Original Research Article

Modeling the Detection of Cyber Intrusion with Network Traffic Features: A Regression-Based Study

Yu Milan

Stuyvesant High School, 345 Chambers St, New York, NY 10282, United States

ABSTRACT

Cyber-attacks continue to impose serious threats to modern digital systems, creating an urgent need for interpretable and effective methods in detecting intrusions. This study examines the use of network traffic features to predict cyber intrusions by specifically applying a regression-based quantitative framework. Using the publicly available NSL-KDD intrusion detection dataset, this study conducted a quantitative analysis with a total of 125,973 records of network connections that were labeled as either normal traffic or intrusion attempts. Connection duration, protocol type, number of failed login attempts, server-side error rate, and connection count were the five chosen network-level features to capture abnormal network behavior. A binary logistic regression model was employed to estimate the likelihood for a given network connection to be classified as an intrusion. When evaluating the model performance, accuracy, precision, recall and a confusion matrix were specifically utilized. The model achieved an overall accuracy of approximately 90.8%, with high precision and recall for detecting intrusion attempts. However, it shall be noted that simulated network traffic was used to derive NSL-KDD dataset as a benchmark dataset. Therefore, the results primarily indicate methodological feasibility rather than deployment performance in the real-world setting. This indicated that the majority of attack attempts were identified correctly, while minimizing false alarms. These findings support how the simple mathematical models may be effective in detecting intrusions in the field of cyber-security and other applications, while highlighting the importance of transparent and quantitative approaches to intrusion detection. This study demonstrates that regression-based modeling may be effective in identifying cyber threats as an interpretable framework in the use of network traffic data.

Keywords: Cyber-security; Intrusion detection; Anomaly detection; Network traffic analysis; Logistic regression; Mathematical modeling; NSL-KDD dataset

INTRODUCTION

How information is stored, transmitted, and accessed has been fundamentally transformed by the rapid expansion of digital infrastructure. With these advances, unprecedented connectivity and efficiency have been enabled, increasing the exposure to cyber-attacks. Due to heavy reliance of modern organizations on networked systems for financial transactions, communication, and data storage, they have become attractive targets for malicious actors. According to recent reports, it has been emphasized that cyber-attacks are currently growing both in the perspective of frequency and sophistication that serious risks have been posed to economic stability,

Corresponding author: Yu Milan , E-mail: jym10234@gmail.com.

Accepted March 13, 2026
https://doi.org/10.70251/HYJR2348.42137142

national security, and critical infrastructure (1,2). As a result, it has become a central challenge to develop effective and reliable intrusion detection mechanisms in cyber-security research.

As traditional cyber-security systems rely on signature-based detection in many cases, incoming network traffic is often compared against a database of known attack patterns. Even if this approach is effective for previously identified threats, it is still problematic to detect novel or evolving attacks that are commonly referred to as zero-day attacks (3). Due to this limitation, researchers were motivated to explore methods for anomaly detections, focusing on identifying deviations from normal network behavior instead of matching predefined signatures. Anomaly detection systems target to develop a model to examine what constitutes normal activity and flag observations that are significantly deviant from this baseline as potential intrusions (4).

Anomaly detection techniques are widely used in the areas, including fraud detection, medical monitoring, and network security (5). In computer networks, anomalies may manifest as unusual connection durations, abnormal traffic volumes, or repeated failed log-in attempts as a possible signal for malicious activity (6-8). Among many approaches possible to intrusion detection, regression-based models seem to be the most appropriate due to their interpretability and mathematical transparency. With regression techniques, researchers are allowed to directly assess how individual network features contribute to intrusion probability (9). Particularly, logistic regression is the best suited for binary classification problems since outcome may turn out to be either normal traffic or an intrusion attempt. Logistic regression provides an insight into which aspects of network behavior are correlated with abnormal activity the most strongly by estimating coefficients for each predictor (10).

