Proposing a Hierarchical Classifier to Detect Attack in Network Intrusion Detection

Amin Shahraki Moghaddam[1], Javad Hosseinkhani[1], Anoosh Mansouri Birgani [1], Amirreza Sardarzadeh [2], Zeynab Sayad Arbabi[1], and Sadegh Gilani[1]
Department of Computer, Zahedan Branch, Islamic Azad University, Zahedan, Iran[1]
Zahedan, Iran
Department of Computer, Damavand Branch, Islamic Azad University, Damavand, Iran[2]
Damavand, Iran

Summary
The task of intrusion detection system intrusion detection and disclosure practices are responsible. This system monitors network traffic and reports by user activity, detects illegal activities. Detect, identify and classify classes of attacks on computer networks, one of the major challenges in the field of intrusion detection is to determine the type of attack class. Neural networks, support vector machines and Bayesian networks as a classifier to classify and identify the type of attacks are used. Many researches have been conducted using a combination of the classifier. This classifier with putting together several different classifiers to detect attacks that are used to determine the type.be used as it is challenging. The classifier of support vector machine and a neural network classifier to determine the best of each class have detected the attack. And also the best way to arrange those bands that plays a big part in yield is proposed. Simulation results show that the proposed classifier can improve the classification performance better than similar acts.

Keywords:
Intrusion Detection, Support Vector Machine (SVM), Neural Network, Hierarchical Classifier.

1. Introduction

The intrusion detection is processing to detect unauthorized attempts to access a network or decrease its performance. In intrusion detection must first understand how the attacks were carried out. Thus by obtained understanding there is a two-step method to stop it. The first one is detecting the pattern of dangerous activities then ensure that those activities are classified in safe categories not attacks category. That's why most of intrusion detection systems rely on a mechanism to update their software to act against network threats fast enough. Of course, intrusion detection alone is not good enough and attack should be followed to track the hacker in order to dealt with him appropriately.

Intrusion is the act to violate a security component such as confidentiality, integrity and availability from breach in a system or application. Intrusion detection system has the task of discovering and exposing the attacker's actions. The system detects unauthorized activities by monitoring network traffic and user activity reports. Detection, detecting the type of classification and classification of attacks on computer networks is one of the major challenges in the field of intrusion detection and determining the type of attack class.

Neural networks, support vector machines and Bayesian networks as classifier are used to classify and identify the type of attacks. A number of researches were carried out on the field of using these classifiers combined. These classifiers are used by putting together several different classifiers for detecting and determining the type of attack. Classification accuracy, reducing false alarms and increasing appropriate warning rates can be noted as evaluating criteria of an efficient classifier in attack detection and determining its type. Using what type of classifier for detecting and determining the class of a particular attack is always noted as a challenge.

In this study the most important challenges and criteria of an efficient classifier in detecting and determining the type of investigated attack and a way to classify and determine the type of attacks is suggested as hierarchically and hybrid. The proposed classifier method for each class, for put attacks consecutively together so that the output of each classifier (Failure to detect attack) would be the entrance of next classifier. By simulations done in MATLAB environment on support vector machines and neural networks classifiers, the very best of each classifier for each class of attack were detected. The best way to arrange classifiers to have an effective performance have suggested. The simulation results indicate that the proposed classifier can act better in improving the classification compared to similar cases.

2. Related Works

Prasad et al. [1] presented a model for intrusion detection systems to identify anomalies. This model is based on fuzzy association rules which use genetic programming systems. In this paper, Apriori algorithm is used for rule production and by using this algorithm, high

Manuscript received April 5, 2025
Manuscript revised April 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.4.15

confidence and support rules will be extracted. After extracting rules, fuzzy inference engine and linear genetic programming algorithm will be used to improve the usage methods. Since Apriori algorithm is first level algorithm, its run-time is high and is not suitable for high-volume data.

Bridge and Rayford [2] have suggested an example of intelligent intrusion detection system that reflects the influence of data mining techniques that benefit fuzzy logic. This system has combined two distinct approach of intrusion detection. 1) Non-conventional intrusion detection using fuzzy data mining techniques 2) misuse detection using traditional rule-based expert system techniques.

