Computers, Materials & Continua
DOI:10.32604/cmc.2021.017502
Article

Tech Science Press

Unknown Attack Detection: Combining Relabeling and Hybrid Intrusion Detection

Gun-Yoon Shin[1], Dong-Wook Kim[1], Sang-Soo Kim[2] and Myung-Mook Han[3,*]

[1]Department of Computer Engineering, Gachon University, Sungnam-si, 13120, Korea
[2]Agency for Defense Development Songpa, Seoul, 05661, Korea
[3]Department of Software, Gachon University, Sungnam-si, 13120, Korea
[*]Corresponding Author: Myung-Mook Han. Email: mmhan@gachon.ac.kr
Received: 01 February 2021; Accepted: 11 March 2021

Abstract: Detection of unknown attacks like a zero-day attack is a research field that has long been studied. Recently, advances in Machine Learning (ML) and Artificial Intelligence (AI) have led to the emergence of many kinds of attack-generation tools developed using these technologies to evade detection skillfully. Anomaly detection and misuse detection are the most commonly used techniques for detecting intrusion by unknown attacks. Although anomaly detection is adequate for detecting unknown attacks, its disadvantage is the possibility of high false alarms. Misuse detection has low false alarms; its limitation is that it can detect only known attacks. To overcome such limitations, many researchers have proposed a hybrid intrusion detection that integrates these two detection techniques. This method can overcome the limitations of conventional methods and works better in detecting unknown attacks. However, this method does not accurately classify attacks like similar to normal or known attacks. Therefore, we proposed a hybrid intrusion detection to detect unknown attacks similar to normal and known attacks. In anomaly detection, the model was designed to perform normal detection using Fuzzy c-means (FCM) and identify attacks hidden in normal predicted data using relabeling. In misuse detection, the model was designed to detect previously known attacks using Classification and Regression Trees (CART) and apply Isolation Forest (iForest) to classify unknown attacks hidden in known attacks. As an experiment result, the application of relabeling improved attack detection accuracy in anomaly detection by approximately 11% and enhanced the performance of unknown attack detection in misuse detection by approximately 10%.

Keywords: Unknown attack; hybrid intrusion detection; fuzzy c-means; relabeling; CART; iForest

1 Introduction

The advances in IT technology have led to its ubiquitous use in various fields, including communication, social networking, IoT, and security, and there is an increasing number of

technologies especially integrating ML and AI. Although such development of IT technology has brought us many benefits, the number of technologies that malicious exploit it is also increasing. The zero-day attack, which attacks a vulnerability unknown to the public, including network system defenders, is one of the major challenges for computer network security as a representative technology exploiting advanced IT technologies [1]. A zero-day attack is composed of unknown attacks in which various malicious behavior take place and can evade detection by means of obfuscation [2].

Intrusion Detection (ID) generates alerts in case of suspicious behavior and known threats [3]. ID aims to detect abnormal behavior in a computer system. Recently, studies have been conducted on the application of ML and Data Mining (DM) to ID techniques. ID can be divided into three categories: anomaly detection, misuse detection, and a hybrid of the two techniques. In anomaly detection, when new data are entered into a system that has learned normal behavior, the system decides whether the new data are normal or abnormal based on the system's normal information criteria. In anomaly detection, ML applicable to clustering or a 2-class problem in classification is used. Misuse anomaly generates signatures and rules based on the previously known attacks and compares them with new data to check if they match each other. In misuse detection, ML applicable to a classification problem is often used. Although anomaly detection is suitable for the detection of new or unknown attacks, its disadvantage is that it cannot detect attacks similar to normal and also generates too many false alarms. Because misuse detection produces signatures or rules, it generates far fewer false alarms, but its disadvantage is that it can detect only known attacks [4].

Hybrid intrusion detection systems that combine anomaly detection with misuse detection have been proposed to overcome the disadvantages of both anomaly and misuse detection. A hybrid intrusion detection system is designed to overcome the problem of excessive false alarms about attacks in anomaly detection and the disadvantage of detecting only known attacks in misuse detection. Also, ML and DM are applied for the detection of unknown attacks [3,5–10]. However, these methods are also difficult to detect hidden attacks such as attacks like normal or unknown attacks similar to known attacks. Detecting hidden or unknown attacks requires additional analysis of the data classified through detection.

The present study proposed a hybrid intrusion detection model for identification of unknown attacks similar to normal and known attacks. In anomaly detection, FCM was used to classify normal and attack, and a relabeling technique was applied to identify attacks falsely classified as normal data. In misuse detection, CART was used for classification of known attacks, while iForest was applied to identify unknown attacks hidden in known attacks. This study aims to detect attacks falsely classified as normal by anomaly detection and to identify unknown attacks similar to known attacks to improve the accuracy of the intrusion detection. Most preceding studies on intrusion detection were conducted with a focus on improving the performance of a classifier, but we aim to reduce the ratio of falsely classified data in anomaly detection and misuse detection to enhance the accuracy of intrusion detection. In the experiment, the evaluation of the proposed hybrid intrusion detection model is performed.

Our paper makes the following contributions:

- In anomaly detection, we proposed a method to identify attack similar to normal;
- In misuse detection, we proposed a method to classify unknown attack similar to known attacks;

- We proposed hybrid intrusion detection methods to detect the unknown attack and evaluated its performance with accuracy, f-measure, and research and validation.

The rest of the paper is organized as follows: Section 2 introduces related works about hybrid intrusion detection and unknown attack detection, Section 3 presents a detailed explanation of our proposed hybrid intrusion detection. Section 4 introduces the results of the experiment, and the paper ends with Section 5, which presents our conclusions and future direction.

