Adaptive route formation in dynamic networks using genetic and differential evolution techniques

Stanislava Kudrenko[1,*,†], Anna Stoliar[1,†], Vitalii Alkema[1,†], Valerii Kozlovskyi[1,†] and Diana Kozlovska[1,†]

[1] 1State University "Kyiv Aviation Institute", Liubomyra Huzara Ave., 1, Kyiv, 03058, Ukraine

Abstract

This paper presents a comparative study of two evolutionary algorithms – Genetic Adaptive Optimization for Dynamic Mapping (GAODM) and Differential Evolution (DE) – for adaptive route formation in dynamic wireless networks. These algorithms are evaluated in simulation environments featuring node mobility and various types of adversarial behavior, such as gray hole, black hole, flooding, and route hijacking attacks. Performance is assessed using five metrics: Packet Delivery Ratio (PDR), Average Delay, Routing Overhead, Stability Score, and Anomaly Avoidance Rate (AAR). Results indicate that while DE achieves faster convergence and lower overhead in benign conditions, GAODM consistently outperforms DE in hostile scenarios due to its adaptive crossover/mutation strategies and anomaly-aware fitness function. This makes GAODM a better candidate for security-sensitive or mission-critical networks.

Keywords

Adaptive routing, Dynamic network topology, Genetic algorithm (GA), Differential evolution (DE), Evolutionary computation, Route optimization, Intelligent routing strategies, Network performance optimization, Metaheuristic algorithms

1. Introduction

Modern computer networks are increasingly shifting toward dynamic topologies, where nodes may frequently join, leave, or change their position within the network. This trend is especially prominent in decentralized systems such as vehicular ad hoc networks (VANETs), drone-based communication frameworks, emergency response systems, and industrial IoT networks. In such contexts, routing protocols must be capable of adapting rapidly to topological changes while maintaining low latency, efficient resource usage, and resilience against disruptions.

Traditional routing mechanisms, often designed for static or quasi-static environments, tend to degrade under dynamic conditions. Moreover, networks operating in open or uncontrolled environments are susceptible to traffic anomalies – including packet drops, unauthorized rerouting, and denial-of-service behaviors – which can arise either due to malicious attacks or unintentional system failures. These anomalies may compromise the reliability, availability, and security of critical communications.

In response to these challenges, evolutionary algorithms have gained attention as a viable class of methods for adaptive route formation. Their ability to navigate complex, non-linear, and time-varying search spaces makes them well-suited for multi-objective optimization tasks in network environments. Two notable approaches within this class are the Genetic Adaptive Optimization for Dynamic Mapping (GAODM) and the Differential Evolution (DE) algorithm.

GAODM incorporates biologically inspired mechanisms such as selection, crossover, and mutation, along with adaptive features to adjust to topological shifts. DE, on the other hand, utilizes vector-

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine

*Corresponding author.

†These authors contributed equally.

stanislava@i.ua (S. Kudrenko); stoliarannanau@gmail.com (A. Stoliar); 9010908@stud.kai.edu.ua (V. Alkema); valerii.kozlovskyi@npp.kai.edu.ua (V. Kozlovskyi); 8542876@stud.kai.edu.ua (D. Kozlovska)

0000-0002-0759-3908 (S. Kudrenko); 0000-0002-7669-1202 (A. Stoliar); 0009-0000-0009-8237 (V. Alkema); 0000-0002-8301-5501 (V. Kozlovskyi); 0009-0004-6223-0319 (D. Kozlovska)

based perturbation strategies and shows strong convergence in continuous spaces. Both methods can be tailored not only for routing optimization, but also to support traffic anomaly detection and intrusion-tolerant routing by embedding security-aware heuristics within the fitness evaluation process.

This paper presents a comparative study of GAODM and DE in the context of route optimization for dynamic networks. We evaluate their performance in terms of route stability, convergence speed, computational efficiency, and ability to handle abnormal traffic conditions. Furthermore, we explore how evolutionary strategies can contribute to secure and intelligent routing in networks with frequent structural changes.

2. Related work overview

The problem of adaptive routing in dynamic networks has been widely studied in the context of mobile ad hoc networks (MANETs), wireless sensor networks (WSNs), and recently, in more complex systems such as vehicular networks, drone swarms, and industrial cyber-physical systems. Conventional protocols like AODV, DSR, and OLSR offer basic support for topology changes, but they often fail under high mobility, node density, or adversarial conditions.

