

BGP Route Anomaly Detection using Fisher-Markov Feature Selection and LSTM Networks

Ajaya Maharjan

Department of Graduate Studies
Nepal College of Information Technology
(Affiliated to Pokhara University)
Lalitpur, Nepal
mrjaj@gmail.com

Nirdosh Adhikari

Department of Graduate Studies
Nepal College of Information Technology
(Affiliated to Pokhara University)
Lalitpur, Nepal
nirdosh@ncit.edu.np

Shashidhar Ram Joshi

Department of Electronics and Computer,
IoE, Pulchowk
Tribhuvan University
Lalitpur, Nepal
srjoshi@ioe.edu.np

Abstract— According to Statistica.com 4.53 billion about 58.8% of total population of the world are connected to the internet and user of internet. And it is increasing at the rate of 1157%. The Internet is a decentralized global network comprised of tens of thousands of Autonomous System. The Border Gateway Protocol is the internet's default interdomain routing protocol that manages connectivity among Autonomous Systems. Border Gateway Protocol has been the defacto interdomain routing protocol since it was introduced and it is the destination based routing nature. Anomaly Detection of BGP traffic is significantly important in improving both security and robustness of the Internet. The objective of this paper is to work on two factor detection and prevention of the anomaly of the Border Gateway Protocol Route using the Deep learning Long Short Term Memory Technique. We developed the model that would classify the anomaly prefix hijack from the Dataset of Border Gateway Protocol Route.

Keywords—Border Gateway protocol, Broader Gateway Protocol Anomaly, Deep Learning, Long Short Term Memory, Broader Gateway Protocol Route

I. INTRODUCTION

BGP exchange routing information and reachability with different edges router with different Autonomous system. BGP is similar to the postal office transferring the letter in the sense that the BGP transfer the packet from source to destination like postal service. Growth of Internet is interconnection with several thousands of Autonomous System (ASes). Network are commonly belongs to the domain of Ases, on which it hold the whole prefix of the router and under controlled with one administrative individual. Routing protocol on the internet among different networks belongs to the BGP protocol only[1]. It comprises of at least one organization that have uniform directing strategies of routing while working autonomously. Web tasks, for example, network and information parcel conveyance are worked with by different Ases.

On a large ISP (Internet Service Provider) and NSP (Network Service Provider) network, BGP is mostly used protocol. Where peering establishing between the router interchange the router information and reachability information between the Autonomous System. Many large network services provider may have one or more autonomous system. BGP is a best dynamic protocol and the version 4 of BGP routing protocol supports a Class less inter domain routing CIDR and IPV6 . BGP relies on 3 way handshaking and which only done with the TCP connection port 179 for maintaining the neighbor relation with the peer boarder router.

BGP protocol is build trust, it consist of AS which should announced just IP prefixes it claims and authorized route to destinations. Still, there are vitriolic ASes can grap benefits of this trust system by announcing others IP prefix or through mould the AS Paths[2]. The four different types of anomalous BGP update which are Multiple-Origin AS (MOAS) conflicts, typos, prepending mistake and Origin change. Hijacking of the BGP route is the problem on the global internet for more than 20 years[3], which is happening frequently with routing incidents. The routing incident 4,739 has been reveal by BGPmon in 2018, which is a globally accepted monitoring service[4]

II. RELATED WORK

Philip Branch, Bahaa Al-Musawi and Grenville Armitage discuss different tools for capabilities of detecting BGP anomalies and key requirements for the next generation of anomaly detection of BGP routes and also presented many system for the real-time detection which will have the ability of detection of different BGP anomalies type. [1]

System. Many large network services provider may have one or more autonomous system. BGP is a best dynamic protocol and the version 4 of BGP routing protocol supports a Class less inter domain routing CIDR and IPV6 . BGP relies on 3 way handshaking and which only done with the TCP connection port 179 for maintaining the neighbor relation with the peer boarder router.

