УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
январь–февраль 2022 Том 22 № 1 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
January–February 2022 Vol. 22 No 1 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2022-22-1-93-100

Dimensionality reduction of the attributes using fuzzy optimized independent component analysis for a Big Data Intrusion Detection System

Rajan Aswanandini[1]✉, Chandran Deepa[2]

[1] KG College of Arts and Science, Coimbatore, 641035, India
[1,2] Sri Ramakrishna College of Arts and Science, Coimbatore, 641006, India

[1] aswanandini1981@gmail.com✉, https://orcid.org/0000-0002-6968-4653
[2] deepapkd@gmail.com, https://orcid.org/0000-0002-1681-9059

Abstract
Big data cybersecurity has garnered more attraction in recent years with the development of advanced machine learning and deep learning classifiers. These new classifier algorithms have significantly improved Intrusion Detection Systems (IDS). In these classifiers, the performance is positively influenced by high relevant features while less relevant features negatively influence the performance. However, considering all the attributes, especially the high dimensional attributes, increases computational complications. Hence it is essential to diminish the dimensionality of the attributes to improve the classifier performance. To achieve this objective, an efficient dimensionality reduction approach is presented through the development of the Fuzzy Optimized Independent Component Analysis (FOICA) technique. The standard Independent Component Analysis (ICA) is coupled with the fuzzy entropy to transform the high dimension attributes into low dimension attributes and helps in selecting high informative low-dimensional attributes. These selected features are fed to efficient hybrid classifiers namely Hyper-heuristic Support Vector Machines (HH-SVM), Hyper-Heuristic Improved Particle Swarm Optimization based Support Vector Machines (HHIPSO-SVM) and Hyper-Heuristic Firefly Algorithm based Convolutional Neural Networks (HHFA-CNN) to classify the cybersecurity data to identify the intrusions. Experiments are conducted over two cybersecurity datasets and real-time laboratory data whose outcomes specify the supremacy of the suggested IDS model based on FOICA dimensionality reduction.

Keywords
big intrusion data, cybersecurity, intrusion detection system, independent component analysis, dimensionality reduction, hyper-heuristic firefly algorithm, convolutional neural networks, NSL-KDD

For citation: Aswanandini R., Deepa Ch. Dimensionality reduction of the attributes using fuzzy optimized independent component analysis for a Big Data Intrusion Detection System. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2022, vol. 22, no. 1, pp. 93–100. doi: 10.17586/2226-1494-2022-22-1-93-100

УДК 004.048

Снижение размерности атрибутов с использованием нечетко оптимизированного независимого компонентного анализа для системы обнаружения вторжений в большие данные

Раджан Асуанандини[1]✉, Чандран Дипа[2]

[1] КГ Колледж искусств и науки, Коимбатур, 641035, Индия
[1,2] Колледж искусств и наук Шри Рамакришны, Коимбатур, 641006, Индия

[1] aswanandini1981@gmail.com✉, https://orcid.org/0000-0002-6968-4653
[2] deepapkd@gmail.com, https://orcid.org/0000-0002-1681-9059

Аннотация
Исследования кибербезопасности больших данных в последние годы стали привлекать большое внимание благодаря разработке передовых классификаторов машинного и глубокого обучения. Новые алгоритмы классификаторов значительно улучшили системы обнаружения вторжений. На производительность

классификаторов положительно влияют наиболее релевантные функции, в то время как наличие менее релевантных функций отрицательно влияет на их производительность. Учет всех атрибутов, особенно атрибутов высокой размерности, увеличивает вычислительную сложность. По этой причине, важно уменьшить размерность атрибутов для повышения производительности классификатора. Для достижения этой цели представлен эффективный подход к снижению размерности атрибутов посредством разработки метода нечеткого оптимизированного анализа независимых компонентов (Fuzzy Optimized Independent Component Analysis, FOICA). Стандартный независимый компонентный анализ (Independent Component Analysis, ICA) сочетается с нечеткой энтропией для преобразования атрибутов высокой размерности в атрибуты низкой размерности и помогает в выборе высокоинформативных атрибутов низкой размерности. Выбранные функции передаются в эффективные гибридные классификаторы, а именно в гиперэвристические машины опорных векторов (Hyper-heuristic Support Vector Machines, HH-SVM), гиперэвристические машины опорных векторов с улучшенной оптимизацией роя частиц (Hyper-Heuristic Improved Particle Swarm Optimization based Support Vector Machines, HHIPSO-SVM) и сверточные нейронные сети на основе гиперэвристического алгоритма светлячков (Hyper-Heuristic Firefly Algorithm based Convolutional Neural Networks, HHFA-CNN) для классификации данных кибербезопасности и выявления вторжений. Проведены эксперименты с использованием двух наборов данных о кибербезопасности и лабораторных данных в реальном времени. Полученные результаты подтвердили превосходство предложенной модели Intrusion Detection Systems на основе уменьшения размерности FOICA.

