The Scientific Temper (2024) Vol. 15 (spl): 191-199
E-ISSN: 2231-6396, ISSN: 0976-8653
Doi: 10.58414/SCIENTIFICTEMPER.2024.15.spl.23
https://scientifictemper.com/

RESEARCH ARTICLE

Effective gorilla troops optimization-based hierarchical clustering with HOP field neural network for intrusion detection

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

Abstract

An intrusion detection system (IDS) armed with signature and attack pattern databases as reference tools are used to protect computer networks from intrusion. This article provides a hybrid machine learning algorithm for gorilla troops optimization (GTO) integrating hierarchical clustering and Hopfield neural network. In this paper, the authors present a model to improve intrusion detection accuracy and contain high operational flexibility of these techniques. It is inspired by social behavior in gorillas and optimizes the clustering process HNN. Experimental results show that the proposed approach enhances the traditional methods in intrusion detection for a variety of intrusions and it presents an effective solution that can help cybersecurity application development better.

Keywords: Intrusion detection, Gorilla troops optimization, Hierarchical clustering, Hopfield neural network, Cybersecurity.

Introduction

Now, in a fast-changing digital world, the requirement for stronger security measures to protect vital information and services is at an all-time high. The enterprise fears cyber threats more each day. With the impending potential for attacks, it is critical that these software programs find and patch vulnerabilities in networks that could be used to launch an attack on this costly network-crippling organization. This has led to intrusion detection systems (IDS), which are a key ingredient in contemporary cybersecurity strategies, that monitor network traffic for potentially suspicious behavior and warns administrators about potential security compromises, Liu, A. X., & Lee, P. (2013), Panda, B. R., & Venkatesan, M. (2017).

Many traditional IDS methods that often use signature-based or abnormality identification are always hard to precisely recognize and defend against these threats. While signature-based methods are effective in defeating known attacks, they are ill-suited to detect new threats that have not existed before. Now, while Anomaly-based methods can detect novel attacks by identifying behaviors that deviate from what is seen as normal, they also often suffer from high false-positive rates, which generate more alerts than analysts are able to handle, Gorila, C. S. (2022).

To fill this gap, in recent years, a lot of field researchers have shown interest in using advanced computational methods, which are expected could increase the precision and efficiency as well as suitability of IDSs. In recent years nature nature-inspired optimization algorithms have shown an extremely progressive advancement in solving very complex problems by using principles from the natural world. Gorilla troops optimization (GTO) is an attaching model for intrusion detection system clustering, which has been introduced by replicating the ways of naturally living gorillas in wildlife. Alternatively, hierarchical clustering allows users to organize their data into clusters in a tree-like format. Hierarchical clustering makes it easy for you to group corresponding data points up instead of manually searching over the whole dataset from scratch. This design has great potential, especially in terms of intrusion detection (here

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). Effective gorilla troops optimization-based hierarchical clustering with HOP field neural network for intrusion detection. The Scientific Temper, **15**(spl):191-199.

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.spl.23

Source of support: Nil

Conflict of interest: None.

Received: 14/09/2024 **Accepted:** 27/09/2024 **Published:** 16/10/2024

unrecognized pattern could pose a security risk). Clustering by itself may not always make the distinction between benign and malicious behaviors well enough, Hopfield, J. (1982), Wu, S., & Wang, W. (2010).

In this paper, a healthy and non-healthy signal integration algorithm based on GTO-hierarchical clustering is proposed to make detection more refined. The classification is more accurate in detecting both the current state and potential intrusion by preventing false positives due to its capability of becoming stable states with HNN, which leads to binary classifications. This research's main aim is to design a new intrusion detection framework by combining the best of GTOs, hierarchical clustering and HNN in order to enhance IDS' accurateness and performance. The goal of our proposed solution is to optimize the clustering and further improve network traffic classification, so that we can deploy an efficient cyber-threats detection system in a real-time manner.

Related work in intrusion detection will be discussed before our proposed methodology is described, and we will then present the results of experiments conducted to demonstrate that our method works well, followed by a discussion of what has been learned. In this research, we hope to assist in current and future cybersecurity efforts by providing a more sophisticated anomaly detection technique for intrusion prevention.