BGP protocol is build trust, it consist of AS which should announced just IP prefixes it claims and authorized route to destinations. Still, there are vitriolic ASes can grap benefits of this trust system by announcing others IP prefix or through mould the AS Paths[2]. The four different types of anomalous BGP update which are Multiple-Origin AS (MOAS) conflicts, typos, prepending mistake and Origin change. Hijacking of the BGP route is the problem on the global internet for more than 20 years[3], which is happening frequently with routing incidents. The routing incident 4,739 has been reveal by BGPmon in 2018, which is a globally accepted monitoring service[4]

Hongbo Zhou, Qiang Cheng and Jie Cheng has implemented "The Fisher-Markov selector algorithm for which fast selecting maximally separable feature subset for the multiclass classification with application to high-dimensional data". A new feature selector of class is planned in the soul of fisher's class partition model of minimizing within-class variations and maximizing between-class separability. The FMS algorithm could be implemented to

general data which has numerous class arbitray dimensions and the chosen feature subset is valuable for general classifiers and the experiment results has better effectiveness of Fisher-Markov Selector Algorithm. [2]

Hua Tian, Mingxia Liu, Yilin Bei, Deyun Yang and Yingkun Hou on “New Algorithm for texture classification based on Fisher-Markov selector” LIBSVM is used as classifier with a RBF kernel by performing an exhaustive grid search using the range from -10 to 10 at a step size of 1.[3]

Slobodan Obradovic, Marijana Cosovic and Emina Junuz “Deep Learning for Detection of BGP Anomalies” design a system of identification of anomaly in light of artificial neural networks with two hidden layers by using the cross validation for determining the neurons required for each layers. And concluded emplotiing AS-Path and volume features through update messages of BGP can prompt legitimate order of RTL occasions. [4]

Wenjuan Wang, Na Wang and Xianbo Dai “Application of machine learning in BGP anomaly detection” abstract the classification of anomalies detection proposed a super vector machine-based BGP anomalies identification process for the binary classification and found the F1 score 95.03% with the accuracy of 91.36%. [5]

Zhiliang Wang along xingang shi, Yan Yang, Xia Yin “The Power of Prefix Hijacking in Internet Hierarchy” deployed the model with RPKI on both location and degree. As for the greater attacking/ protecting strength of Ases in each layer there should be more layers. [6]

Ljiljana Trajkovic ,Guangyu Xu, Zhida Li and Ana Laura Gonzalez Rios, and “Machine Learning Techniques for classifying Anomalies and Intrusions” GRU and LSTM deep neural network with variable number of hidden layers, expanding the feature which is planned highlights and upgrade of node led to good performance. [7]

Ali Jahanshahi, Hadi Zamani Sabzi, Abbas Mazloumi and Mohsen Karimi, “Border Gateway Protocol Anomaly Detection Using Neural Network” classification of the three data set of different worms attacks previously using the 8 feature based of update message of BGP. [8]

Ricardo Bennesby, Edjard to S. Mota, Paulo Fonseca “BGP Dataset Generation and Feature Extraction for Anomaly Detection” discuss regarding the extraction of BGP data set from the Raw BGP update message time series on BGP feature. [9]

Tao Wan, P.C. Van Oorschot Evangelos Kranakis “Asekeive Introduction to Border Protocol (BGP) Security Issues” discuss regarding the centralize record for the IP prefix ownership record. [10]

Mengying Xu, Xing Li “BGP Anomaly Detection Based on Automatic Feature Extraction by Neural Network” automatically extracts the feature of BGP by using the neural network by implementing with Real BGP data and performed the promising. [11]

R. Hakimi and M. J. Reed “Deep Learning-based stock price prediction using LSTM and Bi-Directional LSTM Model” concluded that on stock prediction it has high accuracy than regression method, by adjusting the different parameter. [12]

For the efficient classification the multiple numbers of features that need to be subset for which Fisher-Markov selector has been used for the feature selection of the BGP

feature[5]. It selects the features that are most useful for the classification of the anomalies of BGP route. The feature selection and classification both is independent to each other. The Fisher-Markov selector algorithm selects the feature by weighting of the dimension for ability to distinguish the categories. It has low computational intricacy for the huge-scale information and also ensures the global optimization. The important index of the each 37 features has been found out accordingly and the highest important index among the 37 feature for which 10 feature has been selected for the prefix hijack classification. And the classification for the prefix hijack is quite similar and satisfied with the 37 features.

The 37 feature which has been collected are not necessary important feature for the classification of anomaly and regular data. For which the FMS algorithm[6] is used to find out the most important feature among the 37 features.

