КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.892
UDC 004.056.5:621.396.96:004.8

Oleksii Novikov
Doctor of Technical Sciences, Professor,
Director of the Education and Scientific Physics and Technology Institute
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.
ORCID ID: 0000-0001-5988-3352
o.novikov@kpi.ua

Mykola Ilin
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Information Security
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.
ORCID ID: 0000-0002-1065-6500
m.ilin@kpi.ua

Iryna Stopochkina
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Information Security
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID ID: 0000-0002-0346-0390
i.stopochkina@kpi.ua

Mykola Ovcharuk
PhD student of the Department of Information Security
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID ID: 0009-0000-5791-3925
m.ovcharuk@kpi.ua

Andrii Voitsekhovskyi
PhD student, Assistant professor of the Department of Information Security
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID ID: 0009-0004-6009-9492
a.voitsekhovskyi@kpi.ua

APPLICATION OF LLM IN UAV ROUTE PLANNING TASKS TO PREVENT DATA EXCHANGE AVAILABILITY VIOLATIONS

Abstract. This paper presents a novel approach to unmanned aerial vehicle (UAV) route planning under conditions of cyber-physical threats that affect system availability. In hostile and contested environments, UAVs are increasingly exposed not only to natural obstacles and electronic interference, but also to targeted cyber threats. The proposed method addresses both intentional and unintentional disruptions to communication and control, including interference from electronic warfare (EW) systems, jamming, and the propagation of malicious signals. Importantly, EW devices are considered not only as sources of electromagnetic noise, but also as potential vectors for malware distribution or attacks on wireless protocols, making them critical components of the cybersecurity threat landscape.To ensure mission success and maintain reliable data exchange, the method integrates terrain elevation maps, open for use digital elevation models (DEMs), and geospatial data services) with reasoning powered by large language models (LLMs). The system constructs UAV routes that preserve line-of-sight communication, avoid high-risk zones, and adapt to topological and adversarial constraints. A modular architecture is introduced, incorporating data preprocessing, mission-context prompt generation, LLM-based inference, and post-processing validation. Custom

prompt templates are developed to inject mission-specific cyber and physical context, guiding the LLM to avoid hallucinations and enhance security-aware planning. A computational experiment using real elevation data and the Claude Sonnet 4 model confirms the applicability of the proposed solution. Results demonstrate that LLMs, when integrated with cybersecurity-aware geospatial data, can support dynamic UAV route planning and reduce the risk of availability violations caused by both physical interference and cyber intrusion.

Keywords: cyber-physical security; UAV; availability and integrity violations; route planning; LLM.

INTRODUCTION

In modern applications of unmanned aerial vehicles (UAVs) in military, reconnaissance, and humanitarian missions, the task of constructing a secure and efficient flight path under conditions of limited availability has become increasingly critical [1], [2]. In this context, availability refers not only to physical accessibility in environments with obstacles, but also to cybersecurity-related availability, which leads to the ability to maintain control over the UAV, access navigation and communication channels, and ensure secure data transmission even under active adversarial influence.

Electronic warfare (EW), GPS jamming, attacks on network infrastructure, loss of command-and-control links, or intentional disruption of telemetry can result in partial or total denial of access to the UAV. Such conditions place the mission at significant risk. Traditional path planning algorithms (such as A* [3], Dijkstra [4]) often prove inadequate in these scenarios, as they rely on complete knowledge of the environment and require a stable communication channel to recalculate trajectories. Moreover, they lack the capacity to account for semantic or high-level constraints, such as the need to avoid zones of potential cyberattack or dynamically changing threat landscapes.

The use of large language models (LLMs) as a component of UAV path planning offers a novel solution to these limitations by integrating heterogeneous data sources: terrain elevation maps, mission objectives, EW zones, areas at risk of cyber intrusion, energy constraints, and potential communication blackouts. LLMs are capable of generating routes that account not only for physical obstacles, but also for information security logic — avoiding zones of possible signal interception, minimizing time spent in communication-degraded areas, and ensuring return-to-safe-zone behavior in case of control loss.

Importantly, LLMs can interpret mission context expressed in natural language and generate adaptive solutions even in the absence of a fully structured model of the environment. This enables autonomous operation in conditions where not all threats are known in advance or where the operational environment changes during the mission. Furthermore, LLMs can propose multiple alternative routes with explanations of their trade-offs, supporting interactive decision-making in command-and-control systems.

Thus, LLM-based UAV path planning under conditions of constrained availability, both physical and cyber, is a highly relevant research and engineering challenge. It combines intelligent planning methods, enhanced autonomy, contextual awareness, and the integration of cybersecurity risk mitigation. This approach expands the operational scope of UAVs in real-world, dynamic, and hostile environments by ensuring continuity of control, access to mission-critical functions, and the reliability of mission execution.

