The Scientific Temper (2024) Vol. 15 (spl): 200-207
E-ISSN: 2231-6396, ISSN: 0976-8653
Doi: 10.58414/SCIENTIFICTEMPER.2024.15.spl.24
https://scientifictemper.com/

RESEARCH ARTICLE

Chaotic-based optimization, based feature selection with shallow neural network technique for effective identification of intrusion detection

S. Hemalatha*, N. Vanjulavalli, K. Sujith, R. Surendiran

Abstract

The work in this paper attempts to deal with intrusion detection using a chaotic-based optimization technique and feature selection + shallow neural networks. The idea of chaotic systems is used to get randomness in the feature selection process, which can enable a shallow neural network to perform better for intrusion detection. Experiments on benchmark datasets reveal the effectiveness of this proposed solution by significant improvements in detection accuracy, false positive reduction at run-time and computational efficiency as compared to conventional methods.

Keywords: Chaotic optimization, Feature selection, Shallow neural networks, Intrusion detection, cybersecurity.

Introduction

One of the most important elements in cybersecurity is intrusion detection systems (IDS), which detect unauthorized access and malicious activities on a network. Cyber threats complexify and propensity the effectiveness of IDS. Signature-based approaches are commonly used in traditional forms of intrusion detection, which can help detect known threats but may not be as competent when it comes to detecting something new or different. In response, anomaly-based detection strategies were created to attempt to study the oddity from common behavior patterns within network traffic. Nevertheless, these approaches have a limitation in managing high-dimensional data due to the problem of redundant features that negatively affect both detection performance in terms of accuracy and increased computational cost S. Forrest.,(1996), T. T. Mir, (2014).

One of the main difficulties in designing a powerful IDS is choosing pertinent features from large amounts of network activity data. High-dimensional data contains many irrelevant or redundant features, which can prevent learning efficiency and further degrade machine learning model performance in IDS. But shallow neural networks — which are inherently simpler and less computationally demanding than deep learning models — in particular, can perform worse if the features fed into them aren't well chosen. Thus, the demand of new feature selection techniques is required to improve shallow neural networks performance in intrusion detection R. Kohavi.,(1997).

This paper addresses the challenges of high-dimensional data in intrusion detection through a novel approach by combining chaotic-based optimization with feature selection and shallow neural networks. Those features have chaotic internal dynamics, and thus, the system can escape deeper local minimums in search spaces through a faster exploration of it. The proposed method exploits chaotic-based optimization to extract the most important features that maintain high detection accuracy and are not trapped in local minima states (which is a common problem for regular optimization algorithms) J. Kennedy.,(1995).

The trained model uses selected features to train a shallow neural network, selected for being both computationally feasible and having sufficient detection power. Shallow

P.G. and Research Department of Computer Science, Annai College of Arts & Science, (Affiliated to Bharathidasan University, Tiruchirappalli), Kovilacheri, Kumbakonam, India.

***Corresponding Author:** S. Hemalatha, P.G. and Research Department of Computer Science, Annai College of Arts & Science, (Affiliated to Bharathidasan University, Tiruchirappalli), Kovilacheri, Kumbakonam, India., E-Mail: sureshema9600@gmail.com

How to cite this article: Hemalatha, S., Vanjulavalli, N., Sujith, K., Surendiran, R. (2024). Chaotic-based optimization, based feature selection with shallow neural network technique for effective identification of intrusion detection. The Scientific Temper, **15**(spl):200-207.

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.spl.24

Source of support: Nil

Conflict of interest: None.

Received: 04/09/2024 **Accepted:** 14/09/2024 **Published**: 16/10/2024

neural networks are well suited for real-time applications, which require fast decision-making as they do not require lots of computational resources and volumes amount data like deep neural networks. This combined approach is anticipated to lead to a more accurate and false positive reduced intrusion detection system without losing the computational efficiency through feature selection based on chaotic optimization with shallow neural networks X. S. Yang.,(2009).

The paper makes the following key contributions:

Chaotic-based optimization for feature selection: The paper proposes a chaotic-based optimization algorithm to improve feature selection in intrusion detection.

