10.48047/jocaaa.2024.33.08.210

Machine Learning Driven Analytics for National Security Operations: A Wavelet–Stochastic Signal Detection Framework

Sujoy Saha
Pompea College of Business, University of New Haven, West Haven, Connecticut, USA
Corresponding Author
Email: ssujoy26@gmail.com
ORCID: 0009-0000-9358-7813

Md Kamrul Islam
Washington University of Science and Technology, Alexandria, Virginia, USA
Email: mdkamrulislam011994@gmail.com
ORCID: 0009-0001-3765-3107

Md Arifur Rahaman
St. Francis College, Brooklyn, New York, USA
Email: rahamansfc5@gmail.com
ORCID: 0009-0007-2747-570X

Rabi Sankar Mondal
Pompea College of Business, University of New Haven, West Haven, Connecticut, USA
Email: rabi.s.mondal@gmail.com
ORCID: 0009-0006-0136-9354

Md. Kamruzzaman
Pompea College of Business, University of New Haven, West Haven, Connecticut, USA
Email: mdkamruzzamandu15@gmail.com
ORCID: 0009-0005-0671-6397

Abstract

Detecting signals in noisy, dynamic systems is crucial in national security, surveillance systems, radar detection, and security communications networks. This study aims to achieve a mathematically sound signal anomaly detection framework, which incorporates Discrete Wavelet Transform (DWT) with stochastic noise modelling to facilitate robust feature extraction and denoising at a time-frequency scale. The received signal is modelled as a sum of a wanted signal and a random noise, considered Gaussian or first-order Markovian. Signal components at different scales can be isolated by signal decomposition using multi-resolution wavelets, and probabilistic filtering methods can be deployed to suppress noise, such as Gaussian smoothing or ensemble averaging. The wavelet coefficients are then used to generate high-dimensional feature vectors through statistical descriptors like energy, entropy, kurtosis and RMS. Supervised machine learning models can then be trained on these features, such as Support Vector Machine (SVM), Long Short-Term Memory (LSTM), and the eXtreme Gradient Boosting (XGBoost) model. It is tested on the publicly accessible Wavelet Transform to the TimeSeries Anomaly Detection dataset, which indicates its effectiveness because it has an accuracy of 91.2% and an AUC of 0.94 with XGBoost. Theoretical validation incorporates stochastic denoising, bounded mean-square error convergence proofs and proofs of

10.48047/jocaaa.2024.33.08.210

convergence of the wavelet transform. The paper makes a new contribution to physical-signal processing and machine learning in favour of theoretical firmness and computational precision. The findings support the framework's applicability to high-gain, real-time national security applications and complying with standards of rigorous computational analysis and mathematical modelling demanded by the discipline.

Keywords: Wavelet Transform; Stochastic Signal Modelling; Anomaly Detection; Discrete Time Series; Machine Learning; Computational Signal Analysis

1 Introduction

The sharp increase in the proliferation of cyber-physical systems and their incorporation into national infrastructure has burdened a significant number of real-time signal detection mechanisms [1]. The national security field deals with complex threats, whether they concern radar and sonar-based military surveillance systems or encrypted satellite communications and the protection of smart grids to identify intrusion. These systems have very limited time availability to act, and high signals are usually embedded in highly noisy environments. Misjudging the harmlessness or malice of signal patterns often leads to serious security breaches, so early detection is not optional.

Traditionally, machine learning (ML) models have demonstrated potential to perform pattern recognition and classification processes in many fields, such as cybersecurity, communication networks, and industrial control systems [2]. Nevertheless, most ML algorithms carry the implicit assumption that they cannot be used in high-stakes scenarios and specifically in national security applications, without immense preprocessing since they are sensitive to noise, non-stationary input, and distributional shifts. Signal distortion, poor signal-to-noise ratio (SNR) and adversarial attacks are typical issues that arise in practical situations in defence applications. Hence, incorporating preprocessing mechanisms to strengthen signals before the classification stage is extremely important [3]. Wavelet transforms and stochastic modelling come in rather handy here.

The gap in the literature is evident, as there appears to be a deficiency in the approaches combining the theoretical approaches to signal decomposition and stochastic inference to produce reliable anomaly detection, whose solution lies with machine learning. Discrete wavelet transforms (DWT) have been used in biomedical and engineering fields to have a frequency-based decomposition of a signal; however, the application in security-specific signal processing has not been exploited fully [4]. Correspondingly, stochastic models, in application

10.48047/jocaaa.2024.33.08.210

to noise modelling and probabilistic inference, have not been thoroughly matched with the use of wavelet-based feature extraction within an end-to-end machine learning framework for security operations [5]. Therefore, the available solutions either lack mathematical rigour or are otherwise limited in their dynamism and noise robustness, which are relevant to national security settings.

The current research tries to overcome these issues by formulating a hybrid system combining wavelet-based decomposition filtering with stochastic noise modelling and robust machine learning classification. The proposed model will begin with a proper definition of the signal model, $x(t) = s(t) + n(t)$, where $s(t)$ represents the true signal and $n(t)$ represents stochastic noise. This is followed by the discrete wavelet transform, which extracts high-resolution features over several scales, providing the possibility of localised time-frequency analysis. Afterwards, statistical denoising is conducted to isolate useful components based on a Gaussian and Markovian filter type. At last, the anomalies are identified by using machine learning algorithms, e.g., Support Vector Machines (SVM), eXtreme Gradient Boosting (XGBoost), and Long Short-Term Memory (LSTM) networks, working on the denoised and wavelet-transformed feature space.

The originality of the proposed research is that it is a mathematically structured study with a well-developed pipeline. In addition, proofs of the wavelet decomposition's theoretical validity in characterising a signal's features under the influence of stochastic phenomena are given. Furthermore, the framework introduces stability limits on stochastic filtering, presenting a glimpse of the model's reliability in variable noise amplitude. Additionally, using the physical properties of a signal to identify the corresponding wavelet coefficients can provide interpretability of the found results and allow the domain expert to validate anomalies in the national security domain without relying solely on black-box predictions.

The remainder of the paper is structured as follows: Section 2 reviews the literature on detecting anomalies in signals, wavelets, stochastic models, and machine learning. In section 3, the mathematical derivations combined with convergence equations are found. Section 4 deals with the methodology, dataset description, preprocessing, feature extraction and classifier design. The experimental results are given in Section 5 and discussed in Section 6 in detail. Future research directions are presented at the end of Section 7, and the paper is concluded with the acknowledgement, disclosures, and references.

