Vol. 16 (2026): Proceedings of the 2026 International Conference on AI and Technological Innovation Applications (AITIA 2026)
E-ISSN: 3105-0522 P-ISSN: 3105-0514
DOI: https://doi.org/10.70267/aitia.2026194199

A Theoretical Analysis of Feature Selection Methods in Machine Learning-Based Intrusion Detection Systems

Junlin Yao*

College of Information, University of Maryland, Maryland, United States

**Corresponding author: Junlin Yao.*

Abstract

With the increasing complexity of the network environment, more and more machine learning-based Intrusion Detection Systems (IDS) are now being applied to identify unusual behaviour in network traffic. Many Dimensions and excess Redundancy reduce Detection Accuracy and Computation Efficiency. Therefore, to enhance the generalisation power of the model, feature selection can be employed. This paper offers theoretical research on feature selection for machine learning-based intrusion detection systems. Systematically review the traditional machine learning algorithms of Support Vector Machines (SVM), Decision Trees, Random Forests, etc., and explore their applications in intrusion detection. The three categories of feature selection are shown in more detail below: filter methods, wrapper methods and embedded methods. The change in detection accuracy and false-positive rate, as well as computational efficiency and model stability, are all related to feature selection. The study shows that feature selection plays a critical role in improving intrusion detection performance by reducing dimensionality, eliminating redundant features, and enhancing model generalization. The aim of this paper is to provide comprehensive theoretical support for the investigation of cooperation between feature selection methods and machine learning models in intrusion detection systems, and to offer a new reference for future research on high-efficiency and intelligent cybersecurity solutions.

Keywords

intrusion detection system (IDS), machine learning, feature selection, cybersecurity, anomaly detection

1. Introduction

With the rapid development of Internet technology, both cloud computing and the Internet of Things (IoT) have grown in scale and complexity to a certain extent, thus increasing network traffic [1]. At the same time, cyberattacks are increasingly varied, covert and advanced. The former kind of intrusion detection system (IDS) has developed a rule and signature database, which can only detect existing types of attacks and not unknown new ones [2]. The above methods are prone to reduced detection accuracy and a high rate of false positives in large-scale and dynamic network environments. Therefore, in recent years, many large-scale research projects have been launched to improve the flexibility and stability of IDS in cybersecurity [2].

In recent years, many ML methods have been used to detect network intrusions by learning from data and identifying abnormal behaviours in the data. Train models on network traffic to improve the automation of

detection and expand the scope of recognising new attacks with machine learning. SVM, Decision Trees, Random Forests, K-Nearest Neighbors (KNN) and neural networks are some typical algorithms. The above ways have shown good results in attack classification and anomaly detection tasks [4]. However, the network traffic data is usually high-dimensional, redundant and noisy. Irrelevant or redundant features will increase the computational cost and may lead to overfitting; therefore, they will reduce the accuracy and generalisation ability of the model.

Therefore, many ML-based intrusion detection systems are now using feature selection. Feature selection aims to find a relatively small, highly informative set of features by eliminating redundant and less useful ones to reduce the dimensionality of data. Feature selection keeps the original semantic meaning of the features and is thus more interpretable than feature extraction. The three categories of existing methods are filters, wrappers and embedded methods. Statistical measures are used in filter methods to evaluate features and are relatively easy to compute; wrapper methods select a subset of features based on model performance but are computationally intensive; embedded methods incorporate feature selection during the training process of the model and are both efficient and accurate [6]. Feature selection methods and ML models interactively affect the performance of IDS in practice. Some Problems have arisen in recent years. Existing methods lack uniformity in the data and are not generalizable. Many of the above are not suitable for a changing network environment. Deep learning models can handle high-dimensional data well; however, they are generally computationally expensive and less interpretable. As both the amount of encrypted traffic and the number of IoT devices have increased, so too have the traditional problems of feature selection methods. Therefore, the following studies will examine the effects of various feature selection methods on machine learning models. This paper will offer a theoretical basis for feature selection in machine learning-based intrusion detection, introduce the current methods and their characteristics, and explore how they are used with various learning models. Finally, the paper presents current deficiencies and suggests future directions for research to advance the development of high-efficiency, intelligent intrusion detection systems.

