Intrusion Detection for IoT Devices based on RF Fingerprinting using Deep Learning

Conference Paper · June 2019

DOI: 10.1109/FMEC.2019.8795319

6 authors, including:

Joshua Bassey
Prairie View A&M University
11 PUBLICATIONS **168** CITATIONS
SEE PROFILE

Damilola Adesina
Prairie View A&M University
9 PUBLICATIONS **135** CITATIONS
SEE PROFILE

Xiangfang Li
Institute of Electrical and Electronics Engineers
269 PUBLICATIONS **6,871** CITATIONS
SEE PROFILE

Lijun Qian
Prairie View A&M University
234 PUBLICATIONS **3,449** CITATIONS
SEE PROFILE

Intrusion Detection for IoT Devices based on RF Fingerprinting using Deep Learning

Joshua Bassey, Damilola Adesina, Xiangfang Li, Lijun Qian
CREDIT Research Center
Prairie View A&M University, Texas A&M University System
Prairie View, TX 77446, USA
Email: jbassey, dadesina, xili, liqian@pvamu.edu

Alexander Aved, Timothy Kroecker
Information Directorate
US Air Force Research Laboratory (AFRL)
Rome, NY 13441, USA
Email: alexander.aved, timothy.kroecker@us.af.mil

***Abstract*—Internet of Things (IoT) and 4G/5G wireless networks have added huge number of devices and new services, where commercial-of-the-shelf (COTS) IoT devices have been deployed extensively. To ensure secure operations of these systems with wireless transmission capabilities, Radio Frequency (RF) surveillance is important to monitor their activities in RF spectrum and detect unauthorized IoT devices. Specifically, in order to prevent an adversary from impersonating legitimate users using identical devices from the same manufacturer, unique "signatures" must be obtained for every individual device in order to uniquely identify each device. In this study, a novel intrusion detection method is proposed to detect unauthorized IoT devices using deep learning. The proposed method is based on RF fingerprinting since physical layer based features are device specific and more difficult to impersonate. RF traces are collected from six "identical" ZigBee devices via a USRP based test bed. The traces span a range of Signal-to-Noise Ratio, to ensure robustness of the model. A convolutional neural network is used to extract features from the RF traces, and dimension reduction and de-correlation are performed on the extracted features. The reduced features are then clustered to identify IoT devices. We show that the proposed method is able to identify devices that are not observed during training. The results not only highlight the benefit of deep learning based feature extraction, but also show promising prospects for being able to distinguish new devices (classes) that are not observed during training.**

***Index Terms*—RF fingerprinting, Deep Learning, ZigBee, Internet of Things.**

I. Introduction

Despite its promising benefits, Internet of Things (IoT) systems, devices and networks with wireless interfaces, remain vulnerable to various kinds of attacks due to the broadcast nature of wireless transmissions [1]. The last line of defense tailored specifically sustaining system security are Intrusion Detection Systems (IDS) [2].

To provide a context for this work, assume a number of authorized IoT devices with wireless interfaces (e.g., WiFi) are deployed in a secure building. These devices are typically connected to an access point. Several types of intrusion are possible. For example, an intruder with an unauthorized device attempts to impersonate an authorized device in order to gain access to a secure server. In this case, there are many existing approaches to mitigate this type of intrusion effectively such as certificate-based authentication methods. Thus this type of intrusion is *not* considered in this work.

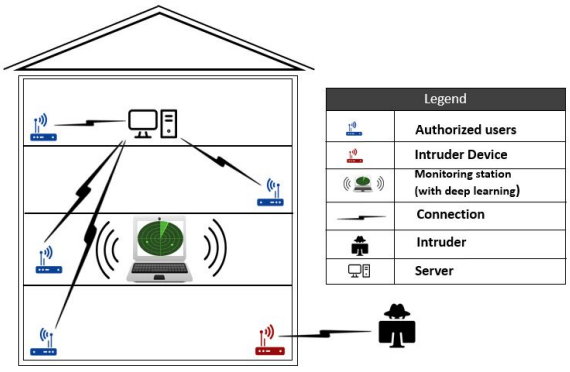

Fig. 1. Motivating Example Scenario

On the contrary, consider the following scenario (Fig. 1): An intruder succeeds in smuggling a device such as a smart phone into the building, obtains data such as pictures or video and transfers the data to a receiving device outside the building wirelessly. In this case, intrusion occurs even though the intruder does not require access to the secure servers. Hence certificate-based methods are not effective in preventing such intrusion.

