Network Anomaly Detection Using LightGBM: A Gradient Boosting Classifier

Md. Khairul Islam

Prithula Hridi

Md. Shohrab Hossain

Husnu S. Narman

Outline

1. Motivation
2. Problem definition
3. UNSW-NB15 dataset
4. Prior arts
5. Our contribution
6. Methodology
7. Result
8. Future works

Motivation

- As internet is being more popular in our daily life, the risk of malicious attacks are increasing also.
- Intrusion detection systems are built to defend users from such attacks.
- Signature based systems can detect previously seen attacks.
- But anomaly detection techniques are better at catching zero-day attacks.

Problem Definition

- Network intrusion detection systems
  - Signature based
  - Anomaly based
    - Point anomaly: User to Root (U2R), and Remote to User (R2U)
    - Collective anomaly : DOS attack
    - Contextual anomaly: Probe attack

Our goal is to detect whether a network traffic data is an anomaly, using supervised machine leaning techniques.

UNSW-NB15 dataset

- A recent benchmark dataset for NIDS (Network Intrusion Detection Systems) created by Moustafa et al. [1] at Cyber Range Lab of Australian Center of Cyber Security.
- Presents more recent and modern network traffic compared to other NIDS benchmark dataset (KDDCup99, NSL-KDD, DARPA).
- Contains nine major families of attacks. However, we only worked on binary classification (anomaly or normal).
- Has separate train and test set.

UNSW-NB15 dataset

- **UNSW-NB15 dataset description:**

Type	Train	Test
Normal	56,000	37,000
Anomaly	119,341	45,332
Total	**175,341**	**82,332**

Prior arts

The prior works on binary classification of UNSW-NB15 dataset, can be grouped based on the model evaluation process :

- Validation on the same data used for training [2-3].
- Validation on separate test data [10-11, 12-13].
- Ten-fold cross-validation on
  - Combined (train + test) data [7-8] .
  - Train data [4-6]
  - Test data
- Five-fold cross validation on train data [9].

Our contributions

- All prior arts focus on one model evaluation process. So it is difficult to compare their contributions with prior arts following a different evaluation process. However, we have presented a through study with all evaluation processes found in prior arts for this dataset.
- We performed feature preprocessing and engineering to make the model more generalized.
- Our model presents state-of-the-art performance for most metrics in all evaluation setups.

Methodology

Data preprocessing :

- Dropping unnecessary columns.
- Feature engineered categorical columns.
- Used StandardScaler on all numerical columns.
- Dropped features with less than 0.5% average feature importance in ten-fold cross-validation on train data. 7 features are dropped.
- Used one-hot encoding for categorical columns.
- Finally we had 53 feature columns in our dataset.

Methodology

Choosing the best classifier: We applied ten-fold cross-validation on train data and chose LightGBM based on f1-score and accuracy.

Classifier	Accuracy(%)	F1 score(%)
LogisticRegression	93.54	95.42
GradientBoosting	94.58	96.11
DecisionTree	94.99	96.32
RandomForest	96.08	97.14
LightGBM	96.18	97.21

Result

Evaluating model on the same data used for train:

Metrics(%)	Train	Test
Accuracy	99.60	99.98
Precision	99.52	99.97
Recall	99.89	99.98
F1 score	99.71	99.98
FPR	0.01	0.0004
AUC	99.99	99.99
Time(s)	243	237

Result

Evaluating model on the same data used for train:

- Mogal et al. [2] achieved 99.96% accuracy.
- Kanimozhi et al. [3] achieved 98.3% accuracy.
- But this approach overfits on train data and will perform poorly on test data.
- We have shown that our model when overfitted on train data, only achieved 86.88% accuracy and 89.14% f1 score on test data.

Result

- **Ten-fold cross-validation:** Followed by [4-7].

Metrics(%)	Train	Test	Combined
Accuracy	96.18	98.18	95.19
Precision	96.54	98.87	96.84
Recall	97.89	97.80	95.58
F1 score	97.21	98.33	96.21
FPR	7.47	1.37	5.51
FAR	3.82	1.83	4.81
AUC	99.44	99.81	99.26
Time(s)	628.1	281.1	838.8

Result

Ten-fold cross-validation:

- On train data our model accuracy is 96.17%. Where accuracy achieved by prior arts are Suleiman et al. [4] 90.14%, Meftah et al. [5] 82.11%, Hanif et al. [6] 84% .
- On combined data our model accuracy is 95.19%. Where accuracy achieved by prior arts are Koroniotis et al. [8] 93.23%, Nawir et al. [7] 94.6% .

