Publications

4-8-2021

Zero-bias Deep Learning Enabled Quick and Reliable Abnormality Detection in IoT

Yongxin Liu
Embry-Riddle Aeronautical University

Jian Wang
Embry-Riddle Aeronautical University

Jianqiang Li
Shenzhen University

Shuteng Niu
Embry-Riddle Aeronautical University

houbing song
Embry-Riddle Aeronautical University, SONG4@erau.edu

Scholarly Commons Citation

Liu, Y., Wang, J., Li, J., Niu, S., & song, h. (2021). Zero-bias Deep Learning Enabled Quick and Reliable Abnormality Detection in IoT. *IEEE Internet of Things Journal, 11*(4). Retrieved from https://commons.erau.edu/publication/1772

Zero-bias Deep Learning Enabled Quick and Reliable Abnormality Detection in IoT

Yongxin Liu, Jian Wang, Jianqiang Li, Shuteng Niu, and Houbing Song, *Senior Member, IEEE*

***Abstract*—Abnormality detection is essential to the performance of safety-critical and latency-constrained systems. However, as systems are becoming increasingly complicated with a large quantity of heterogeneous data, conventional statistical change point detection methods are becoming less effective and efficient. Although Deep Learning (DL) and Deep Neural Networks (DNNs) are increasingly employed to handle heterogeneous data, they still lack theoretic assurable performance and explainability.**

This paper integrates zero-bias DNN and Quickest Event Detection algorithms to provide a holistic framework for quick and reliable detection of both abnormalities and time-dependent abnormal events in Internet of Things (IoT). We first use the zero-bias dense layer to increase the explainability of DNN. We provide a solution to convert zero-bias DNN classifiers into performance assured binary abnormality detectors. Using the converted abnormality detector, we then present a sequential quickest detection scheme which provides the theoretically assured lowest abnormal event detection delay under false alarm constraints. Finally, we demonstrate the effectiveness of the framework using both massive signal records from real-world aviation communication systems and simulated data. Code and data of our work is available at https://github.com/pcwhy/AbnormalityDetectionInZbDNN

***Index Terms*—Internet of Things, Big Data Analytics, Zero-bias Neural Network, Deep Learning, Abnormality Detection, Quickest Detection.**

I. Introduction

Deep Learning (DL) has reformed the ecosystem of the Internet of Things (IoT). On the one hand, they have been successfully applied in smart devices for accurate recognition of complicated inputs [1]–[3]. On the other hand, deep learning models do not require high-quality features and reduce the time-consuming feature engineering in conventional machine learning schemes [4], [5]. As a representative technology within the scope of DL, Deep Neural Network (DNN) classifiers aim to use hierarchically stacked convolution layers to extract latent features to make accurate decisions.

Although DL and DNNs are successful in general purpose applications, applying DNNs in safety-critical systems requiring assured performance is still controversial. Firstly, DNNs perform well on known subjects but cannot distinguish unseen abnormal data. Abnormal signals, such as cyberattacks, are required to identify in real-time with constrained false alarms [6]. Secondly, deep neural networks lack explainability, while applications in safety-critical systems require making accurate decisions with known and explainable behaviors. Thirdly, in safety-critical systems, classifiers are supposed to evolve efficiently within a manageable behavior. The three obstacles impede the deployment of DL and DNNs in IoT of safety-critical systems. Compared with DNNs, the nearest neighbor matching algorithms naturally overcome these obstacles and gain popularity in safety-critical systems.

To address the first challenge, existing works use deep Autoencoders or Generative Adversarial Networks (GANs) to capture the latent features of the domain-specific inputs by compressing and accurately reconstructing them. However, training deep autoencoders or GAN models is even more computationally expensive than training DNN classifiers on a specific domain. Moreover, autoencoders or GAN models do not guarantee to respond in time with constrained false alarms [7].

For the second problem, the eXplainable AI (XAI) has been proposed [8]. However, most of the related works treat DNN models as Black Boxes and focus on visualizing the importance of input features, i.e., whether a DNN model is picking the right features to make decisions and do not provide insights on models' performance boundaries. In safety-critical scenarios, decision boundaries or interfaces to diagnose the error risks are more important factors for assurability.

Finally, to support dynamic evolving DNN models, continual learning models such as Elastic Weight Consolidation (EWC [9]) and Knowledge Replay (KR [10]) are proposed. However, knowledge replay requires training old data generators, which is computationally expensive while EWC algorithms are efficient, but they are subject to numerical stability issues.

In this paper, we utilize an enhanced deep learning framework based on our previous work [11], the zero-bias dense layer enabled DNN, for quick and reliable detection of abnormalities with assured performance. We use zero-bias dense layers to facilitate DNNs with both non-impaired and explainable performance in distinguishing known or abnormal inputs and rapidly react to abnormalities with minimum latency and false alarm constraints. Furthermore, our solution efficiently derives abnormality detectors from existing DNN classifiers. The effectiveness of the proposed framework in handling massive signal recognition has been demonstrated. The contributions of this paper are as follows:

- We provide a novel method to use a zero-bias dense layer to visualize and analyze existing DNN models' decision boundaries. With this approach, we can diagnose the class boundaries of DNN models.

Yongxin Liu, Jian Wang, Shuteng Niu and Houbing Song are with the Department of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University, Daytona Beach, FL 32114 USA

Jianqiang Li is with the College of Computer Science and Software Engineering, Shenzhen University, China

Manuscript received March 19, 2021; revised XXX.

- We clarify the internal mechanism of abnormality detection in the zero-bias dense layer enabled DNN classifiers and provide a novel method to efficiently transfer existing DNN classifiers into DNN abnormality detectors with assured performance.
- We combine our zero-bias DNN model with the Quickest Change Detection theory, and our validation on massive real signal detection demonstrates the effectiveness of our integral solution.

Our research offers a solution to accurate identification of abnormalities with assured performance, thus useful in promoting trustworthy IoT and deepening the understanding of deep neural networks. Besides, the success of the zero-bias layer enables the move from IoT to real-time control.

The remainder of this paper is organized as follows: A literature review of related works is presented in Section II. We formulate our problem in Section III with the methodology presented in Section IV. Performance evaluation is presented in Section V with conclusions in Section VI.

II. Related works

Abnormality detection plays an increasingly important role in safety-critical and latency-constrained IoT, e.g., the aviation communication system in this research. Especially in the era of Big Data, multisource heterogeneous data are generated timely in huge volumes. Therefore, quick and reliable identification and detection of abnormal events and abnormalities are increasingly discussed. This section covers the state-of-art from three perspectives:

A. Abnormality detection in deep neural networks

A critical problem for learning based device identification is that classifiers only recognize pretrained data but can not deal with novel data presented during training. One intuitive alleviation is to remove the Softmax function. In [12], the authors first trained a CNN model with a Softmax output on known data. They then remove the Softmax function and turn the neural network into a nonlinear feature extractor. Finally, they use the DBSCAN algorithm to perform cluster analysis on the remapped features and show that the method has the potential of detecting a limited number of novel classes.

From the perspective of Artificial Intelligence, this issue is categorized as the Open Set Recognition [13], [14] problem. In [15], the authors use the Generative Adversarial Network (GAN) to generate highly realistic fake data. Then they exploit the discriminator network to distinguish whether an input is from an abnormal source. In [16], the authors provide two methods to deal with abnormalities: i) Reuse trained convolutional layers to transform inputs to feature vectors, and then use Mahalanobis distance to judge the outliers. ii) Reuse the pretrained convolutional layers to transform signals to feature vectors, and then perform k-means (k = 2) clustering to discover the groups of outliers.

B. Quickest event detection

Real-time event detection is a critical function in safety-critical IoT. From the perspective of input data, we may categorize them into single-shot and sequential detection paradigms. In single-shot detection [11], event detections are performed per observation, and the past data will not be retained for future use. In contrast, the sequential detection paradigm allows accumulating information from past observations [7].