2 Related Work

In this section, representative hybrid intrusion detection and unknown attack detection are introduced. Most of the researches, combining misuse detection and anomaly detection based on ML.

2.1 Hybrid Intrusion Detection

The past research of ID proposed unknown attack detection as the identification of abnormal activities and the creation of rules for attacks and normal activities. However, most IDs generate too many false alarms and have a low detection accuracy. To overcome these problems, researchers propose a hybrid intrusion detection. This method attempts to complement the problems that anomaly detection and misuse detection have, thereby solving the problem of generating false alarms for large numbers of attacks that anomaly detection has and detecting only known attacks that misuse detection has. It improves detection performance, and also enables detection of unknown attacks contained in datasets.

In Khraisat et al. [3] propose intrusion detection using a Decision Tree (DT) and Support Vector Machine (SVM). DT was applied to effectively handle high-dimensional data, and a decision boundary was presumed by adding a relaxation parameter to each data sample in SVM to improve performance. Kim et al. [5] propose a detection system using DT and SVM for the detection of attacks. Traffics are captured to extract meaningful features, and DT is used to check whether they would belong to the existing attacks. SVM is used to classify those data found not to belong to the existing attacks into unknown attacks or normal. AlEroud et al. [6] propose a method that combined a misuse detection which used the context profile of an attack with an anomaly detection using 1-nn. In misuse detection, it creates a profile for an attack based on the past data using conditional entropy and checks matching with newly entered data. If their matching is not complete, anomaly detection is done based on 1-nn. Hussain et al. [7] propose a hybrid method integrating misuse detection based on DT with anomaly detection based on SVM. DT is used to create rules in known attacks, and SVM is used to create a boundary about normal for the detection of unknown attacks. Lekha et al. [8] propose a method to create rules and classify known attacks using CART, it uses an Extreme Learning Machine (ELM) for the classification of normal and abnormal activities. Bitaab et al. [9] propose a method to do misuse detection based on DT and anomaly detection based on a Gaussian Mixture Model for classification of normal and unknown attacks. Al-Yaseen et al. [10] propose an intrusion detection system based on SVM and ELM. Unlike the two-stage classifier of most hybrid intrusion detection, they propose a five-stage classifier for the detection of unknown attacks.

As such, hybrid intrusion detection methods improve performance by complementing the problems of anomaly detection and misuse detection with each other, and unknown attack detection is possible. However, it does not accurately detect hidden attacks such as attacks like normal or unknown attacks similar to known attacks. A method to overcome the false alarms problem in general hybrid intrusion detection is to reduce false alarm in anomaly detection by

classifying known attacks through misuse detection first, reducing known attack data. Because this approach is preprocessing of input data for anomaly detection, unknown attacks similar to normal or known attacks cannot be accurately detected.

2.2 Unknown Attack Detection

Detection of unknown attacks means detection of previously unseen attacks and their related data. The detection identifies how much an unknown attack is similar to which type of attack or checks the features of the unknown attack. The most representative method of its kind is anomaly detection. This method detects how much an unknown attack differs from normal, how much it is similar to other attacks, and how much it differs from other attacks.

Detection methods for unknown attacks are mainly divided into two. The first method is to create and detect unknown attacks and variants; attacks are usually created using Generative Adversarial Network (GAN) [11,12]. The advantage of this method is that because it generates unknown attacks, it can clearly detect attacks that are completely different from the previously collected attacks, but its disadvantage is that it is difficult to create a new attack and to find out whether the created attack could actually perform malicious behavior. The second method is to define a certain class of the collected dataset as an unknown attack. This method has been commonly applied by most studies. A study was carried out by specifying some classes of the collected dataset as unknown attacks and by removing labels on them. The advantage of this method is that various kinds of datasets can be used, and could be carried out on many different attack types. However, the limitation is that most of them were known attacks; so it is uncertain whether it could accurately detect an unknown attack that might actually occur in fields.

Hu et al. [11] propose malgan, which used a GAN to create adversarial attacks based on malware; they generate adversarial attacks using malgan and detect adversarial attacks. Kawai et al. [12] propose a method to improve the limitations of malgan, including the problem with the feature number and the use of various malware; they generate attacks using the proposed method and detected them. Liu et al. [13] propose a framework based on the Generative Adversarial Cooperative Network (GACN) for the detection of known and unknown attacks. K-means is used to execute the clustering of known and unknown attacks generated by GACN, and attacks are detected based on similarity. Lin et al. [14] propose a hybrid attack detection method based on short term memory and attention mechanism for unknown attack detection. Ji et al. [15] propose deeparmour, a model to detect attacks that differ from the existing attacks that might occur by transformation and poisoning of data. Huda et al. [16] propose a method to extract the features of classes using a semi-supervised method and use an improved SVM to identify an unknown attack. Duessel et al. [17] propose a model to detect attacks using a message within an application layer. It detects attacks using extraction and normalization of data in a message, feature extraction, similarity calculation, and anomaly detection. Lai et al. [18] propose opensmax for the detection of botnet attacks by combining open set recognition based on domain generation algorithms with openmax.

