. Security*, 2014, pp. 73–78.
[40] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, 2015, pp. 606–611.
[41] 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.
[42] Y. H. You and H. K. Song, "Efficient sequential detection of carrier frequency offset and primary synchronization signal for 5G NR systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 9212–9216, Aug. 2020.
[43] D. P. Kingma and M. Welling "An introduction to variational autoencoders," *Found. Trends Mach. Learn.*, vol. 12, no. 4, pp. 307–392, 2019.
[44] C. Zhou and R. C. Paffenroth, "Anomaly detection with robust deep autoencoders," in *Proc. 23rd ACM SIGKDD Int. Conf. Knowl. Disc. Data Min.*, 2017, pp. 665–674.
[45] A. Géron, *Hands-on Machine Learning With Scikit-Learn, Keras, and TensorFlow*. Sebastapol, CA, USA: O'Reilly Media, 2022.
[46] E. Bingham and H. Mannila, "Random projection in dimensionality reduction: Applications to image and text data," in *Proc. 7th ACM SIGKDD Int. Conf. Knowl. Disc. Data Min.*, 2001, pp. 245–250.
[47] A. Al-Shawabka et al., "Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting," in *Proc. IEEE Conf. Comput. Commun.*, 2020, pp. 646–655.
[48] "Datasets release: An IEEE 802.11 A/G (WiFi) massive-scale and labeled datasets for radio fingerprinting." Accessed: Oct. 22, 2022. [Online]. Available: https://wiot.northeastern.edu/wp-content/uploads/2020/07/dataset_release.pdf
[49] A. Sokolov and D. Rachkovskij, "On handling replay attacks in intrusion detection systems," *Int. J. Inf. Theor. Appl.*, vol. 10, no. 3, pp. 341–347, 2003.
[50] U. Rührmair and M. van Dijk, "PUFs in security protocols: Attack models and security evaluations," in *Proc. IEEE Symp. Security Privacy*, 2013, pp. 286–300.
[51] 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.
[52] 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.
[53] C. Möbius, W. Dargie, and A. Schill, "Power consumption estimation models for processors, virtual machines, and servers," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 6, pp. 1600–1614, Jun. 2014.
[54] L. Lannelongue, J. Grealey, and M. Inouye, "Green algorithms: Quantifying the carbon footprint of computation," *Adv. Sci.*, vol. 8, no. 12, 2021, Art. no. 2100707.

Keshav Sood (Associate Member, IEEE) received the Ph.D. degree from Deakin University in 2018. Following his Ph.D., he worked as Research Fellow with The University of Newcastle, NSW, Australia. He worked on the project funded by the Defence Science and Technology Group. He is currently a Lecturer with Deakin University, Melbourne. Some of his work is funded by the Department of Defense, Australia, and Cyber Security Cooperative Research Centre, Australia.

Dinh Duc Nha Nguyen received the bachelor's degree from the Posts and Telecommunications Institute of Technology, Vietnam, and the master's degree from the Queensland University of Technology, Australia. He is currently pursuing the Ph.D. degree with Deakin University, Melbourne, Australia. He has been awarded a place on the Dean's list of excellent academic performance two consecutive times in 2020. He has more than six years of industry experience as a network analyst and software engineer.

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 is currently working as a Research Fellow with the Centre for Cyber Security Research and Innovation, Deakin University, Australia. He has more than ten years of industry experience in ICT field.

Neeraj Kumar (Senior Member, IEEE) received the Ph.D. degree in CSE from Shri Mata Vaishno Devi University, Katra, India. He was a Postdoctoral Research Fellow with Coventry University, Coventry, U.K, where he is a Visiting Professor. He is currently a Full Professor with the Department of Computer Science and Engineering, Thapar University, Patiala, India, and also with the School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India.

Frank Jiang received the Ph.D. degree from The University of Technology Sydney and the master's degree in computer science from the University of New South Wales, Australia, where he gained post-doctoral research experience for three and half years. He has published over 120 highly reputed SCI/EI indexed journals/conferences articles.

Morshed Chowdhury received the Ph.D. degree from Monash University, Australia, in 1999. He is currently an Academic Staff Member with the School of Information Technology, Deakin University, Australia. Prior to joining Deakin University, he was an Academic Staff with the Gippsland School of Computing and Information Technology, Monash University. He has more than 12 years of industry experience in Bangladesh and Australia.

Robin Doss (Senior Member, IEEE) is the Research Director of the Centre for Cyber Security Research and Innovation, Deakin University. In addition, he also leads the "Next Generation Authentication Technologies" theme within the National Cyber Security Cooperative Research Centre. He has an extensive research publication portfolio. He was the recipient of the "Cyber Security Researcher of the Year Award" from the Australian Information Security Association in 2019.