Ключевые слова
большие данные о вторжениях, кибербезопасность, система обнаружения вторжений, независимый компонентный анализ, уменьшение размерности, гиперэвристический алгоритм светлячка, сверточные нейронные сети, NSL-KDD

Ссылка для цитирования: Асуанандини Р., Дипа Ч. Снижение размерности атрибутов с использованием нечетко оптимизированного независимого компонентного анализа для системы обнаружения вторжений в большие данные // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 1. С. 93–100 (на англ. яз.). doi: 10.17586/2226-1494-2022-22-1-93-100

Introduction

Advancements in designing malicious software programs have led to serious challenges for the improvement of Intrusion Detection Systems (IDS) [1]. Hazardous attacks are progressively refined, and their recognitions are currently one of the challenging areas of research in recent years [2]. In technology-related applications and concerns, data security is a prime requirement, and hence the security systems are incorporated with the possibility of eliminating all the security threats [3].

The common problem about these IDS models is their low detection rate, mainly due to the ineffectiveness of the classifiers to classify the intrusion events. The false alarm rate in the existing methodologies is also considerably beyond the acceptable range, leading to further degradation of detection rates [4]. Machine learning succeeded in improving intrusion detection, which has to be updated [5]. Therefore, machine learning (ML) and deep learning (DL) models were employed to provide high detection accuracy when provided with sufficiently high-quality intrusion data for training [6]. The ML-based IDS are often used for intrusion detection while the DL-based IDS models are preferred for the intrusion data [7]. With multiple applications, the Support Vector Machine (SVM), Artificial Neural Networks (ANN), random forests, Extreme Learning Machines (ELM), [8] and various deep neural networks [9] have been broadly implemented for detection and prevention of intrusion detections over the network.

In this paper, the Fuzzy Optimized Independent Component Analysis (FOICA) technique has been designed by merging the Independent Component Analysis with the fuzzy entropy estimation process for optimal performance. Using this hybrid approach, we reduced the dimensionality of the features and selected the best features for the classifier. Previously, the Hyper-heuristic Support Vector Machines (HH-SVM) was developed to detect intrusion into big data effectively. To overcome the complexity issues in this model, the HH-SVM [10], Hyper-Heuristic Improved Particle Swarm Optimization based Support Vector Machines (HHIPSO-SVM) [11] and Hyper-Heuristic Firefly Algorithm based Convolutional Neural Networks (HHFA-CNN) [12] models were considered to enhance the classification accuracy in the traffic of big data. These three hybrid classifiers are chosen and the FOICA has been applied for improving their performance for intrusion detection. We performed tests over NSL-KDD and ISCX-IDS datasets to evaluate the results of the suggested FOICA technique. The main results of the work are the developed FOICA technique for feature dimensionality reduction by integration of fuzzy logic and ICA method and boosting the training time by dimensionality reduction and diminishing the problem of the hybrid classifiers.

Proposed methodology

The proposed methodology includes the FOICA and the hybrid classifiers. The framework consists of functioning blocks of the pre-processing unit, features extraction and dimensionality reduction using the proposed FOICA technique, and the classification using three classifiers. The intention is to use the FOICA to diminish the dimensionality of the features and improve the performance of three classifiers. The function flow of the proposed framework is shown in Fig. 1.

Pre-processing

Two network intrusion datasets, namely NSL-KDD and ISCX-IDS are employed in this study. The datasets are preprocessed using the normalization technique to scale down or scale up the attribute data or features. The attribute values of the intrusion dataset vary from $-\infty$ to

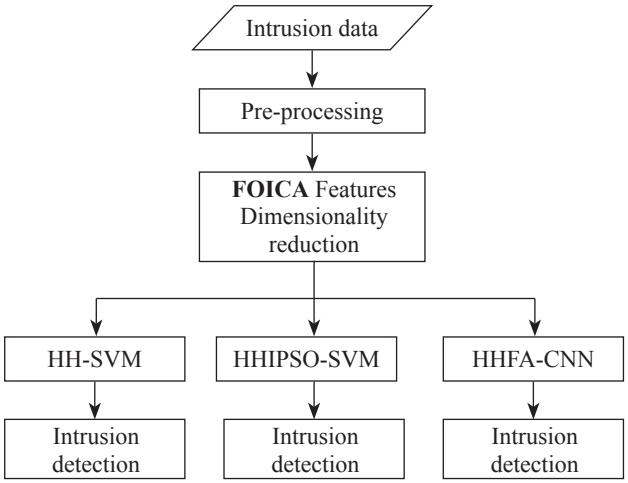

Fig. 1. Functioning of the proposed IDS model using FOICA

+∞, which are not often recognized effectively by the ML classifiers. The ML classifiers require more training time to understand these attribute values in different ranges. Hence it is a must to either scale down or scale up these values to maintain at a specified range such as 0.0 to 1.0, or –1.0 to 1.0, etc. so that they reduce the training time of the classifiers and enable the data classifying process to be performed easily. This process of normalization is also utilized to reduce the overestimation (false positives) and the underestimation (false negatives). In this study, the normalization is implemented to scale down/ up the values of the attributes to regulate their values in the range from 0.0 to 1.0.