Problem definition. Based on the input data in the form of maps and the specified coordinates of adversarial countermeasure devices, taking into account their effective range, this work proposes to use an LLM to develop a route for accomplishing a defined mission.

Review of existing solutions. In work [5], a framework was proposed that enables humans to interact with large language models (LLMs) using natural language and supports bypassing obstacles. In work [6], a similar approach was used to solve the problem of route planning, taking into account path complexity and the computational efficiency of the corresponding algorithm. In work [7], large language models were also employed to address the problem, but the task was solved within the context of urban navigation. In work [8], route planning was performed with a focus on the freshness of the processed data (using the age of information metric). The framework proposed in work [9] performs route planning considering weather conditions. A set of prompts is provided, primarily related to parcel delivery tasks, accounting for package weight and destination. In work [10], a set of metrics was proposed to assess the quality of decisions generated by LLMs for the given tasks.

The review shows that existing research primarily addresses the problem of goods delivery and urban route planning, with a focus on delivery quality metrics. An open challenge remains: route planning that accounts for natural terrain for drones executing long-range missions and communicating with a controlling drone. A necessary condition for maintaining communication is that the service drone and the relay drone remain within line-of-sight of each other.

Additionally, cyber-physical obstacles may include adversary-operated electronic warfare (EW) devices and the potential spread of malicious software. When planning routes, it is crucial to avoid zones containing such devices, which can be identified in advance using methods such as reconnaissance.

This issue is addressed in the present work, which aims to enhance existing route planning methods by leveraging the capabilities of LLMs, while accounting for availability disruption factors characteristic of military operations.

Purpose of the article. The purpose of the article is to develop an approach to calculating a UAV route with the support of LLM in conditions of cyber-physical threats to availability, and to develop appropriate prompt templates taking into account the device behavior scenario and topological obstacles.

PROPOSED SOLUTIONS

When calculating the route, we consider the following factors: signal strength, interference effects (including the operational zones of adversarial threat devices), and terrain elevation based on open maps data [11]. Additionally, the LLM is guided using structured prompts, for which dedicated templates have been created. These templates are dynamically populated with the required coordinates.

Signal strength is calculated using the formulas outlined below. It is represented as a real number and may take on negative values due to the influence of electronic warfare (EW) jamming devices [12].

The signal strength of a transmitter at a given distance is computed based on the free-space path loss formula when the distance between devices is significantly greater than the signal wavelength is:

$$\frac{S_r}{S_t} = k\left(\frac{\lambda}{d}\right)^2 \quad (1)$$

where S_r is receiver signal strength; S_t is transmitter signal strength; k is constant value; λ is signal wavelength; d is distance between transmitter and receiver.

ISSN 2663 - 4023

Calculating the received signal strength from the transmitter is made by expression:

$$\underline{S_r} = min(S_t, S_{rmax}) \quad (2)$$

where $\underline{S_r}$ is received by receiver signal strength; S_{rmax} is maximum receiver signal strength.

Calculation of suppressed signal strength.

Electronic warfare (EW) devices degrade communication between other devices, i.e., reduce the strength of their signals.

$$\hat{S} = S - S_s \quad (3)$$

where S is initial signal strength; $\hat{S}$ is suppressed signal strength; S_s is EW signal strength.

Thus, we can enter the availability zones for each specific UAV device, and take into account the possibility or prohibition of routing through the territories located in the corresponding zones.

We will offer examples of the structure of prompts that explain the details of the mission to the LLM to clearly establish the context, in order to prevent hallucinations. In brackets {.} are given the specific data that is loaded into the LLM input in the json file of the specified structure.

```
MISSION TYPE: Reaching destination point
MISSION ID: Destination Point-{DATE}-{SEQUENCE}
PRIORITY: {HIGH/MEDIUM/LOW}
OPERATIONAL TIMEFRAME: {START_TIME} to {END_TIME}
PRIMARY OBJECTIVE: Disrupt enemy {RADAR_TYPE} radar operation in
{GEOGRAPHIC_DESCRIPTION}
SECONDARY OBJECTIVES:
- Collect electronic signatures during engagement
- Assess effectiveness of jamming operations
- Maintain concealment of friendly positions
RULES OF ENGAGEMENT:
- Minimize civilian infrastructure impact
- Maintain electronic emission discipline
- Coordinate with friendly air operations in AO
A MISSION SUCCESS CRITERIA:
- Enemy radar down time >80% during critical window
- No compromise of friendly jammer positions
- Collection of target radar characteristics
```

Fig. 1. Mission description prompt template

The Fig. 1 presents the structure of a prompt template designed to convey the UAV mission context to the LLM. The template includes key mission parameters such as the type of task (e.g., reconnaissance, delivery, surveillance), starting and target coordinates, constraints related to timing and risk zones, and behavioral rules in case of signal loss or threat detection. Each field is structured to provide the LLM with sufficient context to generate a relevant and secure route plan. The use of structured placeholders ({...}) enables dynamic filling of mission-specific data during automated pre-processing, ensuring consistency and minimizing ambiguity in model interpretation.