According to prior studies, intrusion detection systems have been extensively explored using machine learning and artificial intelligence techniques, such as neural networks and support vector machines (11). These methods often achieve high predictive performance. However, many studies still emphasize algorithmic complexity over mathematical interpretability. In addition, system architecture or implementation challenges are underscored by a few studies without presenting a clear quantitative framework that may be easily reproduced or analyzed (12). Although many studies conducted for the analysis of intrusion detection used complex machine-learning algorithms, relatively few studies focused on interpretable statistical model to clearly quantify how particular network traffic features affect probability of intrusion. Therefore, mathematically transparent regression-based approaches still remain underrepresented in the literature of intrusion detection. Furthermore, the importance of selecting meaningful network-level features, including connection duration, protocol type, failed authentication attempts, and error rates has been highlighted by several surveys and technical reports. However, how these variables jointly influenced intrusion likelihood has not been much researched through a quantitative framework (6, 11). As a result, there is a need for studies to apply well-defined network features into a quantitative framework while maintain predictive performance.

To address this literature gap, this study develops a logistic regression model to detect cyber intrusions by using selected network traffic features from the simulated NSL-KDD dataset. The goal is to evaluate whether a simple and interpretable regression framework can achieve strong performance for classification, while maintaining transparency in how individual features in the network contribute to intrusion detection. With focus on a limited set of interpretable network features, this study concentrates on clarity, reproducibility, and quantitative rigor. The goal of this study is not to replace advanced machine learning systems but to show how even a simple quantitative framework may achieve high detection accuracy when combined with carefully chosen features and an optimized decision threshold (13). This study particularly seeks to answer the research question about how accurate it is to use network traffic features to predict whether a network connection shows an intrusion attempt through a regression-based quantitative model. This study hypothesizes that logistic regression framework conducted by using selected network traffic features will achieve higher accuracy in classification than a baseline random classification model.

METHODS AND MATERIALS

Data Source

In this study, the NSL-KDD intrusion detection dataset, a widely used benchmark dataset in the field of cyber-security research, was used. Specifically, the KDDTrain+ subet of the NSL-KDD dataset was used for developing a model. This subset contained 125,973 labeled network connecting records that each showed either normal traffic or an intrusion attempt. There were no personal identifiers or human subject data in the dataset that was obtained from an academic repository

and imported into spreadsheet software for analysis.

Each observation in the dataset indicated a single network connection that was described by many network-level features. A subset of features was specifically selected in this study for the purpose of interpretability, while aligning with anomaly detection theory. These chosen features captured temporal, protocol-level, and error-based characteristic of network behavior.

Study Design

This research employed a quantitative, observational study design through secondary data. An individual network connection was the unit of the analysis in this study. The main objective was to predict whether a given connection indicated an intrusion attempt according to observable network traffic features. The outcome was binary that made the study suitable for regression-based modeling in the data analysis.

Variables

Intrusion status coded as a binary outcome with 0 being normal network traffic and 1 being an intrusion attempt was the dependent variable used in this study. The independent variables included the following five network-level features: connection duration, protocol type, number of failed login attempts, server-side error rate, and connection count. Connection duration indicated the length of time when a connection remained active. Protocol type showed whether the connection used TCP, UDP, or ICMP. Number of failed login attempts captured authentication anomalies. Server-side error rate reflected abnormal communication behavior. Lastly, connection count measured recent traffic volume to the same host.

Aforementioned variables were specifically chosen since prior research indicated how they were strong indicators of abnormal or malicious network activity.

Data Preparation

Raw text files were first converted into a tabular format that was comparable with spreadsheet analysis. Categorical variables, including protocol type, were then numerically encoded so that intrusion was included in the regression model. Protocol type was encoded using dummy variables that indicated TCP, UDP, and ICMP connections. Continuous variables, including connection duration, error rate, and connection count were standardized before performing regression analysis to ensure comparable scaling across predictors. The intrusion models were transformed into a binary outcome variable. For these selected features, it was ensured that there were no missing values, and no additional imputation was required.

Mathematical Model A binary logistic regression model was specifically used to estimate the probability where a network connection indicated an intrusion. Logistic regression model was appropriate as it modeled the relationship between a set of predictor variables and the probability of a binary outcome. The model was expressed as follows:

$$\text{Logit}(p) = \ln\left(\frac{p}{1-p}\right) = \beta_0 + \beta_1(Duration) + \beta_2(Protocol) + \beta_3(FailedLogin) + \beta_4(ErrorRate) + \beta_5(ConnectionCount)$$

Regression coefficients were estimated using maximum likelihood estimation. Odds ratios were computed to interpret the strength of association between each predictor and the probability of intrusion detection.

