Mobile Edge Computing-Based Data-Driven Deep Learning Framework for Anomaly Detection

BILAL HUSSAIN1, (Student Member, IEEE), QINGHE DU1, (Member, IEEE), SIHAI ZHANG2, (Member, IEEE), ALI IMRAN3, (Member, IEEE), AND MUHAMMAD ALI IMRAN4, (Senior Member, IEEE)

1Shaanxi Smart Networks and Ubiquitous Access Research Center, School of Information and Communications Engineering, Xi’an Jiaotong University, Xi’an 710049, China
2Key Laboratory of Wireless-Optical Communications, Chinese Academy of Sciences, University of Science and Technology of China, Hefei 230026, China
3School of Electrical and Computer Engineering, University of Oklahoma, Tulsa, OK 74135, USA
4School of Engineering, University of Glasgow, Glasgow G12 8QQ, U.K

Corresponding author: Qinghe Du (duqinghe@mail.xjtu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant No. 61671371, and in part by the Fundamental Research Funds for the Central Universities.

ABSTRACT 5G is anticipated to embed an artificial intelligence (AI)-empowerment to adroitly plan, optimize and manage the highly complex network by leveraging data generated at different positions of the network architecture. Outages and situation leading to congestion in a cell pose severe hazard for the network. High false alarms and inadequate accuracy are the major limitations of modern approaches for the anomaly—outage and sudden hype in traffic activity that may result in congestion—detection in mobile cellular networks. This indicates wasting limited resources that ultimately leads to an elevated operational expenditure (OPEX) and also interrupting quality of service (QoS) and quality of experience (QoE). Motivated by the outstanding success of deep learning (DL) technology, our study applies it for detection of the above-mentioned anomalies and also supports mobile edge computing (MEC) paradigm in which core network (CN)’s computations are divided across the cellular infrastructure among different MEC servers (co-located with base stations), to relief the CN. Each server monitors user activities of multiple cells and utilizes $L$-layer feedforward deep neural network (DNN) fueled by real call detail record (CDR) dataset for anomaly detection. Our framework achieved 98.8% accuracy with 0.44% false positive rate (FPR)—notable improvements that surmount the deficiencies of the old studies. The numerical results explicate the usefulness and dominance of our proposed detector.

INDEX TERMS Cellular network, anomaly detection, call detail record, deep learning, big data analytics, sleeping cell, congestion detection.

I. INTRODUCTION

To address the manifold capacity thirst in upcoming generation of cellular systems (5G), researchers are actively investigating advanced technologies: ultra-dense networks, massive multiple-input multiple-output (MIMO) systems, cognitive radios, etc. [1]. These will enforce radical changes to the cellular infrastructure making it more complex; an artificial intelligence (AI)-empowerment will therefore be pivotal in many aspects to efficiently manage the network.

The associate editor coordinating the review of this manuscript and approving it for publication was Junaid Shuja.
et al. defined anomaly as a city scene (highway, tourist area, railway station, etc.) that has unusual contextual meaning. Wang et al. [11] defined anomaly as a city scene (highway, tourist area, railway station, etc.) that has unusual network performance indicator values and characteristics, to carry out network optimization. Papadopoulos et al. [12] utilized billing-related information to identify anomalous mobile devices that carry out attacks against cellular network. In [13], a significantly deviated user QoE as compared with the predicted QoE is defined as an anomaly, and is utilized for network optimization.

In this paper, we treat and henceforth refer both network performance-related problems—sleeping cell and soared traffic that might result in congestion—as anomalies. Since sleeping cell or possible congestion can lead to a situation having unusually low or high cell traffic activity, respectively; we use anomaly in cell traffic pattern as proxy for anomaly in the network performance. Hence, we leverage subscriber call detail records (CDRs) for the anomaly detection. Traditionally, CDRs are compiled and maintained for administrative use (such as, for keeping proof of user’s network usage for billing purpose), but nowadays they are also exploited for diverse purposes: Securing 5G networks against cyberattacks [12], analyzing cell site [14], enabling energy efficient networks [15], and studying human mobility patterns [16].

