Zero-bias Deep Learning Enabled Quickest Abnormal Event Detection in IoT

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

***Abstract*—Abnormal event detection with the lowest latency is an indispensable function for safety-critical systems, such as cyber defense systems. However, as systems become increasingly complicated, conventional sequential event detection methods become less effective, especially when we need to define indicator metrics from complicated data manually. Although Deep Neural Networks (DNNs) have been used to handle heterogeneous data, the theoretic assurability and explainability are still insufficient. This paper provides a holistic framework for the quickest and sequential detection of abnormalities and time-dependent abnormal events. We explore the latent space characteristics of zero-bias neural networks considering the classification boundaries and abnormalities. We then provide a novel method to convert zero-bias DNN classifiers into performance-assured binary abnormality detectors. Finally, we provide a sequential Quickest Detection (QD) scheme that provides the theoretically assured lowest abnormal event detection delay under false alarm constraints using the converted abnormality detector. We verify the effectiveness of the framework using real massive signal records in aviation communication systems and simulation. Codes and data are 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) and DNNs have been applied extensively in IoT. On the one hand, DL and DNNs have been successfully applied in smart devices for accurate recognition of complicated inputs [1]–[4]. On the other hand, time-consuming feature engineering is not always required as in conventional machine learning schemes [5]–[7]. Therefore, DL and DNNs are regarded as versatile tools to implement learning components in smart systems [8].

Although DL and DNNs are successful in general applications, DNNs in safety-critical systems requiring assured performance are still controversial. Firstly, applications in safety-critical systems require making accurate decisions with explainable behaviors, which is a major weakness of DNNs. Secondly, DNNs perform well and can be adopted to the domain of similar tasks. However, they cannot distinguish unseen data [9], termed as abnormalities, from specific abnormal events such as cyber-attacks. Although these unseen novel data are not usually available during network training, they are required to be detected in real-time with constrained false alarms [10]. The two obstacles impede the deployment of DL and DNNs in safety-critical systems.

For the first challenge, the eXplainable AI (XAI) has been proposed [11]. However, the XAI methods are insufficient for applying AI in safety-critical systems. Most of the related works treat DNN models as blackboxes and can only explain the importance of input dimensions for decision making and do not provide insights into the models' latent space. In safety-critical scenarios, knowing the models' behavior and performance boundaries are also important aspects for assurability.

To address the second challenge, deep autoencoders (AE) or Generative Adversarial Networks (GANs) are employed to capture the latent features of the domain-specific inputs by compressing and accurately reconstructing them. However, training AE or GAN models is even more computationally expensive than training DNN classifiers [12], [13]. Moreover, autoencoders or GAN models do not guarantee to respond with constrained false alarms [14]. Existing works have broadly covered single-shot (nonsequential) abnormality detection but do not provide methods to aggregate information when a single-shot detector is not always reliable. In our work, a single-shot abnormality detector can be treated as an early warning generator, and we can then use sequential event detection methods to aggregate information for abnormal event confirmation. Therefore, the detection of abnormal events is facilitated by the sequential detection of abnormalities. One popular method is Quickest Detection, it ensures the lowest latency under predefined false alarm constraints [15]. However, there are still some gaps in integrating DNN with sequential event detection algorithms.

In this paper, we utilize an enhanced deep learning framework based on our previous work, the zero-bias DNN [16], for the detection of abnormal events based on a hybrid event detection paradigm. Compared with the previous work, we apply zero-bias DNN as a single-shot warning generator in the sequential event detection paradigm. Moreover, Quickest Event Detection is employed for sequential processing with minimum latency and false alarm constraints. Additionally, we provide a thorough analysis of the latent space characteristics of zero-bias DNN, especially for abnormalities and classification errors. The effectiveness of the proposed framework in

Yongxin Liu and Shuteng Niu were with the Security and Optimization for Networked Globe Laboratory (SONG Lab), Embry-Riddle Aeronautical University, Daytona Beach, FL 32114 USA. Yongxin Liu and Lei Wu are with the Department of Computer Science, Auburn University at Montgomery, Montgomery, AL 36117 USA.

Jian Wang and Houbing Song are with the Security and Optimization for Networked Globe Laboratory (SONG Lab), Embry-Riddle Aeronautical University, Daytona Beach, FL 32114 USA (email:h.song@ieee.org)

Shuteng Niu is with the Department of Computer Science, Bowling Green State University, Bowling Green, OH 43403 USA

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

Manuscript received March 19, 2021; revised XXX.

handling massive signal recognition has been demonstrated. The contributions of this paper are as follows:

- We thoroughly analyze zero-bias DNNs' latent space characteristics. We explore the decision boundaries of different classes and reveal the essence of classification errors.
- We provide a novel method to efficiently convert existing DNN classifiers into binary DNN abnormality detectors, which are with assured performance and better adaptivity.
- We integrate the zero-bias DNN with Quickest Detection to provide a novel sequential abnormal event detection framework. We validate the solution on the detection of identity spoofing attacks on real Automatic Dependent Surveillance Broadcasting (ADS-B [17]) signals.

Our research offers a solution to accurate detection of abnormal events and abnormalities with an assured performance, thus useful in promoting trustworthy IoT and deepening the understanding of deep neural networks. Besides, this framework can be applied in other scenarios that require sequential event detection, such as stock investment or pandemic reaction [15]. Some of our works are presented in [18]. In this paper, we significantly improved the methods with better adaptivity and validated the methods using more datasets and experiments.

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 and abnormal event detection plays an increasingly important role in safety-critical and latency-constrained IoT. Nowadays, heterogeneous data are generated timely in large volumes. Therefore, quick and reliable identification and detection of abnormal events and abnormalities are increasingly discussed.

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 [19], the authors first trained a CNN model 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, abnormality detection is categorized as the Open Set Recognition [20], [21] problem. In [22], the authors used a GAN model to generate highly realistic fake data. Then they used the discriminator network to distinguish whether an input is from an abnormal source. In [23], the authors provided 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. In [24], the authors dynamically trained GAN networks to identify the poisoned input generated by adversaries in federated learning [25]. In [26] the authors employed autoencoders for robust abnormal detection in industrial IoT.