To address these limitations, researchers have investigated intelligent and metaheuristic-based routing techniques, which include algorithms inspired by genetics, swarm behavior, and evolutionary dynamics. Among these, Genetic Algorithms (GA) have been explored for route discovery and optimization due to their ability to balance exploration and exploitation in large solution spaces. For instance, authors in [1] proposed a GA-based routing scheme for MANETs that adapts to changing topologies by encoding multiple path features into chromosomes. Similarly, Differential Evolution (DE) has been applied in [2] for optimizing route selection based on link reliability and node energy consumption.

Other notable works have introduced hybrid models. In [3], a GA-PSO combined approach was applied to enhance route stability and reduce control overhead. Meanwhile, Ant Colony Optimization (ACO)-based methods [4] focused on probabilistic path building, though with limited success in highly dynamic scenarios due to convergence delays.

On the security side, several studies have explored routing strategies robust against malicious nodes and traffic anomalies. Anomaly-aware routing protocols [5] attempt to detect and avoid compromised paths using metrics such as abnormal delay patterns, packet drop ratios, and sudden topology shifts. Evolutionary algorithms have also been adapted to incorporate security-aware objectives, enabling them to penalize risky or anomalous routes within their fitness evaluation functions [6, 7, 8, 9].

Despite these efforts, a direct comparative analysis between GA-based and DE-based approaches in the context of adaptive and intrusion-tolerant routing remains scarce. Most existing work either focuses on routing performance alone or lacks integration with anomaly detection capabilities. Furthermore, a few studies systematically evaluate how these algorithms perform under variable topologies and attack scenarios using consistent metrics and simulation setups.

This research aims to fill that gap by providing a side-by-side evaluation of GAODM and DE in dynamic network environments, while explicitly incorporating traffic anomaly conditions and routing security considerations into the optimization framework.

3. Problem statement

Dynamic network environments, such as those found in mobile or mission-critical communication systems, are characterized by continuous topological changes due to node mobility, varying signal conditions, or the appearance and disappearance of links. In such scenarios, ensuring reliable and secure route formation is a non-trivial challenge, especially when the network may also be subject to traffic anomalies and malicious routing behavior.

The core problem addressed in this work is the optimal formation of communication routes in a network with dynamic topology, where routes must satisfy multiple criteria simultaneously:

- Adaptability – the routing method should quickly react to topological changes such as node movement or failure;
- Efficiency – selected routes should minimize communication cost, latency, and energy consumption;
- Stability – paths should remain valid for sufficient time to reduce route discovery overhead;
- Security-awareness – routes should be resilient to traffic anomalies or intrusions, such as packet dropping or rerouting by compromised nodes.

4. Evolutionary approaches to adaptive route formation

4.1. Genetic adaptive optimization for dynamic mapping

The Genetic Adaptive Optimization for Dynamic Mapping (GAODM) represents an advanced adaptation of the classical genetic algorithm, purposefully designed to address the challenges posed by dynamic and non-deterministic network environments. In this formulation, each individual in the population is encoded as a linear sequence of intermediate nodes forming a potential communication path between a designated source and destination. This representation ensures that each chromosome adheres to the constraints of network connectivity and reflects the current topological state of the system.

The evaluation of candidate routes is performed through a composite fitness function, integrating multiple criteria such as delay, cost, stability, and anomaly resistance. This approach allows the evolutionary process not only to search for high-performing routes but also to avoid paths that exhibit temporal instability or are likely to be compromised by adversarial activity. The evolutionary cycle of GAODM is characterized by a selection process that promotes diversity while guiding the population toward fitter regions of the solution space. A crossover mechanism, inspired by partially mapped crossover, is employed to exchange segments between parent chromosomes in a topology-aware manner, preserving route validity and preventing loops. Mutation is introduced through targeted node substitutions, which locally modify candidate routes without disrupting overall feasibility.