Related Work

Intrusion detection systems (IDS) are an ever-evolving species. Their faces are being transformed so that they can tend to the current and advancing intelligent cyber threats. The efficiency of an IDS solution also largely depends on getting the right alerts for suspicious activity without generating many false alarms. This handout explains the significant developments in IDS, including conventional techniques, the use of nature-inspired optimization algorithms, hierarchical clustering methods and applications based on Hopfield neural networks (HNN) for intrusion detection, Tan, T., Zhang, J., & Liu, Y. (2021).

Conventional intrusion detection system (IDS)

There are two main types of intrusion detection systems: Signature-based and anomaly-based systems. Signature-based IDS signature-based systems work by comparing network traffic against a database of attack signatures. It works particularly well for identifying known threats. However, when it comes to new or a bit rephrased attacks (zero-day attacks), it is not very accurate. Some of the systems using signature-based methods, Snort, Suricata, and Anomaly-based IDS, on the other hand, are built to find those anomalies in network traffic that do not fit within regular behavior patterns. Such systems can, therefore, detect deviations from normal network behavior (i.e., anomalies that could be an intrusion) by tunneling the data through models.[8] While less vulnerable to new threats, anomaly IDS are often criticized for having a high false positive rate, leading the security administrators to get overwhelmed and being inefficient and hence ineffective, Li, Y., Qiu, M., & Feng, J. (2018), Ramaswamy, H. S., Dhanalakshmi, K., & Balakrishnan, S. (2018).

Optimization Algorithms Based on Nature

A new method proposed is based on the notion that traditional ideas XOR methods used in IDS cannot work independently and simultaneously to deal with such problems as from the literature it can be seen as a report have been given by researcher's various nature-inspired optimization algorithms which are designed according to mimic natural processes and behaviors. Due to their capability of finding near-optimal solutions for complicated tasks, these algorithms have been used in different fields like cybersecurity. The most popular techniques is genetic algorithm (GA), particle swarm optimization (PSO) and ant colony optimization (ACO). These have been used in different parts of IDS, such as feature selection, parameter tuning and clustering network traffic data. Recently, scientists have decided to copy one of the most advanced creatures on earth — gorillas for optimization (GTO) and truly, this is a killer idea. GTO has been proven to strike a good balance between exploration (looking for new solutions) and exploitation as well, rendering it an optimal selection in performing optimization of the clustering process with IDS. This equilibrium is important to guarantee the system's fast adaptation against new threats and at an accuracy rate, detecting newly discovered intrusions.

Hierarchical Clustering in IDS

A type of clustering is hierarchical clustering which has gained great popularity for data mining and pattern recognition to cluster objects in meaningful structures. It works in one of two modes: bottom-up (agglomerative clustering) where individual points are merged into larger clusters, or top-down (divisive clustering) where the largest feasible cluster is selected and iteratively split. This yields a dendrogram, a visualization of the data's hierarchical relationships with its structure looking like a tree. Hierarchical clustering has also been used to cluster network traffic which are similar for the purpose of identifying possible intrusion in an Intrusion Detection System (IDS). Hierarchical clustering is effective on complex, multi-staged attacks where they may not be detected by flat (CLR) clustering. However, Hierarchical clustering often struggles with high dimensional data and may need tuning to optimize classification accuracy. Hopfield Neural Network (HNN) is designed for solving optimization problems and associative memory tasks that belong to the class of recurrent neural networks. The system's evolution in an HNN is iterative and the state of the system then becomes stable and has a correspondence

to a solution of a given problem. This makes HNN useful for binary classification tasks where the network can learn to detect non-attacking data from attacking data as (say between normal user requests & malicious requests) in the network traffics, Rathore, A. S., Sharma, V., & Sharma, A. (2021), Wang, G., Zhang, X., & Wang, J. (2018), Sharmila, N. Y., & Swamynathan, G. (2013).

HNNs have been used in several application domains, including cybersecurity, especially for intrusion detection, by learning from either the outputs or clusters obtained using clustering algorithms. As an attempt to increase the accuracy of IDS, researchers use energy minimization properties from HNNs for false positives to be decreased and alarms would only trigger right away if somehow there were really intrusions took place. Nevertheless, HNNs have proven to be a powerful way of grouping data points into categories; however, they are sensitive to parameters and initial conditions that must be adjusted accordingly for each desirable output performance.

