DOI: 10.15849/IJASCA.230320.02

Int. J. Advance Soft Compu. Appl, Vol. 15, No. 1, March 2023
Print ISSN: 2710-1274, Online ISSN: 2074-8523

Machine Learning based Anomaly Detection for High Dimensional Time-Series data in Linear Neural Network

Pritika Mehra, Mini Singh Ahuja

Khalsa College for Women/Department of Computer Science, Guru Nanak Dev University Amritsar, India
e-mail: pritikacsc.rsh@gndu.ac.in
Department of Computer Science and Engineering, Guru Nanak Dev University Regional Campus Gurdaspur, India
e-mail: mini.csegsp@gndu.ac.in

Abstract

Anomaly detection has an active research contribution to large-scale industrial production equipment; time-based performance indicators; and frequent healthcare monitoring queries. The network behavior identified in time series data monitoring for different analyses and results is irrelevant due to high dimensional data. The existing neural network frameworks do not provide continuous network behaviors and the computation process does not fulfill the time series analysis [1] [2]. The proposed system is integrated with long-term memory access and a time series data behavior analysis system. Long-term memory access processes time series context and accurately predicts behavior. The linear neural network model trains the high-dimensional data, extracts the content, and circulates it to get high accuracy [1] [2]. The linear neural network model supports a distribution system to train the network behavior identification. We propose a linear neural network model with a long-term memory access experiment in time series data to show its frequent efficiency and accuracy. The experimental results show that the network behavior prediction accuracy is as high as 99.95%, which is a highly improved one than any other conventional model that did not utilize time series data.

Keywords: *Linear Neural Network, Long Term Memory Access, High Dimensional Data, Behavior Monitoring, Anomaly Detection.*

Received 7 November 2022; Accepted 12 January 2023

1 Introduction

With the improving data transmission rate in multiple applications, anomaly detection plays a vital role in real-time scenarios, which supports continuous productivity and reduces revenue loss. Time series based on current industrial sensor devices such as IoT devices, healthcare wearable monitoring sensor devices, and industrial-based sensor devices produce high-dimensional time-based observations from time series [3] [4]. To improve accuracy, Linear Neural Network Model-based Anomaly Detection is introduced. The existing algorithms are compared (e.g., DBN–BiGRU (Deep Belief Network-Bidirectional Gated Recurrent Unit), LSTM–RNN (Long Short Term Memory-Recurrent Neural Network), and hybrid-based LSTM autoencoder) with efficiency, accuracy, and scalability. The existing DBN algorithm is facing difficulty in adapting to volume-based network traffic, which impacts the accuracy. Industrial needs include critical automation to reduce production downtime [5] [6]. The experiments go towards the machine learning algorithm to increase productivity such as one-class support vector machines, effective approaches to attention-based neural Machine Translation, Computational Intelligence, and Machine Learning. Anomaly detection in medical wireless sensor networks using machine learning algorithms is utilized to protect network security from various threats. [7] [8]. The industrial requirements consider highly standardized technology improvements to operate multi-dimensional data which leads to data threats. In recent years, experiments have required high accuracy and scalability. Network behavior monitoring is more important to control production. Anomaly detection is a highlight needed for the automotive manufacturing sector, in which the devices are connected through the internet to control and monitor production. The production downtime affects the financials, and there remains a shortage of supplies. The anomaly detection provides network behavior results and extracts the behavior of the nodes. The industrial-based time series data is captured for distribution. The proposed system is designed with long-term memory access to process the linear neural network model to learn the high-dimensional data.

Industrial devices are monitored continuously through neural network algorithms that are adapted to identify threats. Only the proposed linear neural network algorithm utilizes the time series based input with the linear model. The existing setup did not provide a continuous monitoring system and it does support data set based analysis. The preprocessing stage observes continuous network behaviors and analyzes data for providing a complex free environment. The preprocessing stage applies the Linear model for analyzing network behavior and it reflects the performance [8][9][10].

Time series based network behaviors are captured to identify an anomaly in a multidirectional transmission unit. This model is adapted to a multivariate transform system (MTS) and can represent low-dimensional and high-dimensional data.
We propose a continuous time series model for high-dimensional time series. It reduces computation time.

We propose a linear neural network learning-based model which can identify the network behavior in high-dimensional data and it follows the below techniques.

1. It gives a continuous time series training model for a huge volume of data.
2. It supports data distribution for high latent representations for the linear model, which provides better computational time.
3. It applies long-term memory access for running the learning model and validates the representation before taking the efficiency and accuracy test.

We have implemented the linear neural network with a long-term memory access algorithm for large-scale data integration. This preprocessing stage improves the accuracy and scalability of industrial infrastructure.