3 Hybrid Intrusion Detection Process

In this paper, we proposed a method to detect hidden unknown attacks based on hybrid intrusion detection, such as Fig. 1. In anomaly detection, we classified normal and attacks and used the membership degree of the FCM to detect attacks similar to normal contained within classified normal. Misuse detection exploited known attack classification and iForrest to classify

unknown attacks similar to known attacks hiding in them. Our system was based on three stages process:

- Stage 1: Anomaly detection using relabeling to detect hidden attacks
- Stage 2: Misuse detection using iForest to detect hidden unknown attacks

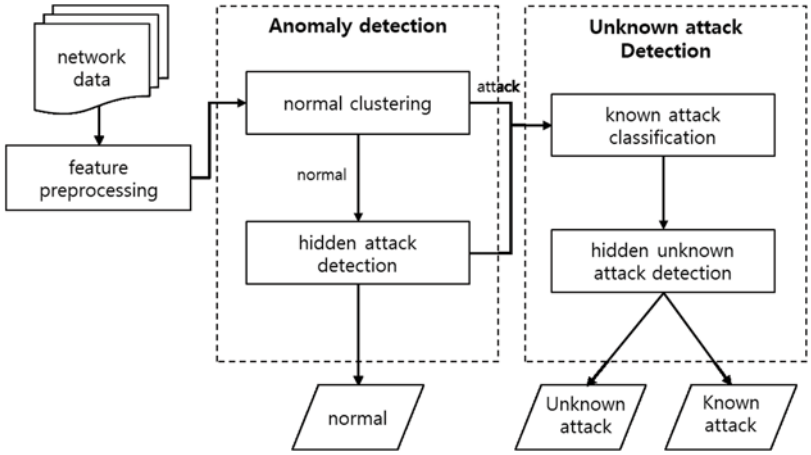

Figure 1: Processes of the proposed hybrid intrusion detection

3.1 Feature Preprocessing

In feature pre-processing, recursive feature elimination (RFE) was used to select important features [19]. RFE, one of the most widely used methods for feature selection, selects high influenced features in performing ML [20]. RFE removes the least important feature among all features one by one until a specified number of features is reached. It improves performance on models that perform machine learning-based learning. And we applied the minmax scaler to reduce the deviation of the values that each feature has.

3.2 Anomaly Detection for an Attack Similar to Normal

Detection of unknown attacks depends on how accurately it can classify normal and known attacks from data. In this stage, FCM was used for the classification of normal and attacks, and relabeling was applied based on a membership degree created in each cluster to detect an attack hidden in data classified as normal.

FCM is a soft-clustering method. Unlike hard clustering, in which each datapoint belongs to one cluster, FCM measures the membership degree of datapoint in each cluster. For instance, if there are three clusters, the membership degree of datapoint x in each cluster of c_1, c_2, and c_3 is expressed respectively as $c_1 = 0.2$, $c_2 = 0.65$, and $c_3 = 0.15$. The advantage of FCM is that it allows data to have a membership degree in each cluster, unlike other clustering methods that measure data as either 0 or 1; hence data can belong to more than two clusters with different membership degrees [21].

Each data is assigned a fuzzy membership function to each cluster. FCM aims to minimize object function, which can be measured using Eq. (1). m is the real number in a domain ($1 \leq m < \infty$); c is the number of clusters; n is the number of data samples; u_{ij} indicates the membership degree of data x_j in the jth cluster; and c_j is the cluster center.

$$J_m = \sum_{i=1}^{n} \sum_{j=1}^{c} u^{m_{ij}} \left\| x_i - c_j \right\|^2 \tag{1}$$

FCM updates the cluster center c_j and the fuzzy membership u_{ij} by repeated executions, which are computed using Eqs. (2) and (3).

$$c_j = \frac{\sum_{i=1}^{n} \left(u_{ij}\right)^m x_i}{\sum_{i=1}^{n} \left(u_{ij}\right)^m} \tag{2}$$

$$u_{ij} = \frac{1}{\sum_{k=1}^{c} \left(\frac{\left\| x_i - c_j \right\|}{\left\| x_i - c_k \right\|} \right)^{\frac{2}{m-1}}} \tag{3}$$

Therefore, we used membership degree to perform the detection of attacks similar to normal. In other words, we detected hidden attacks classified as normal.

Some attacks have characteristics similar to normal, so anomaly detection cannot distinguish important differences between normal and attacks [22]. Because an attack similar to a normal might exist in data predicted and classified as normal, classification was performed with data classified as normal through FCM in relabeling. This enabled a more accurate classification of attacks similar to normal. First, it computed differences between membership degrees in clusters using for each datapoint created by FCM and checks whether it was within a threshold range defined by a user. data within the threshold range measured the distance from each cluster center. The formula was as follows:

$$Relabeling\,(R) = \begin{cases} if \;\; |MD\,(c_{normal} x_i) - MD\,(c_{attack} x_i)| \leq Threshold & 1 \\ else & 0 \end{cases} \tag{4}$$

MD refers to membership degree in each cluster created by FCM; x_i is the entire dataset where $i = 1, \ldots, n$; c_{normal} and c_{attack} refer to normal and attack clusters; threshold means a value defined by a user. The threshold ranges from 0 to 1. Only if the relabeling result is 1 is distance computed. In this paper, a threshold was defined by a user, and by relabeling the contained data in the threshold, we detected attacks similar to normal that exist between the data classified as normal.

3.3 Unknown Attack Detection

In this stage, unknown attacks included in them are identified based on the attack data classified through anomaly detection. First, the known attacks were classified based on CART, and the unknown attacks were detected by applying iForest. Because an unknown attack that has characteristics similar to that of a known attack could be classified as being an already defined class, it was detected by two stages to solve this problem.