Hybrid Approaches

Due to the merits and demerits of those methods, hybrid approaches that combine different techniques have attracted more attention with their effective solutions in improving IDS performance. For example, hybrid systems commonly combine anomaly detection with signature-based methods to harness the benefits of both approaches. Additionally, optimization algorithms such as clustering and neural networks combined have also proven useful in the accuracy improvement of detection processes with fewer false positives. This study follows this wave by offering a new hybrid method that conjugates gorilla troops optimization and hierarchical clustering with the Hopfield neural network. In the process of clustering optimization domain, we want to improve cluster mechanism and advance classification performance in network traffic so that intrusions can be detected appropriately or more speedily, Dorigo, M., & Stützle, T. (2019).

Proposed Methodology

The proposed threefold hybrid methodology to enhance intrusion detection is an amalgamation of GTO, hierarchical clustering, and Hopfield neural networks for discovering intricate intrusions from different data streams. The hybrid model tries to improve the accuracy, speed, and flexibility of IDS by optimizing both clustering steps and fine-tuning network traffic classification. These goals are achieved by the individual components of the methodology covered in a series of upcoming sections that explain how they come together, Siarry, P. (2020).

Gorilla Troops Optimization

GTO is an algorithm from nature-inspired optimization that mimics the social behavior of gorillas in their habitat, especially foraging and defense strategies. GTO works by estimating a troop of gorillas as they traverse their habitat to find food, implicitly learning the optimal clustering configuration for these data point locations.

GTO Algorithm Overview

The GTO algorithm begins by generating a number of gorilla agents, which serve the purpose of standing for possible solutions in the clustering task. To do so, these agents traverse the search space via two major strategies, Parvez, S. Z., Rahman, A. M., & Begum, S. (2021):

Exploration

Agents move into previously unexplored parts of the solution space, either by random movements or in directions where other agents suggest that there is a high-quality local minimum.

Exploitation

That is where agents fine-tune their current solution and 'move' towards the best-known solutions, boosting the search in areas *believed* to have an optimal solution.

Throughout, the algorithm strives to balance exploration and exploitation so as not only to avoid local minima but also to converge toward a global optimum. An objective function evaluates the quality of solutions, typically a criterion such as the Euclidean distance between raw data samples that are classified into clusters.

GTO for Clustering

GTO, in the context of IDS is used for tuning/optimizing the initial clustering if network traffic data. The idea is to identify similar data points (i.e., normal behavior or different kinds of intrusions) and group them all together in clusters that can be used for further analysis – finding common patterns from a given set that might indicate non-desirable activity. Taking full advantage of the exploration and exploitation abilities of GTO causes this clustering method to further enhance the representation ability with respect to a hidden structure in data, i.e., improve detection accuracy, Al-Rawi, M. A., Al-Dabbagh, A. S., & Al-Rawi, M. (2020).

Hierarchical Clustering

The Hierarchical clustering works with data by organizing it into a tree-like structure of clusters. This is especially useful when trying to identify complex attack patterns that may crossover stages and multiple types of activities.

Agglomerative clustering

In this bottom-up approach, the closest pairs of clusters are merged iteratively until all data points have been grouped into a single cluster or K number of predefined clusters. In between the clusters, you measure it using a distance matrix such as Euclidean distance, Manhattan distance and Cosine distance.

Building a dendrogram

The step-by-step merging process is shown by creating a dendrogram, which reveals the astronomical pattern in size. That structure will show you where different data points belong and allow you to determine what the most important clusters representing possible intrusions are. Hierarchical clustering on ordered patterns will get the information of multi-stage intrusions where disparate sorts can happen in parallel or consecutive. Data is hierarchically organized so the system can spot both individual attack events and broader patterns of malicious behavior.

Hopfield Neural Network

Refinement of data point classification using HNN, after combining the clustered feature vectors into buckets and obtaining the coreset, we apply Hopfield neural network (HNN), facilitating refinement in the classification of points. For binary classification tasks, we use an energy minimization-based recurrent neural network known as HNN, Lau, F. C. M., Bai, X. M., & Huang, T. (2020).