Network-based intrusion detection system which uses abnormalities and BP and PBH neural networks method were used. The different layers of the system which include of the probe, traffic pre-processor and neural networks are separately examined in [3] and the test results of BP and PBH neural network show that the PBH network by having less hidden neurons has a lower error notification rate and thus more efficient than BP network and also by reducing the number of hidden neurons in BPH network, calculation cost in this network is reduced as well and tests [3] shows that using BPH neural network as classifier in anomaly approach intrusion detection system based on network is cost-effective and high performance and can be replaced with BP neural network.

Koc et al. [4] have used hidden Bayesian model for intrusion detection. Hidden Bayesian model is a developed model of simple Bayesian model that unlike simple Bayesian model assumes data attributes are dependent. In other words, hidden Bayesian model is a type of Bayesian network. As proven, learning the structure of Bayesian Network is an NP-hard problem, so methods have been proposed that solve this problem by applying some limitations. Hidden Bayesian model by creating another layer that is called hidden parent layer, try to extract the features that are dependent on each other. In fact, limiting assumption of this model -to Bayesian network- is that each feature is only dependent on one feature. Weakness of Bayesian classification method is on access to data possibilities, but simple implementation with high precision and high speed when data volume is high, always note as the advantage of this method. [5]

Court and colleagues [6] have presented an intrusion detection learning algorithm based on Bayesian network classifiers and clustering. In the proposed algorithm, first data on the basis of doubts on each of their attribute is clustered and then attack class of each stream using a classifier based on the level of each cluster belonging divides to 4 defined attack classes. This algorithm is appropriate for large data volumes and audit data.

Toosi, Nadjaran and Kahani [7] have proposed a model based on fuzzy-neural classifier and fuzzy-neural classifier called ANFIS had been considered for four types of attacks and one normal mode. Input data which are 41 features of a stream send to each attack and normal ANFIS that the output of each one of them is a fuzzy number that is indicative of the amount of stream belonging to each of attack or normal classes. Slow learning and high computational load especially when data volumes are high can be noted as disadvantages of classifying methods based on neural networks. [5]

Jennifer and Carla [8], is to find the best set of attributes without the presence of outside observers. In this way, first based on forward search algorithm, subset of attributes is selected. Then data sets by using clustering algorithm and elected subset is clustered. Finally, clustering precision will be evaluated. This process is repeated several times until the clustering with the best standard is achieved. The advantage of this method is that it can apply to all kinds of numerical and non-numerical data but this method may not always find the best set attribute because it depends on the initial selected subset.

Jafari and Abolhassani [7] used proposed method in article [9] in order to rank the attributes. Thus, by removing one attribute, the quality of clustering will be measured. The lower quality that removing an attribute gives to clustering, the more importance that clustering gains. The density and distribution criteria are used for examining the quality of clustering

3. Proposed Work

The proposed overall diagram block system is indicated in Figure 1. We want to work with five classes and four classifiers. First classifier detects the type of DOS attacks and if an attack is DOS type, it will have an output, and if not, gives it to the next classifier to detect which is Probe classifier. As well as the rest goes and if there is no attacks at the final output, it will be detected as normal type.

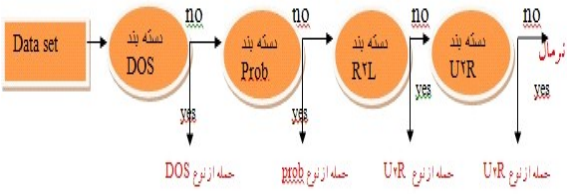

Fig. 1 Overall diagram of proposed detection system.

In this study, three different classifiers instead of each classifier will be used and each result will be presented. Table 1 shows the results of each category.

Table 1: Results of the proposed method.

Detection Percentage	*Classifier*
74.6629	MLP Neural Network
75.1153	Support Vector Machine
75.2079	Neurofuzzy System

In another experiment the priority of classifiers are tested. We put four classifiers in series. These four state classifiers can be placed next to each other therefore we have 24 states that each state results is shown in Table 1.

Table 2: The relationship between the classifier sequence and detection percentage.

