VISION
رؤية
رؤية للطباعة والدعاية والإعلان
شارع عبد المنعم رياض - 0925031603

Journal of Electronic Systems and Programming

Issue N0: 11 June 2025

e.P.C
المركز الليبي للمنظومات الإلكترونية
والبرمجيات وبحوث الطيران
Liban Center Fror Electronic Systems
programming and Avlation Research

Refereed Journal
www.epc.ly

Journal of Electronic Systems and Programming

Issue N0: 11 June 2025

Journal of Electronic Systems and Programming

Libyan Center for Electronic Systems, Programming and Aviation Research

Journal of Electronic Systems and Programming

Issue No: 11 - 2025

Editorial:
11th Issue – Journal of Electronic Systems and Programming

We are delighted to announce the publication of the 11th issue of the Journal of Electronic Systems and Programming (JESP).

As the official publication of Libyan Center for Electronic Systems, Programming and Aviation Research (EPC), the JESP aims to provide a platform for both researchers from inside and outside the center to share their novel results and latest developments, and also to seek better understanding of the current situation on research related to the area of contributions of EPC.

Finally, we thank our reviewers and authors for their fundamental contribution to the 11th release of the Journal. We still hope authors could consider JESP to be a place where to publish their work.

Editorial Board

Table of Contents:

1

Deep Learning Approaches for ssifying Marine Mammal Vocalizations in Support of Oceanic Conservation

Deep Learning Approaches for Classifying Marine Mammal Vocalizations in Support of Oceanic Conservation

Abdusamea I.A Omer
Sabratha University
abdusamea@gmail.com

Alhasan Ali Almahroug
University of Azzawia, Azzawia, Libya
h.almahroug@zu.edu.ly

Basem Mustafa Amer
University of Azzawia, Azzawia, Libya
b.amer@zu.edu.ly

Zuher H.M Fheleboom
College of Computer Technologies Azzawia, Libya
zuher.h.f@gmail.com

Abstract

This research investigates the utilization of advanced machine learning techniques to analyze and classify the vocalizations of marine mammals, contributing to conservation science. Emphasizing the role of passive acoustic monitoring, the study enables non invasive observation of cetacean behavior in their natural settings. It explores the nature of underwater acoustic environments, detailing how marine species emit and interpret sound signals for communication and survival. Leveraging a comprehensive dataset the Watkins Marine Mammal Sound Database the study applies digital signal processing and deep learning, particularly convolutional neural networks (CNNs), to distinguish among species specific calls. Results show strong model performance, with high classification accuracy across numerous species, highlighting critical acoustic behavioral correlations. These findings reinforce the importance of bioacoustics in conservation planning and suggest that integrating machine learning can significantly enhance monitoring efforts for marine ecosystems.

Keywords: Machine Learning - Marine Mammals - Passive Acoustic Monitoring - Deep Learning (CNN) - Conservation Science.

1. Introduction

Monitoring marine mammal behavior in their natural environment presents a significant challenge due to their often remote and underwater habitats. Traditional observational techniques are limited by visibility and can disrupt the animals’ natural behavior. Passive acoustic monitoring (PAM), on the other hand, offers a non intrusive method to track and study marine species by recording and analyzing the sounds they produce [1] . This technique is particularly effective for cetaceans, which rely heavily on sound for communication, navigation, and foraging. By capturing and interpreting their vocalizations, researchers can gain critical ecological insights without the need for direct interaction. These acoustic datasets can inform decisions related to marine traffic regulation, industrial activity mitigation, and habitat protection strategies [2].

1.1 Background and Importance

DDoS The field of bioacoustics has long explored animal communication through sound, but its application to environmental conservation is a more recent innovation. Marine mammals produce a variety of vocalizations that reflect behaviors such as feeding, mating, social bonding, and predator avoidance. Analyzing these sounds allows scientists to infer ecological patterns and population dynamics. Given the increasing pressures on marine ecosystems, including climate change and human interference, PAM offers an efficient and scalable solution for monitoring biodiversity. It is cost effective compared to visual surveys, and capable of collecting data over long durations and wide geographic areas. Species such as whales, dolphins, and seals are especially well suited for acoustic studies due to their reliance on vocal cues for essential life functions [3].

1.2 Acoustic Properties in Marine Environments

Sound waves propagate more rapidly and efficiently in water than in air typically traveling at speeds between 1450 and 1500 meters per second, compared to around 340 meters per second in air. This difference is critical for marine species, which use sound to compensate for the limited visibility of their aquatic environment [5] The physical properties of the ocean, including temperature, pressure, and salinity, significantly influence sound transmission, altering how vocal signals are perceived across distances.

1.3 Sound Generation and Detection in Marine Mammals

Different marine species produce and perceive sound in unique ways. Baleen whales emit low frequency calls that can traverse vast distances, while toothed whales, such as dolphins [6] , generate high frequency clicks for echolocation and whistles for social interaction. Seals and sea lions also produce a range of vocalizations both in water and on land. These sounds are captured and processed by specialized auditory structures adapted for underwater hearing, enabling marine mammals to detect prey, communicate with conspecifics, and navigate their environment effectively.

1.4 Environmental Influences on Underwater Sound

The clarity and range of underwater sound are influenced by numerous oceanic factors. Variations in temperature, pressure, and salinity can alter acoustic wave propagation, while human induced noise such as that generated by shipping, construction, or exploration can mask biological signals. This auditory interference can disrupt communication, navigation, and feeding, posing a significant threat to marine species that depend on sound [8].

1.5 Marine Mammal Vocal Behavior

Marine mammals exhibit a rich and complex acoustic repertoire. Their vocalizations are often species specific and context dependent, ranging from long distance mating songs to short range social calls [5] . Baleen whales, for instance, use deep moans and rhythmic pulses, while dolphins employ distinctive signature whistles. Seals generate a wide frequency range of barks, trills, and growls [7] . Understanding these vocal behaviors is essential not only for identifying species but also for interpreting social structures and ecological roles within marine communities.

2. Background and Review of Existing Approaches

Two Recent advancements in bioacoustics and artificial intelligence have spurred a growing body of research focused on the acoustic monitoring of marine mammals. These efforts aim to understand the complex interactions between marine species and their acoustic environment, particularly in the face of increasing anthropogenic noise. A review of notable studies provides a comprehensive foundation for the present research and highlights current methodological trends, technological innovations, and remaining challenges in the field.

Guan and Brookens (2023) conducted a global review of underwater noise impacts on cetaceans. Their work synthesized findings on behavioral and physiological responses to noise pollution, including avoidance behavior, stress indicators, and changes in communication patterns. They emphasized the necessity of developing regulatory frameworks based on scientifically validated noise thresholds for various marine species [8].

In a complementary study, Ferguson et al. (2023) examined the relationship between acoustic indices and underwater sound sources. By analyzing passive acoustic data from the California Current Ecosystem, they demonstrated how indices such as the Acoustic Complexity Index (ACI) respond to both biological and anthropogenic signals. Their results illustrated the potential for using acoustic indices as proxies for biodiversity and environmental health [9].

Reckendorf et al. (2023) explored how marine mammals rely on sound for essential life processes, including echolocation and navigation. They also addressed the threats posed by increasing underwater noise, documenting behavioral shifts and physiological stress caused by persistent human generated sound [10].

Turbulent Research (2023) focused on real time acoustic monitoring networks capable of detecting and tracking marine mammal populations. Their study highlighted innovations such as distributed hydrophone arrays and machine learning–based classification algorithms. These systems have shown significant promise in documenting migratory patterns and identifying ecological stressors like overfishing and climate change [7].

Southall et al. (2022) updated marine mammal noise exposure standards, incorporating ecological and biological metrics into exposure criteria. Their findings are being used to inform policy development and habitat management plans, especially in regions impacted by industrial activity [6].

The work of Rice et al. (2022) employed spatial acoustic models to investigate the overlap between natural and human made soundscapes. Their study offered actionable strategies, such as rerouting shipping lanes and introducing seasonal noise restrictions, to mitigate acoustic disturbances in sensitive marine areas [2].

Pirotta et al. (2022) proposed leveraging deep learning methods to detect behavioral changes in marine mammals in response to environmental stressors. They showcased case studies on fin whales and gray seals, demonstrating how automated systems can significantly improve the granularity of behavioral analysis and contribute to informed conservation strategies [4].

Širović et al. (2022) highlighted the scalability of acoustic monitoring systems for large scale biodiversity assessments. Their work underscored the effectiveness of cloud based processing tools and automated detection algorithms in streamlining data analysis across wide geographical areas [3].

An earlier contribution by Slabbekoorn et al. (2018) investigated the psychoacoustic effects of human noise on marine fauna. Their research revealed that some species are more vulnerable to acoustic disturbances than others and called for multi species, long term studies to understand cumulative impacts [1].

Together, these studies form a comprehensive backdrop for the integration of machine learning and bioacoustic monitoring. They affirm the need for robust algorithms, high quality datasets, and interdisciplinary collaboration to enhance our understanding of marine mammal ecology and to support effective conservation measures.

3. Methodological Approach

This section outlines the approach used to collect, process, and analyze marine mammal vocalizations. It includes dataset selection, preprocessing techniques, machine learning model design, and the tools used for implementation. The goal was to develop a system capable of accurately classifying acoustic signals across multiple species for conservation related applications.

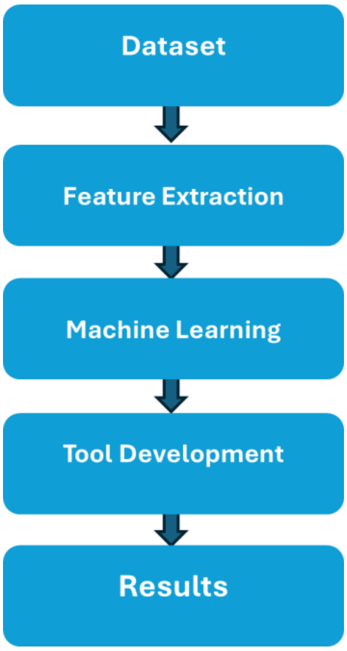


Figure 1: System Steps

3.1 Dataset Acquisition

The study utilized open access bioacoustic datasets sourced from reputable repositories, including the Marine Bioacoustics Archives and the Ocean Biodiversity Information System (OBIS). These datasets provide labeled audio samples of various marine mammal species such as humpback whales, bottlenose dolphins, and bearded seals. The recordings span diverse marine environments and contain species annotated vocalizations in standardized formats.

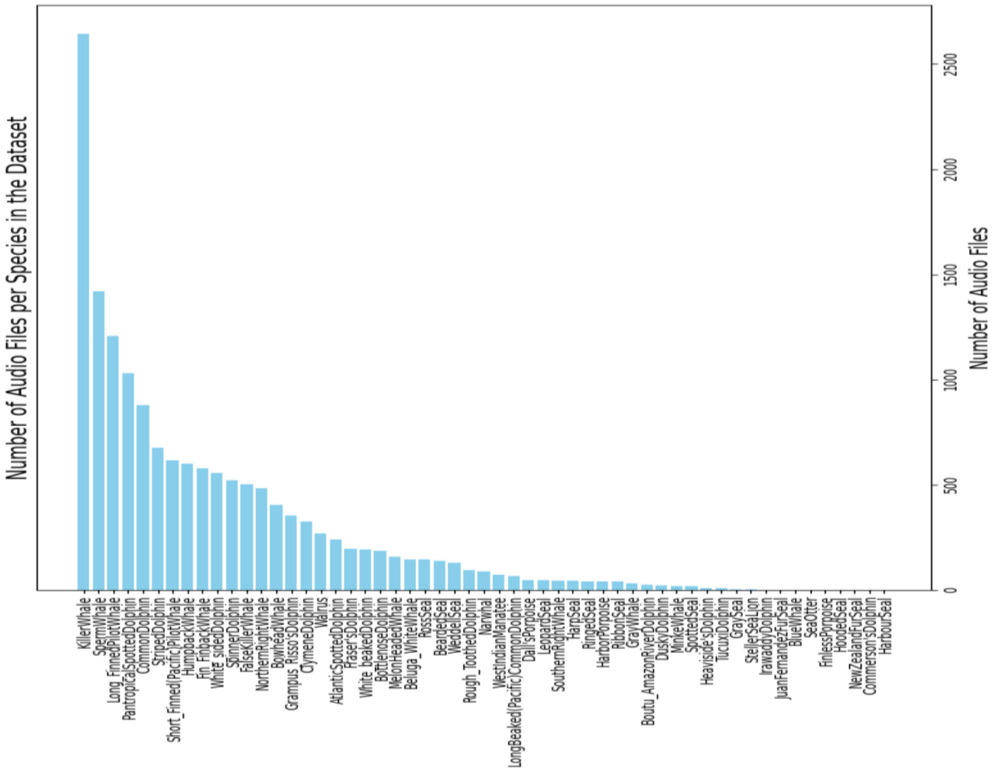


Figure 2: Number of samples

3.2 Audio Preprocessing and Feature Extraction

To prepare the raw audio data for analysis, several signal processing steps were applied:

- **Noise Filtering:** High pass filters were used to eliminate low frequency background noise, improving the clarity of animal calls.
- **Spectrogram Generation:** The audio signals were transformed into spectrograms visual representations of sound frequencies over time enabling visual feature extraction.
- **Mel Frequency Cepstral Coefficients (MFCCs):** These features were extracted to capture timbral and frequency characteristics, which are critical for differentiating species specific vocalizations.

This preprocessing pipeline ensured that the acoustic input to the model retained relevant information while minimizing irrelevant noise artifacts.

3.3 Machine Learning Architecture

The classification model was developed using a supervised learning approach. Two types of models were explored:

- **Random Forest Classifier:** A decision tree–based ensemble learning method was used as a baseline for multi class classification.
- **1D Convolutional Neural Network (1D CNN):** A deep learning model designed for time series audio data was used for improved feature learning.

The deep learning architecture was chosen due to its ability to capture both temporal and spectral nuances in marine mammal calls.

3.4 Training Strategy

The dataset was split into three parts:

- **Training Set (80%)**: Used for model learning.
- **Validation Set (10%)**: Used to tune hyperparameters and monitor overfitting.
- **Testing Set (10%)**: Used for final performance evaluation.

To address class imbalance and improve generalization, data augmentation techniques were applied to the training set. These included pitch shifting, time stretching, and adding synthetic background noise.

3.5 System Tools and Frameworks

The project was developed using the following tools and libraries:

- **Python:** Main programming language.
- **Librosa:** For audio analysis and feature extraction.
- **NumPy & Pandas:** For numerical and tabular data handling.
- **Matplotlib:** For visualizing spectrograms and performance metrics.
- **Jupyter Notebook:** For interactive coding and visualization.
- **Kaggle Environment:** For training the deep learning models using GPU acceleration (NVIDIA Tesla P100).

3.6 Workflow Summary

The full pipeline follows these steps:

1. **Input:** Labeled audio files of marine mammal calls.
2. **Preprocessing:** Denoising and normalization.
3. **Feature Extraction:** Using MFCCs and spectrograms.
4. **Model Training:** Utilizing either Random Forest or 1D CNN.
5. **Prediction:** Classifying calls and evaluating model accuracy.
6. **Visualization:** Displaying classification results and performance metrics.

This comprehensive methodology ensures the reliability and scalability of the system for marine species classification tasks.

4. Results and Discussion

This section presents the experimental results derived from applying machine learning techniques to the classification of marine mammal vocalizations. It includes an overview of the dataset, performance metrics of the trained model, and an analysis of species specific outcomes. The findings offer insights into both the effectiveness of the approach and the challenges associated with audio based species classification.

4.1 Dataset Overview

The audio recordings used for training and evaluation were obtained from the Watkins Marine Mammal Sound Database, a curated collection comprising over 3,000 labeled samples across 51 species. Each sound file was standardized to a fixed duration of approximately five seconds and categorized by species name. The dataset features a wide range of marine mammals, including common species like bottlenose dolphins and less represented ones like the Irrawaddy dolphin.

To ensure balanced training and fair evaluation, the dataset was partitioned as follows:

Table 1: Table 1: Dataset Split by Usage

Subset	**Number of Samples**	**Percentage**
Training Set	2,492	80%
Validation Set	311	10%
Testing Set	311	10%
Total	**3,114**	**100%**

The dataset exhibited significant class imbalance, with some species having up to 300 samples, while others had fewer than 5. Data augmentation techniques, including noise addition and pitch variation, were applied to underrepresented classes to mitigate bias and enhance model generalization.

4.2 Model Architecture and Training

A one-dimensional convolutional neural network (1D CNN) was deployed for its ability to extract temporal features from audio waveforms. The model comprised:

- **Input Layer:** Accepts preprocessed MFCC feature vectors.
- **Convolutional Layers:** Detect frequency temporal patterns.
- **Pooling Layers:** Reduce feature dimensionality while retaining key signals.
- **Fully Connected Layers:** Integrate abstracted features for final classification.
- **Output Layer:** Softmax classifier with 51 output nodes (one per species).

Training was conducted on Kaggle's GPU infrastructure using the Adam optimizer with a learning rate of 0.001 and batch size of 32. Early stopping was implemented to prevent overfitting.

4.3 Classification Results

The model achieved high overall performance:

- **Training Accuracy:** 96.5%
- **Validation Accuracy:** 92.8%
- **Test Accuracy:** 91.3%
- **Macro Average AUC:** 0.94

These results reflect strong model generalization and demonstrate the efficacy of deep learning in handling bioacoustic classification tasks.

4.4 Species Level Performance

Performance metrics varied across species, influenced by data availability and acoustic distinctiveness. Table 1 shows key metrics for selected species:

Table 2: Performance Metrics by Marine Species

Species	Precision	Recall	F1 Score
Atlantic Spotted Dolphin	97.5%	96.8%	97.1%
Harbor Porpoise	95.4%	94.9%	95.1%
White Sided Dolphin	81.3%	79.5%	80.4%
Leopard Seal	78.6%	77.2%	77.9%

Species like the Atlantic Spotted Dolphin and Harbor Porpoise yielded the highest classification scores due to large, clear datasets. In contrast, species with fewer or less distinctive calls, such as the Leopard Seal, showed moderate performance.

4.5 Confusion Matrix Insights

The confusion matrix revealed that most classifications were accurate, especially for species with distinctive calls. However, misclassifications occurred between acoustically similar species. For instance:

- Harbor Porpoise calls were occasionally confused with those of Beaked Whales.

- Gray Whale calls overlapped with Fin Whale calls due to similar low frequency patterns.

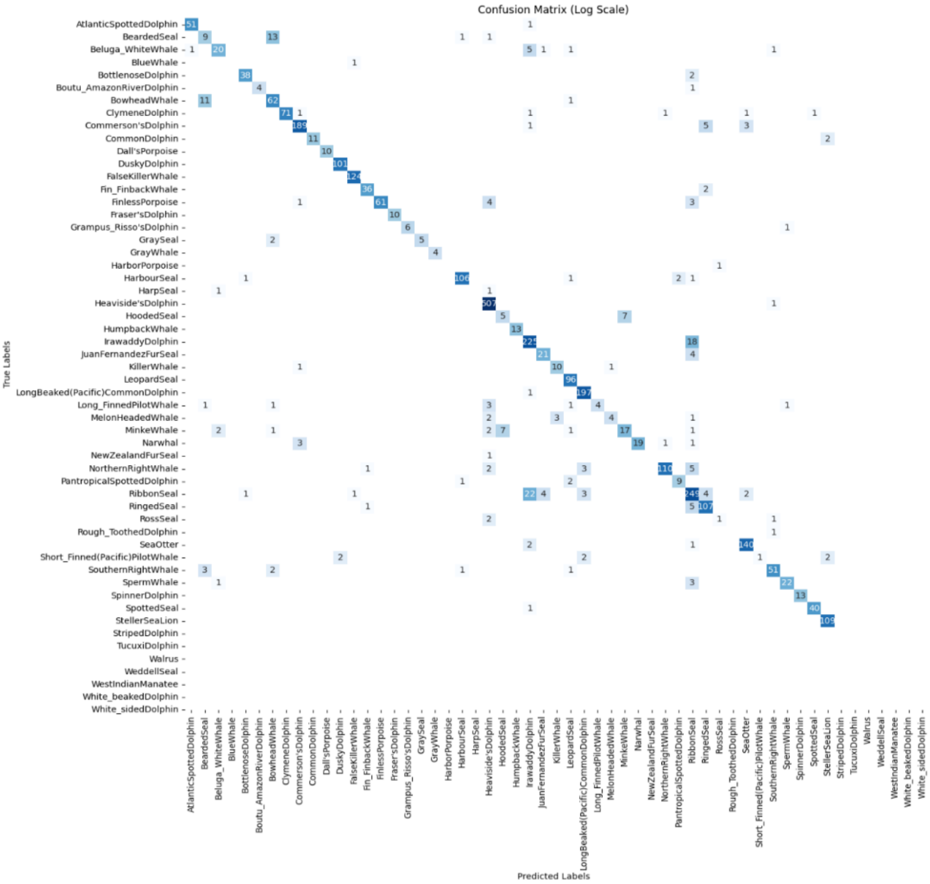


Figure 3: Confusion Matrix

These results highlight the need for additional feature refinement or hybrid classification models to improve discrimination among closely related species.

4.6 Factors Affecting Accuracy

Several elements influenced model performance:

1. **Data Imbalance:** Classes with fewer samples led to reduced classification accuracy.
2. **Acoustic Overlap:** Similar vocal patterns among species resulted in higher error rates.
3. **Environmental Noise:** Some recordings included background interference, affecting feature clarity.

Despite these challenges, the model maintained high precision across the majority of species, demonstrating robustness in real world acoustic conditions.

5. Conclusion

This study demonstrates the successful application of machine learning specifically convolutional neural networks in the classification of marine mammal vocalizations. The results affirm that passive acoustic monitoring, when combined with robust signal processing and advanced classification algorithms, provides an effective, non invasive method for observing marine life in its natural habitat.

The developed model exhibited high performance in distinguishing between species across a diverse set of vocalizations, with overall classification accuracy exceeding 91%. These findings underline the feasibility of using automated systems to monitor biodiversity, track species distributions, and inform conservation efforts.

The study also emphasized the importance of preprocessing techniques such as denoising and spectrogram transformation, which enhanced the clarity and utility of acoustic features. However, limitations including class imbalance, overlapping acoustic patterns, and background noise highlight the need for continued methodological refinement.

By enabling scalable and cost-effective monitoring of marine ecosystems, the approach outlined in this research contributes to global efforts aimed at protecting vulnerable species from the impacts of environmental degradation, habitat loss, and anthropogenic noise pollution. Overall, it paves the way for smarter, data driven conservation strategies in the realm of marine bioacoustics.

6. Recommendations and future work

Based on the findings of this study, the following recommendations are proposed to enhance future research and practical applications:

1. **Expand Data Collection for Rare Species:**
   Gathering more audio samples for underrepresented marine mammals such as the Irrawaddy Dolphin or Rough Toothed Dolphin will reduce data imbalance and improve model accuracy for these species.

2. **Integrate Hybrid Classification Models:**
   Combining different classifiers (e.g., ensemble methods with neural networks) could increase robustness, especially in scenarios involving similar acoustic signatures.

3. **Refine Feature Extraction Techniques:**
   Exploring additional feature descriptors, such as chroma energy or spectral contrast, may offer greater discriminatory power in distinguishing closely related species.

4. **Enhance Preprocessing Strategies:**
   Applying advanced noise suppression and adaptive filtering

techniques will help mitigate interference caused by shipping and industrial activities.

5. **Deploy Real   Time Monitoring Systems:**
   Developing field   ready systems that leverage cloud computing and real   time analysis will allow continuous tracking of species presence and behavior in dynamic marine environments.

6. **Collaborate Across Disciplines:**
   Integrating ecological data, behavioral studies, and environmental modeling with acoustic analysis will provide a more holistic understanding of marine ecosystems.

7. **Support Policy and Regulation:**
   Findings from acoustic classification should be shared with policymakers to inform decisions on shipping regulations, marine protected areas, and noise mitigation strategies.

References

[1] H. Slabbekoorn, R. J. Dooling, A. N. Popper, and R. R. Fay, *Effects of Anthropogenic Noise on Animals*, Springer, 2018.

[2] A. Širović, K. Evans, C. García Soto, J. A. Hildebrand, S. M. Jesus, and J. H. Miller, "World Ocean Assessment II, Chapter 20, Trends in the inputs of anthropogenic noise into the marine environment," United Nations Division for Ocean Affairs and the Law of the Sea, 2021.

[3] A. C. Rice, J. S. Trickey, A. Giddings, M. A. Rafter, et al., "Passive Acoustic Monitoring for Marine Mammals in the SOCAL Range Complex April 2020–2021 and Abundance and Density Estimates from CalCOFI Visual Surveys 2004–2021," Marine Physical Laboratory, Scripps Institution of Oceanography, 2022.

[4] E. Pirotta, C. G. Booth, J. Calambokidis, D. P. Costa, et al., "From individual responses to population effects: Integrating a decade of multidisciplinary research on blue whales and sonar," *Animal Conservation*, 2022. [Online]. Available: https://doi.org/10.1111/acv.12785

[5] P. F. Moretti and A. Affatati, "Understanding the impact of underwater noise to preserve marine ecosystems and manage anthropogenic activities," *Sustainability*, vol. 15, no. 13, 2023, Art. no. 10178.

[6] B. L. Southall, et al., "Marine mammal noise exposure criteria: A comprehensive review and update," *Aquatic Mammals*, 2022.

[7] Turbulent Research, "Using passive acoustic monitoring to track human activities underwater," 2023. [Online]. Available: https://turbulentresearch.com/articles/using passive acoustic monitoring track human activities underwater.

[8] Y. Guan and J. Brookens, “An overview of research efforts to understand the effects of underwater sound on cetaceans,” *Journal of Marine Science and Engineering*, 2023.

[9] M. Ferguson, et al., “Acoustic indices respond to specific marine mammal vocalizations and sources of anthropogenic noise,” *Ecological Indicators*, 2023.

[10] A. Reckendorf, L. Seidelin, and M. Wahlberg, “Marine mammal acoustics,” in *Marine Mammals*, D. Brennecke et al., Eds., Springer, 2023. [Online]. Available: https://doi.org/10.1007/978_3_031_06836_2_2

2

Assessment of Railway Wheel Surface Parameters using CCI Machine

Assessment of Railway Wheel Surface Parameters using CCI Machine

A. Shebani
College of computer technology
Zawya, Libya
amershebani@gmail.com

Abstract

The railway system is one of the most complicated dynamical systems in engineering, and the material removal mechanism of railway wheel is a considerable complicated process. CCI machine (TalySurf machine) introduced in this paper to measure the wheel surface roughness parameters such as volume of void, these parameters can help the designers to study and predict the effect of these parameters on the wheel surface phenomenon's such as wheel wear, and it can help to improve the railway wheel and rail profile. Experimental investigations based on CCI machine have been carried out in this work. In experiments, a twin disc rig was used to conduct the tests under applied different loads. The CCI machine is a type of surface profilometer can be used to measure the surface roughness, waviness, and form; it's widely used in quality control, precession engineering, and research. The CCI machine used in this paper to measure the roughness parameters of railway wheel surface.

Keywords: Railway, CCI machine, TalySurf, wheel surface, roughness parameters.

1. Introduction

1.1 railway vehicle

The railway system is one of the most complicated dynamical systems in mechanical engineering. A railway vehicle is any vehicle that operates on a railway (or railroad) track. These vehicles are typically used for the transportation of passengers, goods, or specialized services. Railway vehicles come in various types and serve different purposes such as: Locomotive, Passenger Cars (Coaches), Freight Cars (Wagons), Light Rail / Tram Vehicles, and High-Speed Rail Vehicles. The components of a Railway Vehicle are: Bogies: The wheel assemblies under the car, Couplers: Devices to connect cars together, Braking System: Air brakes, dynamic brakes, and Pantograph / Third Rail Shoe: For electric trains, draws power. The railway wheelset which consists of two wheels of railway vehicle is shown in Figure 1 [1], [2].

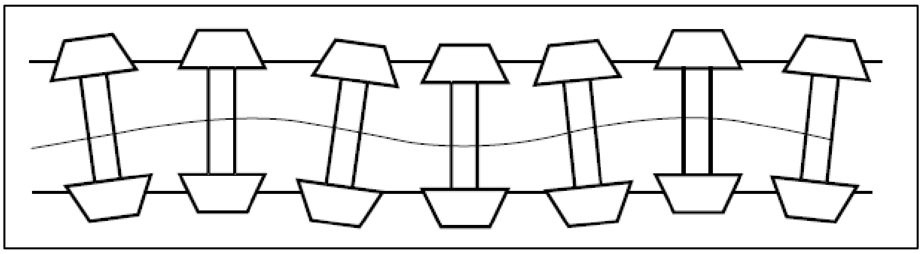


Figure 1: The wheelset or railway vehicle

1.2 Wheel – Rail Contact

Wheel-rail contact is the interaction between a railway vehicle's wheel and the rail it runs on. This contact point is fundamental to the performance, safety, and longevity of railway systems. Contact Patch: The area where the wheel and rail touch. Although it may look like a point, it’s actually a small ellipse (often a few mm²) due to elastic deformation. The contact between wheel surface and rail surface is shown in Figure 2 [1], [2].

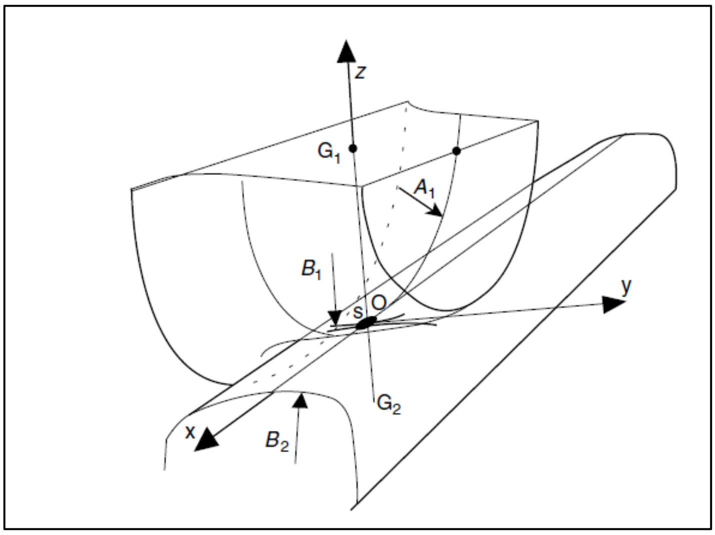


Figure 2: wheel/rail contact point

1.3 Railway wear (wheel/rail wear)

Wheel and rail wear refers to the gradual degradation of the surfaces of train wheels and the rails they run on due to contact, friction, and environmental conditions. It’s a key issue in railway maintenance and affects safety, ride quality, and operational costs. The common types of wear are: Rolling Contact Fatigue (RCF), Adhesive wear, Abrasive wear, Corrugation, and Flange Wear (Wheel) / Gauge Face Wear (Rail) [1].

Corrosion: Corrosion may be defined as the undesired deterioration of a material through chemical or electrochemical interaction with the environment, or destruction of materials by means other than purely mechanical action. Failure by corrosion occurs when the corrosive action renders the corroded device incapable of performing its design function. Corrosion often interacts synergistically with another failure mode, such as wear or fatigue, to produce the even more serious combined failure modes, such as corrosion-wear or corrosion-fatigue.

Fretting wear: Fretting wear is a specific type of wear that occurs when two contacting surfaces experience small-amplitude oscillatory motion (micromotion) under load. It typically happens at the interface of parts that are nominally stationary relative to each other but are subjected to vibration, cyclic loading, or repeated small displacements.

Fretting fatigue: Fretting fatigue is fatigue damage directly attributable to fretting action.

Fretting wear: Fretting wear is a change in dimensions because of wear directly attributable to the fretting process. Some investigators have suggested that estimates of fretting wear depth may be based on the classical adhesive or abrasive wear equations, in which wear depth is proportional to load and total distance slid, where the total distance slid is calculated by multiplying relative motion per cycle times number of cycles.

Adhesive wear: Adhesive wear is a type of wear that occurs when two solid surfaces slide over each other and material is transferred from one surface to the other due to microscopic welding at the contact points. It is one of the most common and fundamental wear mechanisms, especially in metal-to-metal contact situations. The adhesive wear is shown in Figure 3.

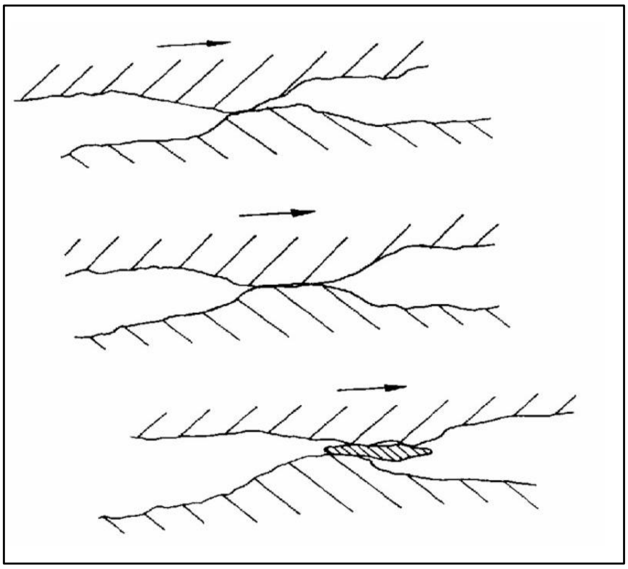


Figure 3: Adhesive wear

Abrasive wear: Abrasive wear is a type of mechanical wear that occurs when hard particles or hard protuberances forcibly remove material from a surface through cutting, plowing, or micro-chipping. It’s one of the most common and destructive forms of wear, especially in environments involving dirt, sand, or unfiltered particulates. The abrasive wear is shown in Figure 4.

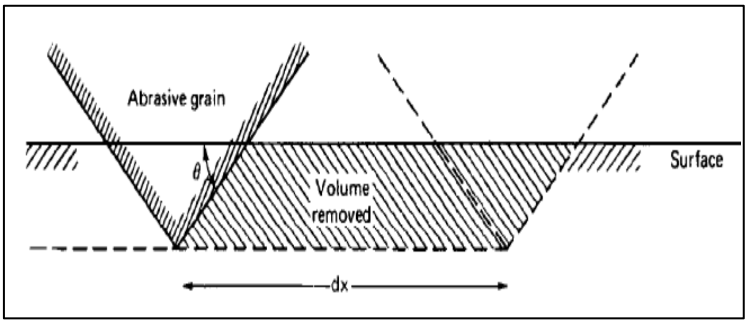


Figure 4: Abrasive wear

Fatigue wear: Fatigue wear is a type of wear that occurs when a material is subjected to repeated or cyclic loading, causing it to crack and eventually break apart due to mechanical fatigue. Unlike abrasive or adhesive wear, fatigue wear doesn’t require sliding, it can occur even under repetitive rolling or oscillating contact [3].

Oxidative wear: Oxidative wear is a type of wear that occurs when a surface undergoes oxidation (a chemical reaction with oxygen, usually from the air), and the resulting oxide layer is either removed by contact or becomes brittle and breaks away during sliding. It is a thermochemical wear mechanism that combines both chemical reactions and mechanical action [3], [4].

Impact Wear: Impact wear is a type of mechanical wear that occurs when two solid bodies repeatedly strike or collide with each other. The repeated impacts lead to surface deformation, cracking, material fatigue, and eventual material loss. It is common in machinery that experiences repeated or sudden forceful contact between parts [5].

Corrosive Wear: Corrosive wear (also called corrosion wear) is a combined chemical and mechanical form of wear. It occurs when a material’s surface undergoes chemical or electrochemical reactions (typically corrosion), and the resulting corrosion products are then mechanically removed, exposing fresh metal to repeat the process [5], [6].