2 Related Work

The time series based anomalies occurred in valuable data-containing experiments. However, they concern different aspects of anomaly detection in time series, with short sections discussing the detection of anomalies in high-dimensional time-series data, in which large-volume data sets are created with high complexity in terms of anomaly detection. To overcome the problem in the detection part, the proposed neural network [1] is integrated with a long-term memory-based generative adversarial network. Early works by authors in review capture the distributional high-dimensional data where the neural network model is prepared to learn the temporal relationship and traditional reconstruction errors based anomaly scores are assigned each time to step up the process. The existing experimental setup determines the low efficiency and short-term utilization [1].

Anomaly detection attracts various research fields depending on the nature of the data. However, effective anomaly detection for large data sets and high-dimensional time series is a challenging task. The authors in [3] proposed a hybrid approach constructed with an LSTM autoencoder to learn normal data sequences. The hybrid model is combined with an SVM classifier for anomaly detection. The LSTM encoder pre-training allows efficient representation of normal data records, and there are no representative values for abnormal records. The LSTM neural network autoencoder is so efficient that it can handle normal real-time classification tasks. The experiment results outperform linear time series in terms of classification rate [3].

In real time, application scenarios are adopted with cloud computing, big data, and mobile applications in which security threats are becoming a serious problem for users' personal information. Time series based network anomaly detection involves behavioral network identification, which protects network security. The authors in [4] highlighted that existing frameworks do not represent the efficient time series data process between continuous network behaviors and real-time dataset classification representation does not match the algorithm. The proposed model in [4] combines a deep belief network with a bidirectional gated recurrent unit and a preprocessing scheme that processes the original real-time feature analysis files. This proposed detection model performs past and future behavior information detection, which failed in continuous time series behavior detection.

The experimental results show cases with high accuracy and high dimensional character analysis, whereas continuous prediction accuracy failed in time series information [4].

In real-time scenarios, anomaly detection plays a key role in data mining and retrieval processes. The authors in [2] highlighted a proposed system that improves computational efficiency in terms of streaming data with a large quantity of retrieval. The application of anomaly detection is limited to the uni-dimensional case, and the SAX-based transformation can be utilized for each dimension. Generalizing for multi-dimensional data did not have the proper approach to process the streaming data. The proposed method is not efficient for processing streaming data with low resources. In this experiment, the optimal one-dimensional reduction ratio determines the detector dimensionality reduction [2].

The continuous real-time application usage explored with anomaly detection is a must for IT infrastructure. The frequent monitoring of large-scale data sets and machines causes scalability problems. The proposed system coarse-to-fine transfer model framework [5] provides accuracy and scalability for anomaly detection. The coarse-to fine model is trained to extract and compress features for distribution, clusters for distribution, and high-accuracy distribution. The framework limitations are in terms of continuous time series analysis, latent representation and efficiency. It has high scalability and accuracy to show production data in terms of equal time intervals [5].

The proposed outlier detection in time series is based on recurrent autoencoder ensembles [6]. It exploits autoencoders built using sparsely connected recurrent neural networks (S-RNNs) [6]. The recurrent neural network generates multiple autoencoders with multiple structures. The ensemble framework combines multiple S-RNN-based autoencoders to enable outlier detection. The highlighted network reduces the effects of some autoencoders being overfitted to outliers, this way improving overall detection quality. The experimental setup showcases effective performance in baselines and state-of-art methods. The existing system did not provide clarity on the data size and scalability and a multi-dimensional way [6]. These are the parts that are still not performing well in the deep neural network.

3 Methodology

Anomaly detection aims at multi-dimensional data from various credentials, and the distance between one another is completely difficult to identify. The distributed significant data vary depending on the occupied content, and attributes can be matched with the detection model and present prediction classification. Detection models are adapted to banking online systems, healthcare analysis, industrial IoT equipment, and online tracking applications. The existing model is trained only on samples, and new observations are not trained under the one-class support vector machine. [11] [12]. The proposed linear neural network trained new observations and classified the data. Normally, the classification process takes a long time to complete the computation time, so the usage of energy and memory is too high. In terms of the LNN model, it adapts a

complex free infrastructure to handle the dataset and attributes. It consists of long-term memory access, which supports long-term average path distances. The highlighted model constructs the training inputs and new observations for efficient sequence latent representations. The construction system allows all the inputs without any loss. This learning model adapts a reconstruction system and long-term memory access maintains the data, which avoids reconstruction errors [13][14]. The unsupervised learning model provides inputs from new observations and data. We followed a linear approach to learn different latent representations. Due to its efficiency, data was extracted accurately and new observations were classified successfully. The proposed model proves that the linear neural network adapted the time series with successful data transmission and successful classification over the network observations. [15] [16].