In order to defend against this type of intrusion, a Radio Frequency (RF) surveillance station could be installed in the building to monitor the RF spectrum and collect all RF traces in and around the building. Then intrusion detection is performed at the physical layer using RF features. Unlike identifiers at other layers such as MAC addresses and International Mobile Subscriber Identity (IMSI) numbers, RF features are very difficult to impersonate [3], [4].

However, there exist many challenges:

- An intruder might acquire and attempt to use the "same" device as an authorized device. By "same" we mean that a device that is of the same model from the same manufacturer. This means that the signal characteristics emanating from the devices will be almost identical.
- Most data-driven approaches that rely on machine learning and deep learning require data from all classes of interest to train the models. However, the RF traces of an intruder are not available for training in practice.

978-1-7281-1796-6/19/$31.00 ©2019 IEEE

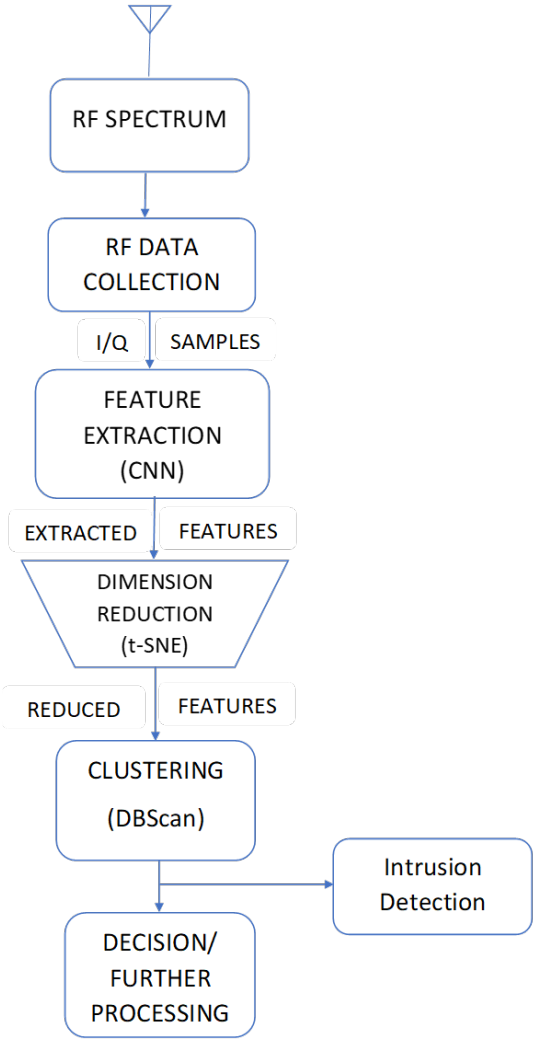

Fig. 2. Proposed Model Pipeline

- Factors like variation in channel conditions, device mobility and noise will cause variations in the SNR levels of the RF signal. The intrusion detection system should be robust to these changes.

To address these challenges, a novel deep learning based detection scheme is proposed in this paper. Specifically, we rely on the fact that RF features at the physical layer are unique to each device. Even for RF devices of the same model from the same manufacturer, there are hardware imperfections inherent to electronic components that result from factors such as solder variations, MMIC fabrication imperfections and tolerances on passive and active devices, that affect inherent signaling characteristics, and allow us to get unique fingerprint of any device [5], [6].

