Defence Science Journal, Vol. 75, No. 2, March 2025, pp. 243-249, DOI : 10.14429/dsj.20464

Vessel Trajectory Route Spoofed Points Detection Using AIS Data: A Bi-LSTM Approach

Nitish Raj[!,*] and Prabhat Kumar[#]

[!]*Weapons and Electronics System Engineering Establishment, Delhi - 100 66, India*
[#]*National Institute of Technology, Patna - 801 503, India*
[*]*E-mail: raj.nitp@gmail.com*

ABSTRACT

The Automatic Identification System (AIS), which provides real-time vessel information for collision avoidance and marine domain awareness, is vital to maritime navigation and safety. However, AIS is vulnerable to GPS spoofing attacks, where malicious actors transmit false GPS signals to mislead vessels about their location. These attacks pose significant risks to maritime safety and security. In this paper, a novel approach to detect spoofed points within vessel trajectory routes using AIS data is proposed. The methodology leverages the power of Bidirectional Long Short-Term Memory (Bi-LSTM) networks, a deep learning architecture adept at capturing temporal dependencies in sequential data. By analysing AIS data streams, the proposed model identifies anomalies and deviations from expected patterns, effectively pinpointing instances of spoofing. Numerous tests using real-world AIS datasets were carried out, which showed that the suggested Bi-LSTM model outperformed other spoofing detection techniques. The work advances the realm of marine cybersecurity by offering a more reliable and accurate method of AIS spoofing attack detection.

Keywords: Ship trajectory prediction; Neural network; Automatic identification system, Spoofing points detection

NOMENCLATURE

M : Bi-LSTM model
D : AIS data set
F : Feature vector
τ : Classification threshold value

1. INTRODUCTION

The Automatic Identification System (AIS) has revolutionized maritime navigation and safety. It mandates vessels to broadcast their position, course, speed, and other vital information, enabling real-time tracking and enhancing situational awareness. However, the reliance on GPS for AIS positioning exposes a critical vulnerability: GPS spoofing Jafarnia-Jahromi[1], *et al.* Spoofing attacks involve the transmission of false GPS signals, manipulating a vessel's reported position and potentially leading to catastrophic consequences, such as collisions, grounding, or intentional misdirection for illicit activities.

The accurate and timely detection of spoofed AIS data is paramount for ensuring maritime safety and security. Traditional methods, often based on rule-based systems or statistical analysis, have limitations in detecting sophisticated spoofing attacks that mimic normal behaviour. Therefore, there is a pressing need for advanced techniques that can effectively identify subtle anomalies in AIS data streams, signalling potential spoofing activity.

Received : 06 August 2024, Revised : 09 December 2024
Accepted : 31 December 2024, Online published : 24 March 2025

This research presents a novel approach to handle this difficulty by utilizing the capabilities of Bidirectional Long Short-Term Memory (Bi-LSTM) networks. Recurrent neural networks (RNNs), such as bi-LSTM networks, are made to process sequential data in both forward and backward directions. This bidirectional capability allows them to capture dependencies not only from past inputs but also from future inputs, making them well-suited for analysing AIS data, where the context of surrounding messages is crucial for identifying spoofing.

2. LITERATURE REVIEW

Anomalies in maritime AIS data pose significant challenges to maritime safety and security. Research over the years has explored various methods to detect and address these anomalies effectively. In their 2012 study, Jafarnia-Jahromi[1], *et al.* reviewed the vulnerabilities of GPS to spoofing threats and discussed various anti-spoofing techniques. They provided a comprehensive overview of methods to enhance GPS robustness, including cryptographic approaches and signal authentication. Recent reviews by Wolsing[2], *et al.* have examined the evolving approaches to anomaly detection in maritime AIS tracks. Their work highlighted the use of statistical models and machine learning techniques to detect outliers and anomalous behaviours, emphasizing the need for continuous advancements in detection methodologies.

A practical approach for real-time anomaly detection was proposed by Brandsæter[3], *et al.* They focused on

integrating machine learning techniques, such as clustering and classification algorithms, into operational ship systems, demonstrating how these methods can enhance safety through effective online monitoring.

