Impersonation Attack Detection in IoT Networks

*Dinh Duc Nha Nguyen, *Keshav Sood, *Yong Xiang, **Longxiang Gao, ***Lianhua Chi
*School of IT, Deakin University, Geelong, 3220, VIC, Australia
**Qilu University of Technology and National Supercomputer Center, Jinan, China
***La Trobe University, Melbourne, Australia
(Corresponding author: nguyendinh@deakin.edu.au)

GLOBECOM 2022 - 2022 IEEE Global Communications Conference | 978-1-6654-3540-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/GLOBECOM48099.2022.10001392

***Abstract*—The deployment of Internet of Things (IoT) networks is growing at an extraordinary speed from last decade and has expanded the interconnection of billions of nodes, providing a range of flexible communication and computing services, etc. We note that this significant expansion of the IoT surface has expanded the attack surfaces and is a danger to companies of every size from security aspects. The IoT devices are easy to compromise and therefore the attacker can easily act as an impersonator to impersonate other legitimate IoT nodes. This is known as impersonation attacks or spoofing attacks in wireless IoT networks. In this paper, we propose a new methodology to detect an impersonation attack in IoT networks. We use Mahalanobis Distance correlation theory based two-stage attack detection model to resist IoT node spoofing. The approach is evaluated on cloud platforms and is compared with the recent state-of-the-art literature. The proposal is deployed as a pluggable module in cloud networks. The key metrics of our evaluation and comparisons are accuracy with respect to the varying size of the IoT network, classification metrics, attack detection time, and CPU utilization.**

***Index Terms*—Authentication, Heterogeneity, IoT, Next generation networks, Security.**

I. Introduction and Background

An ever increasing of IoT devices in day to day life for a variety of reasons such as sensing etc. are transmitting significant amounts of data [1], [2], [3]. As new-age technologies grow (such as IoT), the threat landscape is increasing, and business leaders are worrying about the data security [4], [5], [6]. This has raised significant concerns of security and privacy [7], [8]. Particularly, using social engineering methods the malicious user can easily launch the identity-based attack, also known as impersonation attack or spoofing attack [9], [10], [11]. In a recent report published by Check Point, it is seen that Microsoft and Google impersonation attacks are on the rise[1]. Therefore, it is important to defend IoT networks from impersonation attacks.

We first provide a state-of-the art to discuss the recent solutions and their limitations as well. In 2019, Bassey *et al.* [12] proposed an intrusion detection model based on RF fingerprinting to prevent the impersonation attacks. Their solution uses I/Q (In-phase and Quadrature) mismatching for the unique feature of RF fingerprinting. After capturing the raw I/Q samples, the data is preprocessed with the dimensionality reduction, de-correlation and clustering algorithms, then the data is trained with CNN (Convolutional Neural Networks) algorithms to find a signature of an IoT device. Further, Wang *et al.* [13] introduced an framework using two RF layer features, Carrier Frequency Offset (CFO) and spatial-temporal link signature on LoRa (Long Range) devices. The experiments evaluate the performance via two metrics: True Positive Ratio and False Positive Ratio, the SVM model (Support Vector Machine) is employed for classification tasks.

In another research work [14] also focused on preventing identified-based attack, called IMPACT (IMPersonation Attack detecCTion). Instead of RF fingerprinting technique, IMPACT provides a specific solution on machine learning algorithms for detecting impersonation attack. The method uses SVM to reduce the dimensional data and Stacked Autoencoder (SAE) to identify the spoofing attack. They tested their solution on Aegean WiFi Intrusion Dataset (AWID). The evaluation measures used are Accuracy, Detection Rate, False Alarm Rate, F1 score and Time To Build (TTB).

