Anomaly Detection Tool Applying Adversarial Variational Bayes in Wireless Networks

Tyagaraj Gopal Naik
Department of MCA
RV College of Engineering
Bengaluru, India
tyagarajgn.mca21@rvce.edu.in

Dr.S.S.Nagamuthu Krishnan
Department of MCA
RV College of Engineering
Bengaluru, India
ssnk@rvce.edu.in

Abstract— Adversarial Variational Bayes (AVB), a novel paradigm for efficient anomaly detection in network data, is presented in this research. AVB uses variational inference and adversarial learning to combine their strengths in order to learn a reliable representation of typical network traffic patterns. An adversarial network and an anomaly detection model make up the framework's two primary parts. While the adversarial network seeks to distinguish between the latent representations of typical and abnormal traffic occurrences, the anomaly detection model uses a variational autoencoder (VAE) to train a low-dimensional latent representation of network traffic. It eventually develops the ability to tell the difference between routine occurrences and aberrant ones. AVB outperforms current state-of-the-art anomaly detection techniques in terms of both detection accuracy and false positive rate, according to experimental assessments performed on a real-world network traffic dataset.

Keywords— anomaly detection, adversarial variational Bayes (AVB), adversarial learning, variational inference, variational autoencoder (VAE) , adversarial network, detection accuracy, false positive rate, latent representation

I. Introduction

Computer networks are susceptible to different security risks and abnormalities in network traffic due to their constant expansion and complexity. The security and stability of these networks are largely dependent on anomaly detection, which entails spotting unusual patterns or behaviors in network data. The predefined thresholds or statistical models used in conventional approaches to anomaly detection may have trouble capturing the complex and varied nature of network behaviors. In recent years, machine learning algorithms have shown promise in tackling the difficulties of network traffic anomaly detection. Particularly, adversarial learning and variational inference have become effective methods in deep learning. A model is trained through adversarial learning to outwit an enemy.

Gather dan order to accurately detect abnormalities, AVB aims to learn a robust representation of typical network traffic patterns. An adversarial network and an anomaly detection model make up the framework's two primary parts. The variational autoencoder (VAE), a deep generative model capable of learning low-dimensional latent representations of complex data, is the foundation for the anomaly detection model. The VAE encodes incoming network traffic samples into a latent space and reconstructs them. On the other hand, the adversarial network seeks to distinguish between latent representations of typical and abnormal network traffic events. To distinguish between the latent representations produced by the anomaly detection model, it has been trained.

The anomaly detection model learns to capture the statistical characteristics and underlying structures of typical network traffic by optimizing this adversarial objective, making it increasingly resistant to identifying anomalies. The accurate detection of anomalies is facilitated by the use of variational inference in AVB, which enables the learning of latent representations that offer a concise and understandable representation of network traffic patterns.

II. LITERATURE REVIEW

In research by S. Guo, Y. Liu, and Y. Su. [1] address the security concerns present in software-defined networking (SDN), this work provides a simple method for detecting network anomalies. This methodology mines the built-in OpenFlow messages in SDN to describe the network state and identify anomalies, unlike other methods that rely on analyzing packets or flow entries. The suggested method offers a more effective and precise anomaly detection solution by doing away with the necessity for additional message gathering from switches or installing new modules. The technique achieves excellent detection accuracy while lowering the burden on the SDN controller, according to evaluation results. This development has the potential to significantly improve SDN security by reducing security concerns frequently connected to conventional anomaly detection methods.

Another study by A. Liguori, G. Manco, F. S. Pisani, and E. Ritacco et al. [2] suggests ARN, a semisupervised adversarial reconstruction-based method for anomaly production and detection. In order to recreate variations of typical cases with the fewest possible differences, ARN uses a regularised autoencoder, which efficiently detects outliers. The inclusion of regularisation and adversarial reconstruction results in both realistic outlier production and strong detection capability, as well as helps to stabilize the learning process. By modeling the true limits of the data manifold, ARN outperforms the current state-of-the-art techniques and achieves superior anomaly detection performance, as shown by experimental findings on several benchmark datasets.

