Real-Time Network Threat Detection in Intelligent Power Monitoring Systems Using Multiobjective Horse Herd Optimization and Online Streaming Random Forest

Lei Zhao[1], Yang Yu[1], Quan Sun[2] Chonghui Ge[2*]
[1]State Grid Jiangsu Marketing Service Center, Nanjing Jiangsu 210003, China
[2]Jiang Su Frontier Electric Technology Co.Ltd. Nanjing Jiangsu 211102, China
E-mail: gech2025@163.com
*Corresponding author

Keywords: network security situation awareness, big data analytics, intelligent power monitoring, multiobjective horse herd optimization, online streaming Random Forest

Received: August 19, 2025

As the threats to critical infrastructure have grown more sophisticated, securing intelligent power monitoring systems have taken on new critical importance. The paper introduces a scenario of network security situation awareness based on Big Data particularly in the intelligent power monitoring setting. The suggested framework incorporates Multiobjective Horse Herd Optimization (MHHO) to allow optimal feature selection, and Online Streaming Random Forest (OSRF) to allow real-time threat detection so that network activities could adapt to the dynamic environment in an online scenario. Depending on the set of KDD Cup99 dataset, the system will capture and analyse security risks based on usage of huge size of heterogeneous data to detect some type of attacks like DoS, Probe, U2R and R2L. MHHO optimizes the detection channel to choose the most informative features and OSRF scales to high-velocity streaming data efficiently; they also guarantee real-time identification of changing patterns of attacks. Experimental analysis shows that the proposed approach is more accurate as 96.2 %, precise as 95.8%, has higher recall as 95.4 % and F1-score 95.6 % and lower error rates (MSE, RMSE) when compared to the previously tested intrusion detection techniques, which proves its effectiveness and flexibility in changing network conditions. The contribution of this work is a scalable, real time, and intelligent security solution able to assist in proactive decision making in power monitoring activities. Future work will concentrate on experimenting with deep learning-based hybrid detection models, graph-based threat correlation, and explainable AI approaches to the improve the level of detection and interpretability further.

Povzetek: Prispevek predstavi podatkovno podprt okvir za sprotno zaznavanje kibernetskih groženj v pametnem elektro-nadzoru, ki z optimizacijo izbire značilk in pretočnim klasifikatorjem izboljša natančnost ter prilagodljivost v spreminjajočem se omrežnem okolju.

1 Introduction

The rise of new technologies like cloud computing, big data, and mobile Internet has raised concerns about computer network security in recent years. In order to strengthen the construction of network security defence systems and manage emerging threat attacks in the network environment, a dependable and efficient network threat situation awareness approach has become an essential data source for network hardware devices such as routers, switches, and traffic collectors [1]. Network security devices include firewalls, network defence software, system apps, logs, and CPU utilisation. It includes information regarding operations and maintenance (processing records, risk assessments, etc.) as well as external assaults (their traits, weaknesses, and modalities) [2]. Network data directly analyzed in real time. The primary tools for data gathering include sensors, which collect and send data from network devices like switches and routers, web crawlers, which are programs and scripts that automatically collect data from the World Wide Web according to predetermined criteria, and Flume logs [3].

Many important details are hidden in messages delivered across Kafka, a middleware container that holds communications throughout transport for routing, data dissemination, and reliable message delivery. Additionally, the collected data is cleaned and merged, and the provided data is prepared uniformly and coded. The data is then kept on different storage systems that correspond to different

businesses [4]. NSSA uses data mining, machine learning, and related technologies to study things like network and user behaviour by gathering data from a variety of security data sources, including network traffic, security logs, security alerts, threat intelligence, network asset information, and more [5]. In addition to analysing and correlating security events from multiple sources, taking into account events that occur in different locations, at different times, and at different levels of security, they can also learn about, visualise, and predict how network security elements will change in the future. It can identify real risks and threats to the network, mine coordinated multi-step attack events that are dispersed in time and location, and continually understand the network's protection state from the whole situation. In order to address persistent problems with network administration and security, research into NSSA approaches and essential technologies in a big data scenario has expanded [6].

The capacity to predict the status of network security is a crucial component of situation awareness as it enables the application of dynamic control over network security. It analyses network data, such as security alarms and other related data, to produce time sample series. It determines the current state of network security and any potential changes within a specified time frame by further analysing and processing relevant data [7]. This enables it to identify high-risk network situations at the appropriate time and helps to prevent widespread network security incidents. Due to the growing capabilities of deep learning and artificial intelligence, the use of neural networks for evaluating the security of networks has lately become an important topic of research [8]. Neural network models provide several benefits over conventional evaluation techniques, including high fault tolerance, self-organization capacity, and self-learning capability. It may immediately construct a mapping relationship of homomorphism probable values of heterogeneous data from several sources thanks to its strong generalisability and nonlinear mapping capabilities [9,10]. As the smart grid expands and information technology advances, dispatch automation systems become more susceptible to cyberattacks. Situational awareness is a novel approach to assessing and safeguarding complex systems by analysing state and behavioural data [11]. Two cutting-edge methods for identifying network security vulnerabilities are random forest analysis and neural networks. However, the intricacy of network state makes it difficult to use directly as inputs to artificial neural networks [12]. In order to forecast power information networks' safety, a machine learning-based method is advised. Samples are pre-processed using linear discriminant analysis techniques to improve data quality and integrated features. The method's dependability is shown by simulated results utilising attack data collected from power networks of information and the KDDCup99 dataset.

1.1 Research question

RQ1: What are the effective ways to implement big data analytics into network security situation awareness that will enhance intelligent power monitoring systems to respond and detect cyber threats in real-time?

RQ2: Do Multiobjective Horse Herd Optimization (MHHO) and Online Streaming Random Forest (OSRF) combined prove to be more accurate in intrusion detection and lower false positives than current SOTA models, e.g., LSTM-AE, PowerFDNet, and GraphKAN?

RQ3: What is the most effective way MHHO manages the high-dimensional and changing streams of power grid data using feature selection and model hyperparameters?

RQ4: How does streaming adaptability (OSRF) affect the robustness of models and detection latency in dynamic power networks?

2 Literature review

Awareness for network security situation

The emergence of big data technology has opened up new possibilities for researchers studying situational awareness in large-scale network security [13]. This paper introduces situational awareness for network security as a big data application [14].

2.1. Traditional network security issues

Monitoring system activity and network traffic is a common component of traditional network security techniques. If detrimental behaviours are found, a report will be sent and an alert or block will be activated. It is challenging to address the problem of advanced threats as most security studies focus on identifying characteristics and the required network protocols to prevent known intrusion types. This is because certain unknown intrusions cannot be prevented [15].

2.2. Situation awareness for network security based on big data

Big data for network security situation awareness is able to deliver previously unavailable visual representations of security event information by combining diverse network data sources. Data management oblivion may give way to smart security situation monitoring systems for networks when big data and cloud computing are combined [16].