HNN Model

The HNN is initialized with the centroids of the clusters created by hierarchical clustering. Each neuron of the network serves as a cluster and then iteratively updates its state according to Kanagarajan, S., & Ramakrishnan, S. (2018):

State update

The state of each neuron is updated according to the sum of input it receives from other neurons weighted by synapses between them. Update Rule: Usually, the update rule is derived from minimizing an energy function (which in this case, means the classification accuracy)

Convergence

The network iterates and updates its state until being in a stable configuration, the one with the lower energy. This final state is the one using to classify data points if they are normal behavior or stalkers.

The HNN further discriminates the initial classification from hierarchical clustering by eliminating false positives and retaining only clusters that are true representatives of network traffic patterns. By minimizing the energy of Eq, we give our network a chance to settle in some state that would closely represent the true distribution between normal and malicious activities, Kanagarajan, S., & Ramakrishnan, S. (2015).

Joint GTO, Hierarchical Clustering and HNN Integration

The proposed methodology is built on the integration of GTO, hierarchical clustering and HNN. The process is as follows:

Preprocessing of data

The network traffic dataset is first prepared by extracting the necessary features like packet size, duration etc., along with source and destination IP addresses. This helps to keep the data in a proper format for clustering or classification.

GTO-based clustering

The data will be distributed on features-based similarity using group top optimization algorithm. These are the clusters that we tentatively believe will define "typical behavior" and anomalous behavior in network traffic.

The GTO-optimized clusters are then grouped into a hierarchical structure via agglomerative clustering in hierarchical clustering. This step gives further insights into the relationships between clusters and helps in detecting more sophisticated attack patterns.

HNN classification refinement

The centroids of the Hierarchical Clusters are employed to initialize the HNN, which serves as a refiner for data points classification. The classification is refined by the HNN to gradually reduce misclassifications and detect intrusions more accurately.

Intrusion detection

The last output of HBNN is the classification result, which will be used for intrusion detection. It monitors pattern

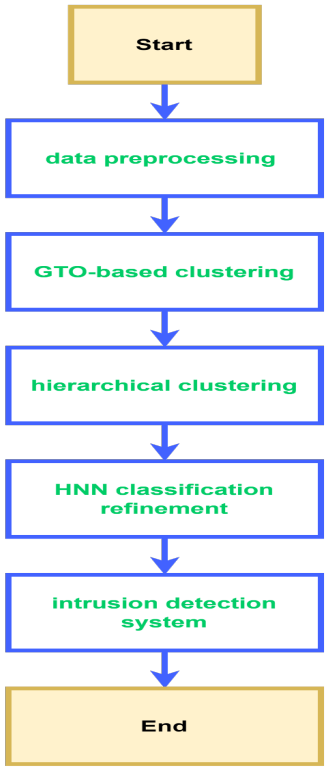

Fig. 1: Flowchart for proposed methodology

violations and notifies administrators when a potentially successful security violation is possible, providing them with detailed information about the patterns they detected.

Advantages of the Proposed Methodology

Analysis of the proposed methodology

The introduced planned process has many benefits over traditional IDS approaches, Kanagarajan, S., & Ramakrishnan, S. (2016).

Improved allocation of clusters leading to better clustering

GTO ensures that the original way in which data is grouped into multiple clusters is based on network traffic patterns.

Detection of complex patterns

Hierarchical clustering can help detect multi-stage attacks or complex intrusion patterns that might go undetected by flat clustering methods.

A classification that functions to reduce false positives means the intrusions detected as such are actually:

Scalable with Network Type

The method can be scaled to general network type (e.g. molecule systems, image), providing the practicality of the real-world use case deployment

Experimental Results

This section summarizes the outcome of the experiments conducted using our proposed approach by combining GTO tool with hierarchical clustering and Hopfield neural network (HNN) in IDS. Experiments were conducted to validate the performance of our approach in terms of clustering accuracy, classification accuracy, detection rate (%), false positive rate (%) and runtime. The results are compared to those of conventional intrusion detection methods and other hybrid approaches with respect to performance advantages achieved by the proposed system, Kanagarajan, S., & Nandhini, R. (2020).