A. A. Pol, V. Berger, C. Germain, G. Cerminara, and M. Pierini et al. [4] This work uses the deep conditional variational autoencoder (CVAE) as its primary model. By adding more conditional information during training, the CVAE expands on the conventional VAE. In this instance, the hierarchical structure of the trigger system data is probably connected to the conditional information. The authors' goal in using the CVAE is to accurately capture and model the hierarchical connections that exist in the data, which will increase the precision of anomaly identification. The authors introduce an innovative loss function to allow for the discrimination of anomalous events. Although the section does not go into detail about the loss function, it is intended to direct the optimization procedure when the CVAE model is being trained.

In another research by Y. Sun, H. Ochiai, and H. Esaki et al. [10] the authors gather network traffic information from a LAN and transform it into controlled 480-bit chunks. For subsequent processing and analysis, this procedure most commonly entails segmenting the raw network traffic data into fixed-size chunks. The authors' goal is to capture the natural properties and patterns of the network traffic utilizing raw network traffic observation and measurement rather than manually creating features or pre-processing techniques.

Y. Pawar, M. Amayri, and N. Bouguila et al. [8] introduced a paper by proposing an accelerated variational technique for learning an infinite generalized inverted Dirichlet mixture model, This study presents a novel way of addressing the concomitant difficulties of clustering and feature weighting. The strategy makes use of a statistical framework with a Dirichlet process prior to the generalized inverted Dirichlet (GID), which has shown useful in clustering semi-bounded data. Accurately choosing relevant and informative characteristics in high-dimensional domains is essential to getting correct clustering results. The suggested approach uses feature weighting strategies to emphasize the significance of pertinent features in order to overcome this. Through an application centered on anomaly detection, the authors exhibit the value of their strategy and highlight the useful advantages of the suggested framework.

K. Kayabol, E. B. Aytekin, S. Arisoy, and E. E. Kuruoglu, et al. [6] In this study, a multivariate skewed t-distribution (MVSkt) is introduced as a unique method for detecting hyperspectral anomalies. The MVSkt model is intended to improve the effectiveness of anomaly detectors that use autoencoders (AE). In this approach, a skewed t-distribution is used to describe the reconstruction error of a deep AE. Hyperspectral data cubes are utilized as input in an adversarial learning technique to train the deep AE network. A variational Bayesian technique is used to estimate the t-distribution model's parameters. For the purpose of detecting pixel-wise anomalies, a detection rule based on MVSkt is defined. Using actual hyperspectral datasets, the suggested method is contrasted with methods based on robust MVN variance-mean mixture distributions and multivariate normal (MVN) distributions.

G. Slavic, M. Baydoun, D. Campo, L. Marcenaro, and C. Regazzoni et al. [3] The suggested approach combines Dynamic Bayesian Networks (DBNs) and Neural Networks (NNs) to find abnormalities in video data at different abstraction levels. A variational autoencoder (VAE) is used to lower the dimensionality of video frames and capture visual and dynamic data. Additionally, optical flows between succeeding images are computed to produce a latent space that resembles low-dimensional sensory data, such as positioning and steering angle. An Adapted Markov Jump Particle Filter is used to forecast future frames and spot anomalies in video data.

A. A. Pol, V. Berger, C. Germain, G. Cerminara, and M. Pierini, et al. [4] introduce a technique The technique optimizes the reconstruction of normal instances while minimizing the discrepancies between these reconstructions and the actual normal examples. It does this by using a regularised autoencoder. Outliers or anomalies are therefore defined as these little differences. In order to generate realistic outlier samples while preserving excellent anomaly detection abilities, ARN achieves a more stable learning process by combining regularisation approaches with adversarial reconstruction. The results of trials done on several benchmark datasets show that ARN performs significantly better than the state-of-the-art approaches at this time.