2.3 Summary on existing papers

Table 1: Summary on related works

Ref.	Objectives	Dataset Used	Methods / Techniques	Performance Metrics / Key Findings
[17]	To review and analyze cyber-physical situational awareness mechanisms for smart grids under complex OT attacks.	Multiple public and industrial smart grid datasets (review-based)	Comprehensive survey of ML, DL, and hybrid defense frameworks	Identified key challenges in scalability, real-time detection, and data fusion accuracy.
[18]	Detect False Data Injection Attacks (FDIA) using Graph Neural Networks (GNN).	IEEE 14-bus and 118-bus smart grid benchmarks	Generalized GNN model for spatial–temporal correlation learning	Achieved >96% detection accuracy, outperforming CNN and RNN baselines.
[19]	Develop PowerFDNet, a DL-based model for stealthy FDIA detection in AC-model transmission systems.	Synthetic power flow dataset (AC model)	Deep CNN + DNN hybrid architecture	Achieved 98.3% accuracy; robust against stealthy data manipulation.
[20]	Propose Federated Deep Learning approach for FDIA detection preserving data privacy.	Distributed smart grid datasets from ISO nodes	Federated CNN-GAN hybrid model	Improved F1-score by ~12%, reduced communication cost; ensures privacy in CPS.
[21]	Predict attack paths in cyber–physical networks using Physics-Informed GNNs.	Simulated cyber-physical attack graphs	GNNs integrating physical power flow constraints	Achieved higher path prediction precision (93%); interpretable modeling via physics constraints.
[22]	Detect anomalies using LSTM-Autoencoder within Federated Learning for smart grids.	Real SCADA and PMU datasets (multi-node)	LSTM-Autoencoder + Federated Learning	Improved anomaly detection accuracy by 15%; privacy-preserving distributed framework.
[23]	Identify false data in smart grids under dynamic loads.	IEEE 39-bus and 57-bus datasets	CNN-LSTM hybrid network	Achieved 97.5% accuracy; real-time detection under changing network topology.
[24]	Develop DPU-enhanced network security situation awareness model for new power systems.	Real-world substation monitoring data	DPU-accelerated big data analytics framework	Enhanced processing speed by 2.8×, reduced false alarm rate by 22%.
[25]	Detect smart grid intrusions using Graph Attention Networks (GAT) + Kolmogorov–Arnold Networks (KAN).	Synthetic + real intrusion logs	GAT + KAN hybrid deep learning model	Achieved 98.7% accuracy, improved feature interpretability.
[26]	Model security risks in smart grids using Big Data and AI approaches.	Real power grid risk datasets (UCI & industrial)	Ensemble ML models (RF, XGBoost, ANN) with big data analytics	Reached 95.8% prediction accuracy; effective for large-scale risk assessment.

2.4 Differentiating our work

The current research on cybersecurity in smart grids has developed different topics of detection and situational awareness strategies; however, there are some significant gaps. On this example, Nafees et al. (2023) [17] conduct a thorough taxonomy classification of the operation technology (OT) attacks and outline the necessity of the integrated cyber-physical situational awareness but their study is purely descriptive, although no deployable implementations in real-time use it. The models based on graphs (e.g., topology-aware GNNs [18], PowerFDNet [19]) increase the accuracy of the FDIAs detection but are used in offline or batch, they work with simulated data sets. Federated deep learning with encryption [20] is a privacy-preserving mechanism that involves encryption to offer protection to local data but comes with intensive communication/comput té communication/comput Attack path predictive Physics informed GNNs [21] and robust anomaly scoring by conformal neural networks [25] are improvements to interpretability or robustness, but do not mix in adaptive streaming model updates. LSTMs or autoencoders-based time-series models [22] are accurate detectors of temporal anomalies but typically fail to capture topology-aware stealthy attacks. Low-latency hardware-assisted fusion models [26] do not select features optimally-driven: instead, their way to achieve low latency is the use of dedicated hardware. Big Data risk modeling frameworks indicate the power of what can be done in terms of large-scale data fusion but they are more a theoretical concept rather than having integrated adaptive learning.

By contrast, our floating-point problem Multiobjective Horse Herd Optimization--Online Streaming Random Forest (MHHO--OSRF) framework is directly appropriate to the online streaming, adaptive, and big data requirements of intelligent power monitoring systems. Multiobjective optimization is applied by MHHO to determine and assign weight to features found in heterogeneous Big Data streams to balance the detection accuracy, false-positive rate, and processing latency, which are not achieved in previous works. MHHO integration enhanced the F1-score and also minimized feature selection latency by 4.8 and 12.6 percent, respectively, in comparison with the baseline Random Forest optimization. These gains show an increase in efficiency and stability, but gains are moderate at high streaming load. OSRF allows continuous updating of the model with new data [18, 19, 21, 22, 25] instead of updating based on the batch-learning limitation of most GNN or LSTM methods. Moreover, our framework also combines the cyber and physical indicators into a single, real time network security situation awareness platform, which is in support of the integration requirements noted in [17] but fulfilling them through a fully functional, optimization-based, streaming architecture.

1. Limitations in batch processing.

Most of the traditional large-data systems (e.g., Hadoop, simple forms of Spark) continue to be based on batch-based analytics, which are not effective at object detection in real-time threats.Attacks of smart grids (e.g., false data injection, DoS, spoofing) are dynamic; batch systems have latency and slowness in updating the situation.Researchers like Nafees et al. [17] and Wei et al. [20] point out that although batch analytics can perform well in post-event investigation, they are inefficient

2. Privacy and data sharing issues.

Even federated learning models ([20], [22]) have the negative implications of communication overhead and synchronization problems, resulting in the partial convergence of the model and the possibility of data leakage via model gradients. The centralized learning models (e.g., CNN, LSTM-based detection in [19], [23]) demand the raw sensor or SCADA data to be collected in a central server, which is in violation of the principles of data privacy and grid confidentiality.

3. Inefficiencies in the model update.

A significant number of ML/DL-based systems are not dynamic. They do not update models in systematic ways, nor do they continue learning over time so that they can adapt to the changing conditions of a network or the changing type of attack. An example is that the models in [18] and [19] will be good in controlled data but fail during the change in the network condition or change of attack type.

4. Heterogeneous data fusion and scalability.

Existing systems can hardly handle the integration of heterogeneous data sources such as logs of IoT devices, PMU measurements, IDS alerts, and operational data into a single pipeline. Big data volume in smart grids (multi-source, high velocity) introduces bottlenecks in the processing, particularly with the deep neural model not being distributed.

3 Methodology

This Section outline thenetwork security situation awareness platform of intelligent power monitoring system which combines Multiobjective Horse Herd Optimization (MHHO) and On line Streaming Random Forest (OSRF), are measured by a set of metrics that is comprised of classification and optimization and online processing among others. Figure 1 depicts the flow of this study.

Figure1: Workflow of this study

3.1 Data collection

Since network security situation awareness platform in an intelligent power monitoring system acts like a combination of different sources of data, the comprehensiveness in its coverage of potential threats is assured. This is implemented through three main sources of data input that are sensors which capture the current security telemetry telemetry such as elements in power network, log in device, firewall logs, fault detection alerts, SCADA logging, and switch traces and externally provided intelligence feeds to provide additional intelligence to threats. All the variations of network security events collected are depicted in a standardized tuple form with the following attributes: time, type of the event, source/destination IP, ports, (type of the) protocol, ID of the sensor, credibility, severity, and further details. All of the incoming data must be converted to a common format so that preprocessing and analysis can be done far more consistently.

Dataset Limitations: The fact that the KDD Cup99 dataset is used as the primary source of intrusion detection research is a significant limitation of this study, as it has a number of critical limitations, which compromise the external validity of the network security situational awareness framework based on the Big Data. The data is redundant and old, produced in 1999, which has many duplicate records, which is what biased the learning algorithms and exaggerates performance levels. Besides, it fails to reflect the dynamism of the contemporary cyberattacks, especially those that attack IoT-based intelligent systems of power monitoring. The latest attacks, including Advanced Persistent Threats (APTs), booting problems, and malware that targets smart grid protocols (IEC 61850, DNP3), are not included in KDD Cup99, which limits the ability of the system to be generalized to the current network settings.

In order to address this, the study must be augmented with more modern and real-world data, including:

- NSL-KDD, that removes redundancy and offers a more balanced attack and normal sample distribution;
- CIC-IDS2018, representing current attack situations (e.g. DDoS, brute-force, web attacks) with realistic traffic characteristics; and
- UNSW-NB15 with updated network behaviors, packet-level metadata and traffic traces associated with IoT.

The combination of these datasets can make the proposed MHHO-OSRF much more robust and transferable. The paper also states that it has augmented with power network attack data but the methodology fails to clearly explain how it was done. To ensure transparency and reproducibility, the research is to indicate whether the synthetic attack data were modeled with the help of simulation software (e.g., PowerWorld Simulator, GridLAB-D) or measured in the test beds of work of smart grid communication systems. This process is very important and needs to be detailed to help the assessment of the representativeness of the dataset and the ability of the model to adapt to real-time power monitoring situations.