Recently, the increasing utilization of near field communication (NFC) has raised attention on security, in this aspect Wang *et al.* [15] proposed a solution to detect impersonation attacks based on RF fingerprinting technique. They used Deep Neural Network (DNN) algorithms as a classification method and conducted experiments on 50 NFC tags. They compared their solution with other algorithms by using some classification metrics: Accuracy, F1-score, Area under the curve (AUC) and Receiver Operating Characteristic (ROC). Another research [16] investigates the classification and detection of UAVs (unmanned aerial vehicles) by using RF fingerprints. They have tested the solution, using a real UAV data set, with many machine learning classification algorithms and KNN (k-nearest neighbor) provides the best performance. Accuracy and computational Time are two key metrics of the study.

Very recently, Nosouhi *et al.* [17] introduced a spoofing resistant approach for IoT networks based on RF fingerprinting. The method explores the RF beam patterns of received signals by using Deep Autoencoder training model to detect the attack, with the strong argument that the RF signatures are impossible to mimic (or extremely expensive). They employ synthetic dataset by MATLAB to evaluate their method under different settings. Detection accuracy is the only metric to evaluate the performance. It is unfortunate that the evaluation results only considered the model tuning parameters (in addition to the accuracy) as main key metrics to evaluate the effectiveness of the study. We argue that the model tuning parameters cannot be considered as metrics to show the strength of the proposed

[1]https://blog.checkpoint.com/2020/11/23/microsoft-google-impersonation-attacks-are-on-the-rise-how-to-stay-safe/

work.

From the notable works, preventing impersonation attacks, we have discussed above, we note that there are key issues. Main drawback of these studies is that they focus more on the accuracy of authentication instead of impersonation attacks. In addition, studies claimed that the RF features are difficult to mimic, so it can be used to prevent spoofing attacks. We note that the Software Defined Radio which can simulate signal characteristics has posed a critical threat to imitate RF fingerprinting features [18].

Furthermore, the existing solutions are not lightweight, IoT devices with limited computation and energy resources cannot fully run the conventional cryptography solutions, in mission-critical applications latency (attack detection time as well as maintaining end-to-end QoS service requirements of the application) is still a critical issue. Unfortunately, none of the existing works consider node authentication time and the utilization of resources as well as the trade-off between accuracy and time consuming which are the key metrics for supporting real-time applications in the Next Generation Networks. Furthermore, the methods are not evaluated on any next generation networks test bed.

Motivated from this, we propose a two-stage authentication approach to prevent impersonate attack (in Section III). In the first stage, we use RF features/signatures of IoT devices for binary classification (legitimate or illegitimate nodes) using Mahalanobis Distance correlation theory. The second stage is the node authentication stage which monitors any change in the node topology based on Received Signal Strength Indicator (RSSI). The combined output of these two stages is used to prevent impersonation attacks. We have compared our results with [12], [14], and [17]. The theories we have used are known (in pattern recognition and other medical domains [19], [20], [21]), however, have not been used in RF fingerprint based anomaly detection in IoT networks and related research works.

Our contributions in this paper are below.

1) We propose a two-stage impersonation attack prevention methodology based on radio-frequency fingerprinting exploiting standard statistical analysis. Our approach is based on Mahalanobis Distance theory. The combined output of these two stages enforce the node authentication decision to prevent impersonation attack. We have compared our approach with three recent works.
2) We demonstrated that the proposed approach is effective and can be integrated with next generation networks. We used OSM-MANO (open source 5G-NFV test bed) for our evaluation. The proposed architecture is implemented as a virtual network function on Amazon Web Services (AWS) cloud platform. Our approach is significantly less computationally intense than standard approaches.

The remainder of this paper is organized as follows. Section II provides the preliminary work to discuss Mahalanobis Distance theory. In Section III we discuss our proposed scheme in detail. The performance evaluation is shown in Section IV. Further discussion is given in Section V. Finally, Section VI concludes this paper and discusses some future works.