FOICA for feature dimensionality reduction

ICA is a multivariate data processing method that is an extended generalization of the popular Principal Component Analysis (PCA) method. The main purpose of the ICA is to decompose the input data into statistically independent components for reducing dimensionality. While PCA projects the data into new solution space, the ICA determines the linear description of the non-Gaussian data as statistically independent components. The ICA can effectively identify the functional relationships and clusters of the data. In this study, fuzzy entropy is used to select the prominent independent components for the classifier and hence reduce the complexity associated with high dimension features.

Initially, FOICA follows the simplest functions of ICA where the attribute data are taken as scalar random variables denoted as $\{x_1, x_2, \ldots, x_n\}$. These variables are assumed as linear combinations of the m unknown independent components denoted as $\{S_1, S_2, \ldots, S_m\}$ which possesses zero mean and are statistically conjoint and self-regulating. When the attribute data is denoted by x_j are rearranged as a Vector $X = (x_1, x_2, \ldots, x_n)^T$, they can be modelled as the linear combination of m random variables denoted as $S = (S_1, S_2, \ldots, S_m)^T$. Appraising these terms into the matrix form leads to $X = AS$, A denoting the mixing matrix formed by the ratio of intensities in X.

To estimate the independent components, the FOICA uses the fixed point iteration scheme that estimates the components faster than the standard PCA and ICA. This fixed point scheme is based on the maximization of negentropy (reverse entropy) which is utilized as the divergence function for approximation. It is denoted as $J(u)$.

$$J(u) = H(u_G) - H(u). \quad (1)$$

Here u_G denotes a Gaussian random vector of the same covariance matrix as u, H denotes the marginal entropy that can be computed as $H(u_i) = -\int p(s_i)\log p(s_i)ds_i$. G denotes any non-quadratic function, u_i and s_i are the independent component and linear combination elements, respectively. $p(.)$ denotes the probability density function.

The mutual information metric can be used as a natural measure to determine independence between two random variables. It is given by

$$MI = J(u) - \sum_i J(u_i). \quad (2)$$

Minimizing this mutual information in FOICA can provide the estimation of the independent components. It is noted that diminishing the mutual information is comparable to maximizing the negentropy. Hence it can be approximated as

$$J_G(u_i) = [E\{G(u_i) - E\{G(y)\}]^2. \quad (3)$$

Here $E\{.\}$ denotes the expectation values and represents a Gaussian variable with zero mean and unit variance. Fuzzy entropy is used as a selection measure for the independent components. The best independent components act as an effective solution for the feature selection and thus improvise the dimensionality reduction. Fuzzy entropy differentiates the pattern distribution better than the ICA alone and appraises the separability of each independent element of the attribute data. Using ICA alone will cause increasing the number of components equal to the number of observed variables that leads to computational complexity in the classification process. This can be overcome by using fuzzy entropy to tune FOICA for optimal dimensionality reduction. The separability property of each component will enhance the classification, and it depends on the fuzzy entropy values. The lower the fuzzy entropy values, the higher the separability of the components. The fuzzy entropy is computed based on the Shannon probabilistic entropy.

$$F(A) = -\sum_{i=1}^{n}(\mu_A(u_i)\log\mu_A(u_i) + (1 - \mu_A(u_i))\log(1 - \mu_A(u_i))). \quad (4)$$

Here $\mu_A(u_i)$ are the fuzzy values of the independent components. This fuzzy entropy is a measure of fuzziness that is used to estimate the global discrimination from the normal fuzzy sets of independent components. The fuzzy set of A with $\mu_A(u_i) = 0.5$ provides the maximum ordering capability, and hence the values are adjusted based on $\mu_A(u_i)$.

In this method, the class ideal vectors representing the class i are created initially as $V_i = (v_1(f_1), v_2(f_2), \ldots, v_i(f_i))$ which can be user-defined. A generalized mean is used to create the class ideal vectors. Then the similarity $S(x, V_i)$ between the x samples and V_i are computed to obtain the j similarities. These similarities are gathered

in a similarity matrix and the fuzzy entropy is computed using Eq. (4) to estimate the similarity between the independent components. The highly similar independent components are selected and used as the vehicle for the selection of the best features to feed the classifiers. In this stage, the forward selection is used to select the relevant features, while backward elimination is used to terminate the irrelevant features until the function termination is obtained. Thus the performance of ICA is improved through fuzzy entropy to optimize the dimensionality reduction and feature selection process.