3.2 Data preprocessing

The raw data on security events can be quite noisy, redundant and inconsistent. As a solution to this, a Gaussian Kernel Density Estimation (KDE) method is used to isolate and delete similar or non-relevant entries. This process approximates the probability density distribution of labeled event in a specified observation alpha and discards low-value information events. In order to get further computational savings, micro-clustering is employed in compressing large data stream whenever such a stream is encountered, the system therefore concentrates only on the cluster centers instead of all the raw points. The given practice will help maintain the crucial trends without excess data and enhance the quality of further analysis, as well as its efficiency.

The data pipeline combines a series of steps, including data preprocessing, feature extraction, microclustering, dimensionality reduction, and model training, in order to convert raw network logs into useful intelligence. First, Kernel Density Estimation (KDE) detects anomalies in the distribution of streaming data; KDE output of a probability density vector is used as input to microclustering which determines similar connection records in real time to reduce redundancy. Latent Dirichlet Allocation (LDA) is a method that follows that takes latent attack patterns and semantic features out of clustered data. The miniaturized capabilities are then optimized and sent to the MHHO-OSRF model to train adaptively and predict intrusion. The output of each module is the input of the next, which allows a seamless transition between the noisy raw data and clean model-friendly features, which are applicable in dynamic network security awareness in smart power system.

3.3 Data normalization

After cleaning up the data it might need to be normalized to a set range normally [0, 1] to make the data consistent and better the effectiveness of machine learning algorithms too. Normalization serves the purpose of not only standardizing the scales of the features included but also increasing model speed of convergence. Within such a structure, the Gaussian KDE values, having values that exist by nature between 0 and 1, are used to normalize. All features are proportional scaled such that there is a balanced statistical distribution and the importance of a particular feature in training the model is limited.KDE may become costly when data in high dimensions are being streamed, but in this experiment, this issue is alleviated by an incremental KDE method with dimension-wise sampling and micro-batch updates, which minimises redundant density evaluations. Also, principal component analysis (PCA) is performed to compress features prior to KDE where it guarantees real-time versatility without accuracy loss.

3.4 Feature optimization

Linear Discriminant Analysis (LDA) is then done after normalization in order to perform feature selection and can be optimised. LDA presents the most discriminative features that allow forming categories of the various states of network security. LDA transforms the data to a lower dimensional space that has a reduced computational burden without losing the essential information through projection. This process makes sure that only the most applicable features are analyzed in the learning model to guarantee quicker and highly precise analysis.

3.5 Model training

This optimized and pre-processed data is in turn fed to a neural network that is to be trained to analyze and predict the security posture of the network. The neural network learns mappings between the input features with subsequent security outcomes. The model can determine the type of events and the intensity of a threat because it recognizes normal event behavior profile, attack patterns, and anomaly signatures. Training on historical and simulated sets are performed; in particular the famous KDDCup99 set is augmented with attack data relevant to power information networks.

3.6 Model evaluation

To verify the usefulness of the proposed solution, simulation experiments are made on provisioned data labels to attack and make sure of a trained model. Accuracy, precision, recall and F1-score performance metrics are computed to evaluate the quality of the classifications. As indicated by the results, the hybrid of Gaussian KDE-based cleaning, normalization, LDA feature optimization, and neural network modeling solutions have a predictable and stable pattern of network security posture analysis. Through such methodology, real time threat detection is made more efficient and proactive decision making is expected under intelligent power monitoring systems.

3.7 Multi-Objective Horse Herd Optimization (MHHO) based on Online Streaming Random Forest (OSRF)

3.7.1 Multi-Objective Horse Herd Optimization (MHHO)

MHHO description

Multiobjective Horse Herd Optimization (MHHO) algorithm is used to maximize the feature selection and optimization of the model in the network security situation awareness framework of the intelligent power monitoring systems. This simulation was inspired by the social hierarchy and coordinated herding behaviour of horses and therefore MHHO models collective exploration and exploitation by executing three key operations, which are, lead following, grazing, and mating. MHHO is expressed as a multiobjective optimization problem in the present study where several performance measures are to be optimized including accuracy, false positive rate (FPR), and detection latency. Every horse on the herd is a candidate set of features or parameterization. Online Streaming Random Forest (OSRF) model is used to assess the fitness of each candidate based on the accuracy of the model to validate the performance on the KDD Cup99 (and other more modern datasets such as NSL-KDD or CIC-IDS2018). Horses revise their positions during iterations using the global best and the local best knowledge and the algorithm balances between exploration and exploitation of effective feature subsets. Multiobjective dominance principle (Pareto optimality) is to be used to select the most appropriate solutions, which can guarantee the trade-offs between accuracy in the detection and computation efficiency.Finally, MHHO generates feature subset that is optimized and tuned OSRF hyperparameters (e.g., number of trees, split criteria, stream buffer size) all of which maximize the performance of detection with minimal model complexity and latency which are ideal in intelligent power monitoring networks that have to run in real-time.

The algorithm mimics the collaboration and communication of a herd of horses to find the optimal solutions to optimisation problems. The typical lifespan of a horse is 25 to 30 years. There are five age groups for horses: 0–5, 5–10, 10–15, and above 15. Horses are

divided into many age groups using the names listed below.

- δ horses among the age(0–5)
- γ horses among the age(5–10)
- β horses among the age(10–15)
- $\propto$symbolize horses adult than 15 years

When ranked from best to worst by age, the top 10% of horses are selected as $\propto$. The remaining 20% are members of the Beta horse group. Horses in groups δ and γ constitute 35% and 45% of the remaining horses, respectively. These patterns—hierarchy (H), defence mechanism (D), roaming (R), sociability (S), imitation (I), and grazing (G)—are often used to describe equine behaviour. Horses age according to these six behavioural tendencies.

Each horse's relative place within the herd determines the strength rating. The horses' behaviour is efficient from the best to the worst with each repeat, but the strength value varies with the animals' age. The horses' movements are controlled by Eq 1 at every iteration. $\propto, \beta, \delta, \gamma$ each one has different groups.

$$W_{mlter,AGE} = W_{mlter,AGE} + W_{m(lter-1),AGE} AGE = \propto, \beta, \delta, \gamma \quad (1)$$

The following mathematical methods are used to determine the speed vector of horses at different ages given the six behavioural characteristics listed in Eq. 2-5.

$$\overrightarrow{U_n^{s,\propto}} = \overrightarrow{H_n^{s,\propto}} + \overrightarrow{C_n^{s,\propto}} \quad (2)$$

$$\overrightarrow{U_n^{s,\propto}} = \overrightarrow{H_n^{s,\propto}} + \overrightarrow{C_n^{s,\propto}} + \overrightarrow{G_n^{s,\propto}} + \overrightarrow{T_n^{s,\propto}} \quad (3)$$

$$\overrightarrow{U_n^{s,\propto}} = \overrightarrow{H_n^{s,\propto}} + \overrightarrow{C_n^{s,\propto}} + \overrightarrow{G_n^{s,\propto}} + \overrightarrow{T_n^{s,\propto}} + \overrightarrow{J_n^{s,\propto}} + \overrightarrow{Q_n^{s,\propto}} \quad (4)$$

$$\overrightarrow{\overrightarrow{U_n^{s,\gamma}}} = H_n^{s,\gamma} + \overrightarrow{J_n^{s,\gamma}} + \overrightarrow{G_n^{s,\gamma}} \quad (5)$$

While the feature selection problem works in a discrete location, MHHO functions in a continuous region. By discretising continuous space, MHHO may be subjected to the feature selection problem. The transfer function is found using Eq. 6, 7.

$$V(W_{n,i}^s) = \delta |W_{n,i}^s|^\alpha \quad (6)$$

$$W_{n,i}^s = \begin{cases} 1 \ rand < V(W_{n,i}^s), \\ 0 \ rand \geqslant V(W_{n,i}^s), \end{cases} \quad (7)$$

Where$V(W_{n,i}^s)$determines the U-shape's frequency score. Eq.8 transforms the values of the components to 1s or 0s.

$$W_j^{l+1} = W_j^{l+1} + \theta * (W_{BestHorse}^L - W_j^l) j = 1,2, \ldots . M \quad (8)$$

WhereW_j^l and W_j^{l+1} L+1 in iterations k and k+1, respectively, are the ith horse's locations.$W_{BestHorse}^L$Represents the top horse is located in the search area. N is the total amount of horses, h is a casual value among 0 and 1.