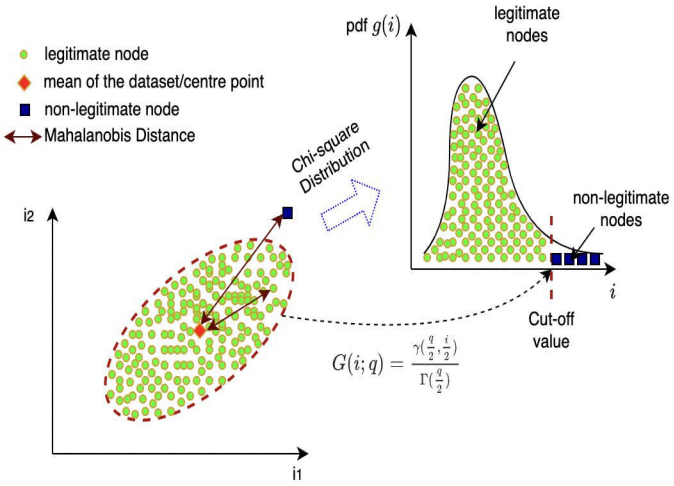

Fig. 1. A high level view of Mahalanobis Distance theory and Chi-square Distribution.

II. Preliminaries: Mahalanobis Distance Theory and Chi-square Distribution

Mahalanobis Distance is a measure of the distance between a variable i and a distribution which is calculated by a mean and the covariance matrix [22]. This theory is often utilized by pattern recognition researchers to measure the similarity between the data distribution of train and test samples [23]. Hence MD is postulated to be a multivariate normal distribution. As seen in Fig. 1, the region of persistent MD around the center point constructs an ellipse in two-dimensional space (assuming 2 variables are measured). If a new node enters in the network (red dot outside the MD region), the MD calculates the distance between a new node and the mean of the dataset (from the centred point shown as an orange dot). The formula to compute MD is as below:

$$d_M = \sqrt{(i - m_i)^T . C^{-1} . (i - m_i)} \tag{1}$$

Here, $(i–m_i)$ is the distance of the vector from the mean. We then divide this by the covariance matrix (or multiply by the inverse of the covariance matrix). From the equation, it can be seen that the distance has an inverse relationship with covariance. Furthermore, the covariance reveals the correlation of the variables in the dataset.

Chi-square distribution results in the continuous distribution of the total of squared random variables in case the variables are independent [24]. It demonstrates the confidences encompassing the variance and standard deviation of a point to a normal distribution. Furthermore, it is also employed to evaluate how good sample data shape to the actual population [25]. From the equation (1), it can be seen that the MD is a subbranch of Chi-square distribution with q degrees of freedom (q) is a number of dimensions of the dataset). Although it is true that in real-time that variables do not often follow the

assumption of normality. In such cases, the conversion to Chi-square p-values (probability of observing a test statistic) serves to recode the MD to a 0-1 scale. As MD have no upper limit, so this rescaling may be convenient for analyses. In general the p-value reflects the probability of seeing a MD value as large or larger than the actual MD value, p values close to 0 reflect high MD values and hence they are very dissimilar (legitimate nodes) to the ideal combination of new variables. p-values close to 1 reflect low MD (non-legitimate nodes) and are hence very similar to the ideal combination of new IoT nodes. (sometimes called predictor variables).

Mathematically, the Chi-squared Distribution (also χ^2-distribution) is the distribution of a total of the squares of q. Suppose $i_1, i_2, ...j_k$ are independent variables, so the total of their squares as:

$$S_q = \sum_{k=1}^{q} {i_k}^2 \tag{2}$$

so, the chi-square distribution with q is denoted as

$$D_\chi \sim \chi^2(q) \text{ or } D_\chi \sim \chi_q^2 \tag{3}$$

The probability density function is defined as:

$$g(i;q) = \frac{i^{\frac{q}{2}-1}e^{-\frac{i}{2}}}{2^{\frac{q}{2}}\Gamma(\frac{q}{2})}, q > 0 \tag{4}$$

The Cumulative Distribution Function (CDF) of Chi-square distribution is denoted as:

$$G(i;q) = \frac{\gamma(\frac{q}{2}, \frac{i}{2})}{\Gamma(\frac{i}{2})} \tag{5}$$

The cut-off value (see Fig. 1) is determined by the CDF which separates the rejection region (illegitimate nodes) and the sampling distribution (legitimate nodes). A node is confirmed as legitimate if its MD to the mean of the dataset is less than the cut-off value.