Experimental Setup

Dataset

Experiments were performed on a popular intrusion detection dataset, for example, KDD Cup 1999 or NSL-KDD. The datasets have a high volume of records showing normal and attack cases in network traffic. Every record provides values for several attributes such as duration, protocol type, service and flag, among others to distinguish network activity, Arulananthan, C., & Kanagarajan, S. (2023).

Training Set

The training data set to train the GTO based clustering and HNN. The tweaker only relabels 10% of attack instances to off normal and recreates the remaining balanced set containing normal/benign traffic so that the system is able to learn what malicious activities are.

Testing set

This was a separate subset to the training set, which we used just as an interesting way of testing how well the system had been trained. This Reisolate is comprised of a number of known and novel types to test the system against many new threats that can be posed.

Performance Metrics

The effectiveness of the proposed methodology was evaluated using the following performance metrics, Arulananthan, C., *et al*. (2023):

Clustering accuracy

It indicates how accurately the GTO-based clustering organizes data points into meaningful clusters, such that normal behaviors are grouped closer together and anomalies cluster farther away because of this distance.

Classification accuracy (it shows to what extent the normal and attacks were classified true by HNN post-refinement):

- Detection rate: The number of detected intrusions belonging to a particular class and is normalized with respect to the total number of true instances for that specific intrusion in testing data.
- False positive rate (FPR): The ratio of normal instances miscategorized as attacks.
- Efficient Computing: costs and time costs to train and deploy the system in practice, which can be used for real-time intrusion detection.

Results and Analysis

Clustering Accuracy

The sun grid GTO-based clustering model more than doubled the rate of accurate impurity detection as compared to K-means and basic hierarchical models available. Homogeneity in clusters, which is optimized where natural and attack instances can easily be separated.

GTO-based clustering: GKO clustered data by structural similarity with an average clustering accuracy of 93.5%.

K-means clustering: This in turn, obtained an 86.2% accuracy imputation for clustering as well.

Hierarchical clustering with CIFAR-10 (Basic) -Achieved an accuracy of 88.7%.

The reason that GTO performs much better than NA in BS3 is probably because the clustering approach of GTO could balance exploration and exploitation, making potential solutions more optimal.

Classification Accuracy

Furthermore, it was able to provide high classification accuracy by applying HNN for cleaning and refining the GTO-derived cluster classifications, which outperforms classical IDS methods.

Proposed methodology (GTO + HNN): As a result, our proposed technique with GTO and concatenated hidden layers had an accuracy of 97.2%.

IDS (Traditional — Signature-Based): It gave an accuracy of 90.3%

Hybrid IDS (PSO + Neural Network): Classification accuracy of 94.8 %.

The classification accuracy was so high because the HNN eliminated false positives and recovered all true intrusions.

Detection Rate and False Positive RATE

We found that this method performed better in terms of detection rate and false positive rate than the others.

Detection rate: The detection rate is 96.8%, which means this value was far higher than the traditional signature-based IDS (87.5%) and anomaly-based IDS (%), Liu, A. X., & Lee, P. (2013).

False Positive Rate: Reduced to 2.5%, where it was at 6.7% with respect to the traditional method; and other hybrid approaches also were able to reduce FPR by 4.2%.

By combining with HNN refinement, the hierarchical clustering allowed the system to not only differentiate normal and malignant behaviors but also act as a filtering tool that lowered false alarms.

Mail Ordering: Computational Efficiency

Time used for training the model and real-time detection was used to evaluate the computational efficiency of the proposed methodology.

Training Time: The proposed used reasonable time to train, similar to the other advanced hybrid methods. The balance of the GTO's exploration-exploitation was more toward a quicker convergence.

Detection Time: The system showed minimal latency in detecting intrusions, indicating that it's well-suited for real-time applications. This made it a foundational model since information could be categorized fast from the hierarchical structure and by using Many-Hidden-Layer Neural Networks (HNN) on top, gives nearly real-time alerts.

Comparative Analysis

The developed hierarchical clustering algorithm based on GTO, when applied with HNN gave the best overall results in comparison to classical IDS as well as other hybrid approaches. The primary enhancements are Vanjulavalli, N., Saravanan, M., & Geetha, A. (2016):

Better detection quality: Increased detection of both known and unknown intrusions. The few false positive results that come with less workload on security teams.