Algorithm 1: FOICA
Begin
Obtain normalized intrusion data
Initialize attribute data as n scalar random variables
Assign m unknown independent components
Rearrange the attribute data as X with $n >> m$
Estimate the mixing element A using X and S
Set $n = m$
Invert the mixing element A to form U *or* S
Apply the fixed point iteration scheme
Compute the negentropy ($J(u)$) and mutual information (MI) using Eq. (1) & (2)
Maximize MI to approximate independent components using Eq. (3)
Create class ideal vectors using the generalized mean
Estimate similarities between components
Form similarity in $S(x, V_i)$
For each component
    Compute fuzzy entropy using Eq. (4)
    If $F(A)$ is lower, then
        Determine as higher separability
    Else
        Determine as low separability
    End if
End for
Return high similarity independent components
Assign features for components
Apply forward selection & backward elimination
Return best features for classification
End

Classification

After the process of FOICA is complete, the classification is performed using three different classifiers. HH-SVM [13], HHIPSO-SVM [14] and HHFA-CNN are three hybrid classifiers.

— **HH-SVM**: Introduced by Sabar et al. [13], this model is designed by combining the hyper-heuristic optimization with the standard SVM to form hyper-heuristic SVM for the effective intrusion classification. The high-level strategy is to control the selection of low-level heuristics to generate a new optimal SVM configuration.

— **HHIPSO-SVM**: An enhancement of HH-SVM was developed in [14] using a hybrid optimization model of hyper-heuristic particle swarm optimization for tuning the hyper-parameters of SVM to determine its optimal configuration. This hybrid model utilized multiple objectives for tuning the parameters without violating the overall classifier process.

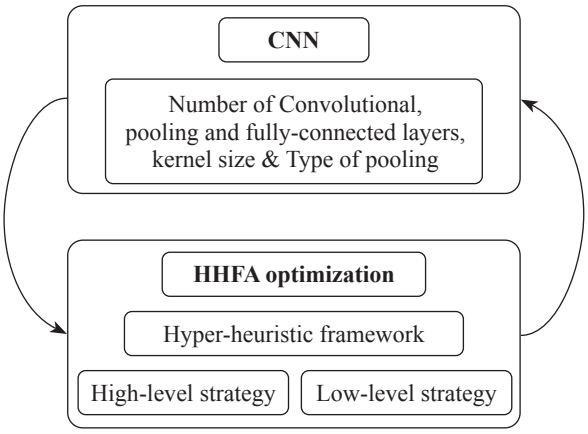

Fig. 2. HHFA-CNN classifier

— **HHFA-CNN**: In this model, a hybrid optimization model of the Hyper-Heuristic Firefly Algorithm is presented to optimize the hyper-parameters of the CNN for enhancing the classifier performance. This model tunes the number of convolution layers, number of pooling layers, pooling type, number of fully connected layers and kernel size to optimize the configuration of CNN. Fig. 2 shows the architecture of HHFA-CNN. The three classifiers are individually utilized to classify the intrusion data to estimate the performance of the proposed FOICA.

Experimental results and discussion

The evaluation of the proposed FOICA model for feature dimensionality reduction is performed using two benchmark instances of cyber security problems, NSL-KDD and ISCX-IDS datasets. NSL-KDD problem instance consists of 311,027 training samples and 77,289 testing samples which are classified as either normal or malicious. ISCX-IDS consists of 208,667 training samples and 78,400 testing samples that are classified as either normal or attack activities are used for this evaluation. Both benchmark instances are available at https://www.unb.ca/cic/datasets/index.html. The experiments are conducted in MATLAB 2016b (version 9.1). The system configurations are given in Table 1.

In addition to the benchmark instances, the real big data traffic instances are also collected using a Local Area Network (LAN) based cloud system through the Wire shark tool with 200 fake source IP addresses in the

Table 1. System configurations

Operating System	Windows 10, 32 bit
Processor	Intel core i5 3470 3.2 GHz
RAM	4 GB DDR3
Storage	500 GB Intel SSD SC2CT060A3 ATA device
Network bandwidth	1 Gbps
Simulation tool	MATLAB v.2016b
Simulation time, s	180

attacker host and 50 trusted sources in the laboratory hosts to simultaneously generate attack and normal traffic. In this analysis, two typical attacks, namely ICMP flooding (Type I) and TCP SYN flooding (Type II), were tested with an observation time of 5 s. The total data samples collected during the testing time included 190,355 samples with 176 legitimate features and one class label. The evaluations are made in the order of classification without dimensionality reduction and with the use of FOICA. Once the best classifier is known, FOICA is compared to existing models with the previously selected best classifier. The performance metrics are accuracy, precision, recall, f-measure and processing time to detect the intrusions.