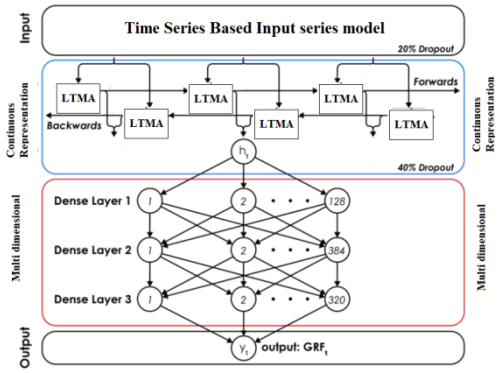

Fig. 1 Long-Term Memory

Fig. 1 illustrates a memory cell that can process data based on observations. It supports data reconstruction and avoids data loss. Long-term memory gates are allowed for forwarding data, maintaining data, and erasing data.

4 The Proposed Method

4.1 Problem Description

This section describes the problem description of existing work for anomaly detection.

Given a dedicated healthcare-oriented real-time dataset H_{Real} $D^{s \times m}$ with abnormal data and a real-time dataset H_{test} $D^{s \times m}$, where s is the time series context and M is the multidimensional series input, The existing model determines only for a normal pre-trained real-time dataset. In the real-time dataset, the infrastructure is monitored through key performance indicators (network behaviour statistics, system memory, and computational time) and these values are collected at random intervals. Thus, each system is formulated as a static trained model, which is also called a conventional network [17][18]). The series data monitoring would produce RT vectors on a specific schedule. (e.g., RT = 4540 for one week and RT = 16485 for one month). We analyzed $K_{x, y, \text{and } z}$ as the targeted dataset, and K1 is the first system considered as multidimensional sub-

sequences in the real-time data set. To determine whether a multidirectional subsequence in a real-time dataset is anomalous or not, the indicator values can't read the multidimensional anomaly indicator score. Normally, the conventional method is described as anomalous if the indicator score is greater than the threshold, and in other cases, it is considered normal [19].

4.2 The Linear Neural Network Architecture

This section elaborates the proposed Linear Neural Network differently by using long-term memory access in high-dimensional data series with a new observation-based detection system. The new observations are temporal convolution data and time series based temporal classification of the prediction network. The proposed model is inspired by the traditional reconstruction model based on anomaly scores in which optimal weights are considered. The autoencoder is a predefined neural network that collects lower-dimensional data and reconstructs it. Linear neural networks are used to represent high-dimensional and low-dimensional data by focusing on key performance indicator vectors that show exact noise and delay. The proposed model incorporates a reconstruction-based optimal weight analysis method and provides weights for a series of time contexts [18] [19].

The long-term memory access consists of an encoder and decoder network. The encoder tries to create a precise representation that maintains the major properties of the input sequences and allows for reasonable reconstruction in subsequent phases. The encoder takes an input sequence, runs it through an LNN network, uses a convolutional layer to lower the dimension of the feature map, and then uses an average-pooling layer to down-sample the series along the time axis by a predetermined factor [20][21]. Using the encoder's output as input, the decoder attempts to reconstruct the original input sequence. The original series' length and dimension must be restored to achieve the reconstruction.

Linear neural network architecture allows new observations to be processed within the neural network. Time Series Approximation tries to capture the most important information from time series [22][23]. A piecewise aggregate approximation function is used in the proposed model, which divides the time series into parts and applies the approximation inside the segments. This aids in the reduction of a time series' complexity by eliminating the requirement to find a global approximation function for the entire time series.

4.2.1 Data Analysis stratergies

The previous model is trained on a new dataset during the transfer process. There are numerous options available in this procedure, such as continuing to train all LNN convolutional layers or training hidden layers (particularly convolutional data layers, such as LNN layers). The data transferability of various neural network layers was investigated by reconstruction process. They discover that the hidden data layers offer more advantage for a variety of data and contain more generic information. LNN layers, in comparison, require more fine-tuning to meet new tasks because they are more specific. Additionally,

this approach was used to classify data's. We are the first to practise LNN model tweaking in the infrastructure operation area.According to the evaluation's findings, in our case, this is the best option.Anomaly detection method with long short memory access provided train models for more data entities and it uses real time data for training and testing to achieve the anomaly detection. The Linear neural network is adapted to handle time series input sequence dependence. The data setup is analyzed by packet capture analysis. The packet analysis indicates how data monitored throughout the operations. The successful frame transfer indicates the accuracy of the continuous time series performance.

4.3 Objective system

Additionally, anomaly detection in network security is to differentiate between unlawful or malicious activities and typical network system activity. Building models of typical network activity, anomaly detection can be seen as a classification task where the goal is to find novel patterns that significantly vary from the model. The majority of recent research on anomaly identification is grounded in the study of both typical and abnormal behaviors. In this paper, we propose linear neural network learning and feature operating-based real-time collective anomaly detection approach. A long-term memory access system and a time series data behavior analysis system are often trained exclusively on multidimensional data, and they are capable of forecasting multiple time steps ahead of multiple inputs. In our method, a live prediction is made for each time step after an LTMA LNN has been trained using typical time series data. The observation of prediction errors from a given number of time steps is now suggested as a novel method for discovering collective anomalies instead of taking into account each time step independently. A collective anomaly will be indicated if the prediction errors from several of the most recent time steps exceed a certain threshold.