From the perspective of the stochastic process, a Cyber-Physical System in different states can be described by distributions with measurable statistical properties [17]. Therefore, transitions within states cause the change of those properties. The quickest detection aims to detect the change as quickly as possible, subject to false alarm constraints [18]. The process is essentially an optimization problem. Considering whether prior observations are independent of an abnormal event's appearance, the optimization scheme can be defined in different forms as reviewed in [19].

We can also categorize the quickest event detection methods into two branches: a) detecting events with known postchange distributions. b) detecting events with unknown postchange distributions. Generally, detecting known events is faster with CUSUM algorithm can be applied directly [20]. A postchange distribution may not be known in some scenarios in advance, and nonparametric strategies have to be used and bring higher latency.

Quickest detection provides a performance-assured solution to detect change points (related to events) in sequential data. However, the selection of statistic metrics still depends on trial-and-error. We focus on real-time sequential detection of events, especially on integrating the quickest detection theory with deep learning to provide an automated and performance-assured solution to latency-constrained CPS.

III. Problem definition

The system model of our proposed framework is depicted in Figure 1. We aim to use deep learning models to process heterogeneous data from IoT and spot the abnormal data. We then use the quickest event detection algorithm to detect ongoing abnormal events with minimum latency.

In IoT systems, states are highly correlated with time-dependent events, e.g., abnormal events or normal operations. *We define that abnormalities are suspicious data caused by abnormal events*. Intuitively, abnormalities could trigger variation of specific indication metrics. Analyzing the drift or variations of these metrics, abnormal events can be detected sequentially. Therefore, we can convert the real-time abnormality detection problem into an online sequential event detection scheme, in which a surveillance oracle can sequentially collect its target system's state signals or heterogeneous data denoted as:

$$X = \{\boldsymbol{X_1}, \boldsymbol{X_2}, \dots \boldsymbol{X}_j \dots \boldsymbol{X}_{j+m} \cdots\} \tag{1}$$

where $\boldsymbol{X_j}$ denotes a state variable or record in vector form, an abnormal event appears at j and disappear at $j+m$. Real-time abnormal event detection requires triggering an alarm before $j+m$ with minimum assured latency.

Well-known methods are provided in the Quickest Change Detection (QCD) theory. For example, in the Cumulative Sum (CUSUM) Control Chart algorithm, a likelihood ratio test is

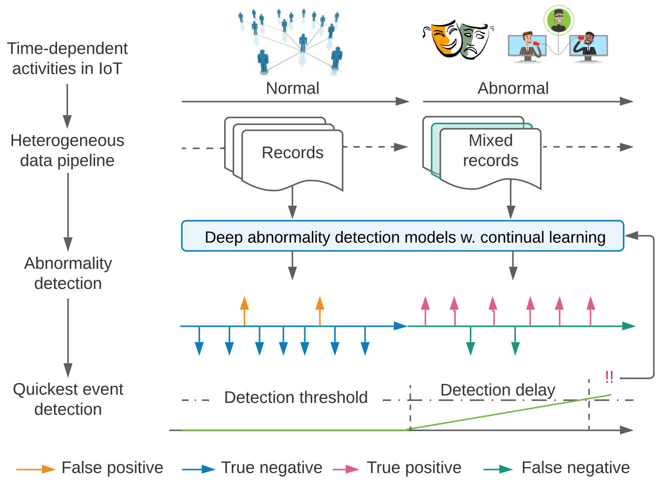


Fig. 1. System model of zero-bias deep learning enabled quick and reliable abnormality detection in IoT.

employed to sequentially process the observed data at each timestamp k, denoted as:

$$g(k) = ln(\frac{P_1(\boldsymbol{X}_k)}{P_0(\boldsymbol{X}_k)}) \tag{2}$$

Where $g(k)$ is a sufficiency metric, $P_0(\cdot)$, $P_1(\cdot)$ denotes the probabilistic density functions of abnormal and abnormal states, respectively. A constrained cumulative sum of sufficiency metrics is used as an indicator, denoted as:

$$S(k) = max(0, S(k-1) + g(k)) \tag{3}$$

An alarm will be sent once $S(k)$ is greater than a predefined threshold, h. The CUSUM algorithm has been proved to provide the lowest worst-case detection latency at specific false alarm intervals. However, CUSUM-style quickest detection algorithms can hardly handle high-dimension data, where $P_0(\cdot)$ and $P_1(\cdot)$ are difficult to obtain. Even though some works use DNNs to derive the sufficiency metric $g(k)$ from high dimension data, the DNNs' uncertain responses when encountering abnormalities make performance assurance a theoretic challenge. To enable deep learning for quick and reliable abnormality detection, the following efforts are needed:

- We need a DNN driven abnormality detection model to process complex data and provide theoretically assured performance. If possible, the deep abnormality detection model should be derived without a large overhead.
- We need to develop an efficient method to jointly apply performance-assured DNN and quickest event detection to provide theoretically guaranteed performance in detecting abnormal events.

IV. Proposed Framework

This section will first introduce the zero-bias DNN and its application in the explainability of DNN models. We then provide a method to convert zero-bias DNN into a performance assured abnormality detector efficiently. Finally, we provide our method to integrate zero-bias DNN with the quickest detection algorithms.

A. DNNs with zero-bias dense layers

This subsection provides an extended analysis of the zero-bias dense layer's characteristics, which serves theoretic backgrounds. Additionally, we show that the decision boundaries of DNNs with zero-bias dense layers can be visualized conveniently. Hereon, we will use the term DNNs with zero-bias dense and zero-bias DNN alternatively.

We have discovered that the last dense layers of a DNN classifier perform the nearest neighbor matching with biases and preferabilities using cosine similarity in [11]. We then show that DNN classifiers' accuracy will not be impaired if we replace their last dense layers with our zero-bias dense layers, in which biases and preferabilities are eliminated. We can denote the mechanism of the zero-bias dense layer as:

$$\begin{aligned} \boldsymbol{Y}_0(\boldsymbol{X}) &= \boldsymbol{W}_0\boldsymbol{X} + \boldsymbol{b} \\ L(\boldsymbol{X}) &= cos(\boldsymbol{Y}_0, \boldsymbol{W}_1) \end{aligned} \tag{4}$$

Where $\boldsymbol{X}$ is the output of the prior layer, a.k.a., feature vectors. $\boldsymbol{W}_1$ is a matrix to store fingerprints of different classes. $\boldsymbol{X}$ is an N_0 by q matrix, where N_0 denotes the number of features while q denotes the batch size. $\boldsymbol{W}_0$ is an N_1 by N_0 matrix where N_1 denotes the number of new feature dimensions. $\boldsymbol{W}_0\boldsymbol{X}+\boldsymbol{b}$ performs linear dimension reduction as long as $N_1 < N_0$. Finally, W_1 is a C by N_1 matrix in which C denotes the number of classes, Please be noted that in W_1, each row represents a fingerprint of corresponding class whilst in $\boldsymbol{Y}_0$ each column represents a feature vector within a batch. Therefore, the cosine similarity can be implemented by:

$$cos(\boldsymbol{Y}_0, \boldsymbol{W}_1) = \boldsymbol{RU}(\mathbf{W_1}) \times \boldsymbol{CU}(\mathbf{Y_0}) \tag{5}$$

Where $\boldsymbol{RU}(\cdot)$ and $\boldsymbol{CU}(\cdot)$ denote deriving column-wise and row-wise unified (vectors' magnitudes normalized to one) vectors of the input matrix, respectively. Our prior results [11], [21] also prove that zero-bias DNN can be trained using common loss functions (e.g., binary crossentropy, MSE, and etc.) and back-propagation mechanisms.