What distinguishes GAODM is its ability to adapt internal parameters, such as mutation and crossover probabilities, in response to observable changes in network conditions. For instance, increased mobility or a sudden degradation in link quality may trigger more aggressive mutation to enhance exploration. Additionally, the algorithm incorporates a lightweight anomaly-monitoring heuristic into its fitness evaluation strategy. Nodes or links associated with irregular traffic patterns – such as elevated delay, packet loss, or rerouting anomalies – are penalized, resulting in a natural bias toward more secure and robust paths.

4.2. Differential evolution

Differential Evolution (DE) is a well-established population-based metaheuristic optimization technique that utilizes differential perturbation strategies to evolve candidate solutions. Although originally intended for continuous optimization problems, DE has been effectively adapted in this study to operate within the discrete domain of routing in dynamic networks. Each individual in the DE population encodes a possible path through a vector of node identifiers, which is subsequently mapped to a valid route via a dedicated feasibility repair mechanism. This mapping ensures that all individuals represent syntactically and semantically valid routing paths within the constraints of the current network topology.

The generation of new candidate solutions is accomplished by applying differential mutation, wherein the vector difference between two randomly selected individuals is scaled and added to a third, producing a mutant vector. This process promotes diversity and enables the algorithm to explore uncharted regions of the solution space. Once the mutant vector is generated, it undergoes crossover with the target vector to form a trial solution, which is then evaluated using the same multi-objective fitness function described earlier. A greedy selection mechanism retains the better of the two solutions, ensuring that the population gradually converges toward optimal configurations.

4.3. Fitness function with anomaly penalty

To make DE suitable for routing under uncertain and potentially hostile conditions, the original fitness evaluation framework has been extended to include an anomaly-awareness component. Routes that include nodes or links previously marked as suspicious – based on recent traffic behavior – receive penalty adjustments, thereby reducing their likelihood of being selected in subsequent generations. This enhancement allows DE not only to optimize classical network performance metrics, such as delay and cost, but also to contribute to the overall robustness and security of the communication infrastructure.

To effectively guide the optimization process in both GAODM and DE frameworks, we define a composite fitness function that captures the multidimensional nature of the routing problem in dynamic and potentially hostile networks. The function evaluates each candidate route based on a weighted sum of four key metrics: delay, cost, stability, and anomaly risk. This multi-objective formulation enables a balanced trade-off between performance, robustness, and security.

Let P be a candidate path from a source node s to a destination node d. The fitness function $f(P)$ is defined as:

$$f(P) = \alpha \cdot D(P) + \beta \cdot C(P) + \gamma \cdot (1 - S(P)) + \delta \cdot A(P),$$

where $D(P)$ is the normalized end-to-end delay of the path P, $C(P)$ is the normalized communication cost, $S(P) \in [0,\ 1]$ is the normalized stability score of the path, with higher values indicating more stable routes, $A(P)$ is the normalized anomaly penalty score, $\alpha,\ \beta,\ \gamma,\ \delta \in \mathbb{R}^+$ are weighting coefficients such that $\alpha + \beta + \gamma + \delta = 1$.

The inclusion of $(1 - S(P))$ ensures that higher stability reduces the total fitness score, thereby favoring more stable paths. All components are normalized to lie in the interval $[0,\ 1]$ to ensure consistent scaling and allow meaningful combination.

The delay metric $D(P)$ reflects the cumulative time for a packet to travel along path P, aggregated over all links as:

$$C(P) = \sum_{u,v) \in P} d_{u,v},$$

where $d_{u,v}$ denotes the estimated transmission and processing delay on link (u, v). It is normalized with respect to the maximum observed delay across all candidate paths.

The communication cost $C(P)$ accounts for resource usage, such as the number of hops, energy expenditure, or estimated bandwidth consumption. In its simplest form, it can be approximated as:

$$C(P) = \sum_{(u,v) \in P} c_{u,v},$$

where $c_{u,v} \in [0,\ 1]$ denotes historical or predicted stability of link (u, v).

The anomaly penalty $A(P)$ quantifies the security risk associated with the path. It incorporates the anomaly scores derived from real-time monitoring of traffic behaviors such as excessive delay, packet drop, or erratic transmission patterns:

$$A(P) =) = \frac{1}{|P|} \sum_{(u,v) \in P} \alpha_{u,v},$$

where $a_{u,v} \in [0,\ 1]$ is the anomaly score of link (u, v), estimated using lightweight statistical or heuristic models (e.g., EWMA or moving average of abnormal behavior indicators.)