Yan[4], *et al.* developed a behaviourally-based approach to ship categorization and anomaly detection using space-borne AIS data. Their approach involved feature extraction and classification techniques to analyse ship behaviours and identify anomalies, showcasing the benefits of spaceborne data in maritime security.

The detection of anomalies in ship movements was further advanced by Liu[5], *et al.* through their work on specialized distance measures. Their method, presented at the 18th International Conference on Information Fusion, employed tailored distance metrics to identify deviations in ship trajectories. Rong[6], *et al.* explored data mining techniques for characterizing shipping routes and detecting anomalies based on AIS data. By applying clustering and statistical analysis methods, they identified patterns and outliers in maritime trajectories, highlighting the effectiveness of data mining in anomaly detection.

A novel context-aware approach for anomaly detection was introduced by Pedroche[7], *et al.* Their method, published in Neurocomputing, involved learning contextual information from ship trajectory clusters to improve detection accuracy, demonstrating the advantages of context-aware models.

Xie[8], *et al.* created a technique for trajectory-based anomaly detection that is specific to ship behaviour trajectories. Their approach, featured in Ocean Engineering, utilized trajectory analysis and machine learning to detect anomalies, emphasizing the value of behavioural patterns in identifying deviations.

The integration of clustering with anomaly detection was showcased by Zhang[9], *et al.*. Their novel method combined clustering algorithms with anomaly detection techniques to analyse ship trajectories, presenting a sophisticated approach to maritime safety.

A novel satellite-ship communication system with deep learning for anomaly detection was proposed by Wu[10], *et al.* in 2024. Their work, published in Multimedia Tools and Applications, combined satellite communication with advanced deep-learning algorithms to enhance detection capabilities in maritime contexts.

Gaussian process active learning for marine anomaly detection was demonstrated by Kowalska[11], *et al.* at the 15th International Conference on Information Fusion. Their method focused on improving detection accuracy through active learning, showcasing the potential of Gaussian processes in this field.

A comprehensive statistical framework for detecting AIS spoofing and abnormal deviations was presented by d'Afflisio[12], *et al.*. Their work, featured in IEEE Transactions on Aerospace and Electronic Systems, utilized statistical models to identify malicious and stealth anomalies, emphasizing the need for robust statistical techniques.

Kobayashi[13], *et al.* used moving-baseline analysis and multipath monitoring to address spoofing detection on ships. Their method, discussed at the ION GNSS+ 2020 conference, employed advanced signal processing techniques to detect spoofing, illustrating the use of multipath signals in anomaly detection. Zheng[14], *et al.* introduced a statistical learning approach to detect abnormal ship trajectory points. Their method utilised statistical models to identify deviations, contributing to the advancement of statistical learning in maritime anomaly detection.

Finally, Liang[15], *et al.* articulated an unsupervised method for maritime anomaly detection using AIS data. Their method employed unsupervised learning techniques to detect anomalies without labelled data, showcasing the potential of unsupervised methods in this domain.

While these existing methods offer valuable insights into AIS data analysis and anomaly detection, they have limitations in effectively detecting spoofed points in vessel trajectories. The proposed Bi-LSTM-based methodology aims to overcome these limitations by incorporating bidirectional processing to capture both past and future dependencies, enabling more accurate and robust detection of spoofed points.

3. METHODOLOGY

The proposed methodology for maritime anomaly detection involves several key stages: dataset acquisition, pre-processing and cleaning, data augmentation, modelling, and classification. The same has been architect and shown in Fig. 1. These stages are explained in the subsequent sub-section of this section.

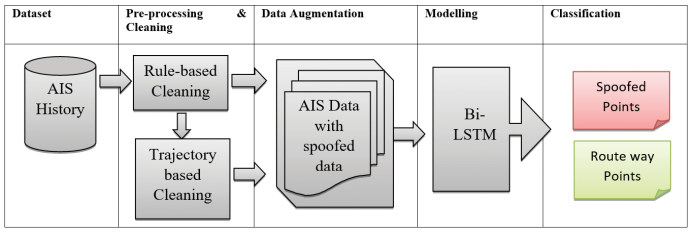

Figure 1. Architecture for detecting spoofing points in maritime trajectories.