Model Evaluation

Model performance was assessed according to accuracy, precision, and recall, along with a confusion matrix to summarize outcomes of classification. In addition, receiver operating characteristic (ROC) analysis was performed, while calculating the ROC curve (AUC) to provide a threshold-independent evaluation of classification performance. These metrics were selected for the purpose of assessing both overall predictive performance and the balance between false positives and false negatives as a critical component in the context of cyber-security.

RESULTS

In the data analysis, a total of 125,973 network connection records from the NSL-KDD dataset were included. Each observation indicted a single network connection that was labeled as either normal traffic or an intrusion attempt. As the dataset contained a great amount of intrusion instances, the regression model was used to evaluate both normal and malicious traffic patterns. Five network-level features, namely; connection duration, protocol type, number of failed login attempts, server-side error rate, and connection count, were used as predictors in the model with binary classification.

Overall Model Performance

According to the logistic regression model, there was a strong overall performance in distinguishing between

normal network traffic and intrusion attempts. Applying a classification probability threshold of 0.50, the model indicated an overall accuracy of around 90.8%. This indicated how the majority of network connections were classified correctly. This high level of accuracy suggested that a substantial amount of information was contained by the selected network features as relevant to intrusion detection, even when analyzed through a relative simple quantitative framework.

Confusion Matrix Results

This study further examined model predictions through a confusion matrix that summarized the number of correct and incorrect classifications for each class (Figure 1). A total of 64,144 normal connections were identified by the model as normal traffic (true negatives), and a total of 50,229 intrusion attempts were identified as intrusions (true positive). However, a total of 3,199 normal connection were classified incorrectly as intrusions (false positive), while a total of 8,331 intrusion attempts were classified incorrectly as normal traffic (false negatives).

These findings suggested that the model turned out to be effective in identifying both cases with a higher reported rate of correct classification for normal traffic relative to intrusion attempts. With the presence of false negatives, it was highlighted that there exists the challenge of detecting all malicious activity. However, the relatively small number of false positives indicated how the model did not excessively flag good traffic as malicious.

Precision and Recall

In order to further evaluate the performance of classification, both precision and recall were calculated for the intrusion class (Figure 2). It turned out that precision for intrusion detection was around 0.94. This means that, about 94% of the time, the model correctly predicted a connection to be an intrusion. This high precision rate reflected a low false-positive rate, suggesting that the relatively few unnecessary intrusion alerts were generated by the model.

It also turned out that recall for intrusion detection was around 0.86. The recall value of 0.86 represents that 86% of actual intrusion attempts were identified correctly by the model. Even if several intrusion events were missed, the recall value indicated how the majority of malicious connections presented in the dataset were captured by the model. Taken together, these metrics indicated how a balanced performance was achieved the model, detecting most intrusions, while still maintaining a low rate of false alarms. The F1-score

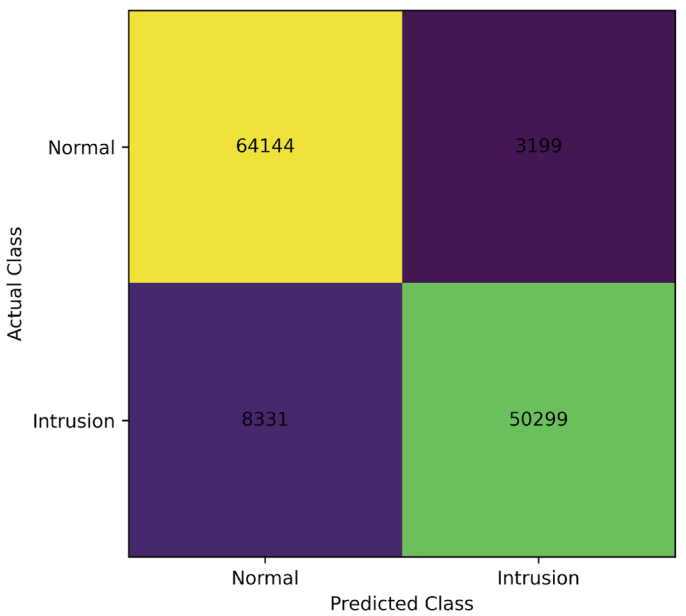

Figure 1. *Confusion matrix summarizes classification results of the logistic regression model that is applied to the NSL-KDD dataset (n=125,973). True positives show correctly detected intrusion attempts, while false positives show normal traffic that is incorrectly flagged as attacks. The classification threshold was set to be 0.50.*

