A

Report

On

Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks and Federated Learning on Graphs

By

JAGAN MADDELA (23MCMT11)

1. OBJECTIVE

Elliptic data set is a transaction graph collected from the Bitcoin blockchain. A node in the graph represents a transaction; an edge can be viewed as a flow of Bitcoins between one transaction and the other. Through the Elliptic data set we are designed, implemented, and optimized graph conventional networks with a focus on enhancing their efficiency, scalability, and performance in processing and analyzing complex graph-structured data, thereby enabling more accurate and efficient solution to rectify the every transactional information. And further improved Federated Learning Technique Using Flower (flwr), known as a framework for building federated learning systems. Flower provides the infrastructure to do exactly that in an easy, scalable, and secure way. Flower presents a unified approach to federated learning, analytics, and evaluation. It allows the user to federate any workload, any ML framework, and any programming language.

2. DATASET

The Elliptic Data Set maps Bitcoin transactions to real entities belonging to licit categories versus illicit ones. The task on the dataset is to classify the illicit and licit nodes in the graph.

This anonymized data set is a transaction graph collected from the Bitcoin blockchain. A node in the graph represents a transaction; an edge can be viewed as a flow of Bitcoins between one transaction and the other. Each node has 166 features and has been labeled as being created by a "licit", "illicit" or "unknown" entity.

The graph is made of 203,769 nodes and 234,355 edges. Two percent (4,545) of the nodes are labelled class1 (illicit). Twenty-one percent (42,019) are labelled class2 (licit). The remaining transactions are not labelled with regard to licit versus illicit.

3. GCN MODEL

A Graph Convolutional Network, or GCN, is an approach for semi-supervised learning on graph-structured data. It is based on an efficient variant of convolutional neural networks which operate directly on graphs.

For this model, the key Functions are:

1. run_experiment()
2. display_learning_curves()
3. create_ffn()

The key Components for building of GCN Model are:

4. GraphConvLayer()
5. GNNNodeClassifier()

3.1 run_experiment()

The Function ‘run_experiment’ that takes a neural network model (‘model’), training data (‘x-train’ and ‘y-train’), and runs an experiment by compiling and training the model. The training process includes early stopping based on the validation accuracy.

Model Compilation:

- The model is compiled using the Adam optimizer with a specified learning rate.
- Sparse categorical crossentropy is used as the loss function, assuming the model's output is logits.
- The metric being monitored during training is sparse categorical accuracy.

Early Stopping Callback:

- An early stopping callback is created to monitor the validation accuracy (‘val_acc’).
- The patience parameter is set to 10, meaning training will stop if there is no improvement in validation accuracy for 10 consecutive epochs.
- ‘restore_best_weights=True’ ensures that the model's weights are restored to the ones that achieved the best performance on the validation set.

Model Training:

- The model is trained using the ‘fit’ method.
- Training data (‘x_train’ and ‘y_train’) are provided.
- The number of epochs, batch size, and a validation split of 15% are specified.
- The early stopping callback is included in the training process.

3.2 display_learning_curves()

The Function ‘display_learning_curves’ that takes a **history** object as input and plots the training and validation loss on one subplot and the training and validation accuracy on another subplot. This function relies on the matplotlib library for plotting.

3.3 create_ffn()

The Function ‘create_ffn’ that generates a feedforward neural network (FFN) using keras. This function takes 3 parameters:

1. **hidden_units:** A list specifying the number of units in each hidden layer.
2. **dropout_rate:** The dropout rate used in each dropout layer.
3. **name:** An optional name for the Sequential model.

The function creates a list fnn_layers containing BatchNormalization, Dropout, and Dense layers and then uses ‘keras.Sequential’ to create a feedforward neural network with the specified architecture.

- **i.** **fnn_layers.append(layers.BatchNormalization()) :** Adds a BatchNormalization layer to the list. Batch normalization is a technique used to improve the training stability and performance of neural networks.
- **ii.** **fnn_layers.append(layers.Dropout(dropout_rate)) :** Adds a Dropout layer to the list. Dropout is a regularization technique that helps prevent overfitting by randomly setting a fraction of input units to zero during training.
- **iii.** **fnn_layers.append(layers.Dense(units, activation=tf.nn.gelu)) :** Adds a Dense layer to the list. The Dense layer is a fully connected layer, and ‘tf.nn.gelu’ is used as the activation function. GELU (Gaussian Error Linear Unit) is an activation function that has been shown to perform well in neural networks.