3.1 AIS Data Preprocessing

The AIS data preprocessing as described in Algorithm 1, stage involves several crucial steps:

3.1.1 Data Collection

AIS messages are collected from historical AIS databases from source[16]. The dataset, sourced from the Marine Cadastre platform, includes data from diverse maritime regions and vessel categories to ensure representativeness and reduce sample bias.

3.1.2 Data Augmentation

AIS messages were augmented with spoofed points which have classical cases off-the-course, track-deviation, and CPA approaches.

3.1.3 Data Cleaning

The raw AIS data is cleaned to remove noise, outliers, inconsistencies, and duplicate messages. Filtering techniques may be applied to ensure data quality and reliability. Rule-based cleaning such as COG does not exceed 360. SOG should

not impart beyond 100 Knots, etc domain specific range checks have been applied.

3.1.4 Feature Extraction

Relevant features are extracted from the AIS messages. These features typically include:

- Vessel geographical (Lat and Long)
- position
- Course over ground (COG)
- MMSI ID (vessel identification information)
- Timestamp
- Speed over ground (SOG)

3.1.5 Feature Scaling

The extracted features are normalized or standardized to ensure that they are on a similar scale, which is important for the subsequent model training process.

Algorithm 1: AIS Data Preprocessing

Input*: Raw AIS data (lat, lon, SOG, COG, ts, MMSI)*
Output*: Pre-processed AIS data (D_train, D_test)*

1. *D <- Collect raw AIS data (lat, lon, SOG, COG, ts, MMSI)*
2. *D_clean <- clean_data(D)*
3. *F <- extract_features(D_clean)*
4. *F_norm <- normalize(F)*
5. *D_train, D_test <- train_test_split(D_clean)*

3.2 Bi-LSTM Model Architecture

The suggested approach for identifying spoofed AIS messages is based on the Bi-LSTM model design. Recurrent neural networks (RNNs) that process data in both forward and backward directions are called bi-LSTM networks. This feature allows the model to incorporate dependencies from inputs that come from the past and the future. This bidirectional capability is crucial for analysing AIS data, where the context of surrounding messages is essential for identifying spoofing. Algorithm 2 is presented for the building and execution steps of the Bi-LSTM model.

3.2.1 Model Layers

3.2.1.1 Input Layer

Receives pre-processed AIS features as input.

3.2.1.2 Bi-LSTM Layers

Processing of the input sequence is done both forward and backward by many Bi-LSTM layers. Two LSTM layers, one for each direction, make up each Bi-LSTM layer. The forward LSTM layer processes the input sequence from start to finish, while the backward LSTM layer processes it from end to start. The model can incorporate dependencies from both past and future inputs because of this structure.

3.2.1.3 Dense Layers

One or more dense layers may be added after the Bi-LSTM layers to further process the extracted features.

3.2.1.4 Output Layer

Produces a probability score indicating the likelihood of an AIS message being spoofed.

3.2.2 Model Compilation and Training

Bi-LSTM model requires vast computation, experiments were conducted using a high-end system with an NVIDIA RTX 3080 GPU, 32 GB RAM, and an Intel Core i7 (8th Generation) processor, ensuring optimal performance during training and inference. While the training phase was computationally intensive, it was performed offline to adjust model parameters without affecting real-time performance. For real-time implementation, the inference phase was optimized by batching input data and utilizing parallel processing to improve speed and accuracy, enabling timely anomaly detection and predictions. The model is built using the Adam optimizer and the binary cross-entropy loss function. The binary cross-entropy loss function is suitable for binary classification tasks, and the Adam optimizer is chosen because of its efficiency and ability to alter the learning rate. Early stopping is used to monitor the validation loss and prevent overfitting by terminating the training process if the validation loss does not improve after a predefined number of epochs (patience).

3.2.3 Model's Hyperparameters Tuning

To maximize the proposed model's performance of Bi-LSTM, hyperparameter adjustment is necessary. The number of Layers, LSTM units, batch size, learning rate, and the number of epochs are the main hyperparameters.

3.2.3.1 Number of LSTM Units

The dimensionality of the output space is determined by the number of LSTM units. Although the model may capture more complicated patterns with a bigger number of units, overfitting is also more likely.

3.2.3.2 Number of Layers

The number of layers increases the danger of overfitting and computational complexity, but it can also capture more complicated characteristics.