Result

- **Five-fold cross validation**: Followed by Meghdouri et al. [9].

Metrics(%)	Train [9]	Train
Accuracy	99.0	96.18
Precision	85.9	96.56
Recall	85.1	97.87
F1 score	84.9	97.21
ROC AUC	99.8	99.43

Result

- **Five-fold cross validation**: Followed by Meghdouri et al. [9].

Metrics(%)	Test [9]	Test
Accuracy	98.9	98.08
Precision	84.9	98.79
Recall	85.1	97.7
F1 score	84.9	98.24
ROC AUC	99.8	99.81

Result

Validation on test data: Followed by [10-11, 12-13]. Our FAR and AUC scores for this case are 8.05% and 98.67%.

Metrics(%)	Ours	RF [12]	REP Tree [13]
Accuracy	91.95	90.3	93.56
Precision	89.59	98.8	83.3
Recall	96.60	86.7	83.2
F1 score	92.96	92.4	83.25
FPR	13.75	-	2.3

Result

Validation on test data:

- Bhamare et al. [10] achieved accuracy 89.26%, 93.7% TP and 95.7% TN. Where our accuracy, TP, and TN are 91.95%, 97%, and 86%.
- Moustafa et al. [11] achieved 85.56% accuracy and FAR 15.78% . Our accuracy is 91.95% and FAR 8.05%.

Future works

- Perform multiclass-classification on the UNSW-NB15 dataset.
- Apply deep learning techniques on this dataset.

Reference

[1] M. I. Ashiq, P. Bhowmick, M. S. Hossain, and H. S. Narman, “Domain flux based dga botnet detection using feedforward neural network,” in *IEEE Military Communications (MILCOM)*. Norfolk, VA, USA: IEEE, 12-14 Nov., 2019.

[2] D. G. Mogal, S. R. Ghungrad, and B. B. Bhusare, “Nids using machine learning classifiers on unsw-nb15 and kddcup99 datasets,” *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, vol. 6, no. 4, pp. 533–537, 2017.

[3] V. Kanimozhi and P. Jacob, “Unsw-nb15 dataset feature selection and network intrusion detection using deep learning,” *International Journal of Recent Technology and Engineering*, vol. 7, pp. 443–446, 01 2019.

[4] M. Suleiman and B. Issac, “Performance comparison of intrusion detection machine learning classifiers on benchmark and new datasets,” in *28th International Conference on Computer Theory and Application*, 10 2018, pp. 447–489.

[5] S. Meftah, T. Rachidi, and N. Assem, “Network based intrusion detection using the unsw-nb15 dataset,” *International Journal of Computing and Digital Systems*, vol. 8, no. 5, pp. 478–487, 2019.

Reference

[6] S. Hanif, T. Ilyas, and M. Zeeshan, “Intrusion detection in iot using artificial neural networks on unsw-15 dataset,” in *16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI)*. IEEE, 2019, pp. 152–156.

[7] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, “Effective and efficient network anomaly detection system using machine learning algorithm,” *Bulletin of Electrical Engineering and Informatics*, vol. 8, no. 1, pp. 46–51, 2019 .

[8] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, “Towards developing network forensic mechanism for botnet activities in the iot based on machine learning techniques,” in *International Conference on Mobile Networks and Management*. Springer, 2017, pp. 30–44.

[9] F. Meghdouri, T. Zseby, and F. Iglesias, “Analysis of lightweight feature vectors for attack detection in network traffic,” *Applied Sciences*, vol. 8, no. 11, 2018.

Reference

[10] D. Bhamare, T. Salman, M. Samaka, A. Erbad, and R. Jain, “Feasibility of supervised machine learning for cloud security,” in *International conference on Information Science and Security*. Pattaya, Thailand: IEEE, 2016, pp. 1–5.

[11] N. Moustafa and J. Slay, “The evaluation of network anomaly detection systems: Statistical analysis of the unsw-nb15 data set and the comparison with the kdd99 data set,” *Information Security Journal: A Global Perspective*, vol. 25, no. 1-3, pp. 18–31, 2016.

[12] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. AlNemrat, and S. Venkatraman, “Deep learning approach for intelligent intrusion detection system,” *IEEE Access*, vol. 7, 2019.

[13] P. Dahiya and D. K. Srivastava, “Network intrusion detection in big dataset using spark,” *Procedia computer science*, vol. 132, pp. 253–262, 2018.