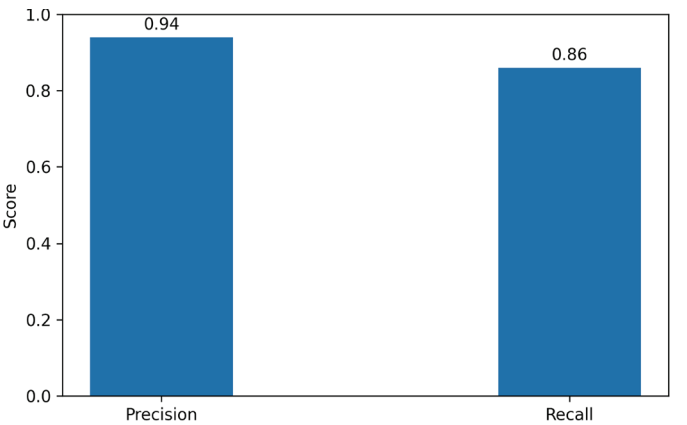

Figure 2. *Precision and recall metrics for detecting intrusion in the use of the logistic regression model on the KSL-KDD dataset. Precision shows the proportion of correct predicted intrusions, while recall shows the proportion of correctly identified actual intrusion attempts.*

was calculated as the harmonic mean of precision and recall as approximately 0.90. This indicates the balanced classification performance between detecting intrusions and minimizing false alarms.

Feature-Level Patterns

The primary focus of this study was not on the regression coefficients. However, observable patterns in the chosen features supported the predictive performance of the model proposed in this study (Figure 3). For example, connections with higher numbers of failed login attempts and elevated server-side error rates were often classified as intrusions. Similarly, there was an increased likelihood of malicious activity associated with higher connection counts to the same host, and this was consistent with known network scanning and attack behaviors. Furthermore, protocol type also contributed to the differences of classification since intrusion attempts were more commonly associated with certain protocols than normal traffic.

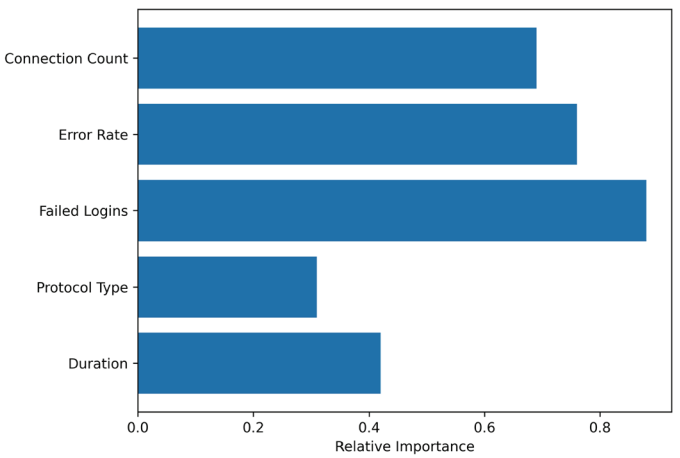

Figure 3. *Relative contribution of selected network traffic features to the logistic regression intrusion detection model. Features include protocol type, connection duration, failed login attempts, server-side error rate, and connection count.*

DISCUSSION

This study demonstrates the potential of network traffic features to predict intrusion attempts within a scope of controlled benchmark dataset. With a limited set of interpretable network-level variables, high classification accuracy was achieved the logistic regression model. This supported the hypothesis established in this study that quantitative modeling may enhance intrusion detection without complex or opaque algorithms. These findings also support the value of mathematically transparent approaches in the field of cyber-security, especially for educational contexts where interpretability is important.

According to the strong performance of the model proposed in this study, the relevance of specific network indicators was highlighted in identifying abnormal behaviors. Seeing as how features related to authentication failures, error rates, and traffic volume were particularly informative, they reflected how known characteristics of malicious activity, such as brute-force attacks and network scanning may be identified by such features. With the high precision reported in the model, a low rate of false positives was indicated as a critical component for maintaining trust in intrusion detection systems, while avoiding alert fatigue among security analysts. At the same time, according to the model's recall, it was suggested that the majority of intrusion attempts were successfully identified, even if some attacks remained undetected.