3.2.3.3 Learning Rate

Regulates the gradient descent step size. Although it might take more epochs, a lower learning rate can result in greater convergence.

3.2.3.4 Batch Size

The quantity of samples processed before updating the internal parameters of the model. More memory is needed for smaller batch sizes, but the gradient can be estimated more accurately.

3.2.3.5 Epochs

The number of epochs specifies how many times the training dataset will be run through by the learning algorithm. By ending training as soon as the model's performance on the validation set ceases becoming better, early stopping can aid in the prevention of overfitting.

Table 1. Hyperparameter tuning

Hyperparameter	*Values explored*	*Final value*
LSTM units	30, 62, 128	*62*
Batch size	16, 30, 62	*30*
Learning rate	0.004, 0.01, 0.1	*0.004*
Epochs	20, 50, 100	*50*

Table 1 summarises the hyperparameter values explored during the tuning process and indicates the final selected values.

The hyperparameter values were chosen based on a balance between model performance and computational efficiency. For LSTM units, a value of 62 was selected after testing 30 and 128, as it provided the best trade-off between model complexity and overfitting, capturing the necessary temporal patterns without excessive computational cost. The batch size of 30 offered an optimal balance, ensuring stable gradient updates and efficient training without the instability observed with smaller batch sizes or the high memory demand of larger ones. The learning rate of 0.004 was chosen for its ability to provide stable convergence, avoiding the issues of slow learning with lower rates and instability with higher rates. Finally, 50 epochs were selected as the optimal number, as extending to 100 led to overfitting, while 50 epochs allowed for sufficient training without compromising generalisation.

Algorithm 2: Bi-LSTM Model Architecture

Input: Pre-processed AIS features (F_norm)
Output: *Compiled Bi-LSTM model (M)*

1. *M <- Sequential()*
2. *M.add(Bidirectional(LSTM(62, return_sequences=True)))*
3. *M.add(Bidirectional(LSTM(30)))*
4. *M.add(Dense(1, activation='sigmoid'))*
5. *M.compile(loss='binary_crossentropy', optimizer='adam', metrics=['accuracy'])*
6. *early_stopping <- EarlyStopping(monitor='val_loss', patience=p)*
7. *M.fit(D_train, epochs=e, batch_size=b, validation_split=v, callbacks=[early_stopping]))*

3.3 SPOOFING DETECTION

Once the Bi-LSTM model is trained, it can be used to detect spoofed points in vessel trajectory routes. The process involves the following steps:

3.3.1 Anomaly Score Calculation

For each AIS message in a trajectory, the model calculates an anomaly score based on the deviation of the message from the expected pattern. This anomaly score represents the probability that the message is spoofed.

3.3.2 Threshold Determination

In determining the optimal threshold value τ for detecting spoofed AIS messages, a value of 0.6 was chosen based on a combination of empirical evaluation and practical considerations. This threshold was established through extensive testing and validation on a dedicated dataset, where various threshold values were assessed to identify the most effective balance between detection accuracy and false positive rates. The choice of 0.6 reflects a pragmatic approach, optimizing the F1-score—a metric that balances precision and recall—to ensure robust detection of spoofed messages while minimizing errors. Thresholds ranging from 0.2 to 0.8, with intervals of 0.1, were systematically tested, and a value of 0.6 was chosen as it optimized the F1-score, balancing precision and recall for robust and reliable spoofing detection. In the maritime domain, where the safety implications of spoofed AIS messages are significant, this conservative threshold helps to ensure that potential spoofing incidents are not overlooked, even if they result in a higher number of false positives. This approach aligns with best practices and expert recommendations, prioritizing safety and reliability in maritime navigation and security.

3.3.3 Classification

If the anomaly score of an AIS message exceeds the threshold, it is classified as spoofed; otherwise, it is classified as genuine.

3.4 Anomaly Score Calculation

Using the trained Bi-LSTM model, the anomaly score for every AIS message is determined. Based on the model's understanding of normal vessel behaviour, the score reflects the likelihood of the message being spoofed. The formula for the anomaly score s_i of an AIS message $\boldsymbol{i}$ is given by:

$$s_i = M(Fi)$$

where $\boldsymbol{M}$ is the trained Bi-LSTM model and $\boldsymbol{F_i}$ is the feature vector of the AIS message $\boldsymbol{i}$.