B. Quickest 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 [16], 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 [14].

From the perspective of the stochastic process, a system in different states can be described by distributions with measurable statistical properties [27]. Therefore, transitions within states cause the change of those properties. The QD algorithms aim to detect the change as quickly as possible, subject to predefined false alarm constraints [28]. 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 [29].

Given that the characteristics of the observed system prior to some specific events are usually known in advance [29]. We can 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 and many sequential change point detection algorithms can be applied directly [30]. For example, in Cumulative Sum Control Chart (CuSum) algorithm, the statistic metric of an ongoing event is calculated periodically. The current metric is then compared with the metrics in the known normal status. And the discrepancies between the two metrics can be transformed into a 1-D time series. Finally, the CuSum algorithm sends an alarm when the cumulative sum of the discrepancies reaches a threshold. However, a postchange distribution may not be known in some scenarios. Consequently, 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.

TABLE I
Comparison of methods

Methods	Category	Feature Extraction	Assurability	Controllable False Alarms	Model Explainability
QD and manual metric-based Abnormal Event Detection	Sequential Detection	Manual	High	Yes	High
DL Enabled Known Event Detection	Single-shot Detection	Automatic	No	Yes	Low
DL Enabled Abnormal Event Detection	Single-shot Detection	Automatic	No	No	Low
Our approach: Integration of QD & DL	Sequential Detection	**Automatic**	**High**	**Yes**	**Median**

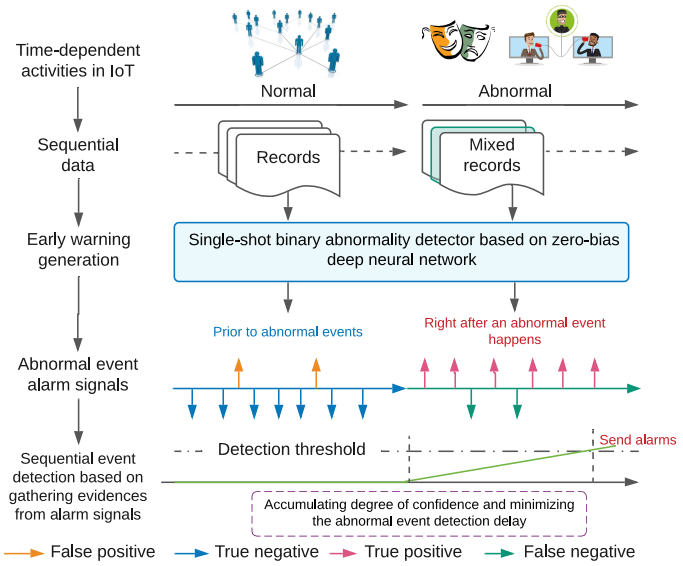


Fig. 1. System model of zero-bias deep learning enabled quickest abnormal event detection in IoT.

However, the selection of statistic metrics still depends on manual trial-and-error. A comparison of existing methods is given in Table I. We focus on real-time sequential detection of events, especially on integrating the quickest detection with deep learning seamlessly, and provide an automated and performance-assured solution for latency-constrained CPS.

III. Problem Definition

In many 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 variations of specific statistical indicator metrics. By analyzing the drift or variations of these metrics, abnormal events can be detected sequentially. Our proposed framework is depicted in Figure 1. We aim to use deep neural networks to process heterogeneous data from IoT and spot abnormal events through complex data. We then use the quickest event detection algorithm to detect ongoing abnormal events with minimum latency. In this research, the single-shot abnormality detector is also termed as an early warning generator.

We assume that a surveillance oracle can sequentially collect a system's state variables, denoted as:

$$S = \{\boldsymbol{S_1}, \boldsymbol{S_2}, \dots \boldsymbol{S}_j \dots \boldsymbol{S}_{j+m} \dots\} \tag{1}$$

where $\boldsymbol{S_j}$ denotes a state variable or record in vector form, an abnormal event appears at j and is detected at $j+m$. Real-time abnormal event detection requires minimizing m with constrained false alarm.

Some well-known methods are provided in the Quickest Detection algorithms. For example, in the CuSum algorithm, a likelihood ratio test is employed to sequentially process the observed data at each timestamp k, denoted as:

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

where $g(k)$ is the indicator metric, also termed as the sufficiency metric, $P_0(\cdot)$, $P_1(\cdot)$ denotes the probabilistic density functions of normal 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 [15], [31]. However, CuSum-style quickest detection algorithms can hardly handle high-dimension data, where the analytical form of $P_0(\cdot)$ and $P_1(\cdot)$ are difficult to obtain. Even though some works use DNNs to derive $g(k)$ from high dimension data numerically, the uncertain responses of DNNs make the theoretical performance assurance impossible. To enable deep learning for quick and reliable abnormality detection, we need to: i) use a DNN driven abnormality detection model to process complex data and provide theoretically assurable and predictable performance. ii) 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 latent space characteristics. We then provide an efficient method to convert zero-bias DNN into a performance assured abnormality detector. Finally, we provide our method to integrate zero-bias DNN with the quickest detection algorithms.

A. Zero-bias Neural Networks

This subsection analyzes the characteristics of zero-bias neural networks, an enhanced neural network model with transparent decision characteristics.