In order to learn these unique fingerprints and use them to detect unauthorized RF devices, a novel integrated approach using convolutional neural networks (CNN), dimension reduction and de-correlation, and clustering is proposed. The CNN is trained using RF traces collected from authorized devices. The goal is not for classification, but to "extract" the relevant and device inherent features from the RF traces. In other words, the proposed intrusion detector only use the feature extraction part of the CNN. The dimension of the features are then reduced, and clustering is performed to distinguish different devices. Because each device will have unique features, the number of clusters represents the number of RF devices. The unauthorized device will be detected when the number of clusters exceed the number of the authorized devices. Fig.2 highlights our proposed approach. The proposed scheme is tested using real RF traces collected from six ZigBee devices. Samples from one device were excluded from the training and mixed with samples from the other five devices during testing. It is observed that RF samples not used during training can be identified. The proposed method achieves 78% detection accuracy in our experiments.

The remainder of the paper is structured in the following manner: In Section II, details on the approach employed in the collection of the RF signals from ZigBee devices are provided. In Section III we provide details about the proposed framework and model architectures. Section IV contains the experimental results and corresponding evaluations. Section V outlines related research on IoT device intrusion detection based on RF, and sheds some light on factors that affect performance. Finally Section VI presents conclusions and future works.

II. Dataset Generation

The RF data used in this work was obtained from MICAz-MPR2400, a Mote module from Crossbow Technology. It incorporates a IEEE 802.15.4 compliant ZigBee ready RF transceiver operating from 2.4 to 2.48 GHz. ZigBee, a technology developed for low-cost, low-power communications in wireless IoT networks, is a protocol that guarantees interoperability of products irrespective of manufacturers. A core advantage offered is long battery life due to the very small duty cycle and very low latency. In this work, the MICAz motes are configured for data transfer two times per second.

The RF IQ traces were captured for six ZigBee devices using NI USRP-293x Software Defined Radio Devices in receiver mode via LabVIEW. The USRPs are tunable RF transceivers with a high-speed analog-to-digital, and digital-to-analog converter for streaming baseband I and Q signals to a host PC over 10 Gigabit Ethernet. The USRP-293x is able to capture signals at frequencies up to 4.4GHz and bandwidth up to 20MHz. In our experimental testbed, the carrier frequency is configured on channel 26 in order to have minimal interference from other devices in the 2.4GHz ISM band. All six ZigBee devices were configured to transmit at 0, -1, -5,-10, and -15 dBm SNR. this is done to simulate real life scenario which include the effect of degraded and distant signals, varying channel conditions, noise and device mobility. Furthermore, all devices were moved during part of the transmission in order to represent real -life dynamic environment.

The features consist In-phase (I) and Quadrature (Q). An example of the collected I and Q data at 0 dBm is shown in Figure 3. The total data size for all six devices is about 300

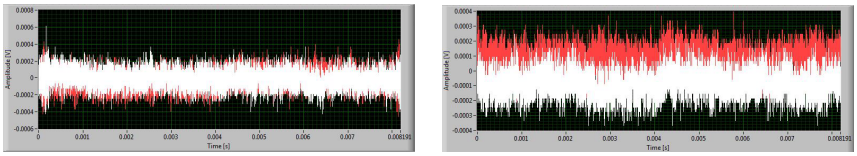

Fig. 3. Captured RF Data from 2 ZigBee devices (20 Frames at 2 Frame/Second)

GB, approximately 50 GB of collected RF data per ZigBee device. For each of the collected classes, data collected at each SNR adds up to approximately 10 GB for 5 minutes of collected data. The RF traces were filtered to capture only the areas of burst transmission; as is peculiar with ZigBee transmissions and the number of samples used were restricted to 100 million samples per device. This filtering greatly reduces the data size. Five (out of six) Zigbee radios are assumed to be authorized devices, while the sixth radio is the intruder.

The raw RF data from the authorized Zigbee radios was filtered and fed into the model pipeline for training as highlighted in Figure 2, which is comprised of a deep learning model for feature extraction, dimension reduction and a clustering algorithm. After training, the obtained model pipeline will cluster the data from authorized devices into five clusters, each corresponds to one of the authorized device. When the RF data from the sixth radio go through the trained pipeline, it will be clustered as a new cluster (the intruder).