The loop iterates over the ‘hidden_units’ list, adding the specified layers for each hidden unit.

Finally, the function returns a Sequential model created from the list of layers.

3.4 GraphConvLayer()

- This layer is designed to operate on graph-structured data, where nodes are connected by edges. The layer takes node representations, edges, and edge weights as inputs and produces updated node embeddings as outputs.
- The Functionalities used in GraphConvLayer() are:

3.4.1 Initialization

The layer is initialized with parameters such as hidden_units, dropout_rate, aggregation_type, combination_type, and normalizes.

- **‘hidden_units’:** A list specifying the number of hidden units for each layer in the feedforward neural network used in the graph convolution layer.

- **‘dropout_rate’:** The dropout rate applied to the feedforward neural network.
- **‘aggregation_type’:** Specifies the type of aggregation used for combining neighboring node features. It could be "mean" or another type based on the application.
- **‘combination_type’:** Specifies how the updated node features are combined. It could be "concat" or "gated" based on the application.
- ‘**normalize’:** A boolean indicating whether to normalize the aggregated features.

Feedforward Neural Network (FFN): The ‘ffn_prepare’ attribute is initialized using a function ‘create_ffn’, which is expected to create a feedforward neural network with the specified parameters (hidden units and dropout rate).

Combination Type: If ‘combination_type’ is "gated," a GRU (Gated Recurrent Unit) layer is used as the update function (‘update_fn’). If it's not "gated," a feedforward neural network is used as the update function

3.4.2 Prepare Function

Input:

- **‘node_representation’:** This is a tensor representing node representations with shape ‘[num_edges, embedding_dim]’. Each row in this tensor likely corresponds to the representation of a node in a graph.
- **‘weights’:** An optional tensor of weights with shape ‘[num_edges]’ that can be used to modulate the messages. If provided, the messages are element-wise multiplied by these weights

Feedforward Neural Network (FFN):

- The method applies the feedforward neural network (‘ffn_prepare’) to the input ‘node_representations’. This involves passing the node representations through a series of layers defined by the ‘create_ffn’ function. The result is stored in the ‘messages’ variable

Weights Modulation:

- If ‘weights’ provided (i.e., not ‘none’), the messages are element-wise multiplied by the weights. This step allows for the modulation or adjustment of the messages based on the provided weights

Output:

- The method returns the computed messages. The shape of the output tensor is the same as the input ‘node_representation’, i.e., ‘[num_edges, embedding_dim]’.

3.4.3 Aggregation Function

Input:

- **‘node_indices’:** A tensor with shape ‘[num_edges]’ representing the indices of nodes for which the messages need to be aggregated.
- **‘neighbour_messages’:** A tensor with shape ‘[num_edges, representation_dim]’ containing the messages from neighboring nodes

Number of Nodes:

- **‘num_nodes’** is computed as the maximum value in ‘node_indices’ plus 1. This assumes that the node indices are zero-based and consecutive. This value represents the total number of nodes in the graph

Aggregation Types:

- The method supports three types of aggregation: "sum," "mean," and "max." The appropriate aggregation operation is selected based on the value of ‘self_aggregation_type’.

Aggregation Operations:

- If ‘self.aggregation_type’ is "sum," the method uses ‘tf.math.unsorted_segment_sum’ to sum the neighbor messages for each node.
- If it's "mean," it uses ‘tf.math.unsorted_segment_mean’ to compute the mean of neighbor messages for each node.
- If it's "max," it uses ‘tf.math.unsorted_segment_max’ to find the maximum neighbor message for each node.

Error Handling:

- If an invalid aggregation type is provided, a ‘ValueError’ is raised

Output:

- The method returns the aggregated messages, where each row corresponds to the aggregated message for a specific node. The shape of the output tensor is ‘[num_edges, representation_dim]’.