We have shown that the last dense layers of a DNN classifier perform the nearest neighbor matching with biases and weights using cosine similarity in [16]. To eliminate unwanted biases and weights, we convert a regular DNN model into a zero-bias DNN by replacing its classification dense layer (the dense layer before Softmax function) with a zero-bias dense layer. We can formulate the zero-bias dense layer as:

$$\boldsymbol{Y}_0(\boldsymbol{X}) = \boldsymbol{W}_0\boldsymbol{X} + \boldsymbol{b} \tag{4}$$

$$L(\boldsymbol{X}) = cosineDistance(\boldsymbol{Y}_0, \boldsymbol{W}_1) \tag{5}$$

where $\boldsymbol{X}$ is the feature vector. $\boldsymbol{W}_1$ is a matrix to store fingerprints of different classes. For any feature vector, A zero-bias dense layer consists of two functions, linear transform (equation 4) and fingerprint matching (equation 5). In this paper, $\boldsymbol{X}$ 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

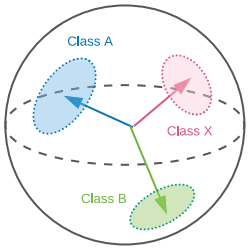


Fig. 2. The latent space (hyperspherical surface) for classification in zero-bias DNNs. Please note that even for a regular neural network, its classes' governing region can be represented and visualized using a 3D unit spherical surface [34]

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 of q elements. Therefore, $L(\cdot)$ performs the final label association. $L(\cdot)$ can be implemented by:

$$L(\boldsymbol{X}) = \boldsymbol{RU}(\boldsymbol{W_1}) \times \boldsymbol{CU}(\boldsymbol{Y_0}) \tag{6}$$

where $\boldsymbol{RU}(\cdot)$ or $\boldsymbol{CU}(\cdot)$ denote scaling vectors in each row or column of the input matrix into unit vectors. Our prior results [16], [32] also prove that zero-bias DNN can be trained using common loss functions (e.g., binary crossentropy, MSE, and etc.).

B. Classification Boundaries of Zero-bias DNN

Mathematically, the cosine similarity in Equation 6 represents the similarity matching of fingerprints and feature vectors on an N_1-D unit hyperspherical surface. *This hyperspherical surface is termed as the latent space of the zero-bias DNN.* A 3-D concept is depicted in Figure 2. Fingerprints divide the unit hyperspherical surface into several subregions. If we remap the dimension of class fingerprints and feature vectors into 2D, Voronoi Diagram [33] can be used to analyze their relationship and decision boundaries.

For example, in the DNN enabled MNIST handwritten digit recognition [35], the network's last dense layer is replaced by a zero-bias dense layer with $N_1 = 10$. The Voronoi diagrams at two training stages (accuracy being 85% and 97%) of class fingerprints in the latent space are depicted in the left first column of Figure 3. In the figure, we also depict the feature vectors from the test set.

In the second (central) column of Figure 3, we present the latent space of our major task with the zero-bias DNN (architecture presented in Figure 9). In this experiment, the neural network is trained to recognize aircraft through their signals.

Finally, in the third (right) column of Figure 3, we present the latent space of a drones' RF signal recognition task [36] using the DNN model as in Figure 9) with dataset in [37]. In this task, the neural network is trained to recognize three drones and nine different operational states.

From the observation, even though different datasets and models are used, there are some similar characteristics in the latent space of zero-bias DNNs: i) at the early stage of training, data from different classes are mapped into overlapped clusters. ii) As the training moves on, the data clusters are gradually separated distinctively. We conclude that in zero-bias DNNs, the classification error results from overlapped clusters in the latent space.

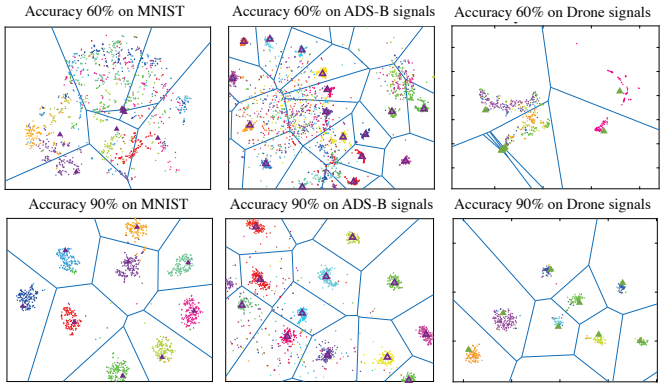


Fig. 3. Class fingerprints (purple rectangle), feature vectors (points), class boundaries (blue lines) and latent space feature vectors (represented by dots in different colors) from different dataset (MNIST hand written digits [35], Aviation ADS-B signals [38] and Drones' RF signals [36], [37]) under different training stages. All vectors are projected to a 2D space using *t-SNE* [39].

C. Abnormality detection with zero-bias DNN

The effectiveness of zero-bias DNN for nonsequential (single-shot) abnormality detection has been demonstrated in our prior results [16], [32]. It is better than regular DNN and comparable to one-class SVM [40]. 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 detectors from existing DNN classifiers: In Figure 3, feature vectors from known classes are closely projected to the vicinity of the corresponding class fingerprints. However, for abnormality detection with assurable performance, we need to understand the detector's characteristics under normal and abnormal data.

We use two different datasets to analyze the relation of normal and abnormal data:

1) We train the zero-bias DNN to recognize handwritten digits from 1 to 7 and use digits 8, 9, and 0 as abnormal data. The Voronoi diagram of class fingerprints stacked with known and abnormal data is depicted in the left part

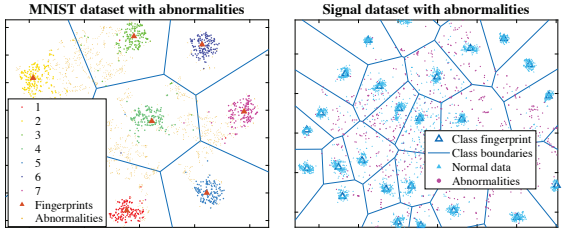


Fig. 4. Class fingerprints and feature vectors in the latent space of different models. The two models are trained with 92% accuracy.

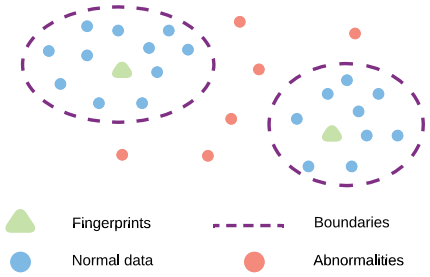


Fig. 5. Distribution of normal (trained) and abnormal data in the latent space of zero-bias DNNs.