Yanmiao Li; Xuan Kong; Jiangang Hou; Xin Li; Kun Zhao; Wei Liang et al. [9] introduced research A key component of maintaining the security of network infrastructure is network traffic anomaly detection, which is frequently handled as a traffic categorization issue. However, conventional classification techniques are losing their potency as a result of the Internet's dynamic nature and the growing complexity of network traffic conditions. The authors of this research provide a brand-new traffic classification system created exclusively for network anomaly detection. Their method's main innovation is that it uses the raw traffic data directly, rather than depending on feature extraction or pre-processing procedures. They use the NIN-DSC network, a neural network architecture created expressly for this purpose, to extract pertinent elements from the data.

X. Zhou, Y. Hu, W. Liang, J. Ma, and Q. Jin.. et al. [7] introduce the discrepancy between dimensionality reduction and feature retention in imbalanced IBD is discussed in this article, and a solution is suggested. The suggested method uses reconstructed feature representations to add a variational long short-term memory (VLSTM) learning model for intelligent anomaly identification. In order to extract low-dimensional feature representations from highly dimensional raw data, the model uses an encoder-decoder neural network with a variational reparameterization technique.

III. ALGORITHMS

1. Variational Autoencoder (VAE)

The core algorithm employed in the suggested methodology for anomaly identification is the Variational Autoencoder (VAE). An encoder network and a decoder network make up its two primary parts. The decoder network reconstructs the data from the latent space after the encoder network translates the input data to a lower-dimensional latent space. A regularisation term, typically the Kullback-Leibler (KL) divergence, which encourages the latent representation to follow a prior distribution, is combined with a reconstruction loss, which measures the similarity between the reconstructed and original data, during training. The VAE effectively captures the key characteristics of the input data by learning the latent space representation.

2. Adversarial Training

The variational autoencoder (VAE) can detect anomalies better thanks to a technique called adversarial training. In order to discriminate between typical and anomalous latent representations produced by the VAE, a separate discriminator network must be trained. The VAE is trained to produce latent vectors that can trick the discriminator and make it easier to distinguish between typical and anomalous cases. The VAE gains the ability to produce latent representations that are consistent with the distribution of typical examples through joint training, improving the ability to distinguish between typical and anomalous data points in the latent space. Adversarial training increases the VAE's capacity to recognize distinguishing traits of typical data and reduce the representation of anomalies, enhancing the performance of anomaly detection as a whole.

3. Reconstruction Error

Using metrics like mean squared error (MSE), binary cross-entropy (BCE), or other divergence measurements, it measures how different the reconstructed data are from the original input. A higher divergence or reconstruction error suggests a higher chance of an abnormality. Cases with reconstruction errors above the threshold can be labeled as anomalies by choosing a suitable threshold. The reconstruction error/divergence plays a critical part in the anomaly identification process as a key signal for spotting anomalies.

4. Threshold Determination

Setting a threshold to classify data instances as normal or anomalous based on their anomaly scores is a vital stage in the anomaly detection process. Different methods, including statistical indicators (such as quantiles or standard deviations) or domain knowledge, are used to define this decision limit. The trade-off between false positives and false negatives in anomaly detection is directly influenced by the threshold selection. An ideal threshold for efficiently separating typical instances from probable anomalies can be found by carefully examining the distribution of anomaly scores, utilizing domain expertise, and assessing the performance objectives.

TABLE I. COMPARISON TABLE OF DIFFERENT ALGORITHM USED

Algorithm	**Computational complexity**	**Parameter Tuning**
Variational Autoencoder	High	high
Adversarial Training	low to moderate	moderate
Reconstruction error	low	low
Threshold Determination	moderate	moderate

