УДК 004.942:656.61.052

COLLECTIVE CYBERSECURITY OF AUTONOMOUS MARITIME VESSELS BASED ON DECENTRALIZED INTELLIGENT ANALYSIS

Kozachok Y., *graduate student, Kherson State Maritime Academy, Ukraine, e-mail: kozak9995@gmail.com, ORCID: 0009-0005-6430-3961;*
Simanenkov A., *Ph.D., Associate Professor, Ship Electrical Equipment and Automation Appliances Exploitation Department, Kherson State Maritime Academy, Ukraine, e-mail: Simanenkov.andrii@gmail.com, ORCID: 0000-0003-0797-527600:54;*
Zinchenko S., *Sc.D., Associate Professor, Ship Handling Department, Kherson State Maritime Academy, Ukraine, e-mail: srz56@ukr.net, ORCID: 0000-0001-5012-5029.*

This paper presents a comprehensive approach to enhancing the collective cybersecurity of autonomous maritime platforms through the integration of intelligent data analysis methods, decentralized coordination mechanisms, and a custom hybrid architecture that combines Long Short-Term Memory (LSTM) neural networks with onboard large language models (LLMs). The core innovation lies in augmenting traditional LSTM-based anomaly detection with LLM-driven semantic interpretation of navigational inconsistencies — a fundamentally novel strategy for self-governing maritime environments.

Particular attention is paid to the detection, explanation, and decentralized coordination of responses to Global Positioning System (GPS) spoofing attacks, which pose a significant threat to navigational accuracy, operational safety, and the overall coherence of fleet activities. The proposed system, built on a proprietary LSTM-LLM configuration, equips each vessel with multi-level cognitive capabilities: real-time anomaly detection, natural language generation of contextual explanations, and autonomous formulation of strategic responses without dependence on centralized oversight or communication infrastructure.

Unlike conventional centralized solutions, the system empowers each vessel to independently analyze situational data, derive human-understandable contextual insights, and adapt its behavior accordingly. The architecture includes a lightweight protocol for structured message exchange in JavaScript Object Notation (JSON) format, enabling efficient, resilient, and secure inter-vessel communication. Additionally, a decentralized consensus mechanism, based on a dynamically updated trust matrix, enhances the fleet’s robustness against partial compromise and improves operational integrity.

The effectiveness of the proposed approach is demonstrated through a simulated GPS spoofing scenario involving one compromised vessel within a five-vessel fleet. The results confirm the system’s ability to detect anomalies accurately, isolate the compromised unit, and successfully adapt the navigational strategies of the remaining vessels — thus maintaining uninterrupted mission continuity despite active cyber disruption.

Key words: *autonomous vessels; collective cybersecurity; large language models; decentralized coordination; Ollama; Long Short-Term Memory; artificial Intelligence; cyber resilience; multi-agent systems; trust matrix consensus.*

DOI: 10.33815/2313-4763.2025.1.30.006-015

Introduction. The active development of autonomous maritime transport creates new opportunities for improving the efficiency, safety, and economy of maritime transportation. Modern autonomous vessels increasingly rely on navigation, communication, and computational systems that function without direct human intervention. Under these conditions, ensuring cybersecurity becomes a critical issue, both for individual platforms and for entire fleets.

Modern autonomous vessels heavily rely on complex navigation, communication, and computational systems that must operate reliably without direct human intervention. These systems process vast amounts of real-time data, including Global Positioning System (GPS) signals, Automatic Identification System (AIS) broadcasts, inertial navigation system (INS) inputs, and environmental sensor data. A disruption or manipulation of this information can critically impact a vessel’s decision-making processes, making cybersecurity not merely a technical concern but a foundational requirement for safe and efficient operations.

One of the most dangerous threats is GPS spoofing attacks, where an attacker falsifies global positioning signals, causing the vessel to incorrectly determine its own location. In multi-vessel (collective) missions, where movement coordination relies on shared routes, even a single attack can have critical consequences for the entire fleet, including collisions, loss of orientation, mission disruptions, and more.

In response to these challenges, this article proposes a hybrid system for collective response to cyber threats, combining:

– Neural network models for anomaly detection in navigation data;

– Large Language Models (LLM), particularly Ollama, serving as situational interpreters and strategic decision generators onboard;

– Mechanisms for decentralized interaction between vessels, allowing coordinated responses to attacks without a centralized control point.

The proposed system enables an autonomous vessel not only to detect its own vulnerabilities but also to inform other fleet participants, initiate consistency checks for coordinates, receive recommendations from local artificial Intelligence (AI) assistants, and adjust the collective trajectory. Thus, it ensures collective cyber resilience capable of adapting to dynamic threats in real-time.