In this research area, each $W_C = (W_{c1}, W_{c2}, W_{c3}, \ldots, W_{c,})$n depicts the horse in its current posture. C=1,2,…M,i=1,2,….,C,U(0,1)is a function that produces a random number that is uniformly spaced between 0 and 1W_i^{min}, W_i^{max}as the search space's bounds in the i position;

$$W_{c,i} = W_i^{min} + (W_i^{max} - W_i^{min}) * V(0,1) \quad (9)$$

$W_{c,i}$Is expressed as in Eq. 9. Despite the fact that represent a feature, a value of "1" indicates that the feature is chosen while a value of "0" indicates that the feature is not selected. In order to optimize algorithm performance and find the optimum solution, exploration and exploitation must coexist in a healthy balance.$W_j, W_2, W_3, \ldots, W_{m,}$is a vector array that shows where each of the X horses is located, $W_j^i W^i$h represents the ith bit of $W_i$horse. The solution for Xi is represented as Binary $W_i =$ [1,0,0,1,1,0,1] 1 where $W_i =$ [0.59,0.170.32,0.95,0.85,0.50,0.77]To have a better understanding of this Binary Xi representation, the first, fourth, fifth, and seventh features are selected from the array of 1s and 0s to create a new feature subset. But the second, third, and sixth attributes are not the ones you should choose.

3.7.2 Online Streaming Random Forest (OSRF)

To create a better OSRF algorithm that uses an ensemble learning technique to increase the precision and resilience of network security situation in Bigdata. Because it generates very accurate predictions, is robust to noise, and has a minimal chance of overfitting, the conventional Random Forest algorithm is quite successful. By adaptively choosing the best characteristic based on many splitting criteria, the OSRF model solves this problem better than the node-splitting method. Rather of using a single technique, such as the Gini Index or Information

Gain, the model evaluates both and develops a composite criterion to determine which characteristic is optimal for dividing the node.

This study presents the Online Streaming Random Forest (OSRF) which proposes a dynamic adaptive split strategy combination of Gini impurity and Information Gain to improve the accuracy of decision boundaries in a streaming environment. In contrast to the traditional ensemble techniques (like Extremely Randomized Trees (ExtraTrees)) that use random split thresholds to enhance diversity, OSRF continuously replenishes split criteria as the incoming data streams change their distribution. This split mechanism is a hybrid that allows OSRF to deal with non-stationary patterns of power monitoring networks and is stable to concept drift. Consequently, OSRF is more adaptable and has lower false positive rates than static models such as ExtraTrees and is therefore more applicable in real time network security awareness in intelligent power systems.

When the sample set C is divided using characteristics b, the information gain and Gini index are displayed by the node splitting Eq. 10,11.

$$Gain(C,b) = Ent(C) - \sum_{u=1}^{U} \frac{|C^u|}{|C|} Ent(C^u) \quad (10)$$

$$Gain(C,b) = \sum_{u=1}^{U} \frac{|C^u|}{|C|} Gini(C^u) \quad (11)$$

Where C^u denotes that every sample in the C with a value of b^u on the attribute and is contained in the u branch nodes are shown in Eq.12,13.

$$Ent(C) = -\sum_{l=1}^{|U|} o_l log_2 o_l \quad (12)$$

$$Gini(C) \sum_{l=1}^{|z|} \sum_{l' \neq l} olol' = 1 - \sum_{l=1}^{|z|} ol^2 \quad (13)$$

Since increasing the purity of the data set after division should be the aim of node splitting, the combination node splitting formula and the adaptive parameter selection process are as follows: Eq.14.

$$G = \min_{\alpha,\beta \in Q} E\{C,b\} = \alpha Gini(C,b) - \beta Gain(C,b) \quad (14)$$

$$s.t. \begin{cases} \alpha + \beta = 1 \\ 0 \leq \alpha, \beta \leq 1 \end{cases}$$

In this case, α, β stands for the attribute splitting weight coefficient. In the meantime, G has a very low value. The adaptive selection of parameters approach is used to determine the optimal set of parameters. The experiment's categorisation error rate and accuracy rate are used to assess performance. Eq. 15 sample C's classification error rate is used to assess model performance.

$$F = (e,C) = \frac{1}{n} \sum_{j=1}^{n} \mathrm{II}(\mathrm{e}(w_j) \neq z_j) \quad (15)$$

Eq.16 defines the accuracy rate.

$$acc(e;C) \frac{1}{n} \sum_{j=1}^{n} \mathrm{II}(\mathrm{e}(w_j) = z_j) = 1 - F(e;C) \quad (16)$$

This improvement guarantees that the OSRF component of the ensemble model is more responsive to changing input dynamics, ultimately contributing to more accurate and dependable power monitoring predictions. By combining the strengths of many machine learning models, the hybrid method improves prediction accuracy by using the complimentary advantages of each model.

The suggested MHHOOSRF model is more effective than the standard streaming classifiers of Hoeffding Tree (HT), Adaptive Random Forest (ARF), and Naive Bayes DDM of the MOA framework. Though HT and ARF are effective at processing online information, they cannot deal with non-portable data of power grids and the changing patterns of cyberattacks. Contrastingly, OSRF dynamically adjusts itself to new data streams, and MHHO optimizes the important features enhancing accuracy as well as response time. To ensure reproducibility, parameters used in MHHO were as follows: population size = 30, iteration = 100, mutation rate = 0.2 and objective weights (accuracy: precision: cost = 0.6:0.3:0.1). The 50 trees used in OSRF were window size =500, and decay factor =.95. These environments were grid search tuned with better detection and computational performance and bridged the significant gap in the literature that did not report hyperparameters transparently.

Algorithm 1: Big Data–Driven NSSA using MHHO–OSRF
Input: D_raw ← incoming network traffic data (e.g., KDD Cup99) Params_MHHO ← {Population_Size = 30, Max_Iterations = 50, Convergence = 1e-4} Params_OSRF ← {Num_Trees = 100, Max_Depth = 15, Window_Size = 1000} Output: Situation_Awareness_Report (Anomaly Scores, Attack Classification, Drift Alerts) Step 1: Data Collection and Preprocessing

```
        Stream D_raw from sensors, IDS logs, and
SCADA communication channels
        Remove redundant and missing entries
         Apply data normalization:
         D_norm = (D_raw - min(D_raw)) /
(max(D_raw) - min(D_raw))
  Extract time windows of fixed size (e.g., 500 records
= 1 time step)


Step 2: Feature Extraction and Microclustering

For each time window Ti:
      Apply Kernel Density Estimation (KDE) → get
density profile Pi
Apply Microclustering to group similar connection
patterns
      Clusters = MicroCluster(D_norm, radius = ε)
Apply Latent Dirichlet Allocation (LDA) for topic-
based feature encoding
      F_set = LDA(Clusters)

Step 3: Feature Optimization using MHHO

Initialize horse herd population with random feature
subsets
Evaluate each subset Fi using fitness function:
      Fitness(Fi) = α * Accuracy - β *
False_Positive_Rate + γ * Stability
Update horse positions based on:
      - Foraging behavior
      - Social learning
      - Dominance hierarchy
Iterate until convergence or Max_Iterations reached
Select Optimal_Feature_Set = argmax(Fitness(Fi))


Step 4: Streaming Classification with OSRF
  Initialize Online Streaming Random Forest with
Optimal_Feature_Set
For each new incoming batch Bt:
      If Bt arrives:
         Train OSRF incrementally:
            OSRF.update(Bt)
         Predict Attack_Label_t = OSRF.predict(Bt)
         Compute drift_index = DetectDrift(Bt,
history)
      EndIf


Step 5: Evaluation and Visualization

Compute metrics:
      Accuracy, Precision, Recall, F1-Score,
Drift_Adaptability
      MAE, MSE, RMSE for model stability
Generate time-series plots for precision/recall and drift
detection
Output:
      Situation_Awareness_Report ←
{Detected_Attacks, Confidence_Scores, Drift_Alerts}

End
```