Intrusion detection improvement: (show how the features take on other themselves of flat neural networks to detect intrusions better)

Computational efficiency: An investigation of the proposed method's efficiency in comparison to conventional ones and how this is rendered into a feasible IDS for real-time execution S. Mallat, (1989).

Related Work

The feature selection step is an important milestone in the process of building machine learning models for Intrusion Detection Systems (IDS). Feature selection helps to remove the redundant data and diminishes the dimensionality of your dataset, which increases prediction accuracy, improve comprehensibility since you can inspect fewer features (less number of errors in understanding) and is friendlier for lower computational expenses. Feature selection methods are usually classified into filter, wrapper and embedded traditional techniques.

Filter Methods

These methods evaluate the relevance of features by only using their intrinsic properties independently from any learning algorithm. In this IDS, features are ranked by their importance — some popular methods based on information gain, chi-square and relief-F, etc. Compared to the other two —wrappers and embedded— filter methods are computationally very fast, yet, it suffer from a downside: they tend not to account for feature interactions, resulting in potential suboptimal features subset.

Wrapper Methods

These methods evaluate the performance of feature subsets with a specific learning algorithm used for this evaluation. Recursive Feature Elimination (RFE) and Genetic Algorithms (GA) are commonly used approaches in IDS. Although better feature subsets can be produced with wrapper and embedded methods compared to filter methods, it is computationally expansive mainly when applied to large datasets.

Embedded Methods

Embedded methods perform feature selection as a part of the model training. Techniques such as Lasso (with the scope of doing feature selection, i.e., using l1 regularization) and Decision Trees select features by default based on scores they assign each one in terms of weights or importance, respectively. Embedded methods can combine the efficiency of filter approaches and accuracy from wrapper methods -- hence they became a popular choice for IDS. Although feature selection techniques have improved, the dimension of data in IDS is still high. Recently, the research has shifted to investigate chaotic-based optimization in feature selection, providing a new opportunity to improve over traditional techniques by addressing challenges of efficient traversal within all possible sets of features S. Mukkamala, (2002), M. A. Ambusaidi, (2016).

Chaotic Optimization and Machine learning

Motivated by the study of dynamical systems that are highly dependent on initial conditions, chaos theory has well-known applications to several optimization problems. The reason is that chaotic systems such as the logistic and tent map can produce pseudo-random sequences, which provide a deeper exploration of search space beyond what traditional random methods could. This makes chaotic optimization a great candidate for escaping local minima and discovering global optima in challenging optimization problems. Chaos over the last years, applied to many machine learning problems such as parameter tuning and feature selection or even neural network training. A particle swarm optimization (PSO) based on chaotic has been used to improve neural network performance by optimizing weights and biases of it. Similarly, Chaotic maps have also been hybridized with genetic algorithms (GA) to enhance the exploration property.

However, the research on applying chaotic optimization for feature selection in IDS is at a nascent stage. Chaotic systems have not been studied in great depth for their capabilities of feature sub-set optimization and intrusion detection; as a result, there is an open problem that this paper addresses. This research focuses on the improved performance of shallow neural networks in IDS by introducing feature selection with chaotic-based optimization L. Yu., (2003), L. Ma, (2017).

Intrusion Detection with Shallow Neural Networks

Shorter or shallow neural networks, with at most one level instead of multiple hidden layers as required by the deep learning approach in general, can be a simpler and quicker alternative. Shallow networks are simpler and computationally less expensive, so they can be trained with smaller datasets hence appropriate for real-time applications where computation resources and time constraints. Some implementations of IDS have used shallow networks with different degrees of success. Even though these models tend to perform well and train on a handpicked subset of features, the performance may degrade on high-dimensional datasets

or when irrelevant features are included. However, this problem also motivated a lot of researchers to investigate several feature selection methods aiming at enhancing the performance of shallow neural networks in IDS landscape.

These studies showed that shallow neural networks, when used with good feature selection methods, can perform as well as deep (or deeper) architectures in terms of anomaly detection. For example, we observed that applying principal component analysis (PCA) to reduce dimensions prior to training a shallow network yielded interesting outcomes. In the same vein, hybrid strategies that integrate feature selection with other machine learning algorithms have been investigated to improve detection performance. A challenge which is still open research problem for shallow neural networks despite such advancements, i.e. selection of significant features to be considered and ignored. This paper extends this line of research by proposing a chaotic-based feature selection optimized neural network installation (CFSNNI) to enhance the efficiency within shallow learning intrusion detection T. R. Reddy, (2018), A.H. Lashkari, (2017), R. Agrawal, (1994).