3.5 Threshold Determination & Classification

The threshold $\boldsymbol{\tau}$ for classifying AIS messages as spoofed or genuine is determined through experimentation and validation. The threshold is set to balance the detection of true spoofed messages while minimizing false positives. Optimizing evaluation parameters like precision, recall, and F1-score on a validation dataset can serve as a basis for choosing $\boldsymbol{\tau}$.

The classification process involves comparing the anomaly score of each AIS message with the threshold $\boldsymbol{\tau}$. The message is categorized as spoofing if the anomaly score is higher than the cutoff; if not, it is categorized as genuine. The classification rule is:

Classify i as spoofed if si > τ

Algorithm 3: Spoofed points detection

Input: Preprocessed AIS features (F_norm)
Output: *Compiled Bi-LSTM model (M)*

```
1. I_spoofed <- [ ]
2. for each i in D:
   2.1 s_i <- M(F_i)
   2.2 if s_i > τ:
   2.2.1 Classify AIS message i as spoofed.
   2.2.2 I_spoofed.append(i)
3. return I_spoofed
```

The indices of detected spoofed messages are stored in a list of $_{Ispoofed}$, which is returned as the output of the spoofing detection algorithm.

The crucial problem of AIS data spoofing, which seriously jeopardizes marine navigation and security, is addressed by the Spoofed Points Detection method. AIS is essential for tracking vessel positions, courses, and speeds, but it can be compromised by GPS spoofing attacks, where false signals are transmitted to mislead vessels about their true locations. The algorithm leverages a trained Bi-LSTM model to detect these spoofed AIS messages.

The algorithm begins by initializing an empty list to store the indices of detected spoofed messages. Relevant information, including geographical position, speed over ground, timestamp, course over ground, and vessel identifier, are extracted for every AIS message in the collection to create a feature vector. The trained Bi-LSTM model then predicts an anomaly score for each AIS message, which reflects the likelihood of it being spoofed. Because it can recognise complex temporal patterns in sequential data and process information both forward and backward to enhance comprehension of the AIS messages, the Bi-LSTM model is a good fit for this task.

Following the acquisition of the anomaly score, it is evaluated against a predetermined decision threshold. This threshold is set based on prior experimentation and validation to balance the detection of true spoofed messages and minimize false positives. If the anomaly score exceeds this threshold, the AIS message is classified as spoofed, and its index is added to the list of detected spoofed messages. If the score is below the threshold, the message is considered genuine.

The final output of the algorithm is a list of indices corresponding to the AIS messages identified as spoofed. This approach is highly effective because it can detect subtle anomalies that traditional methods might miss. The Bi-LSTM model's ability to process and analyse AIS data sequences allows it to identify a wide range of spoofing attacks, including those that mimic normal vessel behaviour or involve gradual deviations from expected patterns.

The Spoofed Points Detection algorithm significantly enhances maritime safety and security by providing a robust solution for identifying spoofed AIS messages. Ensuring the integrity of AIS data helps prevent potential collisions, groundings, and other safety incidents caused by misleading information. Additionally, it aids in protecting vessels from malicious activities that exploit AIS vulnerabilities. This algorithm represents a sophisticated application of deep learning in the maritime domain, offering a reliable method for detecting and mitigating the risks associated with AIS spoofing.

4. RESULT & DISCUSSION

Large-scale tests were carried out using real-world AIS datasets, which were sourced from source[16], which contains historical AIS databases, to evaluate the Bi-LSTM model's performance. The model's performance was validated on unseen regions and vessel types, demonstrating its ability to generalize effectively and reliably detect anomalies across various maritime scenarios. Several metrics that are frequently employed for binary classification tasks must be assessed to generate outcomes and assess the Bi-LSTM model's efficacy in comparison to alternative machine learning methodologies. Table 2 summarizes the results and comparison. F1-Score, Detection Rate, Precision, and Recall are some of these measurements. The suggested model was thoroughly contrasted with the outcomes of SVM, Random Forest, and conventional LSTM models. The results were generated using hypothetical 95 % confidence.