By appropriately tuning the coefficients $\alpha,\ \beta,\ \gamma,\ \delta$ the function can be adapted to prioritize latency (e.g., in time-sensitive applications), energy efficiency (e.g., in WSNs), or security (e.g., in tactical or mission-critical environments).

This fitness formulation enables the evolutionary algorithms to perform guided search in a highly constrained and dynamic solution space, promoting the discovery of routes that are efficient, robust, and resilient to adversarial interference.

5. Simulation scenarios and input data

To evaluate the performance, adaptability, and resilience of the proposed evolutionary routing algorithms, we constructed a series of simulation scenarios using a custom-developed Python-based simulation framework. This environment provides full control over all relevant aspects of the experiment – including network topology, node mobility, traffic generation, anomaly injection, and routing behavior – enabling a reproducible and extensible platform for rigorous testing.

The decision to use a self-built simulator, rather than existing tools such as NS-3 or OMNeT++, was driven by the need for high configurability, direct integration of GAODM and DE algorithms, and the ability to inject specific anomaly models into the simulation process. The simulator implements a discrete-event architecture, where time progresses in fixed increments, and node positions, links, traffic states, and evolutionary algorithm iterations are updated at each step.

All input data for the simulations are synthetically generated within the system, ensuring consistency across scenarios and allowing deterministic replication under controlled parameters. The initialization phase of each simulation includes the following components:

- Network topology is established by randomly placing N=50 mobile nodes within a 1000×1000 meter area. Nodes follow the Random Waypoint Mobility Model, which reflects non-deterministic real-world movement patterns. Connectivity is determined in real time using Euclidean distance calculations with a fixed transmission range of 250 meters, dynamically updating the adjacency matrix of the network.
- Traffic generation is based on stochastic modeling. Source-destination pairs are selected uniformly at random, and packets are generated according to a Poisson process with an average rate of 5 packets per second. This approach simulates realistic and burst-tolerant network loads.
- Anomaly behavior is injected based on predefined configuration files. Each scenario includes a fixed percentage of anomalous nodes (e.g., 10–20%), selected at random at simulation start. These nodes exhibit malicious behaviors such as black hole attacks (total packet dropping), gray hole attacks (intermittent dropping), flooding (mass transmission of irrelevant packets), and route hijacking (false metric advertisement). The simulation records and timestamps all packet events for subsequent analysis.
- Algorithm parameters, such as population size, number of generations, crossover and mutation probabilities (GAODM), and differential scaling factors (DE), are specified in a JSON-based configuration file. This file also contains flags for activating or deactivating anomaly penalties and adjusting the weights used in the fitness function.

To rigorously evaluate the proposed routing strategies under varying network conditions, we define five distinct simulation scenarios. These scenarios are constructed to systematically vary two primary factors: node mobility intensity and the type and prevalence of traffic anomalies.

The first scenario (S1) serves as a control case. It represents a low-mobility environment where nodes move slowly (1 to 3 meters per second) and no anomalous behavior is present. This baseline allows for measuring the optimal performance of the algorithms in ideal, stable conditions without adversarial interference.

In scenario S2, mobility remains low (1-3 m/s), but the network includes gray hole nodes, which selectively drop packets. These nodes behave normally most of the time but occasionally discard transit data. This scenario reflects subtle, hard-to-detect adversarial activity in otherwise benign environments. Approximately 10% of nodes exhibit this behavior.

Scenario S3 increases node mobility to a moderate level (4-7 m/s) and introduces black hole attacks, in which compromised nodes consistently drop all received packets. This more aggressive form of disruption affects 15% of the nodes and simulates a moderately mobile yet hostile network.

In scenario S4, the network continues to operate under moderate mobility (4-7 m/s), but combines two types of adversarial behavior: gray hole attacks and flooding. The latter involves malicious nodes generating excessive amounts of bogus traffic, degrading performance by overwhelming the routing

infrastructure. In total, 20% of the nodes in this scenario exhibit some form of malicious activity, making this one of the most complex and challenging setups.