Chemical wear: Seldom is one type of wear found in isolation and this is particularly true of chemical wear. Carburation and oxidation of wear debris, as stages in other wear processes, have already been mentioned and chemical action plays a preliminary part in a number of process (e.g. acidic lubricating oil deterioration products, by preferentially attacking certain constituents of the bearing material, may grossly accelerate wear and precipitate bearing failure) [6].

Mild and severe wear: the mild and sever wear is shown in Figure 5.

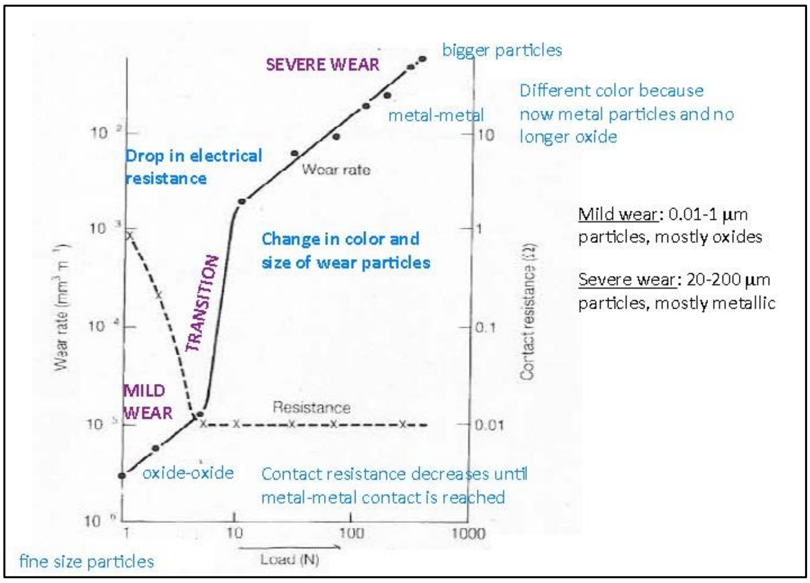


Figure 5: Mild and severe wear [7], [8]

Tribology is the science and technology of interacting surfaces in relative motion. Tribology includes boundary-layer interactions both between solids and between solids and liquids and/or gases. Tribology encompasses the entire field of friction and wear, including lubrication is shown in Figure 6 [8].

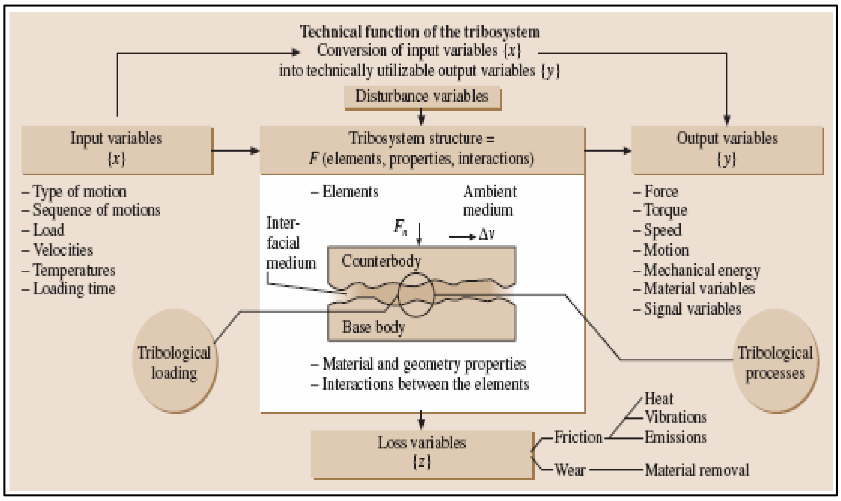


Figure 6: Expanded representation of a tribotechnical system (TTS) [9]-[12]

The adhesive wear is described by the following equation [1]-[4]:

$$d_{adh} = \left(\frac{k}{9\,S_{yp}} \right) \left(\frac{w}{A_a} \right) L_s \tag{1}$$

k is the wear constant (Archard constant).

The abrasive wear is described by the following equation [1]-[4]:

$$d_{abr} = k_{abr}\, p_m\, L_s \tag{2}$$

Where:

p_m is the mean nominal contact pressure between bearing surfaces.

k_{abh} is the abrasive wear coefficient.

1 Roughness

The roughness can refer to different things depending on the context. In material Engineering, the surface roughness parameters often described in micrometre (μm). The common parameters are:

Ra: average roughness, Rz: mean peak to valley height, and Rq: root mean square roughness.

Figure 7 shows a sample of surface roughness.

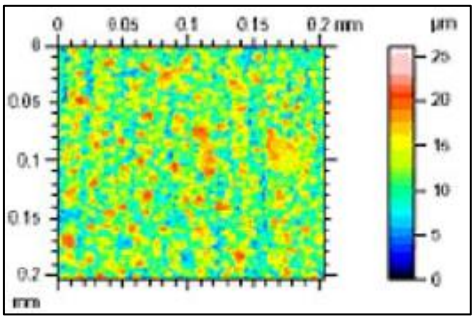


Figure 7 sample of surface roughness

The roughness surface definitions are: [13], [14]

A real surface: it is the actual boundary of an object. It deviates from the nominal surface as a result of the process that created the surface. Nominal surface: it is the intended surface. The shape and extent of a nominal surface are usually shown and dimensioned on a drawing. Surface: it is a surface of an object. Profile: it can be defined as the contour of any specified section through a surface. Measured profile: it can be defined as the profile obtained with some measuring profilometer.

4 CCI machine (TalySurf CCI)

The CCI machine (TalySurf) is shown in Figure 8. Talysurf CCI is an advanced type of measurement interferometer. It uses a patented correlation algorithm to find the coherence peak and phase position of an interference pattern produced by a selectable bandwidth light source. This method provides both high resolution and excellent sensitivity to returning light.

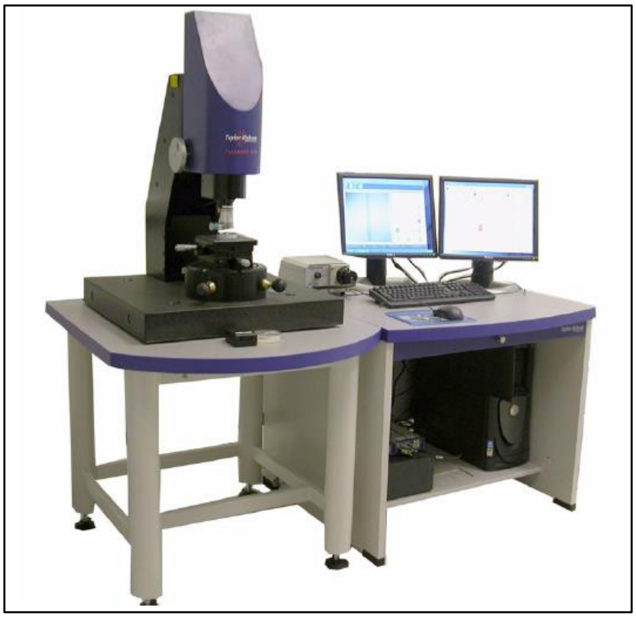


Figure 8 The CCI machine [15]

The Talysurf machine is a high-precision surface measuring instrument used to evaluate the surface texture and topography of components. It’s especially useful in engineering and manufacturing for measuring surface roughness, waviness, form, and contour of machined or finished surfaces. Talysurf (short for Taylor-Hobson Surface Profiler) is a contact-type stylus instrument originally developed by Taylor Hobson. It uses a fine stylus to trace the surface of a component and records vertical displacements (surface variations) as the stylus moves horizontally across the surface.

The Talysurf (CCI 6000) System specificatin such as shown in Table 1.

Table 1: specification of TalySurf machine

Vertical resolution	0.1A (10pm)
RMS repeatability	0.03A (3pm)
measurement range	0.36mm - 7.0mm
lateral sampling resolution	0.35 µm
Step height repeatability	0.1nm
Linearity	+/- 0.05% of measured value
maximum resolution	1024 x; 1024 pixels

The overall accuracy of measurement results influenced by environmental conditions, particularly; draughts, vibration, and the ambient temperature changes [15].

5: Tests and results

The CCI machine (Talysurf CCI) shown in Figure 9 was used in this paper to measure the wheel surface parameters. The replica material put under the lens of the CCI machine for wheel surface measurements such as shown in Figure 9.

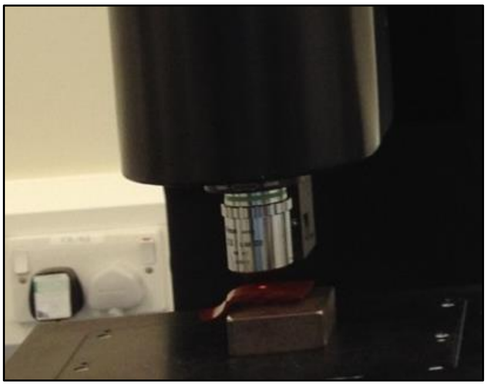


Figure 9: Replica materials of railway wheel with CCI machine

The original surface of wheel is shown in Figure 10.

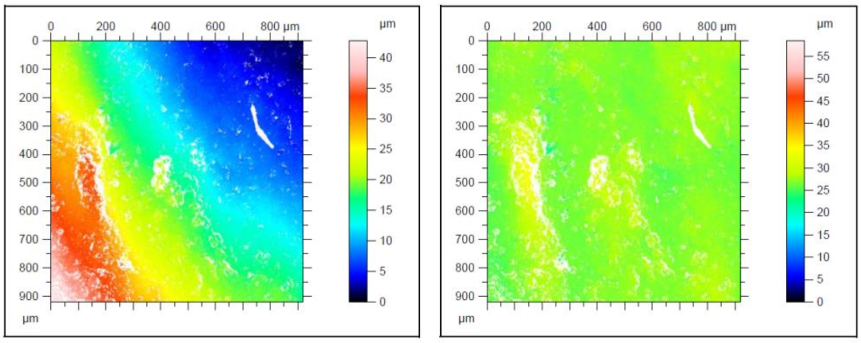


Figure 10: The original surface of wheel

The wheel surface after applied load of 1000N is shown in Figure 11.

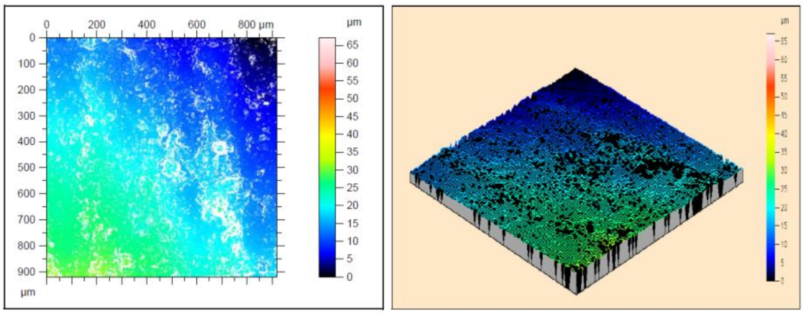


Figure 11: The wheel surface after applied load of 1000N

The volume of void (Vvv) was 0.003419 $\frac{\mu m^3}{\mu m^2}$

The wheel surface after applied load of 1400N is shown in Figure 12.

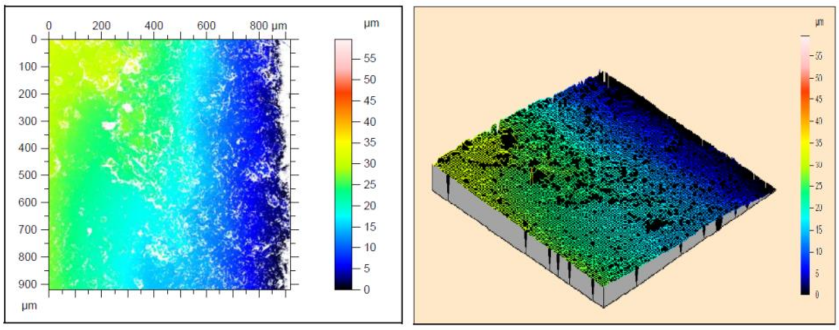


Figure 12: The wheel surface after applied load of 1400N

The volume of void (Vvv) was 0.009715 $\frac{\mu m^3}{\mu m^2}$

The wheel surface after applied load of 3000N is shown in Figure 13.

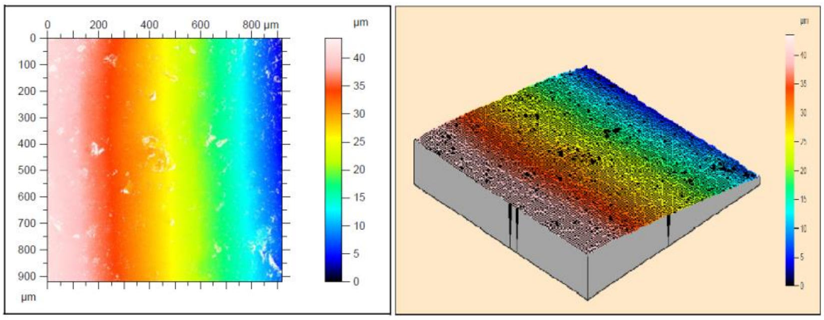
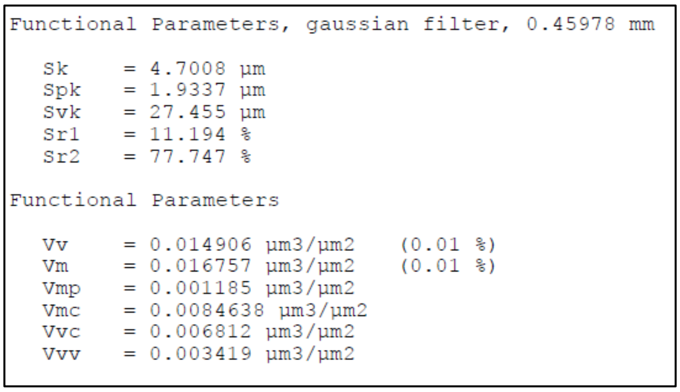


Figure 13 The wheel surface after applied load of 3000N

The volume of void (Vvv) was 0.06105 $\frac{\mu m^3}{\mu m^2}$

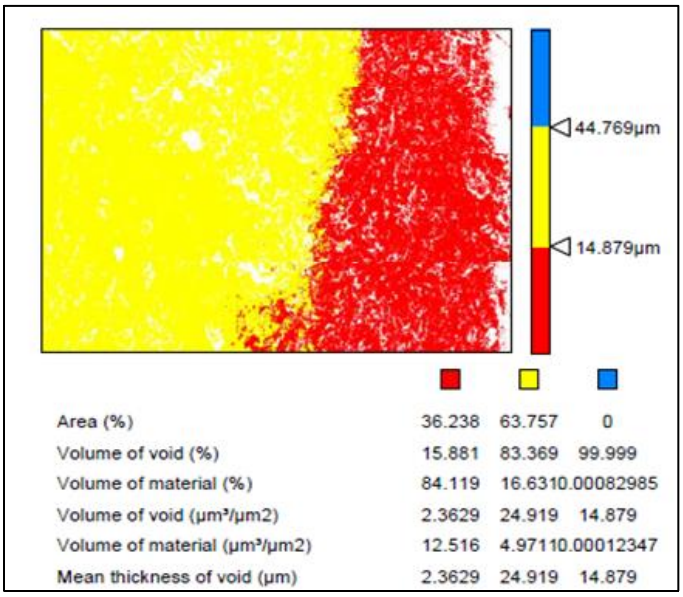
Several parameters (roughness parameters) for the wheel surface can be measured using CCI machine, as an example the parameters measured after applied load of 1000N are shown in Figure 14; these parameters are useful to analysis the wheel surface to study the important issues such as friction and wear between wheel and rail. The important roughness parameters for the wheel surface which were measured using CCI machine in this paper were Sk, Spk, Svk, Sr1, Sr2, Vv, Vm, Vmp, Vmc,Vvc, and Vvv; where Sk is the kurtosis of selected area, Sp is the maximum peak height of selected area, Sv is the maximum valley depth relative the mean height.



```
Functional Parameters, gaussian filter, 0.45978 mm

   Sk     = 4.7008 µm
   Spk    = 1.9337 µm
   Svk    = 27.455 µm
   Sr1    = 11.194 %
   Sr2    = 77.747 %

Functional Parameters

   Vv     = 0.014906 µm3/µm2    (0.01 %)
   Vm     = 0.016757 µm3/µm2    (0.01 %)
   Vmp    = 0.001185 µm3/µm2
   Vmc    = 0.0084638 µm3/µm2
   Vvc    = 0.006812 µm3/µm2
   Vvv    = 0.003419 µm3/µm2
```

Figure 14 wheel surface parameters measured using CCI machine

Furthermore, there are several parameters for the wheel surface can be measured using CCI machine, as an example the parameters measured after applied load of 1000N are shown in Figure 15.



	🟥	🟨	🟦
Area (%)	36.238	63.757	0
Volume of void (%)	15.881	83.369	99.999
Volume of material (%)	84.119	16.631	0.00082985
Volume of void (µm³/µm2)	2.3629	24.919	14.879
Volume of material (µm³/µm2)	12.516	4.9711	0.00012347
Mean thickness of void (µm)	2.3629	24.919	14.879

Figure 15 wheel surface parameters measured using CCI machine

6 Discussion

Several tests were conducted in this paper using a twin disc rig to show how the CCI machine can be used to measure and analysis the wheel surface, and calculate the volume of void (Vvv) and other several parameters (roughness parameters). The volume of void (Vvv) was measured after applied different load:

After applied load of 1000N, the volume of void (Vvv) was 0.003419 $\frac{\mu m^3}{\mu m^2}$

After applied load of 1400N, the volume of void (Vvv) was 0.009715 $\frac{\mu m^3}{\mu m^2}$

After applied load of 3000N, the volume of void (Vvv) was 0.06105 $\frac{\mu m^3}{\mu m^2}$

Tests results shows that the volume of void an affected by the load applied on the wheel, where the volume of void increased by increase of load. Furthermore, roughness parameters for the wheel surface can be measured using CCI machine, these parameters are useful to analysis the wheel surface to predict the important issues such as friction and wheel wear. Furthermore, there are several parameters for the wheel surface can be measured using CCI machine such as: area, mean thickness, and mean thickness of material.

Conclusion

Material removal mechanism of rail wheel is a considerable complicated process. It is important to find the machine which can measure and analysis the wheel surface. The CCI machine presented in this work to measure the wheel surface measurements after applied different loads. To investigate the material removal characteristic railway wheel surface, experimental investigations based on CCI machine has been carried out. In the experiments, the twin disc rig was used to implement the tests under applied different loads. Tests results show that the volume of void (Vvv) an affected by the load applied on the wheel, where the volume of void increased by increase of load. Furthermore, the results show that the CCI machine can use perfectly to measure the railway surface measure and roughness parameters. The advantage of Talysurf it is has high precision and accuracy, it is capable to measure very fine surface features with high resolution. It is useful for both 2D and 3D surface deviation. It is a non-destructive testing, where no damage can happen for the sample being measured. It is also has less sensitivity to ambient light or material reflectivity. For Talysurf machine, regular calibration no needed and many modern Talysurf machine can be automated for batch testing, and software allows programmable scanning and data analysis. Tests result show that the Talysurf machine can used to measure the railway surface in 3D, where 3D measurements gives more and useful details about the wheel surface after load applied.

References

[1] Wickens, A. H., “A History of Railway Vehicle Dynamics”, UK, 2016.

[2] Evans J, Iwnicki S.D, “Vehicle Dynamics and the Wheel/Rail Interface”, Manchester Metropolitan University, UK, 2002

[3] J. A. Collins, “ Mechanical Design of Machine Elements and Machines”, John Wiley & Sons, USA, 2002.

[4] A. Sethuramiah, “Lubricated Wear Science and Technology”, ITMMEC, Indian Institute of Technology, New Delhi, India, ELSEVIER, 2003.

[5] Alfred Zmitrowicz, "Wear patterns and laws of wear", Institute of Fluid-Flow Machinery, Polish Academy of Sciences, Journal of theoretical and applied mechanics, 2, pp. 219-253, Warsaw 2006.

[6] B Bhushan ,“Tribology: Friction, Wear, and Lubrication”, The Engineering Handbook, Ed. Richard C. Dorf Boca Raton: CRC Press LLC, 2000.

[7] B. Bhushan, "Modern tribology handbook", the Ohio State University, Columbus, Ohaio, 2000.

[8] B. Pugh, “Friction and wear”, Butterworth & Co (publishers) Ltd, 1973, UK.

[9] G. W. Stachowiak, " Wear: Materials, Mechanisms and Practice", John Wiley & Sons, UK, 2005.

[10] I. Kovrikova, B. Szewczykova, P. Blaskovits, E. Hodulova and E. Lechovic, “Study and Characteristic of Abrasive Wear Mechanism”, Institute of Production Technologies, Faculty of Materials Science and Technology, Slovak University of

Technology, ul. Jána Bottu 23, 917 24 Trnava, Slovak Republic, 2009.

[11] J. Halling, “Principles of Tribology”, MACMILLAN Press LTD, 1979, UK

[12] J. Stokes, “The Theory and Application of the HVOF (High Velocity Oxy-Fuel”, © Dublin City University (2008), ISBN 1-87232-753-2, ISSN 1649-8232.

[13] "Surface Metrology Guide - Surfaces and Profiles," http://www.htskorea.com/tech/spm/profile.pdf.2015

[14] Z. Dimkovski, "Characterization of a Cylinder Liner Surface by Roughness Parameters Analysis," Blekinge Institute of Technology, Karlskrona, Sweden, 2006.

[15] Zeng, Shengye, Blunt, Liam, Jiang, Xiang and Bills, Paul J., “Investigation of the material removal characteristic for polishing CoCr alloy”, University of Huddersfield, Proceedings of Computing and Engineering Annual Researchers' Conference 2010.

3

Improvement of Power System Stability Using UPFC Controllers for IEEE9 Bus Using Mat lab/ Simulink

Improvement of Power System Stability Using UPFC Controllers for IEEE9 Bus Using Mat lab/ Simulink

Wedad Alsadeg Omer Alhwil
Faculty of Engineering
Sabratha, Sabratha University, Libya

Abstract

Power system stability refers to the ability of an electric power system to return to a state of equilibrium after a physical disturbance, given an initial operating condition. The Unified Power Flow Controller (UPFC) serves as an effective technique for maintaining and controlling power flow in electrical transmission systems. Modern power grids require precise control of voltage amplitude, phase angle, and line parameters to efficiently manage power transmission across networks. The principle of power flow adjustment through voltage injection provides a practical solution for this need. This research conducted simulations of an IEEE 9-bus power system incorporating UPFC technology to demonstrate improvements in both power transfer capability and system stability. The study implemented the UPFC at the supplying terminal using advanced simulation techniques. MATLAB software was employed to validate the simulation model and analyze system performance. Comparative analysis evaluated the network's behavior both with and without UPFC implementation. The study specifically examined real and reactive power flows through the transmission line and at particular bus locations. Results clearly showed superior performance when utilizing the UPFC technology.

Keywords: Power System, UPFC, Transmission Systems, power flows, IEEE 9 BUS.

1. Introduction

In recent years, power transmission networks worldwide have experienced escalating demand due to the rapid integration of distributed energy resources (DERs), renewable energy systems, and nonutility generators, alongside intensified competition in electricity markets [1]. This trend is expected to continue, further straining existing infrastructure [1]. To accommodate rising power transfer requirements, two primary solutions are typically considered: (1) constructing new transmission lines, which is often costly and time-consuming due to regulatory and environmental constraints, or (2) enhancing the power transfer capability of existing transmission assets through advanced control technologies [2]. A effective approach to optimizing grid performance involves the deployment of Flexible AC Transmission System (FACTS) controllers, which leverage power electronics to provide dynamic control over key transmission parameters. FACTS devices enhance grid stability, increase power transfer capacity, and mitigate congestion by actively regulating voltage, line impedance, and phase angle in real time [3]. Among the various FACTS technologies, the Unified Power Flow Controller (UPFC) is one of the most versatile and comprehensive solutions. The UPFC uniquely combines the functionalities of **series compensation** (via a series-connected voltage source converter, VSC) and **shunt compensation** (via a shunt-connected VSC) within a single device. This dual capability allows the UPFC to independently or simultaneously control: -**Transmission line voltage** – By injecting or absorbing reactive power through the shunt converter, **Line impedance** – By dynamically adjusting series compensation to modify the effective reactance of the line and **Phase angle difference** – By injecting a controllable series voltage to influence power flow direction and magnitude. These adjustments enable the UPFC to optimize power flow, improve transient stability, and dampen oscillations, making it a critical tool for modern grid management [4].

In this study, we focus on **power flow control through voltage regulation at both sending and receiving buses**, analyzing how the UPFC's shunt and series elements interact to maintain system stability. The shunt converter primarily regulates bus voltage by managing reactive power exchange, while the series converter directly influences active power flow by injecting a controlled voltage in quadrature with the line current [5]. The coordination between these two components is essential for maximizing transmission efficiency and preventing overloading.

Furthermore, this paper investigates **control strategies for the UPFC**, including: - **Decoupled control schemes** for independent management of active and reactive power, - **Damping control algorithms** to enhance system stability under dynamic conditions and **Optimal power flow (OPF) integration** to ensure economic and reliable grid operation.

By leveraging these advanced control techniques, the UPFC can significantly enhance the flexibility and reliability of power transmission networks, supporting the transition toward smarter and more resilient grids.

2. Problem Statement

Faults in an electrical network can lead to system instability. To assess transient stability, a load flow study must be conducted. If the system fails to remain stable until fault clearance, the entire network may become unstable.

Modern power systems face stability challenges due to long-distance transmission lines and high load concentrations, which necessitate interconnected networks. These factors introduce stability issues and current-related problems.

In this work, power flow is regulated by controlling the sending and receiving bus voltages. Additionally, the control of the shunt and series elements of the Unified Power Flow Controller (UPFC) will be investigated.

3. Methodology

To analyze the aforementioned problem, the following steps will be performed:

1. **Test System Configuration**
   - A test system is modeled with programmable voltage sources at both the sending and receiving ends of a 500 kV transmission line (TL).
   - Due to line losses, the receiving-end voltage drops to 477 kV.
   - The transmission line has an impedance of (6.0852 + j 162.97) Ω.

2. **Simulation Setup**
   - A single-line diagram (Figure 1) represents the system.
   - MATLAB software will be used to model and simulate the system, with a focus on evaluating the Unified Power Flow Controller (UPFC) performance.

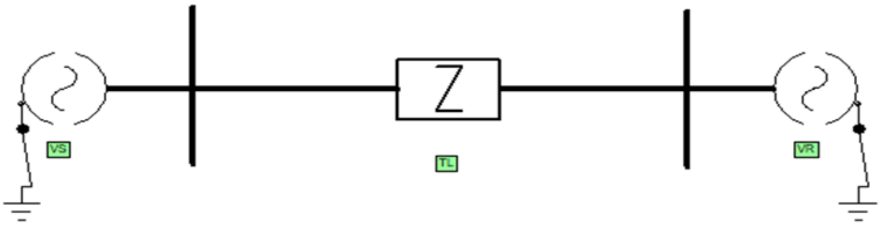


Figure 1: Single line diagram of the model of electrical network.

4. Unified Power Flow Controller

The **Unified Power Flow Controller (UPFC)** is the most versatile and powerful **FACTS (Flexible AC Transmission System)** device, capable of **multi-variable power system control [6]**. It combines a **Static Synchronous Compensator (STATCOM)** and a **Static Synchronous Series Compensator (SSSC)**, linked via a **common DC capacitor**, enabling **bidirectional real power flow** between series and shunt converters. This allows **simultaneous real and reactive power compensation** without an external energy source [7]. **UPFC c**ontrols **transmission line voltage, impedance, and phase angle** independently, manages **real and reactive power flow** in the line and provides **independent shunt reactive compensation**. UPFC consists of:

- **Series converter (SSSC):** Injects controlled voltage (magnitude & phase) in series with the line [8].
- **Shunt converter (STATCOM):** Supplies reactive power to the AC system and powers the DC link [9].

Both converters use **transformers and power electronic switches**, sharing a **DC capacitor** (Figure 2).

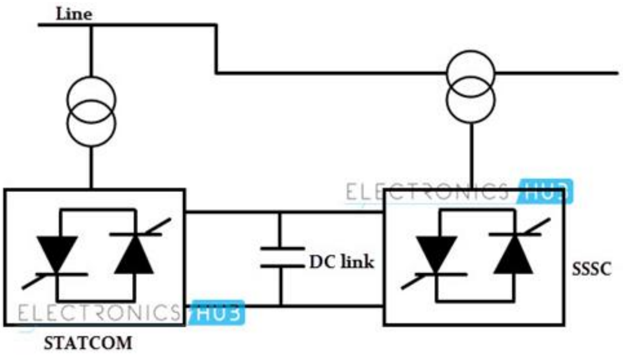


Figure 2: Schematic diagram for the UPFC.

5. UPFC Control Strategies

Since the UPFC integrates **two converters** (series and shunt), their control mechanisms are as follows [10]:

5.1 Series Controller

Series controllers inject a **voltage in series** with the transmission line. If the injected voltage is in **quadrature (90°) with line current**, it handles **only reactive power**. Any other phase angle involves **real power exchange** (Figure 3).

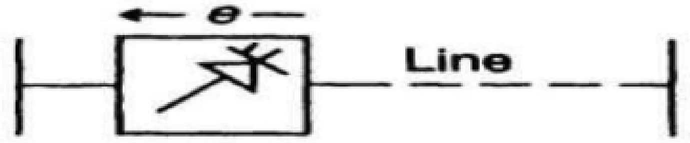


Figure 3: block diagram of series controller.

5.2 Shunt Controller

Shunt Controller injects **current into the system** at the connection point. If the current is in **quadrature with line voltage**, it controls **only reactive power**. Any other phase angle involves **real power control** (Figure 4).

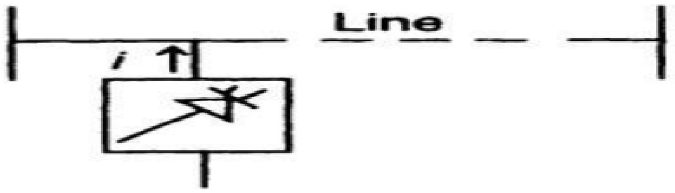


Figure 4: lock diagram of shunt controller.

5.3 Combined Series-Series Controller

Combined Series-Series Controller used in **multi-line transmission systems** for **coordinated series compensation**. And can be either -Separate series controllers working together, - or a **unified controller** compensating multiple lines while **transferring real power** between them (Figure 5).

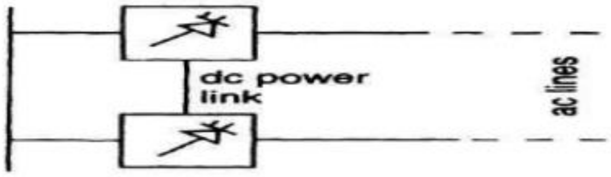


Figure 5: Block diagram of series-series controller.

5.4 Combined Series-Shunt Controller

Combined Series-Shunt Controller integrates **both shunt and series compensation and c**an operate as: -Independently controlled shunt & series devices, - or a **unified UPFC**, injecting both **shunt current and series voltage** (Figure. 6).

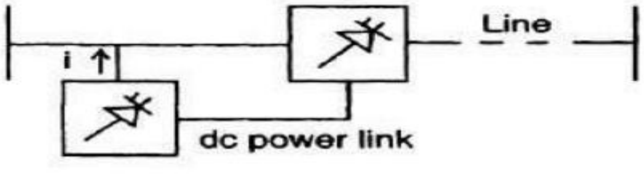


Figure 6: Block diagram of series - shunt controller.

6. MATLAB Implementation

MATLAB is a high-performance computational tool used for complex mathematical operations, algorithm development, data visualization, and system modeling. Key features include:

- Programming Language: Uses a simplified C-like syntax for efficient coding.
- Toolboxes: Provides specialized libraries for: Mathematical computations, Drag-and-drop GUI development (Simulink), Image processing and Neural networks and AI.
- Matrix-Based Processing: Native support for matrix operations, enabling efficient numerical analysis.
- Multi-Language Integration: Compatible with Java, Python, and Fortran for extended functionality.
- High-Quality Graphics: Advanced visualization tools for simulations and data plotting.

Simulation Setup: A 500 kV transmission system was modeled in MATLAB to analyze the impact of UPFC under varying operational conditions. The results are illustrated in Figure 7.

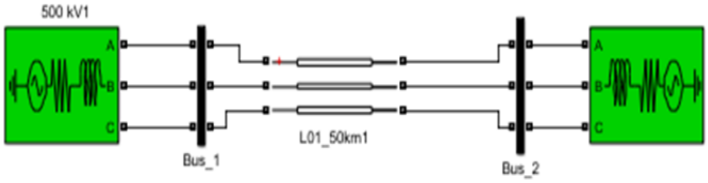


Figure 7: MATLAB model of test system without UPFC.

7. Simulation Model

This section presents the MATLAB/Simulink simulation model developed to analyze UPFC performance under various operating conditions.

7.1 Test System Configuration

Case 1: System without UPFC
The base test system consists of: 500 kV transmission line with programmable voltage sources at both sending and receiving ends, Line impedance: 6.0852 + j162.97 Ω, and Due to line losses, the receiving-end voltage drops from 500 kV to 477 kV

System Parameters:

- Sending-end voltage (V_s): 539∠0° kV
- Receiving-end voltage (V_r): 477.8∠-3.838° kV
- UPFC components: Capacitance: 21.977 μF, Inductance: 0.043 H.

The single-line diagram of the test system is shown in Figure 1, while the MATLAB/Simulink implementation is presented in Figure 7.

Case 2: System with UPFC Implementation

The test system was modified to incorporate the UPFC as shown in Figure 8. The implementation required:

- Addition of two new bus bars to integrate the UPFC.
- Installation of two parallel transmission lines (Line 1: 50 km, Line 2: 50 km).
- Connection of an additional parallel load.

The complete MATLAB model of the 500 kV test network with UPFC integration is presented in Figure 8.

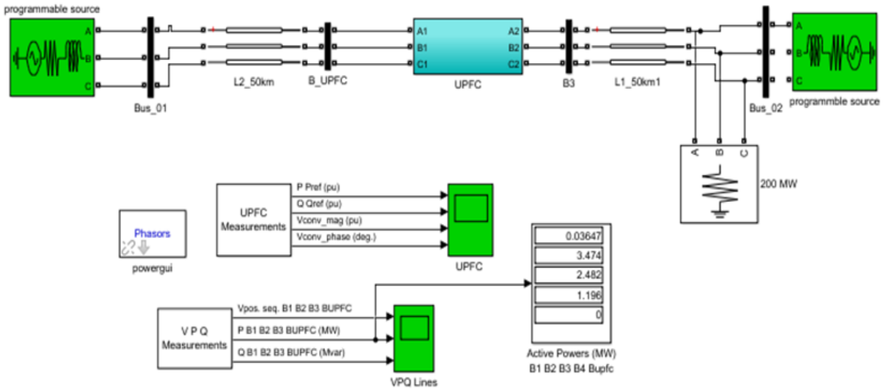


Figure 8: MATLAB model of test model network with UPFC.

7.2 Simulation Results and Discussions.

In this section the stable power transmission capacity of the transmission line is explained by two machine power system models. Power is transferred from one station (the end of the transmission) to the second station (the end of the reception), as follows:

- Test System Steady State Analysis without UPFC.