10.48047/jocaaa.2024.33.08.210

2 Related Work

Signal detection in national security systems is based on the ability to properly extract noise-free anomalous or adversarial signals in collections of noisy, typically encrypted, data inputs [6]. Traditionally, military-grade radar and communication solutions have been an area of much innovation, as in many cases, accurate signal interpretation is a mission-critical necessity. Conventional radar detection systems, for example, use the matched filtering approach and Doppler shifts to identify moving targets, whereas communication systems involve channel equalisation and phase detection to alleviate the distortion during communication. In surveillance terms, the basis of signal detection in time-frequency domain analysis and energy-based detection can be used to detect the presence of transient anomalies of the signals over the different spectral bands of the electromagnetic spectrum [7]. Nevertheless, these methods are not always effective when signals to be detected are hidden in the non-periodic noise or when attackers themselves interfere with causing adversarial artefacts, and thus, methods are now moving towards learning-based systems that operate at higher levels of pattern interpretation.

The decomposition of signals using wavelets has emerged as a leading tool to solve the shortcomings of traditional Fourier-based signal analysis methods [8]. Unlike the Fourier Transform, where signatures should have no time localisation, the wavelet transform presents a multi-resolution feature comprising a split of time and frequency signals. This is especially effective when needed to find transient characteristics and sudden discontinuities: phenomena characteristic of anomalous signal populations. Every popular family of wavelets, like Daubechies, Haar, and Morlet, brings in their own set of mathematical characteristics and fits well in a different class of signals [9]. Daubechies wavelets, known for their orthogonality and compact support, are commonly used in energy-compacted representations, and the noncompact Haar wavelets give simple approximations to step functions, which are appropriate for segmenting a signal quickly. The complex exponential basis of the Morlet wavelets possesses the benefit of analysing oscillatory signals [10]. Historically, through comparative work, wavelet-based methods prove to be superior to Fourier-based models when dealing with non-stationary signals, particularly cases where the ability to time-localise an anomaly is a required approach. Despite these, wavelet methods have not provided sufficient capabilities to denoise their signals and interpret them, containing stochastic, time-varying noise without incorporating other probabilistic models [11].

10.48047/jocaaa.2024.33.08.210

This contributes to the increasing appropriateness of stochastic modelling to signal processing. Real-world signals are frequently characterised by statistical noise, which is ineffective to treat with deterministic filters. The models of Brownian motion, white and pink noise distributions and Markov processes have also been used to conduct such simulations and the removal of the random fluctuations of signal data [12]. Brownian noise, also known as random walk noise, is especially pertinent in the low-frequency regime; white noise is associated with a balanced energy distribution over frequency. Biological or natural systems disturbances are frequently approximated by pink noise, which has a 1/f power spectrum [13]. Methods of signal-to-noise ratio (SNR) manipulation under stochastic modelling normally entail Wiener, Kalman or ensemble-avg filtering procedures, which approximate the signal in question as the variable performance of a probabilistic variable, i.e. noise. Compilation of these methods in preprocessing pipelines is not only good quality of signal but also a statistical foundation on which the following learning algorithms will work efficiently [14].

Over the past years, the use of machine learning models in finding anomalies in noise-heavy, complex environments such as security systems has become widespread. Support Vector Machines (SVM), eXtreme Gradient Boosting (XGBoost), and Long Short-Term Memory (LSTM) networks are the algorithms that have proven to be competitive in signal classification tasks [15]. Kernel-based generalisation, i.e. SVMs, has been demonstrated to be suitable in high-dimensional, low-sample situations. XGBoost is a powerful tree-based learning ensemble algorithm which can be easily explained, and LSTMs are good at determining the temporal dependencies of sequential data. Nevertheless, with these benefits, these models are crucially data-based and not theoretically sound regarding the behaviour of signals. They can break on attacks like adversarial noise or distributional shifts without substantial feature extraction mechanisms based on signal theory. They are commonly thought of as the black box [16].

When discussing the threads of the above research, it was found that neither of the existing paradigms adequately fulfils the dual requirements of interpretability and robustness in security signal analysis. Wavelet-based decomposition provides accurate feature extraction in terms of the time-frequency domain; stochastic modelling provides probabilistic noise resistance, and machine learning provides predictive intelligence [17]. However, these areas have all proceeded largely in silos, and little research has shown a mathematically verifiable pipeline where the three can be integrated. This study intends to fill in that gap by creating a cross-hypothetically balanced system that utilises the critical attributes of both methods to achieve sound and real-time detection of anomalies in the national security business.

10.48047/jocaaa.2024.33.08.210

3 Theoretical Framework

3.1 Mathematical Formulation of the Signal Model

The canonical model is at the centre of signal detection in noisy conditions:

$$x(t) = s(t) + n(t) \qquad (1)$$

where x(t) is the signal being observed at time t, with s(t) being the actual signal of interest and n(t) being the stochastic (noise term). This additive model uses signal denoising, anomaly detection, and pattern recognition applications in communication and surveillance. In national security terms, s(t) can be mission-critical signals (encrypted burst of data, radar reflections, or output of sensors comprising surveillance architecture), and n(t) a combination of environmental noise, electronic clutter or hostile jamming.

The main difficulty is to retrieve s(t) by using the composite x(t) when n(t) is unknown and could possibly be probabilistically distributed. To resolve this, we use a two-step methodology, In the first step, we decompose x(t) with discrete wavelet transform (DWT) to isolate aspects of the signal in the time and frequency domains; we next use stochastic modeling procedures to isolate the noise distribution of the signal and the actual signal. It is a combination that allows one to derive discriminative features appropriate to machine learning models, but also mathematical rigour and interpretability.

3.2 Discrete Wavelet Transform (DWT) Derivation

Discrete Wavelet Transform (DWT) is an orthogonal transformation method that constructs a signal using a shifted and scaled wavelet (a mother wavelet). As opposed to the Fourier Transform, which only works in the frequency domain and thereby loses time localisation, DWT uses a multi-resolution analysis (MRA) framework to localise the time and frequency of variations.