Analysis of Recent Research and Publications. With the increasing level of automation in vessel navigation, autonomous vessels become more vulnerable to cyber threats. Cyberattacks on autonomous maritime vessels can vary in nature and impact vectors, affecting navigation, sensors, communication, and software components. One of the most dangerous types of attacks is GPS spoofing, in which an attacker alters the coordinates perceived by the vessel, misleading it about its actual location [1]. Another common threat is GPS jamming, which can lead to a complete loss of navigation capability. Similarly, the AIS, responsible for information exchange between vessels, can also be spoofed. Furthermore, interference with the INS is possible, leading to accumulated errors in coordinate determination over time.

These threats can disrupt navigation systems, creating significant safety risks. Research [2] highlights that cyberattacks can result in loss of vessel control, physical damage, and navigational system disruptions.

Resource [3] describes a new type of Distributed Denial of Service (DDoS) attack, the largest in history, which resulted in a 30-minute outage affecting 15% of global internet services and several major providers, significantly impacting maritime systems as well. Special attention should be given to the vulnerability of satellite navigation systems. Work [4] emphasizes the necessity of enhanced protection against cyberattacks for maritime systems, especially when combined with terrestrial components of advanced long-range navigation systems.

Among contemporary approaches for detecting anomalies in navigational data, neural network models such as Long Short-Term Memory (LSTM) show promise. Specifically, study [5] demonstrates the effectiveness of the LSTM encoder-decoder algorithm in identifying deviations in Automatic Dependent Surveillance–Broadcast message sequences within air transportation. The proposed method autonomously models expected object behavior and detects discrepancies, an approach equally applicable to GPS spoofing detection in maritime environments. Despite the aviation focus of the research, its principles can directly transfer to tasks involving the safe navigation of autonomous vessels in open waters.

Recently, the Ollama platform has attracted researchers' attention due to its ability to locally deploy LLM, even in resource-constrained environments. Work [6] analyzed the performance of 28 quantized Ollama models deployed on Raspberry Pi devices, evaluating energy consumption, accuracy, and inference latency. Results demonstrate that local LLMs can effectively handle real-time tasks on autonomous devices. In an industry-specific context, research [7] explored using Ollama to develop PDF bots capable of efficiently processing technically complex documents. The authors underline the importance of adapting Retrieval-Augmented Generation (RAG) architectures to domain-specific requirements, particularly relevant to maritime contexts with extensive regulatory data, routing charts, and instructions.

The integration of LLMs, such as Ollama, into autonomous vessel systems opens new possibilities for interpreting and explaining detected threats. LLMs can provide clear recommendations to crew members or automated systems regarding further actions upon detecting anomalies caused by cyberattacks. Research [5] underscores LLMs' potential for contextual understanding and response generation, enhancing cybersecurity systems' effectiveness.

Analysis of current research [8–11] indicates that effective cybersecurity in autonomous maritime navigation requires a comprehensive approach, encompassing anomaly detection, decentralized coordination, and intelligent systems for threat interpretation. Integrating large language models into these systems can significantly improve their effectiveness and adaptability to emerging challenges.

Purpose and Objectives of the Research. The purpose of the research is to develop and experimentally verify a hybrid intelligent system for detecting and collectively responding to cyberattacks (particularly GPS spoofing) within a network of autonomous maritime vessels, utilizing a local language assistant based on an Ollama, which ensures decentralized adaptation and cybersecurity resilience of the fleet.

Main Section. Within the framework of this research, a hybrid cybersecurity system is proposed, combining anomaly detection in navigational data using neural network models [12–16] with LLM for interpreting and explaining threats, as well as forming context-dependent actions. A critical aspect of the system is its distributed nature, enabling autonomous vessels to exchange risk assessments and coordinate collective responses without centralized management.

The system comprises the following functional modules:

– Anomaly Detection Module: Built on an LSTM network trained on normal GPS/AIS coordinate behavior to forecast subsequent values. Deviations from actual values indicate potential attacks. LSTM networks represent a special class of recurrent neural networks (RNNs) specifically designed to learn and model temporal sequences and long-range dependencies. Unlike traditional RNNs, which often suffer from the vanishing gradient problem, LSTM networks utilize a gated cell structure that enables them to retain information over extended periods of time. Each LSTM cell incorporates input, output, and forget gates, allowing the network to dynamically control which information is stored, updated, or discarded. This architecture makes LSTM models particularly effective in tasks involving sequential data analysis, such as time series prediction, natural language processing, and anomaly detection. In the context of autonomous maritime systems, LSTM networks are widely employed for detecting anomalies in navigation data, predicting vessel trajectories, and enhancing situational awareness by modeling complex temporal patterns.

– Language Model: Implemented via the local Ollama platform which are advanced AI systems built upon large-scale transformer-based architectures capable of understanding, generating, and reasoning over human language with high contextual awareness. These assistants leverage pre-trained deep learning models, often containing billions of parameters, fine-tuned to perform a wide range of tasks, including question answering, decision support, summarization, and real-time information retrieval. Due to their ability to process complex queries and generate contextually relevant responses, LLM Assistants are increasingly integrated into autonomous systems to enhance their decision-making capabilities. In autonomous maritime platforms, LLM-based assistants can provide real-time situation analysis, interpret anomalous sensor data, and support the coordination of collective behavior among multiple vessels, offering a significant improvement in operational autonomy and cyber-resilience.