Deep learning (DL) outperformed the performance of many conventional ML techniques and accomplished breakthroughs in various domains: computer vision, natural language processing, and genomics [18]. Additionally, mobile edge computing (MEC)—based on decentralized computation, network management, and storage, as compared with centralized cloud computing architecture—has recently gained attention for its potential utility in 5G networks to push computation towards the network edges (e.g. access points and base stations). It aims to relief core network (CN) from executing heavy-computation tasks and enables latency-critical and computation-intensive applications at resource-constrained mobile devices by leveraging huge idle storage space and computation power already available at the network edges [19], [20]. We contemplate DL blended with MEC can play a decisive role in the anomaly detection that will in turn improve user’s QoE and network’s QoS, increase customer retention, and reduce OPEX for the cellular operators.

This research addresses the detection problems in the viewpoint of DL and MEC. We build upon our previous work [21] and present an enhanced MEC-supported anomaly detection framework, executed at each MEC server monitoring a group of cells. The framework is based on L-layer feedforward deep neural network (DNN) that relies on real CDRs and aims to detect the anomalies with higher accuracy and lower false positive rate (FPR). In contrast to our rudimentary work [21], this extended research contains the following additional features:

1. Proposes MEC-based framework in which computation is offloaded to MEC servers, distributed across the cellular network, for efficient and robust anomaly detection.
2. Utilizes an advanced optimization technique known as adaptive moment estimation (ADAM) as compared with its predecessor known as momentum. Comparative analysis of ADAM’s performance with previously used optimization method is also performed using various additional measures: error rate, precision, recall and F1.
3. Introduces additional results to compare the training time of our model implemented by utilizing different optimization techniques.
4. Presents preprocessing algorithm, and explains the CDR data in more details with data visualization and a sample of raw CDR dataset to fully describe the DNN’s implementation.

Overall, this study makes the following contributions:

1. Applies an MEC-based DL framework that capitalizes on several modern DL techniques from the literature, to attain optimal performance for each cell and reliefs CN of heavy computation.
2. Exploits historical data to infer past user behavior’s trend for anomaly detection in recently-collected 10-minute user activity log datum (test instance).
3. Integrates an extra feature by considering Internet usage activity (neglected in the previous works) besides call and SMS, for a more robust framework.

The remainder of paper is organized as follows. Relevant work is summarized in Section II. Preliminaries to our DL based anomaly detection framework are explained in Section III. Framework’s implementation is described in Section IV. Subsequently, results and framework’s performance evaluation are discussed in Section V. Finally, discussion on results and concluding remarks are drawn in Section VI.
II. RELEVANT WORK

Current and old cellular networks treat anomaly detection as an important issue due to its apparent benefits to the network operators and the users. It is addressed in the literature by using variety of methods—mostly by utilizing various ML methods on some key performance indicators (KPIs) or measurements collected via minimize drive testing (MDT) feature of third generation partnership project (3GPP) release 10 [22].

Detection of sleeping cell engendered by hardware malfunction in the base station was carried out in [3], [23]–[26], in which catatonic sleeping cell (a cell in which user activity completely halts) was focused. On the other hand, [4], [27] oriented their studies to detect sleeping cell caused by RACH failure, in which crippled sleeping cell (a cell in which user traffic abates in contrast to normal) was targeted. In contrast, following studies dealt with the problems by employing data analytics on CDR dataset and proposed a lighter ML-based solution as their method utilized the existing data (CDRs) rather than KPIs; procurement of KPIs demands additional resources that burdens the network [1]. Parwez et al. [6] applied k-means and hierarchical clustering algorithms to detect soaring traffic (that may lead to congestion) in a cell by analyzing past one week data. Although the approach resulted in 90% accuracy, but it was time-inefficient as past one week data were considered to find the anomaly. Improving upon their work, [1] utilized a statistical-based semi-supervised ML approach to detect sleeping cell (both, catatonic and crippled) and the situation leading towards congestion in past hour’s data (having records for outbound and inbound call and SMS activities) by exploiting CDR dataset that had information about past several week’s user activities. They reported 92% accuracy; however, they also gained 14% false positive rate (FPR)—such a high FPR means that false alarms may waste a significant OPEX and resources.