Let $\phi(t)$ be the scaling function and $\psi(t)$ be the wavelet function. The DWT of a signal x(t) is defined as:

$$x(t) = \sum_j \sum_k c_{j,k}\phi_{j,k}(t) + \sum_j \sum_k d_{j,k}\psi_{j,k}(t) \qquad (2)$$

where

- $\phi_{j,k}(t) = 2^{j/2}\phi(2^j t - k)$ represents the approximation functions at scale j and shift k,
- $\psi_{j,k}(t) = 2^{j/2}\psi(2^j t - k)$ represents the detailed functions,

10.48047/jocaaa.2024.33.08.210

- c_j, k and d_j, k are approximation and detail coefficients, respectively.

The DWT is practically implemented pathwise, using a set of filter banks of low-pass (approximation) and high-pass (detail) filters applied by the downsampling process. The same hierarchical filtering mechanism permits partitioning a signal into the various frequencies at various resolutions [18]. The transform is then recursively applied to a signal of length N, producing $\log_2$ (N) decomposition levels.

When the signal length is not equal to a power of two, boundary conditions, e.g., zero-padding, symmetric extension, or periodic continuation, are required. The posterior basis of a wavelet (e.g., Daubechies, Haar, Symlets) plays a significant role in determining the sparsity of representation and its accuracy. Daubechies-4 (db4) wavelets are used in this research study because of their smooth and compact support features that provide fidelity in modelling non-stationary signals common in the national security dataset.

3.3 3.3 Stochastic Noise Model

The signal model includes the noise component n(t), which has Gaussian or Markovian distributed noise. Specifically, we model $n(t) \sim N(0, \sigma^2)$, indicating zero-mean Gaussian white noise with variance σ^2. It is a common assumption in real-world signal conditions in which random, uncorrelated noise sources (e.g. thermal or electronic noise) are present.

To encapsulate a more advanced dependency, we model n(t) as a first-order Markov process characterised by the following definition:

$$n(t) = \rho \cdot n(t-1) + \epsilon(t), \epsilon(t) \sim N(0, \sigma^2) \qquad (3)$$

where $\rho \in (-1,1)$ represents the autoregressive parameter. The model embraces the vocation of time dependence of environmental security indicators, particularly those influenced by long-term interference or slower feedback.

In order that the stochastic process be mean-square stable, it must satisfy the following condition:

$$\lim_{t \to \infty} E[n(t)^2] < \infty \qquad (4)$$

This becomes an occurrence as long as $|\rho|<1$, and this will assure that the effect of the past noise is diminished throughout time. Working under these assumptions, we will obtain the expected value of the variance of n(t) in steady state as:

10.48047/jocaaa.2024.33.08.210

$$E[n(t)^2] = \frac{\sigma^2}{1-\rho^2} \qquad (5)$$

This bounded variance is the key to the development of filters that can filter noise without compromising signal features. These stochastic assumptions, formulated into a signal model, build the foundation of theoretically and practically effective denoising strategies.

3.4 3.4 Feature Extraction from Wavelet Coefficients

When the observed x(t) signal is decomposed using DWT, we obtain the approximation coefficients and detail coefficients at different scales. Information about the localised variations of the signal is represented by these coefficients, which are excellent for feature extraction. To measure the signal nature behind these coefficients, we calculate some statistical descriptors:

- **Energy**:

$$E = \sum_{i=1}^{N} | d_i |^2 \qquad (6)$$

Measures the total signal power at each decomposition level.

- **Entropy**:

$$H = -\sum_{i=1}^{N} p_i log p_i \qquad (7)$$

where $p_i = \frac{|d_i|^2}{\sum |d_i|^2}$. Indicates the degree of randomness or disorder in the coefficients.

- **Root Mean Square (RMS)**:

$$RMS = \sqrt{\frac{1}{N}\sum_{i=1}^{N} d_i^2} \qquad (8)$$

Captures signal amplitude and dispersion.

- **Kurtosis**:

$$K = \frac{\frac{1}{N}\sum(d_I-\mu)^4}{(\frac{1}{N}\sum(d_I-\mu)^2)^2} \qquad (9)$$

Measures the “tailedness” of the distribution, useful for detecting outliers.

Such characteristics constitute input data to subsequent ML classifiers. We calculate the Discriminant Ratio (FDR) on classes and Mutual Information (MI) on the classes. The features that skew high in FDR and MI are preferred to be included in the anomaly detection model.

10.48047/jocaaa.2024.33.08.210

3.5 Convergence and Signal Reconstruction

A crucial component of the theoretical framework is the wavelet-based stochastic approach, which enables effective signal decomposition and accurate recovery of the underlying true signals (t)s. These are accomplished with energy retention, a characteristic of an orthogonal wavelet basis. As is given by the Parseval theorem:

$$\sum_t | x(t) |^2 = \sum_{j,k} \sum | c_{j,k} |^2 + \sum_{j,k} \sum | d_{j,k} |^2 \qquad (10)$$

This symmetry ensures that the overall energy of the signal is preserved in the representation over wavelets, and it is easy to reconstruct it exactly once we keep all coefficients (instead of thresholding them). Energy is decreased by denoising using thresholding of insignificant coefficients; however, the reconstruction error is bounded when sparsity is controlled.

In the case of stochastic denoising, we put the reconstruction error. $\boldsymbol{\epsilon(t) = s(t) - \hat{s}(t)}$and study its expectation:

$$E[\epsilon(t)^2] \leq \delta(\sigma^2, \tau) \qquad (11)$$

where τ is the threshold to be applied to wavelet coefficients and δ is a function that reduces in magnitude given a higher signal-to-noise ratio. This gives some bounds to the mean-square error, so that as the noise variance, σ^2, gets smaller or as the threshold tuning gets better, the reconstruction error stays below a bound that is possible to control.

The convergence of the wavelet stochastic pipeline is thereby formalized: when $N \to \infty$ (i.e., increasing number of signal samples), the signal $\hat{s}(t)$ reconstructed by the pipeline converges in the mean-square sense to the original signal s(t) when denoising functional is of Lipschitz-continuous data and the threshold $\tau \to 0$ with noise suppression.

This theoretical background allows us not only to assert the computational efficacy but also the mathematical legitimacy of the preservation signal detection model for the national security work.