Classification of anomaly of BGP using LSTM design. In the deep learning field an artificial recurrent neural network design refers to LSTM. In 1997 Sepp Hochreiter and Jurgen Schmidhuber proposed this algorithm[7]. LSTM manages the detonation and vanishing gradient issue which early comes in RNN. The LSTM block contains cells, inputs gate, output gate and output gate. The cell recollects values throughout self-assertive time stretches and the three gates direct the progression of information all through cell. While moving to LSTM from RNN we are introducing more and more controlling knobs, due to which the control ability and better Result is expected. On the other hand more complexity and Operating cost will also arise. It accomplishes the universal superlative of the class distinguishable standard without attachment of the unwanted noise parts

A. Fisher Markov Selector algorithm

For the efficient classification the multiple numbers of features that need to be subset for which Fisher-Markov selector has been used for the feature selection of the BGP feature[5]. It selects the features that are most useful for the classification of the anomalies of BGP route.

Algorithm 1: Feature Selection Using FMS

Input:

$X = [x_1, x_2, \dots, x_n] \in \mathbb{R}^{p \times n}$

$Y = [y_1, y_2, \dots, y_n], y_k \in \{w_1, w_2, \dots, w_g\}$

β, γ

Output:

$\alpha^* = [\alpha_1^*, \alpha_2^*, \dots, \alpha_p^*] \in \{0,1\}^p$

1: **BEGIN**

2: **FOR** $j \leftarrow 1$ **TO** p **DO**

3: $\theta_j \leftarrow (1/n) \sum_{i=1}^n \lg [(1/n_i) (\sum_{v=1}^{n_i} x_{j,v})^2]$

4: **IF** $\theta_j > \beta$ **THEN**

5: $\alpha_j^* \leftarrow 1$

6: **ELSE**

7: $\alpha_j^* \leftarrow 0$

8: **END IF**

9: **END FOR**

10: **RETURN** α^*

11: **END**

The feature selection and classification both is independent to each other. The Fisher-Markov selector algorithm selects the feature by weighting of the dimension for ability to distinguish the categories. It has low computational intricacy for the huge-scale information and also ensures the global optimization. The important index of

the each 37 features has been found out accordingly and the highest important index among the 37 feature for which 10 feature has been selected for the prefix hijack classification. And the classification for the prefix hijack is quite similar and satisfied with the 37 features.

The 37 feature which has been collected are not necessary important feature for the classification of anomaly and regular data. For which the FMS algorithm[6] is used to find out the most important feature among the 37 feature.

Kyryk et al. used SHAP to examine which BGP features matter most to an LSTM anomaly detection model. Their analysis shows how individual features contribute to detecting different types of anomalies. This supports the importance of choosing relevant features before training an LSTM model for BGP anomaly detection.[13]

Muosa and Ali [14] developed an LSTM-based auto encoder to identify anomalies in BGP updates. By learning patterns of normal routing activity, the model detects updates that deviate from those patterns. Their study shows how LSTM can capture changes in routing behavior over time.

Scott et al. analyzed BGP activity as a time series and used Matrix Profile to identify unusual routing patterns. Their method detected anomalies in publicly available BGP data without needing a training dataset. The study offers an alternative approach to assessing routing anomalies alongside LSTM-based methods.[15]

B. Long Short Term Memory

Classification of anomaly of BGP using LSTM design. In the deep learning field an artificial recurrent neural network design refers to LSTM. In 1997 Sepp Hochreiter and Jurgen Schmidhuber proposed this algorithm[7]. LSTM manages the detonation and vanishing gradient issue which early comes in RNN. The LSTM block contains cells, inputs gate, output gate and output gate. The cell recollects values throughout self-assertive time stretches and the three gates direct the progression of information all through cell. While moving to LSTM from RNN we are introducing more and more controlling knobs, due to which the control ability and better Result is expected. On the other hand more complexity and Operating cost will also arise. It accomplishes the universal superlative of the class distinguishable standard without attachment of the unwanted noise parts.