As compared with the above works, our MEC-based solution utilizes data analytics (by incorporating past data with temporal features into the decision making, yielding in detecting long-term anomalies rather the instantaneous ones) and state-of-the-art techniques in DL literature to generate maximum accuracy and minimum FPR by analyzing each 10-minute CDR data-segment. The provided solution is (1) lighter for CN, as it is based on distributed deployment of MEC servers that distributes computation for anomaly detection instead of burdening the CN; (2) agile, as it utilizes CDR dataset instead of requesting addition data from the network; (3) robust, as it incorporates an extra Internet activity feature, apart from call and SMS activities; and (4) high-precision, as it has lesser false alarms and higher accuracy.

III. PRELIMINARIES

A. TOPOLOGY OF SYSTEM, AND VISUALIZATION AND CHARACTERIZATION OF THE DATASET

Topology of system, shown in FIGURE 1 (with functioning of the MEC server) and fully portrayed in Section IV, is established upon long term evolution - advanced (LTE-A) cellular
FIGURE 2. Data visualization: The spatiotemporal data are divided spatially into 100 × 100 cells across Milan city and temporally into 10-minute logs for a total of 62 days starting from 1st Nov., 2013 to 1st Jan., 2014. (a) An overlay of the 10,000 cells with Milan’s map (taken from Bing Maps). Each cell has a 235 m side length. A region, indicated by a red square, is zoomed-in for clarity. (b) Cell ID 5638, covering portion of a road alongside San Siro stadium, is shown. (c) and (d) illustrates user traffic activities of the cell ID 5638 in terms of SMS and call (both outbound and inbound), and internet, respectively.


<table>
<thead>
<tr>
<th>Cell ID</th>
<th>Time stamp (milliseconds)</th>
<th>Country code</th>
<th>SMS in</th>
<th>SMS out</th>
<th>Call in</th>
<th>Call out</th>
<th>Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3621</td>
<td>1388539800000</td>
<td>39</td>
<td>0.628319</td>
<td>0.274365</td>
<td>0.137755</td>
<td>0.058992</td>
<td>10.355361</td>
</tr>
<tr>
<td>3621</td>
<td>1388540400000</td>
<td>0</td>
<td>0.136609</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3621</td>
<td>1388540400000</td>
<td>39</td>
<td>0.374871</td>
<td>0.373152</td>
<td>0.147633</td>
<td>0.059278</td>
<td>15.282042</td>
</tr>
<tr>
<td>3621</td>
<td>1388541000000</td>
<td>39</td>
<td>0.265904</td>
<td>0.509475</td>
<td>0.000286</td>
<td>0.118844</td>
<td>12.445180</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Each entry represents beginning of a 10 minutes interval in Unix epoch. For example, 1388539800000 interprets as Wednesday, 01 January 2014, 1:30:00 AM (GMT). We can calculate end of the interval by adding 600000 milliseconds to this value.

* Some entries are missing that indicates no activity is recorded for the specified field [30].

network [1, Fig. 1]. CDR dataset utilized in this study was generated at LTE-A’s CN and made available by Telecom Italia [30].

The geo-referenced spatiotemporal (CDR) data contain over 319 million user-activity records for a 100 × 100 cells spread across Milan, Italy. An overlay map of these 10,000 cells with Milan’s map is shown in FIGURE 2(a). The dataset is temporally divided into 10-minute timestamps for a two-months duration from 1st Nov., 2013 to 1st Jan., 2014; provided in 62 files, each containing records of a single day. Each file contains on average 5.15 million records and each record contains five user-specific activity features: SMS incoming, SMS outgoing, call incoming, call outgoing and Internet usage. Some details pertaining to the subscriber—phone number, location and exact number (or unit) of each activity—are removed in order to preserve privacy. However, the provided quantity of activities is proportional to the real amount of activities [1]. A sample of the CDR dataset is given in Table 1.