3.4.4 Update Function

Inputs:

- **‘node_representation’:** A tensor with shape ‘[num_edges, representation_dim]’ representing the current node representations
- **‘aggregated_messages’** A tensor with the same shape ‘[num_edges, representation_dim]’ representing the aggregated messages from neighboring nodes

Combination Types:

- The method supports three types of combinations: "gru," "concat," and "add." The appropriate combination operation is selected based on the value of ‘self.combination_type’

Combination Operations:

- If ‘self.combination_type’ is "gru," the method creates a sequence of two elements (‘node_representation’ and ‘aggregated_messages’) along the second axis and stacks them using ‘tf.stack’.
- If it's "concat," it concatenates ‘node_representation’ and ‘aggregated_messages’ along the second axis using ‘tf.concat’.
- If it's "add," it adds ‘node_representation’ and ‘aggregated_messages’.

Processing Function:

- The combined tensor ’h’ is passed through the processing function ‘self.update_fn’. If the combination type is "gru," this function is expected to be a GRU layer.
- If the combination type is "gru," the final element of the sequence is extracted using ‘tf.unstack’.

Normalization:

- If ‘self.normalize’ is ‘True’, the resulting node embeddings are L2-normalized along the last axis using ‘tf.nn.l2.normalize’

Output:

- The method returns the updated node embeddings.

3.4.5 Call Function

‘call’ method is the main processing function of the GraphConvLayer class. It takes a tuple of three elements (‘node_representations’, ‘edges’, and ‘edge_weights’) as inputs and produces the node embeddings.

Inputs:

- **‘node_representations’:** A tensor with shape ’[num_nodes, representation_dim]’ representing the current node representations.
- **‘edges’:** A tuple containing two tensors (‘node_indices’ and ‘neighbour_indices’) with shape ‘[num_edges]’ representing the indices of source and target nodes for edges in the graph.
- **‘edge_weights’:** A tensor with shape ‘[num_edges]’ representing the weights associated with the edges.

Node and Neighbour Indices:

- Extract ‘node_indices’ and ‘neighbour_indices’ from the ‘edges’ tuple.

Neighbour Representations:

- Use ‘tf.gather’ to obtain the representations of neighbouring nodes (‘neighbour_representations’) based on the ‘neighbour_indices’.

Prepare Messages:

- Call the ‘prepare’ method to prepare messages from the neighbouring representations, considering the edge weights

Aggregate Messages:

- Call the ‘aggregate’ method to aggregate the prepared neighbour messages based on the specified aggregation type

Update Node Representations:

- Call the ‘update’ method to update the node representations based on the aggregated messages

Output:

- The method returns the updated node embeddings

3.5 GNNNodeClassifier()

3.5.1 Initialization

- **‘graph_info’:** Information about the graph, including node features, edges, and edge weights.
- **‘num_classes’:** Number of classes for node classification.
- **‘hidden_units’:** Number of hidden units in the neural network layers.
- **‘aggregation_type’:** Type of aggregation used in GraphConv layers (default is "sum").
- **‘Combination_type’:** Type of aggregation used in GraphConv layers (default is "concat").
- **‘dropout_rate’ :** Dropout rate for regularization (default is 0.2).
- **‘normalize’:** Boolean indicating whether to normalize edge weights (default is True).
- **‘*args. **kwargs’ :** Additional arguments and keyword arguments.

3.5.2 Attributes

- ‘node_features’, ‘edges’ and ‘edge_weights’ are extracted from ‘group_info’.
- If ‘edge_weights’ is not provided. It is set to ones.
- The ‘edge_weights’ are then scaled to sum to 1.

3.5.3 Layers

- **‘preprocess’:** A feedforward neural network (FFN) layer created using the ‘create_ffn’ function
- **‘conv1’** and **‘conv2’:** Two instances of the GraphConvLayer class, presumably implementing graph convolutional operations.
- **‘postprocess’:** Another FFN layer for post-processing.
- **‘compute_logits’:** A dense layer to compute the final logits, with the number of units equal to ‘num_classes’.

3.5.4 ‘call’ Method

1. **Preprocess Node Features:**
    - ‘x’ is the result of preprocessing the ‘node_features’ using the ‘preprocess’ layer.
2. **First Graph Convolutional Layer(‘conv1’):**
    - ‘x1’ is the result of applying the first graph convolutional layer (‘conv1’) to the preprocessed node features.
    - A skip connection is implemented by adding ‘x’ to ‘x1’.
3. **Second Graph Convolutional Layer(‘conv2’):**
    - ‘x2’ is the result of applying the second graph convolutional layer (‘conv2’) to the output of the first layer plus the original node features.
    - A skip connection is implemented by adding ‘x’ to ‘x2’.
4. **Postprocess Node Embeddings:**
    - The result, ‘x’, is then passed through the ‘postprocess’ layer for post-processing.
5. **Node Embeddings for Input Node Indices:**
    - Node embeddings for the specified ‘input_node_indices’ are extracted using ‘tf.gather’ on the processed ‘x’.
6. **Compute Logits:**
    - The final step involves passing the node embeddings through the ‘compute_logits’ layer to compute the logits.