The cosine similarity in Equation 5 represents the similarity matching of fingerprints and feature vectors on an N_1-D unit hyperspherical surface. A 3-D example is depicted in Figure 2. Fingerprints divide the unit hyperspherical surface into several subregions, and we can reduce the dimension of fingerprints and use Voronoi Diagram [22] to visualize their decision boundaries as in Figure 3. The decision boundaries of a specific fingerprint denote the boundaries of a class. Hereon, we will use the terms class boundaries and fingerprint's boundaries alternatively.

Please be noted that, even if we eliminate the magnitude and bias constant for each fingerprint, we do not need to worry about the capacity of zero-bias DNN models in distinguishing different classes. A numerical example for quantifying the maximum theoretic number of classes that a zero-bias DNN will reliably learn is given in Figure 6b. .

For example, in the DNN enabled MNIST handwritten digit recognition [23], the network's last dense layer is replaced by a zero-bias dense layer with $N_1 = 10$. The Voronoi diagrams at two stages (85% and 97% accuracies) using fingerprints in the zero-bias dense layer and feature vectors from the

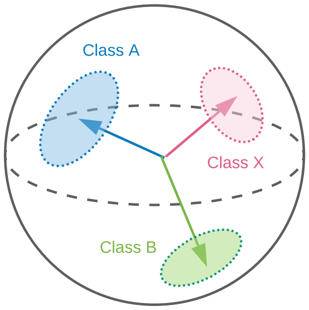
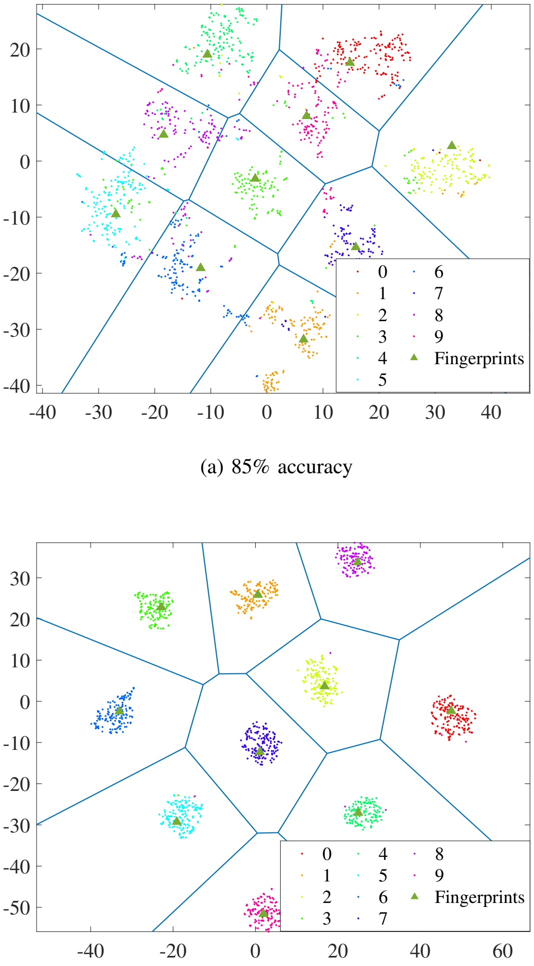


Fig. 2. 3D unit hyperspherical surface in zero-bias DNNs.

validation set are depicted in Figure 3 with solid blue lines representing the decision boundaries of topologically adjacent classes. Please be noted that the Voronoi diagram can not be applied directly to DNN models without adapting zero-bias dense layers.



(a) 85% accuracy

(b) 97% accuracy

Fig. 3. The Voronoi diagrams of dimension-reduced fingerprints and validation set at different training stages. Fingerprints and feature vectors are projected to a 2D space using *t-SNE* algorithm [24].

From the observation, we conclude that during training, a DNN with a zero-bias dense layer learns to project input data from identical classes closer to the corresponding fingerprints and separate data from different classes far away. The feature extractors in prior layers and fingerprints in the zero-bias dense layer are optimized simultaneously. In DNNs with zero-bias dense layer, classification errors result from two perspectives:

- If fingerprints are not distantly separated, data from the corresponding classes are highly possible to get confused. This fact is verified in our previous work in [11].
- The prior layers are poorly trained and the feature vectors are sparsely projected as depicted in Figure 3a.

Please be noted that zero-bias dense layer can be easily adapted to existing DNN models via transfer learning.

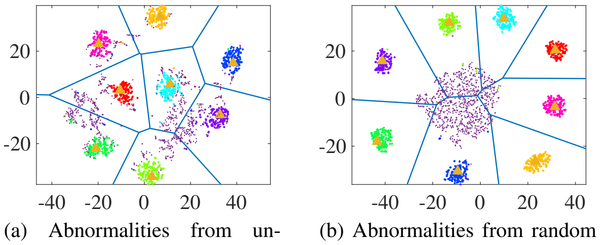
B. Abnormality detection in DNN with zero-bias dense layer

The effectiveness of zero-bias DNN for nonsequential abnormality detection has been demonstrated in our prior results [11], [21], briefly, it is significant better than regular DNN and comparable to one-class SVM [25]. In this section, we deepen our previous research and present a solution to convert zero-bias DNN models into abnormality detectors with predictable and assurable performance.

1) Deriving abnormality detector from existing DNN classifiers: In Figure 3b, feature vectors from known classes are closely projected to the vicinity of the corresponding fingerprints. As a result of cosine similarity matching, we come to our first remark:

Remark 1. *Abnormal data from an unknown novel class are less likely to be projected into any existing classes' close vicinity as there is no specific fingerprint for these data.*

We use the MNIST example to demonstrate Remark 1 with the results in Figure 4. We train the zero-bias DNN to recognize handwritten digits from 1 to 8 and use digits 9 and 0 as abnormal data. The projection feature vectors of known and abnormal data and fingerprints are depicted in Figure 4a. We then replace the abnormal data with pure Gaussian random noise ($N(0, 2)$) and repeat the experiment. Results are depicted in Figure 4b.



(a) Abnormalities from unknown classes

(b) Abnormalities from random noise $\sim N(0, 2)$

Fig. 4. Voronoi diagrams of dimension-reduced fingerprints, validation set and abnormal data. Data are projected to a 2D space using *t-SNE* algorithm [24].

It can be noticed that abnormalities from an unknown class of the same domain could be even more difficult to detect than pure random noise. Although Figure 4a has shown that abnormalities from unknown classes are more sparsely distributed in the unit hyperspherical surface, Remark 1 still holds. Therefore, we can derive a basic principle (depicted in Figure 5.) to convert a zero-bias dense layer enabled DNN classifier into an abnormality detector:

Remark 2. *We can model the spatial distribution and boundaries of normal data in the hyperspherical surface. Then the incoming feature vectors that are out of normal data boundaries are regarded as abnormalities.*

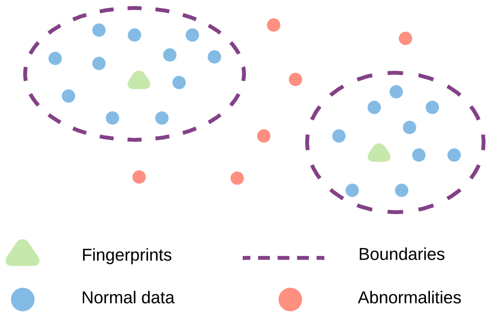


Fig. 5. Relation of normal and abnormal data.

For a given DNN model with zero-bias dense layer, we model the boundaries of different classes as follows:

Step 1: The training set is utilized to learn the boundaries of known classes while the validation set will be mixed with abnormal data ($\boldsymbol{A_0}$) to measure the performance of converted abnormality detector.