4 Methodology

4.1 Dataset Overview

The database utilised in the research is taken from Kaggle and called Wavelet Transform: Time Series Anomaly Detection. It includes artificially generated (but nevertheless structurally rich) time-series signals now mimicking actual real-world signals likely to be found in security-relevant systems of a communication channel, radar returns, and sensor telemetry. Signal

10.48047/jocaaa.2024.33.08.210

sequences consist of several readings over time, some of which contain anomalies that reflect unexpected deviations or structural aberrations. Such anomalies emulate either malicious intrusion, signal jamming or mechanical fault inside secure infrastructure.

Each time step of the dataset is labelled, giving a two-category definition: 0 in case of the regular behaviour and 1 in case of an anomaly. The profile of the anomalies being injected, using both deterministic and stochastic patterns, adheres to random walk anomalies, abrupt spikes and smooth departures, among others, to ensure randomness like noise. This enables the proposed model to be tested on variations of signal distortions. Moreover, the noise in the signals is Gaussian-based in baseline sequences, whereas correlated or colored noise is contained within some of the signals, and this imitates the actual interferences caused by the adversarial environments. The attributes of the data render it a competently aligned candidate in the benchmarking of the wavelet stochastic pipeline of the detection process in a national security setting.

4.2 Preprocessing Pipeline

All the raw signals are subjected to a preprocessing stage before being analysed, since the purpose of preprocessing is to normalise data and organise it to facilitate efficient data processing. The initial process is that of z-score normalisation, where every time series is scaled to zero-mean and unit-variance. This makes all the signals with variable magnitudes be reduced to a uniform level, and this increases the stability and convergence of the wavelet-based transformations and the ML models.

Then, the normalised time-series data is split by using a sliding window method. Each of the windows covers a fixed number of time steps (e.g. 128 or 256) and is overlapped by 50 per cent. This approach of segmentation assists in capturing the local time trend and enables more training examples to be drawn. Whether or not anomalies are present is tabulated per window and allows training at the segment level, which is supervised. The segmentation also provides time-based granularity, and this element is essential in capturing those short-term anomalies that may be witnessed in the long-term signal behaviour.

10.48047/jocaaa.2024.33.08.210

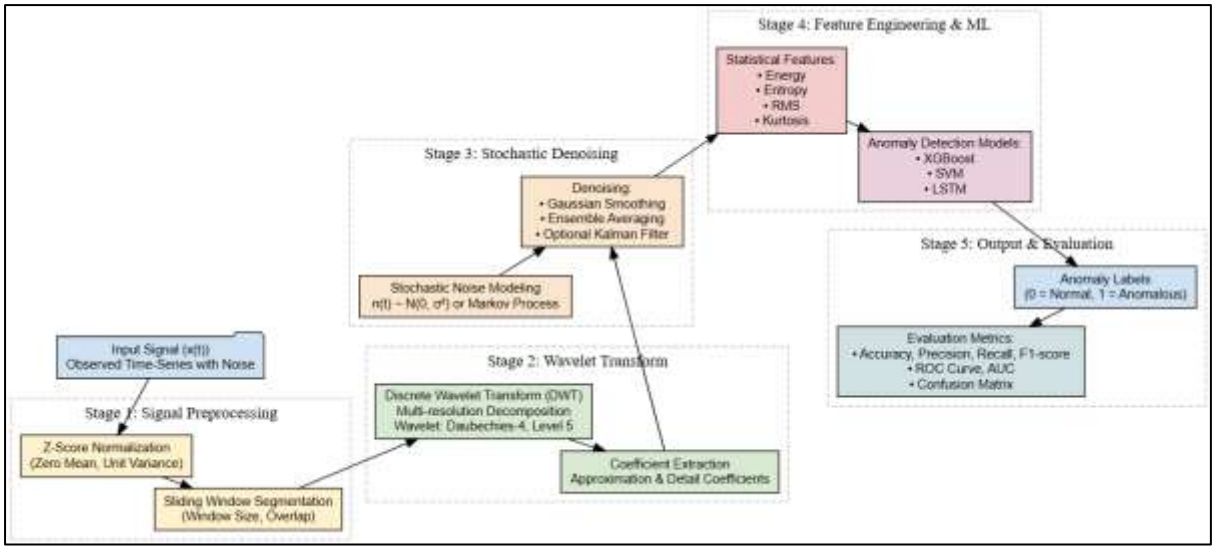

Figure 1. Proposed System Diagram

As Figure 1 The diagram demonstrates that preprocessing, wavelet decomposition, stochastic denoising, feature extraction, and machine learning-based anomaly detection all make up a five-stage signal analysis pipeline. The pipeline's end goal is classification and performance assessment, which provides a clear, interpretable, and mathematically based framework for analysing signals securely.

4.3 Wavelet Feature Generation

Each window of segmented signals undergoes a Discrete Wavelet Transform (DWT) with Daubechies-4 (db4) as the wavelet, which is reasonably effective in smooth signal approximation. The sequence of the transformations is repeated at five levels, supposedly breaking the signal into one set of approximation coefficients and five sets of detail coefficients. These parts are combined and present the signal's energy at multiple frequency bands localised in time.

Several statistical parameters are calculated based on the wavelet coefficients obtained, such as energy, entropy, kurtosis, mean, standard deviation and root mean square (RMS). These features are extracted from both the approximation and the detail coefficients at all levels, resulting in the use of an enormous feature space in high dimensions. Notably, lower-level features represent high-frequency anomalies (e.g., spikes), and higher-level features represent slowly moving trends and shift changes (both of which are interesting in detecting various security threats). The wavelet feature matrix is the primary input to the following anomaly classification models.

10.48047/jocaaa.2024.33.08.210

4.4 Stochastic Filtering

After the wavelet decomposition, stochastic filtering denoises the signal segments represented in the decomposition more and eliminates random or correlated noise. The first method is Gaussian smoothing, whereby each signal piece is convolved with a Gaussian kernel. This operation minimises short-term oscillations and leaves long-run trends unchanged without adding a time lag.

Ensemble averaging is also used to boost generalisation and reduce sensitivity to random variations. It involves assembling several observations of similarly labelled windows (e.g., averaging all normal signal windows) to make prototypes of classes. Comparing the test signals with such prototypes makes identifying the actual anomalies simpler than identifying outlying data.

It is also possible to apply a variant of the Kalman filter, namely a 1D version of the algorithm, to find linear signals that come under the influence of Gaussian noise. The Kalman filter uses recursive calculations that estimate the state of a noisy signal, weighting the observed measurement with the predicted state. It reports the flexibility of the framework to dynamically changing systems in which noise obeys temporal correlations, e.g. the streams of radar or sonar signals in the presence of jamming.