ISSN 2663 - 4023

```
Terrain Description Prompt Template
TERRAIN ANALYSIS (Pre-processed):
Area of Operations: Grid reference {UTM_COORDINATES}
DEM Analysis:
- Elevation range: {MIN_ELEVATION}m to {MAX_ELEVATION}m
- Dominant terrain features: {HILLS/VALLEYS/RIDGES} at bearings
{AZIMUTH_LIST}
- Line-of-sight calculations completed for target area
Key Terrain Features:
- Hill Mass Alpha: {COORDINATES}, elevation {HEIGHT}m, provides
{MASKING/OBSERVATION}
- Valley Bravo: {COORDINATES}, width {DISTANCE}m, concealment factor
{HIGH/MEDIUM/LOW}
- Ridge Charlie: {COORDINATES}, commanding view of
{AREA_DESCRIPTION}
Visibility Analysis:
- Dead zones: {COORDINATE_POLYGONS}
- Optimal observation positions: {COORDINATE_LIST} with
{LOS_DISTANCE}km range
- Concealed approach routes: {ROUTE_DESCRIPTIONS}
Terrain Constraints:
- Impassable areas: {COORDINATES_AND_REASONS}
- Seasonal limitations: {WEATHER_DEPENDENT_FACTORS}
- Civilian activity zones: {RESTRICTED_AREAS}
```

Fig. 2. Landscape description prompt template

The Fig. 2 shows a structured prompt template used to communicate terrain-related context to the LLM. It contains information derived from digital elevation models, in our research open maps [11] were used. Data can include relative height values, slope characteristics, and notable topographical features (e.g., ridges, valleys, plateaus). This data helps the LLM evaluate visibility, line-of-sight constraints, and the feasibility of maintaining communication between the UAV and relay nodes. The template supports dynamic population of elevation data and terrain segments, enabling adaptive route generation that accounts for physical obstacles and signal attenuation.

```
HOSTILE ELECTRONIC WARFARE THREAT ASSESSMENT:
PRIMARY TARGET:
- System Type: {RADAR_DESIGNATION} ({FREQUENCY_BAND}-band radar)
- Location: {PRECISE_COORDINATES} (confidence: {HIGH/MEDIUM/LOW})
- Technical Characteristics:
  * Operating frequency: {FREQUENCY_RANGE} MHz
  * Detection range: {RADAR_RANGE}km
  * Azimuth coverage: {DEGREES} degrees
  * Elevation scan: {MIN_ANGLE} to {MAX_ANGLE} degrees
  * Pulse repetition frequency: {PRF_RANGE}
  * Peak power output: {POWER_ESTIMATE}W
SUPPORTING EW INFRASTRUCTURE:
- Communication links: {FREQUENCY_BANDS} at {POWER_LEVELS}
- Backup power systems: {GENERATOR_SPECIFICATIONS}
- Operator patterns: {ACTIVITY_SCHEDULE}
DEFENSIVE MEASURES:
- Physical security: {DEFENSIVE_POSITIONS}
- Relocation capability: {MOBILE/STATIC} with {MOVEMENT_TIME} setup
time
```

a)

```
SECONDARY THREATS:
- Adjacent radar systems: {LOCATIONS_AND_TYPES}
- Communication intercept assets: {SIGINT_POSITIONS}
- Air defense coverage: {SAM_LOCATIONS_AND_RANGES}
VULNERABILITY ASSESSMENT:
- Susceptible frequencies: {VULNERABLE_BANDS}
- Power threshold for disruption: {JAMMING_POWER_REQUIRED}
- Critical timing windows: {OPTIMAL_ENGAGEMENT_TIMES}
```

b)

Fig. 3. Enemy devices description template: a)electronic warfare cyberphysical characteristics description, b)secondary characteristics for cyber-physical vulnerability assessment

Fig. 3 shows the structure of the prompt used to describe known or suspected adversarial assets, such as electronic warfare systems, jammers. The fields include geolocation, operational range, expected signal impact (e.g., jamming strength), and threat classification. This information is critical for cybersecurity-aware planning, allowing the LLM to generate routes that avoid areas with high risk of communication disruption or malicious signal injection. The template ensures that each device's characteristics are clearly defined and can be incorporated into threat-aware route computations.