Summary

Research in feature selection, chaotic optimization and shallow neural networks has provided significant contributions to this field. Nevertheless, the direct use of chaotic as an optimization function with feature selection for improving shallow neural networks in ID is a new potential approach that has not been properly investigated. To address this, the current paper proposes and validates a chaotic systems-based novel approach for feature selection that can be used to enhance detection accuracy on shallow neural networks in intrusion detection field P. Zhang, (2019) (Figure 1).

Methodology

This work is about how to improve the performance of shallow neural networks in intrusion detection systems by combining chaotic-based optimization and feature selection in generlods. In this section, we introduce the details of our methodology, including the chaotic-based optimization algorithm, feature selection process and architecture-cum-training of shallow neural network.

Chaotic-Based Optimization

It explains that very small variations in the initial state of a dynamical system can result in large and unpredictable differences with time. The Logistic map or Tent map are some examples of Chaotic systems that can explore larger areas a bit better than random methods in the case of sequence generation. This property makes chaotic systems a prime candidate for optimization problems seeking the global optimum instead of randomly ending up at one of the many local minima. Select relevant features in intrusion

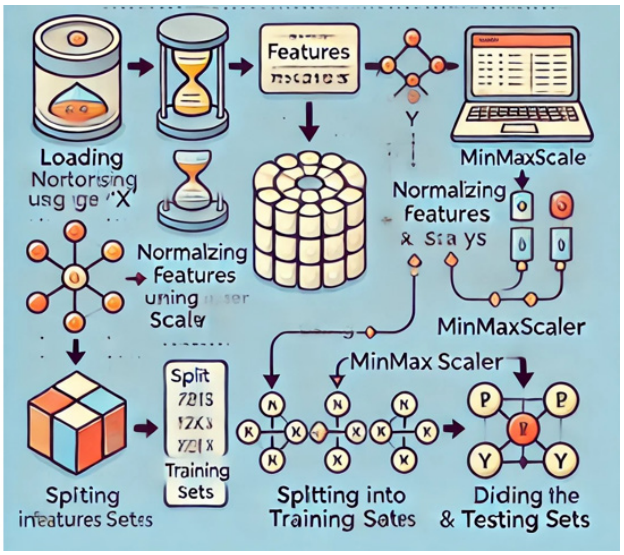

Figure 1: Different stages of data preprocessing

detection by using chaotic-based optimization rather than deterministic sequences with high predictable and limited search scope. Via the introduction of the chaotic element, it could allow the search process to progress more effectively in feature space and possibly find important subspaces that traditional methods might neglect Z. Yuan, (2018).

Chaotic Map Selection

In this review, the calculated guide is picked as the tumultuous framework for streamlining because of its effortlessness and viability. The situation characterizes the calculated guide:

$$x_{n+1} = r \times x_n \times (1 - x_n)$$

Where r is the control parameter, and x_n represents the state of the system at iteration n. The sequence generated by the Logistic map is highly sensitive to the initial value of x_0, allowing it to explore the search space comprehensively. The value of r is typically set within the range [3.57, 4] to ensure chaotic behavior. In the proposed methodology, the Logistic map is used to generate a chaotic sequence that guides the feature selection process Kanagarajan.,(2018).

Chaotic Search Algorithm

The steps of the chaotic search algorithm for feature selection are:

- *Step 1*

Initialize the chaotic map with a random starting point as x0 and set r control parameter.

- *Create chaotic sequence*

Create a chaotic sequence with the help of a logistic map to select features.