TABLE I
KEY NOTATIONS

Notation	Explanation
d_M	the Mahalanobis distance
i	RF feature vector
m_i	vector of mean values of the variables
T	transpose vector
C	the covariance matrix
q	the number of RF features
cv	cut-off value
γ	the lower incomplete gamma function
Γ	the gamma function
$g(i;q)$	the probability density function
$G(i;q)$	the cumulative distribution Function

III. Proposed Solution

A high-level view of the proposal is shown in Fig. 2. It is divided into two phases: Feature extraction and Authentication. The first phase is used to collect RF features of IoT devices for data pre-processing. The processed data is passed onto the next phase which is divided into two stages: Classification and topology-based node authentication. In the Classification stage, we use MD and Chi-square Distribution theoretical approaches to accurately determine/classify whether a new IoT node is legitimate or not. In the next stage, we use the mean value of RSSI of the node and Mahalanobis and Chi-square Distribution theory to predict any change in the original topology.

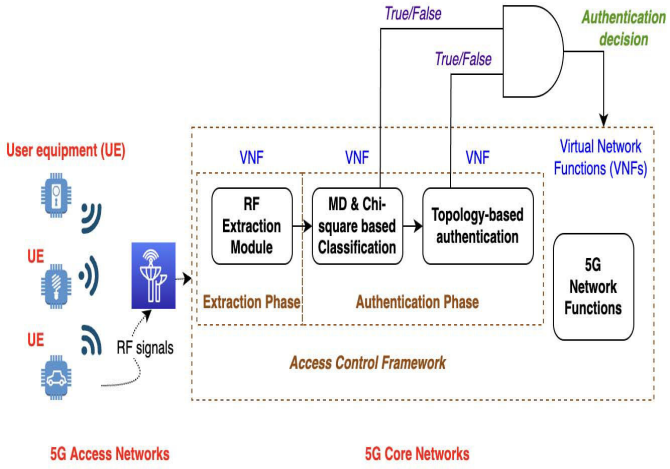

Fig. 2. A high level architecture of the proposed approach.

The workflow of this stage is illustrated in Fig. 3. It shows normal and abnormal topology and legitimate and non-legitimate flows. We assume that there are four nodes/users in the topology. One of the nodes (red) was a part of the normal topology boundary (solid dark line) before it was compromised and has changed its position. With this RSSI of this node will change which is detected by the topology-based authentication sub module in Fig. 3. Although the classification module will consider this node as legitimate, but the topology-based authentication sub-module will treat it as a compromised node. The combined AND Gate output (as per Fig. 3 and Table II) will be low (means attack).

Finally, the authentication decision module (AND gate operation) takes the output of both these two sub-module and enforces the decision to authenticate nodes or to prevent Impersonation Attack. We emphasize that it is possible that any legitimate node can get access to a network but with our solution, we firstly classify nodes into legitimate and non-legitimate categories. However, in our solution, it does not mean that the node is authenticated, rather we use a second sub-module for verifying this. Once the output of both modules are true (high), then we consider that the node is legitimate as well as the node is authenticated. The algorithm of the proposed solution is given below.

IV. Performance Evaluation

We evaluate our method by conducting experiments under various scenarios. We use the Wireless Waveform Generator toolbox of MATLAB to generate a dataset (matrix vector is 500 x 1000). We have 500 testing devices, for each device

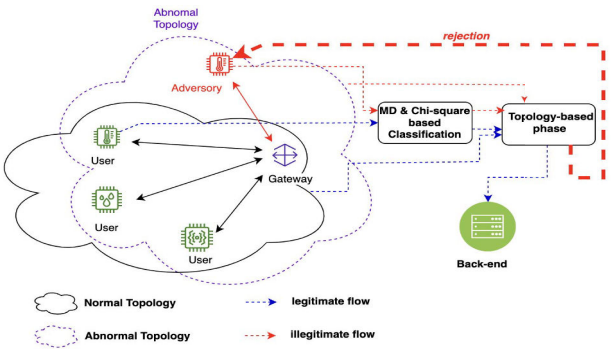

Fig. 3. Monitoring the abnormal topology to detect the illegitimate node.