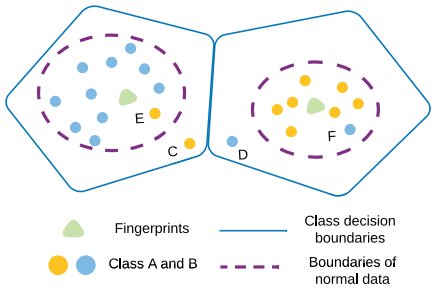


Fig. 6. Distribution of erroneously classified data in the latent space of zero-bias DNN, feature vectors of C, D, E and F are erroneously projected into governing regions.

of Figure 4. Here, the handwritten digits dataset is only an example to demonstrate the phenomenon.

2) We train the DNN model in Figure 9 on the aviation communication signal dataset in [38]. We use the 30 most frequently seen aircraft signals as normal data for the neural network is trained to recognize. In comparison, the remaining aircraft's signals are treated as abnormalities. The result is presented in the right part of Figure 4.

Even though we used different datasets and models, we observed a similar phenomenon. That is, the abnormal data are sparsely distributed in the latent space, and they have few chances to mix into clusters of normal data, as also depicted in Figure 5, we come to our first remark:

Remark 1. *In the latent space of zero-bias DNN, data from unknown novel classes, which are termed as abnormalities, are less likely to mix into the clusters of existing trained classes.*

We can also derive a basic principle 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 latent space. Then the incoming data's feature vectors that are out of normal data boundaries are regarded as abnormalities.*

For a given DNN model with the 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 the converted abnormality detector. We pass accurately classified data of ith known class from the training set, denoted as $\boldsymbol{KX}_i$, through layers of the DNN model and obtain the compressed feature vectors before fingerprint matching, denoted as:

$$\boldsymbol{Y}_0[F_{n-1}(\boldsymbol{KX}_i)] = \boldsymbol{W}_0 F_{n-1}(\boldsymbol{KX}_i) + \boldsymbol{b} \quad (7)$$

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

$$\begin{aligned} \boldsymbol{c}_0^i &= mean(\boldsymbol{Y}_0[F_{n-1}(\boldsymbol{KX}_i)]) \\ \boldsymbol{P_i} &= cov(\boldsymbol{Y}_0[F_{n-1}(\boldsymbol{KX}_i)], \boldsymbol{Y}_0[F_{n-1}(\boldsymbol{KX}_i)]) \end{aligned} \quad (8)$$

Step 3: Calculate the Mahalanobis distances [41] 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 $\boldsymbol{KX}_i$:

$$CO_i = max\ \boldsymbol{D_m}[\boldsymbol{Y}_0[F_{n-1}(\boldsymbol{KX}_i)], \boldsymbol{c}_0^i] \quad (9)$$

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

Step 4: Abnormality detection using cut-off boundaries on input data ($\boldsymbol{X}$) is formally defined as:

$$D(\boldsymbol{X}) = \begin{cases} 1 & \exists\ i,\ \boldsymbol{D_m}[\boldsymbol{Y}_0[F_{n-1}(\boldsymbol{X})], \boldsymbol{c}_0^i] \leq CO_i \\ 0 & \text{Otherwise} \end{cases} \quad (10)$$

These steps convert zero-bias DNNs into abnormality detectors with binary outputs, also termed as early warning generators. In essence, we construct statistical models for each class to describe the distribution of corresponding normal data with a hard cut-off distance to form its boundary (denoted as dashed purple lines in Figure 5). From the perspective of Domain Adaption, abnormalities and normal data are separated into different domains with different distributions [42].

2) Theoretic performance Analysis: We introduce the hard cut-off distances of class fingerprints. Therefore, a binary abnormality detector converted from zero-bias DNN becomes a binary classifier. We derive two important properties of this type of binary 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 6. 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 6 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 the binary 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 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:*

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

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:*

$$RU_{FNR} = \frac{\sum_{i=1}^{N_c} S_{hsp}^{i}(N_1)}{A_{hsp}(N_1)}$$
$$With\ FNR \leq RU_{FNR},\ TPR \geq 1 - RU_{FNR} \tag{12}$$

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. $S_{hsp}^{i}(N_1)$ is the surface area of normal data of the ith class.

Analytically calculating $S_{hsp}^{i}(N_1)$ is difficult since the shapes of these occupied subregions are unknown. Therefore, we use the Monte Carlo method to estimate RU_{FNR} directly. Corresponding pseudo code is presented in Algorithm 1. Specifically, we first generate M random points uniformly distributed on the surface of the N_1-D unit hypersphere (in line 2). We then count the number of points that are within the cut-off distance of each known class (from line 5 to 10). Finally, the ratio $\frac{chx}{M}$ is the sum of the covered areas of known classes' regions. The captured rate directly indicates the value of RU_{FNR}. Empirically, we set $M = 50,000$. In essence, we sample the latent space randomly and count the number of points captured by known classes' regions.

Algorithm 1 Estimating RU_{FNR}

```
1: function RU_FNR(N_1, N_c, M, List[CO], List[c_0^i])
2:     HX ← UniformHypersphereRand(N_1, M)
3:     chx ← 0
4:     for k ← 1 ... M do
5:         for i ← 1 ... N_c do
6:             if D_m[HX_k, c_0^i] ≤ CO_i then
7:                 chx ← chx + 1
8:                 break
9:             end if
10:        end for
11:    end for
12:    return chx / M
13: end function
```

D. Zero-bias DNN for quickest abnormal event detection

1) Sequential formalization and detectability: Given the theoretic analysis of the binary abnormality detector in section IV-C2, 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 [43]:

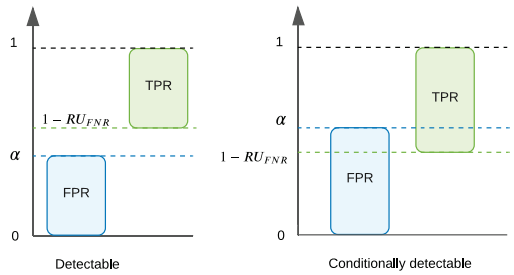


Fig. 7. Range of true positive and false positive rates and detectability criteria.