Autoencoder:

The continuous data representation provides a semantic relationship between the data. The long-term memory access autoencoder realizes the sequence of data in a linear neural network. The autoencoder is adapted for learning an internal representation of the input data sequence captured from various size vectors [18] and [19]. The decoder part reproduces the vector input with a minimum reconstruction error [24] [25]. The autoencoder process analyses vector inputs for recreation with the encoding and decoding part. The long-term memory access creates performance evaluation in its recreation input sequences.

Considering a sequence of transactions T, represented by a vector $A = \{a_{1,} ,,,, a_x\}$ where $a_t \epsilon R_n$ is the area considered for the transaction at scheduled time t.

Encoder:

The Linear Neural Network considers transaction age and area sequences as W, in the specific time t, corresponding vector values of the encoder C_t^{en} is a function of a_t, C_{t-1}^{en},

Definition 3.1 $C_t^{en} = f_{en}(a_t, C_{t-1}^{en})$

Long-term memory access allows the sequence input to a different weight over the complete sequences.

Decoder:

The Linear Neural Network considers transaction parameter-based sequences and it is specified by age and area, the representation of the Decoder C_t^{dn} as the denoted input to perform the reconstruction of the sequence arrangements [6] [26].

Definition 3.2 $C_t^{dn} = f_{dn}(a_t, C_{t-1}^{dn})$

Here, C_t^{dn} is the continuous sequence vector of the decoder at the transaction parameter area and age. The proposed model is constructed with an encoder and decoder and linear network transaction functions are followed by age and area sequence at a specific time.

Definition 3.3 $L_t = S(C_t^{dn})$

The continuous function is processed by the long-term memory access specified with the age and area vectors of the generated input parameters.

Definition 3.4 $L_{MA} = \sum_{t=1} (L_t - L_{t1})^2$

The linear model keeps the encoder and decoder models until the transaction are completed in the sequence. The linear sequence encodes the input into continuous network performance. The continuous network performance is considered input for a linear neural network. The network transactions are processed in continuous sequence format, and they would be encoded for the processing stage without any interval.

5 Results, Analysis and Discussions

The experimental setup evaluated linear neural network continuous representation on unsupervised data with a continuous simulation schedule. The Linear neural network is designed to handle time series sequence dependence. The simulation is analyzed by packet capture analysis. The packet analysis indicates how simulation performance is fulfilled. The successful packet transmission indicates the accuracy of the continuous time series performance.

We have implemented real-time industrial production with the Ns3 back end using Python by optimizing the packet analysis format using Wire Shark. The Long Term Memory Access autoencoder takes the input value of 1000x1000 width and length. We are considering these values to maximize the production capacity and produce high-dimensional time series data. The long-term memory access autoencoder takes

continuous time-series data sequence records from packet capture analysis format, whereas for the high dimensional area, inputs are converted to datasets.

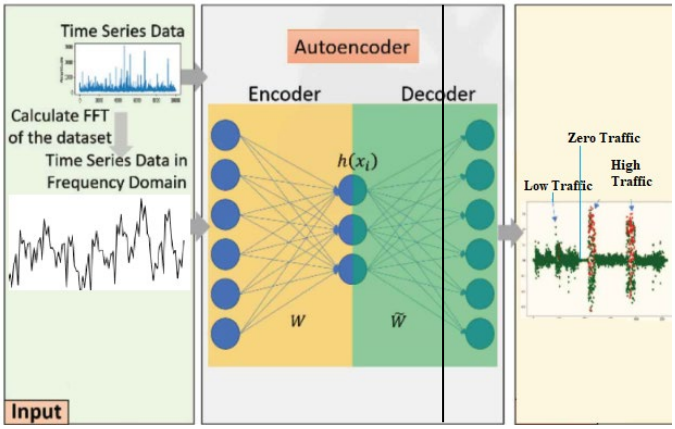

Fig. 2 Framework of the proposed system

We have implemented long-term memory fragments which are not stored in the database or in other formats of data files and simultaneously the data has been encoded and stored as input for the autoencoder. The processed encoder stored values are considered as the high dimensional time series data. Encoder values are compiled with low-traffic to high-traffic time series data.

In this section, a linear neural network model was implemented to improve the anomaly detection accuracy and evaluated the results. The distribution system creates data upgrades in legitimate clients and measures the access time. The network traffic rate is mentioned in N_{TR} and the anomaly detection traffic rate is mentioned in A_{TR}. The normal network client request transaction and anomaly detection request transaction rates are mentioned as N_{RT} and A_{RT}. Our proposed model implemented long-term memory access with time series identifies network behaviors in legitimate user request access time and anomaly request access time.