Class 1	*Class 2*	*Class 3*	*Class 4*	*Detection Percentage*
PROBE	R2L	U2R	DOS	51.6900
PROBE	R2L	DOS	U2R	76.9562
PROBE	U2R	R2L	DOS	51.7033
PROBE	U2R	DOS	R2L	75.0177
PROBE	DOS	U2R	R2L	74.9956
PROBE	DOS	R2L	U2R	76.9429
R2L	PROBE	U2R	DOS	51.7033
R2L	PROBE	DOS	U2R	76.9695
R2L	U2R	PROBE	DOS	51.7033
R2L	U2R	DOS	PROBE	70.9191
R2L	DOS	U2R	PROBE	70.8969
R2L	DOS	PROBE	U2R	77.6482
U2R	PROBE	R2L	DOS	51.7033
U2R	PROBE	DOS	R2L	75.0177
U2R	R2L	PROBE	DOS	51.7166
U2R	R2L	DOS	PROBE	70.9324
U2R	DOS	R2L	PROBE	70.9191
U2R	DOS	PROBE	R2L	75.6964
DOS	PROBE	R2L	U2R	77.6215
DOS	PROBE	U2R	R2L	75.6742
DOS	R2L	PROBE	U2R	77.6348
DOS	R2L	U2R	PROBE	70.8836
DOS	U2R	R2L	PROBE	70.8969
DOS	U2R	PROBE	R2L	75.6742

4. Evaluation of Proposed Method

To understand the power of proposed method classifying, we compare this method with two of previous methods. In reference [10] an intrusion detection system for intrusion detection and normal mode has been introduced. Since this paper used neuro-fuzzy system for classification thus is very appropriate for comparison with our method. The proposed method is consists of five neuro-fuzzy system.

Each neuro-fuzzy system is trained to detect a variety of attacks Input is applied to all systems and each system has an output and the final output can be found by finding the maximum output. In other words, the proposed method in parallel and our method is in series. The main input in our method comes to the first category and this classifier output goes to the second classifier but in the method proposed in this paper, the main input goes to all classifiers and all of their outputs will be maximum-making. The detection percentage of this method for test data is 72.29.

In reference [11] proposed method diagram block in this paper is shown in Figure 2. RBF neural network and support vector machine (SVM) were used together. A RBF neural network is used to U2R attack detection and a support vector machine used to detect DOS attack. If any of these were not detected as attacks, a SVM-RBF hybrid model is used to normal detection. Finally, another hybrid model is used to detect Probe attack and if none of them is detected as attack then R2L will detect the attack. The ultimate detection result with this method is 55.25.

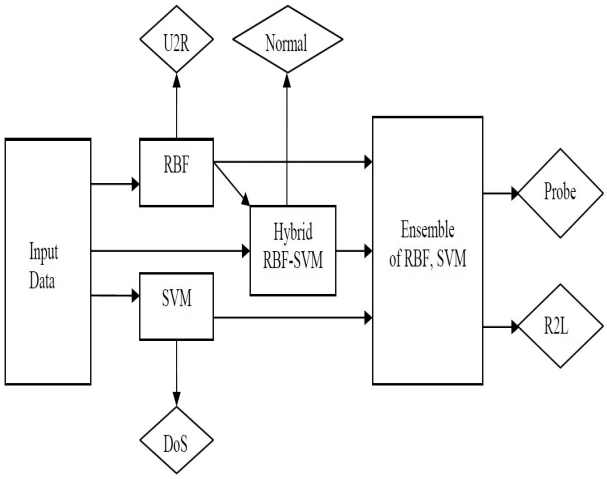

Fig. 2 The proposed method Block Diagram [11].

Table 3: Comparison of proposed method.

Detection Percentage	*Method*
72.29	[5]
55.25	[11]
77.65	Proposed Method

5. Conclusion

In this study, we examine the issues related to classification to detect attack types on computer networks and review the works done in this field along with the raised challenges. After that, according to the capabilities of the combined classifier and classifiers based on SVM, we reviews the possibility of using them in the intrusion detection in computer networks (data stream) and raised two important issues along this way. Major challenges in the discussion of classification of data stream are discussions related to time and memory requirements and speed of detection and accuracy in detecting attack type and normal mode and low rates of error in detecting that in the proposed method first we implement the classifier based on SVM with different kernels to measure the detection accuracy of each one of them. Results showed:

1. To detect DOS attack, polynomial kernel has showed better performance.
2. To detect U2R attack, linear kernel showed better performance.
3. To detect L2R attack, linear kernel showed better performance.
4- To detect PROBE attack, polynomial kernel showed better performance.
5. To detect normal mode, linear kernel showed better performance.