The given prompts have a detailed description of the devices, the mission. If necessary, unnecessary fields can be excluded. These indicators are taken into account by LLM depending on the mission goal.

A complete list of developed prompt templates is given in [13].

Architecture of the proposed solution

1. The architecture for automating the task includes the following components:
2. Preprocessor (python script) that parses height maps, converts coordinates into a normalized grid and creates JSON with context for LLM, which includes height maps, targets, constraints, starting points.
3. Prompt generator (python script) — prepares the mission template for the current view, substitutes coordinates, heights from maps, constraints and other information. The instruction for LLM (prompt) is adjusted by a human operator taking into account the goals of a specific mission, the generator can provide typical examples.
4. LLM — component (via API) — receives the generated prompt and contextual data, processes them and outputs the path and/or sequence of actions in structured JSON.
5. Postprocessor (python script) — visualizes the route, performs route validity checks, visualizes on the map, if necessary, launches a repeated request to LLM.

Computer experiment

Using the developed prompt templates, the task was specified. The prompt that instructs the LLM to perform the necessary actions is shown in Fig. 4.

This figure displays the control prompt used to initiate UAV route planning via interaction with the LLM. The prompt combines mission-specific context, terrain data, and threat information into a cohesive natural-language instruction, formatted to guide the LLM in generating a secure and feasible route. It serves as the primary input that triggers the model's reasoning process, incorporating dynamic values such as starting point, destination, restricted zones, and operational constraints. This prompt acts as the central coordination message that binds together the information prepared by preprocessing modules and instructs the LLM to

ISSN 2663 - 4023

solve the routing task within the specified scenario. Also, operator can five the preferred output format options, as given in Fig. 5.

```
Generate a complete tactical drone mission dataset in JSON
format for the following scenario:
MISSION PARAMETERS:
Single drone reconnaissance mission
Start point: [latitude, longitude]
Target: [specific facility type] at [latitude, longitude]
Mission duration: [X hours]
Flight profile: NOE (Nap-of-Earth) stealth operations

THREAT ENVIRONMENT:
[N] Electronic Warfare stations with [X]km radius danger zones
[N] No-fly zones (cities, military bases)
Terrain elevation data available for optimization

ROUTE REQUIREMENTS:
Follow lowest possible terrain elevations for maximum stealth
Maintain minimum [X]km separation from all EW threat zones
Avoid populated areas and restricted airspace
Include detailed reconnaissance pattern at target
Use different ingress/egress routes for operational security

TACTICAL CONSIDERATIONS:
Prioritize terrain masking over speed
Ensure EW avoidance calculations are verified
Include reconnaissance pattern (perimeter survey)
Plan contingency routes
Maintain realistic flight speeds and timing

Generate tactically sound, operationally realistic mission data
that could be used for actual flight planning visualization and
analysis.
```

Fig. 4. Control prompt

```
OUTPUT FORMAT REQUIRED:
Mission metadata (name, duration, drone count, classification)
Threat objects with precise coordinates:
EW stations (type: "ew_zone", radius_km, threat_level)
Urban areas (type: "urban_area", population, restrictions)
Infrastructure (type: "factory"/"military"/"infrastructure")

Optimized waypoint sequence with:
Precise coordinates (6 decimal places)
MSL altitude (terrain + 50m AGL for stealth)
Timestamp for each waypoint
Tactical action description
Terrain elevation notes
Mission timeline with key events
Safe corridors data with elevation statistics
```

Fig. 5. Prompt, which sets requirements for data output

The example map, which is used for the test case, is based on open data elevation maps. The data was pre-processed using a python script, the corresponding heights are given in json format. The Claude Sonnet 4.0 model was used as the LLM.

Fig. 6 visualizes a piece of the open map with terrain conditions, green shows lowlands, yellow and brown are elevations, which can interfere with the drone's communication with the repeater. Yellow triangles show the location of facilities that can cause a disruption in the cyber-physical system and be a potential source of the spread of electronic warfare, so the route was laid taking into account their bypass. The labels show the location of the target and the starting point. In other words, yellow triangular markers indicate locations of adversarial devices,

ISSN 2663 - 4023

including electronic warfare systems, which are considered both as jamming sources and potential vectors for harmful signal propagation or malware injection. The LLM-generated route (shown as a path connecting the start and target locations) strategically avoids these high-risk zones, maintaining terrain-aware connectivity and minimizing exposure to cyber-physical threats. The example illustrates the model's ability to reason over geospatial and adversarial data, enabling secure and resilient UAV navigation.