– Inter-Vessel Communication Module: Implemented through a lightweight JavaScript Object Notation (JSON) protocol (via Transmission Control Protocol/User Datagram Protocol), it enables the dissemination of threat alerts (including coordinates, timestamps, IDs, and recommendations).

– Collective Decision Mechanism: Each vessel performs a local verification of the attacked node's coordinates, assesses trust levels, consults its own LLM assistant, and subsequently adjusts its trajectory according to the new coordination strategy.

The system features a three-level structure (Fig. 1):

1. Sensory Level – Acquisition of GPS, AIS and INS data;
2. Analytical Level – Anomaly detection, LLM initiation for explanations;
3. Coordination Level – Dissemination of decisions, creation of new routes.

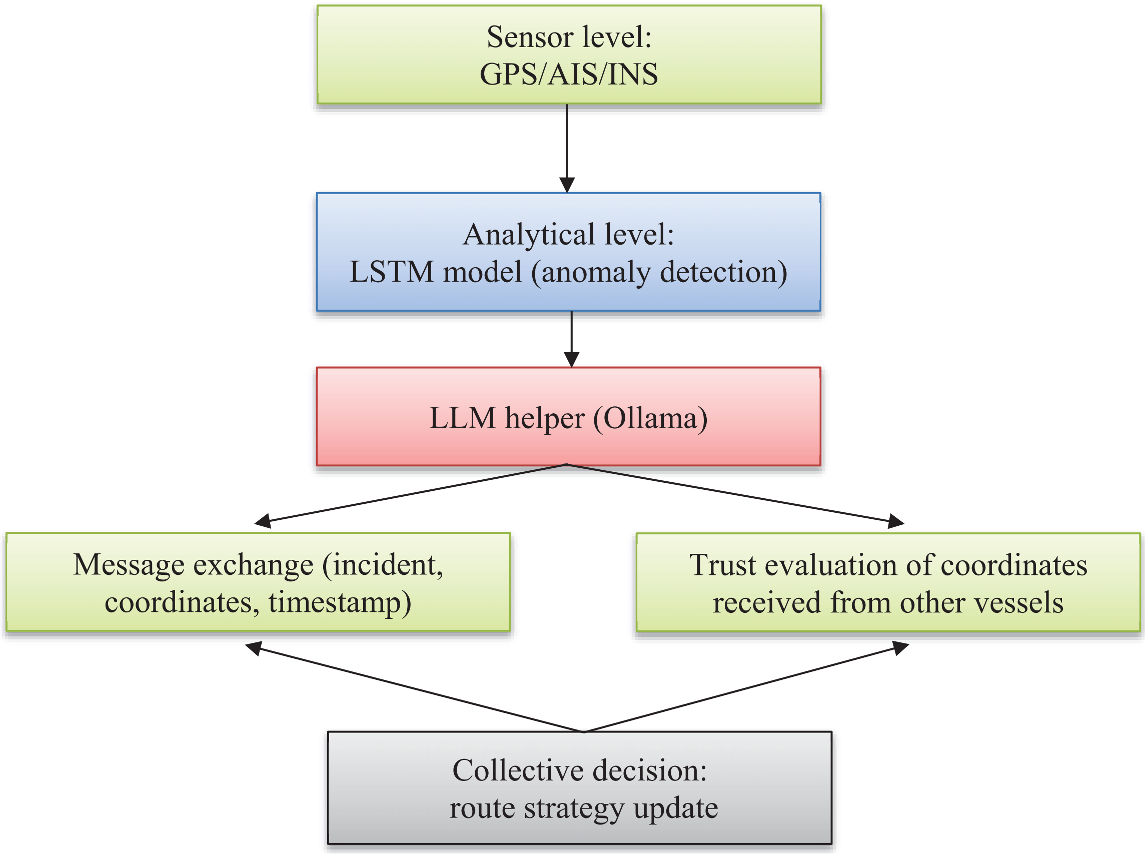

Sensor level:
GPS/AIS/INS
Analytical level:
LSTM model (anomaly detection)
LLM helper (Ollama)
Message exchange (incident, coordinates, timestamp)
Trust evaluation of coordinates received from other vessels
Collective decision:
route strategy update