III. Model Architectures

The problem of intrusion detection of unauthorized IoT devices using RF traces is not a trivial task. Deep learning is most suitable for this problem, having achieved ground breaking success in applications like computer vision, speech, text, and signal processing. However, the problem becomes more complex when detection (or classification) is required for data belonging to devices that are not part of the training. Deep learning is based on the premise that data fed into the model; both training and test data, belong to the same distribution, even though this true distribution is not known. This is where most deep learning based methods to intrusion detection such as RF fingerprinting breaks. RF fingerprinting, although very accurate in many applications, is formulated as a classification problem in previous studies. Therefore, if RF traces belonging to a class that is not seen during training pass through the model for inference, such trace will be misclassified as one of the classes previously observed during training.

To tackle this problem, we use deep learning for feature extraction, rather than classification. In this work, deep learning is used in conjunction with dimension de-correlation and clustering algorithms. Deep learning are neural networks with variant architectures, made up of multiple layers, that are able to learn nonlinear functions. The multiple layer architecture makes it possible to learn representations of data at different levels. Deep learning has proven successful in computer vision, object detection and other applications. There is hardly any other method that is as effective in the automatic generation of relevant features from RF data.

A. Feature Extraction

The deep learning model used for extracting features is the convolutional neural network (CNN). CNNs are a type of feed-forward neural network that are based on the concept of weight sharing. The layers of CNNs are structured in three dimensions; height, width and depth. Furthermore and the neurons in a layer are only connected to a small fraction of neurons in the next layer and not all the neurons. The dimensions are reduced along the depth dimension for the output vector. A CNN architecture can be broadly separated into two components; (i) the hidden layer/Feature extraction section, is the section where convolution and pooling is performed, (ii) the classification part is the part where a probability score is assigned to signify the prediction of the algorithm [7]. CNNs have achieved success in applications involving time series data such as natural language, audio, and in recent times I/Q data [8]. The model training was implemented using TensorFlow on an Nvidia Tesla P100-PCIE-16 GB GPU.

Although a CNN model is typically trained as classification model, it was demonstrated in [9] that it is possible to cluster the features extracted from a CNN. This method, called *supervised bootstrapping*, was applied for modulation classification in radio signal classification. In this method, the CNN was first trained as a classification model. After training the CNN (as a classifier), then by passing the raw I/Q samples in a feed-forward pass for inference, the relevant features are extracted. Specifically, In this work, we modify the idea of the supervised bootstrapping and use the output of the layer just before the Softmax layer as features.

Fig.4 shows the architecture employed for feature extraction. The network was trained using raw I/Q samples that are broken into 2 dimensions based on different window sizes. There are two 2D convolutional layers, followed by a fully connected layer and an output layer. The output layer uses the Softmax activation, all other layers make use of RELU non-linearity. To mitigate over-fitting, dropout was added after each convolutional layer and before the fully connected layer.

B. Feature De-correlation and Dimension Reduction

The accuracy of the CNN model is evaluated from the Softmax outputs of the training data. The better the accuracy of the network, the more representative the features will be. The extracted features from the CNN model were processed for feature de-correlaton and dimension reduction before clustering. There are two reasons for this. The first

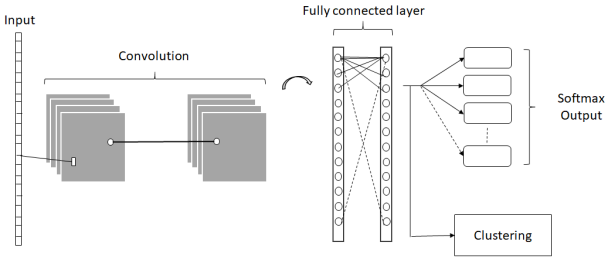

Fig. 4. CNN model for feature extraction

reason is to reduce collinearity between the features for better clustering. The second reason is for dimension reduction and better visualization.

t-Distributed Stochastic Neighbor Embedding (t-SNE) was used for dimension reduction. t-SNE is a non-linear unsupervised learning method that overcomes limitations of Principal component analysis (PCA). It has proven effective in visualization of high-dimensional datasets. t-SNE creates a mapping from the high-dimensional data to a low-dimensional data, while preserving the local distances of the high-dimensional data. In other words, the model tries to preserve the distance between each input vector. The distances between the points in the low-dimensional map are modeled by the t-distribution, and a modified Kullback-Leibler divergence is applied to correct asymmetry.

t-SNE is generally used as for visualization and not in classification models because it does not learn a function from the original space to the new (lower) dimensional space. However t-SNE offers even more potential when used with a non-distance based clustering algorithm like DBScan. Hence, we apply DBScan clustering at the output of t-SNE dimension reduction stage.