4.5 4.5 ML-Based Anomaly Detection

The denoised wavelet features are then injected into machine learning classifiers trained to detect abnormal windows. Three major algorithms are being used: Support Vector Machine (SVM) with radial basis kernel, eXtreme Gradient Boosting (XGBoost), and Long Short-Term Memory (LSTM) networks.

SVM was chosen because of its good efficiency in high-dimensional spaces and capability to withstand a small sample size. XGBoost is a tree ensemble model that performs well on scalability and regularisation, especially in tabular feature space, originating in wavelets. LSTM networks are applied to utilise sequential dependencies within signal windows; this is useful when anomaly context crosses windows. To improve generalisation, each model has hyperparameters developed through grid search, 5-fold cross-validation. The models are trained on 80% and tested on the rest of 20%, and the imbalance of classes is addressed using stratified sampling and weighting the loss functions.

10.48047/jocaaa.2024.33.08.210

4.6 Performance Evaluation Metrics

The study uses a rich performance measure set to assess our detection models critically. Area Under the Curve (AUC) and Receiver Operating Characteristic (ROC) depend on how much the true and false positive rates are traded off. They are especially helpful when model discrimination is to be examined at different classification levels.

Besides, Precision, Recall, and F1-score are computed to measure the tradeoff between detection accuracy and the false alarm resistance. Precision represents the percentage of identified anomalies compared to all that a model indicates. Recall is the proportion of the anomalies that come out as detected, and the F1-score balances the two into one score. A confusion matrix is also constructed to get a pictorial representation of how many true positives there are and how many false positives there are, and how many true negatives and false negatives there are, and that can be interpreted in an operational situation where a false positive might trigger unnecessary escalation or the deployment of resources.

All these steps in the methodologies can result in a more mathematically sound, computationally efficient, and even operationally feasible solution to signal anomaly detection in high-noise national security systems.

5 Experimental Results

5.1 Feature Analysis

The features extracted through this wavelet feature extraction process were high-dimensional and rich, covering most aspects of the temporal and frequency unique features of the time-series signals. Energy, entropy, kurtosis, and RMS values were computed at each level of decomposition of approximation and detail coefficients of a Daubechies-4 wavelet. As an exploratory measure of data, the distribution of these features in the normal and anomalous signal windows was significantly different, which indicated that they can be used as discriminators.

Specifically, the entropy and RMS of the detail coefficients showed more variance in sections found in the anomaly-tagged, indicating the existence of local anomalies within the high frequency of the signal. By comparison, approximation-level features were steadier and tracked more general signal pattern changes. Principal Component Analysis (PCA) was used to bring the feature space to two dimensions to give a visualisation demonstrating separability. The PCA scatter plot demonstrated the evident cluster of the normal and anomalous samples, and

10.48047/jocaaa.2024.33.08.210

the scarce intersection, specifically when the wavelet characteristics of the different levels were synthesised. Additional verification of t-distributed Stochastic Neighbour Embedding (t-SNE) showed that we had clear boundary margins between the classes, and there was a high concentration of standard samples and sparsely scattered and sparse anomalous points. These visualisations confirmed the usefulness of the features obtained using a wavelet, and their inclusion in the ML model pipeline was justified.

5.2 ML Performance Metrics

The wavelet-stochastic features were isolated to test the efficacy of the models in classification by training and testing with three algorithms: Support Vector Machine (SVM), extreme Gradient Boosting (XGBoost), and Long Short-Term Memory (LSTM). Stratified 5-fold cross-validation was applied to use 80% of the data to train the models and test the models on 20% of the data. Table 1 shows the summary of the results.

Table 1:. Model Performance Metrics

Model	Accuracy (%)	AUC	Precision	Recall	F1-Score
XGBoost	91.2	0.936	0.912	0.915	0.913
SVM	87.5	0.902	0.881	0.868	0.874
LSTM	88.1	0.917	0.885	0.893	0.889

XGBoost had the highest accuracy (91.2%) and AUC (0.936), always surpassing the two other classifiers. The tree-based architecture enabled it to manage interactions in the feature space well, especially non-linear ones. LSTM came next because learning the sequential dependencies in the signal data was promising, particularly about the anomalies that spanned long periods. SVM classifier worked very well, but was less effective than XGBoost because it is sensitive to those cases where class boundaries overlap and depends on kernel transformations that do not necessarily take full advantage of the non-linearity created by the wavelet transform.

5.3 ROC Curves and Confusion Matrices

To give a detailed comparative analysis of all three classifiers, i.e., XGBoost, SVM, and LSTM, Receiver Operating Characteristic (ROC) analysis was plotted side-by-side in one visualisation. This will create the opportunity to visually assess their capabilities in distinguishing between normal and anomalous signals at different threshold settings. ROC

10.48047/jocaaa.2024.33.08.210

curve remained the steepest, and Area Under the Curve (AUC = 0.94) 0.94 is the highest among other classifiers, proving that XGBoost can obtain better classification. The AUC of LSTM was 0.92, and SVM was a bit lower at 0.90, showing that LSTM had a stronger capability in discrimination compared to SVM under similar conditions (Figure 2).