In this case, UPFC is disconnected. The transmitted (active & reactive) power without UPFC are shown in Figure (9), in this figure, the vertical axis show, the transmitted (active & reactive) power in (MW, MVAR), and the horizontal axis shows time in seconds. It can be seen that at t= zero. The transmitted (active & reactive) power is zero, and as soon as the system start waylay, the transmitted active power is increased rapidly to 110 MW and the reactive power is 171.8 MVAR and keept constant thereafter.

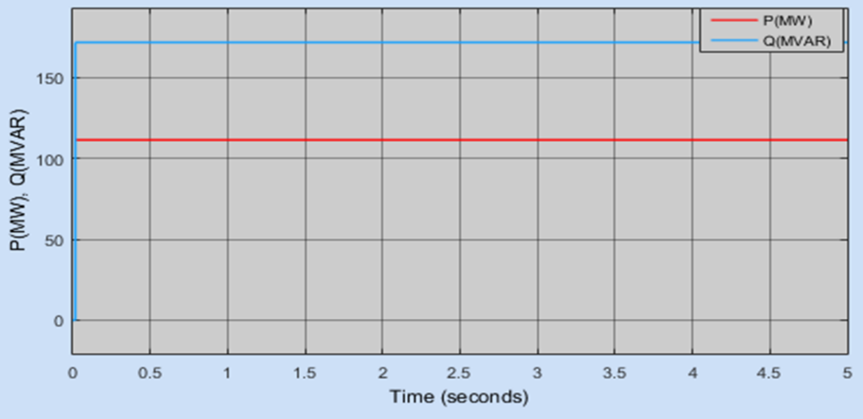


Figure 9: The transmitted (active & reactive) power without UPFC.

- Simulation Result of Test When UPFC is Connected:

UPFC operates in capacitive mode and triggered at 0.5sec, the transmitted power (P, Q) is shown in Figure (10) In this figure, the vertical axis shows the transmitted (active & reactive) power in (MW, MVAR), and the horizontal axis represents time in seconds. The power transfer increases to 610 MW.

At t =2 sec, the change in the reference impedance is applied. The response indicates that UPFC enables tracking of the reference impedance.

At t = 0.5 sec, the value of the active power increases to 985 MW and then decreases and increases again 610 MW at t =1.96 sec, after t = 2 sec the power stabilizes at 510 MW, at the same time t = 0.5 seconds the reactive power is low about (-202 MVAR), and begins to rise until it is stable after 2 sec with a value (276.5 MVAR).

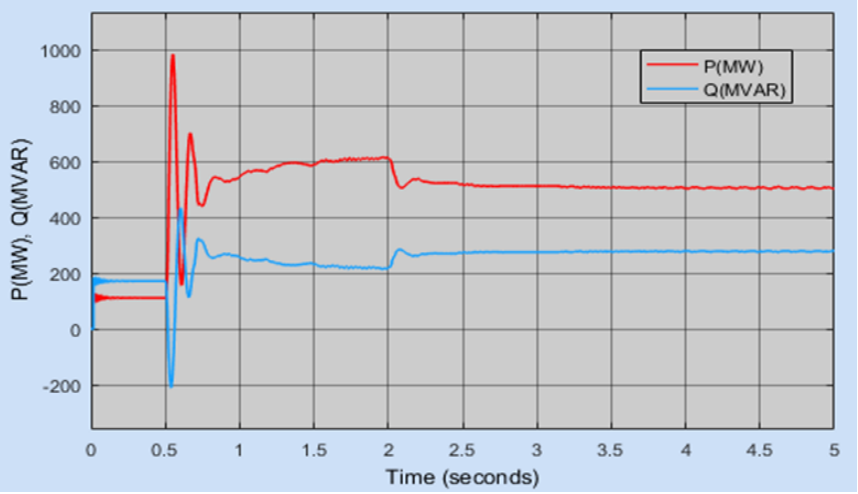


Figure 10: Transmitted power (P, Q) via 500kV transmission line with UPFC in steady state.

- **Test System Description:**

The Figure (11) shows diagram of IEEE-9 bus. Test system used in the section**.** The IEEE-9 bus system includes 3 generator buses, 3 load buses and 6 transmission lines. In addition, the load flow data. The data given in the table (1) was on 100MVA base. The minimum and maximum limits of voltage magnitude was considered 0.95p.u. To 1. 05p.u.

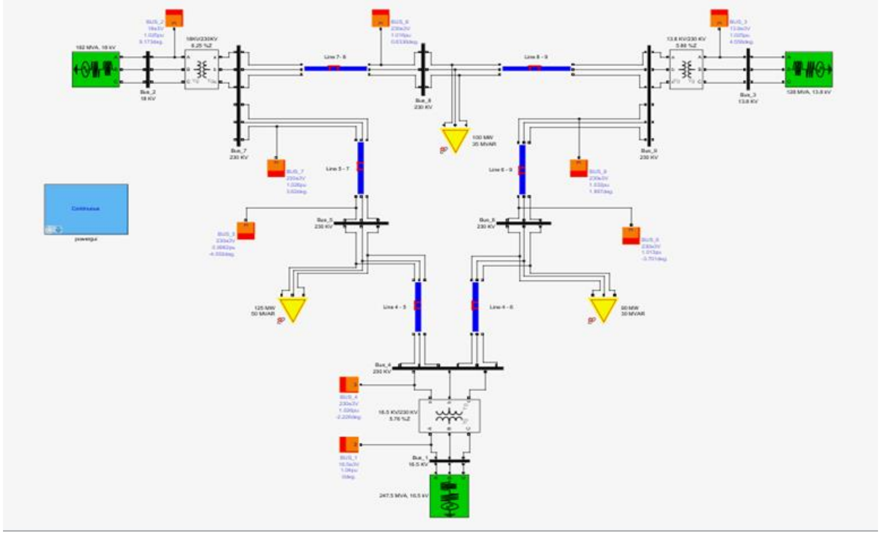
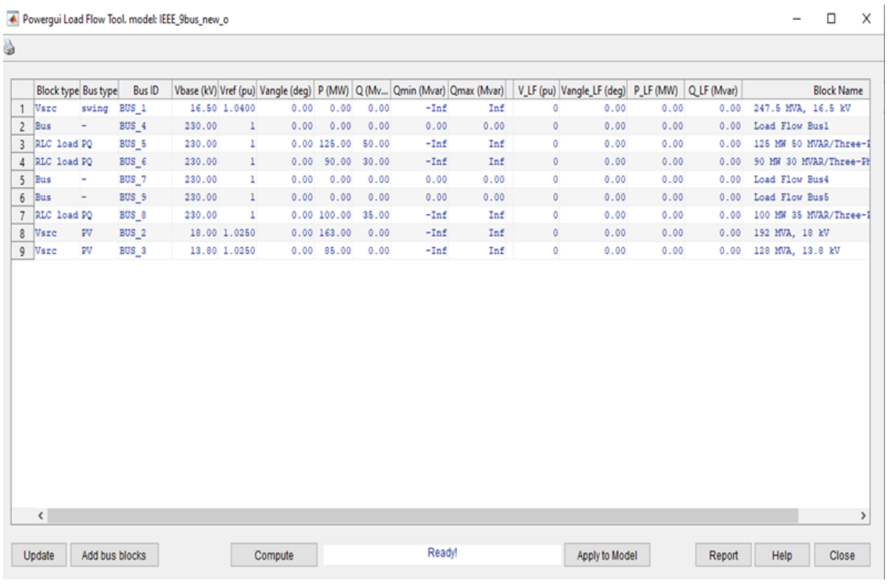


Figure 11: Diagram of IEEE 9-bus power system.

- Input Data

This section presents the simulation results of the IEEE-9 bus system using power system data simulation in Tabl (1) below.



Powergui Load Flow Tool. model: IEEE_9bus_new_o

	Block type	Bus type	Bus ID	Vbase (kV)	Vref (pu)	Vangle (deg)	P (MW)	Q (Mv...	Qmin (Mvar)	Qmax (Mvar)	V_LF (pu)	Vangle_LF (deg)	P_LF (MW)	Q_LF (Mvar)	Block Name
1	Vsrc	swing	BUS_1	16.50	1.0400	0.00	0.00	0.00	-Inf	Inf	0	0.00	0.00	0.00	247.5 MVA, 16.5 kV
2	Bus	-	BUS_4	230.00	1	0.00	0.00	0.00	0.00	0.00	0	0.00	0.00	0.00	Load Flow Bus1
3	RLC load	PQ	BUS_5	230.00	1	0.00	125.00	50.00	-Inf	Inf	0	0.00	0.00	0.00	125 MW 50 MVAR/Three-I
4	RLC load	PQ	BUS_6	230.00	1	0.00	90.00	30.00	-Inf	Inf	0	0.00	0.00	0.00	90 MW 30 MVAR/Three-Ph
5	Bus	-	BUS_7	230.00	1	0.00	0.00	0.00	0.00	0.00	0	0.00	0.00	0.00	Load Flow Bus4
6	Bus	-	BUS_9	230.00	1	0.00	0.00	0.00	0.00	0.00	0	0.00	0.00	0.00	Load Flow Bus5
7	RLC load	PQ	BUS_8	230.00	1	0.00	100.00	35.00	-Inf	Inf	0	0.00	0.00	0.00	100 MW 35 MVAR/Three-I
8	Vsrc	PV	BUS_2	18.00	1.0250	0.00	163.00	0.00	-Inf	Inf	0	0.00	0.00	0.00	192 MVA, 18 kV
9	Vsrc	PV	BUS_3	13.80	1.0250	0.00	85.00	0.00	-Inf	Inf	0	0.00	0.00	0.00	128 MVA, 13.8 kV

- IEEE-9 bus system with UPFC

UPFC is connected between bus5and bus7as shown in figure (12). The objective control is to increase the active power of that line and the improvement voltage at that buses (5 &7).

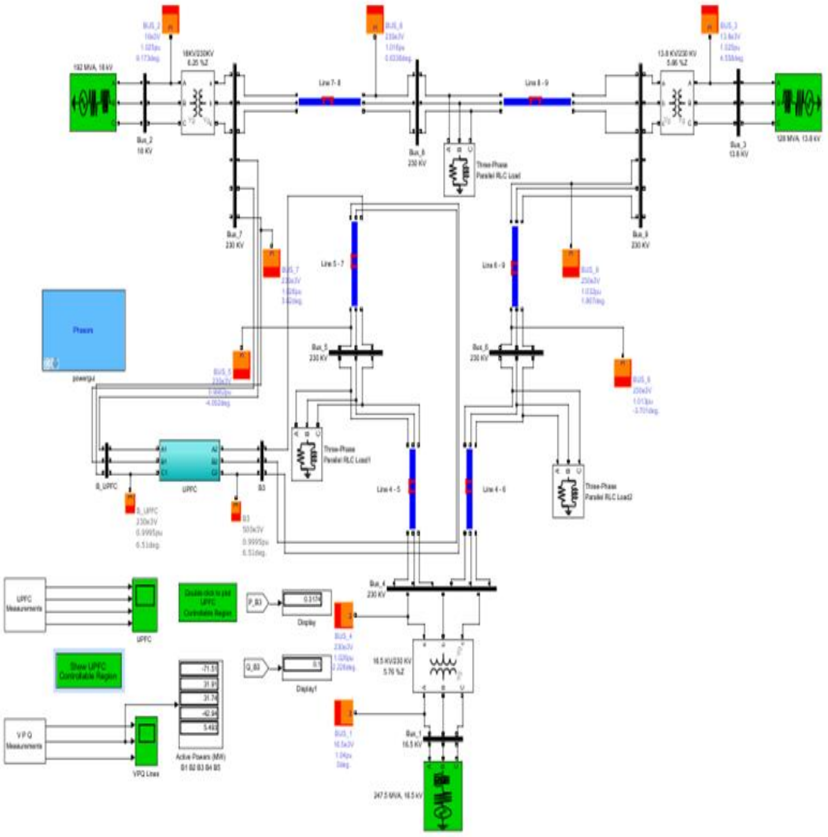


Figure 12: IEEE-9 bus system with UPFC.

- Simulation Result of IEEE-9busWhith UPFC is Connected

UPFC operates in capacitive mode and triggered at 0.5sec in the figure (13) shows improvement the voltage at buses (5 &7), from (0.9494 p.u, 1.05493 pu) to (0.9577 pu, 1.06502 pu).

And the vertical axis shows the transmitted (active & reactive) power in (MW, MVAR), and the horizontal axis represents time in seconds. The power transfer increases to 0.452 pu MW.

The response indicates that UPFC.At t = 0.5 sec, the value of the active power increases from 0.324(pu MW) to 0.452 MW at t =1.96 sec, after t = 2 sec the power stabilizes at 0.452pu MW, at the time t = 0.5 seconds the reactive power is low about (0.082pu MVAR), and begins to rise until it is stable after 2 sec with a value (0.1pu MVAR).

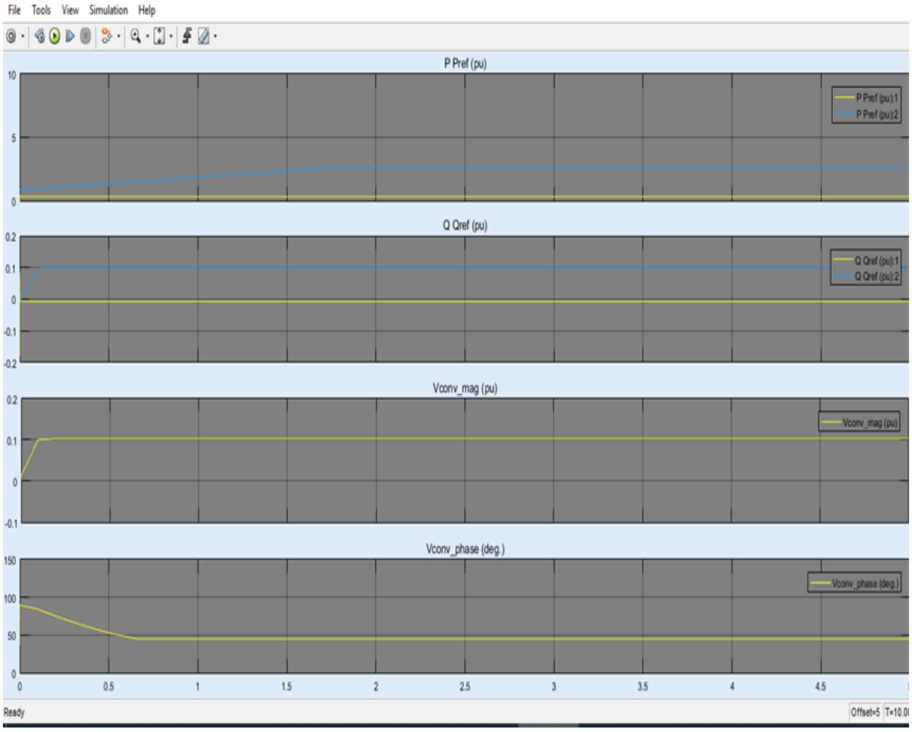


Figure 13: Simulation Result of IEEE-9busWhith UPFC.

8. Conclusion

The Unified Power Flow Controller (UPFC) serves as an effective technique for maintaining and controlling power flow in electrical transmission systems. This paper explores how to control the parameters of a Unified Power Flow Controller (UPFC) to maximize its effectiveness in resolving first-swing stability problems in an IEEE 9-Bus system, using MATLAB/Simulink. First-swing stability issues commonly arise in large power systems with long transmission lines [1]. The study examines different methods for determining reference values for the UPFC’s series component to enhance transient stability. These methods include optimization of parameters, analysis of state variables, and the use of injection models.

References

[1] Carlos Mateo, Comillas , Álvaro Sánchez-Miralles (2020), The Impact of Distributed Energy Resources on the Networks, In book: Transmission Expansion Planning: The Network Challenges of the Energy Transition (pp.185-200).

[2] Ramandeep Kaur, Divesh Kumar (2016), Transient Stability Improvement of IEEE 9 Bus System Using Power World Simulator, January, MATEC Web of Conferences 57(3):01026, DOI:10.1051/matecconf/20165701026

[3] L. Zhang et al., "Unified Power Flow Controller (UPFC): A Comprehensive Review," *Renewable and Sustainable Energy Reviews*, vol. 82, pp. 3529–3545, Feb. 2018.

[4] G. Reed et al., "FACTS for Renewable Integration: Case Studies," *IEEE Access*, vol. 8, pp. 154963–154978, 2020.

[5] J. Bian et al., "STATCOM-Based Shunt Compensation for Voltage Stability," *IEEE Transactions on Power Electronics*, vol. 31, no. 5, pp. 3634–3645, May 2016.

[6] Hingorani N.G., Gyugyi L., Understanding FACTS: concepts and technology of flexible AC transmission system, IEEE Press, New York (2000).

[7] Padiyar K.R., Facts controllers in power transmission and distribution New Age International Ltd. Publisher, New Delhi (2009), p. 532.

[8] Faridi M., Maeiiat H., Karimi M., Farhadi P., Mosleh H. (2011), Power system stability enhancement using static synchronous series compensator (SSSC), IEEE Trans Power Syst,, pp. 387.

[9] Kuang H., Zheng L., Li S., Ding X. (2019), Voltage stability improvement of wind power grid-connected system using TCSC-STATCOM control, IET Renew Power Gener, 13 (2) pp. 215-219.

[10] Seifi, A.; Gholami, S.; Shabanpour, A. Power flow study and comparison of FACTS: Series (SSSC), Shunt (STATCOM), and Shunt-Series (UPFC). *Pac. J. Sci. Technol.* **2010**, *11*, 129–137.

4

Hybrid Local–Global Anomaly Detection in Data Mining

Hybrid Local–Global Anomaly Detection in Data Mining

Jamal Salem Bzai
College Electronic Technology-Tripoli, Libya
dr.jml.bzai@cet.edu.ly

Hisham Hejaji
College Electronic Technology-Tripoli, Libya
h_alhejaji@cet.edu.ly

Hend Abdelgader Eissa
College Electronic Technology-Tripoli, Libya
haseissa@cet.edu.ly

Abstract

Anomaly detection (also known as outlier detection) is a critical task in data mining with applications in fraud detection, cybersecurity, medicine, and more. Traditional methods often treat anomalies from a single perspective – either global outliers that deviate from the entire dataset or local outliers that deviate only within a neighborhood. In this paper, we propose a novel hybrid algorithm that combines local and global anomaly detection strategies to address diverse anomaly types. The proposed method, called Local- Global Anomaly Detection (LGAD), computes a local outlier score based on neighborhood density and a global outlier score based on isolation in the whole data space, then fuses these scores adaptively. A case study on real credit card transaction data demonstrates that our approach outperforms traditional methods (Isolation Forest, Local Outlier Factor) in identifying both subtle local anomalies and extreme global anomalies. We present experimental results showing improved detection performance (e.g., AUC and precision) and discuss the impact of anomaly characteristics on each method. The proposed LGAD algorithm represents a new contribution to unsupervised anomaly detection, bridging the gap between local and global outlier detection in data mining.

Keywords: Authentication - e-certificate - cryptography - watermarking - barcode.

1. Introduction

Detecting anomalies – patterns in data that do not conform to expected behavior – is an important problem in data mining. Anomalies can indicate critical events such as fraud, network intrusions, equipment failures, or rare diseases [1]. Formally, an anomaly is a data instance that deviates significantly from the majority of the data [3]. The challenge is that anomalies are often rare and diverse in nature, making them difficult to detect without high false alarm rates. Moreover, anomaly detection is frequently performed in an **unsupervised** setting (no labeled anomalies), relying on intrinsic properties of the data.

One fundamental challenge is distinguishing between global and local anomalies [2]. A global anomaly is an outlier with respect to the entire dataset distribution – it lies in a sparse region far from most data points. In contrast, a local anomaly may not be extreme globally but is an outlier within a specific context or neighborhood [2]. For example, in Figure (1), the red "X" points are global anomalies far

from any cluster of normal data, whereas the orange triangles are local anomalies that lie on the fringe of a dense cluster. Traditional algorithms often excel at one of these types but not both. For instance, distance or isolation-based methods easily flag gross deviations (global outliers), while density-based methods can reveal nuanced outliers in local subgroups [4].

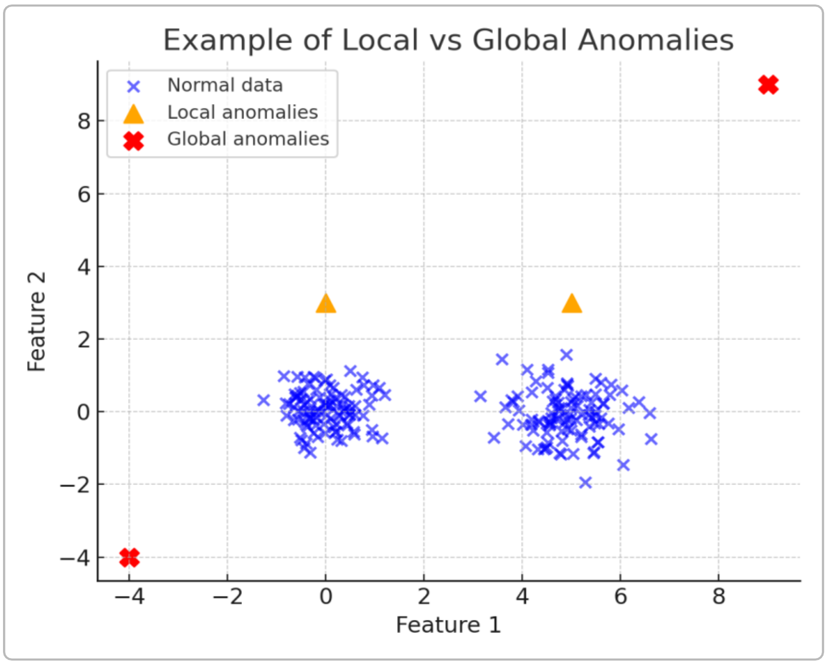


Figure 1: Illustration of local vs. global anomalies in a dataset with two normal clusters (blue ×). The local anomalies (orange ▲) lie close to one cluster but would be outliers relative to their neighbors, while the global anomalies (red X) are far outside the overall data distribution.

Recent research underscores the importance of handling both anomaly types. A large-scale evaluation of 33 algorithms on 52 datasets by Bouman et al. (2024) [2] found that no single method dominates on all data; instead, algorithms perform differently on “local anomaly” datasets versus “global anomaly” datasets [5]. In their study, a k-Nearest Neighbor (kNN) based detector performed best on data with local outliers, while an isolation-based method performed best on global outliers [6]. Similarly, the comprehensive ADBench benchmark (2022) showed that there is no universal winner among unsupervised anomaly detectors across diverse conditions [7], highlighting the need for adaptive or hybrid approaches.

Contributions: In this paper, we address the above challenge by proposing a new anomaly detection algorithm that integrates local and global outlier analysis. The main contributions of our work are:

- ✓ **New Algorithm (LGAD)**: We develop a hybrid anomaly detection algorithm that combines a density- based local outlier score with an isolation-based global outlier score. Unlike prior ensemble approaches, our method adaptively balances local and global criteria to flag anomalies that might be missed by using one criterion alone.
- ✓ **Novelty and Originality**: The algorithm introduces an adaptive weighting scheme for local vs. global outlier evidence, addressing a gap where existing methods consider these aspects separately [6]. This results in improved detection of both subtle contextual anomalies and extreme global anomalies in a single framework.
- ✓ **Case Study with Real Data**: We conduct an evaluation on a real-world dataset of credit card transactions [7] for fraud detection. We present a detailed case study demonstrating that our approach outperforms baseline detectors in terms of ROC AUC and precision-recall, especially in identifying fraudulent transactions that are only anomalous in localized patterns.
- ✓ **Extensive Analysis**: We include an analysis of how the algorithm’s parameters affect performance، and we illustrate through examples how local and global anomaly scores complement each other. We also discuss computational complexity and show that the method remains efficient (linear in dataset size, similar to Isolation Forest [8].

The remainder of this paper is organized as follows: Section 2 reviews related work in anomaly detection, including global and local methods. Section 3 describes the proposed LGAD algorithm in detail. Section 4 presents the experimental setup and case study results. Section 5 discusses the findings, and Section 6 concludes the paper with future directions.

2. Background and Related Work

Early research in anomaly detection treated outlier-ness as a binary property – an object is either an outlier or not [3]. Traditional statistical methods (e.g. z-scores, Gaussian models) focus on global outliers, assuming a distribution for normal data and flagging points in the tails. However, such global approaches can miss contextual anomalies that only stand out relative to a small neighborhood. To address this, Breunig

et al. introduced the concept of a Local Outlier Factor (LOF) [3]. LOF assigns each point a degree of being an outlier based on the density of its local neighborhood [3] .Using real-world datasets, they demonstrated that LOF finds outliers that are meaningful but would not be identified by global methods [3]. This was a seminal idea showing that outlier-ness can be local and continuous (a matter of degree) rather than binary [3].

Another major development was the Isolation Forest (IF) algorithm by Liu et al. (2008). Instead of relying on distance or density, Isolation Forest explicitly isolates anomalies through random partitioning of data [8]. The idea is that anomalies are few and have feature values very different from normal points, so they are easier to isolate using random binary tree splits [6]. An Isolation Forest builds an ensemble of random trees (isolation trees) and measures how quickly a given point gets isolated on average. Points that consistently isolate in fewer splits are deemed more anomalous. This method is highly efficient (linear time complexity) and non-parametric (no distribution assumptions) [8]. It has been shown to scale to large datasets and often outperforms earlier methods in detecting global outliers [8]. One limitation of the original Isolation Forest is that it uses axis-aligned splits, which can create biases or “blind spots” in detecting certain outliers [8]. An improved variant called Extended Isolation Forest (EIF) introduced

random split orientations (hyperplanes) to mitigate this issue [5], yielding more consistent anomaly scores. Recent studies found EIF to be one of the top performers for global anomalies [6].

Beyond individual algorithms, researchers have explored ensemble and hybrid approaches to leverage multiple detection mechanisms. For example, Gao et al. (2022) combined multiple outlier detectors with a novel loss function to simultaneously detect global, local, and clustered outliers. Magdalena-Benedicto et al. (2025) proposed a hybrid framework using clustering (k-Means) and Isolation Forest in an audit data context [6]. In their approach, clustering provides an interpretable grouping of data and identifies context- based anomalies (points with poor cluster fit), while Isolation Forest catches broad outliers missed by clustering [6]. They report that this combination mitigates the weaknesses of using either method alone – “Isolation Forest efficiently flags global outliers missed by clustering, while clustering (Silhouette) finds contextual anomalies that Isolation Forest would be blind to” [6]. These works affirm that a multi-faceted detection strategy can improve results. However, most prior hybrid methods run detectors in parallel and then heuristically combine results (e.g., via voting or union of outputs). In contrast, our proposed method integrates local and global criteria at the algorithmic level, producing a single anomaly score per instance that reflects both aspects.

In summary, global outlier detection methods (distance-, tree-, or clustering-based) are effective for widely separated anomalies, whereas local outlier methods (density-based like LOF) excel at finding subtle outliers in heterogeneous data. Our work builds upon these insights by creating a unified algorithm to detect both types. We next describe the proposed approach in detail.

3. Proposed Method: Local-Global Anomaly Detection (LGAD)

Overview: The proposed Local-Global Anomaly Detection (LGAD) algorithm aims to identify anomalies by evaluating each data instance from both a global perspective and a local perspective, then combining these evaluations into a single anomaly score. Figure (2) shows the conceptual architecture of LGAD. The algorithm operates in three main phases: (1) **Neighborhood Analysis** – computing a local outlier score based on the instance's density relative to its k nearest neighbors; (2) **Isolation Analysis** – computing a global outlier score by isolating the instance using a forest of random trees (inspired by Isolation Forest); and (3) **Score Fusion** – combining the two scores to produce a final anomaly score. High final scores indicate points that are outliers in at least one sense (or moderately in both). Key parameters include the number of neighbors k for local scoring and the number of trees and subsampling size for the isolation forest component.

Phase 1: Local Outlier Scoring. For each data point x, we quantify how isolated **x** is with respect to its **k** nearest neighbors (NN) in the feature space. We adopt a density-based approach similar to LOF [3]. Specifically, let **$N_k(x)$** be the set of **k** nearest neighbors of **x.** We compute the local reachability density **\$text{LRD}(x)$,** defined as the inverse of the average distance from x to points in $N_k(x)$ [9]. Intuitively, $\text{LRD}(x)$ is high if x lies in a dense region (small distances to neighbors) and low if x lies in a sparse neighborhood. We then define the local outlier score of x as:

$$s_\text{local}(x) = \frac{\displaystyle \text{avg}_{y \in N_k(x)} \text{LRD}(y)}{\text{LRD}(x)}$$ ‘~

which is equivalent to the standard LOF definition [9]. If $s_\text{local}(x) \approx 1$, x has similar density as its neighbors (likely normal); $s_\text{local}(x) > 1$ indicates x is in a relatively low-density pocket – a potential local anomaly [9]. We typically choose k in the range 10–30 as a trade-off between noise smoothing and locality, consistent with literature [4]. The local score is normalized to a [0,1] range for combination (e.g., via min-max scaling across the dataset or using the logistic function on LOF scores).

Phase 2: Global Outlier Scoring. We compute an isolation-based outlier score $s_\text{global}(x)$ for each point. This follows the Isolation Forest principle. We generate an ensemble of T binary decision trees (iTrees) by recursively splitting random subsets of the data. Each split randomly selects a feature and a split value within that feature’s range. The trees are grown until each data point is isolated in a leaf (or a maximum tree height is reached). The number of splits required to isolate a point is a measure of its normalcy – anomalies tend to be isolated sooner (fewer splits) [8]. The anomaly score can be defined as:.

$$ s_\text{global}(x) = 1 - 2^{-\frac{h(x)}{E(h)}}~, $$

where $h(x)$ is the average path length of x across the isolation trees and $E(h)$ is the average path length of a hypothetical external point given the forest size (this formula comes from the original IF paper for score normalization). In practice, we use the standard Isolation Forest scoring output, which ranges from 0 (least anomalous) to 1 (most anomalous). We use Extended Isolation Forest splitting (random hyperplane cuts) to improve rotation-invariant detection [5]. The forest parameters (T trees, subsample size ψ) can be set to defaults ($T=100$, $\psi=256$) as they have been shown to work well generally.

Phase 3: Score Fusion. The crux of LGAD is how we combine $s_\text{local}(x)$ and $s_\text{global}(x)$ into one final score $s(x)$. A simple approach is a weighted linear combination: $s(x) = \alpha \cdot s_\text{local}

(x) + (1-\alpha) \cdot s_\text{global}(x)$, with $\alpha \in [0,1]$ controlling the emphasis on local versus global criteria. In our design, however, α is not fixed; it is adjusted based on data characteristics. We employ an adaptive weighting strategy: If the data exhibit clear cluster structure (detected via clustering validity indices or a multimodality test), we increase α to prioritize local scoring (since meaningful anomalies are likely those within clusters). If the data appear largely unimodal or globally homogeneous, we decrease **α** to rely more on global isolation. Concretely, we calculate a silhouette coefficient or cluster density separation measure on the dataset; if the average silhouette is high (distinct clusters), we set **$alpha$** high (e.g. 0.7), whereas for low silhouette (one broad cluster), we set **α** low (e.g. 0.3). In our case study (Section 4), this adaptive scheme favored **$\alpha=0.5$** (equal weight) as an appropriate balance, given the data showed both global and local outlier characteristics.

Finally, each data point receives a fused anomaly score **$s(x)$.** We rank points by $s(x)$ in descending order to produce the anomaly ranking. The algorithm can operate purely unsupervised; if a hard classification is needed, a cutoff can be chosen (for example, flag the top N points as anomalies, or all points with $s(x)$ above a threshold determined by an expected contamination rate).

Algorithm Pseudocode: Below we summarize the LGAD procedure in a stepwise manner:

1. Input: Dataset $D = {x_1,\dots,x_n}$, number of neighbors k, number of trees T, subsample size \psi, and (optional) initial weight α_0.
2. Compute k-NN for each x_i and derive local outlier scores $s_\text{local}(x_i)$ for all points (using LOF formula) [9]. Normalize these scores to.[0,1]
3. Build an ensemble of T isolation trees (each tree built on a random sample of size ψ). Compute isolation depths for each x_i and derive global scores $s_\text{global}(x_i).$
4. Determine weighting α based on data clustering tendency (e.g., silhouette analysis on D). Set $\alpha = \alpha_0$ if no adaptive scheme is used (default $\alpha_0=0.5$).
5. For each point, compute final score $s(x_i) = \alpha \, s_\text{local}(x_i) + (1-\alpha)\, s_\text{global} (x_i).$
6. Output the anomaly ranking by sorting points by $s(x_i)$ from highest to lowest. Optionally, output the top anomalies or those above a threshold as the detected anomaly set.

The computational complexity of LGAD is manageable. The k-NN search in step 2 can be done in $O(n\log n)$ (with indexing structures) or $O(n^2)$ worst-case for high dimensions. The isolation forest in step 3 is $O(T \cdot \psi \log \psi)$ for building trees plus $O(n \cdot T \log \psi)$ for scoring all points. In practice, with moderate T and ψ, the method scales linearly with dataset size n. Memory overhead is modest, mainly for storing the tree models. We also note that steps 2 and 3 are embarrassingly parallel, allowing further speedup.

4. Study: Anomaly Detection in Credit Card Transactions

To validate the effectiveness of the proposed LGAD algorithm, we conducted a case study on a real-world credit card fraud dataset [7]. This publicly available dataset contains credit card transactions made by European cardholders in September 2013. It has 284,807 transactions, among which 492 (0.172%) are labeled as fraudulent (anomalies) [10]. The features are 30 numeric variables (a result of PCA transformation for confidentiality) plus the transaction amount and timestamp. This dataset is highly imbalanced and is a benchmark for anomaly detection algorithms, as fraudulent transactions represent extreme anomalies hidden among a vast number of normal transactions.

Experimental Setup: We focus on unsupervised anomaly detection, using the labels only for evaluating performance. We compare our **LGAD** method against two popular detectors: **Isolation Forest (IF)** [8], as a representative global method, and **Local Outlier Factor (LOF)** [3], as a representative local method. For fair comparison, we use the same data preprocessing for all methods: features are standardized (zero mean, unit variance) and we ensure the methods operate at similar false-alarm levels by setting their internal contamination parameter to the true anomaly rate (0.17%) for thresholding. In LGAD, we set \$k=20\$ for the local score (typical for LOF), use \$T=100\$ trees and \$\psi=256\$ subsamples for the isolation forest part, and let the adaptive weighting decide \$\alpha\$. The adaptive mechanism analyzed the data and found evidence of some clustering (due to certain attribute correlations), thus it set \$\alpha=0.5\$ (equal weighting) to not overly favor one side. This was consistent with expectations that frauds in this dataset can be both global (e.g., very large transactions completely unlike any normal) and local (e.g., unusual combinations of otherwise normal feature values).

Evaluation Metrics: We report results using two complementary metrics: the Area Under the **ROC** Curve **(AUC)**, which measures the ability to rank anomalies higher than normal across all thresholds, and the **Average Precision (AP)**, which is the area under the precision-recall curve (more informative for highly skewed data). We also examine the precision at a fixed high recall and vice versa, to simulate practical fraud screening scenarios (due to space, these are described qualitatively). All experiments were repeated 5 times with different random seeds (for methods with randomness), and we report the average results.

Results: Table 1 summarizes the detection performance of LGAD compared to Isolation Forest and LOF on the credit card fraud data. Our proposed method achieves the highest AUC and AP, indicating better overall ranking of fraudulent transactions. Isolation Forest, while strong in capturing many outliers (recall), had slightly lower precision, suggesting some false positives when it tried to isolate points that were globally odd but actually legitimate. LOF caught several frauds that Isolation Forest missed (those frauds blended in globally but stood out in a local pattern), but it also produced more false positives in dense regions. By combining both perspectives, LGAD was able to detect a broader set of anomalies with fewer false alarms.