To visualize the dataset, we focus on cell ID 5638 that covers an area close to San Siro stadium in western Milan (FIGURE 2(a) and (b)). Since the measurements of SMS and call activities (both inbound and outbound) have same scale [30], we extract and combine them for each hour and 62 days, illustrated in FIGURE 2(c). Similarly, the Internet activity is depicted in FIGURE 2(d). The annotated anomalous traffic activity spikes on 22nd Dec., 2013 correlates with an ongoing soccer match [31]; the one on 1st Dec., 2013 is also due to an ongoing match, and is also evident in the results of [1, Fig. 7(a)] and [6, Table 1].

B. DATA PREPROCESSING AND SYNTHESIS

For each cell, day, and 10-minute timeslot in a 24-hours timeline; raw CDRs are pre-processed to extract the features that are then merged to create a vector $x(i) \in \mathbb{R}^5$ (hereafter, referred as an instance), where $i$ is the index of the example. DL model requires large number (hundreds or even
Algorithm 1 Data Preprocessing

Inputs: CDRDataset: Raw dataset containing subscriber activities, recorded for each 10-minute duration and stored in the form of 62 files, each file representing a single day.
CID: Identification number of the target cell.
TimeStamValues: Contains numeric values of the beginning of every 10-minute time interval (in Unix epoch) during the intended 3-hours range.

Output: X_total

Method:

1: for each file f in CDRDataset
2:   Import file f and store its contents in a matrix.
3:   Replace blanks with 0.0 (to avoid error in summing NaN, in later steps).
4:   Remove the column containing Country codes.
5:   Update the matrix by storing entries only related to CID.
6:   Remove the column containing Cell ID.
7:   for each timestamp t in TimeStamValues
8:     Sum all inbound SMS activity values and store them as SMSin.
9:     Sum all outbound SMS activity values and store them as SMSout.
10:    Sum all inbound call activity values and store them as CALLin.
11:    Sum all outbound call activity values and store them as CALLout.
12:    Sum all Internet activity values and store them as Internet.
13:    Store SMSin, SMSout, CALLin, CALLout and Internet as one example in a vector x.
14:    Store example x as a column entry in matrix X_total.
15:  end
16: end
17: return X_total.

thousands) of examples to work on, that may correspond to CDRs of more than a year; however, we only have a total of 62 examples (for each timeslot and corresponding to 62 days). To overcome this hindrance and for data augmentation, we consider all the examples in a 3-hours range. Thus for a broader scope, we utilize three different timeslots: morning, from 6 to 9 am; afternoon, from 11 am to 2 pm; and evening, from 5 to 8 pm. The preprocessing method is summarized in Algorithm 1. The examples X_total are synchronously shuffled to have an identical distribution and to increase the effectiveness of the algorithm [32, Ch. 8]. We then divide them into training set with 781 examples (70% of the total) and test set having the remaining 335 examples.

Deep neural network (DNN) utilized in our research is based on supervised learning; hence, labeled dataset is compulsory for training and testing the model. Since output label y(i) ∈ R^1 (for each example in the training and test sets) is missing in the CDR data, we synthetically generate it by using Euclidean norm. An example x(i) is considered a point in 5-dimensional Euclidean space. The corresponding output label y(i) is marked 1 (anomaly) if the example’s norm ||x(i)||_2 deviates more than the norm of one standard deviation (SD) σ_SD ∈ R^5 from the mean µ ∈ R^5: ||µ − σ_SD||_2 > ||x(i)||_2 ≥ ||µ + σ_SD||_2; otherwise 0 (normal). Note, a higher SD means inclusion of more points as normal and having lesser anomalous points; this might not work well to detect performance deviations of a cell and hence we choose one SD. We can calculate the elements of mean and SD using the standard equations from statistics. We also utilize train set for this purpose. We arrange the corresponding labels of train and test set examples to form matrices Y_train ∈ R^1 × 781 and Y_test ∈ R^1 × 335, respectively.