Step 2: We pass accurately classified data of each known class in $\boldsymbol{C_1}$, denoted as $\boldsymbol{KX}_i$, through the DNN model and obtain the compressed feature vectors before fingerprint matching, denoted as:

$$\boldsymbol{Y}_0[F_{n-1}(\boldsymbol{KX}_i)] = \boldsymbol{W}_0 F_{n-1}(\boldsymbol{KX}_i) + \boldsymbol{b} \quad (6)$$

Where $\boldsymbol{W}_0$ and $\boldsymbol{b}$ are defined in Equation 4, $F(\cdot)_{n-1}$ denotes all network layers before the fingerprint matching. $\boldsymbol{Y}_0[F_{n-1}(\boldsymbol{KX}_i)]$ denotes feature vectors of accurately classified data in $\boldsymbol{KX}_i$.

Step 3: Calculate the centroid $\boldsymbol{c}_0^i$ and covariance matrix ($\boldsymbol{P_i}$) of $\boldsymbol{KX}_i$ as:

$$\begin{aligned} \boldsymbol{c}_0^i &= mean(\boldsymbol{Y}_0[F_{n-1}(\boldsymbol{KX}_i)]) \quad (7) \\ \boldsymbol{P_i} &= cov(\boldsymbol{Y}_0[F_{n-1}(\boldsymbol{KX}_i)], \boldsymbol{Y}_0[F_{n-1}(\boldsymbol{KX}_i)]) \end{aligned}$$

Step 4: Calculate the Mahalanobis distances [26] from the class centroid $\boldsymbol{c}_0^i$ to all accurately classified feature vectors. Then we use the maximum value as a cut-off distance CO_i of class $\boldsymbol{KX}_i$:

$$CO_i = max\ \boldsymbol{D_m}[\boldsymbol{Y}_0[F_{n-1}(\boldsymbol{KX}_i)], \boldsymbol{c}_0^i] \quad (8)$$

Where $\boldsymbol{D_m}(\cdot, \boldsymbol{c}_0^i)$ denotes the feature vectors' Mahalanobis distances to $\boldsymbol{c}_0^i$.

Step 5: Abnormality detection using cut-off boundaries on input data $\boldsymbol{X}$) is formally defined as:

$$D(\boldsymbol{X}) = \begin{cases} 1 & \exists\ i,\ \boldsymbol{D_m}[\boldsymbol{Y}_0[F_{n-1}(\boldsymbol{X})], \boldsymbol{c}_0^i] \leq CO_i \\ 0 & \text{Otherwise} \end{cases} \quad (9)$$

These steps convert zero-bias DNNs into abnormality detectors with binary outputs. Herein, we will use the term zero-bias abnormality detector alternatively. In essence, we construct statistical models for each class to describe the distribution of corresponding normal data and a hard cut-off distance to form its boundary (denoted as dashed purple lines in Figure 5). Please be noted that other distance functions or modeling methods such as the Local Outlier Factor [27] can also be applied.

Suppose that each fingerprint governs a non-overlapped subregion with a maximum acceptable deviation angle, σ, for normal data. This subregion is named σ-cap, we can analytically evaluate the area of each σ-cap, and its occupied area ratio, $r_0(m)$, as:

$$\begin{aligned} A_c(m) &= \frac{1}{2} A_u(m) r^{n-1} I_{(2rh-h^2)/r^2}\left(\frac{m-1}{2}, \frac{1}{2}\right) \\ A_u(m) &= \frac{2\pi^{n/2}}{\Gamma(n/2)} \\ r_0(m) &= \frac{A_c(m)}{A_u(m)} = \frac{1}{2} I_{(2h-h^2)}\left(\frac{m-1}{2}, \frac{1}{2}\right) \quad (10) \end{aligned}$$

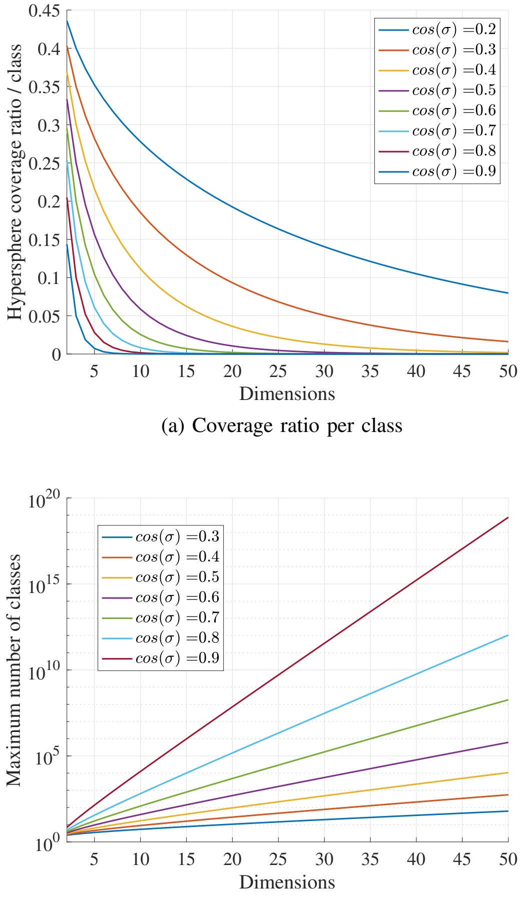
Where $A_c(m)$ is the area of a m-D σ-cap. $A_u(m)$ is the surface area of the m-D unit hypersphere. Additionally, we have $r = 1$ and $h = r - rcos(\sigma)$. I and Γ are the regularized incomplete beta function and the gamma function, respectively. A numerical result is given in Figure 6. As depicted, both a smaller σ and larger number of feature dimensions (N_1) increase the capacity and interclass distinguishability of the zero-bias DNN. Moreover, even if we eliminate some information of feature vectors in zero-bias DNNs, we do not have to worry much about their learning capacity and remaining space for abnormalities, as long as feature dimension N_1 is large.

2) *Theoretic performance Analysis:* We introduce the hard cut-off distances of fingerprints. Therefore, a binary abnormality detector converted from zero-bias DNN becomes a binary classifier. We derive two important properties of this type of zero-bias abnormality detector regarding false positive and false negative rates.

The accuracy of zero-bias DNN models on known classes can be obtained after training. As discussed earlier in Section IV-A, the classification errors are caused by inaccurate projections. From the perspective of decision boundary and class boundary, the scenarios that lead to classification error are depicted in Figure 7. As depicted, the feature vectors C and D are projected into the wrong class boundaries but out of the boundaries of normal data. Meanwhile, E and F are projected into the normal data boundaries of wrong fingerprints.

Suppose that E and F in Figure 7 are moved out of the normal data boundaries. The false-positive rate of abnormality detection reaches its upper bound and equals the classification error α. Furthermore, if C and D are moved into normal data boundaries, the false positive rate equals zero. Therefore, the range of false-positive rate of zero-bias abnormality detector is actually determined:

Remark 3 (Range of the false positive rate)**.** *Suppose that the classification error of the zero-bias DNN is α, as long as our*



(a) Coverage ratio per class

(b) Maximum of distinguishable classes

Fig. 6. The coverage ration per class and maximum number of distinguishable class in zero-bias DNN.

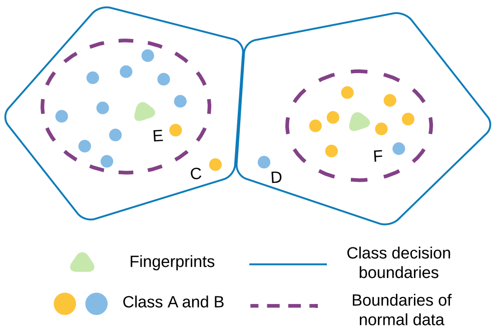


Fig. 7. Classification errors in zero-bias DNN, feature vector C, D, E and F are erroneously projected into governing regions of wrong fingerprints.

statistical model can closely follow the boundary of normal data, the false positive rate of converted abnormality detector is less than or equals to α. Denoted as:

$$FPR \le \alpha \tag{11}$$

Suppose that in a regular case, the feature vectors of abnormalities are mixed with normal data and uniformly distributed on the surface of the unit hypersphere, in this case, the maximum false negative rate is reached.