C. Clustering and Intrusion Detection

The reduced features were then passed through a clustering algorithm. Clustering is a an unsupervised learning paradigm whereby data that are deemed "similar" according to certain features are attributed to the same cluster. cluster formation is either by partitioning (e.g. K-means), hierarchical (e.g. agglomerative clustering), or density-based methods (e.g. DBScan) [10].

In this work, DBScan was used. because partition based clustering would require knowledge of the number of clusters, which is not practical in this application. Also, a comparison of the performance showed that DBScan performed better than hierarchical clustering methods for this application.

DBScan works on a density-based notion of a cluster, and is able to find clusters of arbitrary shape in spatial databases with noise. Points in high-density are grouped together and points that lie alone in low density region are marked as outliers. DBScan is defined by two parameters; (1) the radius of the neighborhood of point p and (2) the minimum number of points in the given neighborhood [10]. 10,000 samples for each selected window (feature) size of 64 were chosen, 80% of the data was used to fit the DBScan model and the remaining 20% for prediction.

TABLE I
CNN ACCURACY SCORES FOR VARYING WINDOW SIZE AND DROPOUT RATE

SNR (dB)	Dropout Rate	Window Size		
		32	64	128
[0]	0.5	96.6%	98.8%	96.4%
	1 (No dropout)	93.2%	98.8%	96.1%
[0,-1,-5,-10,-15]	0.5	97.4%	97.7%	97.3%
	1 (No dropout)	96.1%	97.6%	96.4%

IV. RESULTS

The performance of the CNN model is evaluated to illustrate the ability of deep learning models to extract relevant salient device-dependent features. As stated before, it is assumed that five ZigBee devices (MICAz) are authorized while the sixth is the intruder. Training was done on 80% of the I and Q samples of the data collected from the five authorized devices for a mixture of five SNR levels. The remaining 20% of the data was split into test and validation sets, each containing 10% of the I and Q samples.

It is important to note again that obtaining data for each device at a combination of various SNR levels is used to mimic the effect of variation in channel conditions, noise as well as effect of multipath and device mobility. The testing data from the five authorized devices are mixed with the data from the sixth device (the intruder) that is excluded from training. The learning process was repeated for different learning rates and window sizes to obtain the appropriate model that yields the most representative features.

Table I shows the accuracy scores for the CNN feature extraction model as a function of window size and dropout. With no dropout, the model performs relatively comparably across window sizes. However, the most optimal results seem to be gotten at a window size of 64. The model performs slightly better when a dropout rate of 0.5 is applied after all convolutional layers and before the softmax layer. This is indicative of better generalization of the CNN model. Table II shows the training time of the signal for the same parameters as shown in table I. It can be inferred that the computational time reduces with increasing window size.

It is important to observe that the results obtained when the data gathered is at a single SNR level are comparable to the results obtained when the data gathered includes RF data at various SNR levels. This is indicative of the fact that the CNN is able to extract device-inherent features and its performance is not adversely affected by varying channel conditions and device mobility. This observation is vital as these change in conditions are representative of real life scenarios.

Fig.5 shows an example visualization of the t-SNE dimensionality reduction performed on the extracted features from testing data. The t-SNE model reduces the data to two principal dimensions which are represented by the x and y

TABLE II
CNN TRAINING TIME IN SECONDS FOR VARYING WINDOW SIZE AND DROPOUT RATE

SNR (dB)	Dropout Rate	Window Size		
		32	64	128
[0]	0.5	36.3	29.4	22.7
	1 (No dropout)	46.7	30.3	23.1
[0,-1,-5,-10,-15]	0.5	205.9	130.8	99.3
	1 (No dropout)	208.7	133.64	100.21