2. Machine Learning and Feature Selection Theory

2.1 Intrusion Detection and Machine Learning

A NIDS observes network data to detect unauthorised access and policy violations in a computer network. Traditionally, the rules and signatures of Intrusion Detection Systems (IDS) only cover known attacks, and thus are unable to address new threats or frequent changes in attacks. Given the rising scale and sophistication of cyberattacks, the above approaches are no longer feasible [2].

Machine learning has recently been applied to the problem of anomaly-based intrusion detection to learn data patterns and generalize these to new, unknown samples. Train a machine learning model on historical network traffic data to distinguish between normal and abnormal behaviour, and thus build an adaptable detection system. Machine learning-based IDS have shown better detection accuracy and require less manual feature engineering compared to rule-based systems.

Several classical machine learning algorithms are commonly used for intrusion detection. SVMs are good at handling high-dimensional spaces and have been widely applied to binary and multi-class classification tasks due to their strong generalization ability [7]. Decision Tree models can be used to build understandable decision rules and are also computationally inexpensive, suitable for real-time detection applications. Random Forest is an ensemble learning method that builds multiple decision trees and reduces the risk of overfitting through these trees. The above algorithms serve as the foundation for many older ML-based intrusion detection systems.

2.2 Feature Selection Theory

Feature selection aims to select the most relevant features from the original dataset while removing redundant and irrelevant information. Existing feature selection methods can generally be categorized into filter, wrapper, and embedded methods.

2.2.1 Filter Methods

Filter methods assess the importance of features using statistics and do not employ machine learning models. Information Gain (IG) is used to measure how much entropy is reduced by adding a feature [8].

Information Gain (IG) is the reduction in entropy after adding a feature. It can be shown as follows:

$$IG(D, A) = H(D) - H(D|A) \tag{1}$$

where H(D) represents the entropy of dataset D, and H(D|A) denotes the conditional entropy after feature A is applied. A higher information gain indicates that the feature contributes more to classification.

2.2.2 Wrapper Methods

Wrapper methods evaluate subsets of features through multiple trainings of machine learning models. RFE is a common wrapper method that successively removes the less important features [9].

The optimised objective function is as follows:

$$S^* = \arg\max_{S \subseteq F} \quad Acc(f(S)) \tag{2}$$

In this formulation, f represents the complete set of original features, while S denotes a candidate subset such that $S \subseteq F$. The term $Acc(f(S))$ signifies the performance metric (e.g., classification accuracy) achieved by the model f when trained specifically on subset S. Although wrapper methods often achieve better predictive performance by considering feature interdependence, they are relatively more computationally expensive than the other methods because they need to train and test the model repeatedly for each candidate subset.

2.2.3 Embedded Methods

Embedded Methods include feature selection within the training of a model. The above are reasonably efficient and high-performance methods [10]. LASSO (Least Absolute Shrinkage and Selection Operator) is a typical example that adds an L_1 penalty to reduce the weights of less important feature coefficients to zero. Another popular way is Random Forest-based feature importance, which assesses how much each feature reduces impurity or increases information gain in the decision trees.

2.3 Role of Feature Selection

Feature selection helps to enhance both the accuracy and speed of the intrusion detection system based on machine learning. As the number of features in a network traffic dataset is usually relatively large, and many of them may be irrelevant or redundant, directly using all features can increase computational cost and harm the accuracy of detection. Therefore, some of the characteristic features can be taken as the starting point for the field of intrusion detection research.

First, Feature Selection helps to reduce the dimensions of the dataset. High-dimensional network traffic data is computationally expensive to train and test models on. Remove some unnecessary attributes to reduce the amount of data storage and speed up model training; otherwise, it would be infeasible to operate a large-scale network-based real-time intrusion detection system.

Second, the features help to reduce noise and redundant information in the data. Some network features may contain irrelevant or redundant data that interferes with the training of a machine learning model. Therefore, the model will be more focused on patterns of malicious behaviour and less affected by extraneous factors.

Third, to improve classification efficiency and detection accuracy, select features. Focus on the most distinctive characteristics and thus learn general patterns from the data via machine learning. Improve the accuracy of attack detection and reduce both false positives and false negatives. The amount of network traffic and serious cybercrime has risen, so a new high-performance network device must be introduced.

Feature selection helps prevent overfitting by reducing unnecessary and irrelevant features, thus improving the generalisation ability of machine learning models to new data. It is also more interpretable than a complex model, and a smaller set of features related to the attack can be understood and analysed more easily.