- This ‘call’ method essentially performs a series of graph convolutional operations with skip connections, followed by post-processing, and finally, computes logits for the specified nodes. It's a standard forward pass for a graph neural network for node classification. When using this model, you would typically call this method with input node indices to obtain the logits for those nodes.

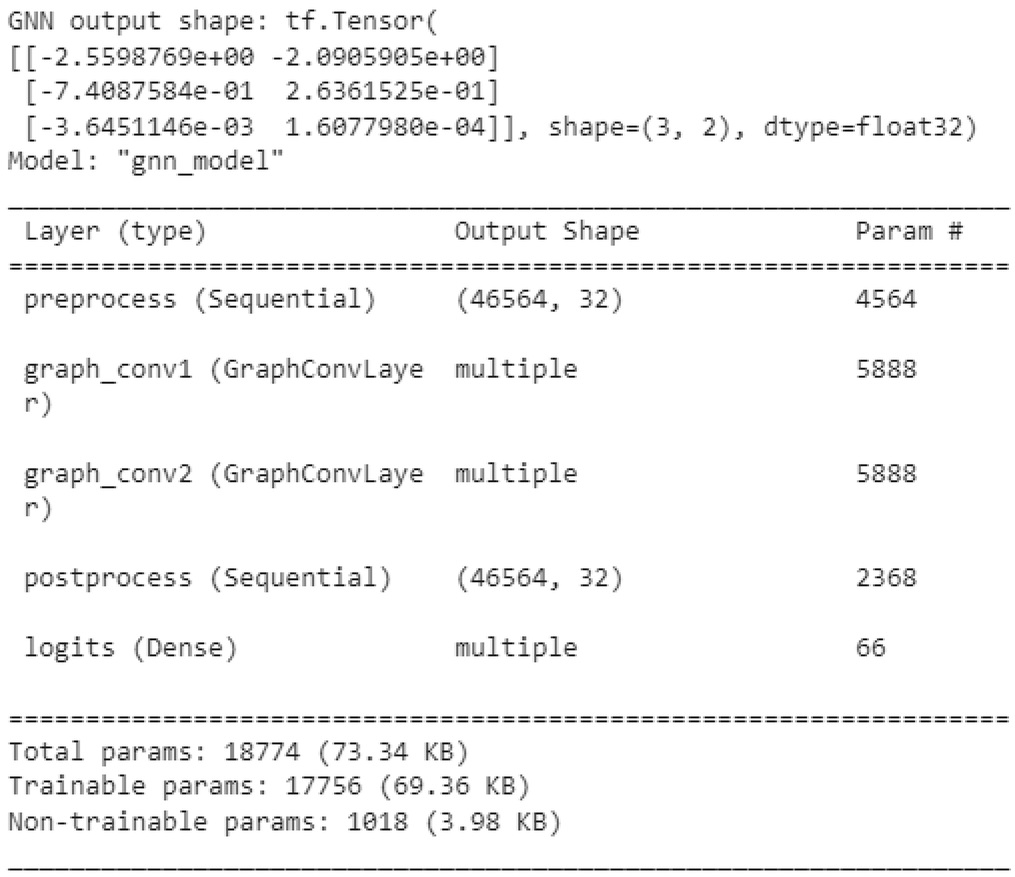
3.6 HyperParameters

No of classes are classified into 2 classes.

- **‘hidden_units’:** A list specifying the number of hidden units in each hidden layer of your neural network. In your case, there are two hidden layers, each with 32 units.
- **‘learning_rate’:** The learning rate determines the size of the steps taken during the optimization process. A higher learning rate may lead to faster convergence, but it could overshoot the optimal values [0.007].