Table 2. Performance evaluation of various models

Model	Precision	Recall	F1-score	Detection rate
Bi-LSTM	0.94	0.92	0.93	0.91
SVM	0.85	0.81	0.83	0.79
RF	0.88	0.84	0.86	0.82
Traditional LSTM	0.90	0.88	0.89	0.87

The Bi-LSTM model achieves the highest scores across all metrics, demonstrating its superior ability to capture complex temporal patterns in AIS data and effectively detect spoofed messages. Its bidirectional processing allows it to understand context from both past and future inputs, enhancing its detection capabilities. The SVM model performs well but falls short compared to the Bi-LSTM. It relies on handcrafted features and cannot automatically learn temporal dependencies, which limits its effectiveness in detecting subtle anomalies indicative of spoofing. Although it provides a reasonable mix between precision and recall, the Random Forest model is not as efficient as the Bi-LSTM.

It benefits from ensemble learning but still cannot fully capture the temporal nature of AIS data. The traditional LSTM model performs better than both SVM and Random Forest but is still outperformed by the Bi-LSTM. While LSTMs are capable of retaining information over sequences, they only process data in one direction, limiting their ability to fully understand the context. Results demonstrate that the Bi-LSTM model consistently outperforms existing spoofing detection methods across all evaluation metrics.

5. CONCLUSION

This research presents a novel method that uses AIS data to identify spoofed points in vessel trajectory paths. The proposed methodology leverages the power of Bi-LSTM networks to model the temporal dependencies in AIS data and identify anomalies indicative of spoofing. Numerous investigations were out on real-world datasets showing that the Bi-LSTM model outperformed alternative methods.

The evaluation results indicate that the Bi-LSTM model provides a more accurate and robust solution for detecting AIS spoofing attacks compared to traditional machine learning techniques like SVM and Random Forest, as well as unidirectional LSTM models. For marine cybersecurity applications where identifying spoofing AIS data is critical, the Bi-LSTM is the recommended option due to its large improvement in performance resulting from its ability to record temporal dependencies in both directions. The study advances

maritime cybersecurity by offering a more reliable and precise method of identifying AIS spoofing attacks.

6. FUTURE SCOPE

The research by Raj & Kumar[17], which demonstrates the effectiveness of integrating long short-term memory & Linear Regression techniques for predicting vessel positions using AIS data to improve maritime operations, can be leveraged to achieve more accurate predictions and may be employed in conjunction with current methods to detect spoofed points in the future. While AIS data patterns vary depending on geographic location and vessel type, the Marine Cadastre dataset used in this research includes diverse data from coastal, inland, and oceanic regions, as well as multiple vessel types. Future work can further enhance the model's robustness by incorporating additional datasets from different geographical areas and vessel categories to extend its applicability globally. Also, exploring the use of Transformer models in the maritime domain could provide valuable insights, especially for handling large-scale, diverse datasets across multiple regions. However, efforts should focus on optimizing the model for real-time performance and reducing computational overhead to make it more feasible for deployment in maritime environments with limited resources. Additionally, further research could explore hybrid models that combine the strengths of both Bi-LSTM and Transformer architectures to enhance accuracy, scalability, and real-time anomaly detection capabilities.