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

where $I_k \in \{0, 1\}$ is the output of the binary abnormality detector with $I_k = D(\boldsymbol{X_k})$. FPR can be estimated on existing data, and the range of FNR and TPR can be estimated using Algorithm 1. 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 abnormality detector's True Positive rate (TPR) lower bound ($1 - RU_{FNR}$) are greater than its 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 7) and we may encounter an extreme case: $TPR = FPR$. Therefore, the abnormal event is only conditionally detectable.

2) Quickest detection algorithm: With Remark 5, we can use Quickest 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 Gener-

alized Likelihood Ratio (GLR) Chart and its approximation, the multiple Bernoulli CuSum Chart, respectively. Compared with the existing nonparametric solutions, we discretize the continuous probabilistic function space. And the detection problem is transformed into a sequential parametric hypothesis testing problem.

Using Bernoulli GLR Chart [44] to sequentially detect abnormal events. We have:

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

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

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

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 [44]:

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

Where ARL is the average run length between false alarms.

Theoretically, we have to store a long sequence ($0 \le \tau \le k-1$) 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 [45] and [44], 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 $h_{CuSum} = h_{GLR}$ [44], [46]. The approximated range of TPR covered by each CuSum chart is:

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

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:

$$\bar{T}_{GLR} \sim \frac{h_{CuSum}}{I(P_1, P_0)} \tag{18}$$

where h_{CuSum} is the threshold for triggering the alarm while $I(P_1, P_0)$ is the Kullback-Leibler information number [31]. 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 [38] to train an aircraft signal identity recognition DNN model. Then we use the proposed method to convert the DNN model into a binary abnormality detector that functions as an early warning generator. Finally, we evaluate the performance of sequential abnormal event detection using different event detection algorithms with various configurations. In this section, the abnormal event is denoted as receiving signals generated by identity spoofing attackers.

A. Dataset and application scheme

Our dataset is available in [38], we use the wide-spreading signals from the ADS-B system [17], which provides a great variety of signals from commercial aircraft's signal transponders with their unique IDs as labels. Specifically, aircraft use transponders at 1090MHz to broadcast their geo-coordinates, velocity, altitude, heading, as well as its unique ID to the Air Traffic Control Center (ATC). The integrity and trustworthiness of ADS-B messages are critical to aviation safety. However, the ADS-B system does not contain cryptographic identity verification mechanisms. Thus, the aircraft IDs can be forged easily, which makes the whole system vulnerable to identity spoofing attacks (depicted in Figure 8). Our previous works [16], [32], [47] have shown that the responses of the zero-bias DNN to known (learned) aircraft and unknown sources (also from unknown aircraft) can be modeled by different probability distributions. Here we define the appearance of unknown aircraft's signals as abnormal events. We use the framework in this paper to convert the original aircraft identification model into a binary abnormality detector. And then use sequential event detection algorithms to process responses from the binary abnormality detector to detect the appearance of the adversaries that transmit fake ADS-B signals.

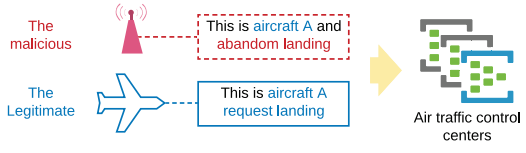


Fig. 8. Identity spoofing attack in aviation communication systems.

From the perspective of DL, the input is the raw signal collected by a Software Defined Radio Receiver (USRP B210), and the DNN is trained to identify the known aircraft through their signals. As in our prior work [16], [32], we take the first 1024 samples from each signal record. And then convert the 1024 samples into a 32 by 32 by 3 tensor, which incorporates pseudonoise, magnitude-frequency, and phase-frequency

features. The architecture of our DNN model is depicted in Figure 9 with a description of the dataset in Table II. After training to recognize known aircraft, the zero-bias DNN model is then converted to a binary abnormality detector as in Section IV-C.

TABLE II
DESCRIPTION OF DATASET

Usage	Description
Training	60% of signal records from 28 aircraft.
Test	40% of signal records from 28 aircraft.
Normal data	The test set.
Abnormal data	Signal records from the remaining 100 aircraft.

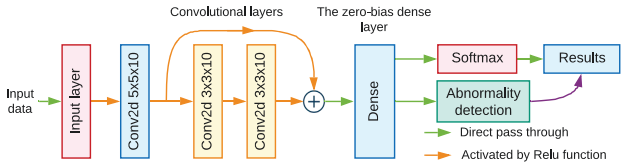


Fig. 9. Deep neural network architecture of zero-bias aircraft identification model [32].

B. Performance of the converted binary abnormality detector

The zero-bias neural network model for aircraft signal recognition is trained with 92% accuracy in identifying known aircraft. After training, its unit hypersphere coverage ratio is 12.7%. The binary abnormality detector trained on our dataset has a true positive and a true negative rate of 95% and 92%, respectively, which is closely matched with our prediction as in Remark 3 and 4. We compare the performance of our binary abnormality detector with the existing methods in Table III. As presented, the binary abnormality detector converted from the zero-bias neural network achieves the best performance. This binary abnormality detector is then used as an early warning generator for sequential abnormal event detection.

The relation of the performance of the converted abnormality detector and the zero-bias DNN model's accuracy before conversion is given in Figure 10a. Meanwhile, the coverage ratio of all classes on the unit hyperspherical surface during training is given in Figure 10b. As predicted, when the accuracy of zero-bias DNN gets higher, the abnormality detector simultaneously produces higher true positive and lower false positive rates. Interestingly, the occupied area becomes smaller when the zero-bias DNN model gets higher accuracy.

TABLE III
COMPARISON OF SINGLE-SHOT ABNORMALITY DETECTORS.

Metric	One-class SVM [1]	Zero-bias DNN [1]	Regular DNN [1]	Ours
False Positive	0.19	0.2	0.2	**0.07**
False Negative	0.05	0.05	0.28	**0.05**

[1] Each of the them requires a threshold value to distinguish abnormalities, thresholds are selected according to the maximum margin of separation as in our previous work [16].