TABLE II
TRUTH TABLE

MD & Chi-square based authentication	Topology-based authentication	Authentication decision
TRUE	TRUE	TRUE
TRUE	FALSE	FALSE
FALSE	TRUE	FALSE
FALSE	FALSE	FALSE

Algorithm 1: The work-flow of the proposed framework

RF Collection and Extraction Phase
Inputs: *raw data* (RF raw signals)
q (number of features)
i_j (address of the jth legitimate IoT nodes)
z (number of legitimate IoT nodes)
l_j (distance of the jth node to gateway)
Outputs: data : $df_{q\times j}$
$df_{l\times j}$

MD & Chi-square based Classification Phase
Inputs: $df_{q\times j}$
The mean: $mean = \sum_{k=1}^{z} i_j/z$
Cut-off value: $cv = \frac{\gamma(\frac{q}{2},\frac{1}{2})}{\Gamma(\frac{q}{2})}$
Mahalanobis Distance: $dM_j = (\sqrt{(i-mean)^T.C(mean)^{-1}.(i-mean)}$
if $dM_j <= cv$:
authenticationA = **TRUE**
else :
authenticationA = **FALSE**
Outputs: *authentication*

Topology-based authentication Phase
Inputs: $df_{l\times j}$
z (number of legitimate IoT nodes)
z_R (number of IoT nodes at time R)
if $z \neq z_R$:
abnormal = **TRUE**
The mean: $meanA = \sum_{k=1}^{z} i_j/z$
Cut-off value: $cvA = \frac{\gamma(\frac{1}{2},\frac{1}{2})}{\Gamma(\frac{1}{2})}$
Mahalanobis Distance: $dMA_j = (\sqrt{(i-meanA)^T.C(meanA)^{-1}.(i-meanA)}$
if $dMA_j <= cvA$:
authenticationB = **TRUE**
else :
authenticationB = **FALSE**

Final authentication phase
if *authenticationA* == **TRUE** *AND* *authenticationB* == **TRUE**:
AccessControl = **grant**
else :
AccessControl = **deny**

TABLE III
RF FEATURES USED IN OUR EXPERIMENTS

No.	Features	Mean	Standard Deviation
1	Carrier Frequency Offset(CFO)	2.4 GHz	48 kHz
2	RSSI	-50 dBm	5 dBm

TABLE IV
COMPARISON OF OUR METHOD WITH OTHER IMPERSONATION ATTACKS AT SNR=30 AND THE NUMBER OF DEVICES ARE 500

Metric	Autoencoder [17]	SAE [14]	CNN [12]	Proposed method
Accuracy score	83.62%	98%	98.01%	99%
F1-score	0.9106	0.9111	0.9872	0.9949
Precision	0.8422	0.8430	0.9852	0.9998
Recall	0.9909	0.9909	0.9936	0.9901

we have slightly changed the Carrier Frequency offset and the RSSI to stimulate the nonideality of RF features. Table III shows the features we have used as well their mean and standard deviation. Each device provides 5000 RF signal data.

We first show the results related to the average detection accuracy of our scheme at different numbers of devices and different values of SNR, shown in Fig. 4. It is seen that the average accuracy does not drop much at varying SNR values, even at high SNR values too. We have also compared our scheme with recent existing research works [12], [14], and [17], as shown in Table IV. We have used four key metrics for our evaluation, accuracy, F1-score, precision, and recall. Our solution outperformed in this comparison.