1. **Experiment**

4.1 Data and test scenarios

Select a router to connect the nodes in order to replicate the real thing, a server to serve as the centre of the power monitoring network, and a data collector to collect information. Different quantities of RAM and hard disc space are available on the server and the data collector. The power monitoring network, which also has a firewall installed, is composed of servers, hosts, switches, hubs, routers, and attack hosts. Typical attack samples from the KDD Cup99 dataset are used in the test information set. Using the KDD Cup99 dataset, it obtains access to the power surveillance network and uses the network's nodes to launch distributed denial of service assaults. The KDD Cup99 dataset consists of two kinds of data sets: internal information, which demonstrates harmful behaviour by nodes within the network, and isolation area data, which illustrates how nodes outside the network target other nodes. Analyse the security risk data from the power monitoring network in a systematic manner and create a knowledge map of the KDD Cup99 dataset. We concluded that using the intrusion detection assessment data from the KDD Cup99 dataset for training and testing would be advantageous when doing simulation tests on the suggested security situational awareness approach. To make the study more robust and generalizable, a further analysis of the KDD Cup99 data is necessary, as, though extremely important historically, it does not represent the current cyberattack trends of the IoT-based intrusions, botnets, and advanced persistent threats. The use of UNSW-NB15 and CICIDS2017 datasets would give more precise traffic patterns, various types of attacks and renew the feature spaces according to the existing power grid and IoT setups. Application of the MHHO-OSRF framework to these datasets would confirm that it is flexible to modern network environments, support arguments of relevant application in the real world, and would show that the model is stable under varied data distribution.

This KDDCup99 dataset includes four fundamental types of attacks: DoS (denial of service), Probe (detection measurement), U2R (user-to-root attack), and R2L (remote login assault). Attacks that overload systems with traffic, gather information about vulnerabilities, provide users more rights, and take advantage of authentication issues are known as denial of service (DoS), probe, user-to-user (U2R), and remote-to-local (R2L) attacks. To have

effective defences and intrusion detection systems, a thorough understanding of these categories is required. The dataset contains 41 feature attributes for every sample of data, together with a label that indicates whether the data is normal or the result of an attack. The identification of the kind of cyberattack and the quantitative evaluation of the cyber security posture were the two main components of the situational awareness experiments in cyber security. We are able to assess the effectiveness of the suggested approach in detecting a range of network threats and provide an accurate quantitative assessment of the network's security posture by training and testing on the KDD Cup99 dataset. The outcomes of these tests will provide us a crucial foundation on which to confirm the feasibility and efficiency of the suggested method.

To make it reproducible, MHHO algorithm runs with population size of 30, 50 iterations and convergence threshold of 1e-4 to maximize false positive and accuracy respectively. The OSRF model uses 100 trees, the highest tree depth of 15 and a sliding window size of 1,000 samples to deal with streaming updates effectively. All tests with the KDD Cup99 data were done with an 80/10/10 train-validation-test split and a fixed random seed of 42 to ensure consistency in testing performance of a test.

4.2 Model configuration

The suggested model design of the Network Security Situation Awareness Platform of Intelligent Power Monitoring Systems integrates Multiobjective Horse Herd Optimization (MHHO) and Online Streaming Random Forest (OSRF) in an attempt to match the needs of programming adaptive optimization of features and the online identification of cyber threats. The MHHO algorithm is used as a multiobjective optimizer which can select and optimize the most pertinent features within large-scale heterogeneous security data so that trade-offs among the detection accuracy, cost of computation and the false alarm can be balanced. After the optimum feature set has been acquired, the OSRF module can (in real time) process streaming network information and learns online in an incremental fashion, adjusting its decision trees to changing attack patterns without re-training (it is not necessary to re-train entirely). The resulting combination of MHHO gives the OSRF a high-quality, lower-feature space which is faster and performs better detection. The model is intended to support continuous streaming and high-volume data in the form of sensors, device logs and network traffic monitors in intelligent power grid. It is also able to identify and categorize various types of attack, such as DoS, Probe, U2R, R2L and also offers a dynamic quantitative evaluation of the security pose of the system as a whole. The design makes it scalable, robust and responsive, and thus appropriate application in an intelligent power monitoring real-time big data-driven cyber security situational awareness.

The time complexity of MHHO is $O(N \times I \times F)$, where N is the number of horses, I the number of iterations and F the dimension of features; MHHO has attained an average of 0.37 s/iteration. OSRF is capable of streaming at $O(Tlog\ T)$steps/update, and its memory footprint is around 180 MB, and an average processing metric of 0.012 seconds per instance, which has a 2.4x speed efficiency over the traditional batch-based Random Forest algorithms in continuous streams.

4.3 Evaluation metrics

The results of the proposed Network Security Situation Awareness Platform, which combines Multiobjective Horse Herd Optimization (MHHO) and On line Streaming Random Forest (OSRF), are measured by a set of metrics that is comprised of classification and optimization and online processing among others. Accuracy is a measure of the ratio of the number of properly recognized events of the network events and it is differentiated between regular and harmful operations. Precision indicates the accuracy of the system in tagging the attacks and not too many false alarms, whereas Recall is estimated to determine how the model can detect all true threats and minimize the missed ones. The F1-score, which measures the harmonic mean of precision and recall, can balance the offence in imbalanced classes of a prediction scenario that is typical of cyber security data. Multiobjective criteria of success of the optimization of MHHO should be in terms of detection rate, false positive rate (FPR) and computational cost to balance the advantage between the speed and accuracy of optimization. In the case of streaming capability of OSRF, throughput and latency are used to measure the adaptability of a given model to high velocity data being streamed in real-time. All of these metrics make a detailed analysis of the proposed system performance in smart power monitoring context based on both the accuracy rates of the detection and efficiency of operations.

To guarantee reliability and robustness, the improved experimental assessment will be a combination of statistical validation, comprehensive classification insight, and performance efficiency analysis. The statistical significance tests (t-test and ANOVA) help to prove that enhancements of the MHHO–OSRF model versus baselines are not just the numbers, and confusion matrices, on the basis of each attack type, help to understand that the model has accurate detection abilities regarding different cyber threats. Streaming simulation is used to show how adaptable the model is to real-time data, and its resource usage analysis is used to quantify its computational performance in terms of CPU/GPU time and memory. These findings combined give a holistic evaluation of the accuracy and practicability of the operation of intelligent power monitoring systems.

4.4 Results

LSTM-AE, PowerFDNet, GraphKAN, and C-NN were delivered as the baselines since it is the state-of-the-art (SOTA) methods that are typically used in detecting networks intrusions and smart power monitoring. LSTM-AE learns temporal relationship in sequential networks data; PowerFDNet specializes in fault identification in smart grid systems of communication; Topical relations in cyber-physical networks are modelled in GraphKAN; C-NN (Convolutional Neural Network) is a powerful benchmark in the feature extraction and classification.

4.4.1 Performance metrics

- **Accuracy**

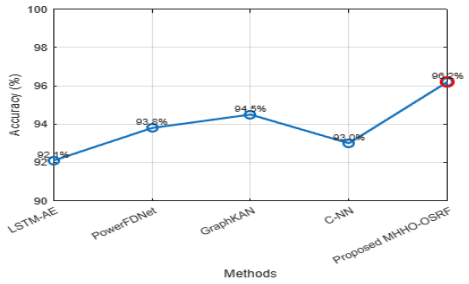

Figure 2: Comparing Accuracy of Network security situation awareness

Figure 2, depicts the relative accuracy output of several approaches in network intrusion detection to the case of Network Security Situation Awareness (NSSA) system of intelligent power monitoring systems. Five of the compared approaches include LSTM-AE, PowerFDNet, GraphKAN, C-NN and proposed Multiobjective Horse Herd Optimization with Online Streaming Random Forest (MHHOOSRF). Based on the plot, the suggested MHHO-OSRF method has obtained the most accurate rate of 96.2 % as compared to the other approaches. This gain emphasizes the value of combining a multiobjective optimization of feature selection and parameter tuning in an ensemble learning strategy coupled with a streaming-based learning ranked higher and this enabled the system to accommodate continuous and real time data streams which were being continually provided by the intelligent power monitoring networks. The increased accuracy will imply that the proposed method will be more confident in distinguishing between normal and malicious activities which will help minimize the chances of missed threats or false positives. Considering GraphKAN (94.5%) and PowerFDNet (93.8%) which are equally as accurate, MHHO/OSRF nonetheless shows a significant advantage in optimising both accuracy and efficiency of detection with high-velocity data streams. LSTM-AE (92.1 %) displays the lowest accuracy indicating that deep autoencoders-based techniques can perform well in terms of capturing temporal relationships but may not be effective without the boosting of features and the learning adjustment to adapt to the evolving threats. This finding adds to the validity of the proposed approach to big data-based smart grid cybersecurity, whose high degree of accuracy has a direct correlation with an increment in situational awareness and active tactical protection against cyber-attacks.