DT is one of the algorithms in intrusion detection that are used to generate rules and use them for the detection of a known attack. It employs various algorithms including ID3, C4.5, C5.0, and CART [3,5,7,8]. CART, which uses the Gini index, which is the generalization of binomial variance, is a binary decision tree that starts from the root node, which includes all the training samples, and is recursively split into two sub-nodes [23]. For feature selection, computes the impurity value for each feature for selection. The Gini index is as follows [24]:

$$GINI = 1 - \sum_{j=1}^{J} p_j^2 \tag{5}$$

p_j is the probability of j, j is the number of the class. Rules, which are usually composed in if-then structure, are created about all attacks used as training data in CART. In this paper, we used it to generate rules for detecting known attacks.

iForest can converge quickly with very few trees, hence can show a high detection performance with only a small sub-sampling. Also, iForest can work well with a partial model without isolating all data or with a small sample. An anomaly score is required to do iForest based anomaly detection. The equation is as follows:

$$s(x, n) = 2^{-\frac{E(h(x))}{c(n)}} \tag{6}$$

where h(x) is the path length to x; c(n) is the average path length, and n is the number of external nodes. In the paper, the score was computed as a value between 0 and 1. If it was close to 1, the data were unknown attacks. If it is below 0.5, the data are known attacks.

4 Experimental Results

In this section, we explored the experiments conducted based on the proposed method. First, we detected attacks similar to normal using relabeling. Then, based on the anomaly detection results, we detected unknown attacks using iForest. And we used a second method used in unknown attack detection studies to remove labels from certain classes that data sets have and define them as unknown attacks.

4.1 Dataset

We used the NSL-KDD [25] dataset. NSL-KDD is a refined version of the KDD CUP 99 [26] dataset, which solved the problem of meaningless and redundant data in KDD CUP 99 [27]. There are 41 features and 23 detailed attack types, which can be divided into four attack classes (see Tab. 1).

Table 1: Detailed attack type based on attack class

Attack class	Detailed attack types
DoS	Back, land, neptune, pod, smurf, teardrop
Probe	Ipseep, nmap, portsweep, satan
R2L	Ftp_write, guess_passwd, imap, multihop, hpf, spy, warezclient, warezmaster
U2R	Buffer_overflow, loadmodule, perl, rootkit

Training data and test data have ratios as seen in Tabs. 2 and 3, in which other attack classes have lower data ratios than dos had. Especially, u2r has the lowest data ratio. In this paper, we converted symbolic features that exist in the data into the binary form [28]. We selected 15 features out of a total of 41 by preprocessing. We also applied minmax scaler to solve the large deviation of the values of those features.

Table 2: Normal and attack data ratio in NSL-KDD

	Normal (%)	Attack (%)
Train data	53.4583	46.5417
Test data	51.6682	48.3318

Table 3: Normal and attack types data ratio in NSL-KDD

	Normal (%)	DoS (%)	Probe (%)	U2R (%)	R2L (%)
Train data	53.4583	36.4578	9.2527	0.0412	0.7898
Test data	51.6682	30.5486	5.8852	0.1969	11.7011

4.2 Evaluation Metrics

Tab. 4 is the confusion matrix of two classes that are often used for evaluating classification. The column of the matrix indicates an instance in the actual class, and the row indicates an instance in the predicted class.

Table 4: Confusion matrix

		Actual class	
		Normal	Attack
Predict class	Normal	True positive (TP)	False positive (FP)
	Attack	False negative (TN)	True negative (TN)

- Accuracy: classification accuracy is the ratio of correct predictions to the total number of prediction

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{7}$$

- Precision: the ratio of total true positives instances divided by total number of true positives and false positives

$$Precision = \frac{TP}{TP + FP} \tag{8}$$

- Recall: the ratio of total relevant results correctly classified, true positives, divided by the total true positives and false negatives

$$Recall = \frac{TP}{TP + FN} \tag{9}$$

- F-measure: the harmony mean of the precision and recall

$$F\text{-}measure = 2 * \frac{Precision * Recall}{Precision + Recall} \tag{10}$$

- Detection ratio: The ratio to unknown number of attack detections

$$Detection\ ratio = \frac{Number\ of\ Detected\ Unknown\ Attack}{Number\ of\ Unknown\ Attack} \tag{11}$$

4.3 Anomaly Detection for an Attack Similar to Normal

We did relabel using membership degrees computed by FCM. This detected attacks similar to normal hiding in data classified as normal. First, we measured anomaly detection accuracy and false positive rate (FPR) according to thresholds to compute the optimal threshold value. The computed threshold value was used for relabeling. We found hidden attacks by measuring the distance from the cluster center against the data point contained within the threshold range. This process detected attacks similar to normal in a classified normal class.

The experimental results of the threshold for relabeling are as seen in Figs. 2 and 3. By comparative analysis on accuracy and FPR, the optimal threshold value was obtained. We found values with high accuracy and FPR below the acceptable range, because FPR dramatically increases false positives beyond the acceptable range, thus we set up the maximum acceptable range.