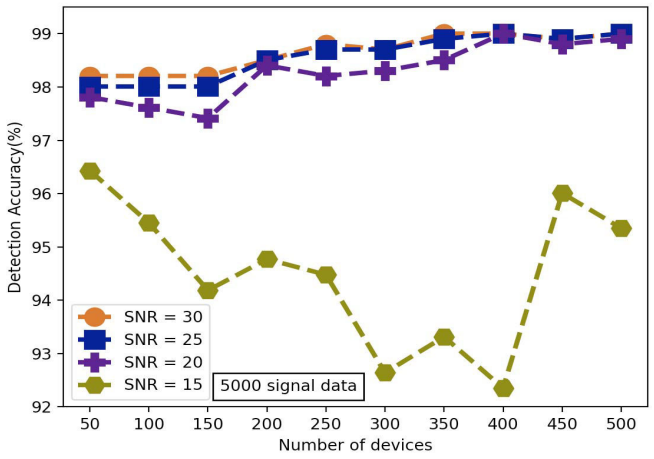

Fig. 4. Average detection accuracy of our scheme at different number of devices and different values of SNR.

As we have mentioned that the proposed modules are deployed as VNFs, so to get insights on the performance of the proposed approach in real-life 5G platform, we use OSM-MANO for our evaluation. The proposed module (as well as sub-modules) is implemented as a VNFs, on Amazon Web Services (AWS) platform. The VNFs are deployed by the Network Service (NS) manager on OSM (Open Source Mano). The Open-Source MANO (OSM) version 10 is installed on an Amazon Elastic Compute Cloud (Amazon EC2). The EC2 has 8 GB of RAM and 4 virtual CPUs (Intel Xeon processors). The OSM links to the AWS-represented Virtualized Infrastructure (VI). In 5G, the system is compliant with the ETSI-NFV architecture. The OSM deploys Classification-VNF and Topology-based authentication-VNF, with each VNF having

16 GB of RAM and 8 vCPU (Intel Xeon processors). Python 3.6.9, Keras 2.8.0 and Tensorflow version 1.15.0 are used in these VNFs. The structural diagram is shown in Fig. 5.

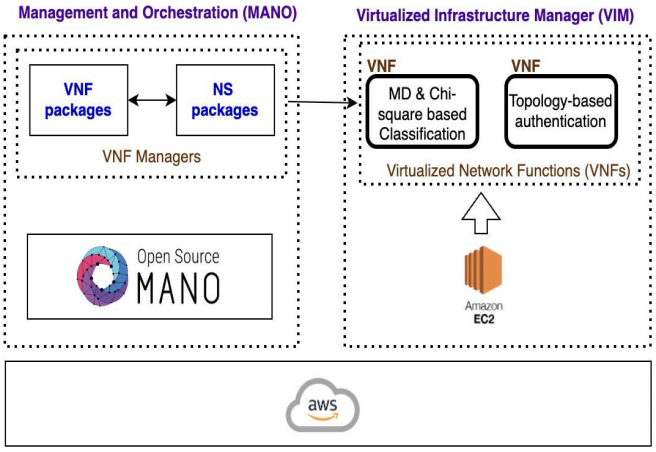

Fig. 5. Structural diagram of our testing platform.

We have rigorously evaluated our approach's performance to see how it actually fits in the real-world deployment. From Fig. 6 we note that in comparisons to other works, the CPU Utilization of our approach is significantly reduced. Fig. 7 shows the time our proposal takes to classify and authenticate the node. This is reasonably better than two approaches but significantly better than CNN model. From our results, we see a trade-off between accuracy and detection time. Overall, the performance of our approach is considerably better than the existing approaches.

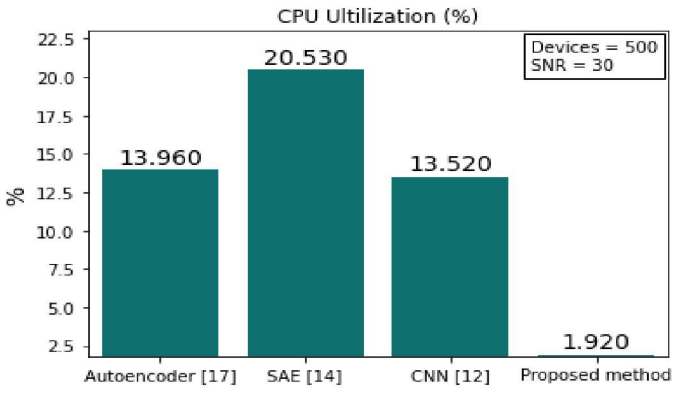

Fig. 6. CPU utilization comparisons.