IV PROPOSED SYSTEM

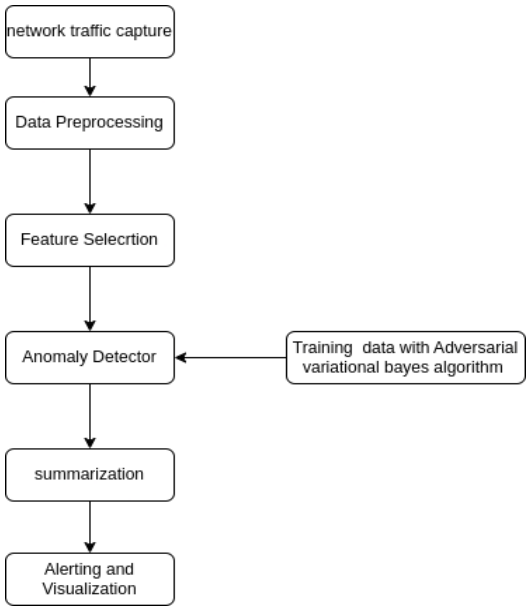

Fig 1 System Architecture

A number of interconnected modules make up the system architecture for an anomaly detection tool that applies adversarial variational Bayes (VB) in wireless networks. The data collection module gathers wireless network traffic data from multiple sources, which is subsequently cleaned, normalized, and extracted key features in the preprocessing module. To capture typical network traffic patterns, the Variational Autoencoder (VAE) Training Module trains a VAE model on the preprocessed data. In order to find potential anomalies, the Anomaly Score Computation Module computes reconstruction errors. Through adversarial training between the VAE and a discriminator

network, the adversarial training module increases the resilience of the model.

The anomaly detection module categorizes network data as normal or anomalous. The Visualisation and Reporting Module offers reports and visualizations for analyzing and deciphering the discovered abnormalities. The tool's performance is evaluated by the Evaluation and Refinement Module, which also makes suggestions for improvements to increase accuracy. This system architecture integrates data processing, VAE training, adversarial training, anomaly classification, and evaluation to provide effective anomaly detection in wireless networks while facilitating network monitoring and security.

The following are the main characteristics and elements of the suggested system:

Data collection: Data preprocessing entails cleansing the data by removing duplicates, missing values, and inconsistencies, normalizing features to a common scale, identifying pertinent features, lowering dimensionality when needed, and formatting the data into a structured format. These procedures guarantee that the data is precise, uniform, and prepared for analysis. Deep learning techniques can find abnormalities and offer important insights into network behavior because preprocessing improves the efficacy and accuracy of future anomaly detection algorithms.

Variational Autoencoder(VAE): Building a generative model with an encoder and a decoder is required for variational autoencoder (VAE) training. The decoder reconstructs the original data from the latent space, while the encoder maps preprocessed network traffic data to a lower-dimensional latent space representation. The VAE minimizes the reconstruction loss during training, which gauges how different the input and recreated data are. The latent space distribution is also regularised by a KL divergence loss term. The VAE learns to capture the underlying distribution of typical network traffic by optimizing these losses. By contrasting reconstruction mistakes or scrutinizing the latent space representation, the trained VAE can subsequently be employed for anomaly identification.

Anomaly Detection Computation: In order to generate reconstructed data, a trained variational autoencoder (VAE) is used in the computation of anomaly scores. An anomaly score is derived from the reconstruction error, which is determined as the difference between the input and reconstructed data. Greater reconstruction mistakes could be an indication of anomalies or a departure from typical trends. This method enables the identification of abnormalities based on the fidelity of reconstruction by taking advantage of the VAE's capability to capture the underlying distribution of typical network traffic.

Evaluation and Refinement:Refinement entails modifying hyperparameters, improving the model's architecture, and repeating the evaluation-refinement cycle while measuring the performance of the anomaly detection tool using metrics like precision, recall, and F1-score. By optimizing its design and modifying it to the specific characteristics of network traffic data, these iterative processes increase the tool's accuracy and efficacy.

IV. EXPERIMENTAL EVALUATION

In addition to employing performance measurements like precision, recall, and F1-score, it involves choosing a dataset, preprocessing, training, and validation. Through comparisons, robustness assessments, scalability analyses, sensitivity analyses, and interpretability assessments, the tool's effectiveness, generalizability, scalability, and interpretability are ensured. To determine viability, actual deployment and evaluation may also be done. The evaluation's overall goal is to validate the tool's usability and usefulness for spotting irregularities in wireless network traffic.