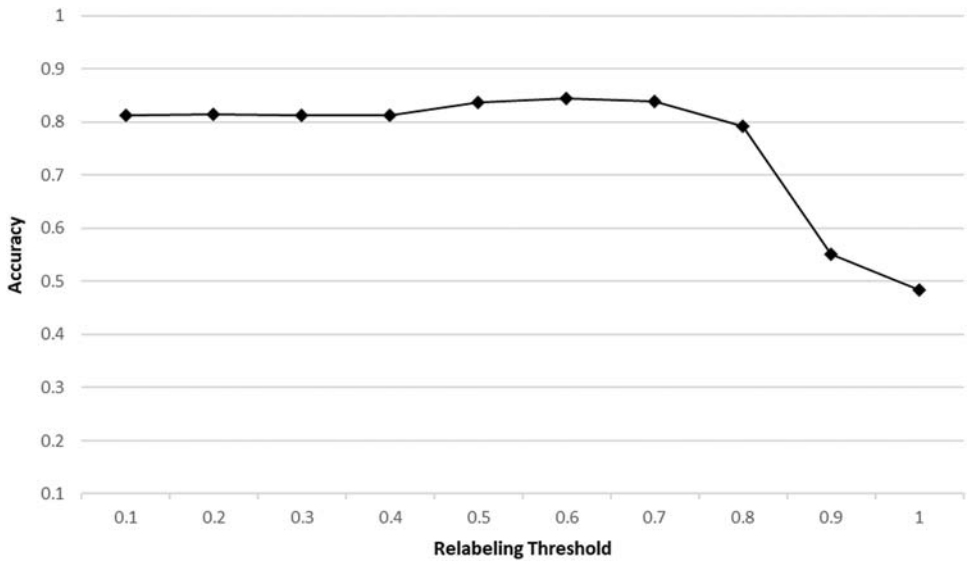

Figure 2: The accuracy rate of change based on relabeling thresholds

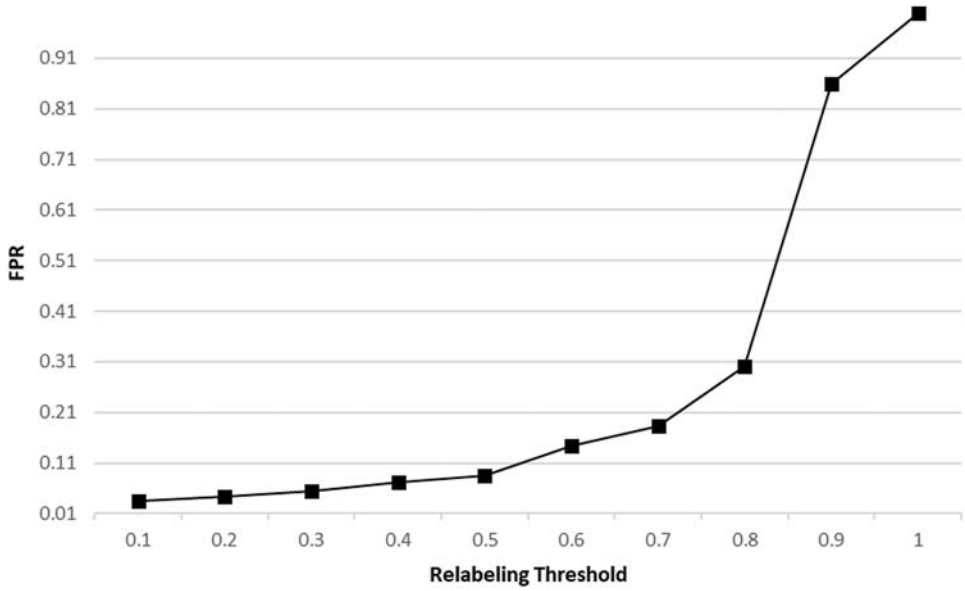

Figure 3: The FPR rate of change based on relabeling thresholds

We did relabel based on the computed threshold and compared the results with the dataset applied only with FCM in terms of anomaly detection accuracy. We found that the proposed model applied with relabeling showed more increases in accuracy and f-measure than when only FCM was applied (see Tab. 5); especially the detection rate of attacks increased by approximately 11% (see Tab. 6). Additionally, when only FCM was applied, the detection rates of u2r and r2l were low, at approximately 72% and 19%, but when relabeling was applied, the detection rates increased by 19% and 23%, respectively (see Tab. 7). This confirmed that when relabeling was done, attacks similar to normal could be detected more clearly. Also, we were confirmed that the proposed method can identify attacks included in the predicted class.

Table 5: Compare classification results for normal and attack

Model	Accuracy	Precision	Recall	F-measure	FPR
FCM	0.8071	0.9056	0.6708	0.7707	0.0654
Proposed	0.8454	0.8833	0.7836	0.8305	0.0968

Table 6: Compare detection rate for normal and attack

Model	Normal	Attack
FCM	93.4603	67.0813
Proposed	90.3193	78.3552

Also, we used t-SNE based visualization to analyze the distribution of datasets applied with FCM and relabeling. Fig. 4 shows the visualized distribution of anomaly detection. If we look at the distribution in the right-side graph applied with relabeling, areas mixed with normal and

attacks were clearly identified as attacks. Fig. 5 shows the visualized distribution of normal data and attack classes. The right-side graph applied with relabeling showed the distribution of attack types more clearly.

Table 7: Compare classification results for normal and attack classes

Model	DoS	Probe	U2R	R2L
FCM	81.3795	87.3417	72.9729	19.4633
Proposed	87.9986	98.9150	91.8919	42.6103