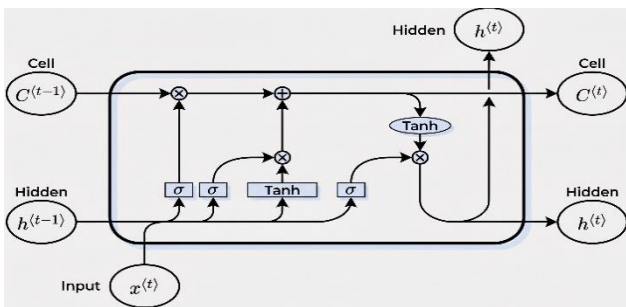


Fig. 1. LSTM Model adapted from [16]

Input given to the LSTM upgrades are as follows:

$$\phi_{\tau} = \hat{f}(\Omega_{\phi} \bullet [\eta_{\tau-1}], \xi_{\tau}) + \beta_{\phi} \quad (1)$$

$$\iota_{\tau} = \hat{f}(\Omega_{\iota} \bullet [\eta_{\tau-1}], \xi_{\tau}) + \beta_{\iota} \quad (2)$$

$$X_{\tau} = \tau \alpha \nu \eta (\Omega_X \bullet [\eta_{\tau-1}], \xi_{\tau}) + \beta_X \quad (3)$$

$$X_{\tau} = \phi_{\tau} * X_{\tau-1} + \iota_{\tau} * X_{\tau} \quad (4)$$

$$o_{\tau} = \hat{f}(\Omega_o [\eta_{\tau-1}], \xi_{\tau}) + \beta_o \quad (5)$$

$$\eta_{\tau} = o_{\tau} * \tau \alpha \nu \eta (X_{\tau}) \quad (6)$$

The three main steps in LSTM are given below: -

First, decide what from the previous cell state is worth memorizing, and advise the cell state to forget the stuff, which is decided as irrelevant. Second, selectively update the cell state dependent on the new input, which is simply observed. Third, selectively decide what part of the cell state yield as the new hidden state

III. METHODOLOGY

A. System model

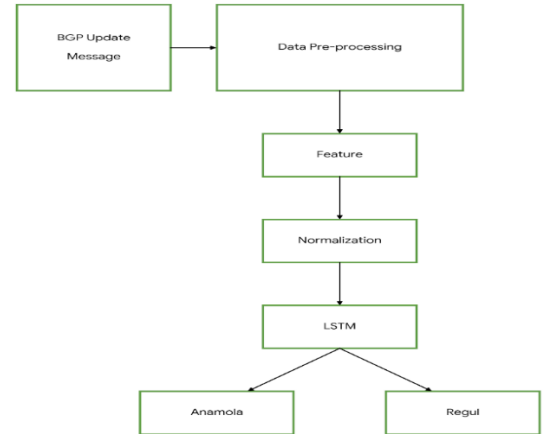


Fig. 2. System Model

The detailed procedure for the proposed model are: -

1. The BGP update Messaged which consist of the information of the BGP route is converted to stational format.
2. The 37 Feature has been Extracted from the BGP Update Message which is formatted in CSV design
3. The selection of features from 37 features Fisher-Markov Selector Algorithm is implemented.
4. Ratio of 70:30 partitions is maintained for training and test dataset.
5. Normalizing the dataset.
6. Hyper-boundaries (epoc,neurons etc) are identified
7. Trained the model.
8. Finally Testing and Classification is done.

The system model is described briefly in the following sections:

1) Data Collection

The data is collected from the Ripe.net[8]. The data are collected in the form of MRT which is the form of compressed data. The BGP data was collected of AS 12654, the data is

collected route updates announced by CIXP member, Geneva [20]. The data which has been collected was from the incident of prefix hijacking about 5 day, 2days before the incident and 2 days after the incident. The data was collected on the incident of prefix hijack by the Pakistan Telecom on 2008 February 24.

2) Data Processing

For the anomaly detection of the BGP route, extracting data from Raw BGP Data is done[9]. The extraction of MRT data with the help of *mrtparse* tool which is written in python code[10], with the help of *mrtparse* we converted the MRT format into the ASCII format. The ASCII format data are again converted into the static format by using the code which is written in Python. In the other hand zebra tool is also used to extract the static base data from the ASCII format. The data was collected in the interval of one minute, for which 7200 data was collected within the 5 days interval.

3) Fisher Markov Selector

The important index of the each 37 features has been found out accordingly and the highest important index among the 37 feature for which 10 feature has been selected for the prefix hijack classification. And the classification for the prefix hijack is quite similar and satisfied with the 37 features.