The network client request follows the below-mentioned factors,

$N_{TR} = \{N_{li} + \ldots\ldots\ldots + N_{ln,,,,}\}$ (1) // Network Client Request

$N_{TRR} = \{N_{liR} + \ldots\ldots\ldots + N_{lnR}\}$ (2) //Network Client Request Response

$A_{TR} = A_{DRi} + \ldots\ldots + A_{DRn}$ (3) //Anomaly Detection Scenario Data Request

$A_{DRR} = A_{DRRi} + \ldots\ldots + A_{DRRn}$ (4) //Anomaly Detection Scenario Data Request Response

The legitimate user average traffic rate is compared with the anomaly detection scenario and showcases the difference in network traffic rate.

$D_{TR} = (\{N_{TR} + N_{TRR}\})$ (5) //Average Network Traffic Data Rate
TR vs. $(\{A_{TR} + A_{DRR}\})$ (6) // Average Anomaly Detection Scenario Data Rate

The network traffic rate values are considered as base values, and the anomaly detection scenario traffic rate is compared with the base value and identifies the difference [22] [23]. The legitimate network behavior is distributed throughout the neighbor nodes and declares the difference between each other in the network.

The distribution system updated the difference in traffic rate and behavior changes to all neighbor nodes.

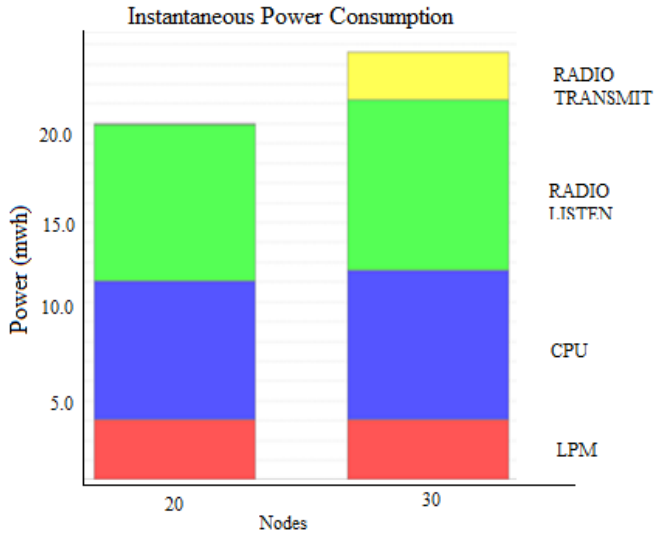

Fig. 3 Legitimate Network Scenario Power Consumption

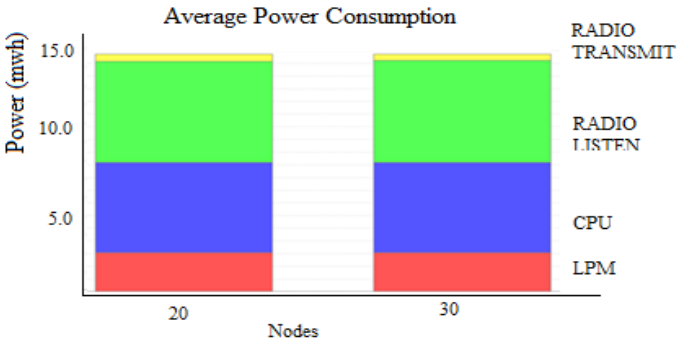

Fig. 4 Anomaly Detection Scenario Power Consumption

The Anomaly detection scenario created heavy network traffic and a power consumption ratio exponentially high. Fig. 3 and Fig. 4 illustrate clearly the power consumption of the

linear neural network in legitimate network scenario and anomaly detection scenario respectively.

Table 1 Power Consumption measurement comparisons in behavior Prediction

S.No	Power Supply	Idle Mode	Transmission Mode	Heavy Network Traffic Mode
Legitimate User Behavior	LPM	0.20 mW	0.35 mW	0.45 mW
	CPU	0.40 mW	0.45 mW	0.55 mW
	Radio Listen	0.42 mW	0.65 mW	0.58 mW
	Radio Transmit	0.10 mW	0.25 mW	0.35 mW
Anomaly Behavior	LPM	0.38 mW	0.45 mW	0.55 mW
	CPU	0.60 mW	0.65 mW	0.75 mW
	Radio Listen	0.50 mW	0.85 mW	0.85 mW
	Radio Transmit	0.20 mW	0.35 mW	0.45 mW
Heavy Network Traffic after Anomaly	LPM	0.35 mW	0.55 mW	0.55 mW
	CPU	0.60 mW	0.85 mW	0.75 mW
	Radio Listen	0.70 mW	0.95 mW	0.95 mW
	Radio Transmit	0.30 mW	0.45 mW	0.65 mW

The above table illustrates the Idle mode, Transmission mode, and Heavy Network Traffic Mode power consumption. In each behavioral system consider LPM, CPU, Radio Listen, and Radio Transmit. The energy consumption measurement mW has been taken in three segments Legitimate user behavior, Anomaly Behavior, and Heavy Network Traffic after Anomaly detection[24][25]. All three stages' power consumption in mW during data transmission can be calculated in table 1.