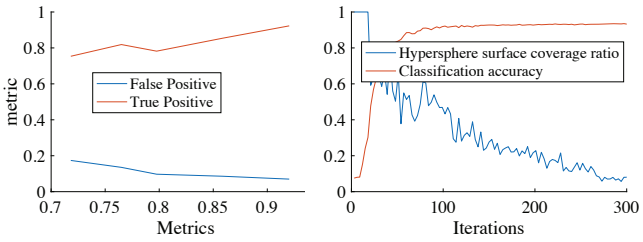


Fig. 10. Comparison of metrics: (a) True Positive and False Positive rates of the converted binary abnormality detector. (b) Latent space (unit hypersphere surface) coverage ratio during the training of a zero-bias DNN model.

C. Quickest abnormal event detection

To further evaluate our proposed method, we first define a quality metric, $Q = \frac{TPR}{FPR}$, for the binary abnormality detector. Then, we can use numerical simulation to evaluate the performance of zero-bias DNN under different Q values and different sequential detection algorithms: CuSum [31], EWMA (Exponentially Weighted Moving Average [48]) chart, and sliding window [49]. We simulate the possible values of h_{GLR}, FPR, and TPR that a binary abnormality detector can encounter with $TPR \in [0.6, 0.99]$, $FPR = 0.4$, $Q \in [1.625, 2.25]$. We configure three sequential detection algorithms as follows:

- *GLR chart:* we set the event detection threshold $h_{CuSum} \in [10, 20.0]$.
- *EWMA chart:* we set $\lambda = 0.15$ and $L \in [3.0, 4.0]$.
- *Sliding window for moving average:* we set the length of the window to $L \in [50, 300]$ with a threshold 0.7.

We select the parameters of all these sequential detection algorithms to cover the full range (0 to 1) of the false alarm rate.

The results are presented in Figure 11a, 11b and 11c, respectively. We summarize the observed phenomenons as follows:

- As in Figure 11a, we compare the detection delay of different algorithms using different parameters. In the GLR chart and sliding window, the detection delay increases linearly as the detection threshold gets higher or the length window gets longer. However, when using the EWMA chart, we observe some nonlinear growth patterns in the detection delay when the quality metric of the binary abnormality detector is low. Therefore, EWMA's detection delay is sensitive to the configuration of parameters. It outperforms the GLR chart and sliding window when the quality metric of the binary abnormality detector is sufficiently high. Meanwhile, the GLR chart provides the lowest detection delay even when the quality metric of the binary abnormality detector is low.
- As in Figure 11b, we compare the relation of detection delay and false alarms. In the three algorithms, we get a

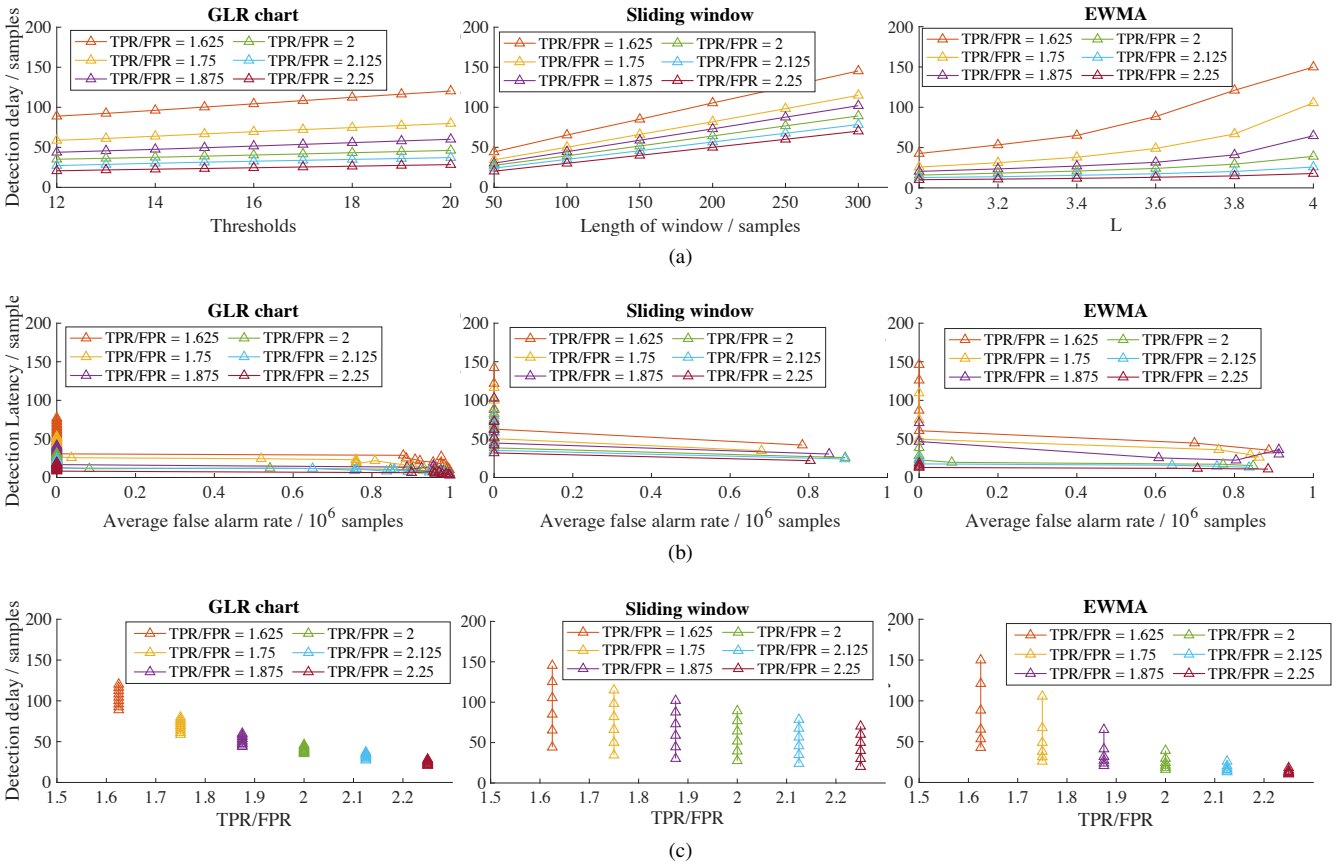


Fig. 11. Comparison of sequential event detectors under various quality metrics: (a) Comparison of detection delays with different configurations of sequential detection algorithms. (b) Comparison of average false alarm rates and detection delays. (c) Comparison of detection delays under zero false alarm constraints

longer detection delay if we want a low false alarm rate. We also notice that the sliding window gets the longest detection delay when the false alarm ratio is constrained to a specific value. Meanwhile, if we allow some false alarms, the GLR chart gets lower detection delay even when the quality metric of the binary abnormality detector is low.