3. Analysis of Intrusion Detection Models Based on Feature Selection

3.1 Relationship Between Feature Selection and Model Performance

The selection of features may reduce the accuracy of an intrusion detection system based on machine learning. Machine learning algorithms are affected differently by various extents of the input features; therefore, selecting different features will result in different classification results [11]. SVM are particularly susceptible to overfitting in the presence of irrelevant and redundant features due to the high dimensionality of the data; thus, increased computation cost and reduced classification accuracy may result [7]. Decision Tree models are relatively insensitive to redundant features, but an excessive amount of noise will also harm the quality of the decision boundary. Random Forest models are relatively stable because they use ensemble learning, but feature optimisation can still enhance both the accuracy and robustness of the detection.

Select some good features to enhance the quality of the training data by including only the most representative attributes of attack behaviour. Optimal feature subsets can help the machine learning model learn more typical traffic patterns to improve the detection rate and stability of the model. Reducing the number of features will also decrease training time and computation; thus, for real-time intrusion detection in a large network, this is necessary.

3.2 Impact of Feature Selection on Intrusion Detection

Feature selection directly impacts the real-world performance of an intrusion detection system in a real network. Select traffic features that are more likely to help the machine learning model focus on attack-related patterns and improve the detection accuracy.

The first will be increased detection accuracy. For example, in the detection of distributed denial-of-service (DDoS) attacks, features that can distinguish between malicious behaviour and normal behaviour include the rate of packet transmission, connection duration and traffic volume, etc [12]. The above representative features can be used by a machine learning model to distinguish between malicious and normal traffic more accurately. Feature Selection can also reduce the false positive rate. In phishing or abnormal login detection, some features are irrelevant and thus will be mistaken for attack behaviour by normal users. By excluding noisy and redundant attributes, the model will be more stable in classifying, and thus fewer spurious security alerts will be raised by the system.

Select some features to improve the speed of the intrusion detection system in real time. IoT devices and edge computing environments are generally low-power in terms of computation. Reduce the number of processed features to lower memory consumption and computational overhead for a high-speed, low-resource intrusion detection and response system.

Optimised feature subsets can also help adapt the intrusion detection system to changes in the network. For example, in a cloud computing environment with fluctuating traffic, a selection should be made of more representative and stable features to keep the detection performance of a machine learning model consistent under all network conditions. Feature selection can improve the detection accuracy of a system and at the same time increase the efficiency, stability and real-world applicability of an intrusion detection system.

3.3 Current Challenges in Existing Research

Many defects in the development of intrusion detection systems (IDS) have been addressed by feature selection so far. First, many existing methods have been evaluated on old benchmark datasets such as KDD Cup '99 and NSL-KDD that do not reflect modern network environments, encrypted traffic and IoT-based behaviour [13]. Therefore, feature subsets optimised under static conditions often show poor generalisation in real-world situations. Second, feature selection methods are not stable; that is, the best-fitting subset of features may change depending on both the data and the learning model. The features that are optimal in one scenario may not be consistently effective with other classifiers or under changes in the network. Third, the existing methods are unable to detect zero-day and new types of attacks. Traditional methods are based on old patterns and may not be able to identify new or modified attack behaviour that is not included in the original feature space. Finally, speed of calculation and detection accuracy are in a trade-off relationship. Wrapper and

embedded methods are generally too computationally intensive for real-time applications, and filter methods may neglect feature dependencies and thus reduce the robustness of detection.

4. Discussion

Currently, both deep learning and feature selection are being jointly employed in research. Deep learning models can automatically extract rich traffic features, and then feature selection methods are used to reduce redundant information and computational load. The two will work together to enhance the accuracy and speed of the model. Deep learning models are generally computationally intensive and less interpretable, so they have been applied to cybersecurity systems less frequently. The other way is dynamic feature selection. Dynamically select different features based on the current state of the network and the characteristics of an attack, rather than using a fixed list. It will be more practical for the intrusion detection system to use in actual operation. At the same time, with the expansion of IoT devices and edge computing, there is now an increased demand for light-weight intrusion detection models.