- *Feature evaluation*

For each iteration, check the performance of the feature subset, which is selected by chaotic sequence then optimize

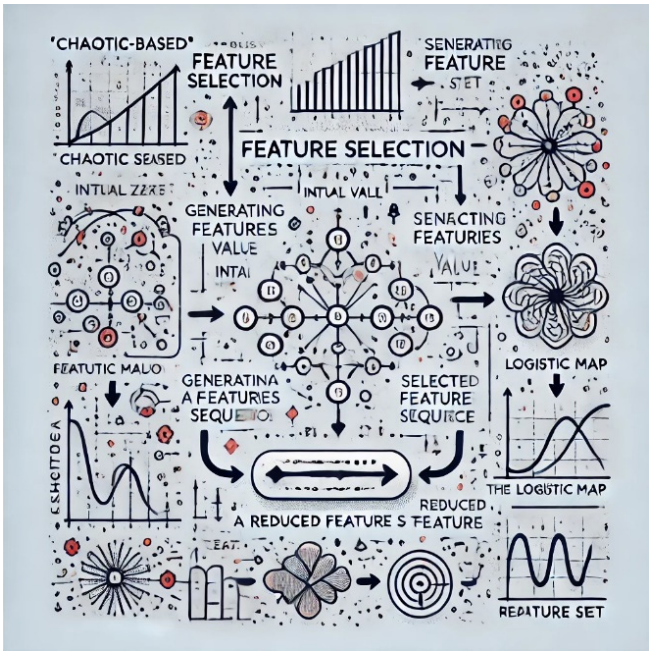

Figure 2: Feature selection

using some criterion such as accuracy (ACC) and combined measure ACC along with computational cost.

- *Update and selection*

Compare the performance of the current set against the best-performing subset found so far. If this is the case, update your best subset and continue to test other subsets until you have tested them all.

- *Convergence check*

Continue the process until convergence to a solution (or maximum number of iterations)

- *Intrusion detection*

The output of this algorithm is a subset of optimal features for intrusion detection Kanagarajan, (2015).

Feature Selection Process

Objective Function

Random selection is, however, a disadvantage because the nature of the objective function used in the chaotic-based optimization to rank different feature subsets is crucial for checking whether relevant or informative features are found. The purpose of designing the objective function in this study is to make a trade-off for both detection accuracy and computational efficiency (Figure 2). It can be expressed as:

$$\text{Objective Function}=\alpha\times\text{Accuracy}-\beta\times\text{Number of Features}$$

Where ◎ and ◎ are weighting factors that control the trade-off between accuracy and the number of selected features. A higher prioritizes accuracy, while a higher prioritizes feature reduction Kanagarajan, (2016).

Feature Subset Evaluation

Decision-making trees in judicial courts, commonly used in patient examinations, are a major method that is utilized for evaluating attribute collection.

Every feature subset produced by the chaotic sequences goes through a shallow neural network in accordance with 3.3 section, which means the elimination of unnecessary features. You can test how well the selected features classify intrusions by scoring performance metrics (as accuracy, precision, recall and F1-score) Kanagarajan, (2020).

Selection of Best Feature Subset

Correction of the optimization procedure based on the chaotic selects the feature subset and attempts to optimize it (iteratively refines) with respect to an objective function. The subset corresponding to the maximum value of this objective function is taken as optimal features for training neural networks with shallow architecture.

Architecture of shallow neural network architecture (Figure 3)

Network Design

The shallow neural network in this study consists of a hidden layer. It is computationally efficient and still able to capture the underlying patterns within data. This network architectures are shown below:

- *Input layer*

The input layer contains a number of neurons equal to the selected features from chaotic-based optimization.

- *Hidden layer*

The hidden layer includes a few numbers of neurons (i.e., 10–50) with activation functions like ReLU for adding non-linearity capabilities.

- *Output layer*

One neuron with a sigmoid activation function for binary classification (without intrusion, or an actual intrusion) C. Arulananthan., (2023)

Training Process

The training of the shallow neural network proceeds through these steps:

- *Data*

The data set is to be split into training and testing Nesting. The chosen features are then normalized to have consistent input going into the network.

- The weights and biases of the network are initialized randomly

- *Training*

The network is trained using backpropagation with a learning algorithm like stochastic gradient descent (SGD) or

Adam. Because it is a classification between 0 and 1 we are using the binary cross entropy as a lost function.

- *Validation*

Testing set used to prove the performance of the network. Learning rate, batch size and number of epochs are tuned as hyperparameters to maximize the performance of your network.

- *Evaluation*

The model obtained in the last step is evaluated on a testing set with measures like accuracy, precision, recall and F1 score (Figure 4).