- **'dropout_rate':** Dropout is a regularization technique where randomly selected neurons are ignored during training. It helps prevent overfitting. Here, you've set the dropout rate to 0.6, meaning 60% of the neurons will be dropped out during training.
- **'num_epochs':** The number of times the entire dataset is passed forward and backward through the neural network. It's a hyperparameter that needs to be tuned based on the specific problem [30].
- **'Batch_size':** The number of training examples utilized in one iteration. A smaller batch size can lead to a more accurate model, but it requires more time to process each epoch [256].

4. MODEL SUMMARY



```
GNN output shape: tf.Tensor(
[[-2.5598769e+00 -2.0905905e+00]
 [-7.4087584e-01  2.6361525e-01]
 [-3.6451146e-03  1.6077980e-04]], shape=(3, 2), dtype=float32)
Model: "gnn_model"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 preprocess (Sequential)     (46564, 32)               4564

 graph_conv1 (GraphConvLaye  multiple                  5888
 r)

 graph_conv2 (GraphConvLaye  multiple                  5888
 r)

 postprocess (Sequential)    (46564, 32)               2368

 logits (Dense)              multiple                  66

=================================================================
Total params: 18774 (73.34 KB)
Trainable params: 17756 (69.36 KB)
Non-trainable params: 1018 (3.98 KB)
_________________________________________________________________
```

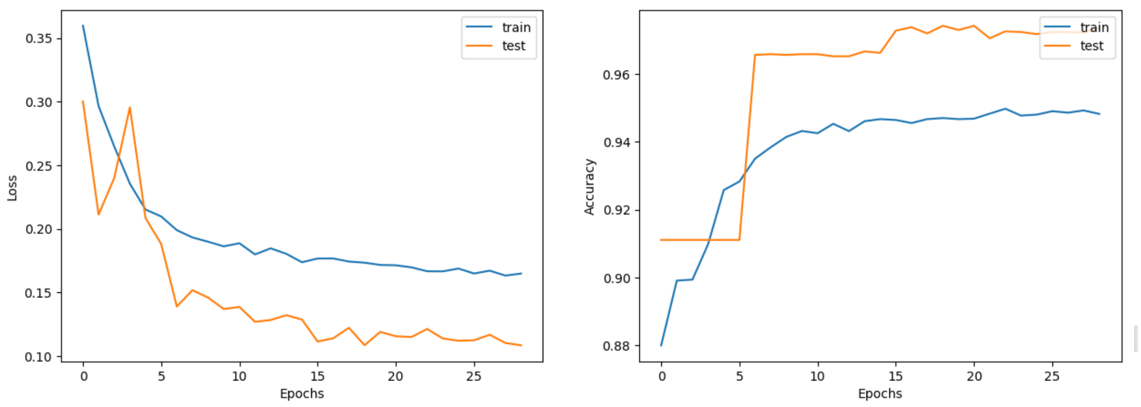
5. TRAIN THE MODEL

- **'x'** is a DataFrame containing the features. It seems to include columns specified in 'tx_features' and the 'txId' column.
- **'y'** is a Series containing the target variable ('class'). The lambda function is used to convert class labels '2' to 0 and all other labels to 1.

- **'train_test_split'** is then used to split the data into training and testing sets. **'test_size=0.3'** indicates that 30% of the data will be used for testing, and **'random_state=117'** ensures reproducibility.
- **'x_train':** Training features; **'x_test':** Testing features; **'y_train':** Training labels; **'y_test':** Testing labels.

```
x_train = X_train.txId.to_numpy()
history = run_experiment(gnn_model, x_train, y_train)
```

```
[23] display_learning_curves(history)
```



- Here the run_experiment takes the GNN model, input features (**'x_train'**), and target labels (**'y_train'**) to perform the training.
- The Left fig. shows the loss of train and test of model.
- The Right fig. shows accuracy of train and test of the model.

6. TEST RESULTS

- Accuracy : 97.19%

```
[24] x_test = X_test.txId.to_numpy()
     _, test_accuracy = gnn_model.evaluate(x=x_test, y=y_test, verbose=0)
     print(f"Test accuracy: {round(test_accuracy * 100, 2)}%")

     Test accuracy: 97.19%
```

- The Precision, Recall, F1 Score and Micro-Average F1 Score values:

```
Convoluted neural network
Precision:0.945
Recall:0.745
F1 Score:0.833
Micro-Average F1 Score: 0.9718682891911239
```