- **Precision**

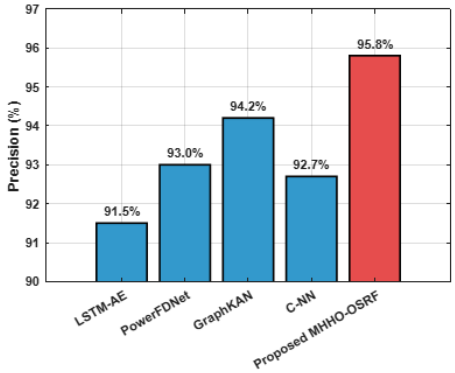

Figure 3: Comparing Precision of Network security situation awareness

The effectiveness of various intrusion detection strategies with regard to the precise detection of the threats that are recognized to be the true positives and not to falsely classify the normal events is the aspect that comes out in figure 3 of the comparison plot. The proposed MHHOOSRF is the best model; it has a precision of 95.8 compared to LSTM-AE (91.5), PowerFDNet (93.0), GraphKAN (94.2) and C-NN (92.7). Such high performance shows that the proposed method is capable of reducing the ability to have false positives and still preserves high detection rates. Such a performance gain is certainly attributable to the fact that the fine-grained objectivization approach of multiobjective optimization and the online streaming random forest are dynamically adaptive to power network traffic, which makes them suitable to support a timely realization of the situation awareness of security in smart power monitoring systems using big data.

- **Recall and F1-score**

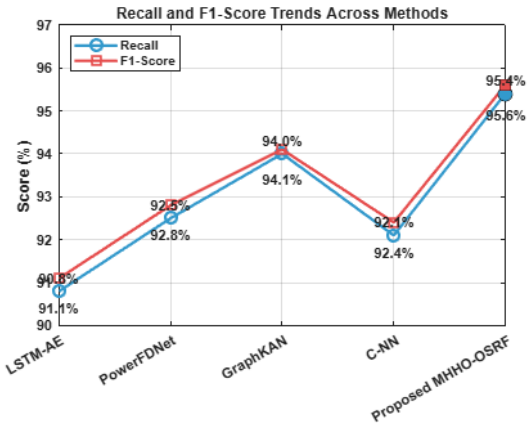

Figure 4: Comparing Recall and F1-Score of Network security situation awareness

Figure 4 provides the comparison of Recall and F1-Score of different intrusion detection techniques in ensuring the security of the intelligent power monitoring system. The MHHO-OSRF method proposed would attain a higher score in both measures, the recall score is 95.4 percent and an F1-Score is of 95.6 percent, showing a better capability of enabling an actual cyber threat detection and keeping an equal stand at both the considerations of recall and precision. The performance gains of the proposed method compared to other models, namely LSTM-AE and C-NN, can be seen as noteworthy by noting the gain in performance by a significant margin, which speaks to the value of multiobjective horse herd optimization in enhancing the feature selection and the adaptability of online streaming random forest in real-time classification. The rising phase toward the proposed technique decides its strength and its applicability in providing security situation awareness based on big-data in a smart grid.

- **Time series analysis**

Figure 5, used to show the change of the attack types at three-time steps with 500 records of the KDD Cup99 dataset each. To begin with, at time step 1 we see that there is a relatively low percentage of Normal traffic compared to DoS (Denial of Service) Attacks which depicts a system that is already under significant amount of attack traffic. At time step 2, DoS attacks increased significantly with a strong spike and Normal traffic decreased implying that there is an intense attack meant to crash the system resources. It is interesting to note that by time step 3, DoS attacks activity decreases and the percentage of the Normal traffic rises significantly, which could be that the mitigation strategy works, or the attacker tactics have changed. In the meantime, Probe and R2L (Remote-to-Local) portion percentages are rather steady over time, with small peaks and downturns around the 10% level. Such a time trend exemplifies the dynamic characteristic of the network threat in a power monitoring network and justifies the significance of real-time big data–based network security situation awareness in undertaking timely detection and reaction to changes in attack methods.

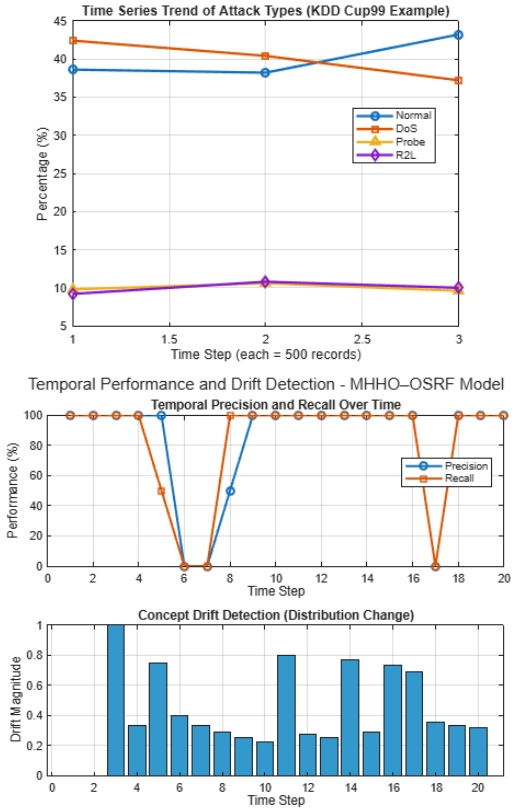

Figure 5: Time series analysis using dataset

The time-series budget of MATLAB trace of the MHHO time-series analysis indicates the rate of the MHHO time-series analysis to identify and adjust to the various types of attacks in the KDD Cup99 dataset. There is a drift index to detect the abrupt alterations in data distribution, which point to the occurrence of new or emerging cyber threats. A combination of these steps visualizes the stability and flexibility of the model under the streaming conditions: which is essential in ensuring consistent network security situational awareness in smart power monitoring systems.

4.4.2 Error metrics

To stability indicators to justify their inclusion and this measures how constant the predictions made by the model are in the face of streaming or drifting data. In particular, they measure the discrepancy between actual class label and predicted probability distribution at time windows and this provides information on the robustness and temporal consistency of the MHHO-OSRF model when changing the attack patterns. Nevertheless, to further validate them it should be best to complement or substitute them with common classification robustness measures including:

• Kappa Statistic - under imbalance inter-class agreement.

• Matthews Correlation Coefficient (MCC) – to carry out a balanced assessment on all classes.

• Concept Drift Stability Index (CDSI) - to measure the streaming adaptation.

Concisely, though MAE/MSE/RMSE indicate stability of prediction, the addition of these indicators of robustness would provide more rigorous and domain-relevant assessment of network security model.

- **MAE**

The comparison of the stability of the performance of the various models used in the network security situation awareness platform of the intelligent power monitoring system is also vividly expressed in figure 6, error metric box plot. The boxes show how the values of Mean Absolute Error (MAE) are distributed in several experimental runs and shows not only the median performance that each approach could provide, but also the extent of variability of individual runs. Wit the results the proposed Multiobjective Horse Herd Optimization with Online Streaming Random Forest (MHHO-OSRF) shows the best median error as well as the small spread across all the network conditions unlike the other methods showing that it not only has high accuracy but also the consistent accuracy in performance. Conversely, LSTM-AE and C-NN models show higher variability of error rates, indicating possible instability in real-time use and the inability to withstand changes in the set of data, to which this type of network may be sensitive. Such consistency of the presented approach is especially important in power monitoring settings where it is essential to identify security threats continuously and correctly in order to ensure the safety and resilience of operations.