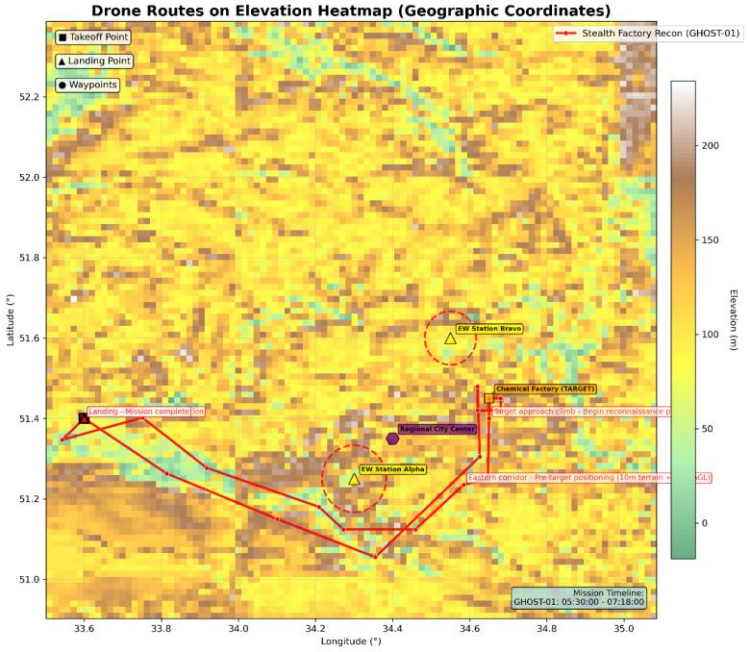
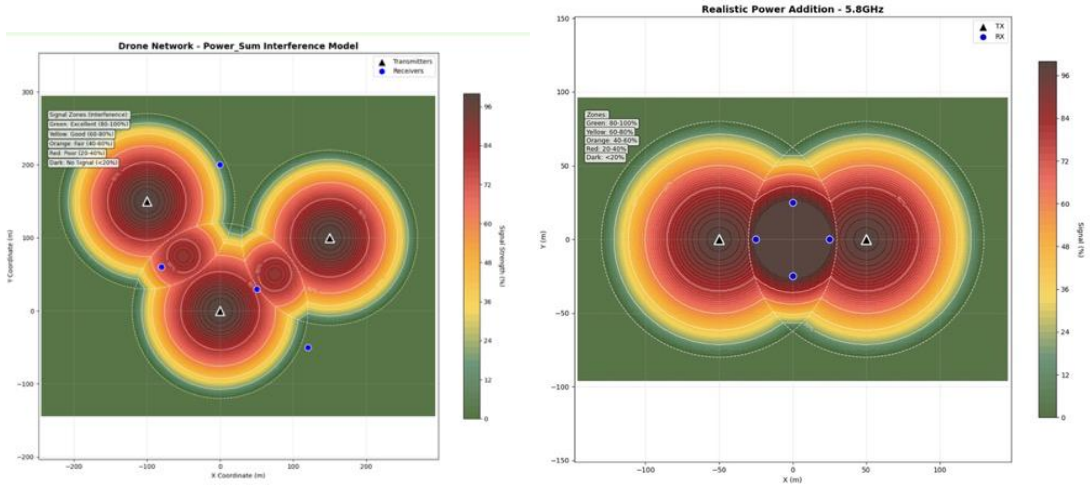


Fig. 6. Experiment results

The developed software also uses calculations of EW activity zones and EW interference. (Figs. 7, 8).



a) *b)*

Fig. 7. Areas of action of interference devices and/or propagation of harmful signals: a)three EW devices, b)two EW devices

Here are the zones of action of devices that disrupt accessibility by introducing radio signals that carry malicious data, or simply by noise of the corresponding radio frequencies.

ISSN 2663 - 4023

When laying a route, depending on the mission objective, it is possible to set the conditions for "bypassing the corresponding zones", which was done in the case of the route in Fig. 6.

In Fig. 7 there are interference zones. Zones are modeled based on the effective range and signal strength of known threat sources, using expressions (1)–(3), and taking into account terrain features and propagation characteristics. UAVs operating within these zones may experience communication loss, sensor malfunction, or cybersecurity risks such as protocol exploitation or data injection attacks. The figure demonstrates how such harmful signal zones are integrated into the route planning model as exclusion areas, prompting the LLM to generate paths that minimize exposure and preserve mission integrity.