- Finally, as in Figure 11c, we compare the distribution of detection delays of the three algorithms when the false alarm ratio is zero. The distribution of detection delays in GLR chart spans within smaller ranges. Meanwhile, the EWMA chart provides the best performance while the quality metric of the binary abnormality detector is sufficiently high.

In general, the quality of the single-shot binary abnormality detector significantly benefits the quick detection of abnormal events in these sequential statistical tests. The CuSum algorithm-enabled GLR chart provides the most balanced performance under various quality metrics of binary abnormality detectors.

VI. Conclusions and Future Scope

In this paper, we have significantly extended the analysis of our previously proposed zero-bias DNN and combined it with the Quickest Detection algorithms. We facilitate the application of Deep Learning in the detection of abnormalities and time-dependent abnormal events with the assured lowest latency. We first used the Voronoi diagram to explore the latent space characteristics of zero-bias DNNs. We then proposed a solution to convert zero-bias DNN classifiers, which are easier to obtain, into binary abnormality detectors with assurable and predictable performance. We developed a method to model the converted abnormality detectors using Bernoulli distribution, which perfectly adapts to the Generalized Likelihood Ratio based Quickest Detection scheme with theoretically assured detection delay under specified false alarms. Finally, we validated the framework using both massive ADS-B signal records from real aviation communication systems.

Our work in this paper contributes to the development of a more reliable and trustworthy AI paradigm for IoT. However, we still have several challenges in the future. Firstly, DNNs have to get trained rapidly facing the requirements of data-intensive applications such as cloud computing [50]. We can exploit the latent space characteristics of DNNs discussed in this paper to develop data-efficient machine learning paradigms. Secondly, it is computationally expensive to retrain DNNs from scratch when we encounter new tasks [51]. Therefore, developing efficient incremental learning algorithms to expand existing DNNs' capability continuously will also be of great significance. Thirdly, DNN models may encounter adversarial attacks in the real world. We need to explore the feature space of DNNs to find protection mechanisms [52]. Finally, in our signal identification and detection application, we may encounter highly realistic fake inputs generated

by Generative Adversarial Networks (GANs) [4]. Such fake inputs will significantly increase the difficulty of detection. Therefore, it is important to introduce fake signal generators when deriving more reliable signal identification and detection networks.

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] Y. Liu, J. Wang, J. Li, S. Niu, and H. Song, "Machine Learning for the Detection and Identification of Internet of Things (IoT) Devices: A Survey," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[5] 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.

[6] 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.

[7] J. Wang, Y. Liu, and H. Song, "Counter-Unmanned Aircraft System (s)(C-UAS): State of the Art, Challenges, and Future Trends," *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 3, pp. 4–29, 2021.

[8] G. Dartmann, H. Song, and A. Schmeink, *Big data analytics for cyber-physical systems: machine learning for the internet of things*. Elsevier, 2019.

[9] M. Wang and W. Deng, "Deep visual domain adaptation: A survey," *Neurocomputing*, vol. 312, pp. 135–153, 2018.

[10] 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.

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

[12] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions," *Electronics*, vol. 9, no. 7, p. 1177, 2020.

[13] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[14] 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.

[15] L. Xie, S. Zou, Y. Xie, and V. V. Veeravalli, "Sequential (Quickest) Change Detection: Classical Results and New Directions," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 2, pp. 494–514, 2021.

[16] 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*, vol. 8, no. 4, pp. 2627–2634, 2021.

[17] J. Sun, "An open-access book about decoding Mode-S and ADS-B data," https://mode-s.org/, May 2017.

[18] Y. Liu, Y. Chen, J. Wang, S. Niu, D. Liu, and H. Song, "Zero-bias deep neural network for quickest rf signal surveillance," *arXiv preprint arXiv:2110.05797*, 2021.

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

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] R. Taheri, M. Shojafar, M. Alazab, and R. Tafazolli, "FED-IIoT: A robust federated malware detection architecture in industrial IoT," *IEEE Transactions on Industrial Informatics*, 2020.

[25] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, 2020.

[26] E. K. Wang, X. Liu, C.-M. Chen, S. Kumari, M. Shojafar, and M. S. Hossain, "Voice-transfer attacking on industrial voice control systems in 5g-aided IIoT domain," *IEEE Transactions on Industrial Informatics*, 2020.

[27] 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*, 2008, pp. 1–5.

[28] H. Poor and O. Hadjiliadis, *Quickest detection*. United Kingdom: Cambridge University Press, Jan. 2008, vol. 9780521621045.

[29] P. Johnson, J. Moriarty, and G. Peskir, "Detecting changes in real-time data: a users' guide to optimal detection," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 375, no. 2100, p. 20160298, 2017. [Online]. Available: https://royalsocietypublishing.org/doi/abs/10.1098/rsta.2016.0298

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

[31] P. Granjon, "The CuSum algorithm-a small review," 2013.

[32] Y. Liu, J. Wang, S. Niu, and H. Song, "Deep learning enabled reliable identity verification and spoofing detection," in *Wireless Algorithms, Systems, and Applications*, D. Yu, F. Dressler, and J. Yu, Eds. Cham: Springer International Publishing, 2020, pp. 333–345.