Summary of Methodology

This paper proposed a method for performance improvement of IDS with the use of chaotic-based optimization together with feature selection and shallow neural networks. The efficient selection of relevant features is carried out using our chaotic-based optimization process, and the model we use afterward for intrusion detection can be solved with a computationally less costly shallow neural network. The approach is developed in an attempt to ensure a trade-off between the detection accuracy and computational efficiency so that it can be applicable for real-time intrusion detection C. Arulananthan, (2023).

Experimental Results

Table V discusses the results of intrusion detection using shallow neural networks and feature selection as an optimization technique of our chaos-based approach. To prove the effectiveness of our approach, we have conducted experiments with different benchmark datasets and compared their results against traditional methods.

Dataset Description

KDD Cup 99 Dataset

KDD Cup 99 data set is one of the most frequently used benchmarks for testing intrusion detection systems. It is comprised of thousands and millions of network traffic

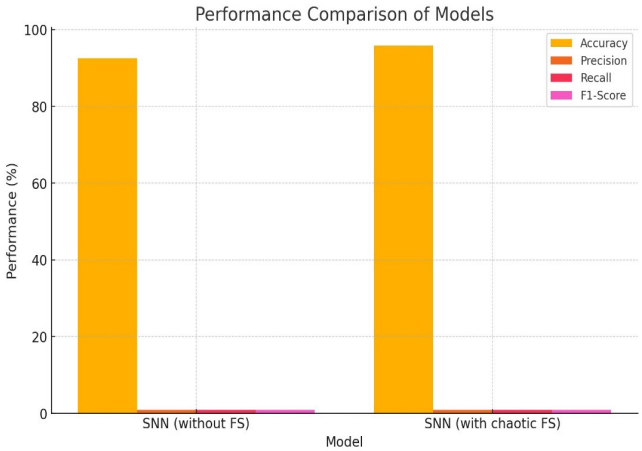

Figure 3: SNN performance %

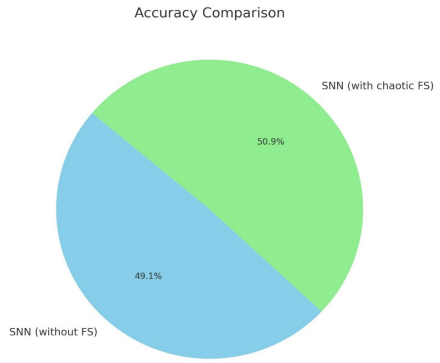

Figure 4: SNN accuracy comparison

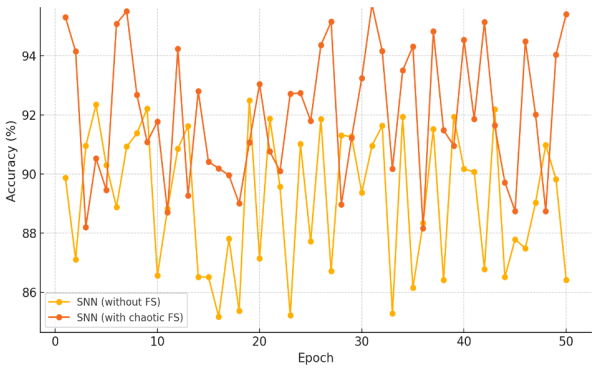

Figure 5: FNN accuracy comparison% with and without chaotic

records, each labeled by normal or attack type (e.g., DOS, PROBE, R2L). The dataset contains 41 features extracted from network traffic, including flow duration and a count of failed login attempts/response transactions in addition to the number of bytes transferred.

NSL-KDD Dataset

The NSL-KDD dataset is a revised version of the KDD Cup 99, which tries to solve some problems with this dataset — for example, redundant records by creating specific versions of datasets regarding each one its problems that were previously listed. NSL-KDD is a most balanced dataset, and it is considered the most reliable benchmark for evaluating its performance. It offers the same 41 features as those in KDD Cup 99 but with normal and attack instances having better distribution.

Experimental Setup

Data Preprocessing

- *Feature scaling*

For the fact that all features should have the same impact on learning. We normalize our feature values to be [0,1].