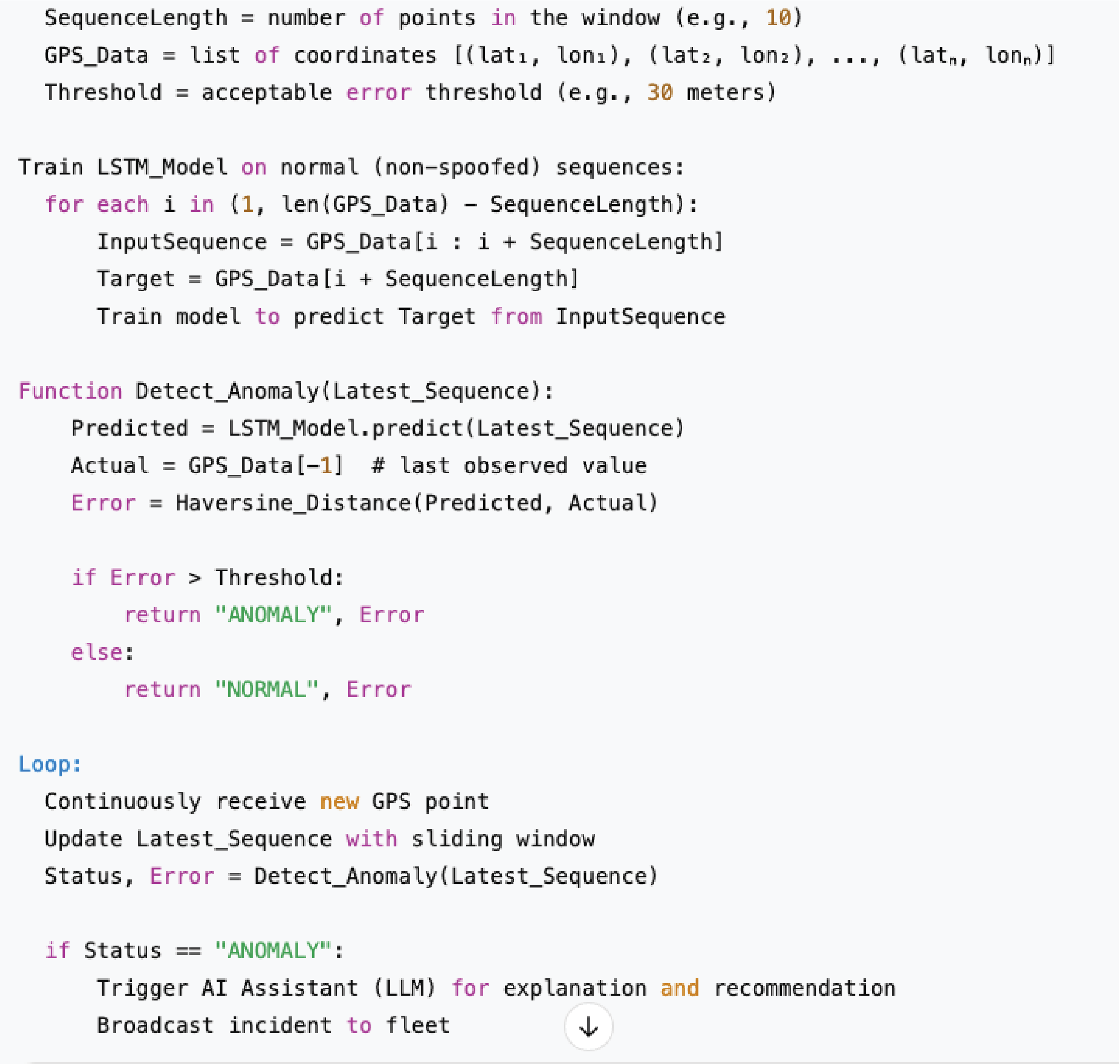
Figure 1 – Overview of the Decentralized Three-Layer Architecture Used in the AI Module

The proposed method for detecting anomalies in navigational data is based on the use of a LSTM network combined with a LLM assistant for explanation and decision support. A sliding window approach is used, where a fixed-length sequence of recent GPS coordinates is continuously processed. The LSTM model is trained on normal (non-spoofed) GPS sequences to predict the next expected position based on the historical input sequence.

During real-time operation, the system receives new GPS data points and updates the latest sequence accordingly. The LSTM model predicts the next expected coordinate, and the predicted value is compared to the actual received value using the Haversine distance formula, which measures the geographical distance between two points on the Earth's surface. If the calculated error exceeds a predefined threshold the system flags an anomaly.

When an anomaly is detected, the onboard LLM assistant is triggered to generate a contextual explanation of the incident and recommend appropriate actions. Additionally, an incident alert is broadcast to other vessels in the fleet, allowing the collective to respond in a coordinated manner. This hybrid LSTM-LLM approach ensures real-time anomaly detection with autonomous situational assessment and collaborative fleet behavior adjustment without reliance on centralized systems. The LSTM model is illustrated using pseudocode in Fig. 2.