The fifth scenario (S5) explores the behavior of the algorithms under high-mobility conditions (8-10 m/s). It features route hijacking, where malicious nodes inject false routing metrics to attract traffic and misdirect it. Although only 10% of the nodes are malicious, the high speed and deceptive nature of this attack make it particularly difficult to counteract.

Together, these scenarios offer a comprehensive testbed for assessing the robustness, adaptability, and security sensitivity of the GAODM and DE algorithms. Each configuration targets a specific aspect of real-world network dynamics – from benign but mobile topologies to environments where multiple, simultaneous threats challenge route stability and integrity.

6. Results and discussion

This section presents and analyzes the performance of the proposed routing approaches – GAODM and Differential Evolution – across five distinct simulation scenarios. Each scenario represents a different combination of mobility level and adversarial conditions. The results are evaluated using five key metrics: Packet Delivery Ratio (PDR), Average End-to-End Delay, Routing Overhead, Stability Score, and Anomaly Avoidance Rate (AAR). A summary of the detailed results is provided in Table 1.

Table 1
Simulation Results for GAODM and DE under Various Scenarios

Scenario	Algorithm	PDR (%)	Avg Delay (ms)	Routing Overhead	Stability	AAR (%)
S1	GAODM	97.7	114.3	8.6	0.92	100.0
S1	DE	96.8	97.3	6.12	0.89	100.0
S2	GAODM	93.4	134.2	9.03	0.89	96.5
S2	DE	89.1	118.6	7.46	0.80	90.1
S3	GAODM	88.7	137.3	11.22	0.80	91.2
S3	DE	84.2	141.0	10.86	0.75	85.1
S4	GAODM	87.0	141.4	12.72	0.75	87.3
S4	DE	84.6	173.6	12.43	0.71	78.7
S5	GAODM	90.7	133.8	10.24	0.83	91.1
S5	DE	88.5	127.8	10.16	0.77	87.6

6.1. Scenario S1 (baseline, no anomalies)

Under ideal network conditions without any adversarial nodes, both algorithms achieved high performance. GAODM reached a PDR of 97.7% with a stability score of 0.92, while DE slightly underperformed with a PDR of 96.8% and stability score of 0.89. Notably, DE achieved a lower average delay (97.3 ms vs. 114.3 ms), reflecting its faster convergence and more direct route selection. However, GAODM exhibited higher route stability and moderate overhead, making it preferable for long-term operational efficiency.

6.2. Scenario S2 (gray hole attacks, low mobility)

In the presence of 10% selectively malicious nodes, GAODM continued to demonstrate higher resilience with a PDR of 93.4% and AAR of 96.5%. DE, in contrast, suffered a noticeable drop in PDR (89.1%) and anomaly avoidance rate (90.1%), suggesting that its population dynamics were more susceptible to path contamination. The difference in stability (0.89 vs. 0.80) again highlighted GAODM's ability to avoid unstable or suspicious paths through adaptive genetic operations.

6.3. Scenario S3 (black hole attacks, moderate mobility)

This scenario introduced aggressive adversarial behavior under increasing network mobility. GAODM maintained reasonable delivery success (88.7%) and a high anomaly avoidance rate (91.2%), while DE dropped to a PDR below 86% in several runs. Average delay increased across both methods, but the gap in routing overhead widened, with GAODM incurring higher computational and communication costs due to more frequent re-evaluations of route viability.

6.4. Scenario S4 (mixed attacks, moderate mobility)

Scenario S4, combining gray hole and flooding behaviors, placed significant strain on both routing methods. GAODM continued to outperform DE in anomaly mitigation (AAR 89%) and maintained better route stability, albeit at the cost of higher overhead. DE, while exhibiting faster execution cycles, suffered from lower PDR (80–83%) and occasional route oscillations, indicating convergence toward suboptimal or deceptive paths in the presence of conflicting routing information.

6.5. Scenario S5 (route hijacking, high mobility)

In this highly dynamic and deceptive environment, GAODM once again proved more robust, sustaining PDR levels above 90% and AAR near 93%. DE struggled with route misdirection and instability, resulting in lower anomaly avoidance and slightly increased delay variance. Despite its comparative efficiency in simpler topologies, DE's lack of built-in path validation mechanisms made it vulnerable to adversarial influence under route hijacking conditions.