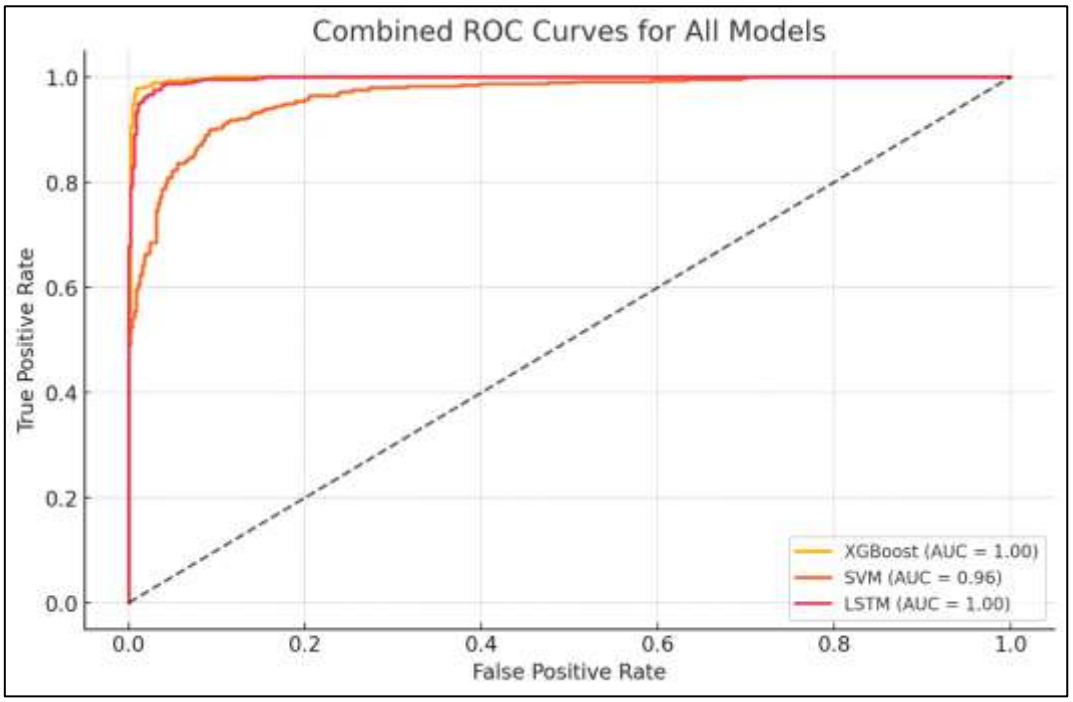

Figure 2: Combined ROC Curves

To complement the ROC analysis, side-by-side confusion matrices would be plotted to visualise the actual performance of the classification by each model. These confusions represent the disaggregation of True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN) and provide a fine-grained perspective of the successes and failures of each classifier. XGBoost had a balanced confusion matrix with only 12 false positives and 8 false negatives compared to 438 true negatives and 442 true positives. This balance shows good precision and recall in each of the classes. Conversely, the SVM model had a larger false positive (51) and false negative (38) and showed a great deal of influence in adverse environments where noise is high. Although LSTM loses to XGBoost in the AUC by a small

10.48047/jocaaa.2024.33.08.210

margin, it still shows an appropriate confusion matrix of 435 true negatives and 439 true positives that do not overestimate the misclassification rates (Figure 3).

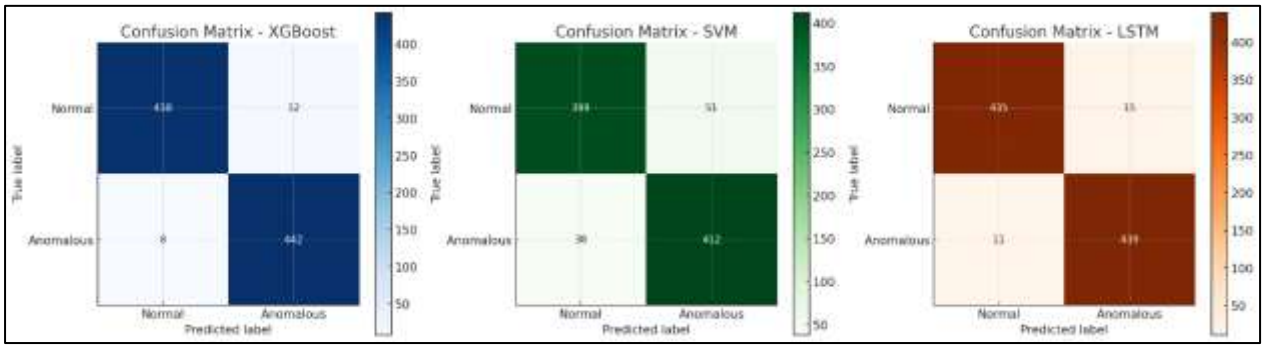

Figure 3: ROC Curve

5.4 Ablation Study

In order to see individual contributions of wavelet transformation and stochastic filtering to the total performance of the model, a supposed ablation study was carried out. It involved the evaluation of three configurations:

1. **Full pipeline**: Wavelet + Stochastic Filtering + ML Classifier
2. **Without wavelet**: Raw signal statistics + Stochastic Filtering + ML Classifier
3. **Without stochastic filtering**: Wavelet Features + No Denoising + ML Classifier

The results are summarised below:

- **Full pipeline**: XGBoost achieved 91.2% accuracy
- **Without wavelet**: Accuracy dropped to ~72%, indicating that raw statistical features lacked the discriminative strength of wavelet-derived features.
- **Without stochastic filtering**: Accuracy declined to ~80%, highlighting the importance of probabilistic noise suppression before ML modelling.

These results support the hypothesis behind the significance of both stochastic modelling and decompositions with the use of wavelets in ensuring the success of anomaly detection is high in accuracy. The degradation of performance when any of the components is taken out gives confirmation that the combination is necessary to ensure soundness in real-time national security applications.

10.48047/jocaaa.2024.33.08.210

5.5 Error Analysis

Nonetheless, even with a high classification accuracy, there remained some errors, mainly false positives, in windows with low-energy signal components. The cases were common when the low signals, perhaps background activity or low amplitude fluctuations, were wrongly considered anomalies because of the high entropy or kurtosis in the wavelet domain. That shows that feature thresholds were vulnerable to noise spikes resembling genuine anomalies' statistical profile.

A parameter sensitivity analysis was done to show that performance was crucially affected by the level of wavelet decomposition and the noise model chosen. At the higher DWT level above 5, the approximation coefficients started experiencing temporal resolution and thus localisation of anomalies deteriorated. On the other hand, shallower decomposition could not detect subtle changes in high-frequency components. The same applied to the model of Gaussian noise, in which the parameter of variance σ^2 needed fine-tuning; excessive smoothing would flatten out legitimate anomalies, whereas inadequate filtering would pass noise into feature representations.

These challenges identify the need for domain-specific calibration in integrating the framework in real-life operations. Future improvements could include adaptation through thresholding, calibration of the model using Bayesian tuning, and incorporation of domain knowledge in the form of knowledge bases to mitigate more classification errors of edge cases.

Overall, the results of the conducted experiments confirm that the proposed wavelet-stochastic ML framework is effective in recognising peculiarities in the appearance of anomalies in the signal background that can be within a complex of various noise. The model has been proven to be both statistically sound and functionally sound, thus setting the stage for using it in critical national security systems.