Performance evaluation over NSL-KDD

The performance of the proposed FOICA is estimated using three classifiers over the NSL-KDD. The performance of the classifiers without FOICA is also evaluated. Table 2 displays the performance comparison of FOICA on three classifiers against the classifiers without dimensionality reduction on the NSL-KDD testing dataset for 25 independent runs.

From Table 2, it can be seen that the performance values of HHFA-CNN, HHIPSO-SVM and HH-SVM are improved by the use of FOICA. When the classifiers are used without FOICA, the resulting accuracy is varies the range of 89 to 97 %. In similar cases, when FOICA is utilized with these classifiers, the accuracy was from 91 to 98 %. Similar results are also obtained for other performance metrics. Among the compared methods, HHFA-CNN with FOICA has achieved high accuracy, precision, recall, and f-measure and minimum processing time. It achieved 1.08 % of high accuracy, 1.96 % of high precision, 8.22 % of high recall, 11.07 % of high f-measure and 0.28 s lesser processing time than the HHFA-CNN model without FOICA.

The performance improvement can be attributed to the fuzzy processing of the features which improved the classifier performance by feeding the vital features and reducing the less relevant ones. The training time is reduced through this deliberated processing in the IDS.

Performance evaluation over ISCX-IDS

Table 3 shows the performance comparison of FOICA on three classifiers against the classifiers without dimensionality reduction on the ISCX-IDS testing dataset for 25 independent runs.

From Table 3, it is seen that the performance of HHFA-CNN, HHIPSO-SVM and HH-SVM are improved by the use of FOICA in ISCX-IDS. All three classifiers with FOICA have achieved better accuracy, precision, precision, recall, and f-measure and minimum processing time than the classifiers without FOICA. The HHFA-CNN classifier with the FOICA model has outperformed the other compared models. It achieved 2.34 % of high accuracy, 0.1 % of high precision, 2.34 % of high recall, 0.78 % of high f-measure and 7.7 s lesser processing time than the HHFA-CNN model without FOICA. This shows the effectiveness of using the FOICA dimensionality reduction approach for intrusion detection.

FOICA has provided this enhanced performance due to their fuzziness in selecting the vital features without any compromise. The transformation of the features through FOICA has also reduced the selection of irrelevant features and the subsequent classifier is trained effectively through this process.

Comparison with existing methods

Since the performance of FOICA is evaluated in Tables 2 and 3, the HHFA-CNN has been the best classifier when using FOICA for dimensionality reduction. Hence in this section, popular algorithms from literature are evaluated and compared with the proposed FOICA with the

Table 2. Performance comparison on NSL-KDD

Algorithm	Metrics, %				Time, s
	Accuracy	Precision	Recall	F-measure	
HH-SVM [13]	89.76	67.10	62.81	62.22	4.65
HHIPSO-SVM [14]	93.33	73.99	64.29	68.37	2.55
HHFA-CNN	96.67	93.94	74	82.79	1.38
HH-SVM + FOICA	91.67	81.52	69.83	89.82	4.02
HHIPSO-SVM + FOICA	94.45	92.03	78.32	92.88	2.16
HHFA-CNN + FOICA	97.75	95.90	82.22	93.86	1.10

Table 3. Performance comparison on ISCX-IDS

Algorithm	Metrics, %				Time, s
	Accuracy	Precision	Recall	F-measure	
HH-SVM [13]	86.60	63.30	60.00	56.19	126.00
HHIPSO-SVM [14]	92.40	69.65	61.10	59.82	49.50
HHFA-CNN	93.33	99.70	93.33	96.55	48.20
HH-SVM + FOICA	88.33	71.87	69.87	79.65	102.00
HHIPSO-SVM + FOICA	94.50	74.78	75.58	82.21	42.88
HHFA-CNN + FOICA	95.67	99.80	95.67	97.33	40.50

Table 4. Performance comparison on NSL-KDD

Algorithm	Metrics, %				Time, s
	Accuracy	Precision	Recall	F-measure	
PCA [15]	86.00	64.50	66.76	78.97	6.30
IG-PCA [16]	97.24	73.56	86.56	81.67	9.40
SCNN [17]	86.64	78.67	82.34	90.23	4.80
CFS-BA [18]	96.11	92.47	90.60	92.30	9.50
PCA-GWO [19]	91.67	90.32	89.18	91.82	7.56
SMO [20]	96.40	93.67	91.33	92.48	3.60
ICA	89.67	71.20	73.50	82.30	3.11
Proposed FOICA	97.75	95.90	82.22	93.86	1.10

Table 5. Performance comparison on laboratory traffic data

Algorithm	Metrics, %				Time, s
	Accuracy	Precision	Recall	F-measure	
HH-SVM [13]	86.67	84.56	86.21	85.36	167.54
HHIPSO-SVM [14]	89.20	87.65	89.98	88.72	155.34
HHFA-CNN	94.56	91.89	93.22	92.50	138.60
HH-SVM + FOICA	91.67	89.67	90.16	89.82	152.50
HHIPSO-SVM + FOICA	93.74	93.66	94.75	94.11	141.67
HHFA-CNN + FOICA	98.89	97.91	98.90	98.25	127.15

HHFA-CNN classifier model acting as the base classifier. Table 4 shows the comparison results of existing models with FOICA over the NSL-KDD data.