Remark 4 (Range of false negative (true positive) rates)**.** *The upper bound of the false negative rate under uniformly distributed abnormalities, equals to ratio of the occupied regions' area of normal data divided by the total surface area of the unit hypersphere, denoted as:*

$$RU_{FNR} = \frac{\sum_{i=1}^{N_c} S^i_{hsp}(N_1)}{A_{hsp}(N_1)}$$

$$With\ FNR \le RU_{FNR},\ TPR \ge 1 - RU_{FNR} \tag{12}$$

Where N_c is the number of known classes, N_1 and $A_{hsp}(N_1)$ are the dimension and surface area of the unit hypersphere, respectively. $S^i_{hsp}(N_1)$ is the surface area of normal data of the ith class.

Analytically calculating $S^i_{hsp}(N_1)$ is difficult since the shapes of these occupied subregions are unknown. Therefore, we use Monte Carlo method to estimate RU_{FNR} directly. Corresponding pseudo code is presented in Algorithm 1, specifically, we generate M random points uniformly distributed on the surface of the unit hypersphere and count the ratio of points that are captured by the normal data boundaries of fingerprints. The captured rate directly indicates the value of RU_{FNR}. Empirically, we set $M = 20,000$.

Algorithm 1 Estimating RU_{FNR}

```
function $RU_{FNR}(N_1, N_c, M, List[\boldsymbol{CO}], List[\boldsymbol{c}_0^i])$
    $HX \leftarrow UniformHypersphereRand(N_1, M)$    ▷ Please refer to [28]
    $chx \leftarrow 0$
    for $k \leftarrow 1 \ldots M$ do
        for $i \leftarrow 1 \ldots N_c$ do
            if $\boldsymbol{D_m}[HX_k, \boldsymbol{c}_0^i] \le \boldsymbol{CO}_i$ then
                $chx \leftarrow chx + 1$
            end if
        end for
    end for
    return $\frac{chx}{M}$
end function
```

C. Zero-bias DNN for quickest abnormal event detection

1) Sequential formalization and detectability: Given the theoretic analysis of zero-bias abnormality detector in section IV-B2, we can model the response of zero-bias DNNs as switching between two probability distributions before and after the appearance of an abnormal event, namely P_0 and P_1, respectively. Since we have converted the zero-bias DNN into a binary abnormality detector, we can formulate P_0 and P_1 into two Bernoulli Distributions [29]:

$$\begin{aligned} P_0(I_k) &= FPR_k^I(1 - FPR)^{1-I_k} \\ P_1(I_k) &= (1 - FNR)_k^I FNR^{1-I_k} \\ &= (TPR)_k^I(1 - TPR)^{1-I_k} \end{aligned} \tag{13}$$

Where $I \in \{0, 1\}$ is the binary output of the abnormality detector with $I_k = D(\boldsymbol{X_k})$. FPR can be deried on existing data, and the range of FNR and TPR from section IV-B2.

As long as the P_0 and P_1 are different, the abnormal event causing drifts from P_0 to P_1 can be sequentially detected. We have the following determinant under regular scenarios:

Remark 5 (Sequential detectability)**.** *Abnormal events are assured to be sequentially detectable if the binary zero-bias detector's true-positive rate (TPR) lower bound ($1-RU_{FNR}$) are greater than the false-positive rate (FPR) upper bound (α).*

Remark 4 shows that the true positive and false negative rates are within different ranges, if $1 - RU_{FNR} \leq \alpha$, the two variables' spanning ranges are partially overlapped (depicted in Figure 8) and we may encounter an extreme case: $TPR = FPR$. Therefore, the abnormal event is only conditionally detectable.

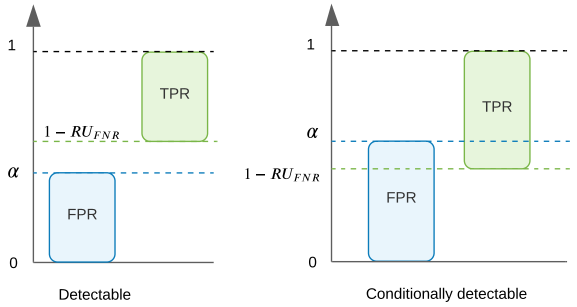


Fig. 8. Range of true-positive and false-positive rates.

2) Quickest detection algorithm: With Remark 5, we can use Quickest Change Detection algorithm to detect the appearance of an abnormal event with the lowest latency at a given false alarm run length. We will present both the Bernoulli Generalized Likelihood Ratio Chart and its approximation, the multiple Bernoulli CUSUM Chart, respectively. Compared with the existing nonparametric solutions, we discretize the continuous probabilistic function space and transform the problem into a parametric sequential hypothesis testing problem.

Using Bernoulli Generalized Likelihood Ratio (GLR) Chart [30] to sequentially detect abnormal events. We have:

$$\begin{aligned} R_k &= \max_{0\leq\tau\leq k-1, \beta\leq TPR\leq 1} \ln \frac{\prod_{i=\tau+1}^{k} TPR^{I_k}(1-TPR)^{1-I_k}}{\prod_{i=\tau+1}^{k} FPR^{I_k}(1-FPR)^{1-I_k}} \\ &= \max_{0\leq\tau\leq k-1} (k-\tau)\ln\left[\widehat{TPR}\cdot\frac{\widehat{TPR}(1-FPR)}{FPR(1-\widehat{TPR})}\right. \\ &\quad \left. + \ln\frac{1-\widehat{TPR}}{1-FPR}\right] \end{aligned} \qquad (14)$$

Where $\widehat{TPR} \approx TPR \in [1 - RU_{FNR}, 1)$ is the estimated true positive rate of zero-bias abnormality detector and τ is the estimated time when an abnormal event happens. $\widehat{TPR}$ is dynamicaly estimated as follows:

$$\widehat{TPR} = min\left\{B_1, max\left[1 - RU_{FNR}, \frac{\sum_{i=\tau+1}^{k}}{k-\tau} I_k\right]\right\} \qquad (15)$$

Where $B_1 = 1-\varepsilon$ is the maximum possible value of TPR and ε is a tiny positive number to assure $\widehat{TPR} < 1$. An alarm is triggered if $R_k > h_{GLR}$ and h_{GLR} is a pre-defined threshold. h_{GLR} can be chosen as suggested in: [30]:

$$h_{GLR} = log_{10}(ARL \cdot FPR) \qquad (16)$$

Where ARL is the average run length between false alarms.

Theoretically, we have to store a long sequence ($0 \leq \tau \leq k-1$) of previous abnormality detection results to detect an abnormal event. Fortunately, we can use a sliding window to store relevant data and reduce the computational complexity. In [31] and [30], it is shown that a GLR chart with a window is asymptotically optimal if the window size m is sufficiently large.

It is also numerically verifiable that the detection latency of Bernoulli GLR charts can be closely approximated with a countable set of Bernoulli CUSUM Charts, where the identical detection threshold h_{CUSUM} is shared among them and $h_{CUSUM} = h_{GLR}$ [30], [32]. The approximated range of TPR is covered by each CUSUM chart is:

$$\widehat{TPR}_i = 1 - RU_{FNR} + \frac{TPR_{max}\cdot i^2}{U^2} \qquad (17)$$

Where U is the total number of CUSUM charts, in which greater than 100 is recommended, i denotes the index of each chart. TPR_{max} is the max possible value of the true positive rate that is less than 1. $1-RU_{FNR}$ denotes the lower bound of the true positive rate. Therefore, given an average run length between false alarms, ARL, we have the worst case average detection delay as:

$$\bar{T}_{GLR} = \bar{\boldsymbol{T}}_{CUSUM} \sim \frac{h_{CUSUM}}{I(P_1, P_0)} \qquad (18)$$

Please be noted that we use the characteristic of multiple Bernoulli CUSUM charts to demonstrate the properties of detection delay.