In the future, the system needs to be both accurate in detection and computationally light so that it can work in a resource-limited real-time environment. Recently, many security research teams have started to use interpretable AI. Enhance the interpretability of the intrusion detection model to enable security analysts to understand the reasons for the model's judgments better, increase trust in machine learning-based systems, and so on. Therefore, future study will improve the detection effect and also consider the simplicity of the model.

5. Conclusion

This paper offers a theoretical study of feature selection for machine learning-based intrusion detection systems. First, machine learning algorithms such as SVM, Decision Trees and Random Forests have been applied to network intrusion detection in previous studies, and they have demonstrated good performance in handling high-dimensional and complex network traffic data. Next, the three types of feature selection will be introduced in order: filter methods, wrapper methods and embedded methods, and their corresponding mathematical foundations and representative technologies. In addition, this paper will examine how feature selection improves the performance of models and determine how to reduce false positives, increase computational speed, and enhance the generalisation ability of the model by removing redundant or irrelevant features. Feature selection and machine learning models are also discussed here, and it has been shown that an optimised subset of features can improve both the stability and generalisation ability of detection in dynamic network environments.

Only theoretical foundations will be presented in this paper, and no large-scale experiments based on real or substantial modern network traffic data will be carried out. In the future, adaptive and lightweight feature selection methods can be combined with deep learning and explainable artificial intelligence (XAI) to enhance the robustness, interpretability and real-time performance of intrusion detection systems in the face of new cyber security threats.

References

[1] Dhingra, S., Madda, R. B., Patan, R., Jiao, P., Barri, K., & Alavi, A. H. (2021). Internet of things-based fog and cloud computing technology for smart traffic monitoring. Internet of Things, 14, 100175.

[2] Abdulganiyu, O. H., Ait Tchakoucht, T., & Saheed, Y. K. (2023). A systematic literature review for network intrusion detection system (IDS). International journal of information security, 22(5), 1125.

[3] Almotairi, A., Atawneh, S., Khashan, O. A., & Khafajah, N. M. (2024). Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models. Systems Science & Control Engineering, 12.

[4] Boateng, E. Y., Otoo, J., & Abaye, D. A. (2020). Basic tenets of classification algorithms K-nearest-neighbor, support vector machine, random forest and neural network: A review. Journal of Data Analysis and Information Processing, 8(4), 341-357.

[5] Xu, D., Lv, Y., Wang, M., Zheng, B., Zhao, J., & Yu, J. (2025). Demgan: a machine learning-based intrusion detection system evasion scheme. Computers, Materials, & Continua, 84(1), 1731.

[6] Chen, C. W., Tsai, Y. H., Chang, F. R., & Lin, W. C. (2020). Ensemble feature selection in medical datasets: Combining filter, wrapper, and embedded feature selection results. expert systems, 37(5), e12553.

[7] Doğan, Ü., Glasmachers, T., & Igel, C. (2016). A unified view on multi-class support vector classification. Journal of Machine Learning Research, 17(45), 1-32.

[8] Saheed, Y. K., & Hambali, M. A. (2021, October). Customer churn prediction in telecom sector with machine learning and information gain filter feature selection algorithms. In 2021 International Conference on Data Analytics for Business and Industry (ICDABI) (pp. 208-213). IEEE.

[9] Nnamoko, N., Arshad, F., England, D., Vora, J., & Norman, J. (2014). Evaluation of filter and wrapper methods for feature selection in supervised machine learning. Age, 21(81), 33-2.

[10] Bashir, S., Khattak, I. U., Khan, A., Khan, F. H., Gani, A., & Shiraz, M. (2022). A novel feature selection method for classification of medical data using filters, wrappers, and embedded approaches. Complexity, 2022(1), 8190814.

[11] Ngo, V. D., Vuong, T. C., Van Luong, T., & Tran, H. (2024). Machine learning-based intrusion detection: feature selection versus feature extraction. Cluster Computing, 27(3), 2365-2379.

[12] Ali, M. H., Jaber, M. M., Abd, S. K., Rehman, A., Awan, M. J., Damaševičius, R., & Bahaj, S. A. (2022). Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT). Electronics, 11(3), 494.

[13] Shehadeh, A., ALTaweel, H., & Qusef, A. (2023, December). Analysis of data mining techniques on KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets for intrusion detection. In 2023 24th International Arab Conference on Information Technology (ACIT) (pp. 1-6). IEEE.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgment

This paper is an output of the science project.

Open Access