V. Further Discussion

We have proposed an approach to mitigate Impersonation Attack in IoT networks. The presented work has shown promising results. However, we note that there are many aspects we have not discussed in this paper. Some of the key aspects are listed here for interested readers.

1) The proposed solution (and the related high-level description) is classical involving features collection and authentication, Nevertheless, it is worth noting that RF collection is simulated, and this is one of the weaknesses of the current version of the work. We counter argue that our simulations provide valid preliminary results and in future instead of relying on custom simulations we plan to use available real-data set. At this stage, our current work is promising and to significant extent addressed the common problems of the existing literature particularly the recent works with whom we have compared our results.
2) In the current version due to time and space, we have provided limited discussion on the processing overhead. It is true that training is CPU/GPU intensive operation, IoT devices are not supposed to do that. In future, we can assume a scenario where a model is trained according to the deployed devices, while only the testing process is run on the device itself (to identify and authenticate the peer). The testing process is well recognized to be less intensive and deployable on any platform.
3) A fundamental and interesting future work, form this version, would be to investigate why the two statistics (Mahalanobis distance and Chi-Square) allow high accuracy without resorting to AI. What do they capture in contrast to previous work is worth investigating.

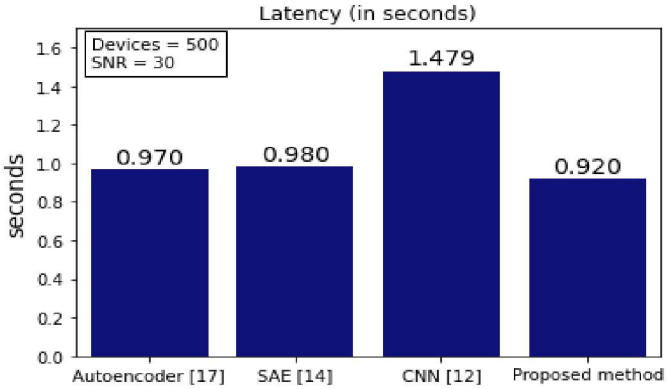

Fig. 7. Detection time comparisons.

VI. Conclusion and Future Work

In the paper, we have proposed a Deep-Learning (DL)-driven method for Physical-Layer Authentication (PLA) of Internet of Things (IoT) devices in the 5G ecosystem. Our method is using metrics such as the Mahalanobis Distance and Chi-square distribution theories. We have tested the proposed approach through simulations, achieving higher classification accuracy than similar methods currently available in the literature, as well as reduced training time. A comparison with current state of art approaches is shown. In future, we plan to address the gaps listed in further discussion section. Particularly, we plan to test the proposed solution by adopting one (or more) of the publicly available datasets involving real measurements.

REFERENCES

[1] F. Alawad and F. A. Kraemer, "Value of information in wireless sensor network applications and the iot: A review," *IEEE Sensors Journal*, vol. 22, no. 10, pp. 9228–9245, 2022.

[2] P. Abichandani, V. Sivakumar, D. Lobo, C. Iaboni, and P. Shekhar, "Internet-of-things curriculum, pedagogy, and assessment for stem education: A review of literature," *IEEE Access*, vol. 10, pp. 38 351–38 369, 2022.

[3] I. Ali, I. Ahmedy, A. Gani, M. U. Munir, and M. H. Anisi, "Data collection in studies on internet of things (iot), wireless sensor networks (wsns), and sensor cloud (sc): Similarities and differences," *IEEE Access*, vol. 10, pp. 33 909–33 931, 2022.

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

[5] S. Rajendran and Z. Sun, "Rf impairment model-based iot physical-layer identification for enhanced domain generalization," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1285–1299, 2022.

[6] K. Sood, K. K. Karmakar, S. Yu, V. Varadharajan, S. R. Pokhrel, and Y. Xiang, "Alleviating heterogeneity in sdn-iot networks to maintain qos and enhance security," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 5964–5975, 2020.