V. Performance Evaluation

In this section, we evaluate the performance of the proposed framework in two folds, we first use a massive real-world signal dataset to test the proposed method for visualizing the class decision boundaries and feature vectors of a deep signal identification network [33]. Then we use the proposed method to convert the identity recognition DNN into an abnormality detection model and evaluate its performance on sequential abnormal event detection.

A. Dataset and application scheme

Our dataset is available in [34], we use the wide-spreading signals from Automatic Dependent Surveillance-Broadcast (ADS-B) system [35], which provides a great variety of signals from commercial aircraft's signal transponders with labels. Specifically, each licensed aircraft use 1090MHz transponders to broadcast their geo-coordinates, velocity, altitude, heading, as well as its unique identifier to the Air Traffic Control (ATC) center. The integrity and trustworthiness of ADS-B signals are critical to aviation safety. However, the ADS-B system does not contain cryptographical identity verification mechanisms and thus is vulnerable to identity spoofing attacks (depicted in Figure 9). Our previous work shows that the responses of the zero-bias DNN on known (learned) and unknown transponders' signals are different. Therefore, we can use the methodology provided in this paper to design a performance-assured quick abnormality detector to detect signals from the malicious masquerading legitimate aircraft.

From the perspective of Deep Learning, the input is the raw signal from a Software Defined Radio Receiver (USRP B210) and the label is the identify of the signal source (aircraft). As in our prior work [11], [21], we take the first 1024 samples from the signal of each intercepted message. And convert the 1024 samples into a 32 by 32 by 3 tensor, which incorporate pseudo noise, magnitude-frequency domain, and phase-frequency domain information, respectively.

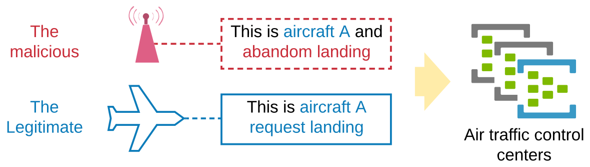

The malicious
This is aircraft A and abandon landing
The Legitimate
This is aircraft A request landing
Air traffic control centers

Fig. 9. Identity spoofing in aviation communication systems.

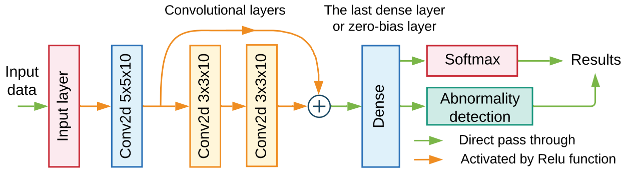


Fig. 10. Deep neural network architecture.

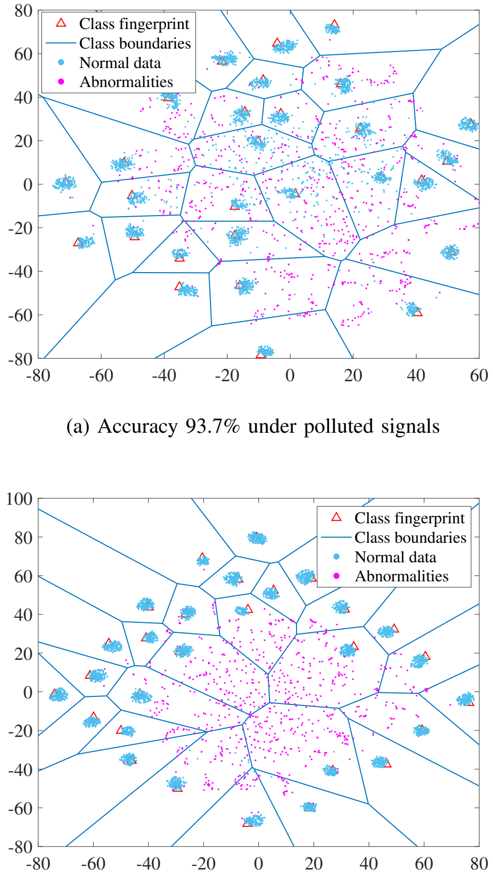
B. Decision boundaries and feature vectors in real-world zero-bias DNN

The architecture of our DNN model is depicted in Figure 10 with a description of the dataset in Table I. In Figure 11 we use two Voronoi diagrams to depict the relation of fingerprints, class boundaries, normal and abnormal data, with the DNN model trained under two scenarios: a) Input signals are polluted by abrupt spike noise due to the signal interference. b) Input signal without abrupt spikes (removed by a Gaussian filter).

As in Figure 11a and 11b, normal data are closely distributed within their fingerprints while abnormalities are sparsely distributed over the feature space. It is interesting to find that if the DNN model is with high accuracy, the abnormalities are less likely to appear in normal data clusters. The DNN signal identifier is with high accuracy within the two scenarios.

TABLE I
DESCRIPTION OF DATASET

Usage	Description
Training	60% of signals, including 28 aircraft with more than 500 randomly selected raw records for each.
Validation	40% of signals, including 28 aircraft with more than 500 randomly selected raw records for each.
Normal data	Validation data that's not been used to train the network.
Abnormal data	Signals including 236 aircraft with less than 200 raw signal records during the data collection period.



(a) Accuracy 93.7% under polluted signals

(b) Accuracy 99.9% under filtered signals

Fig. 11. Voronoi diagram of dimension-reduced fingerprints and validation set two different scenarios. Fingerprints and feature vectors are projected to a 2D space using *t-SNE* algorithm [24].

According to Remark 3 and 4, the abnormality detector's performance is predictable. In reality, the zero-bias abnormality detector trained on noisy data has a true positive and a true negative rate of 91% and 92%, respectively, which is closely matched with our prediction. However, the zero-bias abnormality detector trained on the filtered data has a true positive and a true negative rate of 99% and 91%. The true negative rate is smaller than the expected value due to the model entering the early stage of overfitting. At this stage, the training set's feature vectors can no longer provide sufficient information on the distribution of normal data. Therefore, the estimation of normal data will be misled.

For alleviation, we can set a threshold value of accuracy during training. We derive the cut-off distances, centroids, and covariance matrices at this point. By setting a triggering value of 96% for the validation accuracy on the filtered data, we get a true-positive rate and a false-positive rate of 98% and 95%, respectively. The relation between the performance of the converted abnormality detector and the zero-bias DNN model's accuracy before conversion is given in Figure 12. As predicted, when the accuracy of zero-bias DNN gets higher, the normal data occupies a smaller amount of area on the unit hypersphere surface, and thus produce higher True Positive rates. Meanwhile, lower False Positive rates are achieved when the zero-bias DNN has higher classification accuracy before conversion as predicted.