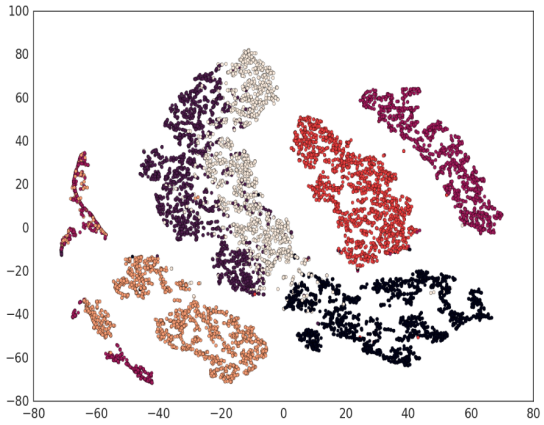

Fig. 5. t-SNE clustered features with one class unseen, for 3000 samples

axes. The testing data include data from the five authorized devices and the data from the sixth device (the intruder, in grey) that is excluded from training. It can be observed that although considered a hard problem in the context of machine learning, our approach is able to correctly cluster a reasonable number of samples even when some of them belong to a cluster that is not trained. In the figure it is seen that the larger cluster in the middle is still further separated into two clusters.

On the contrary, if a CNN model (or any other deep learning model) was trained as a classifier without the data of an additional class, then during testing, the data from that class will be miss-classified. In fact, the data of the additional class will be classified as one of the classes observed during training. Therefore, the proposed method is particularly promising because it can identify previously unobserved class/cluster. Furthermore, the data was collected across a range of SNR levels to ensure a robust model.

TABLE III
PERFORMANCE EVALUATION FOR CLUSTERING / INTRUSION DETECTION

SNR (dB)	Metrics	Window Size		
		32	64	128
[0,-1,-5,-10, -15]	AMI	0.66	0.73	0.79
	RAND Index	0.48	0.62	0.70
	Time (Secs)	31.96	29.71	30.18
[0,-1,-5,-10]	AMI	0.56	0.68	0.71
	RAND Index	0.41	0.60	0.65
	Time (Secs)	31.38	30.13	30.85

Table III shows the performance metrics of the clustering /intrusion detection phase. The performance metrics considered are the Adjusted Mutual Information (AMI) index, the Rand Index, and the training time. AMI is based on Shannon's information theory and is used to compare different clusterings using mutual information. AMI index computes the mutual information (MI) between between two clusterings and makes adjustments for chance [11]. Rand Index is similar to AMI but was inspired by typical classification problems where classification schemes are compared to a correct classification. Rand extends the popular performance measure of computing for all elements, the fraction of correctly classified or misclassified elements. Both AMI and Rand index range from 0 to 1 with higher scores representing better performance.

It can be seen that for a data set containing containing all RF data at all SNR levels, AMI index of up to 78% and Rand index of 70% is obtained. The Rand index is typically lower than the AMI score since there is some penalization for so called false positives. a similar trend is observed for when the data does not contain RF traces for the devices at -15dB. Another interesting observation is that larger window size seems to yield better results but up to an optimal window size of 128. For window size higher than 128, the performance begins to drop.

The training time here considers the t-SNE feature decorrelation and the clustering /intrusion detection as one module because clustering times are almost negligible compared to the time required for t-SNE dimension reduction. However, all times for this phase are comparable. In summary, it is still possible to see the disparities between a majority of both classes of interest when applying our model pipeline. This would otherwise either be impossible or produce poor results if a standalone classifier (as in typical RF fingerprinting), clustering, or even the bootstrap (CNN+clustering) was used.

In this work, we also include a baseline model where all the data (including the data from the intruder) are assumed available for training. Fig.6 shows an example visualization of the t-SNE dimensionality reduction when all the classes in the dataset were used for training. This figure shows that the features generated by the neural network are representative of the RF data obtained from the ZigBee data, because the classes are properly distinguished from each other in separate clusters. This could be another method of performing device fingerprinting.