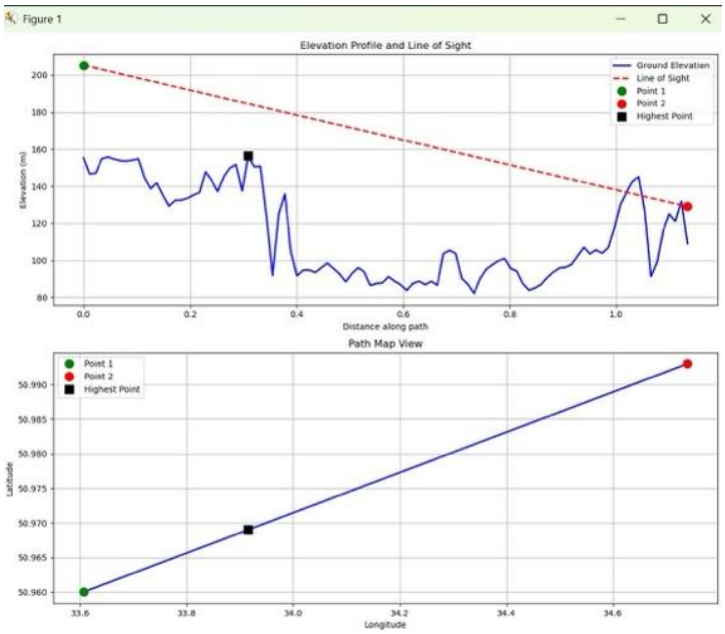


Fig. 8. Line-of-sight between the working drone and the repeater (hub), its projection onto the horizontal plane

When laying a route, zones of zero signal should also be taken into account.

The signal value is directly affected by interference, and the location of the repeater on the "Line-of-sight" (Fig. 8).

The relief heights are read from pre-processed data of height maps and can be taken into account when laying a route.

In Fig. 8, we see that the working drone and the repeater are not in line of sight of each other, because the terrain of the area prevents this. The corresponding zones are considered zero signal zones, in which the drone ceases to be controllable and acts according to the scenario defined in it for such cases (for example, fly vertically upwards until a signal appears).

The validity of the proposed routes was checked using the proposed metrics, including visually, based on expert opinion.

The validity of the route proposed by LLM is checked taking into account the following criteria:

1. Continuity of the route (the distance between any two adjacent points does not exceed the specified ε, all route points $(x_i, y_i, z_i) \in M$, where M is map area under consideration).
2. The route bypasses prohibited positions (areas of enemy dangerous devices).

3. Line-of-sight between the repeater and the drone is not interrupted by terrain heights.
4. The route includes a destination point — a target.

Depending on the mission objectives, it is possible to check for the presence of cycles, loops in the route (revisiting points).

For complex routes, these checks should be performed automatically, however, visual control of the route by a person is desirable.

CONCLUSION

This paper presents a novel approach to the problem of UAV route planning in environments where availability is threatened by both physical and cyber-physical factors. A key contribution is the development of a set of structured prompt templates that enable the injection of mission-specific context, terrain characteristics, and threat data into a large language model. These templates guide the LLM in reasoning over complex, heterogeneous input data and in generating route recommendations that are not only physically feasible but also resilient to cyber-physical disruptions.

To support the practical application of the proposed approach, a modular system architecture was designed and implemented. It includes preprocessing tools for terrain and threat data, dynamic prompt generation based on mission parameters, LLM-based reasoning via API, and postprocessing tools for route validation and visualization. This architecture enables the integration of real-time geospatial intelligence and LLM capabilities into an automated decision-support workflow for UAV mission planning. The computational experiments conducted using real elevation maps and simulated EW threat zones demonstrated the operability and effectiveness of the solution.

Future research directions include extending the approach to handle urban environments with complex structural occlusions, incorporating real-time updates from sensor networks, and addressing accessibility challenges specific to various wireless communication protocols, such as frequency hopping, cognitive radio, or directional beamforming.

ACKNOWLEDGEMENTS

The authors express their gratitude to the students of the Education and Scientific Institute of Physics and Technology Shanidze Davyd and Prykhodko Yurii for their help in setting up practical experiments. The results of the article were obtained within the framework of the tasks of the project under the patronage of the US National Academy of Science (US NAS) Towards Networked Airborne Computing in Uncertain Airspace: A Control and Networking Facilitated Distributed Computing Framework.