The performance results in Table 4 showed that the proposed FOICA has produced better results when used with the HHFA-CNN classifier. It has achieved significantly better performance than the other compared methods in terms of all performance metrics. Although methods like PCA [15], IG-PCA [16], SCNN [17], CFS-BA [18], PCA-GWO [19] and SMO [20] provided comparatively equivalent accuracy, the processing time complexity of these models distances them from the proposed model of FOICA. The utilization of fuzzy entropy to enhance the ICA performance is to be accredited for this performance enhancement. Also, the CNN classifier through deep feature learning has contributed to this effective performance.

Evaluation of laboratory traffic data

Since the laboratory traffic data has been generated over a LAN network setup in real-time, the traffic samples are still raw and extensive preprocessing is required. After the necessary preprocessing, the data is fed to the proposed IDS model. Table 5 displays the performance comparison of FOICA on the three classifiers against the classifiers without dimensionality reduction on the laboratory traffic data.

From Table 5, it can be seen that the use of FOICA has enhanced the performance of the classifiers, as in the case of benchmark data. HHFA-CNN, HHIPSO-SVM and HH-SVM are improved by the use of FOICA with the accuracy increased by about 4–5 %. Similar results are also obtained for other performance metrics. Among the compared methods, HHFA-CNN with FOICA has achieved high accuracy, precision, recall, and f-measure and minimum processing time. It achieved 4.33 % of high accuracy, 6.02 % of high precision, 5.68 % of high recall, 5.75 % of high f-measure and 11.45 s lesser processing time than the HHFA-CNN model without FOICA.

Conclusion

In this paper, we presented an advanced feature dimensionality reduction approach by combining the fuzzy entropy with the standard ICA. This hybrid FOICA model effectively reduced the feature dimension and selected the best features for the classification of big intrusion data. Evaluations were conducted on NSL-KDD and ISCX-IDS datasets and the laboratory data, and FOICA improved the performance of the classifiers. Also, when compared with other existing dimensionality reduction models, the proposed FOICA provided significantly better results. HHFA with the proposed FOICA provided superior performance than the other compared IDS algorithms. In future, other cyber security instances such as UNSW-NB15 will be tested. Moreover, the impact of data sparsity in some data instances will also be studied.