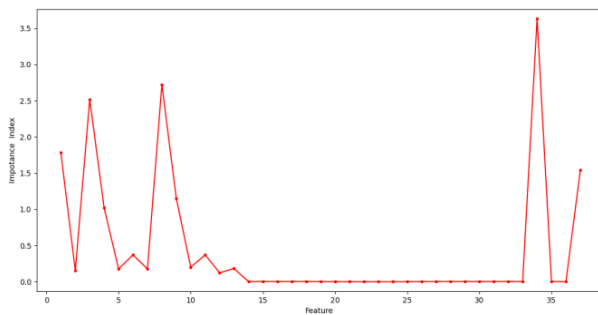


Fig. 3. Importance Index of Feature

1) Data Normalization

Min Max Algorithm is chosen for data normalization process to tune the datasets with the intension to bring the values with in the same range i.e. 0 to 1, although they held different units and ranges.

2) Design of the LSTM

The planned of the LSTM model was done with 37 inputs on the other hands there is 1 output nodes which contains numerous of neurons equal 50 with number of epochs with 1000 during this research and similarly while using the Fisher-Markov Selector Algorithm we use 10 feature inputs and 1 outputs node containing number of neuron equal 50 with number of epochs with 1000. Adam optimizer is used for the LSTM.

3) Dataset

The Dataset for the training and for the testing purpose is done on the ratio 70:30 on which the data for the training is 70 percentages and on other hand data for testing and validation of the proposed Model is 30 percentages.

TABLE I. DATASET FOR THE PROPOSED MODEL

Dataset	Regular	Anomaly
Prefix-Hijack	6200	1000

4) Training of the LSTM Model.

LSTM Network is set with samples of training data. Neural Network consists of 37 feature of BGP route, and while using the Fisher-Markov Selector Algorithm 10 feature has been taken. So Input parameter taken is 37 and 10, for the model LSTM and FMSLSTM respectively. Bias and weights are calibrated according to the difference in the predicted and expected result in the output layer.

5) Testing and Prediction

Testing is done form the data set with and without FMS by various epochs setting. The model has been trained and with the trained pattern prediction has been made accordingly

6) Performance Analysis

Performance analysis of the model design is done with the help of confusion matrix by planning the output of the system. Accuracy, precision, F-Score, specificity, specification has been analysis for the performance analysis of the proposed model

IV. RESULT AND DISCUSSION

The BGP route data was downloaded from the Ripe.net. It collects the BGP route of different country specific router for the further research analysis for future. The data was collected on the 2008 Month of February from 22 to 26 of 5 days interval. The data is downloaded in the MRT format, for which the data is converted to ASCII format with the help of Mrtparse.

All 37 features, which are extracted, are shown in Table II.

TABLE II. BGP ROUTE DATA

Feature extraction. Feature	Definition	Category
1	Number of Announcements	Volume
2	Number of Withdrawals	Volume
3	Number of Announced NLRI Prefixes	Volume
4	Number of Withdrawn NLRI Prefixes	Volume
5	Average AS-PATH length	AS-Path
6	Maximum AS-PATH length	AS-Path
7	Average Unique AS-PATH length	Volume
8	Number of Duplicate Announcements	Volume
9	Number of Duplicate Withdrawals	Volume
10	Number of Implicit Withdrawals	Volume
11	Average Edit Distance	AS-Path
12	Maximum Edit Distance	AS-Path
13	Inter-arrival time	Volume
14-24	Maximum Edit Distance = n, where n = (7, ..., 17)	AS-Path
25-33	Maximum AS-path length = n, where n = (7,...,16)	AS-Path
34	Number of IGP Packets	Volume
35	Number of EGP Packets	Volume
36	Number of Incomplete Packets	Volume
37	Packet size (B)	Volume

A. Visualization of Data of Update Message of BGP Route

The Data distribution of various feature of BGP Route are shown in Fig. 4.

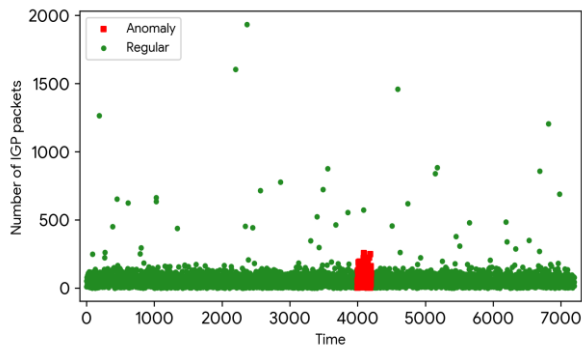


Fig. 4. Data distribution of various feature of BGP Route

B. Comparison of Model with LSTM and FMSLSTM

Performance measure of the Model is observed with the 37 feature and using the fisher markov selector algorithm on which we select the 10 feature and apply the LSTM for classification using 1000 epoch.