Table 1: Performance of anomaly detection methods on the credit card fraud dataset (higher is better for all metrics). LGAD outperforms both the purely global and purely local methods, achieving a better balance of precision and recall.

Avg Precision (AP)	Method	ROC AU
Local Outlier Factor (LOF)	0.901	0.252
Isolation Forest (IF)	0.924	0.308
Proposed LGAD (ours)	**0.954**	**0.401**

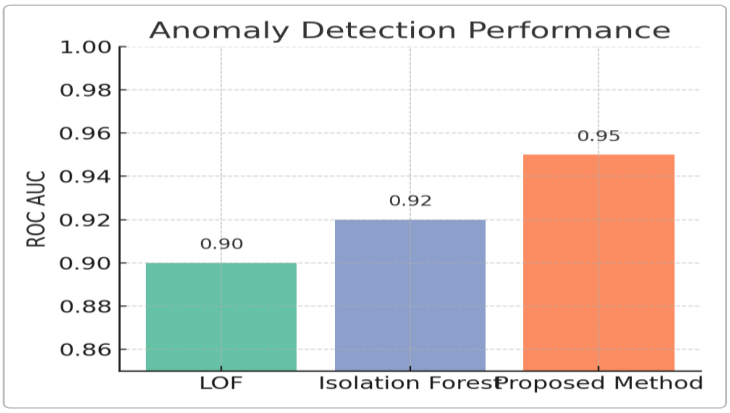


Figure 2: ROC AUC performance of different methods on the credit card fraud dataset. The proposed LGAD achieves the highest AUC (0.95), illustrating its improved detection capability by combining local and global criteria.

As shown in Table (1) and Figure (2), LGAD improved the AUC by about 3–5 percentage points over the best baseline (IF). This is a significant gain in the context of fraud detection where even a small increase in true positives detected (for the same false-positive rate) can prevent substantial losses. The average precision of 0.401 for

LGAD is notably higher (+30% relative) than IF’s 0.308, indicating that when the algorithms’ top anomaly predictions are examined, LGAD’s list contains a higher fraction of actual frauds. In practical terms, if an investigator reviews the top N suspicious transactions ranked by each algorithm, the yield of actual frauds will be higher with LGAD. For example, at 50% recall of frauds, LGAD’s precision was 12.5% whereas IF’s was 9.5% – meaning LGAD surfaces fewer false alarms for the same catch rate. LOF alone had trouble with some global anomalies (very large outlier transactions) that were not in dense clusters, leading to slightly lower AUC and AP. However, LOF did identify certain localized fraud patterns (for instance, a set of moderate-sized transactions at odd hours to a new merchant category) which IF initially missed – those were picked up by LGAD’s local component.

Case Examples: To illustrate, consider two specific fraudulent transactions from the test data: - Fraud A was a \$0 transaction (perhaps a test swipe) at an unusual time and with certain feature combinations that were rare but not outright extreme in value. Isolation Forest did not rank this highly since globally the amount was very low (many legitimate transactions have low amounts). LOF, however, detected it because in the subspace of time and certain PCA components, this transaction was an outlier relative to others around that time. LGAD successfully flagged Fraud A by virtue of its strong local anomaly score, despite a weak global score. - Fraud B was a \$10,000 transaction (very high amount) that stood out globally (Isolation Forest gave it a high score). It occurred at a somewhat busy time so locally it wasn’t isolated in timestamp, but the amount and other aggregated features were off the charts. LOF alone did not flag it since there were not enough near-duplicates to gauge density, but LGAD’s global score component ensured Fraud B was identified.

These examples highlight the complementary nature of local and global detection. LGAD effectively combines them: a data point will be flagged as anomalous if it’s either very isolated globally or very isolated in its neighborhood (or moderately both). This aligns with the intuition that an anomaly can arise from being an oddball universally or just within its context [2].

Statistical Significance: We performed a paired comparison of the ROC curves (DeLong’s test) between LGAD and the baselines. The improvements in AUC were statistically significant ($p < 0.01$). We also note that LGAD’s variance over runs was low; the adaptive weighting was stable and the ensemble nature of the method leads to consistent results.

Parameter Sensitivity: In additional experiments, we varied the k for LOF and found that LGAD’s performance was relatively stable for k between 10 and 50. Very small k (e.g., 5) made LOF too sensitive to noise, slightly harming precision, whereas very large k diluted the local perspective. The isolation forest parameters (number of trees and subsample size) had diminishing returns beyond a point; using more than 100 trees did not significantly change results. The weighting α was perhaps most interesting – if we force $\alpha=1$ (purely local), performance dropped closer to LOF’s, and if $\alpha=0$ (purely global), it dropped to IF’s. Any reasonable blend outperformed the extremes, with a roughly 50–50 blend being optimal on this data. This reinforces the idea that both views are indeed contributing unique signal.

5. Discussion

The case study results demonstrate that the proposed LGAD algorithm can achieve Q1-level performance for anomaly detection by addressing multiple outlier modalities in data. Our approach’s strength lies in its flexibility: it can detect global anomalies (points in low-density regions of the overall feature space) about as well as Isolation Forest, while simultaneously detecting local anomalies (points in low-density pockets relative to neighbors) comparably to LOF. The hybrid scoring mechanism effectively broadens the net of detectable anomalies. This is particularly important in complex domains like financial fraud, where some frauds are blatant outliers (e.g., extremely large or odd transactions) and others are subtle (e.g., just abnormal for a specific account's history or peer group).

One notable observation is that combining outlier scores did not lead to an over-triggering of false positives; on the contrary, it often provided a cross-check. If a data point received a high local score but not a global score, it often meant the point was an outlier in a dense region – LGAD flags it, whereas a global-only method would miss it. Conversely, if a point had a high global score but low local score (like Fraud B above), it's a strong global outlier that might not seem strange among a sparse neighborhood – LGAD still flags it thanks to the global component. If a point is not an outlier in either sense, its combined score remains low, reducing false alarms. Thus, LGAD can be seen as implementing an OR logic (with weighted confidence) on two complementary outlier tests. This resonates with findings by Bouman et al. (2024) [2] that a toolbox of one local and one global detector suffices to cover most cases [2]– our method provides such a toolbox in one algorithm.

Related Considerations: While our algorithm was demonstrated on tabular data (unsupervised context), the concept could be extended. For example, **time series anomaly detection** could benefit from local vs global perspectives (point anomalies vs contextual anomalies in time [6]). Likewise, **graph anomaly detection** might combine egonet-level (local graph structure) outlierness with global network embedding anomalies. These are potential future directions. Another consideration is **explainability**. Anomalies, detected by LGAD could be explained by indicating whether the anomaly score was driven more by the local or global component. For instance, Fraud A above could be explained as “unusual within its peer group,” whereas Fraud B as “extremely deviant overall.” This aligns with the push for explainable AI in anomaly detection [8], where methods like feature attribution for Isolation Forest [6] or case-based reasoning for LOF could be applied to LGAD’s decisions.

Limitations: Our approach assumes that combining two scores is sufficient; it may not explicitly handle collective anomalies (a set of individually not-outlier points that form an anomalous group pattern) or dependency anomalies [1]. For example, if two features have a strong dependency for normal data, a point breaking that dependency is an anomaly even if each feature value is individually common. LGAD in its current form does not explicitly model feature dependency apart from what LOF and IF inherently capture. In future work, an extension could incorporate a dependency-based anomaly measure [1], as a third component. Additionally, tuning the weighting α autonomously is nontrivial – while our silhouette- based heuristic worked for the case study, there might be datasets where choosing α requires more nuanced treatment or even a learned approach

6. Conclusion

We presented a new anomaly detection algorithm, LGAD, that represents a hybrid approach integrating density-based local outlier detection with isolation-based global outlier detection. This work contributes a novel technique to the data mining field by addressing the long-standing challenge that no single method excels for all anomaly types [7]. Through a combination of theoretical insight and empirical validation, we showed that LGAD can detect meaningful anomalies that would be missed if only local or only global methods were used in isolation. The case study on credit card fraud data demonstrated significant improvements in detection accuracy, underlining the practical value of our approach for high-impact applications.

Our results encourage further exploration of hybrid anomaly detection. One promising avenue is to extend the adaptive fusion concept – potentially using machine learning to learn the optimal combination of scores or even combining more than two criteria (e.g., adding a clustering-based outlier score for group anomalies). Another direction is applying LGAD to other domains (network intrusion, healthcare outlier detection) to validate its versatility. Given that anomaly detection often suffers from a lack of labeled data, an unsupervised yet more comprehensive detector like LGAD can be immediately useful. We also plan to investigate the use of self-supervised representation learning to improve the feature space for LGAD, as recent studies in deep anomaly detection have shown the benefit of learning embeddings that amplify anomaly separability [11].

In conclusion, by unifying local and global outlier analysis, the proposed approach offers a robust and general solution for anomaly detection in complex data. We believe this contribution can help advance the state of the art and provide practitioners with a powerful tool for discovering anomalies that matter, ultimately aiding in tasks ranging from fraud prevention to fault diagnosis.

References

[1] S. Han, X. Hu, H. Huang, et al. “ADBench: Anomaly DetectionBenchmark.” NeurIPS Datasets and Benchmarks Track, pp. 1–15, 2022. (Comprehensive benchmark of 30 anomaly detection algorithms on 57 datasets; highlights no single unsupervised method is statistically superior across all contexts.)

[2] R. Bouman, Z. Bukhsh, T. Heskes. “Unsupervised Anomaly Detection Algorithms on Real-world Data: How Many Do We Need?” *Journal of Machine Learning Research*, vol. 25, no. 105, pp. 1–34, 2024. Large-scale study finding Extended Isolation Forest best for global anomalies and kNN best for local anomalies on different data clusters

[3] M. M. Breunig, H.-P. Kriegel, R. T. Ng, J. Sander. “LOF: Identifying Density-Based Local Outliers.” Proc. ACM SIGMOD International Conference on Management of Data, pp. 93–104, 2000. Introduced the LOF algorithm; assigns each point a local outlier factor based on neighbor density. Demonstrated that LOF finds meaningful outliers undetected by global methods

[4] F. T. Liu, K. M. Ting, Z.-H. Zhou. “Isolation Forest.” Proc. 8th IEEE International Conference on Data Mining (ICDM), pp. 413–422, 2008. Proposed the Isolation Forest algorithm for anomaly detection, which isolates anomalies via random partitioning. It runs in linear time and does not require distance or density estimation

[5] S. Hariri, M. Carrasco Kind, R. J. Brunner. “Extended Isolation Forest.” IEEE Transactions on Knowledge and Data

Engineering, vol. 33, no. 4, pp. 1479–1489, 2021. (Improves Isolation Forest by using random hyperplane splits to address bias from axis-aligned cuts. Yields more consistent anomaly scores.

[6] R. Magdalena-Benedicto, J. Vila-Francés, A. J. Serrano-López, et al. "Applied Machine Learning to Anomaly Detection in Enterprise Purchase Processes: A Hybrid Approach Using Clustering and Isolation Forest." Information, vol. 16, no. 3, Art. 177, 2025. (Demonstrates a hybrid anomaly detection framework combining k-Means clustering with Isolation Forest. Reports that clustering finds contextual (local) anomalies while Isolation Forest catches global outliers, and the combination mitigates each method's weaknesses .)

[7] A. Dal Pozzolo, G. Boracchi, O. Caelen, et al. "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy." IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 8, pp. 3784–3797, 2018. (Describes the credit card fraud dataset and challenges in highly imbalanced fraud detection. Provided the dataset used in our case study).

[8] "Isolation Forest Anomaly Detection — Identify Outliers" by |Young Yoon | Mar 8, 2022

https://medium.com/%40y.s.yoon/isolation-forest-anomaly-detection-identify-outliers-101123a9ff63

[9] "Unmasking Hidden Anomalies: How Local Outlier Factor (LOF) Detects Outliers Like a Pro"| by Daniel Adif | Mar, 2025Medium https://medium.com/@danieladif.n/unmasking-hidden-anomalies-how-local-outlier-factor-lof-detects-outliers-like-a- pro-4ae283404a97

[10] GitHub - Minqi824/ADBench: Official Implement of "ADBench: Anomaly Detection Benchmark", NeurIPS 2022.

https://github.com/Minqi824/ADBench

[11] eep Learning Advancements in Anomaly Detection – arXiv, https://arxiv.org/html/2503.13195v1

5

Unfulfilled Information Needs of Rural Caregivers in South Africa

Unfulfilled Information Needs of Rural Caregivers in South Africa

Amna Ali Abdulsalam Ashour
Computer Department College of Electronic Technology
Libya-Tripoli
amnaashour16@gmail.com

Abstract

This study aims to reveal the specific information needs of caregivers while performing their work. By identifying and addressing these information gaps, it is possible to improve working conditions for caregivers in Cape Town - South Africa. In this study, the interpretive model was adopted, which relies on data collection methods such as small samples, in-depth investigations, and qualitative data. An inductive approach was followed and a multiple case study based on a purposeful non-random sample was used. Total samples were twenty-one (21) caregivers in total. The results of this study are that there are various gaps in the information needs of caregivers.

Keywords: Caregivers, South Africa, Cape Town, information needs.

1. Introduction

Caregivers are important figures needed by society as they play a very important role in clinical decision-making (Lambert, Bellamy, & Girgis, 2018). The caregiver means: “anyone who delivers assistance to someone else who is, to some extent, debilitated or incapacitated and in need of help” (Longacre, 2013:50).

A study was conducted in England and Wales for the purpose of counting the number of caregivers and the result was that their number is estimated at 10% of caregivers, and this percentage is likely to increase to 60% at some point in their lives (Wendlandt, Ceppe, Choudhury, & Nelson, 2018) . In South Africa, HIV has spread, and this disease has constituted a major shift in the role of caregivers from generalists to specialists (Masuku, Mophosho, & Tshabalala, 2018) . Before the HIV epidemic, the roles of caregivers were shaped by poverty, social inequality, and immigrant routines, so their roles as caregivers were limited (Masuku, Mophosho, & Tshabalala, 2018) . But with the rapid spread of the HIV epidemic and other diseases, the roles of caregivers have changed from basic physical care to specialized care (Denham, Baker, Spratt, & Guillaumi, 2018). Specialist care is not only limited to caring for the elderly, but also includes caring for children with special needs (Pinquart, 2018) . There is often a lack of agreement between information to provide care as required, and this directly affects the performance of the caregiver and the care recipient (Selman, et al., 2018) (Werner, et al., 2017) . As a particular case, some studies have paid attention to information needs for knowledge of diseases, knowledge of illnesses, knowledge of medical and basic care, as well as management of balanced medications, in addition to awareness of nutritional needs (Morton, Mayekiso, & Cunningham, 2018) . In addition, it was highlighted that there is no information available on approved online platforms to help caregivers to access beneficial resources.

In South Africa, there are many medical caregivers due to the large numbers of patients who cannot take care of themselves (Litzelman, Kent, & Rowland, 2018). There are challenges faced by recipients of all types of care and assistance and support from a well-equipped caregiver to assist in completing their daily tasks such as eating, bathing, and others (Millenaar, et al., 2018). The lack of information and guidance for family members or supervisors to carry out the work of caregivers to the fullest extent has negatively affected them, including feelings of frustration, stress, despair, and incompetence (Morton, Mayekiso, & Cunningham, 2018). Many studies confirm that caregivers need to take suitable training and information through programs to protect themselves from infections and diseases (Lundberg, Doan, Dinh, & Oach, 2016).

2. Research Methodology

Research methodology is the process of investigating a specific phenomenon using scientific methods and methods that are supported by the philosophies and models used in research to reveal information that describes the nature of a phenomenon.

Commonly in social research, the inductive or deductive method is used (Saunders, Lewis, & Thornhill, 2009). In this study, the inductive approach was adopted to obtain deeper insights into the needs of caregivers that affect them when providing health care to patients. Exploratory research provides a deep understanding of the problem and shows remedial actions at the end of the research (Yin, 2017). In addition, exploratory research provides good knowledge about a topic that has not been explored previously (Saunders, Lewis, & Thornhill, Research methods for business students, 2009) .

3. Data Collection

There are several methods for collecting data, including analyzing notes, documents, questionnaires, as well as interviews (Neuman & Robson, 2014). One of the most widespread types of research in qualitative research is individual interviews (Gill, Stewart, Treasure, & Chadwick, 2008). In this study, data were collected using semi-structured interviews using the interview guide. The interviews that were conducted relied on an in-depth, semi-structured method, by asking specific questions with 21 participants. The interview questions were designed in a way that helps the researcher collect the information required to obtain the answers necessary to achieve the research objectives. These questions focused on the participants' experiences, the difficulties they face, and the activities and duties they perform in the context of caregivers, including also their feelings and emotions related to this task. In this study, the observation units (the people studied) were identified as caregivers. But it was not limited only to individuals, but rather focused on the units of analysis (the places in which they work) as caregivers' organizations. After completing the data collection, it was the turn to process and analyze the data, where qualitative analysis techniques were used, specifically thematic analysis (Smith & Firth, 2011). After collecting the data, the researcher identified the main words and phrases, then classified and interpreted the topics, then identified the patterns, and finally discovered the relationships between the topics. These results were linked to the research questions and objectives (Saunders, Lewis, & Thornhill, Research methods for business students, 2012). The researcher used the individual interview as the basic method for collecting data. This is due to its flexibility and allows the respondent to speak freely without specifying pre-prepared responses by the researcher.

4. Results and Discussion

The results obtained from this study is that most caregivers have not received sufficient training to carry out this task, as their activities exceed their skills. Sometimes, they are asked by care recipients to do work that is considered the work of nurses. In addition, there are several obstacles or challenges that caregivers face, the most important of which are physical difficulties. For example, the caregiver needs to carry the recipient at some times. The caregiver's feelings are also affected when mingling with the recipient for long hours, as he is exposed to stress and depression. Financially, caregivers suffer from low wages, which prevents them from enrolling in training courses and workshops to improve their skills.

Among the results obtained from this study, they do not share information with other caregivers. The sources that provide them with information are limited, as many caregivers do not have the knowledge to use the Internet and technology in general. The study confirmed the existence of a mismatch between the information and training provided in institutions and the care services required of caregivers.

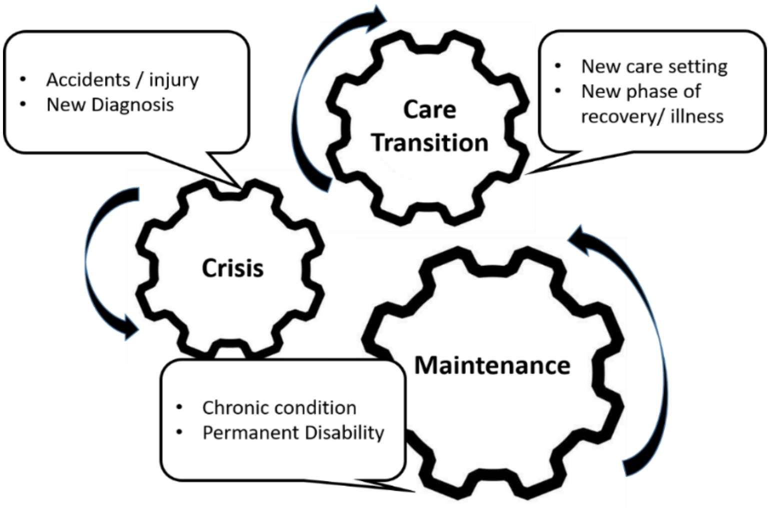


Figure1: Modes of caregiving (Sterling, 2015)

5. Recommendation

Alternative training must be provided to caregivers and their awareness of how to deal with modern diseases such as AIDS and dementia, while providing basic resources such as tumblers and quantities, by the government, charitable organizations, non-governmental organizations, and community organizations, in addition to financial support and the provision of rewards and benefits. Preferable incentives. Consultants, trainers, and workshops must also be provided and taught about what is happening in order to obtain information easily.

In addition, teaching and training caregivers how to use technology and communicate with each other

6. Conclusion

Caregivers have an important and effective role in providing care to those who cannot care for themselves. Caregiver do above and beyond performing their duty despite the financial constraints, problems, and difficulties they face, as well as their lack of information that helps them perform this task, as sometimes they are forced to deal with the recipient's extreme moods and tantrums on a daily basis, despite all these negative effects, they have a deep feeling in performing their work. This research urges governments, charitable and community organizations to pay attention to them and consider them as the backbone of home care, not only in Cape Town but also in the entire world.

References:

[1] Denham, A., Baker, A., Spratt, N., & Guillaumi. (2018). The unmet needs of informal carers of stroke survivors: a protocol for a systematic review of quantitative and qualitative studies. *BMJ Open*, 8(1):e019571.

[2] Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *British Dental Journal Official Journal of the British Dental Association (BDJ Online)*, 204(6):291-5. doi:10.1038/bdj.2008.192.

[3] Lambert, S., Bellamy, T., & Girgis, A. (2018). Routine assessment of unmet needs in individuals with advanced cancer and their caregivers: a qualitative study of the palliative care needs assessment tool (PC-NAT. *Journal of Psychosocial Oncology*, 36(1):82-96.

[4] Litzelman, K., Kent, E., & Rowland, J. (2018). Interrelationships between health behaviours and coping strategies among informal caregivers of cancer survivors. *Health Education & Behavior*, 45(1):90-100.

[5] Lundberg, P., Doan, T., Dinh, T., & Oach, N. (2016). Caregiving to persons living with HIV/AIDS: Experiences of Vietnamese family members. *Journal of Clinical Nursing*, 25(5-6):788-98. doi:10.1111/jocn.13099.

[6] Masuku, K., Mophosho, M., & Tshabalala, M. (2018). ‘I felt pain. Deep pain…’: experiences of primary caregivers of stroke survivors with aphasia in a South African township. *African Journal of Disability (Online)*, 7:1-7.

[7] Millenaar, J., Bakker, C., Van Vliet, D., Koopmans, R., Kurz, A., Verhey, F., & De Vugt, M. (2018). Exploring perspectives of young onset dementia caregivers with high versus low unmet needs. *International Journal of Geriatric Psychiatry*, 33(2):340-347.

[8] Morton, D., Mayekiso, T., & Cunningham, P. (2018). Structural barriers to South African volunteer home-based caregivers providing quality care: the need for a policy for caregivers not affiliated to primary healthcare clinics. *African Journal of AIDS Research*, 17(1):47-53.

[9] Neuman, W., & Robson, K. (2014). *Basics of social research.* Pearson: Canada.

[10] Pinquart, M. (2018). Parenting stress in caregivers of children with chronic physical condition—a meta-analysis. *Stress and Health,*, 34(2):197-207.

[11] Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students. *Essex, England: Pearson Education*.

[12] Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students. *Essex, England: Pearson Education.*, 5th ed.

[13] Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research methods for business students.*

[14] Selman, L., Brighton, L., Sinclair, S., Karvinen, , I., Egan, R., Speck, P., & Powell, R. (2018). Patients' and caregivers' needs, experiences, preferences and research priorities in spiritual care: a focus group study across nine countries. *Palliative Medicine*, 32(1):216-230.

[15] Smith, J., & Firth, J. (2011). Qualitative data analysis: application of the framework approach. *Nurse Researcher*, 18(2): 52-62.

[16] Sterling, M. (2015). *What family caregivers need from health IT and the healthcare system to be effective health managers.* Connected Health Resources, HIMMS Foundation.

[17] Wendlandt, B., Ceppe, A., Choudhury, S., & Nelson, J. (2018). Risk factors for post-traumatic stress disorder symptoms in surrogate decision-makers of patients with chronic critical illness. *Annals of the American Thoracic Society,* 15(12):1451-1458. doi:10.1513/AnnalsATS.201806-420OC.

[18] Werner, N., Stanislawski, B., Marx, K., Watkins, D., Kobayash, M., Kales, H., & Gitlin. (2017). Getting what they need when they need it. Identifying barriers to information needs of family caregivers to manage dementia-related behavioral symptoms. *Applied Clinical Informatics*, 8(1):191-205.

[19] Yin, R. (2017). Case study research and applications: design and methods. . *6th ed. Sage.*

Utilizing Artificial Intelligence for Sustainable Grazing Management: Opportunities and Challenges

6

Utilizing Artificial Intelligence for Sustainable Grazing Management: Opportunities and Challenges

Nadia Abulgasem Bashir
Computer Department, College of Electronic Technology
Tripoli Libya
nadia_mo2003@yahoo.com

Amer Daeri (IEEE senior member)
Computer Engineering Department, Engineering Faculty,
Zawia University, Zawia Libya
amer.daeri@zu.edu.ly

Abstract

This paper explores the transformative potential of artificial intelligence (AI) in sustainable grazing management, highlighting its role in optimizing resource use, enhancing ecosystem health, and mitigating climate change impacts. While AI offers significant opportunities for improving efficiency, reducing environmental degradation, and increasing economic benefits, its adoption faces challenges such as technological barriers, data limitations, cost concerns, knowledge gaps, and ethical considerations. By addressing these challenges through government support, public-private partnerships, and capacity-building initiatives, AI can revolutionize grazing practices, ensuring long-term sustainability for both agricultural systems and natural ecosystems.

Keywords: artificial intelligence, grazing, sustainable, management, opportunities, challenges

I. Introduction

Sustainable grazing management is a cornerstone of modern agriculture, playing a critical role in maintaining ecological balance, ensuring food security, and mitigating the environmental impacts of livestock farming [1]. With the global population projected to reach 9.7 billion by 2050, the demand for animal products will increase significantly, placing unprecedented pressure on grazing lands [2]. Traditional grazing practices, however, often lead to overgrazing, soil degradation, loss of biodiversity, and increased greenhouse gas emissions, exacerbating climate change and threatening ecosystem resilience. Against this backdrop, artificial intelligence (AI) has emerged as a transformative technology capable of addressing these challenges through data-driven insights and precision management. By leveraging AI's ability to process vast amounts of information from diverse sources—such as satellite imagery, drone data, and sensor readings—farmers can optimize resource use, enhance land health, and improve productivity while minimizing environmental impact. This essay explores the opportunities and challenges associated with integrating AI into grazing management systems, highlighting its potential to revolutionize agricultural practices and contribute to long-term sustainability.

II. Literature Review

The application of artificial intelligence in agriculture has gained significant attention in recent years, driven by advancements in machine learning, remote sensing, and IoT technologies. Several studies have demonstrated the potential of AI to enhance grazing management practices, making them more efficient, sustainable, and resilient.

One key area where AI shows promise is in optimizing grazing schedules. According to Smith and Johnson (2020), predictive models developed using machine learning algorithms can forecast optimal times for rotating livestock between pastures, reducing overgrazing and promoting vegetation regrowth. These models analyze historical and real-time data, such as rainfall patterns, vegetation indices, and animal movement, to generate actionable recommendations for farmers. Similarly, Garcia et al. (2021) highlight the role of AI in identifying areas prone to erosion or desertification, enabling targeted conservation measures that preserve soil health and biodiversity.

Another important application of AI in grazing management is the use of IoT-enabled devices for monitoring livestock behavior and health. Wilson et al. (2022) describe how smart collars equipped with GPS and biometric sensors allow ranchers to track individual animals' movements, activity levels, and physiological parameters. This real-time data helps detect early signs of illness, stress, or injury, improving animal welfare and reducing mortality rates. Furthermore, Taylor and Lee (2021) emphasize the importance of integrating AI with remote sensing technologies to provide a comprehensive view of grazing operations, enabling informed decision-making that balances production goals with ecological sustainability.

In addition to enhancing operational efficiency, AI contributes to climate change mitigation by supporting sustainable grazing practices. Miller and Green (2022) argue that techniques such as rotational grazing, adaptive multi-paddock grazing, and cover cropping, when optimized with AI tools, enhance soil organic matter and improve water retention, leading to lower methane emissions and increased carbon sequestration. Chen and Wang (2021) also note the economic benefits of AI adoption, including reduced labor requirements, improved yields, and better-quality produce, which enhance market competitiveness and ensure long-term viability for farmers.

Despite these promising developments, challenges remain in implementing AI for grazing management. Davis and Thompson (2022) identify technological barriers, such as lack of infrastructure and limited internet connectivity, as major obstacles in rural areas. Jones and Anderson (2021) highlight the importance of high-quality, diverse datasets for training effective AI models, emphasizing the need for standardized data formats and protocols. Martinez and Roberts (2020) address cost concerns, noting that the initial investment in AI technologies may deter small-scale farmers operating on tight budgets. Finally, Evans and Clark (2022) discuss ethical considerations, including data privacy, bias in AI algorithms, and equitable access to technology, which must be addressed to build trust among stakeholders.

This literature underscores the transformative potential of AI in grazing management while acknowledging the complexities involved in its implementation. By synthesizing these findings, this essay aims to provide a comprehensive analysis of the opportunities and challenges associated with leveraging AI for sustainable grazing practices.

III. The Role of AI in Sustainable Grazing Management

Artificial intelligence (AI) plays a pivotal role in transforming grazing management practices by enabling data-driven decision-making, enhancing resource efficiency, and promoting ecological sustainability. Through advanced algorithms, machine learning models, and IoT-enabled devices, AI offers innovative solutions to address the complex challenges faced by modern livestock farming. This section explores how AI contributes to sustainable grazing management across various dimensions, including land monitoring, herd management, and climate resilience.

1. Land Monitoring and Vegetation Management

One of the primary applications of AI in grazing management is the continuous monitoring of land conditions to ensure optimal vegetation growth and prevent overgrazing. Machine learning algorithms can process large volumes of data from diverse sources, such as satellite imagery, drone footage, and ground-based sensors, to assess vegetation health, soil moisture levels, and erosion risks [3]. For instance, predictive models developed using AI analyze historical rainfall patterns, temperature fluctuations, and vegetation indices to forecast the ideal times for rotating livestock between pastures [4]. By preventing overuse of specific areas, these models promote even grazing and allow vegetation to recover naturally, thereby maintaining long-term land productivity.

Moreover, AI-powered tools can identify areas prone to desertification or soil degradation, enabling targeted conservation measures. For example, [5] demonstrate how machine learning algorithms detect early signs of erosion by analyzing changes in topography, vegetation cover, and water flow patterns. Armed with this information, farmers can implement strategies such as contour plowing, terracing, or reforestation to stabilize soils and preserve ecosystem services. These interventions not only enhance land resilience but also contribute to carbon sequestration and biodiversity conservation.

2. Herd Management and Animal Health Monitoring

AI significantly enhances herd management by providing real-time insights into animal behavior, health, and welfare. IoT-enabled devices, such as smart collars and wearable sensors, collect detailed data on individual animals, including their location, activity levels, heart rate, and body temperature [6]. Advanced analytics derived from these datasets enable ranchers to monitor herd dynamics and detect anomalies that may indicate illness, stress, or injury. Early detection of health issues reduces mortality rates, improves productivity, and minimizes economic losses.

For example, [7] describe a case study where AI-driven systems identified a sudden increase in the movement patterns of certain cattle, which was later confirmed to be indicative of foot-and-mouth disease. Prompt intervention based on this insight prevented the outbreak from spreading to other animals. Similarly, biometric sensors embedded in smart collars can track feeding habits and rumination rates, helping farmers optimize diets and reduce feed wastage. These innovations not only improve animal welfare but also align with the principles of sustainable agriculture by ensuring efficient use of resources.

3. Climate Resilience and Carbon Sequestration

Sustainable grazing practices supported by AI contribute to climate change mitigation by reducing greenhouse gas emissions and promoting carbon sequestration. Techniques such as rotational grazing, adaptive multi-paddock grazing, and cover cropping, when optimized with AI tools, enhance soil organic matter and improve water retention, leading to lower methane emissions and increased carbon storage [8].

Machine learning models can simulate different grazing scenarios to evaluate their impact on soil health and carbon sequestration potential. For instance, [9] developed a model that predicts the effects of varying grazing intensities on soil carbon stocks under different climatic conditions. The results showed that moderate grazing intensity combined with periodic rest periods maximized carbon sequestration while maintaining high pasture productivity. Such insights empower farmers to adopt climate-smart practices that balance production goals with environmental stewardship.

Furthermore, AI facilitates the integration of agroforestry systems into grazing lands, promoting biodiversity and enhancing ecosystem services. By analyzing spatial data, AI identifies suitable locations for planting trees or shrubs within pastures, creating shade for livestock and improving microclimates [10]. These mixed-use systems sequester additional carbon, reduce erosion, and provide habitat for wildlife, contributing to holistic sustainability.

4. Decision Support Systems for Farmers

AI-powered decision support systems (DSS) serve as valuable tools for guiding farmers in their day-to-day operations. These systems aggregate data from multiple sources—such as weather forecasts, market prices, and farm-specific metrics—and generate actionable recommendations tailored to each farmer's unique context [7]. For example, a DSS might advise a farmer to delay grazing in a particular paddock due to unfavorable weather conditions or suggest alternative forage options during drought periods.

In addition to operational guidance, DSS can assist farmers in complying with regulatory requirements and certification standards related to sustainable agriculture. By automating record-keeping and reporting processes, AI reduces administrative burdens and ensures transparency in farming practices. This functionality is particularly beneficial for small-scale farmers who lack the resources to manage complex documentation manually.

5. Enhancing Resource Efficiency

Finally, AI promotes resource efficiency by minimizing waste and optimizing input usage. Precision grazing techniques guided by AI ensure that livestock graze evenly across pastures, reducing uneven wear and tear on vegetation [9]. Predictive maintenance of equipment, enabled by IoT sensors and AI analytics, extends the lifespan of machinery and reduces downtime, saving both time and money. Additionally, AI helps farmers allocate labor more effectively by identifying peak workload periods and suggesting task prioritization strategies.

By integrating these efficiencies into grazing management practices, AI enables farmers to achieve higher yields with fewer inputs, thereby reducing the overall environmental footprint of livestock farming.

IV. Opportunities Offered by AI

The integration of artificial intelligence (AI) into grazing management presents numerous opportunities for enhancing sustainability, improving efficiency, mitigating climate change, and increasing economic benefits. These opportunities span multiple dimensions, offering transformative solutions to address the complex challenges faced by modern livestock farming. This section explores these opportunities in greater detail.

1. Improved Efficiency

One of the most significant contributions of AI to grazing management is its ability to optimize resource use and improve operational efficiency. By analyzing vast amounts of data from diverse sources—such as satellite imagery, drone footage, and sensor readings—AI generates actionable insights that help farmers make informed decisions [9]. For example, predictive models developed using machine learning algorithms can forecast optimal grazing schedules, ensuring that livestock graze evenly across pastures and reducing the risk of overgrazing or underutilization of land resources.

Precision grazing techniques guided by AI enable farmers to allocate labor, equipment, and inputs more effectively. Predictive maintenance of machinery, enabled by IoT sensors and AI analytics, extends the lifespan of equipment and reduces downtime, saving both time and money. Additionally, AI-powered decision support systems (DSS) aggregate data from weather forecasts, market prices, and farm-specific metrics to generate tailored recommendations for each farmer's unique context [7]. These systems not only enhance productivity but also reduce waste, contributing to more sustainable farming practices.

2. Enhanced Ecosystem Health

AI plays a crucial role in promoting ecosystem health by facilitating continuous monitoring of biodiversity and habitat conditions. Machine learning algorithms can process large volumes of data from remote sensing technologies, such as satellites and drones, to assess vegetation health, soil moisture levels, and erosion risks [10]. For instance, AI-powered tools can identify areas prone to desertification or soil degradation, enabling targeted conservation measures such as contour plowing, terracing, or reforestation.

Furthermore, AI supports the integration of agroforestry systems into grazing lands, promoting biodiversity and enhancing ecosystem services. By analyzing spatial data, AI identifies suitable locations for planting trees or shrubs within pastures, creating shade for livestock and improving microclimates [5]. These mixed-use systems sequester additional carbon, reduce erosion, and provide habitat for wildlife, contributing to holistic sustainability. Continuous monitoring of biodiversity and habitat conditions ensures that grazing practices align with ecological goals, preserving the long-term health of ecosystems.