The methodology is highly adaptable and scalable, as the LSTM model can be retrained for different vessel types, operational scenarios, or navigational environments. Moreover, by relying on learned sequential patterns rather than static thresholds, the system significantly reduces the occurrence of false positives caused by typical navigational noise. Finally, the architecture is designed with efficiency in mind: both LSTM networks and locally deployed, quantized LLMs can operate effectively on modern edge computing hardware, ensuring that real-time processing requirements are met without excessive energy consumption.



```
  SequenceLength = number of points in the window (e.g., 10)
  GPS_Data = list of coordinates [(lat₁, lon₁), (lat₂, lon₂), ..., (latₙ, lonₙ)]
  Threshold = acceptable error threshold (e.g., 30 meters)

Train LSTM_Model on normal (non-spoofed) sequences:
  for each i in (1, len(GPS_Data) - SequenceLength):
      InputSequence = GPS_Data[i : i + SequenceLength]
      Target = GPS_Data[i + SequenceLength]
      Train model to predict Target from InputSequence

Function Detect_Anomaly(Latest_Sequence):
    Predicted = LSTM_Model.predict(Latest_Sequence)
    Actual = GPS_Data[-1]  # last observed value
    Error = Haversine_Distance(Predicted, Actual)

    if Error > Threshold:
        return "ANOMALY", Error
    else:
        return "NORMAL", Error

Loop:
  Continuously receive new GPS point
  Update Latest_Sequence with sliding window
  Status, Error = Detect_Anomaly(Latest_Sequence)

  if Status == "ANOMALY":
      Trigger AI Assistant (LLM) for explanation and recommendation
      Broadcast incident to fleet
```

Figure 2 – Pseudocode of LSTM Algorithm for Anomaly Detection

Let us consider a fleet $F = \{S_1, S_2, ..., S_n\}$ of autonomous vessels operating in a distributed environment and interacting with each other through communication channels with limited latency. The input parameters include the coordinates of vessel SiS_iSi at time ttt and the magnitude of its positional change.

$$p_i(t) = \left(lat_i(t), lon_i(t)\right) \in R^2; \qquad (1)$$

$$\Delta p_i(t) = \left|\left|p_i(t) - p_i(t - \delta t)\right|\right|, \qquad (2)$$

where $p_i(t)$ – the coordinates of the vessel at a given point in time, $\Delta p_i(t)$ – the magnitude of movement Vessel S_k registers a potential deviation if:

$$MSE\left(\hat{p}_k(t), p_k(t)\right) > \tau, \qquad (3)$$

where $p_k(t)$ – the coordinate prediction from the LSTM model, τ – the threshold value of the reconstruction error, MSE (Mean Squared Error) – the mean squared error
Vessel S_k generates a message:

$$\mathcal{A}_\mathrm{k} = \left(\mathrm{t}, \mathrm{S_k}, \mathrm{p_k(t)}, \Delta\mathrm{p_k(t)}, \mathrm{recLLM}(\mathrm{S_k}, \mathrm{t})\right), \tag{4}$$

where recLLM is a recommendation generated by the local LLM assistant based on the Ollama platform. The message $\mathcal{A}_\mathrm{k}$ is broadcast to Sj. Each vessel S_j calculates the relative discrepancy:

$$\mathrm{d_{jk}(t)} = ||\mathrm{p_j(t)} - \mathrm{p_k(t)}||, \tag{5}$$

and determines the trust in the coordinates S_k:

$$\mu_{jk}(t) = \begin{cases} 1, & \text{if } d_{jk}(t) \le \eta \\ 0, & \text{if } d_{jk}(t) > \eta \end{cases}, \tag{6}$$

where η – the allowable inter-vessel error (GPS drift margin).
The vessels construct a trust matrix:

$$\mathrm{M(t)} = \left[\mu_{jk}(\mathrm{t})\right]\mathrm{j} \in \mathrm{F} \setminus \{\mathrm{k}\}. \tag{7}$$

Final trust:

$$\mu_k(\mathrm{t}) = \frac{1}{n-1}\sum\mu_{jk}(\mathrm{t}). \tag{8}$$

If $\mu_k(\mathrm{t}) < 0$, де $0 \in [0,1]$ – a threshold value (e.g., 0.5), then S_k is considered compromised. The fleet transitions to a new state $Sj \in F'$ and performs local trajectory optimization γj(t) taking into account the exclusion of the compromised node:

$$\gamma'_j(\mathrm{t}) = \mathrm{Optimize}(\gamma_j\mathrm{j(t)} \mid \mathrm{S}_k \in/\mathrm{Nj(t)}), \tag{9}$$

where Nj(t) – a set of neighboring vessels for coordinated navigation.

This approach ensures decentralized fleet resilience against GPS spoofing attacks, enabling autonomous agents to respond independently yet coordinately. The experimental part of this study aims to validate the functionality of the proposed collective cybersecurity system for autonomous vessels, integrating local detection of navigation anomalies, explanatory capabilities of the LLM language model, and decentralized fleet interaction under GPS spoofing conditions.

The experiment sought to confirm the LSTM model's capability to detect anomalous coordinate changes in real-time, assess the responsiveness and quality of explanations provided by the local AI-assistant (Ollama), verify the correctness of collective fleet decision-making during a simulated attack on one of the vessels, and evaluate the overall resilience of the system against partial disruption of coordinated navigation control.