TABLE III. LSTM FOR CLASSIFICATION USING 1000 EPOCH

Measure	Accur acy	Sensit ivity	Specif icity	Preci sion	F1 Score
37-Feature LSTM	93.61	93.42	94.22	98.08	95.69
10-Feature with FMSLSTM	95.37	86.87	96.23	77.48	65.28

C. Loss and Accuracy of the Model

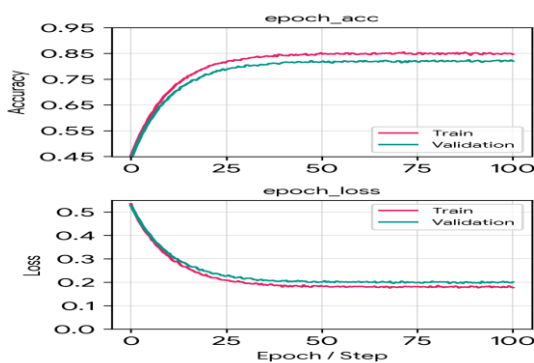


Fig. 5. Loss and Accuracy

The Loss and accuracy of the model during the training and testing phase has been observed as shown in figure below.

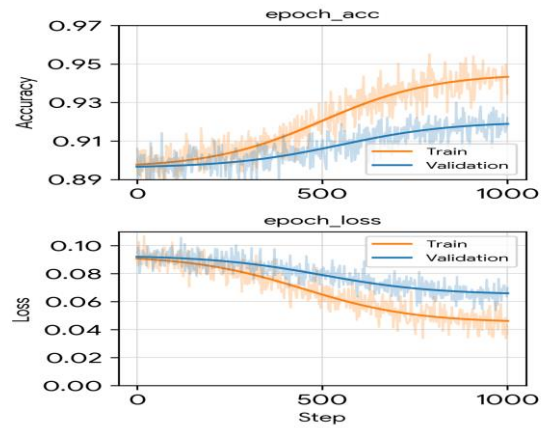


Fig. 6. Epoch loss and Epoch accuracy of the LSTM

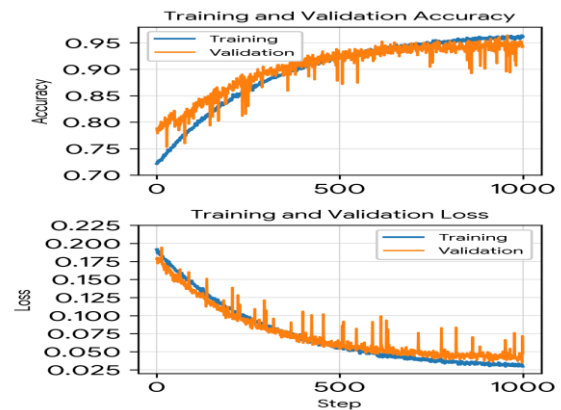


Fig. 7. Epoch loss and Epoch accuracy of the FMS-LSTM with 10 features

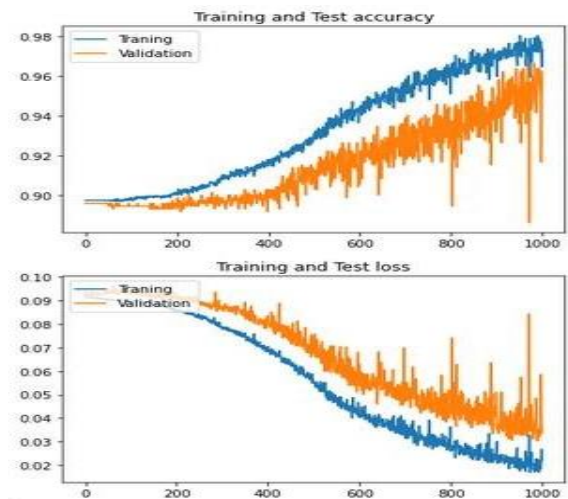


Fig. 8. Training vs. validation for the accuracy and loss of 32 feature LSTM Model

D. Visualization of Actual and Predicted Value

Comparison of Visualization of Actual and Predicted value of two model are as follows