[7] A. N. Bikos and S. A. P. Kumar, "Securing digital ledger technologies-enabled iot devices: Taxonomy, challenges, and solutions," *IEEE Access*, vol. 10, pp. 46 238–46 254, 2022.

[8] K. Sood, M. R. Nosouhi, N. Kumar, A. Gaddam, B. Feng, and S. Yu, "Accurate detection of iot sensor behaviors in legitimate, faulty and compromised scenarios," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2021.

[9] Z. Wang, H. Zhu, and L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods," *IEEE Access*, vol. 9, pp. 11 895–11 910, 2021.

[10] T. Li, Z. Hong, L. Liu, Z. Wen, and L. Yu, "¡italic¿meta-wf¡/italic¿: Meta-learning-based few-shot wireless impersonation detection for wi-fi networks," *IEEE Communications Letters*, vol. 25, no. 11, pp. 3585–3589, 2021.

[11] T. Kwon, "Impersonation attacks on software-only two-factor authentication schemes," *IEEE Communications Letters*, vol. 6, no. 8, pp. 358–360, 2002.

[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 *2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC)*, 2019, pp. 98–104.

[13] X. Wang, L. Kong, Z. Wu, L. Cheng, C. Xu, and G. Chen, "Slora: towards secure lora communications with fine-grained physical layer features," in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, 2020, pp. 258–270.

[14] S. J. Lee, P. D. Yoo, A. T. Asyhari, Y. Jhi, L. Chermak, C. Y. Yeun, and K. Taha, "Impact: Impersonation attack detection via edge computing using deep autoencoder and feature abstraction," *IEEE Access*, vol. 8, pp. 65 520–65 529, 2020.

[15] W. Lee, S. Y. Baek, and S. H. Kim, "Deep-learning-aided rf fingerprinting for nfc security," *IEEE Communications Magazine*, vol. 59, no. 5, pp. 96–101, 2021.

[16] M. Ezuma, F. Erden, C. Kumar Anjinappa, O. Ozdemir, and I. Guvenc, "Detection and classification of uavs using rf fingerprints in the presence of wi-fi and bluetooth interference," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 60–76, 2020.

[17] M. R. Nosouhi, K. Sood, M. Grobler, and R. Doss, "Towards spoofing resistant next generation iot networks," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1669–1683, 2022.

[18] J. Lu, T. Morehouse, J. Yuan, and R. Zhou, "Machine-learning puf-based detection of rf anomalies in a cluttered rf environment," in *2021 IEEE International Symposium on Technologies for Homeland Security (HST)*, 2021, pp. 1–7.

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

[20] J. Jin, Y. Zhu, Y. Zhang, D. Zhang, and Z. Zhang, "Micrometeoroid and orbital debris impact detection and location based on fbg sensor network using combined artificial neural network and mahalanobis distance method," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1–10, 2021.

[21] G. Gallego, C. Cuevas, R. Mohedano, and N. García, "On the mahalanobis distance classification criterion for multidimensional normal distributions," *IEEE Transactions on Signal Processing*, vol. 61, no. 17, pp. 4387–4396, 2013.

[22] D. D. N. Nguyen, K. Sood, M. R. Nosouhi, Y. Xiang, L. Gao, and L. Chi, "Rf fingerprinting based iot node authentication using mahalanobis distance correlation theory," *IEEE Networking Letters*, pp. 1–1, 2022.

[23] S. Sun, "Segmentation-based adaptive feature extraction combined with mahalanobis distance classification criterion for heart sound diagnostic system," *IEEE Sensors Journal*, vol. 21, no. 9, pp. 11 009–11 022, 2021.

[24] N. Su, X. An, C. Yan, and S. Ji, "Incremental attribute reduction method based on chi-square statistics and information entropy," *IEEE Access*, vol. 8, pp. 98 234–98 243, 2020.

[25] Y. Zhu and L. Zhou, "A novel approach for fault detection in integrated navigation systems," *IEEE Access*, vol. 8, pp. 178 954–178 961, 2020.