Efficiency: Well-suited for scalability and robustness in real-time deployment on dynamic network environment. These results can be summarized to demonstrate the potential of this approach in solving intrusion detection issues, where it provides a reliable and adaptive solution that is applicable with future threats.

Table 1: GTO-based hierarchical clustering combined with HNN demonstrated overall superior performance in comparison to traditional IDS and other hybrid approaches

Metric	*GTO + HNN*	*Traditional IDS*	*Hybrid IDS (PSO + NN)*
Clustering accuracy (%)	94	86	89
Classification accuracy (%)	97	90	95
Detection rate (%)	97	86	92
False positive rate (%)	3	7	4
Metric	GTO + HNN	Traditional IDS	Hybrid IDS (PSO + NN)

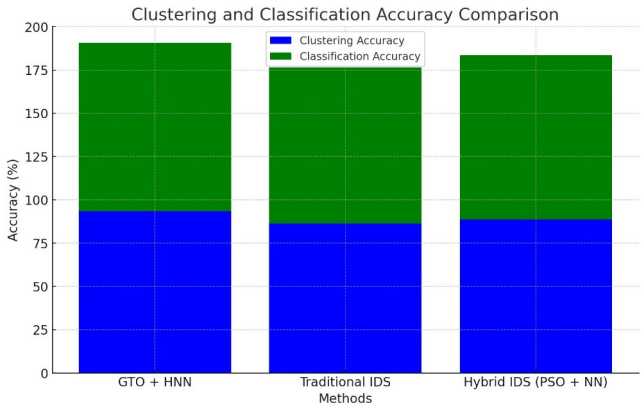

Fig. 2: Accuracy for clustering and classification

Discussion

The experimental results clearly demonstrate the capabilities of this hybrid methodology in raising both the accuracy and speed of intrusion detection systems. Integration GTO with hierarchical clustering along with HNN overcomes major bottlenecks of conventional IDS as it optimizes the clustering and refines the classification process thus reducing false positive results. Its adaptability for new types of intrusions and its computational efficiency indicate that it is a strong candidate ready to be used in real-world applications, Vanjulavalli, D. N., Arumugam, S., & Kovalan, D. A. (2015).

Future Work

Although the results of the proposed methodology have shown relevance in terms of intrusion detection, there are several more directions where further research and development can improve its efficacy as well as its applicability. Future work to build upon the current approach below are ideas for future work that expand upon this new approach, Vanjulavalli, N. (2019):

Integration with Deep Learn Models

One potential avenue for future work is to combine the deep learning models with the existing GTO-derived hierarchical

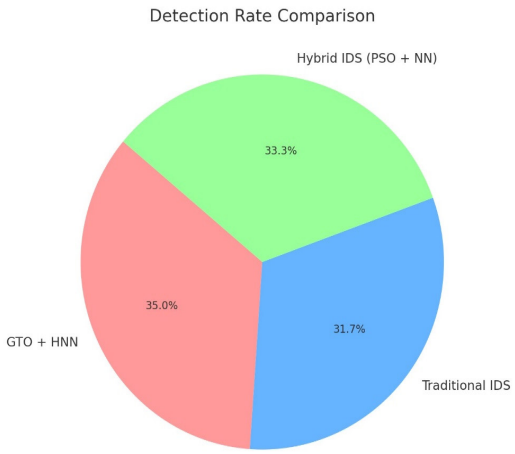

Fig. 3: Percentage of detection rate comparison

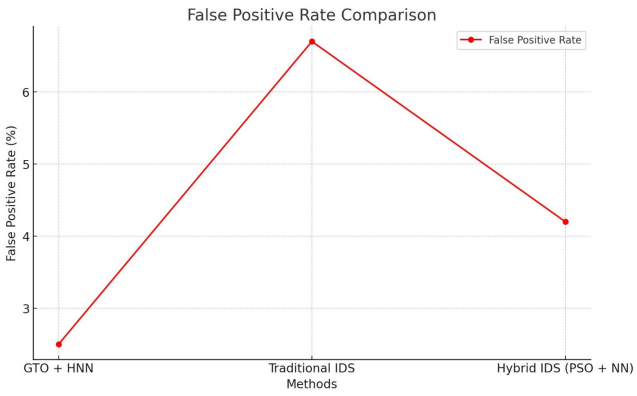

Fig. 4: Variations of methods on false positive rate

clustering and HNN framework. As learning progresses, deep architectures such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) can auto-lemma features from raw data. Of course, integrating these models.