C. PERFORMANCE METRICS

We employed several metrics for our model’s performance evaluation. Their values are calculated using the predicted test set output ˆY test ∈ R^1 × 335 and its comparison with the actual test set labels Y_test; and by using information from the confusion matrix [33], comprised of the following:

- True positive (T^+ve): number of examples labeled as anomalies by the algorithm (in the predicted test set output) that are also anomalies according to the test set labels.
- True negative (T^-ve): number of examples marked as normal and are actually normal instances.
- False positive (F^+ve): number of examples misclassified as anomalies.
- False negative (F^-ve): number of examples mislabeled as normal instances.

Using confusion matrix, we calculate the following performance metrics: accuracy (prediction’s success rate), error rate, precision (fraction of positive instances that are truly positive), recall (fraction of T^+ve from the total number of positive examples), FPR (F^-ve out of all the negative examples), and F_1 (weighted harmonic mean of the precision and recall); by using the following equations [33]:

\[
\text{Accuracy} = \frac{T^+ve + T^-ve}{T^+ve + T^-ve + F^+ve + F^-ve},
\]

\[
\text{Error rate} = \frac{F^-ve}{T^+ve + T^-ve + F^+ve + F^-ve} = 1 - \text{Accuracy},
\]

\[
\text{Precision} = \frac{T^+ve}{T^+ve + F^+ve},
\]

\[
\text{Recall} = \frac{T^-ve}{T^-ve + F^-ve},
\]

\[
\text{FPR} = \frac{F^-ve}{F^-ve + T^-ve},
\]
We apply $L$ over time. The framework residing in the MEC server can utilize the DNN to detect anomalies in the testing phase: when CDRs arrive after every 10-min duration. The framework can occasionally re-train the network as the performance degrades over time.

**IV. IMPLEMENTATION**

In this section, we briefly discuss the implementation details of $L$-layer feedforward deep neural network (DNN), integrated in our anomaly detection framework and how it is trained for each individual cell—optimally tuned in terms of number of layers, number of units each hidden layer contains, weight initialization strategy, regularization, and optimization method to yield maximum performance. Once trained, the framework can be integrated in our anomaly detection framework and how it is performed in a commercial PC (i7-7700T CPU, 16GB RAM, and Windows 10 64-bit operating system).

**A. DEEP LEARNING BASED ANOMALY DETECTOR**

We apply $L$-layer feedforward DNN having an input layer $l = 0$, hidden layers from $l = 1$ to $L - 1$ and an output layer $L$, illustrated in FIGURE 1(b), where $L$ represents number of (hidden and output) layers in the network. Each layer has one or more units (represented by circles in the figure) that uses a non-linear activation function to produce the output. Functions like sigmoid, hyperbolic tangent (tanh), rectified linear unit (ReLU), and leaky ReLU (LReLU) are thoroughly discussed in our previous work [21]; while Swish—gated version of sigmoid activation function—is a new function, reported to yield better results as compared with ReLU [34]. It is mathematically expressed below:

Swish function:

$$g(z) = z \times \sigma(z)$$  

(7)

where, $\sigma$ represents the sigmoid function. Sigmoid function is utilized in the output layer and one of the aforementioned functions is applied in the hidden layers. The model schematics with forward and backward propagations are also explained in [21]. Once the parameters (weights and biases) are fine-tuned, the trained DNN uses forward propagation to predict the output $\hat{Y}_{test}$ by utilizing the test set.

**B. IMPROVING PERFORMANCE OF DNN**

We leveraged different modern DL techniques in our framework, described below, to improve and render optimal performance.

1) **WEIGHT INITIALIZATION METHODS**

Gradient exploding or vanishing is a major problem faced during training phase due to inappropriate weight initialization, that makes learning difficult for the model. Heedful selection of initialization strategy can cure this and improve DNN’s performance by assigning weight values that are neither too small nor too large [17, Ch. 6]. We experiment with the following weight initialization strategies: Common, Xavier, and He (explained in details in [21]) in this study.