REFERENCES

1. Jafarnia-Jahromi, A.; Broumandan, A.; Nielsen, J. & Lachapelle, G. GPS vulnerability to spoofing threats and a review of antispoofing techniques. *Int. J. Navi. and Observ.*, 2012, **2012**(1), 127072. doi: 10.1155/2012/127072
2. Wolsing, K.; Roepert, L.; Bauer, J. & Wehrle, K. Anomaly detection in maritime AIS tracks: A review of recent approaches. *J. Marine Scie. Engin.*, 2022, **10**(1), 112. doi: 10.3390/jmse10010112
3. Brandsæter, A.; Vanem, E. & Glad, I. K. Efficient on-line anomaly detection for ship systems in operation. *Expert Syst. Appl.*, 2019, **121**, 418-437. doi: 10.1016/j.eswa.2018.12.040
4. Yan, Z.; Song, X.; Zhong, H.; Yang, L. & Wang, Y. Ship classification and anomaly detection based on spaceborne AIS data considering behavior characteristics. *Sensors*, 2022, **22**(20), 7713. doi: 10.3390/s22207713
5. Liu, B.; de Souza, E.N.; Hilliard, C. & Matwin, S. Ship movement anomaly detection using specialized distance measures. *In* 2015 18th International Conference on Information Fusion (Fusion), IEEE, 2015, July.
6. Rong, H.; Teixeira, A. P. & Soares, C.G. Data mining approach to shipping route characterization and anomaly detection based on AIS data. *Ocean Engin.*, 2020, **198**, 106936. doi: 10.1016/j.oceaneng.2020.106936
7. Pedroche, D.S.; Herrero, J.G. & López, J.M.M. Context learning from a ship trajectory cluster for anomaly detection. *Neurocomputing*, 2024, **563**, 126920. doi: 10.1016/j.neucom.2023.126920
8. Xie, Z.; Bai, X.; Xu, X. & Xiao, Y. An anomaly detection method based on ship behavior trajectory. *Ocean Engin.*, 2024, **293**, 116640. doi: 10.1016/j.oceaneng.2023.116640
9. Zhang, C.; Liu, S.; Guo, M. & Liu, Y. A novel ship trajectory clustering analysis and anomaly detection method based on AIS data. *Ocean Engin.*, 2023, **288**, 116082. doi: 10.1016/j.oceaneng.2023.116082
10. Wu, D.; Liu, S.; Wei, W. & Sui, Y. A new satellite-ship autonomous communication system with an integrated deep learning anomaly detection algorithm. *Multimedia Tools and Appl.*, 2024, 1-26. doi: 10.1007/s11042-024-18567-4
11. Kowalska, K. & Peel, L. Maritime anomaly detection using Gaussian process active learning. *In* 2012 15th International Conference on Information Fusion, IEEE, 2012.
12. d'Afflisio, E.; Braca, P. & Willett, P. Malicious AIS spoofing and abnormal stealth deviations: A comprehensive statistical framework for maritime anomaly detection. *IEEE Transact. on Aerospace and Electron. Syst.*, 2021, **57**(4), 2093-2108. doi: 10.1109/TAES.2021.3083466
13. Kobayashi, K. & Kubo, N. Spoofing detection on ships using multipath monitoring and moving-baseline analysis. Proceedings of the 33rd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2020) pp. 3283-3293. doi: 10.33012/2020.17563
14. Zheng, H.; Zhu, W.; Wu, Y. & Chen, P. Detection of abnormal ship trajectory points based on statistical learning. *In* 2022 International Conference on Computer Technologies (ICCTech), 2022, pp. 110-115. doi: 10.1109/ICCTech55650.2022.00025
15. Liang, M.; Weng, L.; Gao, R.; Li, Y. & Du, L. Unsupervised maritime anomaly detection for intelligent situational awareness using AIS data. *Knowledge-Based Syst.*, 2024, **284**, 111313. doi: 10.1016/j.knosys.2023.111313
16. Vessel traffic data. Bureau of Ocean Energy Management (BOEM) and National Oceanic and Atmospheric Administration (NOAA). https://marinecadastre.gov/ais/. (Accessed on 23 May 2024).
17. Raj, N., & Kumar, P. A novel & efficient LR LSTM AIS route data prediction for longer range. *Def. Scie. J.*, 2024, **74**(4), 583-591. doi:10.14429/dsj.74.19336

CONTRIBUTORS

Mr Nitish Raj obtained his M.Tech (CSE) from IIT Delhi and working as a Scientist at DRDO, posted at the WESEE, Ministry of Defence in New Delhi. He holds the position of Senior Systems Manager of Naval Combat Systems. His research interests encompass: System design & development, systems integration, and machine learning.

His contributioned to the current is by producing the idea and designing the experiment, optimising the deep learning techniques used in the experiment, analysing the data, and finalising the manuscript.

Dr Prabhat Kumar is a Professor in the Computer Science and Engineering Department at NIT Patna, India. He holds a PhD in Computer Science. His research focuses on Wireless sensor networks, internet of things, cyber security, data science, software engineering, and e-governance.
He made contributions to the current study by assisting in the conceptualisation of the review, helping in the identification and contributing to the analysis.