References

1. Liao H.J., Lin C.H.R., Lin Y.C., Tung K.Y. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 2013, vol. 36, no. 1, pp. 16–24. https://doi.org/10.1016/j.jnca.2012.09.004
2. Ashoor A.S., Gore S. Importance of intrusion detection system (IDS). *International Journal of Scientific and Engineering Research*, 2011, vol. 2, no. 1, pp. 1–4.
3. Wang Q., Lu P. Research on application of artificial intelligence in computer network technology. *International Journal of Pattern Recognition and Artificial Intelligence*, 2019, vol. 33, no. 5, pp. 1959015. https://doi.org/10.1142/S0218001419590158
4. Chen T.M., Walsh P.J. Guarding against network intrusions. *Computer and Information Security Handbook*, 2013, pp. 81–95. https://doi.org/10.1016/B978-0-12-394397-2.00005-2
5. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, 2019, vol. 2, no. 1, pp. 20. https://doi.org/10.1186/s42400-019-0038-7
6. Liu H., Lang B. Machine learning and deep learning methods for intrusion detection systems: A survey. *Applied Sciences*, 2019, vol. 9, no. 20, pp. 4396. https://doi.org/10.3390/app9204396
7. Sultana N., Chilamkurti N., Peng W., Alhadad R. Survey on SDN based network intrusion detection system using machine learning approaches. *Peer-to-Peer Networking and Applications*, 2019, vol. 12, no. 2, pp. 493–501. https://doi.org/10.1007/s12083-017-0630-0
8. Sandhu U.A., Haider S., Naseer S., Ateeb O.U. A survey of intrusion detection & prevention techniques. *Proc. of the 2011 International Conference on Information Communication and Management (IPCSIT)*. Vol. 16, 2011, pp. 66–71.
9. Aldweesh A., Derhab A., Emam A.Z. Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, 2020, vol. 189, pp. 105124. https://doi.org/10.1016/j.knosys.2019.105124
10. Reddy G.T., Reddy M.P.K., Lakshmanna K., Kaluri R., Rajput D.S., Srivastava G., Baker T. Analysis of dimensionality reduction techniques on big data. *IEEE Access*, 2020, vol. 8, pp. 54776–54788. https://doi.org/10.1109/ACCESS.2020.2980942
11. Varma P.R.K., Kumari V.V., Kumar S.S. A survey of feature selection techniques in intrusion detection system: A soft computing perspective. *Advances in Intelligent Systems and Computing*, 2018, vol. 710, pp. 785–793. https://doi.org/10.1007/978-981-10-7871-2_75
12. Almusallam N.Y., Tari Z., Bertok P., Zomaya A.Y. Dimensionality reduction for intrusion detection systems in multi-data streams—A review and proposal of unsupervised feature selection scheme. *Emergence Complexity and Computation*, 2017, vol. 24, pp. 467–487. https://doi.org/10.1007/978-3-319-46376-6_22
13. Sabar N.R., Yi X., Song A. A bi-objective hyper-heuristic support vector machines for big data cyber-security. *IEEE Access*, 2018, vol. 6, pp. 10421–10431. https://doi.org/10.1109/ACCESS.2018.2801792
14. Aswanandini R., Muthumani N. Multi-objective hyper-heuristic improved particle swarm optimization based configuration of support vector machines for big data cyber security. *International Journal of Innovative Technology and Exploring Engineering*, 2019, vol. 8, no. 12, pp. 3892–3897. https://doi.org/10.35940/ijitee.L3401.1081219
15. Vasan K.K., Surendiran B. Dimensionality reduction using principal component analysis for network intrusion detection. *Perspectives in Science*, 2016, vol. 8, pp. 510–512. https://doi.org/10.1016/j.pisc.2016.05.010
16. Salo F., Nassif A.B., Essex A. Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection. *Computer Networks*, 2019, vol. 148, pp. 164–175. https://doi.org/10.1016/j.comnet.2018.11.010
17. Moustakidis S., Karlsson P. A Novel feature extraction methodology using Siamese convolutional neural networks for intrusion detection. *Cybersecurity*, 2020, vol. 3, no. 1, pp. 16. https://doi.org/10.1186/s42400-020-00056-4
18. Zhou Y., Cheng G., Jiang S., Dai M. Building an efficient intrusion detection system based on feature selection and ensemble classifier. *Computer Networks*, 2020, vol. 174, pp. 107247. https://doi.org/10.1016/j.comnet.2020.107247
19. Swarna Priya R.M., Maddikunta P.K.R., Parimala M., Koppu S., Gadekallu T.R., Chowdhary C.L., Alazab M. An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection

Литература

1. Liao H.J., Lin C.H.R., Lin Y.C., Tung K.Y. Intrusion detection system: A comprehensive review // Journal of Network and Computer Applications. 2013. V. 36. N 1. P. 16–24. https://doi.org/10.1016/j.jnca.2012.09.004
2. Ashoor A.S., Gore S. Importance of intrusion detection system (IDS) // International Journal of Scientific and Engineering Research. 2011. V. 2. N 1. P. 1–4.
3. Wang Q., Lu P. Research on application of artificial intelligence in computer network technology // International Journal of Pattern Recognition and Artificial Intelligence. 2019. V. 33. N 5. P. 1959015. https://doi.org/10.1142/S0218001419590158
4. Chen T.M., Walsh P.J. Guarding against network intrusions // Computer and Information Security Handbook. 2013. P. 81–95. https://doi.org/10.1016/B978-0-12-394397-2.00005-2
5. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges // Cybersecurity. 2019. V. 2. N 1. P. 20. https://doi.org/10.1186/s42400-019-0038-7
6. Liu H., Lang B. Machine learning and deep learning methods for intrusion detection systems: A survey // Applied Sciences. 2019. V. 9. N 20. P. 4396. https://doi.org/10.3390/app9204396
7. Sultana N., Chilamkurti N., Peng W., Alhadad R. Survey on SDN based network intrusion detection system using machine learning approaches // Peer-to-Peer Networking and Applications. 2019. V. 12. N 2. P. 493–501. https://doi.org/10.1007/s12083-017-0630-0
8. Sandhu U.A., Haider S., Naseer S., Ateeb O.U. A survey of intrusion detection & prevention techniques // Proc. of the 2011 International Conference on Information Communication and Management (IPCSIT). V. 16. 2011. P. 66–71.
9. Aldweesh A., Derhab A., Emam A.Z. Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues // Knowledge-Based Systems. 2020. V. 189. P. 105124. https://doi.org/10.1016/j.knosys.2019.105124
10. Reddy G.T., Reddy M.P.K., Lakshmanna K., Kaluri R., Rajput D.S., Srivastava G., Baker T. Analysis of dimensionality reduction techniques on big data // IEEE Access. 2020. V. 8. P. 54776–54788. https://doi.org/10.1109/ACCESS.2020.2980942
11. Varma P.R.K., Kumari V.V., Kumar S.S. A survey of feature selection techniques in intrusion detection system: A soft computing perspective // Advances in Intelligent Systems and Computing. 2018. V. 710. P. 785–793. https://doi.org/10.1007/978-981-10-7871-2_75
12. Almusallam N.Y., Tari Z., Bertok P., Zomaya A.Y. Dimensionality reduction for intrusion detection systems in multi-data streams—A review and proposal of unsupervised feature selection scheme // Emergence Complexity and Computation. 2017. V. 24. P. 467–487. https://doi.org/10.1007/978-3-319-46376-6_22
13. Sabar N.R., Yi X., Song A. A bi-objective hyper-heuristic support vector machines for big data cyber-security // IEEE Access. 2018. V. 6. P. 10421–10431. https://doi.org/10.1109/ACCESS.2018.2801792
14. Aswanandini R., Muthumani N. Multi-objective hyper-heuristic improved particle swarm optimization based configuration of support vector machines for big data cyber security // International Journal of Innovative Technology and Exploring Engineering. 2019. V. 8. N 12. P. 3892–3897. https://doi.org/10.35940/ijitee.L3401.1081219
15. Vasan K.K., Surendiran B. Dimensionality reduction using principal component analysis for network intrusion detection // Perspectives in Science. 2016. V. 8. P. 510–512. https://doi.org/10.1016/j.pisc.2016.05.010
16. Salo F., Nassif A.B., Essex A. Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection // Computer Networks. 2019. V. 148. P. 164–175. https://doi.org/10.1016/j.comnet.2018.11.010
17. Moustakidis S., Karlsson P. A Novel feature extraction methodology using Siamese convolutional neural networks for intrusion detection // Cybersecurity. 2020. V. 3. N 1. P. 16. https://doi.org/10.1186/s42400-020-00056-4
18. Zhou Y., Cheng G., Jiang S., Dai M. Building an efficient intrusion detection system based on feature selection and ensemble classifier // Computer Networks. 2020. V. 174. P. 107247. https://doi.org/10.1016/j.comnet.2020.107247
19. Swarna Priya R.M., Maddikunta P.K.R., Parimala M., Koppu S., Gadekallu T.R., Chowdhary C.L., Alazab M. An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection

in IoMT architecture. *Computer Communications*, 2020, vol. 160, pp. 139–149. https://doi.org/10.1016/j.comcom.2020.05.048
20. Khare N., Devan P., Chowdhary C.L., Bhattacharya S., Singh G., Singh S., Yoon B. SMO-DNN: Spider monkey optimization and deep neural network hybrid classifier model for intrusion detection. *Electronics*, 2020, vol. 9, no. 4, pp. 692. https://doi.org/10.3390/electronics9040692

in IoMT architecture // Computer Communications. 2020. V. 160. P. 139–149. https://doi.org/10.1016/j.comcom.2020.05.048
20. Khare N., Devan P., Chowdhary C.L., Bhattacharya S., Singh G., Singh S., Yoon B. SMO-DNN: Spider monkey optimization and deep neural network hybrid classifier model for intrusion detection // Electronics. 2020. V. 9. N 4. P. 692. https://doi.org/10.3390/electronics9040692

Authors

Rajan Aswanandini — PhD, Assistant Professor, KG College of Arts and Science, Coimbatore, 641035, India; PhD Student, Sri Ramakrishna College of Arts and Science, Coimbatore, 641006, India, SC 57211403371, https://orcid.org/0000-0002-6968-4653, aswanandini1981@gmail.com
Chandran Deepa — PhD, Associate Professor, Sri Ramakrishna College of Arts and Science, Coimbatore, 641006, India, SC 56218174800, https://orcid.org/0000-0002-1681-9059, deepapkd@gmail.com

Авторы

Асуанандини Раджан — PhD, доцент, КГ Колледж искусств и науки, Коимбатур, 641035, Индия; докторант, Колледж искусств и наук Шри Рамакришны, Коимбатур, 641006, Индия, SC 57211403371, https://orcid.org/0000-0002-6968-4653, aswanandini1981@gmail.com
Дипа Чандран — PhD, доцент, Колледж искусств и наук Шри Рамакришны, Коимбатур, 641006, Индия, SC 56218174800, https://orcid.org/0000-0002-1681-9059, deepapkd@gmail.com

Received 30.09.2021
Approved after reviewing 25.12.2021
Accepted 29.01.2022

Статья поступила в редакцию 30.09.2021
Одобрена после рецензирования 25.12.2021
Принята к печати 29.01.2022