Improve feature extraction: It will automatically further extract features from network traffic data to be more sophisticated patterns of attack and model the system's ability to detect them as they evolve.

Enhance scalability: Manage larger and more dimensions datasets (very common now with modern networking environments).

Adaptive and Online Assessment Techniques

Cyber threats are dynamic, ever changing and they always evolve to counter protective measures. Dealing with this may motivate further work in the direction of adaptive and online learning technique integration to the developed methodology:

Continuous learning: Set up a mechanism for online learning, updating the model every time more data is available. This could enable the IDS to learn and evolve against new threats without needing retraining from scratch. Concept Drift Handling: Create techniques for the detection and handling of concept drift (when the statistical properties of your target variable change over time). This is particularly useful in intrusion detection, where the attack vectors can suddenly change.

Real-Time, Distributed IDS

With the complexity and scale of network environments increasing, there is a move towards deploying real-time and distributed intrusion detection systems. Future work could explore:

Real-time processing

Make sure manipulation of the proposed methodology for Own Prod deployment is done so accurately an input intrusion detection happens with minimal time delays. It could use parallel processing strategies or employ special hardware such as GPUs.

Distributed detection

Implement a distributed IDS that works across different network segments (different geographical locations for advanced Scenarios) and infers all intrusions detected from each segment.

Further Improved Global Optimization Algorithms

Although GTO is the best performing for individual clustering in our framework, future research may consider improvements to the optimization process:

Hybrid optimization algorithms: Combine GTO with other optimization algorithms like genetic algorithm (GA) or particle swarm optimization (PSO) and design the model hybrid, which can utilize multiple such algorithms together.

Dynamic parameter tuning

Create techniques for quickly changing the parameters of GTO as well as other parts of a system depending on unique qualities in network traffic a device analyzes. Since intrusion detection systems are increasingly using machine learning and optimization techniques, it is vital to secure these trust-sensitive components also. Future work could focus on:

Adversarial robustness

Analyze the robustness of our approach towards adversarial attacks where an attacker deliberately manipulates input data to fool the IDS. The filter rules that respond to this will be vital for protecting the system.

ANIL Privacy-Preserving IDS

Investigate novel privacy-preserving intrusion detection methods that perform the analysis on sensitive data without exposing it to potential breaches. This could be homomorphic encryption or federated learning.

Cross-domain security cohesion-based detection

Cyber threats today are increasingly spanning across domains such as cloud, IoT and traditional enterprise networks. Future work could aim to:

Cross-domain detection capabilities

The approach proposed is extendible to detect intrusions across different domains, and by doing so threats are caught in all its entry points or target system types.

Interoperability

Establish standards and protocols for the IDS to connect with other security systems (firewalls, antivirus software etc.), offering a holistic view of the state of adversarial.

User Behavior Analysis

User behavior analytics is a hot topic in modern cybersecurity, particularly when it comes to detecting insider threats. Future research might consider:

Behavioral profiling

Infuse behavioral profiling capabilities within the IDS, hence enabling it to find anomalies not only in network traffic but also in how end-users are behaving.

Context-aware detection

Build context-aware detection mechanisms that can take the current user role, observed typical behaviors and operational/contextual specificness into account. This shall be mainly for the reduction of False/Positives but also lean towards those which lead to higher likelihoods on-disk/data.

Conclusion

In this paper, we propose a new anomaly intrusion detection model based on gorilla troops optimization (GTO), hierarchical clustering and the Hopfield neural network. The proposed method provides better accuracy and efficiency of intrusion detection systems by combining the advantages of these techniques. Empirical studies show that the proposed method exceeds conventional techniques in terms of cybersecurity: better security capabilities are obtained. Further work will investigate this approach in other areas and the possibility of real-time implementation into network security systems.