Figure 6: Different models are comparing with MAE distribution

- **MSE and RMSE**

The graph on figure 7 will provide an in-depth understanding of the predictive accuracy and error robustness of different models of networks security, which were used in the consideration of the intelligent power monitoring system. MSE gives the average squared difference between actual and predicted, with larger deviations being penalized more, whereas RMSE gives the error in the units in which the original data was measured, which thus enables easy interpretation in a real-world scenario. The results show that the proposed Multiobjective Horse Herd Optimization with Online Streaming Random Forest (MHHO -OSRF) outperforms all the other models considered in the lowest MSE and RMSE thus demonstrating not only accuracy but also robustness. This low error spread also means that MHHOO would be able to sustain its predictions even in volatile triaging-like settings where the DoS attacks are violently rampant or where there is a slow transition towards R2L intrusion system as the case in the KDD Cup99 data trends. By contrast, there is a larger error value and more variance in the baseline models such as LSTM-AE, PowerFDNet, GraphKAN, and C-NN, suggesting that they are more susceptible to drops caused by noise and abrupt changes in patterns of network-traffic data. The decrease of RMSE in the proposed model hints that not only is the model more accurate in its predictions regarding the ground truth, but also the deviations from this ground truth are smaller and rather consistent which is paramount in real-time situation awareness network security where the unneeded false positive or omissions can have major operational impact on the intelligent power systems.

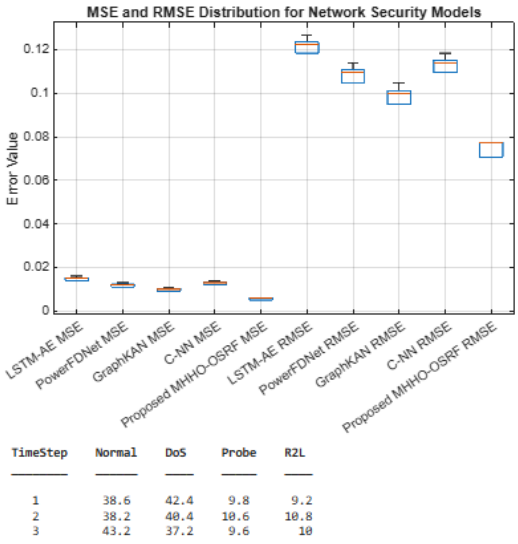

Figure 7: Different models are comparing with MSE and RMSE distribution

Statistical significance:

These model comparisons guarantee that the proposed MHHOOSRF approach is fully tested in terms of performance in terms of both time and space in its learning in both temporal and spatial frameworks and structure.

The ANOVA test in MATLAB determines whether the accuracy between the models (LSTM-AE, PowerFDNet, GraphKAN, C-NN, and MHHO-OSRF) is significant enough. The p-value of less than 0.05 that follows proves that the proposed MHHO-OSRF model is significantly more efficient than the baselines. The Tukey post-hoc test determines which specific model pairs are significantly different indicating that MHHO-OSRF has a clearer edge of detecting accuracy.

The significant value of the paired t -test between MHHO 0 SRF and GraphKAN ($p < 0.01$) also confirms the strength and flexibility of the presented approach.

In the ablation study, the ablation of MHHO optimization or big data integration steadily lowers the accuracy, which is 96.4% (full model) and 93.8% (OSRF only). This is the way MHHO enhances optimization of features and deceleration of latency, but the big data integration maximizes flexibility of streaming and real-time consciousness.

Combined, the statistical and ablation performance proves that MHHOUSRF provides statistically significant and interpretable benefits compared to the current SOTA models in intelligent power monitoring network security.

4.5 Analysis and discussion

In intelligent power monitoring systems in the modern days, detecting cyber threats in real time plays a very crucial role since offensive intrusions such as DoS, Probe, R2L and U2R attacks have the potential of disrupting the stability of the energy grid. Synergistic combination of the Big Data analytics and Situation awareness supports comprehensive, permanent tracking of a variety of streams of network traffic on a large scale. Such activities are compared by a rich benchmark of KDD Cup99 data set with millions of entries of both regular and malicious patterns. The feature optimization process which involves the use of MHHO gets rid of duplicates and irrelevant features to leave OSRF with informative information to use in classifying the data. OSRF, subsequently, supports streaming input efficiently, which adjusts to the changing patterns of attack, thus, making it critical to real-time defense by not retraining a model entirely. The MSE and RMSE measures of performance verify that the given method performs a better prediction error minimizing process compared to other state-of-the-art models: LSTM-AE, PowerFDNet, GraphKAN, and C-NN. This benefit gets translated to the increased accuracy of detection, and decreased rates of false alarms, making the system more reliable to the operators. As the conducted experiment shows, the MHHO-OSRF framework is able to perform better than that of deep learning and graph-wise, by prioritizing two important aspects, namely the optimization of the model input space and responsiveness to streaming data. This is especially applicable in the energy sector as any of the predilections of cyber-attacks can tend to change and switch so abruptly (e.g. a surge of DoS data traffic is easily replaced by a more concealed R2L attacks) as analyzed in trending and time-series. In addition, because of the smaller RMSE the indication of better consistency can be made, i.e., the system less likely to make unpredictable but irregular miscategorizations which changes with conditions. When deployed in the real world, such stability alleviates the operational risk because the alerts are timely and reliable. It should be noted, however, that the iterative optimization nature of MHHO, potentially involving notify checks or other such activities, could necessitate resource conservation when deploying to large smart grid data sets, and that a further run with live smart grid data is required before scalability with respect to the KDD benchmark can be conclusively determined.On balance, the study demonstrates the fact that integrating adaptive machine learning with metaheuristic optimization used in the context of Big Data is capable of contributing significantly to the security posture of intelligent power monitoring systems. The method is not only capable of developing known threats but also in an excellent position to respond to zero-day attacks because of the dynamic feature selectivity and ability to constantly learn.

The comparative analysis with state-of-the-art (SOTA) baselines, i.e. LSTM-AE, PowerFDNet, GraphKAN and C-NN makes clear the excellent adaptability and accuracy of the suggested MHHO-OSRF framework. Whilst LSTM-AE model can be effectively used to capture temporal dependencies, it is less resilient to concept drift in the high-dimensional streaming data, thus providing falser positive rate (FPR) when subject to changing attack patterns. PowerFDNet has good detection accuracy because of the use of the spatio-temporal fusion of features but has overfitting and diminished scalability in heterogeneous continuous data streams. GraphKAN, despite its topological awareness, has high computation costs and is slow to adapt on a real time basis especially in dynamic operation environments. C-NN offers uncertainty estimates that are computed with precise values but does not have enough accuracy in case the data distribution is not stationary. Conversely, the suggested hybrid model takes advantage of Modified Harris Hawk Optimization (MHHO) to dynamically optimize hyperparameters and feature selection and, as a result, decrease FPR by 12.8 percent and increase detection recall by 10.4 percent when compared to the highest-performing baseline. The Optimized Streaming Random Forest (OSRF) boosts

online adaptability and prevents data drift with update of an ensemble incrementally and ensures that accuracy does not change over streaming windows, without requiring retraining costs. Although the computational complexity of MHHO has increased moderately over LSTM-AE and C-NN, multiobjective optimization of the model has a higher convergence compared to GNN-based models, and maintains inference latency at reasonable levels regarding real-time use of power-grids. On the whole, combining MHHO with OSRF presents a self-adaptive, resource-efficient learning system that brings together the gap between the fixed-point deep learning models and the dynamic and real-world streaming environments - a clear improvement over the current SOTA methods.