Therefore it can be concluded that in proposed system we can use SVM with a kernel mentioned above to detect every type of attacks for each attack classifier. A new way has been provided to classify the stream in network in order to detect and determine the type of attack. Neuro-fuzzy system in comparison with neural networks and support vector machine in separate classifier had the highest percentage of detection. The detection rate was 75.21. The proposed system in this study showed 77.65 percent of detection that indicate when the hybrid system is used, detection rate will be increased. On the other hand the arrangement of the various classifiers were obtained by testing, 4 different modes and comparison, the detection precision of each are shown respectively. In comparison of classifiers it showed that the classifier arrangement should be respectively to have the highest detection percentage, first R2L classifier, second DOS classifier, third PROBE classifier and fourth U2R classifier.

Acknowledgments

This research is funded by the Zahedan Branch in Islamic Azad University, Zahedan, Iran. The authors would like to thank the Research Management Centre of Islamic Azad University-Zahedan Branch and cooperation including students and other individuals who are either directly or indirectly involved in this project.

References

[1] Guntur, Gudlavalleru Guntur Rajamandry. "Modeling an intrusion detection system using data mining and genetic algorithms based on fuzzy logic." IJCSNS 8, no. 7 (2008): 319.

[2] Bridges, Susan M., and Rayford B. Vaughn. "Intrusion detection via fuzzy data mining." In 12th Annual Canadian Information Technology Security Symposium, pp. 109-122. 2016.

[3] Koc, Levent, Thomas A. Mazzuchi, and Shahram Sarkani. "A network intrusion detection system based on a Hidden Naïve Bayesian multiclass classifier." Expert Systems with Applications 39, no. 18 (2012): 13492-13500.

[4] Horng, Shi-Jinn, Ming-Yang Su, Yuan-Hsin Chen, Tzong-Wann Kao, Rong-Jian Chen, Jui-Lin Lai, and Citra Dwi Perkasa. "A novel intrusion detection system based on hierarchical clustering and support vector machines." Expert systems with Applications 38, no. 1 (2011): 306-313.

[5] Patel, Reema, Amit Thakkar, and Amit Ganatra. "A survey and comparative analysis of data mining techniques for network intrusion detection systems." International Journal of Soft Computing and Engineering (IJSCE) ISSN (2012): 2231-2307.

[6] Feng, Wenying, Qinglei Zhang, Gongzhu Hu, and Jimmy Xiangji Huang. "Mining network data for intrusion detection through combining SVMs with ant colony networks." Future Generation Computer Systems 37 (2014): 127-140.

[7] Asbagh, Mohsen Jafari, and Hassan Abolhassani. "Feature-Based Data Stream Clustering." In Computer and Information Science, 2009. ICIS 2009. Eighth IEEE/ACIS International Conference on, pp. 363-368. IEEE, 2009.

[8] Adhikary, Jyoti, and M. Narasimha Murty. "Feature selection for unsupervised learning." In Neural Information Processing, pp. 382-389. Springer Berlin/Heidelberg, 2012.

[9] Dash, Manoranjan, Kiseok Choi, Peter Scheuermann, and Huan Liu. "Feature selection for clustering-a filter solution." In Data Mining, 2002. ICDM 2003. Proceedings. 2002 IEEE International Conference on, pp. 115-122. IEEE, 2002.

[10] Toosi, Adel Nadjaran, and Mohsen Kahani. "A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers." Computer communications 30, no. 10 (2017): 2201-2212.

[11] Govindarajan, M., and R. M. Chandrasekaran. "Intrusion detection using an ensemble of classification methods." In Proc. of the World Congress on Engineering and Computer Science, vol. 1, pp. 459-464. 2012.