REFERENCES

1. Xie, J., Jin, L., & Garcia Carrillo, L. R. (2019). Optimal path planning for unmanned aerial systems to cover multiple regions. *AIAA Scitech 2019 Forum.* https://doi.org/10.2514/6.2019-1794
2. Novikov, O., Stopochkina, I., Ilin, M., Voitsekhovskyi, A., & Ovcharuk, M. (2024). Simulation of UAV networks on the battlefield, taking into account cyber-physical influences that affect availability. *Theoretical and Applied Cybersecurity*, *6*(2), 66–76. https://doi.org/10.20535/tacs.2664-29132024.2.318182

3. Foead, D., Ghifari, A., Kusuma, M. B., Hanafiah, N., & Gunawan, E. (2021). A systematic literature review of A* pathfinding. *Procedia Computer Science, 179*, 507–514. https://doi.org/10.1016/j.procs.2021.01.034
4. Fadzli, S. A., Abdulkadir, S. I., Makhtar, M., & Jamal, A. A. (2015). Robotic indoor path planning using Dijkstra's algorithm with multi-layer dictionaries. *2015 2nd International Conference on Information Science and Security (ICISS)*, 1–4. https://doi.org/10.1109/ICISSEC.2015.7371031
5. Tariq, M. T., Hussain, Y., & Wang, C. (2025). Robust mobile robot path planning via LLM-based dynamic waypoint generation. *Expert Systems with Applications, 282*, 127600. https://doi.org/10.1016/j.eswa.2025.127600
6. Wang, X., Liu, H., & Zhou, Q. (2024). LLM-A*: Large language model enhanced incremental heuristic search on path planning. *Findings of EMNLP 2024*, 765–778. https://aclanthology.org/2024.findings-emnlp.60.pdf
7. Lee, T., Zhang, R., & Kumar, A. (2025). UAV visual path planning using large language models. *Transportation Research Procedia, 95*, 721–728. https://doi.org/10.1016/j.trpro.2025.03.081
8. Ahmad, N., Lee, J., & Song, Y. (2025). Large language models for UAVs: Current state and pathways to the future. *arXiv preprint arXiv:2503.23132.* https://arxiv.org/html/2503.23132v1
9. Chen, Y., Li, Z., & Wang, M. (2024). LLM-DaaS: LLM-driven drone-as-a-service operations from text user requests. *arXiv preprint arXiv:2412.11672.* https://doi.org/10.48550/arXiv.2412.11672
10. Sandoval, J. M., Ivanov, D., & Roy, B. (2024). Scenario-driven evaluation of autonomous agents: Integrating large language model for UAV mission reliability. *Drones, 9*(3), 213. https://doi.org/10.3390/drones9030213
11. European Space Agency. (n.d.). *Copernicus Digital Elevation Model datasets (30m).* Retrieved from https://copernicus-dem-30m.s3.amazonaws.com/readme.html
12. Department of Defense. (n.d.). *Electronic warfare fundamentals* (PDF manual). Retrieved from https://falcon.blu3wolf.com/Docs/Electronic-Warfare-Fundamentals.pdf
13. Impress-U-IS-KPI. (n.d.). *UAV routing and mission planning tools* [GitHub repository]. Retrieved from https://github.com/Impress-U-IS-KPI/data_processing , https://github.com/Impress-U-IS-KPI/LLM-based_path_planning

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Новіков Олексій
доктор технічних наук, професор,
директор навчально-наукового інституту фізики та техніки
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0000-0001-5988-3352
o.novikov@kpi.ua

Ілін Микола
кандидат технічних наук, доцент, доцент кафедри інформаційної безпеки
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0000-0002-1065-6500
m.ilin@kpi.ua

Стопочкіна Ірина
кандидат технічних наук, доцент, доцент кафедри інформаційної безпеки
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0000-0002-0346-0390
i.stopochkina@kpi.ua

Овчарук Микола
аспірант кафедри інформаційної безпеки
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0009-0000-5791-3925
m.ovcharuk@kpi.ua

Войцеховський Андрій
аспірант, доцент кафедри інформаційної безпеки
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0009-0004-6009-9492
a.voitsekhovskyi@kpi.ua