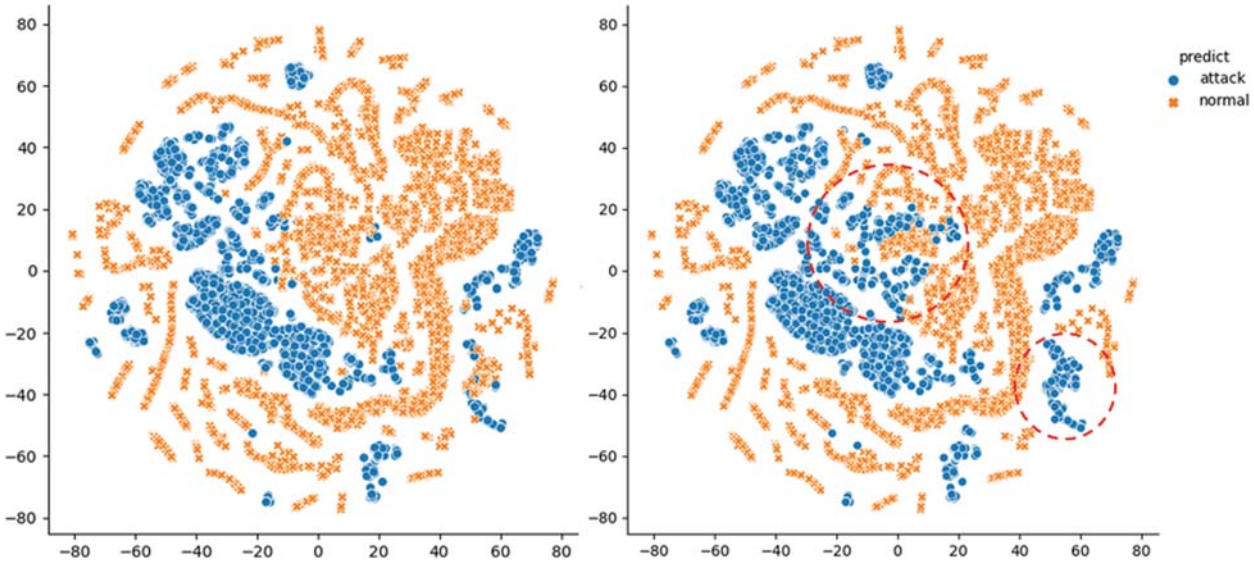

Figure 4: Visualization of normal and attack distribution (left: FCM only, right: FCM + relabeling)

4.4 Unknown Attack Detection

We perform unknown attack detection similar to known attack and rule-based known attack detection with attack data classified through anomaly detection. In this stage, we used CART to create the rules for known attacks and then used iForest to execute the detection of unknown attacks in the class predicted as a known attack. When relabeling was applied, accuracy and f-measure improved in most attack classes, showing the better performance (see Tab. 8). Also, we measured the detection ratio of each attack type; the results are as seen in Tab. 9. The number of detection is a numerical representation of how much each class of attack has been detected. The proposed relabeling-based method showed an improvement of approximately 10% in detection ratio compared to the existing methods, and especially the detection ratios of u2r and r2l improved by approximately 16% and 19%, respectively. In Fig. 6, we can be seen that the detection ratio has been increased for all attack classes. Therefore, we confirmed that the method proposed in this paper enables the identification of unknown attacks similar to known attacks that exist between data classified as known attacks.

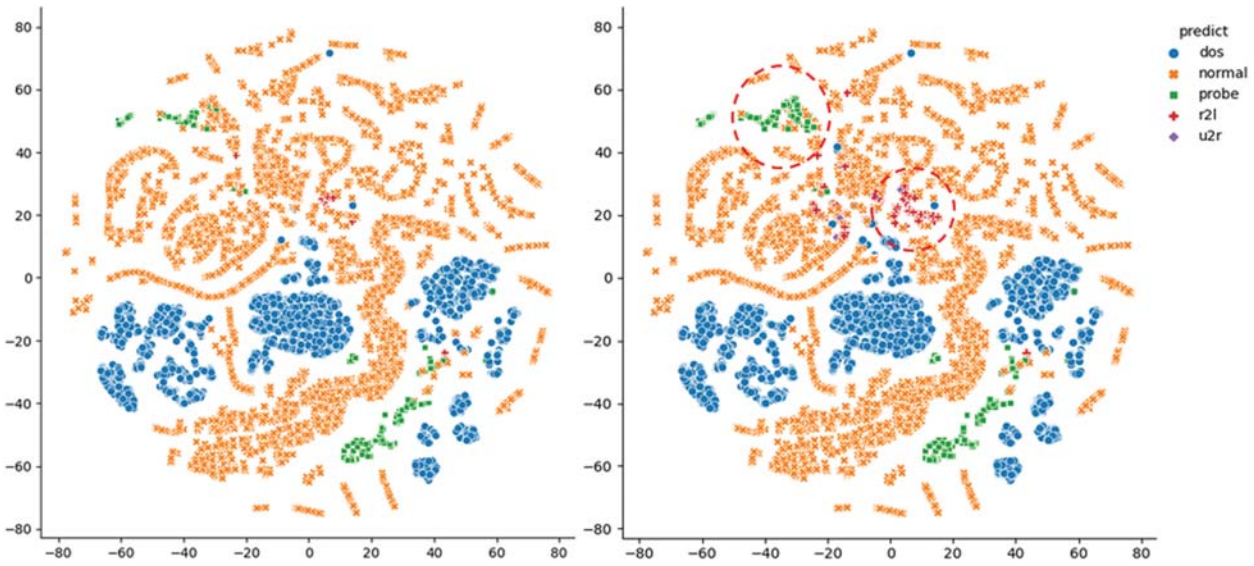

Figure 5: Visualization of normal and attack classes distribution (left: FCM only, right: FCM + relabeling)

Table 8: Evaluating unknown attack detection performance

Model	Unknown types	Accuracy	Precision	Recall	F-measure
FCM	DoS	0.7864	0.6815	0.7875	0.7307
	Probe	0.8703	0.9802	0.8698	0.9217
	U2R	0.8547	0.9979	0.8559	0.9215
	R2L	0.6931	0.7678	0.8529	0.8080
Proposed	DoS	0.8137	0.7549	0.7309	0.7427
	Probe	0.8793	0.9981	0.8642	0.9263
	U2R	0.8288	0.9986	0.8292	0.9060
	R2L	0.7176	0.8069	0.8246	0.8157