V. DISCUSSION AND RELATED WORKS

In [12], the implementation of a passive target intrusion detection in a cognitive radio network (CRN) was proposed. In their work, orthogonal frequency-division multiplexing (OFDM) waveforms were used for active sensing, and support vector machine (SVM) was used in feature-based intrusion detection on collected radio energy data. The SVM was modeled with a "one against all" configuration, where given K classes, K binary classifiers are built to separate each class from all other classes. In [6], the authors performed RF device fingerprinting by using SVM, CNN and deep neural nets, and

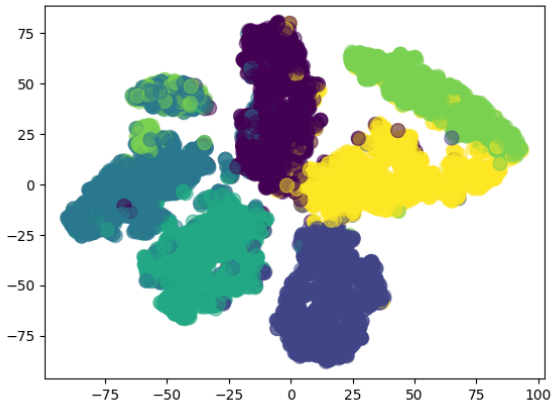

Fig. 6. Baseline model where it is assumed that all data (including the intruder's data) are available for training.

[13] applied deep learning to detect physical-layer attributes for the identification of cognitive radio devices using time-domain complex baseband error signal. These works do not consider that training data of some classes are unavailable.

In [3], the authors used the statistics of the RF based features to fingerprint the individual packet sources in a network. The feature vectors were sorted by the intrusion detector, which also generates a probability distribution for each feature from the feature vectors. Detection is triggered when there is an anomaly in the modal characteristics of previous sequences of the feature vector for each feature. In [14]–[16], the focus is more on the use of dimensionality reduction to improve classification performance, and come up with RF-distinct native attributes (RF-DNA). However, these methods do not use deep learning.

An anomaly detection technique based on a deep predictive coding neural network, for analyzing RF spectrum in wireless systems was proposed in [17]. In their work, frequency-domain data obtained from time-domain data were stored as sequential 2D images. The image sequences were then fed into a deep learning video predictor which attempts to predict the next frame from previous frames. Anomaly detection is triggered when there is a deviation between the actual and predicted spectrum behavior. In [18], an anomaly identification method in temporal-spectral data was proposed. They generate models from historical data and compare the historical data with real-time data for intrusion detection. These approaches do not require RF data from all classes. However, there is a challenge of specifying what normal system behavior means, as well as defining an appropriate threshold.

The authors of [19] employed a CNN to extract features, and DBSCAN clustering to determine the number of emitters. The authors directly cluster the CNN features and use t-SNE only for visualization of clustered output. Furthermore, the model was trained and tested with data of just one SNR value.

To the best of our knowledge, the existing methods in the literature either do not consider the unavailability of data from some classes during training, or train their models with data of only one SNR level. In general, a machine learning classification model must observe example data from each class for which it has to predict. However, this may not be always satisfied in reality. In case there are data from new classes that are not trained, our proposed approach is able to mitigate this major constraint. Furthermore, our approach circumvents the challenge of having to specify what a "normal system behavior" is.

VI. Conclusions

In this work, a novel model pipeline aimed at intrusion detection based on RF fingerprinting using deep learning to enhance IoT security is proposed. We take advantage of the strength of deep learning models driven by wireless big data, dimensionality reduction, and clustering algorithms. The model pipeline is tested on RF traces collected from ZigBee devices over a range of SNR levels, so as to ensure the robustness of the proposed model to varying conditions of the wireless channel. The experimental results demonstrate the effectiveness of the proposed method. In general, a machine learning classification model must observe example data from each class for which it has to predict. However, this is often not true for intrusion detection in reality. In case there are data from an intruder that are not available for training, the classification model would miss-classify. On the contrary, the proposed approach is particularly promising because it can identify previously unobserved class/cluster. Furthermore, the data was collected across a range of SNR levels to ensure a robust model.

There are a number of parameters that affect the performance. For example, different parameters for the t-SNE clustering could have a drastic effect on the dimension reduction and consequently the clustering. To this end, on-going work involves investigating effective methods to learn the most appropriate hyper-parameters for the t-SNE dimension reduction, as well as to quantitatively analyze the scalability of the proposed approach.