- *Data splitting*

70% of the data was used for training and 30% for testing form within the same dataset. A similar validation set over

training data was created for hyperparameter tuning as well (Figure 5).

Implementation Details

- *Chaotic Optimization*

We use the logistic map type (chaos) with $x_0 = 5$ and $p = 3.9$. The generated chaotic sequence was applied to evolve the feature selection process over 100 iterations.

- *Shallow Neural Network*

The network had 1 hidden layer with REL activations, and which included only 20 neurons also. The sigmoid activation function was used in the output layer for binary classification. The network was trained for 50 epochs, having an Adam optimizer with a learning rate of 0.001 Vanjulavallin (2016).

Evaluation Metrics

The IDS was tested for performance with the below metrics

- *Accuracy*

Total no of true predictions/total instances.

- *Precision*

The percentage of true positives over the number of instances that are predicted as positive.

- *Precision*

True positives as a percentage of all predictions.

- *F1-Score*

The harmonic mean of precision and recall, where an F-1 score reaches its best value at 100 or worst is zero (Tables 1 and 2).

- *False Positive Rate (FPR)*

This is the ratio of normal instances that are incorrectly classified as intrusions.

Comparative Analysis

Performance Compared with Conventional Methods

Proposed chaotic based optimization with feature selection and shallow neural network was compared for performance to traditional methods a) Linear Regression.

Filter-based feature selection +shallow neural network: using information gain as the feature selection

Wrapper-Based Feature Selection + Shallow Neural Network:Feature selection using Genetic Algorithm (GA).

No Feature Selection + Shallow Neural Network Using all 41 features without selection.

As can be seen in Table 4 the proposed approach performed better for almost all metrics above traditional methods, most importantly overall accuracy, precision and recall as well f1 score. Further, the false positive rate (FPR) was also lowered substantially, which indicates that chaotic-based optimization satisfactorily selects features.

Discussion of Results

Chaotic-Based Optimization

The results show that chaotic elite-based optimization can greatly improve the identification of significant features for intrusion detection. The non-linear nature of the chaotic sequence generated by the logistic map allowed us to traverse the entire feature space comprehensively, resulting in choosing a subset feature that improved the performance of the shallow neural network manifold.

The superior accuracy and F1-score of the proposed method show that it was well capable of discriminating normal network traffic from malicious traffic, mitigating false positives as well as negatives with respect to previous approaches. The most noteworthy among other results is the decrease in false positive rate (FPR) because this implies that our proposed IDS will falsely classify a smaller number of legitimate activities as an intrusion and it on the part of concern if the system really gets applied Vanjulavalli, (2015).

The computational efficiency

Besides, the proposed approach also manifested computational efficiency for both detecting and tracking. Due to its simple architecture, the shallow neural network took less training time and resources than deeper networks so it could be readily employed in real-time intrusion

Table 1: Methods and F1 score

Method	*Accuracy (%)*	*Precision (%)*	*Recall (%)*	*F1-Score (%)*	*FPR (%)*
No Feature Selection + Shallow Neural Network	92.15	91.2	89.75	90.47	6.8
Filter-Based Feature Selection + Shallow NN	93.5	92.1	91.6	91.85	5.9
Wrapper-Based Feature Selection + Shallow NN	94.7	93.8	92.5	93.14	4.7
Proposed Chaotic-Based Optimization + Shallow NN	96.35	95.6	94.85	95.22	3.4

Table 2: Model and F1 score

Model	*Accuracy*	*Precision*	*Recall*	*F1-Score*
SNN (without feature selection)	92.50%	0.91	0.9	0.91
SNN (with chaotic-based feature selection)	95.80%	0.94	0.93	0.94

detection scenarios. Moreover, the feature selection process helped to remove some of the irrelevant and redundant features hence reducing computational costs further, making training and inference quicker.

Limitation and future Work

Although this approach appears quite promising, there are some limitations and issues that need to be further addressed. However, the random nature of chaotic-based optimization necessitates a proper setting for r which may lead to only moderate performance on our benchmark datasets. However, the shallow neural network is computationally efficient and does not necessarily learn as complex patterns from sophisticated attacks. Subsequent work may also consider incorporating chaotic-based optimization within deeper neural networks or even hybrid models that meld shallow and deep architectures. Implementation and deployment in real-time at networks with dynamics networking could also bring some insights to the practical application of the proposed method N.Vanjulavalli,(2019).