2) **REGULARIZATION**

A fundamental challenge to DNN is of overfitting, in which the model performs well on training set but fails to generalize to new examples. Regularization, which refers to modification of the learning algorithm, is used to control overfitting and reduce the test error [32]. $L^2$ regularization, also known as weight decay, is the most common type of regularization. It penalizes the square values of the weights in the cost function in order to drive all the weights to smaller values. Smaller values lead to simpler hypotheses, which are most generalizable [17].

Dropout [35] is another regularization technique in which neurons (along with their connections) are randomly shut down during training of a DNN; and hence at each iteration, a different model is trained that uses only a subset of the total neurons. The dropped neurons do not contribute to the training in both forward and backward propagations. A better generalization to an unseen data can be achieved as this technique prevents the network to have dependency on any particular neuron by making its presence unreliable [36]. FIGURE 3 demonstrates dropout mechanism using a 4-layer network (for simplicity).

Our experiments embed the above-discussed regularization techniques in the DNN model.

3) **OPTIMIZATION METHODS**

ADAM [37] is one of the most effective adaptive learning rate optimization algorithm for training a DNN that combines ideas from momentum (described in detail in [21]) and RMSProp (another optimization method for the details of which, readers can refer to [38]). ADAM uses the following update rule for weight $W^{[l]}$:

$$W^{[l]} = W^{[l]} - \alpha \frac{\text{v}^{\text{corrected}}}{\sqrt{\text{v}^{\text{corrected}} + \epsilon}}$$  

(8)
where, $v_{\text{corrected}}^{dW[l]}$ and $s_{\text{corrected}}^{dW[l]}$ (given below) are bias corrections, of first moment and second raw moment estimates, respectively, to account for their zero initialization [32, Ch. 8]; and $\epsilon$ is a small number added for numerical stability.

\[
v_{\text{corrected}}^{dW[l]} = v_{dW[l]} - (1 - \beta_1^t) v_{dW[l]}^{1}\frac{\beta_1^t}{1 - (1 - \beta_1^t) t}
\]

\[
s_{\text{corrected}}^{dW[l]} = s_{dW[l]} - (1 - \beta_2^t) s_{dW[l]}^{1}\frac{\beta_2^t}{1 - (1 - \beta_2^t) t}
\] where, $v_{dW[l]}$ and $s_{dW[l]}$ (given below) are exponentially weighted moving averages of historical gradient and the squared gradient, respectively; $t$ counts the steps carried by ADAM update; and $\beta_1, \beta_2 \in [0, 1)$ are hyperparameters that control the two averages.

The update rule for bias parameter $b^{l}$ is similar to the above rule. We implement ADAM in our DNN model and compare its test performance (in terms of various metrics mentioned in Sec. III-C) with gradient descent (GD), mini-batch GD, and momentum. For this purpose, the hyperparameter values mentioned in Table 2 are used, along with $\epsilon = 1 \times e^{-8}$ (suggested default value [32, Ch. 8]). Additionally, we investigate their training time.

V. EXPERIMENTAL RESULTS AND PERFORMANCE EVALUATION

We present various experimental results in this section. Although the CDR dataset contains records pertaining to 10,000 cells, our DNN model performs anomaly detection for a single cell at a time. To demonstrate robustness and transferability of our model, we present results based (averaged) on randomly chosen 1,000 cell IDs out of the total 10,000 cell IDs (available in Milan dataset). In addition, we also present results processed by using a small subset (up to ten cell IDs) for a detailed analysis and comparison. Note that mentioning of morning, afternoon or evening followed by a cell ID indicates that the model is trained and tested on a corresponding 3-hours range data (discussed in Sec. III-B).

A. NUMBER OF LAYERS AND HIDDEN UNITS

The performance of a DNN can vary across the spectrum of $L$ and $n_h^{[l]}$. In practice, framework would search for their optimum values that yield maximum accuracy for each cell by empirically evaluating their impact on the test accuracy of our DNN. To demonstrate this, we vary $L$ from 2 to 20 and $n_h^{[l]}$ from 1 to 50 using data from cell IDs 1 (Afternoon hours), 1943 (Evening hours), 5638 (Morning hours), and 9607 (Evening hours)—due to the inadequate space, we only show outcomes of these four randomly chosen cell IDs.