Table 9: Measure unknown attack detection ratio

Model	Unknown types	Detection Ratio	The number of detection (total number of data)
FCM	DoS	0.7858	4511 (5741)
	Probe	0.8734	966 (1106)
	U2R	0.5676	21 (37)
	R2L	0.1928	424 (2199)
Proposed	DoS	0.8618	4948 (5741)
	Probe	0.9891	1094 (1106)
	U2R	0.7297	27 (37)
	R2L	0.3824	841 (2199)

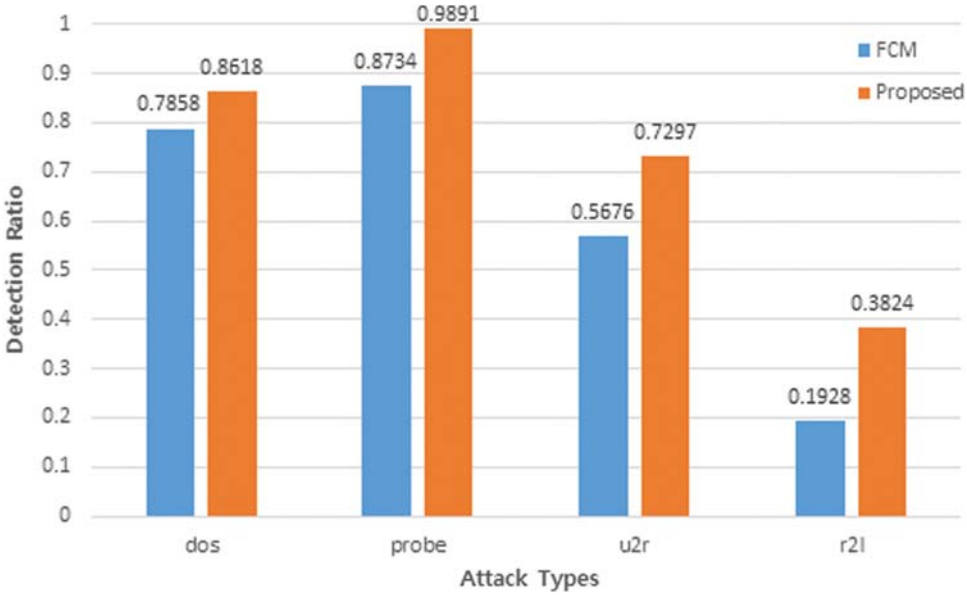

Figure 6: Comparison of unknown attack detection ratio with FCM and proposed methods

Also, we performed a comparative analysis with previously studied unknown attack detection results (see Tab. 10). The average ratio is the average for unknown attack detection rates measured in each study was calculated.

Table 10: Performance comparisons obtained by the proposed method and other previous work

Model	DoS	Probe	U2R	R2L	Average ratio
[8]	N/A	N/A	N/A	N/A	0.5200
[29]	**0.9982**	0.5483	N/A	0.1667	0.5710
FCM	0.7864	0.8703	**0.8547**	0.6931	0.8011
Proposed method	0.8137	**0.8793**	0.8288	**0.7176**	**0.8098**

5 Conclusion

For detection of unknown attacks, we researched a hybrid intrusion detection model that integrated anomaly detection for identification of attacks detection falsely classified as normal with misuse detection for identification of unknown attacks detection falsely classified as known attacks. We applied hybrid intrusion detection to accurately classify known attacks and normal, and to detect hidden unknown attacks, we applied relabeling and iForrest respectively to anomaly detection and misuse detection. The study proceeded in the sequence of the following processes: feature preprocessing, anomaly detection, and misuse detection. As a result, we proposed a hybrid model that could detect unknown attacks more effectively than a single classifier could. In the feature preprocessing, we did feature selection based on an RFE model and selected 15 features. In the anomaly-detection stage, FCM was applied for the classification of normal and attacks, and the application of relabeling made it possible to detect attacks similar to normal, which were hidden in data predicted to be normal. Tab. 7 shows that the detection rates of attacks

by anomaly detection improved by 11%, and Tab. 8 shows that the detection ratio by attack types improved by 6% in dos, 11% in probe, 19% in u2r, and 23% in r2l. This confirmed that if relabeling was performed, the proposed model could better able to detect attacks hidden in data predicted to be normal than conventional methods. In misuse detection, we used CART and iForest for the classification of known and unknown attacks. CART created rules for known attacks, and iForest detected unknown attacks hidden in known attacks. As seen in Tab. 9, the detection ratio by attack classes improved by approximately 10%, and the proposed method in Fig. 6 worked better than did conventional methods.

In the future, we plan to conduct a follow-up study by adding a method to solve the data-imbalance problem of NSL-KDD and to carry out another study on a method for reducing false-positive rates of anomaly detection and misuse detection. And since detecting unknown attacks, such as hybrid intrusion detection, performance depends on what features are used, we will propose an improved feature selection method through further research. We will also improve scalability and robustness for the proposed model by applying various data as well as the data used in this paper.

Funding Statement: This work was supported by the Research Program through the National Research Foundation of Korea, NRF-2018R1D1A1B07050864, and was supported by another the Agency for Defense Development, UD200020ED.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] X. Sun, J. Dai, P. Liu, A. Singhal and J. Yen, "Using Bayesian networks for probabilistic identification of zero-day attack paths," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2506–2521, 2018.

[2] I. You and K. Yim, "Malware obfuscation techniques: A brief survey," in *Broadband, Wireless Computing, Communication and Applications*, Fukuoka, Japan, pp. 297–300, 2010.

[3] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman and A. Alazab, "Hybrid intrusion detection system based on the stacking ensemble of c5 decision tree classifier and one class support vector machine," *Electronics*, vol. 9, no. 1, pp. 173, 2020.