ЗАСТОСУВАННЯ LLM У ЗАВДАННЯХ ПЛАНУВАННЯ МАРШРУТІВ БПЛА ДЛЯ ЗАПОБІГАННЯ ПОРУШЕННЯМ ДОСТУПНОСТІ ОБМІНУ ДАНИМИ

Анотація. У цій статті представлено новий підхід до планування маршрутів безпілотних літальних апаратів (БПЛА) в умовах кіберфізичних загроз, що впливають на доступність системи. У ворожих і спірних середовищах БПЛА все частіше стикаються не тільки з природними перешкодами та електронними перешкодами, але й із цілеспрямованими кіберзагрозами. Запропонований метод стосується як навмисних, так і ненавмисних порушень зв'язку та управління, включаючи перешкоди від систем електронної війни (EW), глушіння та поширення зловмисних сигналів. Важливо, що пристрої РВ розглядаються не тільки як джерела електромагнітних перешкод, але й як потенційні вектори для поширення шкідливого програмного забезпечення або атак на бездротові протоколи, що робить їх критично важливими компонентами ландшафту кіберзагроз. Для забезпечення успіху місії та підтримання надійного обміну даними метод інтегрує карти висот місцевості, відкриті для використання цифрові моделі висот (DEM) та геопросторові дані з міркуваннями, що базуються на великих мовних моделях (LLM). Система будує маршрути БПЛА, які зберігають пряму видимість, уникають зон підвищеного ризику та адаптуються до топологічних та ворожих обмежень. Впроваджено модульну архітектуру, що включає попередню обробку даних, генерацію підказок у контексті місії, висновок на основі LLM та перевірку після обробки. Обчислювальний експеримент з використанням реальних даних про висоту над рівнем моря та моделі Claude Sonnet 4 підтверджує застосовність запропонованого рішення. Результати демонструють, що LLM, інтегровані з геопросторовими даними, що враховують кібербезпеку, можуть підтримувати динамічне

планування маршрутів БПЛА та зменшувати ризик порушень доступності, спричинених як фізичним втручанням, так і кібервтручанням.

Ключові слова: кіберфізична безпека; БПЛА; порушення доступності та цілісності; планування маршрутів; LLM.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Xie, J., Jin, L., & Garcia Carrillo, L. R. (2019). Optimal path planning for unmanned aerial systems to cover multiple regions. *AIAA Scitech 2019 Forum.* https://doi.org/10.2514/6.2019-1794
2. Novikov, O., Stopochkina, I., Ilin, M., Voitsekhovskyi, A., & Ovcharuk, M. (2024). Simulation of UAV networks on the battlefield, taking into account cyber-physical influences that affect availability. *Theoretical and Applied Cybersecurity*, *6*(2), 66–76. https://doi.org/10.20535/tacs.2664-29132024.2.318182
3. Foead, D., Ghifari, A., Kusuma, M. B., Hanafiah, N., & Gunawan, E. (2021). A systematic literature review of A* pathfinding. *Procedia Computer Science*, *179*, 507–514. https://doi.org/10.1016/j.procs.2021.01.034
4. Fadzli, S. A., Abdulkadir, S. I., Makhtar, M., & Jamal, A. A. (2015). Robotic indoor path planning using Dijkstra's algorithm with multi-layer dictionaries. *2015 2nd International Conference on Information Science and Security (ICISS)*, 1–4. https://doi.org/10.1109/ICISSEC.2015.7371031
5. Tariq, M. T., Hussain, Y., & Wang, C. (2025). Robust mobile robot path planning via LLM-based dynamic waypoint generation. *Expert Systems with Applications*, *282*, 127600. https://doi.org/10.1016/j.eswa.2025.127600
6. Wang, X., Liu, H., & Zhou, Q. (2024). LLM-A*: Large language model enhanced incremental heuristic search on path planning. *Findings of EMNLP 2024*, 765–778. https://aclanthology.org/2024.findings-emnlp.60.pdf
7. Lee, T., Zhang, R., & Kumar, A. (2025). UAV visual path planning using large language models. *Transportation Research Procedia*, *95*, 721–728. https://doi.org/10.1016/j.trpro.2025.03.081
8. Ahmad, N., Lee, J., & Song, Y. (2025). Large language models for UAVs: Current state and pathways to the future. *arXiv preprint arXiv:2503.23132.* https://arxiv.org/html/2503.23132v1
9. Chen, Y., Li, Z., & Wang, M. (2024). LLM-DaaS: LLM-driven drone-as-a-service operations from text user requests. *arXiv preprint arXiv:2412.11672.* https://doi.org/10.48550/arXiv.2412.11672
10. Sandoval, J. M., Ivanov, D., & Roy, B. (2024). Scenario-driven evaluation of autonomous agents: Integrating large language model for UAV mission reliability. *Drones*, *9*(3), 213. https://doi.org/10.3390/drones9030213
11. European Space Agency. (n.d.). *Copernicus Digital Elevation Model datasets (30m).* Retrieved from https://copernicus-dem-30m.s3.amazonaws.com/readme.html
12. Department of Defense. (n.d.). *Electronic warfare fundamentals* (PDF manual). Retrieved from https://falcon.blu3wolf.com/Docs/Electronic-Warfare-Fundamentals.pdf
13. Impress-U-IS-KPI. (n.d.). *UAV routing and mission planning tools* [GitHub repository]. Retrieved from https://github.com/Impress-U-IS-KPI/data_processing , https://github.com/Impress-U-IS-KPI/LLM-based_path_planning