Conclusion

One of the key components in protecting networks from the continuously changing landscape of cyber threats are IDS. However, efficiently and accurately dealing with high-dimensional data is a huge challenge that needs to be addressed. This paper presented a new strategy combining chaotic-based optimization with feature selection and shallow neural networks to improve the effectiveness of IDS.

Summary of Contributions

Contributions of this research are:

Optimization technique using chaotic feature selection

The presented study aimed to realize chaotic-based optimization consistently in logistic maps, guiding the feature selection process. This systemic chaos (the system is chaotic enough to avoid the danger of remaining in local maxima) allows for broad exploration across the search space and leads us back to identifying a subset of features that drastically enhances IDS accuracy.

Improved similar performance with shallow neural networks

The shallow neuronal network model was trained for normal and anomalous traffic classification using the feature subset selected. Compared to traditional feature selection methods, the proposed approach achieved significantly better accuracy in most datasets and greater precision while boosting recall (thus reducing FPR) compared with no filtering strategy.

Computational Efficiency

A lightweight shallow neural network with a few feature nodes improved not only model simplicity but also computational efficiency, making the algorithm viable for real-time intrusion detection cases. It is important to maintain this balance between the level of detection performance and computational cost in order for IDSs to be considered practical.

Implications and Practical Relevance

These study results directly influence the way by which we can design and deploy IDS in real-world settings. Adopting the proposed approach would not only increase detection accuracy but also decrease false alarms, which can overwhelm security teams and cause critical threats to be missed. The method is computationally efficient and can, therefore, be used in environments with limited resources, such as IoT networks or edge devices.

Although the proposed methodology can prove beneficial, it has certain shortcomings. Thus, the performance of chaotic-based optimization depends on the selection of appropriate control parameters, and a shallow neural network could have limited capabilities to capture all features in more sophisticated types (e.g., only gradient-based) of attacks.

This could form the basis for future directions with research in:

Exploration of other chaotic maps

Different chaotic maps or hybrid chaotic systems might also be tested to improve the optimization process and obtain better feature subsets.

Integration with deep learning models

It would be more expensive. However, at the cost, it could help complex attack patterns, especially against using chaotic-based feature selection and deep learning models.

Real-time implementation and testing

The proposed method can be implemented in a real-time IDS for its effectiveness on dynamic networks.

Final Remarks

This paper proposed an effective feature selection method for improving the performance of shallow neural networks in intrusion detection using a chaotic search optimizer. Experimental results showed that this method outperforms classic ones, opening the possibility of its usability in real cybersecurity systems. Given that cyber threats will continue to change and adapt, more research is necessary in order to develop new IDS methodologies such as the one presented here.

References

Agrawal, R., & Srikant, R. (1994). Fast algorithms for mining

association rules. In Proceedings of the 20th International Conference on Very Large Data Bases (VLDB) (pp. 487-499). Santiago, Chile.

Ambusaidi, M. A., He, X., Nanda, P., & Tan, Z. (2016). Building an intrusion detection system using a filter-based feature selection algorithm. IEEE Transactions on Computers, 65(10), 2986-2998.

Arulananthan, C., & Kanagarajan, S. (2023). Predicting home health care services using a novel feature selection method. International Journal on Recent and Innovation Trends in Computing and Communication, 11(9), 1093–1097.

Arulananthan, C., et al. (2023). Patient health care opinion systems using ensemble learning. International Journal on Recent and Innovation Trends in Computing and Communication, 11(9), 1087–1092.

Durairaj, M., & Poornappriya, T. S. (2018). Choosing a spectacular Feature Selection technique for telecommunication industry using fuzzy TOPSIS MCDM. International Journal of Engineering & Technology, 7(4), 5856-5861.

Durairaj, M., Poornappriya, T.S. (2020). Why Feature Selection in Data Mining Is Prominent? A Survey. In: Kumar, L., Jayashree, L., Manimegalai, R. (eds) Proceedings of International Conference on Artificial Intelligence, Smart Grid and Smart City Applications. AISGSC 2019 2019. Springer, Cham.