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

[34] L. Yongxin, "Visualization of neural network latent space using unit hypersphere," 10 2021. [Online]. Available: https://github.com/pcwhy/NeuralDBVis

[35] "Create simple deep learning network for classification - MATLAB & Simulink example," https://www.mathworks.com/help/deeplearning/ug/create-simple-deep-learning-network-for-classification.html, (Accessed on 07/12/2021).

[36] M. F. Al-Sa'd, A. Al-Ali, A. Mohamed, T. Khattab, and A. Erbad, "RF-based drone detection and identification using deep learning approaches: An initiative towards a large open source drone database," *Future Generation Computer Systems*, vol. 100, pp. 86–97, 2019.

[37] M. S. Allahham, M. F. Al-Sa'd, A. Al-Ali, A. Mohamed, T. Khattab, and A. Erbad, "DroneRF dataset: A dataset of drones for RF-based detection, classification and identification," *Data in Brief*, vol. 26, p. 104313, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352340919306675

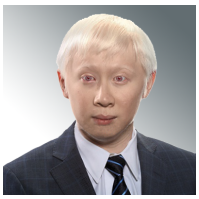
[38] Y. Liu, J. Wang, S. Niu, and H. Song, "ADS-B signals records for non-cryptographic identification and incremental learning." 2021. [Online]. Available: https://dx.doi.org/10.21227/1bxc-ke87

[39] 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.

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

[41] 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.

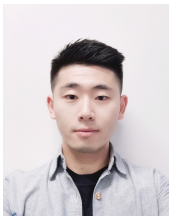
[42] K. You, M. Long, Z. Cao, J. Wang, and M. I. Jordan, "Universal domain adaptation," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2019, pp. 2720–2729.
[43] E. W. Weisstein, "Bernoulli distribution," *https://mathworld. wolfram. com/*, 2002.
[44] W. Huang, 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.
[45] 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.
[46] 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.
[47] Y. Liu, J. Wang, Y. Chen, S. Niu, Z. Lv, L. Wu, D. Liu, and H. Song, "Blockchain enabled secure authentication for unmanned aircraft systems," *arXiv preprint arXiv:2110.08883*, 2021.
[48] N. Ye, S. Vilbert, and Q. Chen, "Computer intrusion detection through ewma for autocorrelated and uncorrelated data," *IEEE Transactions on Reliability*, vol. 52, no. 1, pp. 75–82, 2003.
[49] C.-H. Lee, C.-R. Lin, and M.-S. Chen, "Sliding-window filtering: An efficient algorithm for incremental mining," ser. CIKM '01. New York, NY, USA: Association for Computing Machinery, 2001, p. 263–270. [Online]. Available: https://doi.org/10.1145/502585.502630
[50] S. S. Gill, S. Tuli, M. Xu, I. Singh, K. V. Singh, D. Lindsay, S. Tuli, D. Smirnova, M. Singh, U. Jain *et al.*, "Transformative effects of iot, blockchain and artificial intelligence on cloud computing: Evolution, vision, trends and open challenges," *Internet of Things*, vol. 8, p. 100118, 2019.
[51] Y. Liu, J. Wang, J. Li, S. Niu, and H. Song, "Class-incremental learning for wireless device identification in iot," *IEEE Internet of Things Journal*, pp. 1–1, 2021.
[52] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards deep learning models resistant to adversarial attacks," *arXiv preprint arXiv:1706.06083*, 2017.



Yongxin Liu (Yongxin.Liu@aum.edu) is currently an assistant professor at Auburn University at Montgomery, Alabama, USA. He received his first Ph.D. from South China University of Technology in 2018 and his second Ph.D. from the Department of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University, Daytona Beach, Florida in 2021. He was a graduate research assistant in the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us) from 2018 to 2021. His major research interests include cybersecurity, machine learning, data mining, Internet of Things, and unmanned aircraft systems.

Jian Wang (wangj14@my.erau.edu) is a Ph.D. student in the Department of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University, 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 at 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 received the Ph.D. degree in electrical engineering and computer science from the Embry-Riddle Aeronautical University, FL, in May 2021.

In August 2021, he joined the Department of Computer Science, Bowling Green State University, Bowling Green, OH, where he is an Assistant Professor. He was a graduate research assistant in the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us) from 2018 to 2021. His research interests include machine learning, data mining, and signal processing.

Lei Wu (lwu@aum.edu) received his Ph.D. in Computer Science at the University of Montreal in 2005. His research interests include Artificial Intelligence, Big Data Analytics, Video Game, STEM Education, and Robotics. He is currently a professor and head of the Department of Computer Science, College of Sciences, at Auburn University at Montgomery.

Houbing Song (M'12–SM'14) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, in August 2012.

In August 2017, he joined the Department of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University, Daytona Beach, FL, where he is currently the Director of the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us) and an Assistant Professor. He has served as an Associate Technical Editor for IEEE Communications Magazine (2017-2020), an Associate Editor for IEEE Internet of Things Journal (2020-present), IEEE Transactions on Intelligent Transportation Systems (2021-present), and IEEE Journal on Miniaturization for Air and Space Systems (J-MASS) (2020-present). He is the editor of eight books, the author of more than 100 articles and the inventor of 2 patents (US & WO). His research interests include cyber-physical systems/internet of things, cybersecurity and privacy, AI/machine learning/big data analytics, and unmanned aircraft systems. His research has been sponsored by federal agencies (including US Department of Transportation, National Science Foundation, Federal Aviation Administration, US Department of Defense, and Air Force Research Laboratory) and industry. His research has been featured by popular news media outlets, including IEEE GlobalSpec's Engineering360, Association for Unmanned Vehicle Systems International (AUVSI), Fox News, USA Today, U.S. News & World Report, Forbes, The Washington Times, WFTV, New Atlas, Battle Space and Defense Daily.

Dr. Song is a senior member of ACM and an ACM Distinguished Speaker. Dr. Song was a recipient of the Best Paper Awards from multiple international conferences, including CPSCom-2019, ICII 2019, ICNS 2019, CBDCom 2020, WASA 2020, DASC 2021 and GLOBECOM 2021.