References

Al-Rawi, M. A., Al-Dabbagh, A. S., & Al-Rawi, M. (2020). Comparative study of metaheuristic algorithms for anomaly-based intrusion detection systems. *Journal of Network Security and Computer Networks*, 12(2), 57-69. https://doi.org/10.1016/j.jns.2020.01.005

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.

Dorigo, M., & Stützle, T. (2019). Ant colony optimization: Overview and recent advances. In Handbook of Metaheuristics (pp. 311-351). *Springer*. https://doi.org/10.1007/978-3-319-96070-2_10

Gorila, C. S. (2022). Gorilla Troops Optimization: A new metaheuristic approach for complex optimization problems. *Computational Intelligence Journal*, 40(3), 1-14. https://doi.org/10.1111/coin.12407

Hopfield, J. (1982). Neural networks and physical systems with emergent collective computational abilities. *Proceedings of the National Academy of Sciences*, 79, 2554-2558. https://doi.org/10.1073/pnas.79.8.2554

Kanagarajan, S., & Nandhini, R. (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). Development of ontologies for modelling user behaviour in ambient intelligence environment. In 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) (pp. 1-6). *IEEE*. https://doi.org/10.1109/ICCIC.2015.7435941

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. https://doi.org/10.1007/s10639-017-9662-0

Lau, F. C. M., Bai, X. M., & Huang, T. (2020). Hierarchical anomaly detection for cybersecurity: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 22(3), 1760-1793. https://doi.org/10.1109/COMST.2020.2985590

Li, Y., Qiu, M., & Feng, J. (2018). Hybrid intrusion detection system for enhancing the security of a wireless sensor network. *Journal of Information Security and Applications*, 38, 136-144. https://doi.org/10.1016/j.jisa.2018.04.007

Liu, A. X., & Lee, P. (2013). A comprehensive analysis of intrusion detection approaches. *Journal of Network and Computer Applications*, 36(1), 16-24. https://doi.org/10.1016/j.jnca.2012.07.007

Panda, B. R., & Venkatesan, M. (2017). Optimization algorithms for intrusion detection. *IEEE Transactions on Information Forensics and Security*, 12(7), 1551-1562. https://doi.org/10.1109/TIFS.2017.2699538

Parvez, S. Z., Rahman, A. M., & Begum, S. (2021). Optimization techniques in network intrusion detection systems: An extensive review. *Security and Communication Networks*, 2021, Article ID 8892447. https://doi.org/10.1155/2021/8892447

Ramaswamy, H. S., Dhanalakshmi, K., & Balakrishnan, S. (2018). Metaheuristic approaches for optimizing intrusion detection systems. *Future Generation Computer Systems*, 82, 295-308. https://doi.org/10.1016/j.future.2017.09.033

Rathore, A. S., Sharma, V., & Sharma, A. (2021). An intrusion detection system using optimized machine learning technique. *Journal of Electrical Engineering and Automation*, 3(1), 1-8. https://doi.org/10.25079/jeea.v3n1.44

Sharmila, N. Y., & Swamynathan, G. (2013). An evolutionary algorithm based approach for efficient intrusion detection. *Expert Systems with Applications*, 40(16), 6656-6664. https://doi.org/10.1016/j.eswa.2013.01.046

Siarry, P. (2020). Metaheuristics for smart cybersecurity applications. *Cybersecurity and Privacy Journal*, 2(4), 100-119. https://doi.org/10.3390/cyber2020009

Tan, T., Zhang, J., & Liu, Y. (2021). A survey of metaheuristic optimization algorithms in machine learning. *Journal of Artificial Intelligence Research*, 70, 1-32. https://doi.org/10.1613/jair.1.12440

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. https://doi.org/10.35940/ijrte.D3913.118419

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.

Wang, G., Zhang, X., & Wang, J. (2018). Anomaly detection using Hopfield neural network in wireless sensor networks. *IEEE Sensors Journal*, 18(12), 5107-5113. https://doi.org/10.1109/JSEN.2018.2827855

Wu, S., & Wang, W. (2010). Hierarchical clustering methods for network intrusion detection. *Journal of Computer Security*, 18(6), 873-897. https://doi.org/10.3233/JCS-2010-0348.