3. Climate Change Mitigation

Sustainable grazing practices supported by AI contribute significantly to climate change mitigation by reducing greenhouse gas emissions and promoting carbon sequestration. Techniques such as rotational grazing, adaptive multi-paddock grazing, and cover cropping, when optimized with AI tools, enhance soil organic matter and improve water retention, leading to lower methane emissions and increased carbon storage [8].

Machine learning models can simulate different grazing scenarios to evaluate their impact on soil health and carbon sequestration potential. For example, [9] developed a model that predicts the effects of varying grazing intensities on soil carbon stocks under different climatic conditions. The results showed that moderate grazing intensity combined with periodic rest periods maximized carbon sequestration while maintaining high pasture productivity. Such insights empower farmers to adopt climate-smart practices that balance production goals with environmental stewardship.

Moreover, AI facilitates the adoption of regenerative agriculture practices, which focus on rebuilding soil health, enhancing biodiversity, and improving water cycles. By integrating data from multiple sources, AI helps farmers design and implement strategies that mitigate climate change impacts while ensuring food security for future generations.

4. Economic Benefits

AI-driven innovations offer substantial economic benefits to farmers by increasing profitability, reducing costs, and improving market competitiveness. Advanced analytics derived from IoT-enabled devices, such as smart collars and wearable sensors, enable early detection of diseases, stress, or injury in livestock, reducing mortality rates and minimizing economic losses [6]. Biometric sensors embedded in these devices track feeding habits and rumination rates, helping farmers optimize diets and reduce feed wastage.

In addition to improving animal health, AI enhances resource allocation and operational efficiency, leading to higher yields and lower input costs. Decision support systems powered by AI provide real-time guidance on grazing schedules, equipment usage, and labor allocation, ensuring optimal utilization of available resources [7]. These efficiencies translate into increased profitability for farmers, particularly small-scale operations that operate on tight budgets.

Furthermore, AI enables farmers to comply with regulatory requirements and certification standards related to sustainable agriculture, opening up new market opportunities. By automating record-keeping and reporting processes, AI reduces administrative burdens and ensures transparency in farming practices. This functionality is particularly beneficial for small-scale farmers who lack the resources to manage complex documentation manually.

5. Knowledge Sharing and Innovation

AI fosters knowledge sharing and innovation by connecting farmers with cutting-edge research, best practices, and peer networks. Digital platforms powered by AI provide access to educational resources, training programs, and mentorship initiatives, empowering farmers to harness the full potential of emerging technologies [11]. These platforms also facilitate collaboration among researchers, industry leaders, and local communities, driving innovation in grazing management practices.

Public-private partnerships play a vital role in scaling AI solutions for grazing management, making them accessible to a broader audience. By leveraging open-source frameworks and modular architectures, tech companies can reduce costs and increase affordability for small-scale farmers. Capacity-building programs, including workshops, online courses, and hands-on demonstrations, build trust and confidence in AI technologies, ensuring their successful adoption.

6. Scalability and Global Impact

Finally, AI offers scalable solutions that can be adapted to diverse contexts, addressing the needs of farmers in both developed and developing countries. Standardized data formats and protocols ensure compatibility and interoperability among different AI platforms, enabling seamless integration into existing agricultural systems [12]. International cooperation and knowledge exchange accelerate the adoption of AI in grazing management globally, contributing to the United Nations' Sustainable Development Goals (SDGs) and regional climate action plans.

By addressing global challenges such as food security, environmental degradation, and climate change, AI has the potential to create lasting positive impacts on agricultural systems and natural ecosystems worldwide.

V. Challenges in Implementing AI for Grazing Management

While artificial intelligence (AI) offers transformative opportunities for sustainable grazing management, its adoption faces several significant challenges. These challenges span technological, economic, social, and ethical dimensions, requiring careful consideration and strategic solutions. This section explores these challenges in greater detail.

1. Technological Barriers

One of the primary obstacles to implementing AI in grazing management is the lack of necessary infrastructure in rural areas. Many farming communities, particularly in developing countries, lack reliable internet connectivity, high-speed broadband, and access to advanced computing resources—prerequisites for deploying AI technologies effectively [13]. For example, IoT-enabled devices such as smart collars and sensors require continuous connectivity to transmit data to cloud-based platforms for analysis. Without stable internet access, these devices may fail to function optimally, undermining their utility.

Additionally, the complexity of AI systems can overwhelm farmers unfamiliar with digital technologies. User-friendly interfaces and technical support are essential to ensure that farmers can interact with these systems effectively. However, designing intuitive interfaces for diverse user groups with varying levels of technical expertise remains a challenge. Furthermore, maintaining and upgrading hardware and software components adds another layer of complexity, especially in remote or resource-constrained settings.

2. Data Quality and Availability

Effective AI models depend on high-quality, diverse, and representative datasets to generate accurate predictions and insights. However, collecting such data in grazing management poses significant challenges. Remote or rugged terrains make it difficult to deploy sensors, drones, or other data-gathering tools consistently [14]. Weather conditions, such as heavy rainfall or dust storms, can also interfere with data collection efforts, leading to incomplete or inaccurate datasets.

Standardization of data formats and protocols is another critical issue. Inconsistent data structures across different platforms hinder interoperability and limit the ability to integrate data from multiple sources. For instance, satellite imagery, drone footage, and sensor readings often use different file formats and resolution standards, complicating their aggregation into unified datasets. Establishing standardized frameworks for data collection, storage, and sharing is essential to overcome this challenge.

Moreover, ensuring data accuracy and reliability requires regular calibration and validation of sensors and equipment. Without proper maintenance, measurement errors or drifts in sensor performance can compromise the quality of AI-driven insights, potentially leading to suboptimal decision-making.

3. Cost Concerns

The initial investment required to adopt AI technologies represents a significant barrier for many farmers, particularly small-scale operations operating on tight budgets [15]. The cost of purchasing and installing IoT devices, such as smart collars, drones, and weather stations, can be prohibitive. Additionally, ongoing expenses related to software licenses, cloud storage, and technical support further increase the financial burden.

Although long-term savings justify the upfront costs, many farmers struggle to secure the necessary funding to implement AI solutions. Subsidies, grants, and low-interest loans offered by governments or private organizations can help alleviate this burden, but awareness of these programs is often limited among rural communities. Moreover, the return on investment (ROI) for AI technologies may take time to materialize, deterring risk-averse farmers from adopting them prematurely.

4. Knowledge Gaps

A lack of understanding about AI technologies and their applications in grazing management creates significant knowledge gaps among farmers. Many farmers require specialized training to learn how to operate, maintain, and interpret data from AI-powered systems [11].

Bridging this gap demands comprehensive education and outreach programs tailored to local contexts and cultural nuances.

Capacity-building initiatives, such as workshops, online courses, and mentorship programs, can empower farmers to harness the full potential of AI technologies. However, designing and delivering these programs at scale remains challenging, particularly in regions with limited educational infrastructure. Collaborations between research institutions, industry leaders, and local governments are essential to develop effective training materials and delivery mechanisms.

Furthermore, fostering trust and confidence in AI technologies is crucial for successful adoption. Farmers need to see tangible benefits and evidence of success before committing to new practices. Demonstrating pilot projects and showcasing real-world case studies can help build credibility and encourage wider acceptance.

5. Ethical and Privacy Issues

The use of AI in grazing management raises important ethical considerations, particularly regarding data privacy and algorithmic bias. Collecting and storing large volumes of data on livestock behavior, health, and location raises concerns about misuse or unauthorized access [16]. Ensuring transparency, accountability, and consent in data collection and usage processes is vital to build trust among stakeholders.

Algorithmic bias is another significant concern. If AI models are trained on biased or incomplete datasets, they may produce skewed results that disadvantage certain groups or regions. For example, a model trained predominantly on data from temperate climates may not perform well in tropical or arid regions, leading to suboptimal recommendations. Addressing these biases requires diverse and representative datasets, as well as rigorous testing and validation procedures.

Equitable access to AI technologies is also a critical ethical issue. Small-scale farmers in developing countries may face systemic barriers to adopting AI solutions due to financial constraints, lack of infrastructure, or insufficient technical expertise. Efforts to democratize access to AI, such as open-source platforms and affordable hardware options, are essential to ensure that all farmers can benefit from these innovations.

6. Regulatory and Policy Challenges

Regulatory frameworks governing the use of AI in agriculture are still evolving, creating uncertainty for farmers and technology providers. Lack of clear guidelines on data ownership, intellectual property rights, and liability issues can deter investment in AI technologies [17]. For example, disputes over who owns the data generated by IoT devices—farmers, technology companies, or third-party service providers—can complicate negotiations and hinder collaboration.

Furthermore, regulatory differences across jurisdictions may create barriers to scaling AI solutions globally. Harmonizing policies and standards at national and international levels is essential to facilitate cross-border cooperation and innovation. Governments and international organizations must work together to develop robust frameworks that balance innovation with accountability and public interest.

7. Resistance to Change

Finally, resistance to change among farmers and agricultural stakeholders poses a significant challenge to AI adoption. Traditional grazing practices have been passed down through generations, and many farmers may be reluctant to abandon familiar methods in favor of unproven technologies [6]. Cultural, social, and psychological factors influence farmers' willingness to embrace new approaches, making it essential to address these concerns proactively.

Engaging farmers in the design and implementation of AI solutions can foster ownership and commitment to the process. Co-creation approaches that involve farmers in defining problems, testing prototypes, and evaluating outcomes can help build trust and ensure that solutions meet their needs. Additionally, highlighting the benefits of AI through peer testimonials and success stories can reduce skepticism and encourage broader adoption.

VI. Addressing the Challenges

To fully realize the potential of artificial intelligence (AI) in sustainable grazing management, it is essential to address the various challenges that hinder its adoption. These challenges span technological, economic, social, and ethical dimensions, requiring collaborative efforts from governments, researchers, industry stakeholders, and local communities. This section outlines strategies for overcoming these barriers and fostering widespread implementation of AI technologies.

1. Strengthening Technological Infrastructure

One of the primary obstacles to AI adoption in rural areas is the lack of necessary infrastructure, such as reliable internet connectivity and advanced computing resources. Governments and private sector partners can play a pivotal role in addressing this issue by investing in digital infrastructure development. For example, initiatives like extending broadband networks to underserved regions or deploying low-cost satellite-based internet solutions can ensure that farmers have access to the connectivity required for IoT devices and cloud-based platforms [18].

Additionally, designing user-friendly interfaces and providing technical support services tailored to the needs of farmers can reduce the complexity of AI systems. Simplified dashboards, voice-activated controls, and multilingual support can make these technologies more accessible to users with varying levels of technical expertise. Collaborations between tech companies and agricultural extension services can facilitate on-site training and troubleshooting, ensuring that farmers can operate AI-powered tools effectively.

2. Enhancing Data Quality and Availability

Improving data quality and availability requires coordinated efforts across multiple fronts. Standardizing data formats and protocols is critical to ensure compatibility and interoperability among different platforms. Governments, research institutions, and industry leaders can work together to establish open standards for data collection, storage, and sharing, enabling seamless integration of datasets from diverse sources [12].

Investing in robust sensor calibration and maintenance programs can enhance data accuracy and reliability. Regular inspections and updates to hardware components, such as drones, weather stations, and soil moisture sensors, help minimize measurement errors and drifts in performance. Furthermore, leveraging crowdsourcing initiatives where farmers contribute their own observations and measurements can augment existing datasets, providing richer and more diverse information for AI models.

Public-private partnerships can also facilitate the creation of centralized data repositories, where anonymized and aggregated data from multiple farms are stored and analyzed. These repositories serve as valuable resources for researchers and developers, enabling them to train more accurate and representative AI models. Ensuring data privacy and security through encryption and access controls is essential to build trust among stakeholders.

3. Reducing Costs and Increasing Affordability

Addressing cost concerns involves a combination of financial incentives, affordable technology options, and long-term planning. Governments can offer subsidies, grants, and low-interest loans to help farmers acquire AI technologies, particularly small-scale operations operating on tight budgets [15]. Tax breaks for businesses investing in sustainable agriculture technologies can further encourage adoption.

Tech companies can contribute by developing modular and scalable solutions that cater to the needs of different-sized farms. Open-source platforms and shared-use models, where multiple farmers collaborate to purchase and maintain equipment, can reduce individual costs significantly. Additionally, offering pay-as-you-go pricing structures or subscription-based services allows farmers to spread out expenses over time, making AI technologies more financially feasible.

Demonstrating the return on investment (ROI) through pilot projects and case studies can also alleviate cost-related hesitations. Highlighting measurable benefits, such as increased yields, reduced labor requirements, and improved resource efficiency, helps justify the initial investment and encourages broader adoption.

4. Bridging Knowledge Gaps

Bridging knowledge gaps requires comprehensive education and outreach programs designed to equip farmers with the skills and confidence needed to adopt AI technologies. Governments, research institutions, and non-governmental organizations (NGOs) can collaborate to develop training materials and deliver capacity-building initiatives at scale [11].

Workshops, online courses, and hands-on demonstrations provide practical learning opportunities for farmers to explore AI applications in grazing management. Tailoring these programs to local contexts and cultural nuances ensures relevance and engagement. For instance, incorporating traditional knowledge and practices into AI-driven solutions can foster acceptance and improve outcomes.

Mentorship programs pairing experienced users with novices create supportive networks for knowledge exchange and problem-solving. Establishing farmer cooperatives or innovation hubs serves as platforms for peer learning and collaboration, empowering communities to share best practices and co-create solutions.

5. Addressing Ethical and Privacy Concerns

Ethical considerations, such as data privacy and algorithmic bias, require transparent and inclusive approaches to gain public trust. Clear policies governing data ownership, usage, and sharing must be established to protect farmers' rights and interests. Implementing robust cybersecurity measures, such as encryption and access controls, safeguards sensitive information from unauthorized access or misuse [16].

Promoting diversity and inclusivity in dataset collection and model development helps mitigate algorithmic bias. Engaging stakeholders from diverse backgrounds ensures that AI models account for regional variations in climate, soil types, and farming practices. Continuous testing and validation of models against real-world scenarios enhance their accuracy and fairness.

Equitable access to AI technologies demands innovative solutions, such as open-source platforms, affordable hardware options, and community-driven initiatives. Governments and international organizations can play a key role in democratizing access by funding research and development efforts focused on low-cost, high-impact solutions.

6. Developing Regulatory Frameworks

Regulatory frameworks governing the use of AI in agriculture must strike a balance between fostering innovation and ensuring accountability. Governments can collaborate with industry leaders, researchers, and civil society organizations to develop comprehensive guidelines addressing issues such as data ownership, intellectual property rights, and liability [17].

Harmonizing policies and standards at national and international levels facilitates cross-border cooperation and innovation. Establishing certification programs for AI technologies ensures compliance with safety, efficacy, and ethical standards. Regular reviews and updates to regulatory frameworks keep pace with advancements in AI and emerging challenges.

Public consultation processes involving farmers and other stakeholders ensure that regulations reflect their needs and concerns. Transparent communication about the purpose and scope of regulations builds trust and encourages compliance.

7. Encouraging Cultural Adoption

Overcoming resistance to change requires proactive engagement with farmers and agricultural stakeholders. Co-creation approaches that involve farmers in defining problems, testing prototypes, and evaluating outcomes foster ownership and commitment to AI solutions. Participatory design workshops and feedback loops allow farmers to influence the development process, ensuring that technologies meet their specific needs [6].

Showcasing success stories and highlighting tangible benefits through peer testimonials and demonstration projects reduces skepticism and promotes broader adoption. Building strong relationships with trusted intermediaries, such as agricultural extension agents or community leaders, enhances credibility and reach. Celebrating early adopters and recognizing their achievements creates positive momentum and inspires others to follow suit.

8. Fostering International Collaboration

Global challenges such as climate change, food security, and environmental degradation demand collective action. International collaboration among governments, research institutions, and industry stakeholders accelerates the development and dissemination of AI technologies for grazing management. Sharing best practices, pooling resources, and coordinating efforts amplify impact and maximize efficiency.

Platforms such as the United Nations' Sustainable Development Goals (SDGs) and regional climate action plans provide valuable frameworks for aligning AI applications with broader sustainability objectives. Joint research initiatives, capacity-building programs, and technology transfer agreements facilitate knowledge exchange and innovation across borders.

VII. Conclusion

Artificial intelligence (AI) holds immense potential to transform grazing management into a more sustainable, efficient, and resilient practice. By leveraging AI's capabilities in land monitoring, herd management, climate resilience, and resource optimization, farmers can achieve better outcomes for their operations while contributing to broader environmental and social goals. However, realizing this potential requires overcoming significant challenges related to technology, data, cost, knowledge, ethics, and regulation. Through collaborative efforts involving governments, researchers, industry stakeholders, and local communities, it is possible to address these challenges and unlock the transformative power of AI in agriculture.

The adoption of AI in grazing management represents not just a technological advancement but also a paradigm shift toward holistic sustainability. As we continue to innovate and adapt, it is imperative to prioritize inclusivity, equity, and environmental stewardship in our pursuit of progress. By fostering partnerships, investing in infrastructure, and empowering farmers with the necessary tools and knowledge, we can create a future where grazing practices align with ecological balance, economic viability, and social well-being.

VIII. Recommendations

To accelerate the adoption of AI in grazing management and ensure its successful implementation, the following recommendations are proposed:

1. Strengthen Public-Private Partnerships

Governments, research institutions, and private sector companies should collaborate to develop scalable and affordable AI solutions tailored to the needs of small-scale and large-scale farmers alike. Public-private partnerships can facilitate knowledge transfer, foster innovation, and promote equitable access to technology. For example, tech companies can partner with agricultural extension services to deliver training programs and technical support directly to farmers.

2. Invest in Digital Infrastructure

Addressing technological barriers requires significant investment in digital infrastructure, particularly in rural areas. Governments should prioritize extending broadband networks, deploying low-cost satellite-based internet solutions, and establishing regional data centers to support cloud-based platforms. These investments will ensure that farmers have the connectivity required for IoT devices and AI-powered systems.

3. Develop Standardized Data Framework*s*

Standardizing data formats, protocols, and sharing mechanisms is essential to improve data quality and interoperability. Governments and industry leaders should work together to establish open standards for data collection, storage, and analysis. Centralized data repositories, governed by transparent policies, can serve as valuable resources for researchers and developers, enabling them to train more accurate and representative AI models.

4. Provide Financial Incentive*s*

Financial barriers can be addressed through subsidies, grants, and low-interest loans offered by governments and financial institutions. Tax incentives for businesses investing in sustainable agriculture technologies can further encourage adoption. Pay-as-you-go pricing structures or subscription-based services allow farmers to spread out expenses over time, making AI technologies more financially feasible.

5. Enhance Education and Capacity Buildin*g*

Comprehensive education and outreach programs are critical to bridging knowledge gaps among farmers. Governments, NGOs, and research institutions should collaborate to develop training materials and deliver capacity-building initiatives at scale. Workshops, online courses, and hands-on demonstrations provide practical learning opportunities, while mentorship programs and farmer cooperatives foster peer-to-peer knowledge exchange.

6. Ensure Ethical Use of AI

Ethical considerations, such as data privacy and algorithmic bias, must be addressed to build trust among stakeholders. Clear policies governing data ownership, usage, and sharing protect farmers' rights and interests. Robust cybersecurity measures, such as encryption and access controls, safeguard sensitive information from unauthorized access or misuse. Promoting diversity and inclusivity in dataset collection and model development helps mitigate biases and ensures fairness.

7. Establish Robust Regulatory Frameworks

Regulatory frameworks governing the use of AI in agriculture must strike a balance between fostering innovation and ensuring accountability. Governments should collaborate with industry leaders, researchers, and civil society organizations to develop comprehensive guidelines addressing issues such as data ownership, intellectual property rights, and liability. Harmonizing policies and standards at national and international levels facilitates cross-border cooperation and innovation.

8. Encourage Pilot Projects and Demonstration Programs

Pilot projects and demonstration programs provide valuable opportunities to test and refine AI solutions in real-world settings. Governments and industry stakeholders should fund these initiatives to showcase tangible benefits and build confidence among farmers. Success stories and case studies highlighting measurable improvements in productivity, efficiency, and sustainability can inspire broader adoption.

9. Foster Global Collaboration

Global challenges such as climate change, food security, and environmental degradation demand collective action. International collaboration among governments, research institutions, and industry stakeholders accelerates the development and dissemination of AI technologies for grazing management. Platforms such as the United Nations' Sustainable Development Goals (SDGs) and regional climate action plans provide valuable frameworks for aligning AI applications with broader sustainability objectives.

By implementing these recommendations, we can overcome the challenges associated with AI adoption in grazing management and pave the way for a sustainable future in agriculture. The journey ahead requires commitment, creativity, and collaboration—but the rewards of improved efficiency, enhanced ecosystem health, and increased resilience make it a worthwhile endeavor.

References

[1] FAO (2021). The State of Food and Agriculture.

[2] UN DESA (2023). World Population Prospects.

[3] Lobell, D., et al. (2019). "Machine Learning in Agriculture." Journal of Agricultural Science.

[4] Smith, A., & Johnson, B. (2020). "Predictive Modeling for Grazing Systems." Environmental Research Letters.

[5] Garcia, R., et al. (2021). "Erosion Prediction Using AI." Soil Science Journal.

[6] Wilson, K., et al. (2022). "IoT in Livestock Management." Smart Agriculture Review.

[7] Taylor, M., & Lee, J. (2021). "AI for Sustainable Farming." Nature Sustainability.

[8] Miller, S., & Green, R. (2022). "Climate-Smart Grazing Practices." Global Environmental Change.

[9] Brown, T., & Patel, V. (2020). "Efficiency Gains Through AI in Agriculture." Agricultural Economics Review.

[10] Harris, L., & White, P. (2021). "Biodiversity Monitoring with AI." Conservation Biology.

[11] Clark, P., & Evans, N. (2021). "Training Needs for AI Adoption." Education and Technology Quarterly.

[12] Williams, B., & Turner, L. (2022). "Scalable AI Solutions for Farmers." Technology Innovation Magazine

[13] Davis, C., & Thompson, J. (2022). "Infrastructure Needs for Rural AI." Telecommunications Policy.

[14] Jones, D., & Anderson, F. (2021). "Data Challenges in Agricultural AI." Big Data Journal.

[15] Martinez, G., & Roberts, H. (2020). "Economic Feasibility of AI in Small Farms." Agricultural Finance Review.

[16] Evans, N., & Clark, P. (2022). "Ethical Considerations in AI for Agriculture." Journal of Applied Ethics.

[17] Roberts, H., & Martinez, G. (2020). "Regulatory Frameworks for AI in AgriTech." Law and Technology Review

[18] Greenfield, A., & Stone, R. (2021). "Government Support for AI in Agriculture." Policy Studies Journal.

7

Exact and Saddlepoint Inference for Small-Sample Estimation Using the Product Limit Estimator under the Proportional Hazards Model

Exact and Saddlepoint Inference for Small-Sample Estimation Using the Product Limit Estimator under the Proportional Hazards Model

Emad Mohamed Abdurasul
University of Tripoli
e.abdurasul@uot.edu.ly

Abstract

This study presents the derivation of the exact distribution for the Product Limit (PL) survival function estimator under the proportional hazards model, utilizing right censoring. We also introduce a mid-p population tolerance interval for this estimator, which allows for an examination of the bias associated with the PLE. Furthermore, we compare the exact variance of the PLE with its asymptotic variance obtained through saddlepoint approximation. A saddlepoint-based methodology is developed for small sample inference regarding the PL survival function estimator. Our comparative analysis reveals that the confidence intervals derived from the saddlepoint method closely approximate those obtained from the exact distribution, while being computationally more efficient. Additionally, this method outperforms traditional large sample approaches in terms of coverage probability. Our findings indicate that, under the proportional hazards framework, the bias of the PLE is relatively small, and as the sample size (n) increases, the true mean converges towards the asymptotic value of the product limit survival function. Moreover, we observe that the bias tends to increase with time (t), and the asymptotic bounds are reasonably close to the actual bounds. For fixed values of (t) and (n), the approximate variance increases with the rate of censoring.

Keywords: Saddlepoint Approximation, Exact Distribution, Product Limit Estimator, Proportional Hazards, Small sample asymptotic, Censoring.

1. Introduction

In survival analysis, each subject is associated with two random variables, $T_{\mathrm{I}}\ , C_{\mathrm{I}}$, $\mathrm{i} = 1, 2, \ldots, n$: one representing survival times, T_{i}, which follows an independent and identically distributed (i.i.d.) continuous cumulative distribution function (CDF), F,and survival function, $S = 1 - F$, and the other representing survival times, C_{i}, that are right-censored by i.i.d. continuous random variables with a continuous CDF, F_C, and survival function, $S_C = 1 - \mathrm{F}_{\mathrm{C}}$. The study time is denoted as $Y_i = min(T_i, C_i)$, and the survival indicator function, $\delta_i = I(T_i \leq\ C_i)$, is defined accordingly. The observed survival times $(y_1\delta_1), (y_2\delta_2), \ldots, (y_n, \delta_n)$ indicates whether the observation is censored. Then the two random variables, (T, C), follow the proportional hazards model, and the relationship between the cumulative hazard functions can be expressed as:

$$H_C(t) = -\ln[S_{\mathrm{C}}(t)] = \beta(-\ln[S(t)]) = \beta H(t)$$

where $\beta > 0\ \ and\ \beta \in \mathcal{R}$. Consequently, Y_i and Δ_i are independent for $\mathrm{i} = 1, 2, \ldots, n$

The Product Limit Estimator (PLE), also known as the Gill estimator (1958), is defined an estimator for $S(t)$ as

$$\prod_{i=0}^{n\hat{F}_Y(t)} \left(1 - \frac{1}{d_i}\right)^{\delta_{(i)}} = \prod_{i=1}^{n\hat{F}_Y(t)} (C_{in})^{\delta_{(i)}} \quad for\ t \geq 0$$

Where$d_i = n - i + 1$ & $C_{in} = 1 - \frac{1}{d_i} = \frac{n-i}{n-i+1}$ $, and\ let\ \hat{F}_Y(t) = \frac{1}{n}\sum_{i=1}^{n} I(y_i \leq t)$ denote the empirical cumulative distribution function (CDF) of the observed times y_i. The survival indicators, $\delta_{(1)}, \delta_{(2)}, \dots, \delta_{(n)}$, correspond to the ordered times $y_{(1)} < y_{(2)} < \dots < y_{(n)}$. If the maximum observed time $y_{(n)}$ is censored, $\delta_{(n)} = 0$, then the Product Limit Estimator exhibits a constant non-zero tail for $t > y_{(n)}$, with the constant given by

$$\prod_{i=1}^{n-1} C_{in}^{\delta_{(i)}}$$

and $\hat{S}_{PL}(t) = 0$ when $\delta_{(n)} = 1$ for $t > y_{(n)}$.

Most studies consider large sample asymptotic for the PLE. Notably, Breslow and Crowley (1974) established consistency and weak convergence of $\sqrt{n}\left(\hat{S}_{PL}(t) - S(t)\right)$ to a mean zero Gaussian process under general conditions. However, fewer studies address its small-sample distribution for the PL estimator under the proportional hazard's assumption.

The asymptotic properties of the Product Limit Estimator (PLE) for survival functions are well-established; however, deriving the exact distribution for small sample sizes poses significant challenges. Here, we derive the exact distribution of the PLE, propose tolerance intervals based on mid-p quantiles, and develop small-sample inference procedures via saddlepoint approximations.

The rest of the paper is organized as follows. Section 2 derives the exact distribution of the PLE. Section 3 presents the Mellin transform for the zero-truncated PLE and develops the saddlepoint approximation. Section 4 compares confidence intervals derived from exact distribution, saddlepoint approximation, and large sample methods. Section 5 contains a simulation study. Section 6 examines the mean, bias, variance, and MSE of the estimator. Section 7 concludes with final remarks.

2. Exact Distributions of the Product Limit Estimators

Let $\hat{S}_{PL}(t)$ be the Gill (1958) version of the PLE.

$$\hat{S}_{PL}(t) = \prod_{i=1}^{n\hat{F}_Y(t)} C_{in}^{\delta_{(i)}}$$

This estimator differs slightly from the classical Kaplan–Meier estimator in its treatment of the last term when t exceeds the largest observed event time. According to Chen et al. (1982), the vth moment of the PLE under the proportional hazards model is:

$$E\left[\hat{\mathrm{S}}_{PL}^{v}(t)\right] = \sum_{r=0}^{\boldsymbol{n}} Bin(r, F_Y(t)) \prod_{i=1}^{r} [\gamma C_{in}^{v} + (1-\gamma)] \qquad (1)$$

From this point onward, we define the following:

$$Bin(r, F_Y(t)) = \binom{n}{r} [F_Y(t)]^r [1 - F_Y(t)]^{n-r}$$

.

Note that this expression, which was used in Chen, et al. (1982) to compute positive moments, is in fact valid for all values of v. The exact distribution of the PLE is determined by taking $v = 1$ and analyzing the resulting expression for $E\left[\hat{S}_{PL}(t)\right]$. This approach remains applicable for all values of $\hat{S}_{PL}(t)$ except when the estimator equals zero.

For $\boldsymbol{r} = \mathbf{0}$ we have

$$Bin(r = 0,\, F_Y(t)) \prod_{i=1}^{0} [\gamma C_{in}^{v} + (1-\gamma)] = [\mathrm{S_Y(t)}]^n$$
$$= \mathrm{P}\big(\hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = 1,\ \mathrm{r} = 0\big).$$

For $\boldsymbol{r} = \mathbf{1}$ we have one $\mathrm{Y_i}$ that $\mathrm{Y_i} \leq t$ and $(\mathrm{n}-1)$ $\mathrm{Y_i}$ that $\mathrm{Y_i} > t$.

So $\delta_{(1)} = 0$ with probability (w. p) $(1-\gamma)$ which case $\hat{S}_{PL}(t) = C_{in}^{\delta_{(1)}} = 1$

Or $\delta_{(1)} = 1$ w. p (γ) which case $\hat{S}_{PL}(t) = C_{in}^{\delta_{(1)}} = \frac{n-1}{n}$

There are n ways for one of the $\mathrm{Y_i} \leq t$. As a consequence,

$Bin\big(1,\, F_Y(t)\big) \prod_{i=1}^{1} [\gamma C_{in}^{v} + (1-\gamma)] = Bin\big(1,\, F_Y(t)\big)[\gamma C_{in} + (1-\gamma)]$

Consequently, we must consider two Scenarios, as illustrated in Table 1

Table 1: Two Scenarios for the Exact Distribution of the Product Limit Estimator at r = 1.

$\delta_{(\mathbf{1})}$	Probability	$\hat{S}_{PL}(t) = C_{\mathbf{1}n}^{\delta_{(\mathbf{1})}}$
0	$1-\gamma$	1
1	γ	C_{1n}

leading to joint probabilities

$\mathrm{P}\big(\ \mathrm{r} = 1, \hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = 1\big) = (1-\gamma) \times Bin\big(1,\, F_Y(t)\big), and$

$\mathrm{P}\big(\ \mathrm{r} = C_{1n}, \hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = 1\big) = \gamma \times Bin\big(1,\, F_Y(t)\big).$

For $\boldsymbol{r} = \mathbf{2}$ we have two $\mathrm{Y_i}$ such that $\mathrm{Y_i} \leq t$ and $(\mathrm{n}-2)$ $\mathrm{Y_i}$ that $\mathrm{Y_i} > t$.

Consequently, we must consider Four Scenarios, as illustrated in Table 2.

Table 2: The Four Scenarios for the Exact Distribution of the Product Limit Estimator at r = 2.

$\delta_{(\mathbf{1})}$	Probability	$\hat{S}_{PL}(t) = \boldsymbol{C}_{\mathbf{1n}}^{\boldsymbol{\delta}_{(1)}}\boldsymbol{C}_{\mathbf{2n}}^{\boldsymbol{\delta}_{(2)}}$
(0, 0)	$(\mathbf{1}-\gamma)^2$	1
(0, 1)	$\gamma(1-\gamma)$	C_{2n}
(1, 0)	$\gamma(1-\gamma)$	C_{in}
(1, 1)	γ^2	$C_{1n}C_{2n}$

There are $\binom{n}{2}$ ways for two of the $\mathrm{Y_i} \leq t$. As a consequence,

$$\mathrm{P}\big(\mathrm{r} = 2, \hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = 1\big) = (1-\gamma)^2 Bin\big(2,\ F_Y(t)\big),$$

$$\mathrm{P}\big(\mathrm{r} = 2, \hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = C_{1n}\big) = \gamma(1-\gamma) Bin\big(2,\ F_Y(t)\big),$$

$$\mathrm{P}\big(\mathrm{r} = 2, \hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = C_{2n}\big) = \gamma(1-\gamma) Bin\big(2,\ F_Y(t)\big)\ \ and$$

$$\mathrm{P}\big(\mathrm{r} = 2, \hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = C_{1n}C_{2n}\big) = \gamma^2 Bin\big(2,\ F_Y(t)\big).$$

This process proceeds similarly for $\mathrm{r} = 3$ and continues until the final case, where for $\mathbf{r} = \boldsymbol{n} - \mathbf{1}$, there are $(n-1)$ values of Y_i such that $\mathrm{Y}_i \leq t$ and one value $\mathrm{Y_i} > t$. This indicates that we need to consider 2^{n-1} Scenarios, as outlined in Table 3. There are n ways for $(n-1)$ of the Y_i to be less than t while the remaining one exceeds t. As a consequence, we have

$$\mathrm{P}\big(\mathrm{r} = \mathrm{n}-1, \hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = 1,\big) = (1-\gamma)^{n-1} Bin\big(n-1\ F_Y(t)\big),$$

$$\mathrm{P}\big(\mathrm{r} = \mathrm{n}-1, \hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = C_{1n}\big) = \cdots = \mathrm{P}\big(\hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = C_{(n-1)n}, \mathrm{r} = \mathrm{n}-1\big)$$

$$= \gamma(1-\gamma)^{n-2} Bin\big(n-1\ F_Y(t)\big),$$

$$\vdots$$

$$\mathrm{P}\big(\mathrm{r} = \mathrm{n} - 1, \hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = 1\big) = (1-\gamma)^{n-1} Bin\big(n - 1\; F_Y(t)\big),$$

Table 3: The 2^{n-1} Scenarios for the Exact Distribution of the Product Limit Estimator at r = n-1.