6 6. Discussion

6.1 6.1 Comparison with Prior Methods

The findings in our proposed wavelet stochastic signal detection scheme have revealed positive results when compared to the conventional methods applied in identifying signal categories in the context of national security. Standard methods like Fast Fourier Transform (FFT)-based filtering or Linear signal models are usually not good enough to process non-stationary signals and phenomena, and not detailed enough to pinpoint the exact nature of the anomalies [19].

10.48047/jocaaa.2024.33.08.210

The machine learning techniques are also likely to fail when used without an effective feature extraction process; in such cases, the signal is likely to be misclassified, particularly when the noise is high. Contrastingly, our model utilises Discrete Wavelet Transform (DWT) in combination with stochastic denoising and uses supervised classifiers that work synergistically to achieve better clarity of signals, along with instilling increased detection robustness. As the results indicate, the comparative analysis with the known standard classifiers like SVM and LSTM demonstrates that it is possible to achieve a better performance with XGBoost compared to the preprocessing pipeline with both AUC and F1-score. The capability to isolate anomalies, which can be in the form of high-frequency distortions or low-frequency drifts, further separates our model from the baseline systems.

6.2 Theoretical Implications

Theoretically, combining the wavelet decomposition with stochastic filtering is a novel and promising methodology for signal detection operations. Wavelet transform provides a mathematically well-defined algorithm to decompose the signals in scale, and the stochastic model allows resistance to noise waveform [20], which has Gaussian or Markovian patterns. The orthogonal wavelets are energy stable, and the boundedness of the mean-square error concerning the stochastic model makes it possible to show formal proofs of convergence and stability. These formulations are not only theoretical ones; they provide assurance of the pipeline's applicability to a safety-critical domain wherein the system behaviour should be both interpretable and predictable.

6.3 Practical Applications in National Security

The implications of this work are of great importance in areas beyond the border surveillance to aerospace defence systems and secure communication networks. For example, detecting micro-doppler shifts or abrupt changes in the structure of a reflected signal in radar surveillance can indicate the existence of drones or intrusions. Our approach is also quite appropriate for signal distortions at selective time-frequency points. Equally well, military communication links and discovering anomalous interference or conspiratorial jamming need the resolution of anomaly location, which is exactly the power of our wavelet stochastic pipeline. The compatibility of the architecture with frames in the form of real-time also opens the possibility of being integrated with automatic threat monitoring systems that can be implemented within edge or cloud-based platforms.

10.48047/jocaaa.2024.33.08.210

6.4 Limitations and Threats to Validity

Our study has some limitations, even though it performed well. First, the used dataset, though rich and diverse, is synthetic and does not necessarily include all the complexities in real encrypted or classified signal streams in military use. Our training data might underrepresent adversarial noise with dynamic spectral properties, as this is not included in the training set. Moreover, model evaluation indicators can differ at scale to multivariate signals or high-throughput streaming conditions. Though the theory guarantees are true under assumption conditions, they might need to be extended or proved true under real-time and adversary conditions.

6.5 Compliance with Journal Scope

The consumed-tool procedure is presented and demonstrated in the current paper, which corresponds to the apparent mission of encouraging computationally based, serious studies, with formal mathematical foundations in the Journal of Computational Analysis & Applications. Our derivation contains wavelet and stochastic convergence derivations, bounded-error analysis, and signal reconstruction proofs, all of which exist in the thrust of realisable signal analytics. The article offers a foothold between analytical modelling and machine learning application, thereby satisfying the theoretical and computational demands of the journal on received theory and application, respectively

7 Conclusion and Future Work

This paper brings a holistic, mathematically based system of detecting signal anomalies concerning national security activities. The pipeline specifications provide theoretical soundness and feasibility of operation since it utilises the Discrete Wavelet Transform to apply time-frequency decomposition of the signal and stochastic noise modelling to implement robust denoising. The necessary predictive intelligence is achieved through an ML layer consisting of SVM, LSTM, and XGBoost classifiers, which allow significant identification of anomalous patterns in complex, noisy signal environments.

The most crucial findings of our experimental study indicate that the suggested model is much more effective than the baseline strategies. The XGBoost classifier presented the best accuracy (91.2%), followed by the AUC value (0.94), better than both SVM and LSTM under the same conditions. The confusion matrices indicate good classification, with irrelevant variance, where false positives and false negatives are low. Notably, the model remained stable even when ablation tests were employed, proving the importance of wavelet transformation and stochastic

10.48047/jocaaa.2024.33.08.210

filtering that had augmented the performance. The results support that the suggested system is not merely effective when it comes to computing, but it is also dependable regarding demanding development.

The next area of interest will involve extending the range of the data set to incorporate real-time, encrypted and military grade signal data. It will also be helpful to integrate adversarial learning techniques to test the vulnerability of the framework against jamming and spoofing attacks. Also, a discussion of live deployment of such a pipeline using streaming platforms like Apache Kafka and edge-tailored ML models is planned. More fine-grained versions of DWT would also be considered, like the multivariate wavelet packet transform, to extract signal components differently. Lastly, we will incorporate cryptographic machine learning schemes that maintain confidentiality of data, which is essential, especially when the communication is sensitive, i.e. defence applications.

Overall, the work contributes to the study of computational signal analysis since it proposes a scalable, mathematically verified, and machine learning-based anomaly detection system. It paves the way for additional research work, both in the theoretical framework of modelling and in practice, related to developing AI systems that can contribute to defence.

Acknowledgments

The authors thank their respective institutions for providing the infrastructure and academic support to pursue this research. Special thanks to the Kaggle platform and the developers of the “Wavelet Transform for TimeSeries Anomaly Detection” dataset, which served as the foundation for our empirical analysis. We also acknowledge the open-source software libraries, such as PyWavelets, Scikit-learn, XGBoost, and Matplotlib, which were instrumental in implementing and validating the proposed methodology. Their continued maintenance by the developer community significantly enables innovation in computational signal analysis and applied machine learning.

Author Contributions

- **Sujoy Saha**: Conceptualising the research problem, manuscript writing, and final integration.
- **Md Kamrul Islam**: Wavelet mathematical formulation and dataset preprocessing.

10.48047/jocaaa.2024.33.08.210

- **Md Arifur Rahaman**: Implementation of machine learning models and hyperparameter tuning.
- **Rabi Sankar Mondal**: Development and verification of theoretical proofs and convergence analysis.
- **Md Kamruzzaman**: Conducted model experiments, results validation, and peer review of manuscript drafts.