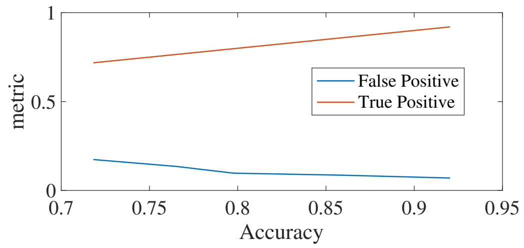
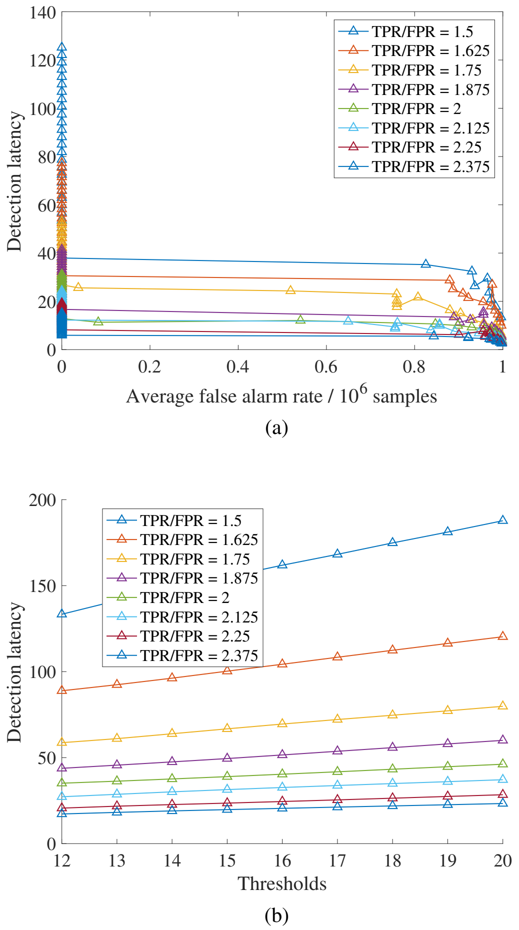


Fig. 12. Performance of the converted abnormality detector.



(a)

(b)

Fig. 13. Abnormal event detection latencies.

C. Quickest abnormal event detection with zero-bias DNNs

Our model can detect abnormalities (the appearance of an unknown aircraft's signal) with almost neglectable latency (less than ten samples on average using GLR chart) as a result of both high true-positive and true-negative rates. To further evaluate our proposed method, we can use numerical simulation results to demonstrate the performance of zero-bias DNN, since its response characteristics prior and after abnormal events are modeled as two Bernoulli distributions in Section IV-C1. We experiment with a collection of possible values of h_{GLR}, FPR, and TPR that a zero-bias abnormality detector can encounter. In which $TPR \in [0.6, 0.99]$, $FPR \in [0, 0.4]$ and $h_{GLR} \in [2, 20]$

The relationship between abnormal event detection latency and false alarm rate is depicted in Figure 13a. We discover a nice cut-off property, in which the average false alarm rate becomes zero as we select a proper detection threshold h_{GLR} or h_{CUSUM}. After the threshold is properly set. Once the detection threshold is greater than a certain value, 12 in our experiment, the detection delay grows linearly as depicted in Figure 13b. A further analysis of the distribution of detection delay with threshold $h_{GLR} \in [12, 20]$ is presented in Figure 14, in general, as TPR/FPR gets larger, average detection latency decreases with less sensitive to h_{GLR}.

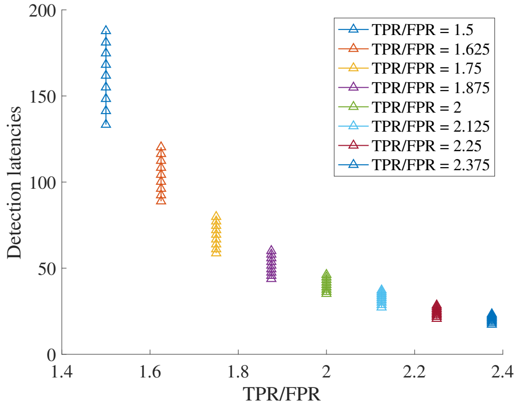


Fig. 14. Distribution of abnormal event detection latencies.

VI. Conclusion

In this paper, we significantly extend the analysis of our previously proposed zero-bias DNN and combine it with the Quickest Event Detection algorithms to detect abnormalities and time-dependent abnormal events in IoT with the lowest assured latency. We first analyze the zero-bias dense layer and provide to use Voronoi diagram to increase the explainability of DNN models. We then provide a solution to convert zero-bias DNN classifiers, which are easier to obtain, into performance assured binary abnormality detectors with assured performance boundaries. Using the converted abnormality detectors, we model their behaviors using Bernoulli distribution, which perfectly adapts to the Generalized Likelihood Ratio based Quickest Detection scheme. In this Quickest Detection scheme, the theoretically assured lowest abnormal event detection delay is provided with predictable false alarms. Finally, we demonstrate the framework's effectiveness using both massive signal records from real-world aviation communication systems and simulated data.

In the future, we will investigate the possibility of using similar methods to visualize conventional deep neural networks' decision boundaries. We only use the Voronoi diagram in the 2D plane in this research, and better data dimension reduction methods and visualization methods specifically focus on the hyperspherical plane would be proposed.

Acknowledgment

This research was partially supported by the National Science Foundation under Grant No. 1956193.

References

[1] C. Xu, B. Chen, Y. Liu, F. He, and H. Song, "Rf fingerprint measurement for detecting multiple amateur drones based on stft and feature reduction," in *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*. IEEE, 2020, pp. 4G1–1.

[2] Y. Jiang, Y. Liu, D. Liu, and H. Song, "Applying machine learning to aviation big data for flight delay prediction," in *2020 IEEE DASC/PiCom/CBDCom/CyberSciTech*. IEEE, 2020, pp. 665–672.

[3] L. Wang, X. Yue, H. Wang, K. Ling, Y. Liu, J. Wang, J. Hong, W. Pen, and H. Song, "Dynamic inversion of inland aquaculture water quality based on uavs-wsn spectral analysis," *Remote Sensing*, vol. 12, no. 3, p. 402, 2020.

[4] S. Peng, H. Jiang, H. Wang, H. Alwageed, Y. Zhou, M. M. Sebdani, and Y.-D. Yao, "Modulation classification based on signal constellation diagrams and deep learning," *IEEE transactions on neural networks and learning systems*, vol. 30, no. 3, pp. 718–727, 2018.

[5] Z. Gao, X. Wang, Y. Yang, C. Mu, Q. Cai, W. Dang, and S. Zuo, "Eeg-based spatio–temporal convolutional neural network for driver fatigue evaluation," *IEEE transactions on neural networks and learning systems*, vol. 30, no. 9, pp. 2755–2763, 2019.

[6] Y. Jiang, M. Wang, X. Jiao, H. Song, H. Kong, R. Wang, Y. Liu, J. Wang, and J. Sun, "Uncertainty theory based reliability-centric cyber-physical system design," in *2019 International Conference on Internet of Things (iThings) and IEEE GreenCom/CPSCom/SmartData*. IEEE, 2019, pp. 208–215.

[7] P. Perera and V. M. Patel, "Efficient and low latency detection of intruders in mobile active authentication," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1392–1405, 2017.

[8] A. Das and P. Rad, "Opportunities and challenges in explainable artificial intelligence (xai): A survey," *arXiv preprint arXiv:2006.11371*, 2020.

[9] J. Kirkpatrick, R. Pascanu, N. Rabinowitz, J. Veness, G. Desjardins, A. A. Rusu, K. Milan, J. Quan, T. Ramalho, A. Grabska-Barwinska *et al.*, "Overcoming catastrophic forgetting in neural networks," *Proceedings of the national academy of sciences*, vol. 114, no. 13, pp. 3521–3526, 2017.

[10] D. Rolnick, A. Ahuja, J. Schwarz, T. Lillicrap, and G. Wayne, "Experience replay for continual learning," in *Advances in Neural Information Processing Systems*, 2019, pp. 350–360.

[11] Y. Liu, J. Wang, J. Li, H. Song, T. Yang, S. Niu, and Z. Ming, "Zero-bias deep learning for accurate identification of internet of things (iot) devices," *IEEE Internet of Things Journal*, 2020.

[12] 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," in *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*. IEEE, 2018, pp. 26–33.

[13] W. J. Scheirer, A. de Rezende Rocha, A. Sapkota, and T. E. Boult, "Toward open set recognition," *IEEE transactions on pattern analysis and machine intelligence*, vol. 35, no. 7, pp. 1757–1772, 2012.