This suggests that the linear neural network model trains high dimensional data for utilizing the power consumption pattern and it's shared via the distribution system. It is needed to save power consumption [26][27]. However, an advantage of the distribution system is its high power consumption that occurs because of malicious activity and identified the scenario.

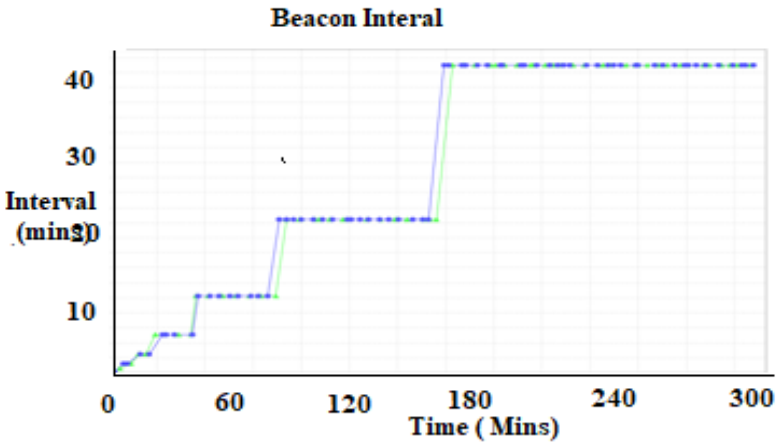

Fig.5. Anomaly Detection Scenario Beacon Interval

The attacker scenario repeats the data request, again and again, to deprive the legitimate data of the source point. The Beacon will transmit its data request to get the data response from the resource [28][29].
The malicious scenario keeps sending a data request to get the response and the beacon interval rate is continuously increasing stage by stage and figure.4 illustrates malicious behavior clearly.

Here, we compare DBN-BiGRU and RNN algorithms with the proposed anomaly detection method based on Long Term Memory Access for anomaly detection in time series data. To experiment the effectiveness of the Linear Neural Network-based high dimensional time series data anomaly detection algorithm, we compared it with existing traditional anomaly detection methods. The performance of the proposed Long Term Memory Access based method showed superiorities, and they are graphically depicted as follows:

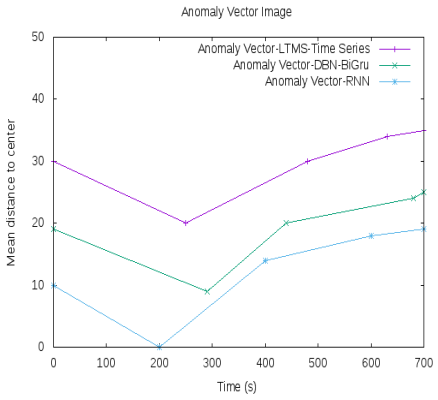

Fig. 6. Mean Distance to center in Anomaly Vector Image

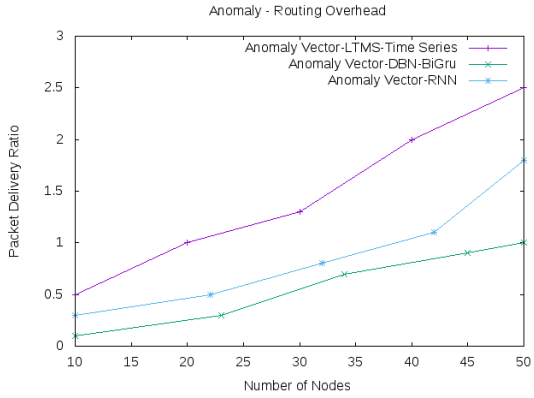

Fig. 7. Packet Delivery Ratio in Anomaly Routing Overhead

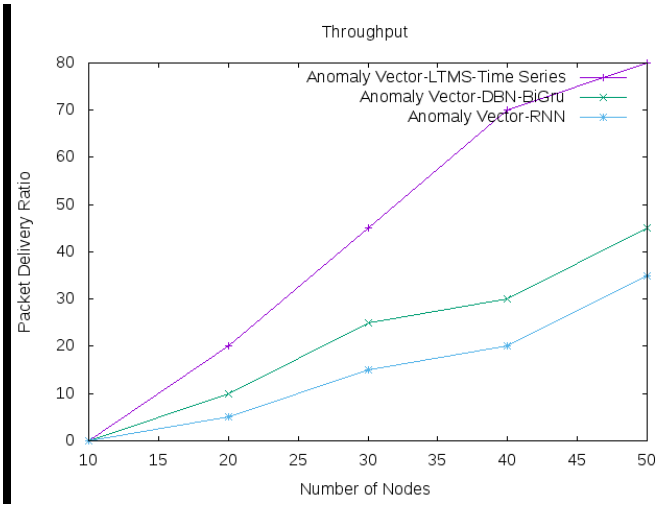

Fig. 8. Packet Delivery Ratio againt number of nodes

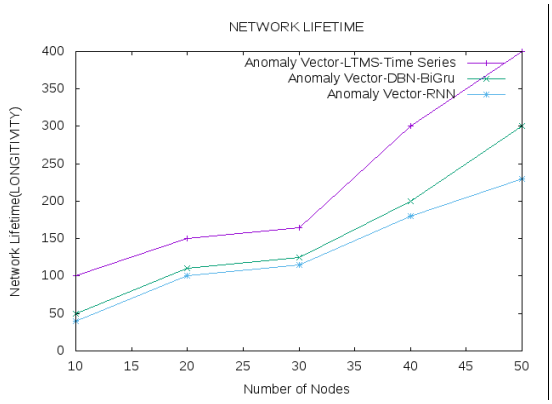

Fig. 9. Network Lifetime against Number of Nodes

Overall, the performance of the proposed method based on Long Term memory access is the best as compared to DBN-BiGRU and RNN. According to the experimental findings,the existing probability of MAE(Mean Absolute Error) less than 30 for the AE-LSTM accuracy rate was 95% [30]network behaviour can be predicted with an accuracy of up to 99.95%, which is far higher than that of any other traditional model that did not make use of time series data.

6 Conclusion

This experimental work proposes a Linear Neural network model for sequence representations of continuous time series. The Linear approach combined with Long Term Memory Access Autoencoder with a continuous framework. The neural network representations are taking the inputs from autoencoders and decoders which provide continuous sequence time series. The neural network continuous representation-based Long Term Memory Access auto encoders provide a complex free process in terms of computation and data transactions; a Linear Neural Network achieved anomaly detection of high dimensional time series data. The application of the linear neural model outperforms in a complex task. The multi-dimensional continuous time series handled unsupervised data within the boundary of complex tasks and outperforms and it is an attempt to showcase accurate results. We will compare the proposed method with state-of-the-art techniques using extensive experiments. The proposed method aims to improve detection accuracy as compared to conventional methods. The multi-dimensional reduction ratios are performed as the detector towards an assigned direction. The successful relationship between multidimensional ratio reduction and anomaly detector processed with real-time simulation data.

References

[1] Sheng Mao, Jiansheng Guo, Taoyong Gu, and Zhong Ma (2020). Dis-AE-LSTM: Generative Adversarial Networks for Anomaly Detection of Time Series Data, 978-1-7281-9146-1/ DOI 10.1109/ICAICE51518.2020.00070.

[2] Konstantinos Bountrogiannis, George Tzagkarakis, (2020). Anomaly Detection for Symbolic Time Series Representations of Reduced Dimensionality, 978-9-0827-9705-3, EUSIPCO 2020.

[3] Zeineb Ghrib, Rakia Jaziri, Rim Romdhane (2020). Hybrid approach for Anomaly Detection in Time Series Data, 978-1-7281-6926-2/20.

[4] Xiaoyue Yu, Tao Li, Aiqun Hu (2020). Time-series Network Anomaly Detection Based on Behaviour Characteristics, 978-1-7281-8635-1/20.

[5] Ming Sun, YaSu, Shenglin Zhang, Yuanpu Cao, Yuqing Liu, Dan Pei, et al (2022). CTF: Anomaly Detection in High-Dimensional Time Series with Coarse-to-Fine Model Transfer, IEEE INFOCOM 2021 - IEEE Conference on Computer Communications, 10-13 May 2021. dOI: 10.1109/INFOCOM42981.2021

[6] Tung Kieu, Bin Yang, Chenjuan Guo and Christian S. Jensen, (2020).," Outlier Detection for Time Series with Recurrent Autoencoder Ensembles" Proceedings

of the Twenty-Eighth International Joint Conference on Artificial Intelligence (IJCAI-19).

[1] Yeji Choi, Hyunki Lim, Heeseung Choi and Ig-Jae Kim, (2020)., et al "GAN-based Anomaly Detection and Localization of Multivariate Time Series Data for Power Plant" 2375-9356/20, IEEE DOI 10.1109/BigComp48618.2020.00-97.

[2] Yue Song, Jinsong Yu, Diyin Tang and Danyang Han., (2020), et al "Telemetry Data-based Spacecraft Anomaly Detection Using Generative Adversarial Networks" 978-1-7281-9277-2/20/2020 IEEE.

[3] Tingfeng Liu, Hui Gao and Jianjun Wu., (2020)., et al "Review of Outlier Detection Algorithms Based on Grain Storage Temperature Data" 978-1-7281-7005-3/20/2020 IEEE.