Our empirical results in the form of heatmaps, illustrated in FIGURE 4, elucidates the impact of various settings of $n_h^{[l]}$ and $L$ on the test accuracy. We also highlighted three particular examples signifying maximum accuracies. It can be seen that deeper layer having moderate number of hidden units yield the highest accuracy. Dual maximum accuracies imply that one might be computationally efficient to attain than other. For simplicity, we set $L$ and $n_h^{[l]}$ to 17 and 25, respectively, for our further experiments (for all cell IDs).

B. ACTIVATION FUNCTIONS

We run our model with mini-batch GD having hyperparameter values listed in Table 2, to find an activation function that yields maximum performance. FIGURE 5 (top) and (bottom) illustrates the effect of utilizing various activation functions in terms of error rate by using a subset of total cell IDs.
FIGURE 4. Test accuracies for cell IDs 1 (Afternoon hours), 1943 (Evening hours), 5638 (Morning hours), and 9607 (Evening hours) for various configurations of $n_h$ (number of hidden unit(s) per hidden layer) and $L$ (number of layers).

FIGURE 5. Impact of utilizing various activations in hidden layers on DNN’s performance.

and 1,000 cell IDs, respectively. We can clearly observe that sigmoid achieved the feeblest performance with highest error rate for most of the cell IDs in FIGURE 5 (top) while Swish also yielded overall poor performance that is evident in FIGURE 5 (bottom). Interestingly, for cell ID 2321, all the activations performed uniformly. Overall, ReLU surpassed other activation functions as evident in both of the figures and hence we choose ReLU for further experiments.

C. WEIGHT INITIALIZATIONS

We continue with our previous model configuration and the randomly chosen cell IDs, and initialize weights according to Common, Xavier, and He initialization methods (explained in details in [21]). We also set ReLU activation in hidden layers for this purpose, as discussed previously. FIGURE 6 exemplifies the impact of selecting various weight initialization schemes on DNN’s test accuracy. We can observe that He surpassed other initialization strategies and yielded highest average accuracy.
D. OPTIMIZATION TECHNIQUES

The superiority of mini-batch GD with momentum and ADAM over ordinary batch GD is clear in FIGURE 7. Although, in cell ID 4671, momentum has slightly better performance than ADAM but overall mini-batch GD with ADAM surpassed all other optimization techniques. It accomplished highest accuracy, recall, and $F_1$; and also, lowest error rate and FPR in most of the cells. Note, for cell ID 7816, ADAM achieved a perfect performance.

In Table 3, we report various performance measures of our anomaly detector, averaged over the results from randomly selected 1,000 cell IDs, along with the improvement we got by utilizing ADAM as compared with the momentum. As compared with our previous work [21] in which we utilized mini-batch GD with momentum for anomaly detection, we achieved significant performance improvements by utilizing mini-batch GD with ADAM in this paper.

E. TRAINING TIME

Another advantage of utilizing ADAM is faster training time that is evident in FIGURE 8 in which we compare the average training time of our model utilizing all the discussed optimization methods. Mini-batch GD with momentum consumes maximum training time, while ADAM deplete the lowest, and is the most suitable optimization method.

VI. CONCLUSION AND INSIGHTS FOR FUTURE WORK

Performance-wise, our MEC-based DL framework eclipsed the previous anomaly detection methods [1], [2], [6]. It can potentially improve network’s QoS and user’s QoE; and truncate OPEX for the network operators. Our proposed framework accomplished 0.44% FPR (Table 3), a significantly reduced value as compared with the reported 14% in [1]; and 98.8% accuracy, a great improvement as compared with the reported 94% accuracy in [2].