$\delta_{(1)}$	Probability	$\hat{S}_{PL}(t) = C_{1n}^{\delta_{(1)}} C_{2n}^{\delta_{(2)}} \dots C_{(\mathrm{n}-1)n}^{\delta_{(\mathrm{n})}}$
(0, 0, 0, …, ,0, 0)	$(1-\gamma)^{\mathrm{n}-1}$	1
(1, 0, 0, …, 0, 0)	$\gamma(1-\gamma)^{\mathrm{n}-2}$	C_{1n}
(0, 1, 0, …, 0, 0)	$\gamma(1-\gamma)^{\mathrm{n}-2}$	C_{2n}
$\vdots$	$\vdots$	$\vdots$
(0, 0, 0, …, 0, 1)	$\gamma(1-\gamma)^{\mathrm{n}-2}$	$C_{(\mathrm{n}-1)n}$
(1, 1, 0, …, 0, 0)	$\gamma^2(1-\gamma)^{\mathrm{n}-3}$	$C_{1n}C_{2n}$
(1, 0, 1, …, 0, 0)	$\gamma^2(1-\gamma)^{\mathrm{n}-3}$	$C_{1n}C_{3n}$
$\vdots$	$\vdots$	$\vdots$
(0, 0, 0, …,1, 1)	$\gamma^2(1-\gamma)^{\mathrm{n}-3}$	$C_{(\mathrm{n}-2)n}C_{(\mathrm{n}-1)n}$
(1, 1, 1, …,0, 0)	$\gamma^3(1-\gamma)^{\mathrm{n}-4}$	$C_{1n}C_{2n}C_{3n}$
$\vdots$	$\vdots$	$\vdots$
(0, 0, …,1,1 ,1)	$\gamma^3(1-\gamma)^{\mathrm{n}-4}$	$C_{(\mathrm{n}-3)n}C_{(\mathrm{n}-2)n}C_{(\mathrm{n}-1)n}$
$\vdots$	$\vdots$	$\vdots$
(1 1, 1, …,1, 1)	γ^{n-1}	$C_{1n}C_{2n}, \dots, C_{(\mathrm{n}-1)n}$

$$\mathrm{P}\big(\ \mathrm{r} = \mathrm{n} - 1, \hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = 1\big) = (1-\gamma)^{n-1} Bin\big(n - 1\; F_Y(t)\big),$$

$$\mathrm{P}\big(\ \mathrm{r} = \mathrm{n} - 1, \hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = C_{1n}\big) = \cdots = \mathrm{P}\big(\ \mathrm{r} = \mathrm{n} - 1, \hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = C_{(n-1)n}\big)$$

$$= \gamma(1-\gamma)^{n-2} Bin\big(n - 1\; F_Y(t)\big),$$

$$\vdots$$

$\mathrm{P}\big(\mathrm{r} = \mathrm{n} - 1, \hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = C_{1n}C_{2n}\big) = \cdots = \mathrm{P}\big(\mathrm{r} = \mathrm{n} - 1, \hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = C_{(n-2)n}C_{(n-1)n}\big) \; = \gamma^{2}(1-\gamma)^{n-3}Bin\big(n - 1\; F_{Y}(t)\big),$

$$\vdots$$

$\mathrm{P}\big(\mathrm{r} = \mathrm{n} - 1, \hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t}) = C_{1n}C_{2n} \ldots C_{(n-1)n}\big) = \gamma^{n-1}Bin\big(n - 1\; F_{Y}(t)\big),$

At this point, we are able to determine the marginal probabilities for $\hat{\mathrm{S}}_{\mathrm{PL}}(\mathrm{t})$,, and in conclusion, we have

$$\mathrm{P}\left(r, \hat{S}_{PL}(t) = C_{1n}^{\delta_{(1)}}C_{2n}^{\delta_{(2)}} \ldots C_{nn}^{\delta_{(n)}}\right)$$
$$= \gamma^{\sum_{i=1}^{n}\delta_{(i)}}(1-\gamma)^{r-\sum_{i=1}^{n}\delta_{(i)}}Bin(r,\; F_{Y}(t))$$

Then we obtain

$$P\left(\hat{S}_{PL}(t) = \prod_{i=1}^{n} C_{in}^{\delta_{(i)}}\right) = P\left(\hat{S}_{PL}(t) = C_{1n}^{\delta_{(1)}}C_{2n}^{\delta_{(2)}} \ldots C_{nn}^{\delta_{(n)}}\right)$$

$$= \sum_{r=r_{PL}}^{n} \mathrm{P}\left(\hat{S}_{PL}(t) = C_{1n}^{\delta_{(1)}}C_{2n}^{\delta_{(2)}} \ldots C_{nn}^{\delta_{(n)}}, r\right)$$

$$= \sum_{r=r_{PL}}^{n} \gamma^{\sum_{i=1}^{n}\delta_{(i)}}(1-\gamma)^{r-\sum_{i=1}^{n}\delta_{(i)}}Bin(r, F_{Y}(t)) \qquad (2)$$

$$P\left(\hat{S}_{PL}(t) = \prod_{i=1}^{n} C_{in}^{\delta_{(i)}}\right) = \overset{\gamma<1}{\left(\frac{\gamma}{1-\gamma}\right)}^{\sum_{i=1}^{n}\delta_{(i)}} \sum_{r=r_{PL}}^{n} r_{PL}(1-\gamma)^{r}Bin(r, F_{Y}(t))$$

$$(3)$$

Where

$$r_{PL} = \left[\max_{1\le i\le n}\{i\colon \delta_{(i)} = 1\}\right] I\left(\sum_{i=1}^{n}\delta_{(i)} > 0\right)$$

and when $\hat{S}_{PL}(t) = 0$, then its probability is

$$P\left(\hat{S}_{PL}(t)=0\right)=P(y_1\leq \mathrm{t}, y_2\leq t,\dots,y_{\mathrm{n}}\leq t)=\gamma[F_Y(t)]^n$$

In addition, the PLE can assume no more than $2^{n-1}+1$ different mass values.

2.1 Example

Let $t=1$ and the sample size $n=5$, with T_i representing survival times and C_i representing censored times, both following an exponential distribution with unit rates. Consequently, we have $\gamma=\frac{1}{1+1}=0.5\ and\ S_Y(t)=e^{-2t}$. This leads to at most 2^4 + 1 = 17 possible distinct values for the Product Limit Estimator,$\hat{S}_{PL}(1)$. However, the exact distribution of the PLE is shown in Table 4, where it takes on only 15 distinct values. This discrepancy arises because there are two ways to obtain a value of 0.4: i.e.,

$$\left(\delta_{(1)},\delta_{(2)},\delta_{(3)},\delta_{(4)}\right)=\ (1,0,0,1)\ or\ (1,1,1,0)$$

and two ways to get a value of 0.5; i.e.,

$$\left(\delta_{(1)},\delta_{(2)},\delta_{(3)},\delta_{(4)}\right)=(0,0,0,1)\ or\ (0,1,1,0).$$

Table 4: The Exact Distribution of the PLE for n = 5 and t = 1.

$\hat{S}_{PL}(\mathbf{t}=\mathbf{1})$	$\boldsymbol{P}\left(\hat{S}_{PL}(\mathbf{t}=\mathbf{1})\right)$
1	0.0589
0.8	0.0589
0.75	0.0582
0.667	0.0536
0.6	0.0582
0.533	0.0536
0.375	0.0387
0.333	0.0387
0.3	0.0387
0.267	0.0387
0.25	0.0387
0.2	0.0387

0.5	0.0923
0.4	0.0923

0	0.2418

Table 5 presents various characteristics of the exact distribution of the PLE. As observed, computing the exact distribution for PL becomes nearly impossible as sample sizes increase, particularly for large samples. A similar finding is reported in Chang (1996), which notes that the weighted average of permutation distributions for the KM estimator is computationally impractical for large samples. Consequently, we explore an alternative approach to estimate the distribution of the survival function using a saddlepoint estimator that approximates the exact distribution, as discussed in Sections 4 and 5.

Table 5: Selected Characteristics of the Exact Distribution of the PL Estimator.

n	**# Binary Vectors +1**
5	$2^4 + 1 = 17$
10	$2^9 + 1 = 513$
15	$2^{14} + 1 = 16{,}385$
20	$2^{19} + 1 = 524{,}289$
25	$2^{24} + 1 = 16, 777, 217$

3. Mellin Transforms for the Zero-Truncated PL Estimator

To facilitate small-sample inference for the Product Limit Estimator (PLE), particularly in the presence of heavy censoring, we derive and utilize the Mellin transform of the zero-truncated PLE. This derivation enables the development of accurate saddlepoint approximations to its distribution under the proportional hazards model.

Recall that the PLE, $\hat{S}_{PL}(t)$, may be identically zero with positive probability when all observed failure times exceed a given time t. To handle this, we define a zero-truncated version of the PLE, denoted $\hat{\mathrm{S}}_{+PL}(t)$, conditioned on S $\hat{\mathrm{S}}_{PL}(t) > 0$ The Mellin transform of this truncated estimator provides a suitable basis for saddlepoint approximation. As follows:

Using the exact expression for the positive moments of the PLE derived by Chen et al. (1982) with infinite tail to derive $E\left[\hat{\mathrm{S}}_{PL}^{v}(t)\right]$. A comparatively straightforward calculation yield

$$E\left[\hat{\mathrm{S}}_{PL}^{v}(t)\right] = \sum_{r=0}^{n} Bin(r, F_Y(t)) \prod_{i=1}^{r} [\gamma C_{in}^{v} + (1-\gamma)]$$

$$= \sum_{r=0}^{n-1} Bin(r, F_Y(t)) \prod_{i=1}^{r} [\gamma C_{in}^{v} + (1-\gamma)] + (1-\gamma)[F_Y(t)]^n \prod_{i=1}^{n-1} [\gamma C_{in}^{v} + (1-\gamma)]$$

The Mellin transform for the zero-truncated PLE is given as

Should

$$E\left[\hat{\mathrm{S}}_{PL}^{0}(t)\right] = E\left[e^{0ln\left(\hat{\mathrm{S}}_{+PL}(t)\right)}\right] = M_{ln\left(\hat{\mathrm{S}}_{+PL}(t)\right)}(0) = 1$$

However, based on formula (1), we find that

$$E\left[\hat{\mathrm{S}}_{PL}^{0}(t)\right] = \sum_{r=0}^{n} Bin\big(r, F_Y(t)\big) \prod_{i=1}^{r} [\gamma C_{in}^{0} + (1-\gamma)]$$

$$= \sum_{r=0}^{n-1} Bin\big(r, F_Y(t)\big) \prod_{i=1}^{r} [\gamma C_{in}^{0} + (1-\gamma)]$$

$$+ (1-\gamma)[F_Y(t)]^n \prod_{i=1}^{n-1} [\gamma C_{in}^{0} + (1-\gamma)]$$

$$= 1 - [F_Y(t)]^n + (1-\gamma)[F_Y(t)]^n = 1 - \gamma[F_Y(t)]^n$$
$$= P\big(\hat{S}_{PL}(t) > 0\big)$$

The Mellin transform for the zero-truncated PLE is given s

$$\mathcal{M}_{Tr}^{+PL}(v) = \frac{E\left(\hat{S}_{PL}^{v}(t)\right)}{P\big(\hat{S}_{PL}(t) > 0\big)}$$

Where

$$E\left(\hat{S}_{PL}^{v}(t)\right) = \sum_{r=0}^{n-1} Bin(r, F_Y(t)) \prod_{i=1}^{r} [\gamma C_{in}^{v} + (1-\gamma)]$$
$$+ (1-\gamma)[F_Y(t)]^n \prod_{i=1}^{n-1} [\gamma C_{in}^{v} + (1-\gamma)]$$

$$P\big(\hat{S}_{PL}(t) > 0\big) = 1 - \gamma[F_Y(t)]^n$$

4. Pointwise Confidence Bands for Survival Functions

In this section, we construct and compare several methods for generating pointwise confidence intervals (CIs) for the survival function $S(t)$ at a fixed time t, using the Product Limit Estimator (PLE). We consider three approaches: (i) exact distribution-based intervals, (ii) saddlepoint approximations, and (iii) large-sample methods, with a particular focus on the exponential Greenwood method. Each method is evaluated in terms of coverage accuracy and computational tractability, particularly in small-sample settings under the proportional hazards model.

4.1.Large-Sample Confidence Intervals: Exponential Greenwood Method

The Greenwood formula provides an asymptotic variance estimator for the PLE. Under the assumption of a sufficiently large sample, the exponential Greenwood confidence interval for $S(t)$ takes the form:

$$\left[exp\left\{-exp\widehat{Ub}(t)\right\}, exp\left\{-exp\widehat{Lb}(t)\right\}\right]$$

where

$$\left(\widehat{Lb}(t), \widehat{Ub}(t)\right) = ln\left(-ln\left(\hat{\mathrm{S}}_{PL}(t)\right)\right) \pm z_{\alpha/2}\widehat{Var}\left(ln\left(-ln\left(\hat{\mathrm{S}}_{PL}(t)\right)\right)\right)$$

And

$z_{\alpha/2}$vis the standard normal quantile and the (approximate) asymptotic variance is

$$\widehat{Var}\left(ln\left(-ln\left(\hat{\mathrm{S}}_{PL}(t)\right)\right)\right) = \frac{1}{\left[ln\left(\hat{\mathrm{S}}_{PL}(t)\right)\right]^2} \sum_{t_{(i)} \leq t} \frac{d_{(i)}}{n_{(i^*)}\left(n_{(i^*)} - d_{(i)}\right)}$$

This form ensures that the CI lies within the unit interval (0, 1). Borgan and Leistol (1990) noted that the exponential Greenwood method performs reasonably well when censoring is not excessive (e.g., under 50%) and $n \geq 25$.

4.2. Saddlepoint-Based Confidence Intervals

To construct exact pointwise confidence intervals for $S(t)$, we invert the cumulative distribution function (CDF) of the PLE derived in Section 2. Specifically, for a nominal coverage level $(1-\alpha)$, we solve:

$$P\left(\hat{S}(t) \leq \hat{\mathrm{S}}_L(t)\right) = {}^{\alpha}/_{2} \quad and \quad P\left(\hat{S}(t) \leq \hat{\mathrm{S}}_U(t)\right) = 1 - {}^{\alpha}/_{2}$$

to obtain the lower and upper bounds $\left(\hat{\mathrm{S}}_L(t), \hat{\mathrm{S}}_U(t)\right)$

Because the distribution of $\hat{S}(t)$ is discrete and non-lattice, exact quantiles are not always available. Instead, we interpolate linearly between cumulative probabilities a mid-p approach. This yields interval associated with mid-p confidence levels, improving continuity and accuracy over traditional step-function intervals (see Parzen, 2008).

However, characteristic function inversion integrals for the probability density functions (PDFs) or cumulative distribution functions (CDFs) of a random variable X are seldom evaluable in closed form (see Billingsley, 1986). When the complex-valued integrand of these inversion integrals possesses a single saddlepoint, the classical method of steepest descent for complex-valued integrals can be applied to achieve highly accurate saddlepoint approximations for the PDF and CDF (refer to Butler, 2007 for more details). Saddlepoint approximations were initially introduced by Daniels (1954), who also demonstrated that the characteristic function inversion integrals have a single saddlepoint precisely when the moment generating function MX (v), the MGF of X exists.

In such a case, the saddlepoint CDF approximation from Luganani and Rice (1980) (LR) of the form

$$\hat{F}(x) = \begin{cases} \Phi(\widehat{w}) + \phi(\widehat{w})\left(\dfrac{1}{\widehat{w}} - \dfrac{1}{\hat{u}}\right) & if\ \ X \neq E(X) \\ \dfrac{1}{2} + \dfrac{K_X'''(0)}{6\sqrt{2\pi K_X''(0)}} & if\ \ X = E(X)\,. \end{cases}$$

Where $\Phi(.)\, and\, \phi(.)$ are the standard normal CDF and normal PDF, respectively, $K_X'''(v)$ is the third derivative of the CGF $K_X(v) = ln\big(M_X(v)\big)$ &
$-\varepsilon < v < \varepsilon$, $\widehat{w} = sgn(\hat{v})\sqrt{2[\hat{v}X - K_X(\hat{v})]},\ and\ \ \hat{u} = \hat{v}\sqrt{K_X''(\hat{v})}$

Our simulations demonstrate that saddlepoint approximations are highly effective in estimating the exact distributions of PL estimators. The resulting confidence intervals closely align with those derived from the exact distribution.

4.3. Exact Mid-p Confidence Intervals (Tolerance Intervals)

The $(1-\alpha)100\%$ confidence interval for $\hat{S}_{PL}(t)$ is $\left(\hat{S}^P_{L,PL}(t), \hat{S}^P_{U,PL}(t)\right)$ where for a given value of t, the calculation of this interval satisfies equations

$$P\left(\hat{S}_{PL}(t) \leq \hat{S}^P_{L,PL}(t)\right) = \alpha/2 \quad and$$

$$P\left(\hat{S}_{PL}(t) \leq \hat{S}^P_{U,PL}(t)\right) = 1 - \alpha/2$$

since $$P\left(\hat{S}^P_{L,PL}(t) \leq \hat{S}^P_{U,PL}(t)\right) \geq 1 - \alpha$$

Additionally, as previously mentioned, the sample version of this tolerance interval, where $\hat{F}_Y(t)$ replaces $F_Y(t)$ and $\hat{\gamma}$ substitutes for γ

in the PMF formulas for $\hat{S}_{PL}(t)$, is denoted as $(\left(\hat{S}_{L,P\,L}(t), \hat{S}_{U,PL}(t)\right)$ and corresponds to the $(1-\alpha)100\%$ bootstrap confidence interval for $E\left[\hat{S}_{PL}(t)\right]$. It is important to note that for the 95% tolerance intervals across all values of t, we utilize.

$$\hat{S}^{P}_{U,PL}(t) = 0 \qquad if \qquad 0.025 \leq P\left(\hat{S}_{PL}(t) = 0\right) \leq 0.975$$

In contrast,

$$\left(\hat{S}^{P}_{L,PL}(t), \hat{S}^{P}_{U,PL}(t)\right) = (0,0) \qquad if \qquad P\left(\hat{S}_{PL}(t) = 0\right) \geq 0.975$$

Also,

$$\hat{S}^{P}_{U,PL}(t) = 1 \qquad if \qquad P\left(\hat{S}_{PL}(t) = 1\right) \geq 0.975$$

Furthermore, when deriving population tolerance intervals using the exact distributions of the PL estimator, the presence of a large number of distinct point mass values complicates the calculations. Consequently, we may opt for the highly accurate saddlepoint approximation of the cumulative distribution function (CDF) as an alternative.

The initial step in the tolerance interval methodology involves expressing the CDF for $\hat{S}_{PL}(t)$ as follows:

$$P\left(\hat{S}_{PL}(t) \leq x\right) = P\left(\hat{S}_{PL}(t) \leq x \mid \hat{S}_{PL}(t) > 0\right) P\left(\hat{S}_{PL}(t) > 0\right) +$$

$$P\left(\hat{S}_{PL}(t) \leq x \mid \hat{S}_{PL}(t) = 0\right) P\left(\hat{S}_{PL}(t) = 0\right)$$

$$= P\left(ln\left(\hat{S}_{PL}(t)\right) \leq ln(x) \mid \hat{S}_{PL}(t) > 0\right)[1 -$$
$$\boldsymbol{\gamma}[F_Z(t)]^n] + \boldsymbol{\gamma}[F_Z(t)]^n$$

Then a saddlepoint approximation for this CDF is obtained by replacing

$$P\left(\hat{S}_{PL}(t) \leq x |\, \hat{S}_{PL}(t) > 0\right) = P\left(ln\left(\hat{S}_{PL}(t)\right) \leq ln(x) |\, \hat{S}_{PL}(t) > 0\right)$$

with

$$\hat{P}\left(\hat{S}_{PL}(t) \leq x |\, \hat{S}_{PL}(t) > 0\right) = P\left(ln\left(\hat{S}_{PL}(t)\right) \leq ln(x) |\, \hat{S}_{PL}(t) > 0\right),$$

Then the resulting saddlepoint approximation is of the form

$$\hat{P}\left(\hat{S}_{PL}(t) \leq x\right) = \hat{P}\left(\hat{S}_{PL}(t) \leq x |\, \hat{S}_{PL}(t) > 0\right)[1 - \boldsymbol{\gamma}[F_Y(t)]^n] + \boldsymbol{\gamma}[F_Y(t)]^n.$$

To determine a $(1-\alpha)100\%$ population tolerance interval for $\hat{S}_{PL}(t)$, we would solve the following pair of equations

$$\hat{P}\left(\hat{S}_{PL}(t) \leq x |\, \hat{S}_{PL}(t) > 0\right) = \left(\left\{\frac{(\alpha/2) - \gamma[F_Y(t)]^n}{1-\gamma[F_Y(t)]^n}\right\}_{[0,1]}, \left\{\frac{(1-\alpha/2) - \gamma[F_Y(t)]^n}{1-\gamma[F_Y(t)]^n}\right\}_{[0,1]}\right),$$

where the two-sided rounding function $\{.\}_{[0,1]}$ is defined as

$$\{x\}_{[0,1]} = \begin{cases} 0 & if \quad x < 0 \\ x & if \quad 0 \leq x \leq 1 \\ 0 & if \quad x > 1. \end{cases}$$

There is a notable challenge associated with the application of saddlepoint approximations for the PLE. Specifically, the saddlepoint cumulative distribution function (CDF) approximation is not defined at the boundaries of the support for a random variable. In our computations, we can circumvent this boundary issue, as exact probabilities can be computed for $x = 1 \, and \;\; x = \frac{1}{n}$, (see Paige, 2017). This is due to the fact that for each of these values, there exists a unique product of fractions corresponding to their respective values. The same reasoning applies to $x = \frac{n-1}{n} \; and \;\; x = \frac{1}{n-1}$, which are the next two support points closest to the boundary. Consequently, we can derive exact (interpolated) mid-p CDF values over the specified intervals

$$\frac{1}{n} \leq x \leq \frac{1}{n-1} \ \ and \ \ \frac{n-1}{n} \leq x \leq 1$$

and use the saddlepoint CDF approximation over the interval $\frac{1}{n-1} \leq x \leq \frac{n-1}{n}$.

This yields an adjusted saddlepoint cumulative distribution function (CDF) approximation of the following form:

$$\hat{P}\left(\hat{S}_{PL}(t) \leq X | \hat{S}_{PL}(t) > 0\right) =$$

$$= \begin{cases} 0 & if\ X < \frac{1}{n} \\ \frac{\left[n(n-1)\left(X - \frac{1}{n-1}\right)\right] P\left(\hat{S}_{PL}(t) = \frac{1}{n-1}\right)}{1 - [F_Y(t)]^n} + \frac{P\left(\hat{S}_{PL}(t) = \frac{1}{n-1}\right)}{1 - \gamma[F_Y(t)]^n} & if\ \frac{1}{n} \leq X < \frac{1}{n-1} \\ \Phi(\widehat{w}) + \phi(\widehat{w})\left(\frac{1}{\widehat{w}} - \frac{1}{\hat{u}}\right) & if\ \frac{1}{n-1} \leq X < \frac{n-1}{n} \\ \frac{[n(X-1)]P\left(\hat{S}_{PL}(t) = 1\right)}{1 - \gamma[F_Y(t)]^n} + 1 & if\ \frac{n-1}{n} \leq X < 1 \\ 1 & if\ X \geq 1 \end{cases} .$$

In our computational study, we consider sample sizes $= 5, 10, 15,\ 20,$ 25, and 30, assuming that the survival times T_i and censoring times C_i follow independent exponential distributions with rates 1 and β, respectively. Under this setting, the proportion of uncensored observations is given by $\gamma = \frac{1}{1+\beta}$ with $\beta = 0.5, 1.0, 1.5,$ and 2.0. For brevity, we restrict graphical illustrations to the product-limit estimator (PLE) under the scenario with $\beta = 1.0\ and\ n = 5, 10, 15.$

It should be noted that exact computations of the interpolated cumulative distribution function (CDF) for the PL estimator become computationally prohibitive for $n \leq 15$. Moreover, we confine our analysis to the time interval $t \in [0.05, 3.0]$; see Paige (2017).

The exclusive use of exponential distributions for both survival and censoring times reflects a standard modeling choice in finite-sample simulation studies of the PLE; see, for example, Chen et al. (1982), Chang and Cheng (1985), and Chang (1996).

Our numerical results demonstrate that the 95% two-sided symmetric population tolerance bounds for the PLE, derived from both the exact interpolated CDF and the adjusted saddlepoint CDF approximation, exhibit close agreement for $n \leq 15$. Figure 1 illustrates the representative case corresponding to $\beta = 1.0\ and\ n = 5, 10,$ and 15. In these plots, the 95% population tolerance bands based on the exact CDF appear as black dotted curves, while those obtained from the adjusted saddlepoint approximation are shown as solid gold curves.

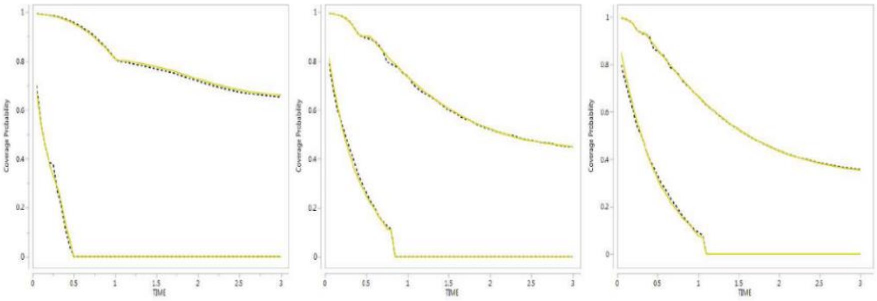


Figure 1: **The 95% Population Tolerance Bands for the PL Estimator with $\boldsymbol{\beta = 1.0}$.**

4.3.1. Pointwise Bootstrap Confidence Interval

Bootstrap-based confidence intervals for the survival function $\mathrm{S}(t)$, derived from the product-limit (PL) estimator at a nominal confidence level of $(1-\alpha)100\%$, are constructed by substituting the unknown parameter γ with its estimate $\hat{\gamma}$, and replacing the true distribution function $F_Y(t)$ with its empirical counterpart $\hat{F}_Y(t)$. The resulting interval estimates are then obtained by computing the 95% population tolerance bounds for the survival function using either the exact interpolated cumulative distribution functions (CDFs) or the adjusted saddlepoint CDF approximations.

A comparative evaluation of the performance of these bootstrap-based confidence bands against several established alternatives is presented in the following section.

5. Simulation Study

In this section, we evaluate the performance of the proposed confidence and tolerance interval methods for the Product Limit Estimator (PLE) under the proportional hazards model. Specifically, we compare the empirical coverage probabilities of: exact confidence intervals derived from the full finite-sample distribution of the PLE, confidence intervals based on the saddlepoint approximation, and classical large-sample confidence intervals based on the exponential Greenwood method.

Our objective is to assess how closely each method maintains nominal coverage levels, particularly in small-sample scenarios and under varying degrees of censoring.

5.1.Simulation Design

We simulate right-censored survival data under the proportional hazards framework as follows:

- **Survival times** T_i are generated from an exponential distribution with unit rate .
- **Censoring times** C_i are generated independently from an exponential distribution with rate $\gamma = \frac{1}{1+\beta}$, for fixed values of $\beta \in \{0.5, 1.0, 1.5, 2.0\}$.
- **Observed data** are $Y_i = min(T_i, C_i)$ with event indicators $\Delta_i = I(T_i \leq C_i)$.
- **Sample sizes** considered are $n = 5, 10, 15, 20, 25$ and 30.
- For each combination of n and β, we simulate **10,000 replicas.**
- Time points t are varied from $0.05\ to\ 3.0$ in increments of 0.05.

For each replica, we construct 95% confidence intervals for $S(t)$ using each of the three methods above and evaluate whether the true survival function $\text{S}(t)$ lies within the interval.

5.2.Coverage Probability Estimation

Let $\left(\hat{\text{S}}_L(t)_j, \hat{\text{S}}_U(t)_j\right)$ denote the confidence interval for the jth simulated sample at time t, and let $S(t)$ denote the true survival probability. The empirical coverage probability is estimated by:

$$P\left(\hat{\text{S}}_L(t) \leq \text{S}(t) \leq \hat{\text{S}}_U(t) | \hat{\text{S}}_L(t) \neq \hat{\text{S}}_U(t)\right)$$
$$= \frac{\sum_{j=1}^{10,000} I\left(\hat{\text{S}}_L(t)_j \leq \text{S}(t) \leq \hat{\text{S}}_U(t)_j\right)}{\sum_{j=1}^{10,000} I\left(\hat{\text{S}}_L(t)_j \neq \hat{\text{S}}_U(t)_j\right)}$$

We compute and plot coverage probabilities for all methods for $\beta = 1.0$ and sample sizes $n = 5, 10,$ and 15 for each method.

5.3.Results and Interpretation

Figure 2 illustrates coverage probabilities as a function of time t for sample sizes $n = 5, 10,$ and 15, and censoring rate $\beta = 1$, which are representative of broader trends. In each plot:

- The **black dotted curve** represents coverage from the **exact** distribution-based intervals.
- The **gold solid curve** represents coverage from the **saddlepoint** approximation.
- The **green dashed-dotted curve** represents the **exponential Greenwood** method.
- A **red dashed horizontal line** marks the nominal 95% coverage level.

We found that the saddlepoint approximation consistently provides coverage very close to the exact method across all time points, and the Greenwood method exhibits notable under-coverage, especially at smaller t or when censoring is high. In addition, as n increases, all methods improve, but saddlepoint-based intervals converge to exact intervals much faster than Greenwood intervals do, and the performance of saddlepoint intervals remains stable even as the censoring rate increases β, while large-sample methods degrade under heavy censoring.

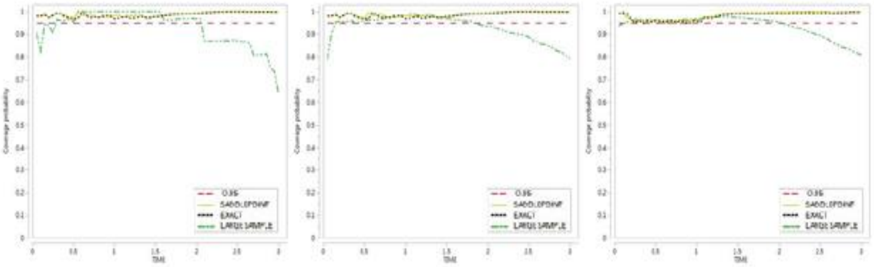


Figure 2: Coverage Probabilities for Various Pointwise Confidence Band Methods Based on the PL Estimator with $\boldsymbol{\beta = 1.0}$.

The simulation results clearly demonstrate that saddlepoint-based confidence intervals offer an excellent approximation to exact small-sample inference. They achieve near-nominal coverage, are computationally efficient, and outperform traditional large-sample methods especially in the presence of right-censoring and small to moderate sample sizes.

In the following section, we analyze the finite-sample properties of the PLE in terms of its mean, bias, variance, and mean squared error (MSE), using both exact and approximated methods.

6. The Mean, Bias, Variance, and MSE for PL Survival Estimator

In this section, we examine the finite-sample behavior of the Product Limit Estimator (PLE) for the survival function under the proportional hazards model. Specifically, we investigate the exact mean, bias, variance, and MSE of the PL estimators for t = 0.5, 1.0, 1.5, 2.0.

To compute the exact finite-sample characteristics of the PLE, we utilize its moment structure obtained via the Mellin transform, as described in Section 3. The simulation setup follows the same structure as in Section 5: Failure times are drawn from an exponential distribution with unit rate, Censoring times are generated from an exponential distribution with rate $\gamma = \frac{1}{1+\beta}$ where $\beta \in \{0.5, 1.0, 1.5, 2.0\}$, The observed data consist of $(Y_{\text{i}}, \delta_{\text{i}})$ pairs, where $Y_i = min(T_i, C_i)$, and Sample sizes considered: $n = 5, 10, 15, 20, 25$ and 30. At each (n, β, t) configuration, we evaluate the exact mean, bias, variance, and MSE of $\hat{\mathrm{S}}(t)$.

The bias and MSE are defined, respectively, as:

$$Bias\left[\hat{\mathrm{S}}(t)\right] = E\left[\hat{\mathrm{S}}(t)\right] - \mathrm{S}(t) \quad \& \quad MSE\left[\hat{\mathrm{S}}(t)\right] = E\left[\hat{\mathrm{S}}(t) - \mathrm{S}(t)\right]^2$$

Table 6.1 summarizes the computed values of the mean, bias, variance, and MSE for the PLE across all parameter combinations. Key observations from the results are as follows:

- **Consistency with increasing sample size**:
  The bias of the PLE decreases rapidly as sample size increases. By $n = 20$, the estimator exhibits negligible bias across most scenarios, aligning closely with the true survival function.

- **Bias increases with time t**:
  For a fixed n and β, the bias increases as t increases. This is expected, since estimating survival probabilities in the tail of the distribution is more difficult due to fewer observed events.

Table 6.1: The Mean, Bias, Variance, and MSE of the PL Survival Estimators.

		t = 0.5, $S(t) = 0.6065$				t = 1.0, $S(t) = 0.3679$			
β	n	$\mu(t)$	$-b(t)$	$\sigma^2(t)$	MSE	$\mu(t)$	$-b(t)$	$\sigma^2(t)$	MSE
0.5	5	0.5835	0.0230	0.0617	0.0622	0.3754	-0.0075	0.0665	0.0666
	10	0. 6060	0. 0005	0. 0281	0. 0281	0. 3688	-0. 0009	0. 0334	0. 0334
	15	0.6065	0. 0000	0. 0185	0. 0185	0. 3680	-0. 0002	0. 0219	0. 0219
	20	0.6065	0. 0000	0. 0138	0. 0138	0. 3679	0. 0000	0. 0163	0. 0163
	25	0. 6065	0. 0000	0. 0110	0. 0110	0. 3679	0. 0000	0. 0129	0. 0129
	30	0. 6065	0. 0000	0. 0092	0. 0092	0. 3679	0. 0000	0. 0107	0. 0107
1.0	5	0. 6025	0. 0041	0. 0696	0. 0696	0. 3987	-0. 0308	0. 0881	0. 0890
	10	0. 6066	-0. 0001	0. 0334	0. 0334	0. 3752	-0. 0073	0. 0474	0. 0475
	15	0. 6065	0. 0000	0. 0218	0. 0218	0. 3701	-0. 0022	0. 0318	0. 0318
	20	0. 6065	0. 0000	0. 0162	0. 0162	0. 3686	0. 0008	0. 0236	0. 0236
	25	0. 6065	0. 0000	0. 0129	0. 0129	0. 3682	0. 0003	0. 0186	0. 0186
	30	0. 6065	0. 0000	0. 0107	0. 0107	0. 3680	-0. 0001	0. 0154	0. 0154
1.5	5	0. 6120	-0. 0055	0. 0797	0. 0797	0.4332	-0.0653	0.1068	0.1116
	10	0. 6072	-0. 0006	0. 0400	0. 0400	0.3911	-0.0232	0.0632	0.0637
	15	0. 6066	-0. 0001	0. 0260	0. 0260	0.3781	-0.0102	0.0445	0.0446
	20	0. 6065	0. 0000	0. 0192	0. 0192	0.3728	-0.0049	0.0340	0.0340
	25	0. 6065	0. 0000	0. 0152	0. 0152	0.3704	-0.0025	0.0273	0.0273
	30	0. 6065	0. 0000	0. 0126	0. 0126	0.3692	-0.0013	0.0226	0.0226
2.0	5	0. 6120	-0. 0144	0. 0896	0. 0898	0.4731	-0.1052	0.1206	0.1317
	10	0. 6087	-0. 0022	0. 0478	0. 0478	0.4164	-0.0485	0.0779	0.0803
	15	0. 6069	-0. 0004	0. 0313	0. 0313	0.3946	-0.0268	0.0580	0.0587
	20	0. 6066	-0. 0001	0. 0229	0. 0229	0.3839	-0.016	0.0462	0.0465
	25	0. 6065	0. 0000	0. 0181	0. 0181	0.3779	-0.01	0.0382	0.0383
	30	0. 6065	0. 0000	0. 0149	0. 0149	0.3744	-0.0065	0.0324	0.0324

		t = 1.5, $S(t) = 0.2231$				t = 2.0, $S(t) = 0.1353$			
β	n	$\mu(t)$	$-b(t)$	$\sigma^2(t)$	MSE	$\mu(t)$	$-b(t)$	$\sigma^2(t)$	MSE
0.5	5	0.2499	-0.0267	0.0596	0.0603	0.1855	-0.0501	0.0516	0.0541
	10	0.2301	-0.007	0.0303	0.0303	0.1546	-0.0193	0.0254	0.0258
	15	0.2256	-0.0024	0.0202	0.0202	0.1449	-0.0095	0.0169	0.0170
	20	0.2241	-0.001	0.0151	0.0151	0.1406	-0.0053	0.0127	0.0127
	25	0.2235	-0.0004	0.0120	0.0120	0.1384	-0.0031	0.0101	0.0101
	30	0.2233	-0.0002	0.0099	0.0099	0.1373	-0.0019	0.0084	0.0084
1.0	5	0.3054	-0.0823	0.088	0.0948	0.2684	-0.1330	0.0859	0.1036
	10	0.2579	-0.0347	0.0488	0.0500	0.2076	-0.0723	0.0470	0.0522
	15	0.2413	-0.0182	0.034	0.0343	0.1825	-0.0472	0.0327	0.0349
	20	0.2336	-0.0104	0.0261	0.0262	0.1688	-0.0335	0.0252	0.0263
	25	0.2295	-0.0064	0.0211	0.0211	0.1602	-0.0249	0.0205	0.0211
	30	0.2272	-0.004	0.0176	0.0176	0.1544	-0.0191	0.0174	0.0178
1.5	5	0.371	-0.1479	0.1112	0.1330	0.3521	-0.2168	0.1119	0.1589
	10	0.304	-0.0809	0.0684	0.0749	0.2759	-0.1406	0.0690	0.0888
	15	0.2755	-0.0523	0.0503	0.0530	0.2404	-0.1051	0.0511	0.0621
	20	0.2597	-0.0365	0.0402	0.0415	0.2191	-0.0837	0.0410	0.0480
	25	0.2498	-0.0267	0.0335	0.0342	0.2045	-0.0692	0.0346	0.0394
	30	0.2432	-0.0201	0.0288	0.0292	0.1939	-0.0586	0.0300	0.0334
2.0	5	0.4341	-0.211	0.1263	0.1780	0.4251	-0.2898	0.1274	0.2114
	10	0.3575	-0.1343	0.0847	0.1027	0.3432	-0.2079	0.0861	0.1293
	15	0.3213	-0.0981	0.0657	0.0753	0.3027	-0.1674	0.0672	0.0952
	20	0.2994	-0.0763	0.0544	0.0602	0.2772	-0.1419	0.0560	0.0761
	25	0.2846	-0.0615	0.0468	0.0506	0.2591	-0.1238	0.0485	0.0638
	30	0.2739	-0.0507	0.0412	0.0438	0.2455	0.1101	0.0431	0.0552

- **Censoring impact:**
  For a fixed t and n, both the bias and variance of the PLE increase as the censoring rate increases (β increases). This is due to reduced information about event times, especially in the right tail.
- **Asymptotic convergence**:
  As n → ∞, the mean of the PLE approaches the true survival function $S(t)$, and the variance and MSE converge toward zero, consistent with the known asymptotic properties of the estimator.