VII. Acknowledgment

This research work is supported in part by the U.S. Dept. of Navy under agreement number N00014-17-1-3062 and the U.S. Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) under agreement number FA8750-15-2-0119. The U.S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Dept. of Navy or the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) or the U.S. Government.

REFERENCES

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct 2017.

[2] L. Santos, C. Rabadao, and R. Gonalves, "Intrusion detection systems in internet of things: A literature review," in *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, June 2018, pp. 1–7.

[3] A. A. Tomko, C. J. Rieser, and L. H. Buell, "Physical-layer intrusion detection in wireless networks," in *MILCOM 2006 - 2006 IEEE Military Communications conference*, Oct 2006, pp. 1–7.

[4] T. OShea and J. Hoydis, "An introduction to deep learning for the physical layer," *IEEE Transactions on Cognitive Communications and Networking*, vol. PP, no. 99, pp. 1–1, 2017.

[5] S. U. Rehman, K. Sowerby, and C. Coghill, "Analysis of receiver front end on the performance of rf fingerprinting," in *2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)*, Sept 2012, pp. 2494–2499.

[6] K. Youssef, L. Bouchard, K. Haigh, H. Krovi, J. Silovsky, and C. P. Vander Valk, "Machine learning approach to rf transmitter identification," 11 2017.

[7] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016, http://www.deeplearningbook.org.

[8] K. O'Shea and R. Nash, "An introduction to convolutional neural networks," 11 2015.

[9] T. J. O'Shea, N. West, M. Vondal, and T. C. Clancy, "Semi-supervised radio signal identification," 2016.

[10] A. Ram, J. Sunita, A. Jalal, and K. Manoj, "A density based algorithm for discovering density varied clusters in large spatial databases," *International Journal of Computer Applications*, vol. 3, 06 2010.

[11] S. Romano, N. X. Vinh, J. Bailey, and K. Verspoor, "Adjusting for chance clustering comparison measures," *J. Mach. Learn. Res.*, vol. 17, no. 1, pp. 4635–4666, Jan. 2016. [Online]. Available: http://dl.acm.org/citation.cfm?id=2946645.3007087

[12] C. Zhang, Z. Hu, T. N. Guo, R. C. Qiu, and K. Currie, "Cognitive radio network as wireless sensor network (iii): Passive target intrusion detection and experimental demonstration," in *2012 IEEE Radar Conference*, May 2012, pp. 0293–0298.

[13] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, "Deep learning for rf device fingerprinting in cognitive communication networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 160–167, Feb 2018.

[14] C. M. Rondeau, J. Addison Betances, and M. A. Temple, "Securing zigbee commercial communications using constellation based distinct native attribute fingerprinting," *Security and Communication Networks*, vol. 2018, pp. 1–14, 07 2018.

[15] T. J. Bihl, K. W. Bauer, and M. A. Temple, "Feature selection for rf fingerprinting with multiple discriminant analysis and using zigbee device emissions," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1862–1874, Aug 2016.

[16] J. Lopez, N. C. Liefer, C. R. Busho, and M. A. Temple, "Enhancing critical infrastructure and key resources (cikr) level-0 physical process security using field device distinct native attribute features," *IEEE Transactions on Information Forensics and Security*, vol. PP, pp. 1–1, 12 2017.

[17] N. Tandiya, A. Jauhar, V. Marojevic, and J. H. Reed, "Deep predictive coding neural network for rf anomaly detection in wireless networks," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2018, pp. 1–6.

[18] Y. Sixing, L. Shufang, and Y. Jixin, "Temporal-spectral data mining in anomaly detection for spectrum monitoring," in *Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing*, ser. WiCOM'09. Piscataway, NJ, USA: IEEE Press, 2009, pp. 5347–5351. [Online]. Available: http://dl.acm.org/citation.cfm?id=1738467.1738767

[19] L. J. Wong, W. C. Headley, S. Andrews, R. M. Gerdes, and A. J. Michaels, "Clustering learned cnn features from raw i/q data for emitter identification," 10 2018, pp. 26–33.