[4] Peiliang Bai, Abolfazl Safikhani, and George Michailidis., (2020) et al., "Multiple Change Points Detection in Low Rank and Sparse High Dimensional Vector Autoregressive Models" 1053-587X/2020 IEEE.

[5] Jessica Lin, Eamonn Keogh., (2020), et al "Experiencing SAX: a Novel Symbolic Representation of Time Series" Computer Science & Engineering Department, University of California – Riverside, Riverside, CA 92521.

[6] Rahul Agrahari , Matthew Nicholson , Clare Conran , Haytham Assem , and John D. Kelleher ., (2022)., et al "Assessing Feature Representations for Instance-Based Cross-Domain Anomaly Detection in Cloud Services Univariate Time Series Data" . IoT 2022, 3, 123–144. https://doi.org/10.3390/ iot3010008.

[7] E. W. Grafarend, Linear and nonlinear models: fixed effects, random effects, and mixed models. de Gruyter, 2006.

[8] N. Laptev, S. Amizadeh, and I. Flint, "Generic and scalable framework for automated time-series anomaly detection," in Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2015, pp. 1939–1947.

[9] D. P. Kingma and M. Welling, "Auto-encoding variational bayes," arXiv preprint arXiv:1312.6114, 2013.

[10] M. Arjovsky, S. Chintala, and L. Bottou, "Wasserstein gan," arXiv preprint arXiv:1701.07875, 2017.

[11] J. Yosinski, J. Clune, Y. Bengio, and H. Lipson, "How transferable are features in deep neural networks?" in Advances in neural information processing systems, 2014, pp. 3320–3328.

[12] M. Long, Y. Cao, J. Wang, and M. Jordan, "Learning transferable features with deep adaptation networks," in International Conference on Machine Learning, 2015, pp. 97–105.

[13] F. Murtagh and P. Legendre, "Ward's hierarchical agglomerative clustering method: which algorithms implement ward's criterion?" Journal of classification, vol. 31, no. 3, pp. 274–295, 2014.

[14] H.-S. Park and C.-H. Jun, "A simple and fast algorithm for k-medoids clustering," Expert systems with applications, vol. 36, no. 2, pp. 3336– 3341, 2009.

[15] C. Tan, F. Sun, T. Kong, W. Zhang, C. Yang, and C. Liu, "A survey on deep transfer learning," in International conference on artificial neural networks. Springer, 2018, pp. 270–279.

[16] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "Bert: Pre-training of deep bidirectional transformers for language understanding," arXiv preprint arXiv:1810.04805, 2018.

[17] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," arXiv preprint arXiv:1409.1556, 2014.

[18] X. Li, J. Lin, and L. Zhao, "Linear time complexity time series clustering with symbolic pattern forest," in Proceedings of the 28th International Joint Conference on Artificial Intelligence. AAAI Press, 2019, pp. 2930–2936.

[19] B. Yang, X. Fu, N. D. Sidiropoulos, and M. Hong, "Towards kmeans-friendly spaces: Simultaneous deep learning and clustering," in Proceedings of the 34th International Conference on Machine Learning Volume 70. JMLR. org, 2017, pp. 3861–3870.

[20] S. Basu, K. Wagstyl, A. Zandifar, L. Collins, A. Romero, and D. Precup, "Analyzing alzheimer's disease progression from sequential magnetic resonance imaging scans using deep 3d convolutional neural networks." NIPS, 2018.

[21] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM computing surveys (CSUR), vol. 41, no. 3, pp. 1–58, 2009.

[22] 28. X. Zhang, J. Kim, Q. Lin, K. Lim, S. O. Kanaujia, Y. Xu, K. Jamieson, A. Albarghouthi, S. Qin, M. J. Freedman et al., "Cross-dataset time series anomaly detection for cloud systems," in 2019 {USENIX} Annual Technical Conference ({USENIX}{ATC} 19), 2019, pp. 1063–1076.

[23] J. Mei, M. Liu, Y.-F. Wang, and H. Gao, "Learning a mahalanobis distance-based dynamic time warping measure for multivariate time series classification," IEEE transactions on Cybernetics, vol. 46, no. 6, pp. 1363–1374, 2015.

[24] Wangyang Wei, Honghai Wu and Huadong Ma., (2019)., "An autoencoder and LSTM-Based Traffic Flow prediction method". **https://doi.org/10.3390/s19132946**.

Notes on contributors

Ms. Pritika Mehra is an Assistant Professor at the Department of Computer Science, Khalsa College for Women, Amritsar. At present, she is a PhD candidate of Guru Nanak Dev University, Amritsar (Punjab), India. Her main teaching and research interests include Data Mining, Machine Learning, Anomaly Detection and Neural Networks.

Dr. Mini Singh Ahuja is an Assistant Professor at the Department of Computer Science and Engineering, GNDU Regional Campus, Gurdaspur, India. Her main teaching and research interests include Complex Networks, Anomaly Detection and Data Mining. She has published several research articles in international journals of Computer Science.