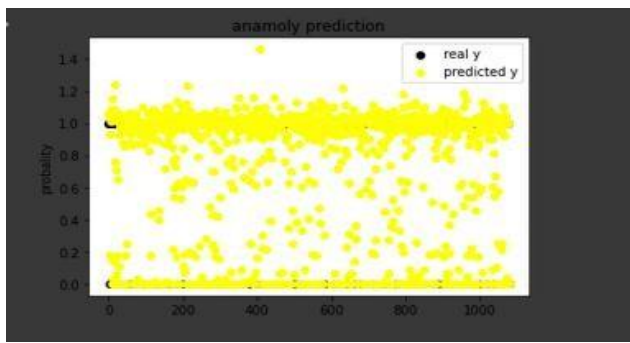


Fig. 9. Real and predicted Value scatter plot along with 32 feature of LSTM

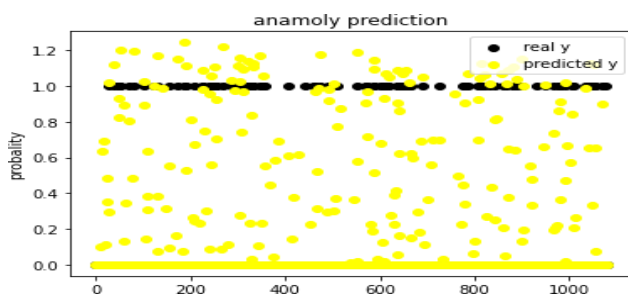


Fig. 10. Real and predicted Value scatter plot of FMSLSTM

E. ROC(Receiver Operating Characteristics) Curve

A receiver operating characteristic curve is a graphical plot that illustrates the ability of binary classifier system to diagnose as tis discrimination threshold is varied

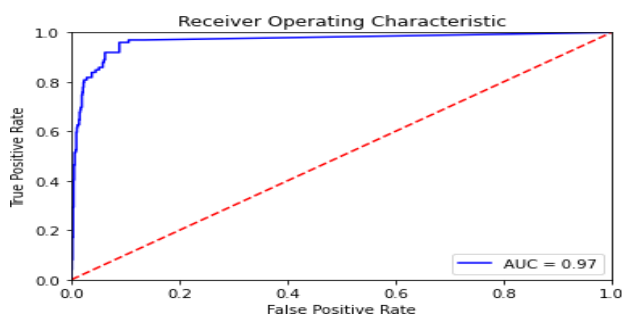


Fig. 11. ROC for LSTM with 37 features

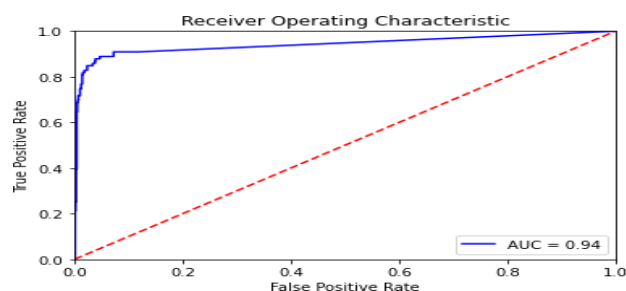


Fig. 12. ROC for the Fisher-Markov Selector LSTM with 10 features

V. CONCLUSION AND FURTHER WORK

The Prefix hijacking incident is occurring due to the intentionally or unintentionally/mistaken till this date which cause a lots of economic and social aspect impact has happened. I have conducted the experiments on my research using the datasets on which the actual incident has happened and which cause the globally outage of YouTube traffic due to some certain configuration change at the router of country Pakistan. Datasets has been collected from the Ripe.net which had stored the update message as dump with MRT format. The 37 feature has been extracted with the help of BGP update messages and then apply the LSTM for the binary classification for which the accuracy of the model appears to be 93.80 percentages on 1000 epoch.

Similarly while using the Fisher-Markov selector algorithm along with LSTM as a binary classification the accuracy for the model is 95.37 percentages observed during the process, which show that the feature selector which we have implemented is very good and it is effectiveness is observed for the prefix hijack classification.

The better results have been occurred at the 1000 epoch for analyze and processing the big data of BGP. As we have almost 7200 data for each feature of BGP update message. For which from the experiment 10 feature, this is sufficient for the prefix hijacking classification. The model which has been proposed with the fisher-markov selector and LSTM is found to be superiority from the performance measures and curve shown above.