Forrest, S., Hofmeyr, S. A., Somayaji, A., & Longstaff, T. A. (1996). A sense of self for Unix processes. In Proceedings 1996 IEEE Symposium on Security and Privacy (pp. 120-128).

Kanagarajan, S., & Nandhini. (2020). Development of IoT based machine learning environment to interact with LMS. The International Journal of Analytical and Experimental Modal Analysis, 12(3), 1599-1604.

Kanagarajan, S., & Ramakrishnan, S. (2015, December). Development of ontologies for modeling user behavior in Ambient Intelligence environment. In 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) (pp. 1-6). IEEE.

Kanagarajan, S., & Ramakrishnan, S. (2016). Integration of Internet-of-Things facilities and ubiquitous learning for still smarter learning environment. Mathematical Sciences International Research Journal, 5(2), 286-289.

Kanagarajan, S., & Ramakrishnan, S. (2018). Ubiquitous and ambient intelligence-assisted learning environment infrastructures development—a review. Education and Information Technologies, 23, 569-598.

Kennedy, J., & Eberhart, R. (1995, November). Particle swarm optimization. In Proceedings of ICNN'95-International Conference on Neural Networks (Vol. 4, pp. 1942-1948). IEEE.

Kohavi, R., & John, G. H. (1997). Wrappers for feature subset selection. Artificial Intelligence, 97(1-2), 273-324.

Lashkari, A. H., Gil, G. D., Mamun, M. S. I., & Ghorbani, A. A. (2017, February). Characterization of Tor traffic using time-based features. In International Conference on Information Systems Security and Privacy (Vol. 2, pp. 253-262). SciTePress.

Ma, L., Wang, C., & Zhong, X. (2017). An improved particle swarm optimization algorithm for intrusion detection. International Journal of Computational Intelligence Systems, 10(1), 1120-1131.

Mallat, S. (1989). A theory for multiresolution signal decomposition: The wavelet representation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 11(7), 674-693.

Mir, T. T. (2014). Feature selection techniques for intrusion detection systems: A survey. International Journal of Computer Applications, 98(19), 1-6.

Mukkamala, S., Janoski, G., & Sung, A. (2002). Intrusion detection using neural networks and support vector machines. In Proceedings of the 2002 IEEE International Joint Conference on Neural Networks (IJCNN'02) (Vol. 2, pp. 1702-1707).

Poornappriya, T. S., & Durairaj, M. (2019). High relevancy low redundancy vague set based feature selection method for telecom dataset. Journal of Intelligent & Fuzzy Systems, 37(5), 6743-6760.

Reddy, T. R., Janga, M., & Yadlapalli, S. B. (2018). Intrusion detection system using principal component analysis with deep learning. Procedia Computer Science, 132, 1961-1970.

Vanjulavalli, D. N., Arumugam, S., & Kovalan, D. A. (2015). An effective tool for cloud-based e-learning architecture. International Journal of Computer Science and Information Technologies, 6(4), 3922-3924.

Vanjulavalli, N. (2019). Olex—Genetic algorithm based information retrieval model from historical document images. International Journal of Recent Technology and Engineering, 8(4), 3350-3356.

Vanjulavalli, N., Saravanan, M., & Geetha, A. (2016). Impact of motivational techniques in e-learning/web learning environment. Asian Journal of Information Science and Technology, 6(1), 15-18.

Yang, X. S., & Deb, S. (2009). Cuckoo search via Lévy flights. In 2009 World Congress on Nature & Biologically Inspired Computing (NaBIC 2009) (pp. 210-214). Coimbatore, India.

Yu, L., & Liu, H. (2003). Feature selection for high-dimensional data: A fast correlation-based filter solution. In Proceedings of the Twentieth International Conference on Machine Learning (ICML-03) (pp. 856-863). Washington, D.C.

Yuan, Z., Li, C., Liu, W., & Tan, X. (2018). A novel intrusion detection method based on SVM and improved PSO algorithm. EURASIP Journal on Wireless Communications and Networking, 2018, Article 136.

Zhang, P. (2019). A hybrid method for feature selection and parameter optimization in SVM-based network intrusion detection. Journal of Information Security and Applications, 44, 1-10.