[4] H. N. Datir and P. M. Jawandhiya, "Survey on hybrid data mining algorithms for intrusion detection system," in *Data Management*. Singapore: Analytics and Innovation, Springer, pp. 291–298, 2019.

[5] G. Kim, S. Lee and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Systems with Applications*, vol. 41, no. 4, pp. 1690–1700, 2014.

[6] A. AlEroud and G. Karabatis, "A contextual anomaly detection approach to discover zero-day attacks," in *Proc. in 2012 Int. Conf. on Cyber Security*, Washington, DC, USA, pp. 40–45, 2012.

[7] J. Hussain and S. Lalmuanawma, "Fusion of misuse detection with anomaly detection technique for novel hybrid network intrusion detection system," in *Recent Developments in Intelligent Computing, Communication and Devices*. Singapore: Springer, pp. 73–87, 2017.

[8] J. Lekha and P. Ganapathi, "Detection of illegal traffic pattern using hybrid improved CART and multiple extreme learning machine approach," *International Journal of Communication Networks and Information Security*, vol. 9, no. 2, pp. 164–171, 2017.

[9] M. Bitaab and S. Hashemi, "Hybrid intrusion detection: Combining decision tree and gaussian mixture model," in *Proc. in 2017 14th Int. ISC (Iranian Society of Cryptology) Conf. on Information Security and Cryptology*, Shiraz, Iran, pp. 8–12, 2017.

[10] W. L. Al-Yaseen, Z. A. Othman and M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," *Expert Systems with Applications*, vol. 67, no. 4, pp. 296–303, 2017.

[11] W. Hu and Y. Tan, "Generating adversarial malware examples for black-box attacks based on gan," arXiv preprint arXiv:1702.05983, 2017.

[12] M. Kawai, K. Ota and M. Dong, "Improved malgan: Avoiding malware detector by leaning cleanware features," in *Proc. in 2019 Int. Conf. on Artificial Intelligence in Information and Communication*, Okinawa, Japan, pp. 40–45, 2019.

[13] A. Liu, G. Xu, D. Zhou, X. Zheng, J. Ning *et al.,* "SFE-GACN: A novel unknown attack detection method using intra categories generation in embedding space," arXiv preprint arXiv:2004.05693, 2020.

[14] P. Lin, K. Ye and C. Z. Xu, "Dynamic network anomaly detection system by using deep learning techniques," in *Proc. in Int. Conf. on Cloud Computing*, Cham, San Diego, CA, USA: Springer, pp. 161–176, 2019.

[15] Y. Ji, B. Bowman and H. H. Huang, "Securing malware cognitive systems against adversarial attacks," in *Proc. in 2019 IEEE Int. Conf. on Cognitive Computing*, Milan, Italy, pp. 1–9, 2019.

[16] S. Huda, S. Miah, M. M. Hassan, R. Islam, J. Yearwood *et al.,* "Defending unknown attacks on cyber-physical systems by semi-supervised approach and available unlabeled data," *Information Sciences*, vol. 379, no. 1, pp. 211–228, 2017.

[17] P. Duessel, C. Gehl, U. Flegel, S. Dietrich and M. Meier, "Detecting zero-day attacks using context-aware anomaly detection at the application-layer," *International Journal of Information Security*, vol. 16, no. 5, pp. 475–490, 2017.

[18] Y. Lai, G. Ping, Y. Wu, C. Lu and X. Ye, "OpenSMax: Unknown domain generation algorithm detection," in *24th European Conf. on Artificial Intelligence*, Santiago de Compostela, Spain, pp. 1850–1857, 2020.

[19] D. W. Kim, G. Y. Shin and M. M. Han, "Analysis of feature importance and interpretation for malware classification," *Computers, Materials & Continua*, vol. 65, no. 3, pp. 1891–1904, 2020.

[20] Q. Chen, Z. Meng, X. Liu, Q. Jin and R. Su, "Decision variants for the automatic determination of optimal feature subset in RF-RFE," *Genes*, vol. 9, no. 6, pp. 301, 2018.

[21] D. J. Bora, D. Gupta and A. Kumar, "A comparative study between fuzzy clustering algorithm and hard clustering algorithm," arXiv preprint arXiv:1404.6059, 2014.

[22] N. Hoque, D. K. Bhattacharyya and J. K. Kalita, "FFSc: A novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis," *Security and Communication Networks*, vol. 9, no. 13, pp. 2032–2041, 2016.

[23] W. Y. Loh, "Classification and regression trees," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 1, no. 1, pp. 14–23, 2011.

[24] A. F. Pinem and E. B. Setiawan, "Implementation of classification and regression tree (CART) and fuzzy logic algorithm for intrusion detection system," in *Proc. in 2015 3rd Int. Conf. on Information and Communication Technology*, Bali, Indonesia, pp. 266–271, 2015.

[25] M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *2009 IEEE Symp. on Computational Intelligence for Security and Defense Applications*, Ottawa, Canada, pp. 1–6, 2009.

[26] "KDD Cup 1999 data," [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[27] A. Thakkar and R. Lohiya, "A review of the advancement in intrusion detection datasets," *Procedia Computer Science*, vol. 167, no. 1-2, pp. 636–645, 2020.

[28] S. M. Mehibs and S. H. Hashim, "Proposed network intrusion detection system based on fuzzy c mean algorithm in cloud computing environment," *Journal of University of Babylon for Pure and Applied Sciences*, vol. 26, no. 2, pp. 27–35, 2018.

[29] M. H. Kamarudin, C. Maple, T. Watson and N. S. Safa, "A logitboost-based algorithm for detecting known and unknown web attacks," *IEEE Access*, vol. 5, pp. 26190–26200, 2017.