V. CONCLUSION

The AVB-based anomaly detection in network traffic project will be improved in the future by adding temporal information to capture sequential dependencies, integrating domain knowledge for better performance, addressing imbalanced data with practical methods, investigating transfer learning and adaptation for dynamic network environments, maximizing scalability and efficiency, enabling real-time anomaly detection, deploying in cloud or edge environments, and ev These improvements aim to improve anomaly detection's precision, effectiveness, adaptability, and application, thereby enhancing computer networks' security and stability.

REFERENCES

[1] Y. Cui, Q. Qian, H. Xing, and S. Li, "LNAD: Towards Lightweight Network Anomaly Detection in Software-Defined Networking," 2020 IEEE 22nd International Conference on High-Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Yanuca Island, Cuvu, Fiji, 2020, pp. 855-860, doi: 10.1109/HPCC-SmartCity-DSS50907.2020.00113.

[2] S. Guo, Y. Liu, and Y. Su, "Comparison of Classification-based Methods for Network Traffic Anomaly Detection," 2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Chongqing, China, 2021, pp. 360-364, doi: 10.1109/IMCEC51613.2021.9482274.

[3] A. Liguori, G. Manco, F. S. Pisani and E. Ritacco, "Adversarial Regularized Reconstruction for Anomaly Detection and Generation," 2021 IEEE International Conference on Data Mining (ICDM), Auckland, New Zealand, 2021, pp. 1204-1209, doi: 10.1109/ICDM51629.2021.00145.

[4] A. A. Pol, V. Berger, C. Germain, G. Cerminara and M. Pierini, "Anomaly Detection with Conditional Variational Autoencoders," 2019 18th IEEE International Conference On Machine Learning And

Applications (ICMLA), Boca Raton, FL, USA, 2019, pp. 1651-1657, doi: 10.1109/ICMLA.2019.00270.

[5] G. Slavic, M. Baydoun, D. Campo, L. Marcenaro and C. Regazzoni, "Multilevel Anomaly Detection Through Variational Autoencoders and Bayesian Models for Self-Aware Embodied Agents," in IEEE Transactions on Multimedia, vol. 24, pp. 1399-1414, 2022, doi: 10.1109/TMM.2021.3065232.

[6] K. Kayabol, E. B. Aytekin, S. Arisoy, and E. E. Kuruoglu, "Skewed t-Distribution for Hyperspectral Anomaly Detection Based on Autoencoder," in IEEE Geoscience and Remote Sensing Letters, vol. 19, pp. 1-5, 2022, Art no. 5510705, doi: 10.1109/LGRS.2021.3121876.

[7] X. Zhou, Y. Hu, W. Liang, J. Ma, and Q. Jin, "Variational LSTM Enhanced Anomaly Detection for Industrial Big Data," in IEEE Transactions on Industrial Informatics, vol. 17, no. 5, pp. 3469-3477, May 2021, doi: 10.1109/TII.2020.3022432.

[8] Y. Pawar, M. Amayri and N. Bouguila, "An Accelerated Nonparametric Bayesian Approach for Anomaly Detection with Feature Selection," 2022 International Electrical Engineering Congress (iEECON), Khon Kaen, Thailand, 2022, pp. 1-4, doi: 10.1109/iEECON53204.2022.9741682.

[9] Y. Li et al., "NIN-DSC: A Network Traffic Anomaly Detection Method Based on Deep Learning," 2022 7th International Conference on Signal and Image Processing (ICSIP), Suzhou, China, 2022, pp. 390-394, doi: 10.1109/ICSIP55141.2022.9886658.

[10] Y. Sun, H. Ochiai and H. Esaki, "Deep Learning-Based Anomaly Detection in LAN from Raw Network Traffic Measurement," 2021 55th Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, USA, 2021, pp. 1-5, doi: 10.1109/CISS50987.2021.9400241.