The following software was used to model the system:

– OpenCPN – as a visualization platform for autonomous fleet navigation;

– gps-sdr-sim – to generate fake GPS signals using pre-prepared NMEA sequences;

– Python – an environment for processing coordinates and implementing the LSTM-based anomaly detection model;

– TensorFlow/Keras – for constructing and training the neural network model;

– Ollama – a local platform for running the LLM;

– Docker – for containerizing each vessel as a separate node with a network API;

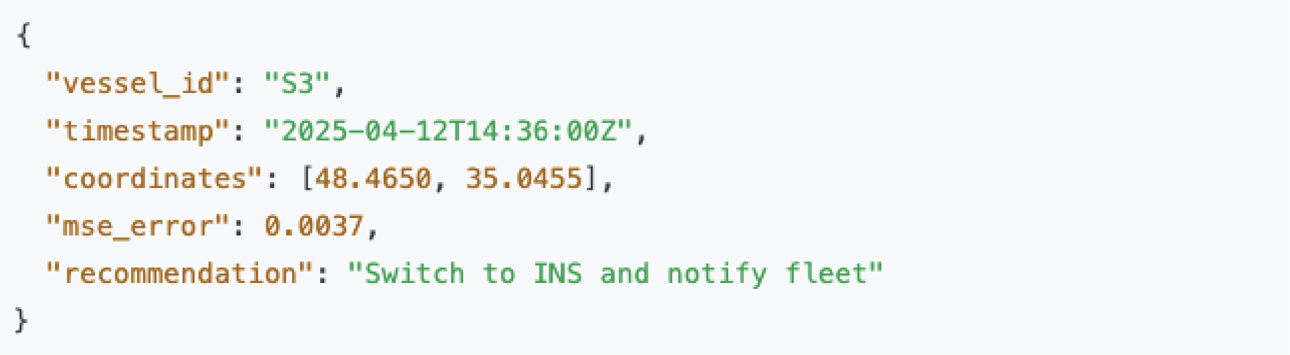
– JSON communication – for exchanging incident information and coordinates between vessels.

The simulation modeled a fleet of five autonomous vessels S= {S1, S2, S3, S4, S5}, initially following identical routes in a parallel formation at a speed of 10 knots. The attack scenario included:

– At t=120 seconds, vessel S3 was subjected to a GPS spoofing attack, shifting coordinates by 70–90 meters within 2 seconds;

– The LSTM model was trained on 10,000 normal observations (without anomalies);

– Each vessel is equipped with a local LLM-assistant using the Ollama API, which receives incident data structured as JSON (Fig. 3).



```
{
  "vessel_id": "S3",
  "timestamp": "2025-04-12T14:36:00Z",
  "coordinates": [48.4650, 35.0455],
  "mse_error": 0.0037,
  "recommendation": "Switch to INS and notify fleet"
}
```

Figure 3 – communication API with LLM

Upon receiving the message, other vessels compare their coordinates with S3, assess the trust level, consult their local LLM-assistants to generate recommendations, and collectively exclude vessel S3 from the coordination matrix.

Main Results and Discussion. To evaluate the results, the following metrics are utilized:

– MSE – widely used to measure prediction accuracy or data reconstruction in machine learning, particularly in regression and anomaly detection tasks;

– LLM response time – the duration taken by the language model to respond to queries;

– Correctness of collective decision-making – evaluating whether the fleet’s collective response to the threat was appropriate;

– Time To Detect (TTD) – the interval from the attack's initiation to its detection (Fig. 4).