[14] A. Bendale and T. E. Boult, "Towards open set deep networks," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 1563–1572.

[15] D. Roy, T. Mukherjee, M. Chatterjee, E. Blasch, and E. Pasiliao, "Rfal: Adversarial learning for rf transmitter identification and classification," *IEEE Transactions on Cognitive Communications and Networking*, 2019.

[16] Y. Shi, K. Davaslioglu, Y. E. Sagduyu, W. C. Headley, M. Fowler, and G. Green, "Deep learning for rf signal classification in unknown and dynamic spectrum environments," in *2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. IEEE, 2019, pp. 1–10.

[17] L. Lai, Y. Fan, and H. V. Poor, "Quickest detection in cognitive radio: A sequential change detection framework," in *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*. IEEE, 2008, pp. 1–5.

[18] H. V. Poor and O. Hadjiliadis, *Quickest detection*. Cambridge University Press, 2008.

[19] P. Johnson, J. Moriarty, and G. Peskir, "Detecting changes in real-time data: a user's guide to optimal detection," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 375, no. 2100, p. 20160298, 2017.

[20] M. Basseville, I. V. Nikiforov *et al.*, *Detection of abrupt changes: theory and application*. prentice Hall Englewood Cliffs, 1993, vol. 104.

[21] Y. Liu, J. Wang, S. Niu, and H. Song, "Deep learning enabled reliable identity verification and spoofing detection," in *International Conference on Wireless Algorithms, Systems, and Applications*. Springer, 2020, pp. 333–345.

[22] M. Erwig, "The graph voronoi diagram with applications," *Networks: An International Journal*, vol. 36, no. 3, pp. 156–163, 2000.

[23] MathWorks, "Create simple deep learning network for classification," https://www.mathworks.com/help/deeplearning/ug/create-simple-deep-learning-network-for-classification.html, May 2018.

[24] L. v. d. Maaten and G. Hinton, "Visualizing data using t-sne," *Journal of machine learning research*, vol. 9, no. Nov, pp. 2579–2605, 2008.

[25] Y.-S. Choi, "Least squares one-class support vector machine," *Pattern Recognition Letters*, vol. 30, no. 13, pp. 1236–1240, 2009.

[26] R. De Maesschalck, D. Jouan-Rimbaud, and D. L. Massart, "The mahalanobis distance," *Chemometrics and intelligent laboratory systems*, vol. 50, no. 1, pp. 1–18, 2000.

[27] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "Lof: identifying density-based local outliers," in *Proceedings of the 2000 ACM SIGMOD international conference on Management of data*, 2000, pp. 93–104.

[28] G. Dorini, "n-dimensional hypersphere in parametric coordinates. MATLAB Central File Exchange. Retrieved November 25, 2020." https://www.mathworks.com/matlabcentral/fileexchange/5397-hypersphere.

[29] E. W. Weisstein, "Bernoulli distribution," *https://mathworld. wolfram. com/*, 2002.

[30] W. Huang, S. Wang, and M. R. Reynolds Jr, "A generalized likelihood ratio chart for monitoring bernoulli processes," *Quality and Reliability Engineering International*, vol. 29, no. 5, pp. 665–679, 2013.

[31] T. L. Lai, "Information bounds and quick detection of parameter changes in stochastic systems," *IEEE Transactions on Information Theory*, vol. 44, no. 7, pp. 2917–2929, 1998.

[32] W. Huang, M. R. Reynolds Jr, and S. Wang, "A binomial glr control chart for monitoring a proportion," *Journal of Quality Technology*, vol. 44, no. 3, pp. 192–208, 2012.

[33] L. Yongxin, "Adabelief-matlab (github)," Nov. 2020. [Online]. Available: https://doi.org/10.5281/zenodo.4248678

[34] Y. Liu, J. Wang, H. Song, S. Niu, and Y. Thomas, "A 24-hour signal recording dataset with labels for cybersecurity and IoT," 2020. [Online]. Available: http://dx.doi.org/10.21227/gt9v-kz32

[35] J. Sun, "An open-access book about decoding mode-s and ads-b data," https://mode-s.org/, May 2017.

YongXin Liu (LIU11@my.erau.edu) received his first Ph.D. from South China University of Technology (SCUT) and currently working towards his second Ph.D. in the Department of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University, Daytona Beach, FL. His major research interests include data mining, wireless networks, the Internet of Things, and unmanned aerial vehicles.

Jian Wang (wangj14@my.erau.edu) is a Ph.D. student in the Department of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University (ERAU), Daytona Beach, Florida, and a graduate research assistant in the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us). He received his M.S. from South China Agricultural University (SCAU) in 2017. His research interests include wireless networks, unmanned aerial systems, and machine learning.

Jianqiang Li (lijq@szu.edu.cn) received his B.S. and Ph.D. degrees from the South China University of Technology in 2003 and 2008, respectively. He is a Professor with the College of Computer and Software Engineering, Shenzhen University, Shenzhen, China. His major research interests include Internet of Things, robotic, hybrid systems, and embedded systems.

Shuteng Niu (shutengn@my.erau.edu) is a Ph.D. student in the Department of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University (ERAU), Daytona Beach, Florida, and a graduate research assistant in the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us). He received his M.S. from ERAU in 2018. His research interests include machine learning, data mining, and signal

Houbing Song (M'12–SM'14) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, in August 2012, and the M.S. degree in civil engineering from the University of Texas, El Paso, TX, in December 2006.

In August 2017, he joined the Department of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University, Daytona Beach, FL, where he is currently an Assistant Professor and the Director of the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us). He served on the faculty of West Virginia University from August 2012 to August 2017. In 2007 he was an Engineering Research Associate with the Texas A&M Transportation Institute. He has served as an Associate Technical Editor for IEEE Communications Magazine (2017-present), an Associate Editor for IEEE Internet of Things Journal (2020-present) and IEEE Journal on Miniaturization for Air and Space Systems (J-MASS) (2020-present), and a Guest Editor for IEEE Journal on Selected Areas in Communications (J-SAC), IEEE Internet of Things Journal, IEEE Transactions on Industrial Informatics, IEEE Sensors Journal, IEEE Transactions on Intelligent Transportation Systems, and IEEE Network. He is the editor of six books, including Big Data Analytics for Cyber-Physical Systems: Machine Learning for the Internet of Things, Elsevier, 2019, Smart Cities: Foundations, Principles and Applications, Hoboken, NJ: Wiley, 2017, Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications, Chichester, UK: Wiley-IEEE Press, 2017, Cyber-Physical Systems: Foundations, Principles and Applications, Boston, MA: Academic Press, 2016, and Industrial Internet of Things: Cybermanufacturing Systems, Cham, Switzerland: Springer, 2016. He is the author of more than 100 articles. His research interests include cyber-physical systems, cybersecurity and privacy, internet of things, edge computing, AI/machine learning, big data analytics, unmanned aircraft systems, connected vehicle, smart and connected health, and wireless communications and networking. His research has been featured by popular news media outlets, including IEEE GlobalSpec's Engineering360, USA Today, U.S. News & World Report, Fox News, Association for Unmanned Vehicle Systems International (AUVSI), Forbes, WFTV, and New Atlas.

Dr. Song is a senior member of ACM and an ACM Distinguished Speaker. Dr. Song was a recipient of the Best Paper Award from the 12th IEEE International Conference on Cyber, Physical and Social Computing (CPSCom-2019), the Best Paper Award from the 2nd IEEE International Conference on Industrial Internet (ICII 2019), the Best Paper Award from the 19th Integrated Communication, Navigation and Surveillance technologies (ICNS 2019) Conference, the Best Paper Award from the 6th IEEE International Conference on Cloud and Big Data Computing (CBDCom 2020), and the Best Paper Award from the 15th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2020).