The trade-off between false positives and false negatives is important when considering the applications in cyber-security. With minimized false positives, unnecessary alerts may be reduced. At the same time, false negatives may be more costly since data breaches or system compromise may be caused by undetected intrusions. The results in this study suggest how a reasonable balance between these two error types may be achieved by a regression-based model. Furthermore, a practical mechanism may be provided by adjusting the classification threshold in tailoring detection behavior to particular priorities in security.

Several limitations need to be considered when interpreting the findings. First, the NSL-KDD dataset shows simulated benchmark data instead of contemporary real-world network traffic. Second, a single logistic regression model was used for the analysis with a limited set of predictors. This may not capture all relevant attack characteristics. Third, the absence of cross-validation or separate training and testing datasets may generate the risk of over-fitting although the dataset provides labeled instances. Lastly, the study did not provide the comparison between the regression model used in the analysis with alternative machine learning algorithms that may provide additional performance benchmarks.

CONCLUSION

This study used a logistic regression modeling framework and examined the effectiveness of selected network traffic features to detect cyber intrusions. With publicly available intrusion data and a small set of interpretable network-level variables, this study proposed a logistic regression model to achieve high predictive accuracy. This demonstrated how meaningful intrusion detection may be achieved without applying highly complex algorithms. The findings in this study supported the hypothesis that network traffic features, including connection duration, protocol type, failed login attempts, error rates, and traffic volumes were strong predictors of abnormal traffic-related behaviors.

With mathematical transparency and reproducibility, this study underscores the value of simple quantitative framework in the field of cyber-security research and education. Even if the analysis in this study was based on a benchmark dataset, the findings suggest how regression-based approaches may be effective in identifying and interpreting intrusion detection. It is recommended for future study to extend this framework by applying more features or assessing performance in the real-world network data.

CONFLICT OF INTEREST

The author declares no conflicts of interest related to this work.

REFERENCES

1. World Economic Forum. Global cybersecurity outlook 2024. Geneva (CH): World Economic Forum; 2024. Available from: https://www.weforum.org/reports/global-cybersecurity-outlook-2024 (accessed 2025-01-22)
2. International Monetary Fund. Rising cyber threats pose serious concerns for financial stability. IMF Blog. 2024 Apr 9. Available from: https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability (accessed 2025-01-11)
3. Sommer R, Paxson V. Outside the closed world: on using machine learning for network intrusion detection. In: Proceedings of the IEEE Symposium on Security and Privacy; 2010 May; Oakland (CA). Piscataway (NJ): IEEE. 2010; p.305-316. https://doi.org/10.1109/SP.2010.25
4. Chandola V, Banerjee A, Kumar V. Anomaly detection: a survey. *ACM Comput Surv*. 2009; 41 (3): 1-58. https://doi.org/10.1145/1541880.1541882
5. Patcha A, Park JM. An overview of anomaly detection techniques: existing solutions and latest technological trends. *Comput Netw.* 2007; 51 (12): 3448-3470. https://doi.org/10.1016/j.comnet.2007.02.001
6. Ahmed M, Mahmood AN, Hu J. A survey of network anomaly detection techniques. *J Netw Comput Appl*. 2016; 60: 19-31. https://doi.org/10.1016/j.jnca.2015.11.016
7. Carrier B. File system forensic analysis. Boston (MA): Addison-Wesley; 2005.
8. Casey E. Digital evidence and computer crime: forensic science, computers, and the internet. 3rd ed. London (UK): Academic Press; 2011.
9. Menard S. Applied logistic regression analysis. 2nd ed. Thousand Oaks (CA): Sage Publications; 2002. https://doi.org/10.4135/9781412983433
10. Hosmer DW, Lemeshow S, Sturdivant RX. Applied logistic regression. 3rd ed. Hoboken (NJ): Wiley; 2013. https://doi.org/10.1002/9781118548387
11. Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Commun Surv Tutor*. 2016; 18 (2): 1153-1176. https://doi.org/10.1109/COMST.2015.2494502
12. Axelsson S. Intrusion detection systems: a survey and taxonomy. Technical Report No. 99-15. Gothenburg (SE): Chalmers University of Technology; 2000.
13. Tavallaee M, Bagheri E, Lu W, Ghorbani AA. A detailed analysis of the KDD Cup 99 dataset. In: Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications; 2009 Jul; Ottawa (ON). Piscataway (NJ): IEEE; 2009; p.1-6. https://doi.org/10.1109/CISDA.2009.5356528