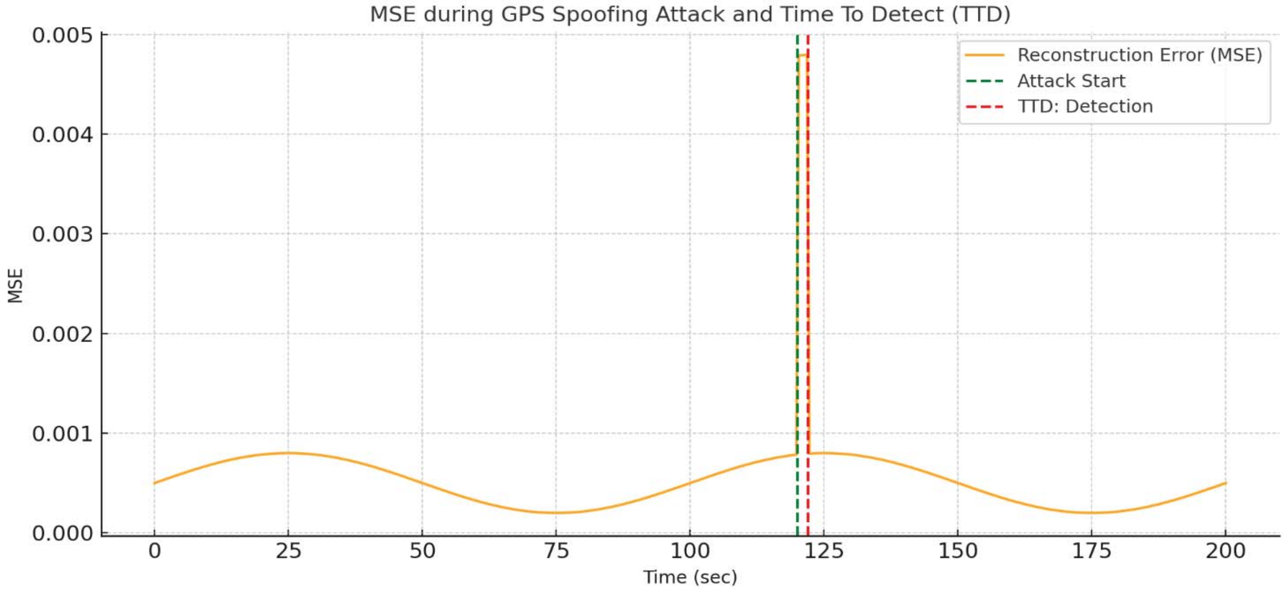


Figure 4 – MSE detection visualization

The experimental simulation results demonstrate that the system can promptly detect GPS spoofing attacks with an average detection delay of 1,8 seconds after the anomaly begins. The developed LSTM model provided high detection accuracy, achieving precision = 0,97 and recall = 0,94, confirming its ability to identify coordinate deviations even under minor external disturbances.

The local AI assistant based on the Mistral model deployed via the Ollama platform generated situational explanations in approximately 0,8 seconds on average, allowing its real-time use. In 100% of the simulation runs, the system correctly identified which vessel was compromised, and all other fleet participants successfully excluded it from collective coordination, adapting their routes according to the new fleet configuration.

These findings confirm that the proposed system can swiftly and reliably detect coordinate anomalies related to GPS spoofing, generate meaningful and practical recommendations using a local AI assistant, and ensure stable collective response among autonomous vessels without the need for centralized control. Thus, the approach ensures functional cyber-resilience of the fleet, even when one of its elements is compromised.

The hybrid system's advantages demonstrate high efficiency under realistic GPS spoofing attack scenarios. Key advantages of the system include

– Decentralization: The system requires no centralized control or server; each vessel autonomously detects anomalies and generates recommendations.

– Intelligent Explanation: Through local deployment of LLM models, each agent can articulate the causes of incidents and suggest actions understandable both by humans and other software.

– Resilience to Partial Fleet Disruption: Even if one fleet participant is compromised, the collective behavior system maintains adaptability.

– Scalability: The architecture enables adding new vessels without modifying interaction principles.

Despite the successful results, the system has certain limitations:

– Model Quality Determines Reliability: An improperly trained LSTM model may fail to detect anomalies or produce false positives.

– Resource Requirements: Running the local LLM assistant demands adequate computational resources, particularly CPU and RAM.

– LLM Security: Language models can be susceptible to prompt injection or may generate ambiguous instructions under complex conditions.

– Network Reliability: Loss of communication between vessels could disrupt the collective coordinate verification mechanism.

– The current evaluation involved a relatively small group of vessels. To ensure robustness and scalability, the system should be validated in larger fleets and more diverse maritime environments.

Conclusions. This study introduces a cybersecurity architecture for autonomous maritime vessels that integrates real-time anomaly detection in navigational data, interpretative capabilities of a locally deployed AI assistant based on a LLM, and decentralized coordination mechanisms among fleet units. The system was evaluated in a simulated GPS spoofing scenario involving a five-vessel autonomous group.

Compared to traditional centralized methods, the proposed solution offers significant advantages in autonomy, scalability, explainability of decisions, and rapid situational response. These attributes make the system a strong candidate for integration into next-generation maritime platforms - including unmanned patrol, cargo, and oceanographic research vessels — where resilience and independence are mission-critical.

Prospects for Further Research. Future directions for research and enhancement of the proposed system may include:

– Multimodal Attack Detection: combining GPS, INS, AIS, and other sensor data into a unified anomaly detection model.

– Contextual Training of the LLM Assistant**:** adapting responses based on vessel type, mission objectives, and weather conditions.

– Model Optimization for Onboard Platforms: using lightweight models (such as Gemma2B) capable of operating on edge devices.

– Agent Voting Mechanisms: instead of simply excluding a compromised node, implementing opinion consensus algorithms (e.g., weighted consensus-based approaches).

REFERENCES

1. Moraes, C. C., de Albuquerque, C. E. P., Machado, R. C. S., & de Sá, A. O. (2021). A triggering mechanism for cyber-attacks in naval sensors and systems. *Sensors*, 21, 3195. https://doi.org/10.3390/s21093195.

2. Balduzzi, M., Pasta, A., & Wilhoit, K. (2014). A security evaluation of AIS automated identification system. In *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC '14)* (pp. 436–445). Association for Computing Machinery. https://doi.org/10.1145/2664243.2664257.

3. Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*, 8(10), 776. https://doi.org/10.3390/jmse8100776.