Anomaly detection for the BGP route is ongoing process for which we can implement the other application for increasing the better accuracy with the less time consuming model. After the development of a BGP Prefix hijack classification, could find out the detection and root cause analyzer, another layer of automation could be added to the mechanism by creating and adding and avoiding the Prefix hijack incident. The classification of anomaly detection could be proceeding on the real time scenario with the traffic flow on the global internet.

REFERENCES

- [1] B. Al-Musawi, P. Branch, and G. Armitage, "BGP anomaly detection techniques: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 377–396, 2017, doi: 10.1109/COMST.2016.2622240.
- [2] S. Goldberg, M. Schapira, P. Hummon, and J. Rexford, "How secure are secure interdomain routing protocols?," *Comput. Networks*, vol. 70, pp. 260–287, 2014, doi: 10.1016/j.comnet.2014.05.007.
- [3] S. Cho, R. Fontugne, K. Cho, A. Dainotti, and P. Gill, "BGP hijacking classification," *TMA 2019 - Proc. 3rd Netw. Traffic Meas. Anal. Conf.*, pp. 25–32, 2019, doi: 10.23919/TMA.2019.8784511.
- [4] "Routing Security-getting better, but no reason to rest." [Online]. Available: <https://www.manrs.org/2019/02/routing-security-getting-better-but-no-reason-to-rest/>.
- [5] C. Blog, "Understanding LSTM Networks." [Online]. Available: <http://colah.github.io/posts/2015-08-Understanding-LSTMs>.
- [6] P. SRIVASTAVA, "Essentials of Deep Learning: Introduction to Long Short Term Memory." [Online]. Available: <https://www.analyticsvidhya.com/blog/2017/12/fundamentals-of-deep-learning-introduction-to-lstm>.
- [7] D. L. Fay, "What Does Artificial Neural Network," *Angewandte Chemie International Edition*, 6(11), 951–952.
- [8] 1967, [Online]. Available: <https://www.techopedia.com/definition/5967/artificial-neural-network-ann>.
- [9] J. Shamsi, A. Amirsoleimani, S. Mirzakuchaki, A. Ahmade, S. Alirezaee, and M. Ahmadi, "Hyperbolic tangent passive resistive-type

- neuron,” *Proc. - IEEE Int. Symp. Circuits Syst.*, vol. 2015-July, pp. 581–584, 2015, doi: 10.1109/ISCAS.2015.7168700.
- [10] D. Blazakis, M. Karir, and J. S. Baras, “BGP-inspect - Extracting information from raw BGP data,” *IEEE Symp. Rec. Netw. Oper. Manag. Symp.*, no. May, pp. 174–185, 2006, doi: 10.1109/noms.2006.1687549.
- [11] M. A. Romo-Chavero, G. de los Ríos Alatorre, J. A. Cantoral-Ceballos, J. A. Pérez-Díaz, and C. Martínez-Cagnazzo, “A hybrid model for BGP anomaly detection using median absolute deviation and machine learning,” *IEEE Open J. Commun. Soc.*, vol. 6, pp. 2102–2116, 2025, doi: 10.1109/OJCOMS.2025.3550010.
- [12] R. Hakimi and M. J. Reed, “Feature analysis and selection for BGP anomaly detection,” in *Proc. 28th Conf. Innovation in Clouds, Internet and Networks (ICIN)*, 2025, pp. 99–106, doi: 10.1109/ICIN64016.2025.10942841.
- [13] M. Kyryk, S. Maruniak, and T. Andrukhiv, “SHAP-based evaluation of feature importance in BGP anomaly detection models,” *Information and Communication Technologies, Electronic Engineering*, vol. 5, no. 1, pp. 34–43, 2025, doi: 10.23939/ictee2025.01.034
- [14] A. H. Muosa and A. H. Ali, “Internet routing anomaly detection using LSTM based autoencoder,” in *Proc. Int. Conf. Computer Science and Software Engineering (CSASE)*, 2022, pp. 319–324, doi: 10.1109/CSASE51777.2022.9759613.
- [15] B. A. Scott, M. N. Johnstone, P. Szewczyk, and S. Richardson, “Matrix profile data mining for BGP anomaly detection,” *Computer Networks*, vol. 242, Art. no. 110257, 2024, doi: 10.1016/j.comnet.2024.110257.
- [16] C. Olah, “Understanding LSTM Networks,” Aug. 27, 2015. [Online]. Available: colah.github.io, Understanding LSTM Networks. [Accessed: Sep. 24, 202