Our study endorses the concept of harnessing the largely untapped CDRs (using big data analytics) instead of utilizing traditional measurements and analytical approaches for the network analysis [1], [15]. Our research’s main innovation is the incorporation of the Internet activity feature (disregarded in previous works [1], [6]) that makes our research more robust as our DL framework can detect anomalies pertaining to a situation when Internet activity swiftly rises/declines but the call and SMS activities are normal. An example of such situation could be an abruptly increased Internet activity during a music festival inferring a necessity of additional network resource allotment. In addition, MEC-based approach relieves core network from heavy computation tasks, offloaded to various MEC servers spread across the network.
A deterrent in practical implementation of our deep learning approach is the requirement of deluge of examples to extract a meaningful pattern in the CDR data; however, utilizing larger dataset—the acquisition of which is another issue due to privacy concerns—can surmount the difficulty. We can then preprocess the dataset using more sophisticated software: Apache Hadoop or Spark [1]. Another restraint on fully employing our approach is the possession of labeled data due to the supervised nature of our algorithm; affixing fault data, generated at the core network and containing historical alarms’ logs [2], with CDRs and then labeling them accordingly can overcome this restraint.

The timestamp interval of 10 minutes is crucial for the results and hence more variation could be tested in the future studies to determine the impact of increasing the time duration granularity to perform more coarse-grained analysis, i.e. take three 10-min intervals instead of just one; or the granularity can also be decreased to perform more fine-grained analysis, i.e. by considering even smaller than a single 10-minute interval (the practical LTE network can be set to generate CDR dataset in such settings). Hence it will be an interesting future direction that could be explored. In this connection, our previous work considered [1] a 1-hour interval instead of 10 minutes—we combined six 10-minute timestamp activities—and detected anomalies in the 1-hour user activity data by using semi-supervised machine learning method. In the current research work, we however chose to decrease the interval so that the anomaly detection could be performed quickly and hence the remedial or diagnostic actions could be taken sooner.

Because of the potential of upcoming cellular networks to have an AI-empowerment, the implemented algorithms need to be quicker, increasingly proficient and less perplexing; future works can explore meliorative methods. We can also extend our study for anomaly detection in Internet of things (IoT) [39]; however, due to the limited resources (such as power consumption) the IoT devices might have entirely different activity pattern that will need more examination. With rising fame of DL technology, which has an enormous potential for utility in 5G networks, our work applies DL to accomplish substantial performance betterments for abnormality detection. This indicates reduction in OPEX for cellular operators along with an improvement in the network’s QoS and user’s QoE.

REFERENCES


VOLUME 7, 2019
B. Hussain et al.: MEC-Based Data-Driven Deep Learning Framework for Anomaly Detection
MUHAMMAD ALI IMRAN (M’03–SM’12) received the M.Sc. (Hons.) and Ph.D. degrees from Imperial College London, London, U.K., in 2002 and 2007, respectively. He is currently the Vice Dean of the Glasgow College, UESTC, and a Professor of communication systems with the School of Engineering, University of Glasgow. He is also an Affiliate Professor with the University of Oklahoma, Norman, OK, USA, and a Visiting Professor with the 5G Innovation Centre, University of Surrey, Guildford, U.K. He has more than 20 years of combined academic and industry experience, working primarily in the research areas of cellular communication systems. He has authored or coauthored more than 400 journals and conference publications and has been a Principal or Co-Principal Investigator on more than 10 million in sponsored research grants and contracts. He has supervised more than 40 successful Ph.D. graduates. He holds 15 patents. He is a Fellow of IET and a Senior Fellow of the Higher Education Academy (SFHEA), U.K. He was a recipient of the Award of Excellence in recognition of his academic achievements, conferred by the President of Pakistan, the IEEE ComSocs Fred Ellersick Award, in 2014, the FEPS Learning and Teaching Award, in 2014, and the Sentinel of Science Award, in 2016. He was twice nominated for the Tony Jeans Inspirational Teaching Award. He was a shortlisted finalist for The Wharton-QS Stars Awards, in 2014, the QS Stars Reimagine Education Award, in 2016, for innovative teaching, and the VCs Learning and Teaching Award at the University of Surrey.

* * *

VOLUME 7, 2019