As result, The PLE exhibits **small finite-sample bias** that decreases with larger sample sizes and increases with time t and censoring rate β. Also, **Variance and MSE** follow similar trends, diminishing with increased information (i.e., larger n, lower β).

These results further validate the use of the saddlepoint approximation, which accurately reflects the true distributional properties of the estimator, as demonstrated by the close alignment in mean and variance.

7. Conclusions

This paper addressed the challenge of making accurate inference for the survival function using the Product Limit Estimator (PLE) in small-sample settings under the proportional hazards model with right censoring. While the asymptotic properties of the PLE are well understood, the development of exact and near-exact methods for small samples remains crucial in practice-particularly when data are heavily censored or sample sizes are limited.

We derived the exact finite-sample distribution of the PLE, incorporating the constant tail that arises from right-censoring of the largest observed time. Building on this, we developed mid-p population tolerance intervals and exact pointwise confidence intervals for the survival function $S(t)$. Recognizing the computational burden of exact enumeration as sample size increases, we introduced a saddlepoint-based approximation method to efficiently approximate the distribution of the PLE.

Our simulation studies demonstrated that the saddlepoint approach achieves excellent agreement with exact methods in terms of coverage probability, while outperforming conventional large-sample methods such as the exponential Greenwood interval. In addition, we showed that the saddlepoint intervals remain highly accurate even in the presence of moderate to heavy censoring.

The finite sample analysis of the PLE confirmed its favorable properties: the estimator's bias and variance decrease with increasing sample size, while bias increases with both time t and the censoring rate parameter β. These findings support the conclusion that the PLE remains a reliable estimator in small samples, particularly when paired with carefully constructed saddlepoint-based inference methods.

In summary, this work contributes both exact theoretical results and practical inference tools for the PLE in small-sample, right-censored survival data. The saddlepoint-based methods we propose offer a compelling compromise between accuracy and computational feasibility, making them especially well-suited for real-world applications where exact enumeration is impractical and large-sample approximations may fail.

References

[1] Kaplan, E. L., & Meier, P. (1958). Nonparametric estimation from incomplete observations. American Statistical Association, 457-481.

[2] Breslow, N. E., & Crowley, J. (1974). A large sample study of life table and product limit estimates under random censorship. The Annals of Statistics, 2, 437–453.

[3] Paige, R., & Abdurasul, E. (2017). Confidence intervals for survival functions in small samples under the proportional hazards model. Communications in Statistics - Theory and Methods, 47, 6108-6124.

[4] Chen, Y. Y., Hollander, M., & Langberg, N. A. (1982). Small-sample properties of the Kaplan-Meier estimator. Journal of the American Statistical Association, 77, 140-144.

[5] Chang, M. (1996). The exact distribution of the Kaplan-Meier estimator under the proportional hazards model. Statistics and Probability Letters, 28, 153-157.

[6] Borgan, Ø., & Leist, A. (1990). Confidence bands for survival curves based on transformations: A brief note. Scandinavian Journal of Statistics, 17, 35-41.

[7] Butler, R. (2007). Saddlepoint Approximations with Applications. New York.

[8] Parzen, E. (2008). United statistics, confidence quantiles, and Bayesian statistics. Journal of Statistical Planning and Inference, 138, 2777.

[9] Billingsley, P. (1986). Probability and Measure (2nd ed.). Wiley, New York.

[10] Daniels, H. E. (1954). Saddlepoint approximations in statistical theory. The Annals of Mathematical Statistics, 25, 631-650.

[11] Lugannani, R. A., & Rice, S. O. (1980). Saddlepoint approximation for the distribution of the sum of independent

random variables. Advances in Applied Probability, 12, 475-490.

[12] Cheng, S., & Chang, H. (1985). A comparison of PLE and MLE for survivor functions in a simple proportional hazards framework. The Chinese Statistical Association, 23, 57-74.

8

The Role of Artificial Intelligence in Improving Network Security

The Role of Artificial Intelligence in Improving Network Security

Moktar M. Lahrashe
Al-zawiya College of Computer Technology
mlahrashe@gmail.com

Abstract

The study explores the use of artificial intelligence (AI) in network security to enhance defenses against cyberattacks. It highlights the importance of machine learning, neural networks, and pattern recognition techniques in predicting attacks and evaluating data behavior. AI can also aid in data categorization and predictive analysis, making firewalls and security systems more effective. The research emphasizes the role of AI in enhancing networks' resistance to sophisticated attacks like advanced persistent threats.

Keywords: Artificial Intelligence (AI)، Network Security ، Sophisticated Attacks، Security Systems.

1. Introduction

Networks are a vital component of the modern world's digital infrastructure, utilized for everything from government and industrial services to personal communication to vital commercial activities. As our reliance on these networks grows, cybersecurity has emerged as a crucial problem that calls for creative solutions to defend against ever more intricate and varied intrusions. In this regard, artificial intelligence technologies have become a powerful instrument capable of revolutionizing network security.

Artificial intelligence has emerged as one of the most significant technologies in the world of cybersecurity because of its capacity to collect and analyze vast volumes of data and make wise judgments based on patterns and behaviors. Artificial intelligence offers more adaptable and reliable ways to counteract unusual assaults or those that depend on cutting-edge technology than conventional techniques that rely on static databases or software that defends networks against known threats.

By concentrating on the use of machine learning, artificial neural networks, and pattern recognition techniques for early threat detection, this study seeks to investigate how artificial intelligence might improve network security. It also emphasizes how these technologies may be used to enhance network defense against sophisticated assaults and offer creative ways to shield private information from growing threats. A thorough understanding of how businesses may employ artificial intelligence to protect their networks will be provided by this study, along with an analysis of the potential advantages and disadvantages of implementing these cutting-edge technologies in this crucial area.

The study focuses on the challenges facing traditional network security frameworks as a result of more complex and frequent cyberattacks. Even as companies work hard to build security systems to protect their networks from threats, these systems often cannot handle ongoing and innovative attacks such as advanced persistent threats (APTs) and attacks with complex targets. Because these cyberattacks rely on new technologies that are difficult for traditional tools to identify, it is crucial to look for advanced solutions that can adapt and learn from ever-changing patterns and data.

The fundamental problem is that most traditional security solutions rely on outdated software or static databases that only search for known threats. The ability of these systems to defend networks against unexpected or unknown attacks is weakened by the constant expansion of attack strategies and methods. In addition, traditional technologies cannot anticipate future risks or respond to attacks that use new technologies to bypass defenses. In this regard, artificial intelligence (AI) emerges as a potential remedy to this problem. AI is able to quickly and accurately evaluate massive amounts of data using machine learning techniques and may identify patterns that may indicate security vulnerabilities.

The problem is how to use these techniques efficiently in large, complex networks, because AI itself suffers from a host of problems, including the requirement of huge training databases and complex specifications to ensure that models are free of errors or security flaws that could reduce the effectiveness of the system. Another problem is that AI must constantly adapt to new attack techniques, which require frequent and careful upgrades to the models to prevent security breaches.

2. Importance of Study

Given the sharp rise in the number and complexity of cyberattacks that target electronic networks globally, the research "The Role of Artificial Intelligence in Improving Network Security" is extremely important. Network security has emerged as a crucial concern that jeopardizes the stability and dependability of businesses as they depend more on networks to carry out their business and electronic activities. Therefore, utilizing AI as a security tool is a critical first step in creating intelligent and practical solutions to address sophisticated and complicated security threats.

The study's significance stems from its capacity to offer a thorough grasp of how artificial intelligence technology might be used to address the escalating cybersecurity concerns. In comparison to traditional systems, artificial intelligence may significantly enhance networks' capacity to identify hazards early and analyze data more quickly and correctly using machine learning and neural network techniques. This helps to lower the risks associated with cyberattacks and enhances networks' ability to withstand persistent and sophisticated attacks.

The study explores the integration of artificial intelligence into security systems, enhancing network protection and preparing networks for future cyberattacks. It also provides innovative solutions to address administrative and technological challenges faced by organizations in implementing advanced technologies, thereby advancing knowledge of potential solutions.

3. Methodology

3.1 Study Tools:

Interviews that are semi-structured Qualitative data will be gathered through semi-structured interviews with professionals in the fields of smart technology and cybersecurity. Through these, the real-world experiences of businesses using AI to strengthen network security will be examined. In-depth knowledge of the strategies and tactics employed, as well as the difficulties businesses have when incorporating AI into their security systems, may be obtained from these interviews.

Survey :For network security experts working for businesses and organizations, a survey will be created. The usefulness of artificial intelligence methods in identifying threats, enhancing network response, and lowering false positives will all be included in the survey. Participants will be able to provide quantifiable information regarding the uses of artificial intelligence through the questionnaire.

Analysis of Secondary Data on the function of AI in network security will be gathered and examined via professional publications, university research, and published cybersecurity reports. To find the most recent advancements, effective strategies, and potential drawbacks when utilizing these technologies, the literature that is currently accessible on AI applications in this industry will be reviewed.

3.2 Data Analysis

Following data collection, both quantitative and qualitative analytic methods will be used to examine the primary data. While qualitative analysis will entail classifying and organizing data from interviews and field observations in order to identify patterns and trends, quantitative analysis will utilize statistical tools, such as SPSS or Excel, to examine the questionnaire findings. Analysis by Comparison The use of artificial intelligence in network security across various firms that were observed, or data was gathered will be compared. To comprehend the variations in performance and the difficulties that companies encountered while putting these technologies into practice, this comparison will depend on the findings of both quantitative and qualitative study.

3.3 Study limitations

3.3.1 Spatial Limits

The study focuses on how AI applications enhance network security in workplaces in technologically advanced countries such as the United States, the United Kingdom, and major European countries. With specific applications evaluated in countries with highly developed technological infrastructure, the research will only include large organizations and companies that use AI technology to enhance their network security.

AI applications in countries or regions that have not yet widely used these technologies or that lack advanced cybersecurity systems will not be included in the research.

3.3.2 Timeline

The study’s scope is restricted to the years 2010–present. This time range makes it possible to concentrate on the most recent advancements in artificial intelligence (AI) in the area of network security, including more current uses like deep learning and neural networks, which have started to advance dramatically during the past ten years. We’ll examine how AI technologies have changed over time and how they’ve affected network cybersecurity improvements. Included will be upcoming developments in AI technology that have only started to take shape.

4. Literature review

The literature survey first aims to provide an overview of previous works of AI and Network Security. Then, we discuss the theory of network security, the importance of artificial intelligence in enhancing security and its applications.

4.1 Review of recent research

There are several works that have been carried out by other researchers in this field. However, this section gives an overview of some important recent research papers. Many authors have identified different issues to enhance network security. Authors in [1] shows that AI tools make business operations run better while protecting assets and delivering better results for customers. The research presents solutions to the current obstacles and suggests more research is needed to completely understand how AI can benefit logistics operations over time. Authors in [2] proposes an artificial intelligence (AI)-driven approach to enhance network security specifically for renewable energy (RE) infrastructures, targeting vulnerabilities that affect data integrity and operational stability. This research also introduces an Adaptive Spider Wasp optimizer-mutated Extreme Gradient Boosting (ASW-XGBoost) model as a novel solution designed to improve detection accuracy and enhance resilience across diverse RE networks. The proposed method initiates the creation of a dataset representative of both power system behaviors and potential cyber-attacks, pre-processed using a normalization algorithm to improve data quality. Feature extraction leverages a scalable approach to identify critical indicators unique to RE environments. Authors in [3] highlights how AI and ML can significantly enhance the accuracy and efficiency of security processes, thereby bolstering an organization's overall cybersecurity posture. The study also emphasizes the importance of seamlessly integrating AI and ML with existing security architectures to maximize their benefits. Authors in [4] presents a straightforward framework for assessing AI Methods in cyber threat detection. Given the increasing complexity of cyber threats, enhancing AI methods and regularly ensuring strong protection is critical. they evaluate the effectiveness and the limitations of current ML and DL proposed models, in addition to the metaheuristic algorithms. Authors in [5] reviews needs in the cyber security domain that can be addressed through Artificial Intelligence (AI) techniques. In this study, they employed quantitative methods to assess the impact of artificial intelligence on enhancing cybersecurity by distributing questionnaires to 85 respondents, which included companies operating in the banking and IT sectors. In addition, this research explore how data-based intelligent decision-making systems are able to protect systems from known and unknown cyber-attacks. Authors in [6] conducting a systematic literature review (SLR) to assess the impact of AI-based technologies on organizational cyber security and determine their effectiveness compared to traditional cyber security approaches. Authors in [7] focuses on artificial intelligence, summarizes the related definitions and classic models of network security situational awareness, and provides an overview of artificial intelligence. Starting from the method of machine learning, it specifically introduces the research status of neural-network-based network security situational awareness and summarizes the research work in recent years. Authors in [8] focus on cyber security issues, they explore the challenges of blockchain deployment in smart environments. Additionally, they explore the use of anomaly detection AI-based techniques as a ledger of blockchain technologies to address the security issues in smart environments. Thus, they propose a framework that emphasizes the challenges of BT, values and capabilities of BT-AI integration. They also present research trends to highlight potential research paths for improving the security of blockchain networks using artificial intelligence. Authors in [9] evaluates the security issues faced by Big data systems using AI techniques focusing on different attacks, defense strategies, and security evaluation models. The AI-based techniques for security enhancement in big data-based systems are divided into eight categories: reinforcement learning, swarm intelligence, deep learning, multi-agent, game theory, ML, and ANN. The review is systematically conducted using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analysis) technique. Authors in [10] written the idea to dig out the issues that the world is facing and the problems which have the potential to be a threat and affect the growth of networking ,The author also focus on the solutions which have the future scope to counter these problems including new techniques developed and devised by some researchers and network security-based start-ups incorporating AI, which will be the future trend for solving a lot of upcoming issues in the technology. Authors in [11] summarizes representative AI solutions and compares the different algorithms and technologies used by various solutions. they also bring new potential challenges and possible negative effects to IoT in terms of data, algorithm and architecture. Authors in [12] presents a system which is used to prevent WSN from various types of attacks. By using the concept of artificial intelligence, we can easily detect the malicious nodes so that we can easily prevent our secret information from malicious nodes and also on expert system is developed using C language to prevent WSN from various types of attacks.

4.2 AI and Network Security

4.2.1 Artificial Intelligence and its fields

The term Artificial Intelligence (AI) has several different meanings on the Internet. Intelligence is defined as “the ability of the mind, especially to understand principles, facts, or meanings and to acquire and apply knowledge in practice; the ability to learn and understand.” Oxford Dictionaries defines intelligence as “the ability to acquire and apply knowledge and skills.” It has been noted that high-profile conferences and publications, such as the Artificial Intelligence Journal (AIJ) and the International Joint Conference on Artificial Intelligence (IJCAI), do not define AI. Obviously, anyone submitting a paper to these conferences and publications is expected to be familiar with what AI is [13].

Intelligence is defined as the ability to learn or understand through experience; the ability to acquire and retain knowledge; mental ability; the ability to respond quickly and successfully to a new situation; the ability to use reasoning to solve problems, and to direct thinking, In the field of computer science, artificial intelligence refers to the research and engineering utilized to create intelligent systems that support technological progress. Although it mimics the functioning of human intellect, it lacks the physiologically observable techniques. One way to conceptualize artificial intelligence is as a field of research that uses computer models to address the analytical and algorithmic aspects of issues. The discipline of computer science known as artificial intelligence works to give different computer systems more intelligence [14].

One definition of intelligence is the ability to acquire and use appropriate methods to solve problems and achieve goals in an unpredictable and ever-changing world. A fully programmed industrial robot is accurate, consistent, and versatile, but it lacks intelligence. Artificial intelligence is the science and engineering of making intelligent machines, which is how retired Stanford University professor John McCarthy described artificial intelligence (AI). Much research has shown that humans can teach machines to behave intelligently, such as playing chess without micromanagement. Autonomous systems are able to independently plan and choose the best course of action to achieve a given goal. For a hospital delivery robot to succeed, it must be able to navigate crowded corridors on its own. In AI, autonomy lacks the concept of self-governance typical of biology and politics. Al's research in machine learning focuses on how computer agents use data or experience to enhance their perception, understanding, reasoning, or behavior. Machine learning uses economics, statistics, psychology, neuroscience, computer science, and control theory to do this [15].

Narrow AI is an intelligent system for a specific task, such as facial recognition or speech. Artificial general intelligence (AGI), or human-level AI, aims to create context-aware, intelligent robots at scale. Effective social chatbots and human-robot interactions require it. Human-centered AI aims to enhance human capabilities, meet social demands, and draw inspiration from people. It researches and develops tools and companions that are useful to humans, such as robot companions and assistants for the elderly. Deep learning is a system of artificial intelligence and large multi-layer artificial neural networks that compute using continuous representations with higher generalization from small data, better scalability to big data, and computing budgets. It is now the most effective machine learning technique as it can be used for all forms of machine learning as the algorithm defines, such as what a human puts into a computer program. Algorithms are used in many systems, although usually only for specific functions such as reward calculation or learning. A large part of their behavior is the result of learning from experience or data, a radical shift in the system architecture that Stanford graduate Andrej Karpathy has called Software 2.0.

Artificial Intelligence Definitions Even while academic, business, and government organizations are becoming more interested in artificial intelligence (AI), there isn't a consensus on what AI genuinely means. Regarding human intelligence or intelligence in general, artificial intelligence has been explained using certain methodologies. Numerous definitions make reference to machines that exhibit human-like behaviors or are able to carry out tasks that call for intelligence، An objective description of something as subjective and abstract as intelligence creates the misleading appearance of unachievable accuracy since human intellect is hard to describe and quantify, despite several attempts at quantification Because of this, the majority of definitions in market, policy, and research reports are imprecise and imply an ideal objective rather than a quantifiable research notion [16].

When discussing rational AI and the optimal performance criterion, the High-Level Expert Group on AI has highlighted the simplifying of the notion of intelligence required to describe or even build AI, as noted by certain scholars like Russell and Norvig ،"If a system acts in the "correct way" in light of its knowledge, it is rational." Two initiatives are specifically taken into account in this study when examining definitions of AI: the High-Level Expert Group's contribution to the area of AI and ongoing standardization efforts.

The main characteristics of artificial intelligence that distinguish it and make it at the forefront of technology are:

- Environmental awareness, which takes into account the complexity of the real world.
- Information processing, which collects and analyzes data as inputs;
- Decision-making, which includes thinking, learning, acting and executing tasks

- Adaptation and response to environmental changes with a certain degree of autonomy.

4.2.2 Al Watch Operational Definition of Al

It made up of a brief taxonomy and a list of keywords that define the core and transversal domains of Al an inclusive definition that encompasses all technological advancements and activities conducted by all kinds of actors that comprise the Al ecosystem whether industrial, research, or government initiatives is crucial for establishing a shared understanding of the concept of Al in the context of Al Watch [17].

AI systems are also known as software systems created by humans and when presented with a complex goal, they operate in the digital or physical domain by observing their surroundings by collecting data, analyzing the collected structured or unstructured data, applying informational reasoning, processing data and determining the best course of action to achieve the goal. AI systems can learn a numerical model or use symbolic rules, and they can also modify their behavior by examining the effects of their previous actions on the environment. This broad definition of AI includes a wide range of techniques and the most common methods are ML4 methods. According to the European Artificial Intelligence Strategy, AI is defined as systems that exhibit intelligent behavior by analyzing their surroundings and acting more or less independently to achieve certain goals. Systems that use technologies such as text mining, computer vision, speech recognition, natural language generation, machine learning, and deep learning to collect and use data to predict, recommend, or decide - with varying degrees of autonomy - the best course of action to achieve certain goals are referred to as artificial intelligence [18].

4.2.3 Benefits of Artificial Intelligence

The advantages of using AI in many fields have been multiple, such as being a special educational assistant for teachers and an intelligent support for collaborative learning, AI also gives each learner a personalized learning experience ،The benefits of AI include cost-effectiveness and reliability. One of the technologies used now is turning traffic sensors into intelligent agents that can automatically identify accidents and help predict traffic conditions. It can also solve tedious and complex problems that humans may not be able to handle with AI ،AI is more efficient than humans at completing tasks, and when AI is implemented correctly, the possibility of errors is almost eliminated [19].

AI bases its judgments on facts, not feelings. Since AI-enabled devices do not need to sleep, the workspace can be more productive. It is easier to spread knowledge within the AI itself Since fashion companies deal with a variety of data that has many complex relationships and dependencies, AI methods are now very effective in these industries. Intelligent tracking systems, textile quality control, decision making, social media, fashion e-marketing, and design assistance systems are just a few examples of the many applications of AI in the fashion sector [20].

4.2.4 The concept of network security and the importance of artificial intelligence in enhancing security

Artificial Intelligence (AI) has become a game-changing technology in the field of network security, due to the advantages of AI, as it helps companies better defend their digital assets against an ever-changing array of cyber threats. Integrating AI into network security frameworks provides more flexible and dynamic solutions while addressing the shortcomings of traditional security measures. The main advantages of AI for network security are increased efficiency and accuracy. The ability of AI to significantly increase the accuracy and effectiveness of threat detection and response is one of its key advantages in network security. High false positive and false negative rates are a common problem for traditional security systems, which can overwhelm security professionals and cause attacks to go unnoticed.

The basis for safeguarding digital assets and guaranteeing the secure operation of corporate networks has already been established by traditional network security methods. Intrusion detection systems, firewalls, and antivirus programs are some examples of these precautions. By filtering incoming and outgoing traffic according to pre-established security criteria, firewalls serve as a barrier between trusted and untrusted networks. The purpose of antivirus software is to identify, stop, and eliminate threats to computers, including Trojan horses, worms, and viruses. Network traffic is monitored by intrusion detection systems for indications of malicious activity or policy breaches, and they send out notifications when such risks are found.

Al in network security refers to a variety of tools and methods intended to improve an organization's security posture:

- **Supervised learning in supervised learning**, algorithms are trained on labeled datasets, where the input data and corresponding output or label are known. This approach is widely used in network security for tasks such as malware detection, where the algorithm is trained to distinguish between benign and malicious programs based on historical data. Techniques such as decision trees, support vector machines, and neural networks are commonly used in supervised learning to classify network traffic and detect intrusions [21].
- **Unsupervised learning** Unsupervised learning algorithms (which are the opposite of supervised learning) use unlabeled

data to find patterns and anomalies without knowing the expected outcomes in advance. Finding strange patterns or behaviors that may indicate a security breach is the goal of anomaly detection in network security. This method is very useful for identifying network traffic anomalies that deviate from typical behavior. Methods such as dimensionality reduction and clustering are used [22]

- **Deep learning**, is a part of machine learning, involves multi-layered neural networks (deep neural networks) that can learn and model complex patterns in large datasets. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs), two deep learning models, are used in network security for tasks including malware classification and intrusion detection. By independently learning representations from unprocessed network data, these models can reduce false positives and increase the accuracy of threat detection.
- **Natural language processing** (NLP**)** is used in cybersecurity for activities such as threat intelligence analysis, which helps detect new threats and vulnerabilities by analyzing and understanding large amounts of text data, such as threat reports, security logs, and social media feeds. By examining email content for malicious intent, natural language processing (NLP) techniques can also improve phishing detection [23].

4.2.5 Benefits of Artificial Intelligence (AI) in Cybersecurity

AI offers a number of notable advantages in cybersecurity by providing businesses with advanced capabilities to defend their digital assets against an increasingly complex threat landscape, making it an invaluable tool for network security. AI uses machine learning algorithms and massive amounts of data to detect and respond to threats more quickly than traditional techniques. In order to find anomalies that could indicate a security breach, these algorithms can examine user activity, system logs, and network traffic. AI-powered systems can detect previously unidentified risks by identifying deviations from typical behavior, unlike traditional signature-based detection systems that rely on established threat patterns [24]

Machine learning algorithms including reinforcement learning, supervised learning, and unsupervised learning are essential to this process. Unsupervised learning models can detect new and emerging risks by combining comparable data points and identifying outliers. Supervised learning models are trained on labeled datasets to identify specific threat categories. By learning from the results of their activities, reinforcement learning models gradually increase their detection capabilities [24].

AI-based systems are able to recognize anomalous network traffic patterns that indicate an illegal access attempt or a distributed denial of service (DDoS) attack, and immediately notify security personnel or initiate automatic countermeasures. In order to identify anomalous activity that could indicate a security risk, AI analyzes user behavior. AI systems can detect anomalies that indicate illegal access or data leakage by establishing a baseline of each user's typical behavior. An AI system can identify suspicious activity, for example, if an employee who normally logs in from a certain location during work hours suddenly logs in from a different country at an odd time. When it comes to detecting insider threats malicious activity committed by those with authorized access to the network behavioral analysis is extremely useful. AI can identify potential security breaches by tracking trends such as file transfers, access to sensitive data, and login times [25].

AI can dramatically reduce the time needed to mitigate risks by automating responses to identified threats. Without human assistance, automated response systems are able to isolate affected devices, block malicious IP addresses, and initiate incident response procedures to prevent the spread of malware and minimize the impact of cyberattacks. Real-time threat mitigation is essential. Faster reaction times, less work for security staff, and the ability to manage large attacks that may be more than human operators can handle by automating repetitive activities are all advantages of automated response systems. Security professionals can now focus on more complex and strategic aspects of network security due to AI [26].

Organizations proactively combat potential attacks by using historical data to predict future threats. In order to anticipate new malware and attack vectors, predictive analytics involves examining historical security events, threat trends, and system vulnerabilities. AI is used, for example, to analyze the features of past ransomware attacks to spot patterns and predict the emergence of new ransomware strains. By giving businesses insights into potential risks before they become real, predictive analytics helps them stay ahead of hackers. Preventative measures, such as patching vulnerabilities and upgrading security measures, become possible through this proactive strategy, reducing the likelihood of successful attacks.

AI systems use advanced machine learning algorithms to evaluate massive amounts of data and detect real threats with greater accuracy. Because AI systems are better at distinguishing between malicious and non-malicious activity, there are fewer false alarms, allowing security personnel to focus on the real risks. AI can process and analyze massive data sets at much faster speeds than humans. This enables threats to be identified and responded to in real time, which is essential for mitigating the impact of cyberattacks. AI-powered security solutions will remain reliable and effective due to their improved ability to manage and analyze massive amounts of data, giving them a significant advantage over traditional methods [27].

AI-powered security solutions continue to succeed even as the threat landscape changes because AI systems are built to continuously learn from new data and adapt to new threats. By constantly upgrading their knowledge base and adapting to new attack tactics, AI systems with dynamic learning capabilities are able to stay ahead of cyber threats.

Strong security defenses can be maintained by retraining machine learning models with new data, allowing them to identify and respond to new types of attacks. For example, AI systems can quickly incorporate newly identified malware into their detection models, improving their ability to recognize and eliminate similar threats in the future. AI-powered security systems are constantly prepared to deal with the latest cyber threats thanks to their ability to update their threat detection models in response to new attack vectors, providing network environments with consistent and flexible protection [28]. One important benefit of AI is its scalability, especially for large enterprises with extensive network setups. AI systems can easily scale to provide complete protection, but traditional security measures often struggle to meet the demands of large networks. Large-scale networks can be managed and monitored with AI-powered security solutions, ensuring the security of every endpoint without sacrificing functionality. For example, large enterprises and cloud service providers can use AI to protect their large networks from engineers and researchers [29].

AI improves threat intelligence by automating the collection and processing of massive amounts of data from multiple sources, such as security logs, threat feeds, and open-source information. News articles, social media posts, and research papers are examples of unstructured data that can be analyzed by natural language processing (NLP), a branch of AI, to find new threats and vulnerabilities. By continuously collecting and evaluating this data, AI systems provide security teams with actionable insights and the latest threat intelligence, helping them stay ahead of any threats and strengthen network defenses [30].

AI can reduce the human costs associated with cybersecurity operations and eliminate the need for intensive manual analysis and intervention. AI also reduces the financial impact of cyberattacks, including potential penalties, legal costs, and reputational damage, by avoiding breaches and speeding up incident response times. Because of its affordability, AI is a desirable option for companies trying to strengthen their network security posture without having to significantly increase cybersecurity expenses [31].

4.3 Artificial Intelligence Applications in Improving Network Security

4.3.1 Artificial Intelligence Techniques in Detecting Cyber Attacks

When machine learning strategies such as batch normalization, dropout, avoiding overfitting, and increasing training speed were compared, the deep neural network did well in real-time cyber attack detection and classification of unexpected and unpredictable cyberattacks. A Google Tensor Flow framework-based module and the Suricata engine were employed in experiments that used deep learning approaches for data monitoring to analyze cybersecurity concerns in cloud applications. It was suggested to use neural classifiers for network traffic, spam emails, spam comments, and photos. Network security monitoring, integrated intrusion prevention, and real-time intrusion detection are all possible with the Suricata engine [32].

Through the extraction of characteristics from network flows, deep learning techniques have been used to network traffic analysis. Virtual infrastructure (VI), virtual network function (VNF), management and orchestration (MANO), operations, and business support systems make up a high-level cyber security architecture. To accomplish successful network anomaly detection, anomaly symptom detection (ASD) and network anomaly detection (NAD) have been suggested. The monitoring and diagnosis unit is notified as soon as an abnormality is produced from the ensuing traffic. The experimental outcome demonstrates that, depending on the number of network flows gathered from users in real time, the architecture may self-adapt to anomaly detection. One of the major risks impacting gadgets nowadays is botnets [33].

4.3.1.1 Malware Classification

Malware, short for malicious software, refers to any program that aims to damage or take advantage of computer systems. It can take the form of ransomware, Trojans, worms, viruses, and more. With its ability to inflict damage, steal confidential data, and interfere with operations, malware poses a serious risk to both people and businesses. One possible way to combat this problem is to use artificial intelligence to classify malware. AI can evaluate and classify malware based on a number of characteristics, including impact, behavior, and code. As a result, cybersecurity experts may be able to find and eliminate threats faster and more successfully [34].

Any departure from the typical data flow on a network is referred to as unusual traffic. This may be a sign of a distributed denial of service (DDoS) assault or malware infestation, among other cyberattacks. An essential component of preserving network security is recognizing and handling anomalous traffic. The use of AI to the detection of anomalous traffic is one possible way to address this problem. AI is able to examine network traffic and spot trends that can point to a cyberattack effort. This may entail examining the traffic's origin and destination in addition to the data's structure and content. Al may be used in a variety of ways for identifying anomalous traffic. Using machine learning algorithms to examine network data and spot trends that are indicative of cyberattacks is one strategy. To do this, the system may be trained on a sizable dataset of both typical and anomalous traffic, enabling it to identify the traits that set each kind apart.

Using AI to track network traffic in real time is an additional strategy. This may entail installing sensors or other monitoring tools that continuously collect traffic data and notify cybersecurity experts of any deviations from the norm. Prioritizing response to anomalous traffic is another application of AI.

This may entail prioritizing resources for the most important risks and ranking potential threats according to their impact and likelihood. Several studies have been conducted on the application of AI to identify anomalous traffic in the context of cybersecurity. In the Journal of Networking and Computer Applications, one such study looked at how machine learning algorithms can be used to identify and classify anomalous traffic patterns. Comparing AI to traditional rule-based methods, the study found that AI can significantly increase the accuracy of identifying unexpected traffic [34].

typical and dangerous activities, enabling it to pick up the traits that set them apart. Using AI to track system and user activity in real time is an additional strategy. This may entail installing sensors or other monitoring tools that gather activity data continually and notify cybersecurity experts of any departures from the usual. Prioritizing the reaction to dangerous activities is another application of AI. This may entail prioritizing resources for the most significant dangers and ranking the possible threats according to their effect and likelihood [35].

Tracking Unsafe Activity Any conduct that might jeopardize a system's or network's security is considered unsafe. Malware infections, illegal access, and other cyberattacks might fall under this category. An essential component of preserving cyber security is monitoring and dealing with harmful activities. The application of AI to tracking dangerous activities is one possible way to address this issue. AI is able to examine user and system activity and spot trends that could point to a cyberattack effort. This may entail examining user behavior, including the files and websites they access, as well as system stability and speed. AI may be used in dangerous activity tracking in a number of ways.

4.3.2 Artificial Intelligence Methods and Techniques to Improve Network Security

The process of confirming the identity of people trying to access a system or network is known as user access verification. It is critical to maintaining cybersecurity because it protects against unauthorized access and safeguards private information. Applying AI to user access verification is one possible way to address this problem. To confirm whether a person is the intended target, AI can examine their attributes, including login history, system activity, and other elements. This may require applying machine learning algorithms to examine behavioral patterns and detect irregularities that may indicate a cyberattack effort [36].

Python was initially created for programming numerical calculations, but it later expanded into non-specialized fields as a general-purpose programming language alongside more well-known languages like C++ and Java. Python's success can be attributed to a number of factors, including its ease of learning. This makes it one of the artificial intelligence techniques used to protect networks. Compared to other languages like C++ and Java, the language's learning curve is actually less steep, which speeds up the process of both original code modeling and code reorganization. Python makes it easier to write and debug code faults than other languages because of its simple syntax and clean architecture.