4. Svilicic, B., Rudan, I., Jugović, A., & Zec, D. (2019). A study on cyber security threats in a shipboard integrated navigational system. *Journal of Marine Science and Engineering*, 7(10), 364. https://doi.org/10.3390/jmse7100364.

5. Greydanus, S. (2017). Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages. *arXiv.org*. https://arxiv.org/abs/1711.10192.

6. Chen, J., Guo, D., Yao, Q., et al. (2024). Sustainable LLM inference for edge AI: Evaluating quantized LLMs for energy efficiency, output accuracy, and inference latency. *arXiv preprint*. https://arxiv.org/abs/2403.15971.

7. Khan, F., & Tomsett, R. (2024). Optimizing RAG techniques for automotive industry PDF chatbots: A case study with locally deployed Ollama models. *arXiv preprint*. https://arxiv.org/abs/2403.18931.

8. Tian, Z., Wang, S., Zhang, J., & Li, J. (2022). Cybersecurity risk assessment of unmanned surface vehicles. *Ocean Engineering*, 248, 110766. https://doi.org/10.1016/j.oceaneng.2022.110766.

9. Luo, Y., & Yu, F. R. (2021). Anomaly detection in autonomous systems using LSTM neural networks. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2020.3039102.

10. Bommasani, R., Hudson, D. A., et al. (2021). On the opportunities and risks of foundation models. *Center for Research on Foundation Models (Stanford University)*. https://crfm.stanford.edu/report.html.

11. Cyber-MAR Project Consortium. (2022). Cyber range simulation for maritime cybersecurity training. *Cyber-MAR Project*. https://cyber-mar.eu.

12. Zinchenko, S. M., & Lyashenko, V. G. (2017). Usage of neural network model of the ship for control tasks. *Scientific Bulletin of KSMA*, 2(17), 231–237. http://journals.ksma.ks.ua/nvksma/article/view/587/524.

13. Kozachok, Y. A. (2024). Automation of information system architecture design for utility payments processing using artificial intelligence. *Tavriyskyi Scientific Bulletin. Series: Technical Sciences*, (2), 62–72. https://doi.org/10.32782/tnv-tech.2024.2.6.

14. Kozachok, Y. A., & Zinchenko, S. M. (2025). Integration of ChatGPT for decision support in autonomous ships in real-time mode. *Scientific Bulletin of Kherson State Maritime Academy*, (2), 111–121. http://journals.ksma.ks.ua/nvksma/article/view/889/903.

15. Tarelko, Wieslaw & Rudzki, Krzysztof. (2020). Applying artificial neural networks for modelling ship speed and fuel consumption. Neural Computing and Applications. 32. https://doi.org/10.1007/s00521-020-05111-2.

Козачок Ю., Сіманенков А., Зінченко С. КОЛЕКТИВНА КІБЕРБЕЗПЕКА АВТОНОМНИХ МОРСЬКИХ СУДЕН НА ОСНОВІ ДЕЦЕНТРАЛІЗОВАНОГО ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ

У даній статті представлено підхід до забезпечення колективної кібербезпеки автономних морських платформ шляхом інтеграції методів інтелектуального аналізу даних, децентралізованої координації та власної гібридної архітектури, що поєднує Long Short-Term Memory (LSTM) з локально вбудованою великою мовною моделлю (LLM). Основна інновація полягає у доповненні традиційної LSTM-моделі компонентом LLM – з метою не лише виявлення, але й семантичного інтерпретування аномалій у навігаційних даних, що є принципово новим підходом для автономного морського середовища.

Особлива увага приділяється виявленню, поясненню та децентралізованій координації реагування на атаки типу GPS-спуфінг, які становлять суттєву загрозу точності навігації та злагодженості дій автономних флотів. Запропонована система, заснована на власній модифікації LSTM-LLM, забезпечує суднам багаторівневу когнітивну здатність: виявлення відхилень у реальному часі, генерацію контекстуальних пояснень природною мовою, а також розробку стратегічних дій без необхідності централізованого управління.

Ключова відмінність від наявних рішень полягає в локальній автономності: кожне судно здатне самостійно аналізувати ситуаційні дані, формувати людиноорієнтовані пояснення та змінювати поведінку відповідно до поточної загрози. Архітектура системи підтримує легкий протокол обміну структурованими повідомленнями у форматі JavaScript Object Notation для швидкої міжсуднової комунікації та децентралізований консенсусний механізм на основі матриці довіри, що динамічно оновлюється.

Ефективність підходу продемонстровано на симульованому сценарії атаки GPS-спуфінг проти одного з п'яти автономних суден. Результати підтвердили здатність системи точно локалізувати джерело загрози, підтримувати цілісність місії флоту та адаптивно перебудовувати навігаційні рішення у відповідь на кіберінцидент.

Ключові слова: *автономні судна; колективна кібербезпека; GPS-спуфінг; великі мовні моделі; децентралізована координація; Ollama; AI-помічник; кіберстійкість; мультиагентні системи, матриця довіри.*

Статтю прийнято до редакції 14.05.2025