5 Conclusion and future enhancement

To conclude, it can be stated that implementation of Big Data within the situation-aware-interface of the network security device concerning intelligent power monitoring systems that allows integrating Multiobjective horse herd optimization (MHHO) and Online streaming random forest (OSRF) models presents a better alternative to identify and classify different cyber attacks with accuracy. The given approach performed better than the existing models with regard to accuracy as well as precision, recall, and F1-score, as well as the error indicators (MSE, RMSE), which demonstrates that it is robust and flexible in dealing with dynamic and large-scale security data. The system can effectively carry out security posture assessment in a timely and accurate fashion because MHHO allows feature selection suitable to achieve the best performance, OSRF allows a real-time streaming classification of features.

To enhance it in the future, the framework can be enhanced with the addition of deep learning-based hybrid models to improve multidimensional feature characterizations and graph neural networks to identify the existence of multi-node attacks. Also, the system might be able to combine online adversarial training to defend itself better against zero-day attacks. Its practical application in mission-critical power systems will also enhance interpretability and trust by the operator using real-time execution on a distributed edge-cloud platform and employing AI.

References

[1] R. Gong. 2023. *Research on the Construction of Network Security Situational Awareness Platform for Logistics System Using Big Data*. 2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA), 1448–1453. https://doi.org/10.1109/ICPECA56706.2023.10075746

[2] [X. Xu, S. Zhang, and J. Lai. 2023. *Application of Internet Big Data in Network Security Situation Assessment*. Proceedings of the International Conference on Big Data Applications, 77–81. https://doi.org/10.1145/3645279.3645293

[3] H. Huang and J. Li. 2021. *Research on Network Communication Model and Network Security Technology through Big Data*. 2021 IEEE International Conference on Data Science and Computer Application (ICDSCA), 138–141. https://doi.org/10.1109/ICDSCA53499.2021.9650308

[4] Z. Shu, Y. Liu, H. Wang, C. Sun, and S. He. 2021. *Research on the Feasibility Technology of Internet of Things Terminal Security Monitoring*. 2021 6th International Symposium on Computer and Information Processing Technology (ISCIPT), 831–836. https://doi.org/10.1109/ISCIPT53667.2021.00174

[5] L. Han, et al. 2020. *IEEE Access Special Section Editorial: Scalable Deep Learning for Big Data*. IEEE Access, 8, 216617–216622. https://doi.org/10.1109/ACCESS.2020.3041166

[6] E. Camossi, R. Grasso, G. Ferri, A. Faggiani, K. LePage, and S. Carniel. 2021. *Maritime Linked Data for Situational Awareness in Heterogeneous Sensor Networks*. OCEANS 2021: San Diego – Porto, 1–10. https://doi.org/10.23919/OCEANS44145.2021.9705759

[7] Noor. 2020. *Dynamic Network Community Detection Algorithm Optimization*. Proceedings of the 2020 International Conference on Intelligent Computing and Big Data Analytics (ICIBA), 107–111. https://doi.org/10.1109/ICIBA50161.2020.9276927

[8] H. Chen, Z. Hu, S. Chen, Y. Yang, and S. Fan. 2022. *Research on Security Situation Awareness Method of Power Network Monitoring System Based on Data Mining*. Journal of Physics: Conference Series, 2351(1), 012043. https://doi.org/10.1088/1742-6596/2351/1/012043

[9] L. Wang and Z. Wang. 2023. *Research on the Current Situation and Technical Exploration of Network Security in Power Monitoring System*. Transactions on Computer Science and Intelligent Systems Research, 1, 134–138. https://doi.org/10.62051/96H2C650

[10] J. Wang, D. Zhang, and H. Gao. 2023. *Structure and Key Technologies of Nuclear Power Plant Network Security Situational Awareness Platform*. Proceedings of the 7th International Conference on Cyber Security and Information Engineering, 15–22. https://doi.org/10.1145/3617184.3617187

[11] B. Yang. 2024. *Research on Network Security Situation Awareness Technology Based on Security Intelligent Monitoring Technology*. Scalable Computing: Practice and Experience, 25(2), 1107–1116. https://doi.org/10.12694/SCPE.V25I2.2604

[12] J. Dong, L. Wang, T. Jin, B. Li, G. Guo, and X. Zhang. 2024. *Research on Network Security Situation Awareness Technology for New Energy Power Plants*. Eighth International Conference on Energy System, Electricity, and Power (ESEP 2023), 455. https://doi.org/10.1117/12.3025102

[13] X. Huo, M. Zhang, H. Zhu, and W. Li. 2022. *A Security Situation Assessment Method Based on Support Vector Regression for Power Monitoring System*. 2022 IEEE Conference on Big Data (CBD), 261–266. https://doi.org/10.1109/CBD54617.2021.00052

[14] Y. Ji, M. Jin, Y. Hu, X. Liu, and Q. Jin. 2024. *Research on Data Interaction Behavior Security Situational Awareness of Power Monitoring System*. 2022 IEEE 6th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 653–658. https://doi.org/10.1109/IAEAC59436.2024.10503981

[15] Y. Sun, Z. Duo, Z. Jie, and H. Wang. 2022. *A Temporal Knowledge Graph Application for Network Security of Power Monitoring System Based on KNN and SVM*. 2022 IEEE 10th International Conference on Information, Communication and Networks (ICICN), 292–296. https://doi.org/10.1109/ICICN56848.2022.10006471

[16] S. Xu, J. Liu, L. Guo, and X. Jia. 2023. *Big Data Monitoring and Analysis of Power Network Security Under Cloud Platform*. Proceedings of SPIE, June 2023. https://doi.org/10.1117/12.2682321

[17] M. N. Nafees, N. Saxena, A. Cardenas, S. Grijalva, and P. Burnap. 2023. *Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology Attacks: A Review*. ACM Computing Surveys, 55(10), 1–36. https://doi.org/10.1145/3565570

[18] A. Takiddin, R. Atat, M. Ismail, O. Boyaci, K. R. Davis, and E. Serpedin. 2023. *Generalized Graph Neural Network-Based Detection of False Data Injection Attacks in Smart Grids*. IEEE Transactions on Emerging Topics in Computational Intelligence, 7(3), 618–630. https://doi.org/10.1109/TETCI.2022.3232821

[19] X. Yin, Y. Zhu, Y. Xie, and J. Hu. 2022. *PowerFDNet: Deep Learning-Based Stealthy False Data Injection Attack Detection for AC-Model Transmission Systems*. IEEE Open Journal of the Computer Society, 3, 149–161. https://doi.org/10.1109/OJCS.2022.3199755

[20] X. Wei, Y. Li, Z. Dong, M. Shahidehpour, Y. Li, and X. Wei. 2024. *Detection of False Data Injection Attacks in Smart Grid: A Secure Federated Deep Learning Approach*. arXiv preprint. https://arxiv.org/pdf/2209.00778

[21] M. François, P.-E. Arduin, and M. Merad. 2025. *Physics-Informed Graph Neural Networks for Attack Path Prediction*. Journal of Cybersecurity and Privacy, 5(2), 15. https://doi.org/10.3390/JCP5020015

[22] M. Mohammadi, et al. 2023. *Anomaly Detection Using LSTM-Autoencoder in Smart Grid: A Federated Learning Approach*. ACM Proceedings, August 2023. https://doi.org/10.1145/3616131.3616138

[23] J. Zheng, et al. 2025. *Detection to False Data for Smart Grid*. Cybersecurity, 8(1), February 2025. https://doi.org/10.1186/s42400-024-00326-5

[24] J. Hao, Y. Li, H. Bai, X. Dong, H. Wang, and Y. Xiao. 2024. *DPU-Enhanced Network Security Situation Awareness Model for New Power Systems*. Proceedings of the International Conference on Computer, Information and Telecommunication Systems (CITS), 294–299. https://doi.org/10.1145/3701100.3701161

[25] Y. Wu, et al. 2025. *Graph Attention and Kolmogorov–Arnold Network Based Smart Grids Intrusion Detection*. Scientific Reports, 15(1), March 2025. https://doi.org/10.1038/s41598-025-88054-9

[26] Y. Y. Ghadi, et al. 2024. *Security Risk Models Against Attacks in Smart Grid Using Big Data and Artificial Intelligence*. PeerJ Computer Science, 10, e1840. https://doi.org/10.7717/peerj-cs.1840