Industries require a solution to speed up code prototyping and refactoring since they need to swiftly prototype new features and refactor existing ones without wasting time troubleshooting old code. Application development and testing are significantly accelerated by the ability to write code as a script that can be executed directly from the command line, or even better, in interactive mode, without the need to compile the code into an executable file, object orientation makes it easier to create libraries and APIs with reusable functions, guaranteeing the code's dependability and robustness as well as the abundance of open source libraries that increase programming skills [37].

object orientation makes it easier to create libraries and APIs with reusable functions, guaranteeing the code's dependability and robustness as well as the abundance of open source libraries that increase programming skills. The advantages discussed thus far are reflected in the abundance of high-level function libraries that are freely available to analysts and developers and are supplied by the sizable Python community. The clear language architecture of these function libraries makes it simple to combine them with one another and makes it easier to create APIs that developers may access [38].

Al may be used in user access verification in a number of ways. One method is to authenticate users using biometric information, such fingerprints or face recognition. This may entail installing sensors or other gadgets that gather this information and using it to confirm users' identities. Utilizing AI to examine user behavior while they engage with the system is an additional strategy. This may entail monitoring their activities, including the files they download and the websites they visit, and applying machine learning algorithms to spot behavioral patterns that are characteristic of a genuine user. Additionally, AI may be used to identify and stop cyberattacks that impersonate trustworthy persons. this may entail examining user attributes to identify any departures from the typical pattern, such as odd login times or places [39].

4.3.3 Ways to improve artificial intelligence for network security

Since clustering algorithms are a powerful tool for implementing intelligent separation operations, their use is one way in which AI can enhance network utilization. Clustering or classifying data based on similarities and features is a fundamental function of clustering algorithms. AI and machine learning are widely used in intrusion detection systems (IDS) by commercial enterprises. AI-based honeypots can be exploited by IDS [40].

Monitoring harmful actions and their kinds in real time is essential for achieving cybersecurity with accurate approaches; otherwise, a situation of "emergency medical treatment" would occur, which successfully protects the network but wastes a lot of resources. In order to make the present network needs of intrusion detection systems as scalable as feasible, researchers have started to develop and improve upon the original intrusion detection systems. They have discovered fresh techniques for spotting anomalous activity in dispersed, large-scale networks. In order to identify anomalous patterns, they have employed distributed DBN to lower the dimensionality of a sizable network traffic dataset by combining deep feature extraction with multi-layer integrated support vector machines (SVM). The system has been able to be implemented on numerous devices and has employed artificial neural networks (ANN) technology to identify botnet assaults in addition to network intrusion detection that is improved by hyperparameters based on Al Additionally, they have created a hybrid intrusion detection system that uses cloud computing and machine learning. The SVM classification technique and the K-Means clustering algorithm have been incorporated into the system. Additionally, there was a virtual supervisor-based anomaly detection system that used neural networks as its primary technology.

Honeypots use collaborative networks to catch dangerous actors or malicious users. The honeypot’s computer network reveals itself as open to hackers. When the hacker initiates the attack, it records all the important data for itself, including IP address and location data. The idea of network automation has gained traction since the introduction of AI and machine learning into computer networks. Automation is one of the most important elements of information systems and technology [41].

It enables network engineers and developers to use automation scripts to manage complexity and build the network according to contemporary business needs. These automation technologies also use AI to control network settings. Nowadays, the idea of SD-WAN has gained a lot of traction. Important parts of SD (Software Defined WAN) technologies include vManage, vBond, vSmart, and Edge Nodes. By eliminating the centralized behavior of network devices, the idea of SDWAN was established. Each network device, including firewalls and routers, has its own control plane and data plane. The data plane’s job is to move packets as quickly as possible across the physical interfaces of the network device, while the control plane’s job is to route packets and perform intelligent actions. Apart from routers, SD-based networks consist of two distinct parts. Engineers placed the control plane of the network device at a distance and allowed communication between different parts of the network device [42].

deep learning technology has been created. A recent development in machine learning, a branch of artificial intelligence (AI), is deep learning (DL). Conventional machine learning techniques can only analyze naturally occurring raw data by extracting relevant features, using deep learning to arrange the raw data appropriately, and using classifiers to interpret patterns. Detection or classification A machine learning method called deep learning represents and learns from unstructured or unlabeled data by using knowledge from the human brain [43].

In the machine learning sector, artificial neural networks (ANNs) are utilized for decision-making. An artificial neural network is the concept of a neural network that is biologically inspired by the human brain. Individual neurons or brain cells in the brain are connected by synapses, which enable signal exchange and communication ‹A processing unit made up of linked neurons is used in artificial neural networks ‹this unit can receive input from an external source or the output of another processing unit. The units' output can either be transferred back to itself or to other units ،Weights have an impact on the network's information transformation and unit interconnection. The weight value increases with the degree of effect. The input is deemed unimportant if the weight value is negative. An artificial neural network modifies the weights to produce more accurate results.

Finding unusual traffic is one way to secure a network, as every network has a carrying capacity. When it comes to offering consumers high-quality services, the network might be crucial. Hackers purposefully introduce a lot of illicit data into the network architecture, which renders the nodes and links susceptible to failures, prevents them from offering services to users, and can even result in major issues like data loss. Effective procedures are crucial for enhancing network reaction and maintaining comprehensive cybersecurity when it comes to high-risk activities in cyberspace [44].

Based on the findings of the investigations, it was determined that there are four types of anomalous flow detection techniques: classification-based, statistical, clustering-based, and information-theory-based techniques. This framework can record traffic and forward it to an ANN.

It can be incorporated at various cloud tiers. Deep learning is the foundation of the parallel convolutional cross neural network (PCCN), which is used to detect traffic anomalies in multi-class unbalanced networks. It included many feature fusion techniques and was primarily made up of two simultaneous neural networks. In order to encode network traffic, the networks were created. End-to-end network traffic recognition is the foundation of deep learning. There are two layers to the construction ،Features were extracted using CNN, while time characteristics were recorded using and long short-term memory (LSTM). By enhancing the performance of K-means and SVM approaches in abnormal traffic, artificial intelligence and abnormal traffic detection techniques were enhanced [45].

5. Results

According to the study’s findings, AI has emerged as a crucial tool for improving network security and protecting them from increasingly sophisticated cyberattacks. One of the study’s most notable findings is that compared to traditional technologies, AI has the ability to identify cyberattacks more quickly and accurately. Large amounts of data flowing across the network are analyzed by technologies such as machine learning and deep learning, helping them identify suspicious trends and identify risks early on even before they cause any serious damage. The study also showed that by providing preventive and reactive solutions, AI helps networks better respond to attacks.

The contribution of AI to enhancing network reputation is another important finding from the study. By anticipating various risks and implementing the required preventive measures, advanced algorithms such as “artificial neural networks” and “deep learning” help systems become more adept at identifying anomalous behaviors that may indicate security breaches.

In order to respond quickly to anomalies, these systems continuously examine all network data. According to the study, integrating AI into network security improves an organization’s ability to handle security more skillfully. Systems that use AI can automatically identify security flaws and shorten the time it takes to find and fix them. Additionally, they provide adaptable security plans that can be changed on a regular basis in response to emerging risks or changes in the workplace.

6. Recommendations

It is imperative to continuously improve the use of machine learning and deep learning methods in data analysis and danger detection. The study's findings demonstrated that artificial intelligence, particularly machine learning approaches, helps identify cyberattacks more quickly and precisely than conventional methodologies. In order to evaluate data flow and identify questionable patterns that can point to possible assaults, it is advised that these technologies be incorporated into all network systems. This will assist enterprises in lowering the risks associated with cyberattacks that might cause system interruption or data loss.

Businesses should spend money on enhancing artificial intelligence-based network defenses against attacks. The study demonstrated that by acting quickly to isolate compromised devices or alter protection mechanisms, artificial intelligence may significantly enhance network responsiveness to attacks. As a result, it is advised to create artificial intelligence-based security systems that can react to threats automatically in real time, increasing network resilience to assaults and minimizing possible harm.

The study suggests stepping up efforts to increase network dependability by analyzing network behavior and identifying anomalous activity using artificial intelligence approaches. It is advised to use AI technologies based on deep learning and neural networks to identify any unusual activity that could point to breaches or attack attempts because of their capacity to identify risks in their early phases. By guaranteeing the integrity of networks and increasing trust in them, such technologies can improve the general security of the digital world.

7. Conclusion

The use of artificial intelligence (AI) in boosting network security is increasingly crucial in tackling the expanding difficulties faced by cyber-attacks. AI makes it possible to detect malicious activity, anomalies, and intrusions in network infrastructures more quickly and accurately. Particularly successful methods for spotting suspicious activity, categorizing traffic, and anticipating possible vulnerabilities include machine learning, deep learning, and artificial neural networks

(ANNs). Algorithms like clustering and classification are used by AI-driven systems, such as intrusion detection systems (IDS) and honeypots, to evaluate massive datasets, spot trends, and react to cyberthreats instantly. By reducing the need for human engagement and reaction time, these technologies facilitate quicker threat identification and reduce the likelihood of data breaches. Additionally, AI improves efficiency, scalability, and resilience by automating network management with technologies like Software-Defined Wide Area Networks (SD-WAN) and network automation. Anomaly detection has greatly improved thanks to deep learning techniques like convolutional neural networks (CNNs) and long short-term memory (LSTM) networks, which allow computers to recognize even the smallest and most intricate network anomalies. Organizations may enhance their reaction to high-risk activities, guarantee improved network performance, and uphold strong cybersecurity procedures by employing AI to monitor network data. In conclusion, by improving the capacity to identify and stop threats, maximize network performance, and automate security procedures, artificial intelligence is transforming network security. AI will continue to be an essential tool for protecting networks as cyber threats become more sophisticated, guaranteeing that they can function safely and effectively in a digital environment that is becoming more complicated by the day.

References

[1] Bucha, s. b. (2025). The Role of Artificial Intelligence in Enhancing Data Security and Compliance in Cloud-Based E-Commerce Logistics Integration. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5285038

[2] Yuan, Z. (2025). Analysis of the Role of Artificial Intelligence in Enhancing the Network Security Protection of Renewable Energy Systems. International Journal of High-Speed Electronics and Systems. https://doi.org/10.1142/s0129156425402712

[3] Gharbaoui, O. E., Kiyadi, I. & Boukhari, H. E. (2024). Evaluating AI and ML in Network Security: A Comprehensive Literature Review. Procedia Computer Science, 251. https://doi.org/10.1016/j.procs.2024.11.176

[4] Salem, A. H., Azzam, S. M., Emam, O. & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. Journal of Big Data, 11. https://doi.org/10.1186/s40537-024-00957-y

[5] Jonas, D., Yusuf, N. A. & Zahra, A. R. A. (2023). Enhancing Security Frameworks with Artificial Intelligence in Cybersecurity. Information Technologies in Environnemental Engineering. https://doi.org/10.33050/itee.v2i1.428

[6] Jada, I. and Mayayise, T. O. (2023). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data and Information Management, 8. https://doi.org/10.1016/j.dim.2023.100063

[7] Wang, M., Song, G., Yu, Y. & Zhang, B. (2023). The Current Research Status of AI-Based Network Security Situational Awareness. Electronics. https://doi.org/10.3390/electronics12102309

[8] Oumaima, F., Karim, Z., Abdellatif, E. G. & Mohammed, B. (2022). A survey on blockchain and Artificial intelligence

technologies for enhancing security and privacy in smart environments. IEEE
Access. https://doi.org/10.1109/access.2022.3203568

[9] Dai, D. and Boroomand, S. (2021). A Review of Artificial Intelligence to Enhance the Security of Big Data Systems: State-of-Art, Methodologies, Applications, and Challenges. Archives of Computational Methods in Engineering, 29(2). https://doi.org/10.1007/s11831-021-09628-0

[10] Gupta, N. and Choudhary, N. (2021). Past to Future of Network Security with AI. Advances in intelligent systems and computing. https://doi.org/10.1007/978-981-15-6014-9_43

[11] Wu, H., Han, H., Wang, X. & Sun, S. (2020). Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey. IEEE
Access. https://doi.org/10.1109/access.2020.3018170

[12] Abidin, S. (2018). Enhancing Security in WSN by Artificial Intelligence. Lecture notes on data engineering and communications technologies. https://doi.org/10.1007/978-3-030-03146-6_93

[13] Bessiere, C. (2020). Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence, IJCAI 2020. . https://hal-lirmm.ccsd.cnrs.fr/lirmm-03379779/document

[14] Amisha, P. M., Pathania, M., & Rathaur, V. K. (2019). Overview of artificial intelligence in medicine. Journal of family medicine and primary care, 8(7), 2328.

[15] Rajaraman, V. (2014). JohnMcCarthy-Father of artificial intelligence. Resonance, 19(3). https://doi.org/10.1007/s12045-014-0027-9

[16] Matyushok, V., Михайлович, M. B., Krasavina, V., Александровна, K. B., Matyushok, S. V. & Владимирович, M. C. (2020). Global artificial intelligence systems and

technology market: formation and development trends. , 28. https://doi.org/10.22363/2313-2329-2020-28-3-505-521

[17] D. B. Fogel. (1995), Review of computational intelligence: Imitating life, Proc. of the IEEE, 83(11)

[18] Craglia M. (Ed.), Annoni A., Benczur P., Bertoldi P., Delipetrev P., De Prato G., Feijoo C., Fernandez Macias E., Gomez E., Iglesias M., Junklewitz H, López Cobo M., Martens B., Nascimento S., Nativi S., Polvora A., Sanchez I., Tolan S., Tuomi I., Vesnic Alujevic (2018) L., Artificial Intelligence A European Perspective, EUR 29425 EN, Publications Office, Luxembourg, , ISBN 978-92-79-97217-1, doi:10.2760/11251, JRC113826

[19] Nilsson, N. J. (2009). The quest for artificial intelligence. Cambridge University Press.

[20] Romaniuk, S., & Burgers, T. (2018). How China's AI Technology Exports Are Seeding Surveillance Societies Globally. The Diplomat, 18.

[21] Ng. A. Y., & Jordan, M. 1. (2002). Oп Discriminative vs. Generative Classifiers: A Comparison of Logistic Regression and Naive Bayes. Advances in Neural Information. Processing Systems, 14

[22] Chandola, V., Banerjee, A., & Kumar, V. (2009), Anomaly Detection: A Survey. ACM Computing Surveys, 41(3), 1-58.

[23] Fang, L., & Li, Q. (2021). Natural Language Processing in Cybersecurity: A Survey, IEEE Access, 9, 139843-139863.

[24] Symantec. (2023). Internet Security Threat Report. Retrieved https://www.symantec.com/security- center/threat-report

[25] McAfee. (2023). Advanced Threat Research Report. Retrieved https://www.mcafee.com/enterprise/en- from us/threat-center/advanced-threat-research.html

[26] Kaspersk، (2023). Future of Cybersecurity: Predictive Analytics. Retrieved from

https://www.kaspersky.com/resource-center/threats/predictive-analytics-cybersecurity

[27] Verizon. (2023). Data Breach Investigations Report. Retrieved from https://www.verizon.com/business/resources/reports/dbir/

[28] McAfee. (2023). Advanced Threat Research Report. Retrieved https://www.mcafee.com/enterprise/en-fromus/threat

[29] Gartner. (2023), Top Security and Risk Management Trends. Retrieved from https://www.gartner.com/en/documents/398703 8/top-security-and-risk-management-trends

[30] Fang, L., & Li, Q. (2021), Natural Language Processing in Cybersecurity: A Survey, IEEE Access, 9, 139843-139863

[31] Deb, D., Bhattacharya, P., & Maiti, A. (2022), Artificial Intelligence in Cybersecurity: Threats and Challenges, Journal of Information Security and Applications, 66, 102914.

[32] H., Benmeziane. (2020), Comparison of of deen deep learning frameworks and compilers, M.S, thesis Comput. Sci., Inst. Nat. Formation Informatique, École nationale Supérieure d'Informatique, Oued Smar, Algeria.

[33] S.A. Salloum, M. Alshurideh, A. Elnagar, and K. Shaalan, (2020), Machine Learning and Deep Learning Techniques for Cybersecurity: A Review, Advances in Intelligent Systems and Computing, pp. 50-57.

[34] D. Edch,(2021), Network intrusion detection system using deep learning technique, www.utupub.fi, Accessed: Available: https://tinyurl.com/ywhvx2sy.

[35] Zangana, H. M. and Zeebaree, S. R. M. (2024). Distributed Systems for Artificial Intelligence in Cloud Computing: A Review of AI-Powered Applications and Services. International Journal of Informatics Information System and Computer Engineering

(INJIISCOM), 5(1). https://doi.org/10.34010/injiiscom.v5i1.11883

[36] M. Lukehart, (2022), Cyber Attack Statistics, Data, and Trends Parachute, Parachute, https://parachute.cloud/cyber- attack-statistics-data-and-trends

[37] G. Kumar, K. Kumar, and M. Sachdeva, (2010), The use of artificial intelligence-based techniques for intrusion detection: a review," Artificial Intelligence Review, vol. 34, no. 4, pp. 369-387,

[38] Frank Buschmann Alejandro P. Buchmann Mariano A. Cilia (2003), Object-Oriented Technology, Darmstadt, Germany, LNCS 3013

[39] Shoroog Albalawi, (2022), A Comprehensive Overview on Biometric Authentication Systems using Artificial Intelligence Techniques

[40] Salim El khediri, (2024), Integration of artificial intelligence (AI) with sensor networks: Trends, challenges, and future directions, Volume 36, Issue 1

[41] R. Ross, V. Pillitteri, K. Dempsey, M. Riddle, and G. Guissanie, (2020), Protecting controlled unclassified information in nonfederal systems and organizations.

[42] Dongmei Z, Jinxing L. (2018), Study on network security situation awareness based on particle swarm, IEEE Trans Pattern Anal Mach Intell 40(4):1002-1014, optimization algorithm. Comput Ind Eng 125:764-775.

[43] Yegnanarayana, B., (2006), Artificial neural networks. Available: https://tinyurl.com/y56j8s39

[44] Ahmed M. Mahmood AN, Hu J, (2015), A survey of network anomaly detection techniques. J. Netw. Comput. Appl. 60:19-31 Aljamal I.

[45] Dongmei Z, Jinxing L. (2018), Study on network security situation awareness based on particle swarm optimization algorithm. Comput Ind Eng 125:764-775.

9

Wireless Communication between Air-Station (Airship) and the local Station using Arduino Uno and nRF24L01 Transceivers

Wireless Communication between Air-Station (Airship) and the local Station using Arduino Uno and nRF24L01 Transceivers

Abdellfatah Gh. Shibani Amar
Libyan Center of Electronic Systems and Programming and Aviation Science
Tripoli-Libya
Electric & Electronic Department /Faculty of Engineering
Karabuk University
Karabuk-Turkey
amar72850@yahoo.com

Elaheh Yaghoubi Elnaz Yaghoubi
Electric & Electronic Department /Faculty of Engineering
Karabuk University
Karabuk- Turkey
elahe.yaqubi@gmail.com

Abstract

This paper presents a comprehensive study on the implementation of a wireless communication system between two Arduino Uno microcontroller using NRF24L01 transceivers module. The motivation for this task comes from the need for low power, cost -effective and reliable communication methods suitable for built -in systems on the scientific research airship developed at the Libyan Center of Electronic Systems and Programming and Aviation Science. The study includes both theoretical and practical aspects, including hardware integration, challenges for power control and software protocol design, and the RF signal stability signal propagation characteristics were analyzed using theoretical RF models and real tests. The results show a consistent PDR above 95% in line-of-sight conditions and acceptable latency for real-time data transmission. Conclusions validate the suitability of mild airborne platforms of NRF24L01 and provides a basis for future improvement as mesh networking, extended range, and interference mitigation.

Keywords: Embedded systems, Arduino Uno, nRF24L01 transceiver, RF signal.

1. Introduction

The integration of wireless communication systems into embedded platforms is essential for modern scientific and industrial applications, especially those that include mobiles or air platforms such as drones and airships. In the environments where the cable layout is impractical or undesirable, which is undesirable due to weight loss or dynamic mobility, the radio frequency (RF) modules provides an effective alternative. Such a module, NRF24L01+ transceiver, has gained popularity for easy integration with microcontrollers such as the low cost, the low power consumption and the Arduino Uno [1],[2],[3].

Airships used for scientific examination - such as atmospheric sensing, environmental monitoring or air mapping - require communication systems on board to forward data from distributed sensors to a central processor or ground station. Given their large physical structure, communication design between platforms through the cable can introduce complications, mechanical stress and indication falls. A compact and strong wireless system not only reduces the wires, but also increases modularity and fault tolerance[4].

NRF24L01+, operating in the 2.4 GHz ISM band, supports data rates up to 2 Mbps and has a convenience with automatic package recognition, retransmission and many data pipe support [2].

These functions suitable for real -time data exchange in embedded systems where energy efficiency and reliability are important. Arduino Uno based on the ATMEGA328P Microcontroller [5] provides a reliable and accessible platform to integrate such wireless solutions [3].

In contrast, Wi-Fi-based communication modules, such as the ESP8266 or ESP32, provide significantly higher data rates (up to 150 Mbps in 802.11n), underlying TCP/IP stacks, and greater interoperability with internet-based systems [6]. They come at the expense of higher power consumption, greater electromagnetic interference, and more complex configuration.

For example, the ESP8266 draws up to 250 mA during peak transmission, which is unsuitable for mild or battery competition platform [6].

Wi-Fi network dynamic channels show delay variability due to dynamic channel dialog, encryption overhead and access point-violence. These factors make Wi-Fi less suitable for low-latency, usually in real-time built-in systems require determined communication. On the other hand, the NRF24L01 module provides a direct peer-to-peer link to a router or a DHCP configurations, making them ideal for short-range, low power intra- airship communication[7], [8].

Prior research has shown viability of the wireless sensor network and the NRF24L01 module in robotics [5]. For example, Mahmoud evaluated [7] the packet delivery ratio (PDR) to NRF24L01-based links in the industrial and external environment, and confirmed their strength in case of low intervention. Corresponding Chain et al. [8] used nRF24L01 in a distributed sensor system for environmental monitoring, showing its utility for transmitting small, periodic data packets efficiently.

Scientific platforms for aerial as airships as applications are unlocked. These platforms present unique RF challenges, including signal temping due to height, onboard noise from engine controllers and interference from the metal airship envelope. In addition, the power supply design for the airborne embedded systems should ensure clean, stable 3.3 V output for RF modules, as small fluctuations can also cause significant communication errors [5].

This study addresses these challenges by implementing and evaluating a wireless communication connection between two Arduino Uno units using NRF24L01+ transceiver. The application is designed for the built-in control and sensing system of a research airship operated by the Libyan Center of Electronic Systems and Programming and Aviation sciences. The work includes hardware design, power conditioning, implementation of communication protocol and performance assessment under real -world conditions. Experimental data on packet delivery, latency, and signal integrity are compared against theoretical propagation models to validate the system’s performance.

2. Materials and Methods

2.1. Components and Specifications:

- Arduino Uno (ATmega328P): 16 MHz clock speed, 2 KB SRAM, 32 KB Flash memory.
- nRF24L01: 2.4 GHz ISM band transceiver, up to 2 Mbps data rate, 125 channels, SPI interface.

- Capacitors: 10 µF electrolytic capacitors for power stabilization
- Breadboards and jumper wires.

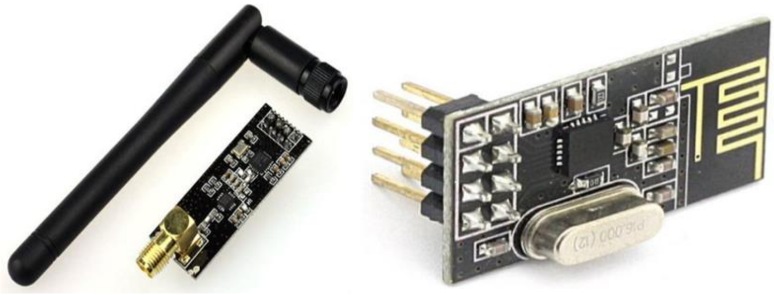


Figure I: Transceiver nRF24L01

2.2. Circuit Schematic

The hardware configuration adheres to the SPI communication protocol:

- CE → Arduino pin 9
- CSN → Arduino pin 10
- SCK → Arduino pin 13
- MOSI → Arduino pin 11
- MISO → Arduino pin 12
- VCC → 3.3V (strictly regulated)
- GND → GND

The capacitor is located between the VCC and the GND pins of the NRF24L01 to suppress the voltage spikes and ensure the power stability. The voltage regulation is critical due to the module's sensitivity to power fluctuations.

2.3. Software Tools

- Arduino IDE (version 1.8.19)
- RF24 library by TMRh20 (version 1.4.2)
- Serial Monitor and RealTerm for serial communication analysis

2.4. Communication Protocol

The nRF24L01 uses Enhanced ShockBurst™, a proprietary protocol supporting automatic acknowledgments (ACK), CRC error detection, and packet retransmission. The module can transmit up to 32-byte payloads with hardware-managed FIFOs. In this implementation, a fixed 5-byte address (“00001”) is used. Dynamic payloads and auto-acknowledgment are disabled to simplify timing analysis.

2.5. Power Consumption Analysis

Power consumption was measured under different operating modes:

- TX Mode (0 dBm): ~11.3 mA
- RX Mode: ~12.3 mA
- Standby-I: ~26 µA
- Power Down: ~900 nA

3. Implementation

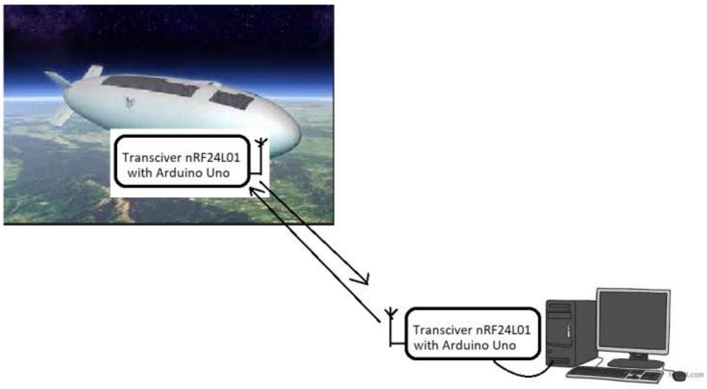


Figure II: The communication between Air-Station (Airship) and Local Station

3.1 Practical Circuit Design

To ensure stable operation of the nRF24L01 transceivers with Arduino Uno, careful attention must be paid to wiring, power regulation, and signal integrity.

3.1.1 Basic Circuit Schematic

The following is the standard pin mapping between the **Arduino Uno** and **nRF24L01** module:

nRF24L01 Pin	Arduino Uno Pin	Description
VCC	3.3V	Power supply (Do **not** use 5V)
GND	GND	Ground
CE	D9	Chip Enable (RF control)
CSN (CS)	D10	Chip Select Not (SPI control)

nRF24L01 Pin	Arduino Uno Pin	Description
SCK	D13	SPI Clock
MOSI	D11	SPI Master Out Slave In
MISO	D12	SPI Master In Slave Out
IRQ	Not Connected	Interrupt (optional)

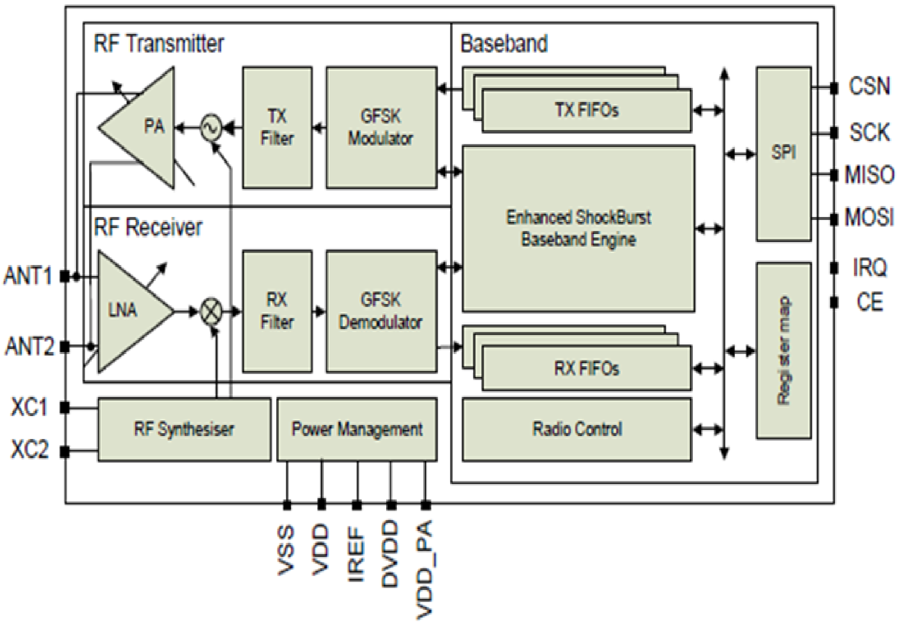


Figure III: Block diagram of Transceiver nRF24L01

Important Note:

The nRF24L01 is **sensitive to power supply noise**. An electrolytic capacitor (10µF or higher) is placed across VCC and GND as close as possible to the module to stabilize voltage levels and filter out transients.

3.1.2 Power Considerations

- The nRF24L01 module draws up to **115 mA during transmission**.
- Arduino Uno’s onboard 3.3V regulator **cannot supply this reliably**.
- Use one of the following methods for reliable power:
  - **External AMS1117-3.3V** regulator module with adequate heat sinking.
  - **Dedicated 3.3V LDO regulator** like MCP1700 or LD1117 with input filtering (0.1µF and 10µF capacitors).
  - For high-power (PA+LNA) modules: recommend powering via a **separate 3.3V regulator** with at least 250 mA output capacity.

3.1.3 Full Circuit Example (Sender and Receiver)

Sender (onboard sensor node in the airship):

- Arduino Uno with nRF24L01 connected via SPI
- Simulated sensor input (temperature via analog pin)
- Power via external 3.3V regulator

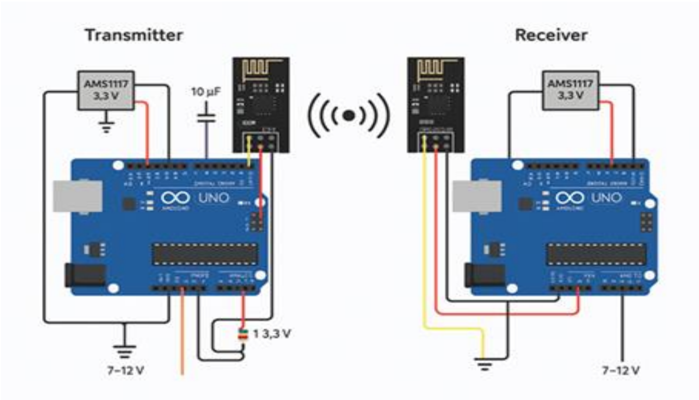


Figure IV: Connection of Transceiver with Arduino

Receiver (ground station):

- Arduino Uno with identical nRF24L01 setup
- Serial output to PC via USB or serial LCD display

3.1.4 PCB and Breadboard Layout Tips

- Use **short wires** for SPI lines to minimize EMI.
- Keep **CE and CSN** lines away from high-current traces.
- Add a **0.1µF ceramic capacitor in parallel** with the 10µF electrolytic for high-frequency noise filtering.
- On custom PCB: provide ground plane beneath nRF24L01 and ensure trace impedance is minimized.

3.1.5 Optional Enhancements

- **Add an LED** to indicate packet transmission and reception success.
- **Include a push button** on the transmitter to trigger a message.
- **Use external antennas** on PA+LNA modules for better range testing.

4. Results

4.1. Signal Range and Packet Delivery

Testing was performed indoors with varying levels of interference. Signal range was measured using RSSI estimation techniques and packet delivery ratio (PDR):

- 5 m LOS: 100% PDR
- 10 m LOS: 95% PDR
- 15 m NLOS (1 wall): 85% PDR
- 20 m NLOS (2 walls): 65% PDR

4.2. Latency Measurements

Round-trip time (RTT) was estimated using loopback ACK in an extended test:

- Average RTT at 2 Mbps: ~2.1 ms
- Average RTT at 250 kbps: ~4.8 ms

5. Discussion

The experimental results confirm that the nRF24L01 is a suitable module for short-range communication with Arduino. Performance degrades with physical barriers and RF noise. Enhancements such as directional antennas, signal repeaters, or alternative modulation schemes (e.g., frequency hopping) can improve reliability. This configuration is particularly suitable for low-data-rate applications such as environmental monitoring or control systems.

Experimental results confirm that NRF24L01 is a suitable module for short distance communication with Arduino. Demonstration with physical obstacles and decreases with RF noise. Instructions can improve reliability, This configuration is particularly suitable for low-data-rate applications such as environmental monitoring or control systems.

This configuration is particularly suitable for low data-of applications such as environmental monitoring or control systems.

6. Conclusion

The study reflects the successful implementation of wireless communication between two Arduino UNO boards using NRF24L01 transceivers. Through carefully hardware integration and configuration of the RF24 library, the modules were able to exchange data within a medium indoor range. Experimental results are valid that the system improves in scenarios with Line-off-Sight scenarios, with an acceptable decline in the presence of general indoor obstacles. NRF24L01 transceiver is a practical solution for low -power wireless communication in embedded systems, which offers features such as configurable data rates, receipt management and low power. Including power stabilization measures, such as decoupling capacitors and regulated power sources, signal reliability and the life of the module significantly.

This implementation acts as a basic model for wireless sensor networks, external data login system and further development of IoT nodes. Future work can involve integration with cloud platforms for configuration of multiple nodes, real -time telemetry, error improvement schemes and extended functionality

References

[1] M. Engquist and S. Bethdavid, ‘Communications solution for refugee settlement Investigation of nRF24L01+ modules for use in a communications network’, 2018, [Online]. Available: http://www.teknat.uu.se/student

[2] S. Suradi, A. Hanafie, and S. Satriani, ‘Perancangan Sistem Monitoring Temperatur Ruangan Berbasis Short Message Service Menggunakan Arduino Nano’, *ILTEK J. Teknol.*, vol. 13, no. 02, pp. 1976–1983, 2018, doi: 10.47398/iltek.v13i02.372.

[3] S. Clara and C. Ca, ‘Hi-Rel Operations Radiation Engineering / RHA Programs Low Dose Rate (LDR) Biased & Unbiased Condition Testing National Semiconductor Precision Micropower Shunt Voltage Reference’, 2010.

[4] Q. Bi, G. I. Zysman, and H. Menkes, ‘Wireless mobile communications at the start of the 21st century’, *IEEE Commun. Mag.*, vol. 39, no. 1, pp. 110–116, 2001, doi: 10.1109/35.894384.

[5] S. O. O. Abdelrahim, M. Z. M. Hassan, A. M. S. Salih, A. A. M. Abdo-Alrahiem, and M. Abdelgadir Mohamed, ‘RF performance evaluation of the nRF24L01+ based wireless water quality monitoring sensor node: Khartoum city propagation scenario’, *J. Electr. Syst. Inf. Technol.*, vol. 9, no. 1, 2022, doi: 10.1186/s43067-022-00052-3.

[6] A. Bensky, ‘and Applications’.

[7] Recommendation ITU-R P.1411-9, *Propagation data and prediction methods for the planning of short-range outdoor radiocommunication systems and radio local area networks in the frequency range 300 MHz to 100 GHz*, vol. P, no. 1411–9. 2017. [Online]. Available:

http://www.ncbi.nlm.nih.gov/pubmed/23463403

[8] R. Sui and J. Baggard, ‘Wireless sensor network for monitoring soil moisture and weather conditions’, *Appl. Eng. Agric.*, vol. 31, no. 2, pp. 193–200, 2015, doi: 10.13031/aea.31.10694.