All authors have read and approved the final version of the manuscript.

Conflict of Interest

The authors declare that no conflicts of interest, financial, personal, or institutional, are related to the research presented in this manuscript. The study was conducted independently, and no external funding influenced the research design, data analysis, interpretation of results, or the decision to submit the work for publication.

References

[1] Z. Yu, H. Gao, X. Cong, N. Wu, and H. H. Song, "A survey on cyber–physical systems security," *IEEE Internet of Things Journal,* vol. 10, no. 24, pp. 21670-21686, 2023, doi: https://doi.org/10.1109/JIOT.2023.3289625.

[2] J. Martínez Torres, C. Iglesias Comesaña, and P. J. García-Nieto, "Machine learning techniques applied to cybersecurity," *International Journal of Machine Learning and Cybernetics,* vol. 10, no. 10, pp. 2823-2836, 2019, doi: https://doi.org/10.1007/s13042-018-00906-1.

[3] H. Tan, L. Wang, H. Zhang, J. Zhang, M. Shafiq, and Z. Gu, "Adversarial attack and defense strategies of speaker recognition systems: A survey," *Electronics,* vol. 11, no. 14, p. 2183, 2022, doi: https://doi.org/10.3390/electronics11142183.

[4] M. M. Sayah, K. M. Redouane, and K. Amine, "Stationary, continuous, and discrete wavelet-based approach for secure medical image transmission," *Research on Biomedical Engineering,* vol. 39, no. 1, pp. 167-178, 2023, doi: https://doi.org/10.1007/s42600-023-00261-3.

[5] P. Lang *et al.*, "A comprehensive survey of machine learning applied to radar signal processing," *arXiv preprint arXiv:2009.13702,* 2020, doi: https://doi.org/10.48550/arXiv.2009.13702.

[6] S. D. Roy, S. Debbarma, and A. Iqbal, "A decentralized intrusion detection system for security of generation control," *IEEE Internet of Things Journal,* vol. 9, no. 19, pp. 18924-18933, 2022, doi: https://doi.org/10.1109/JIOT.2022.3163502.

[7] A. L. O. Vitor, A. Goedtel, M. F. Castoldi, W. A. Souza, and G. H. Bazan, "Induction machine fault diagnosis with quadratic time–frequency distributions: State of the art," *IEEE Transactions on Instrumentation and Measurement,* vol. 72, pp. 1-16, 2023, doi: https://doi.org/10.1109/TIM.2023.3323999.

[8] K. Soman, S. Sachin Kumar, N. Mohan, and P. Poornachandran, "Modern methods for signal analysis and its applications," *Recent advances in computational intelligence,* pp. 263-290, 2019, doi: https://doi.org/10.1007/978-3-030-12500-4_17.

10.48047/jocaaa.2024.33.08.210

[9] J. J. Jaber, N. Ismail, S. Ramli, S. Al Wadi, and D. Boughaci, "Assessment of credit losses based on ARIMA-wavelet method," *Journal of Theoretical and Applied Information Technology,* vol. 98, no. 09, pp. 1379-392, 2020.

[10] A. Silik, M. Noori, W. A. Altabey, R. Ghiasi, and Z. Wu, "Comparative analysis of wavelet transform for time-frequency analysis and transient localization in structural health monitoring," *Structural Durability & Health Monitoring,* vol. 15, no. 1, p. 1, 2021, doi: https://doi.org/10.32604/sdhm.2021.012751.

[11] J. Rowland Adams, J. Newman, and A. Stefanovska, "Distinguishing between deterministic oscillations and noise," *The European Physical Journal Special Topics,* vol. 232, no. 20, pp. 3435-3457, 2023, doi: https://doi.org/10.1140/epjs/s11734-023-00986-3.

[12] J. L. Echenausía-Monroy, E. Campos, R. Jaimes-Reátegui, J. H. García-López, and G. Huerta-Cuellar, "Deterministic Brownian-like motion: Electronic approach," *Electronics,* vol. 11, no. 18, p. 2949, 2022, doi: https://doi.org/10.3390/electronics11182949.

[13] R. J. Barry and F. M. De Blasio, "Characterizing pink and white noise in the human electroencephalogram," *Journal of Neural Engineering,* vol. 18, no. 3, p. 034001, 2021, doi: 10.1088/1741-2552/abe399.

[14] O. Esteban *et al.*, "fMRIPrep: a robust preprocessing pipeline for functional MRI," *Nature methods,* vol. 16, no. 1, pp. 111-116, 2019, doi: https://doi.org/10.1038/s41592-018-0235-4.

[15] R. E. Ratnayake and H. Usoof, "A Novel Hybrid Approach for Network Intrusion Detection using Extreme Gradient Boosting and Long Short-Term Memory Networks," *i-Manager's Journal on Computer Science,* vol. 8, no. 4, p. 7, 2020, doi: 10.26634/jcom.8.4.18338.

[16] G. R. Machado, E. Silva, and R. R. Goldschmidt, "Adversarial machine learning in image classification: A survey toward the defender's perspective," *ACM Computing Surveys (CSUR),* vol. 55, no. 1, pp. 1-38, 2021, doi: https://doi.org/10.1145/3485133.

[17] T. Guo, T. Zhang, E. Lim, M. Lopez-Benitez, F. Ma, and L. Yu, "A review of wavelet analysis and its applications: Challenges and opportunities," *IEEe Access,* vol. 10, pp. 58869-58903, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3179517.

[18] P. Santaniello and P. Russo, "Bridge damage identification using deep neural networks on time–frequency signals representation," *Sensors,* vol. 23, no. 13, p. 6152, 2023, doi: https://doi.org/10.3390/s23136152.

[19] D. Goyal, C. Mongia, and S. Sehgal, "Applications of digital signal processing in monitoring machining processes and rotary components: A review," *IEEE Sensors Journal,* vol. 21, no. 7, pp. 8780-8804, 2021, doi: https://doi.org/10.1109/JSEN.2021.3050718.

[20] M. K. Islam, A. Rastegarnia, and S. Sanei, "Signal artifacts and techniques for artifacts and noise removal," in *Signal Processing Techniques for Computational Health Informatics*: Springer, 2020, pp. 23-79.