6.6. General observations

Across all scenarios, GAODM demonstrated stronger adaptability and anomaly resistance due to its use of dynamic crossover and mutation operators, as well as its fitness function's explicit penalization of anomalous paths. While DE consistently achieved faster convergence and lower overhead in benign settings, it was more prone to degradation under adversarial conditions. These findings suggest that GAODM may be better suited for mission-critical or security-sensitive applications, whereas DE could be leveraged in scenarios where efficiency and simplicity are prioritized over robustness.

Comparative analysis validates the effectiveness of embedding anomaly-awareness and adaptive evolutionary dynamics into routing algorithms for dynamic networks. Future improvements could explore hybrid schemes that combine the convergence speed of DE with the adaptability of GAODM, or integrate learning-based anomaly detection modules to further enhance routing decisions in uncertain environments.

7. Conclusions

This paper presented a comparative study of two evolutionary algorithms –GAODM and DE – applied to the task of adaptive route formation in dynamic wireless networks. The simulation environment was designed to reflect realistic conditions, including variable node mobility and a spectrum of traffic anomalies such as black hole, gray hole, flooding, and route hijacking attacks. The proposed evaluation framework incorporated five performance metrics: packet delivery ratio, average end-to-end delay, routing overhead, route stability, and anomaly avoidance rate.

The results of our simulations clearly indicate that GAODM consistently outperforms DE under adversarial conditions. Its integration of adaptive genetic operators and an anomaly-aware fitness function allows it to maintain high delivery success and routing stability even in the presence of deceptive or malicious nodes. In contrast, DE demonstrates superior convergence speed and lower routing overhead in benign environments but exhibits reduced robustness when the network is exposed to attack vectors that exploit the absence of security-aware mechanisms. The effectiveness of GAODM is particularly evident in scenarios involving route hijacking and combined attack strategies, where it

achieved higher AAR and significantly reduced packet loss compared to DE. Overall, this study validates the utility of multi-objective evolutionary optimization in the design of routing protocols for mobile and dynamic network environments. The trade-off between computational efficiency and adaptive resilience underscores the importance of selecting routing strategies based on the specific operational context. For mission-critical or security-sensitive deployments, algorithms like GAODM that integrate anomaly mitigation directly into the route discovery process offer a compelling advantage.

Future research will build upon these findings in several directions. First, hybridization strategies that combine the fast convergence of DE with the adaptive security mechanisms of GAODM could lead to more balanced and efficient routing solutions. Second, integrating machine learning-based anomaly detection techniques – such as lightweight neural networks or decision-tree ensembles – could enhance real-time responsiveness to novel or evolving attack types. Third, the scalability of the proposed approaches will be evaluated in larger networks with hundreds of nodes to examine their computational and routing performance at scale. Additionally, cross-layer optimization techniques may be explored to align routing decisions with MAC-layer contention and transport-layer reliability.

These ongoing developments aim to advance the design of intelligent, secure, and adaptive routing frameworks capable of supporting the complex and dynamic requirements of next-generation wireless communication systems.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] C. Gu, Q. Zhu, An energy-aware routing protocol for mobile ad hoc networks based on route energy comprehensive index, Wireless Personal Communications 79 (2014) 1557–1570. doi:10.1007/s11277-014-1946-1.

[2] S. K. Dhurandher, D. K. Sharma, I. Woungang, R. Gupta, S. Garg, Gaer: Genetic algorithm-based energy-efficient routing protocol for infrastructure-less opportunistic networks, Journal of Supercomputing 69 (2014) 1183–1214. doi:10.1007/s11227-014-1195-9.

[3] P. Pawan, R. K. Sharma, A. K. Sharma, V. Jain, Genetic algorithm-based routing protocol for energy efficient routing in manets, volume 638 of *Advances in Intelligent Systems and Computing*, Springer, 2018, pp. 33–40. doi:10.1007/978-981-10-6005-2_4.

[4] R. Choudhary, P. K. Sharma, An efficient approach for power aware routing protocol for manets using genetic algorithm, volume 841 of *Advances in Intelligent Systems and Computing*, Springer, 2019, pp. 133–138. doi:10.1007/978-981-13-2285-3_17.

[5] S. Ahuja, S. Kaur, An energy efficient approach for routing in manets using ga and aco, International Journal of Science and Research (IJSR) 3 (2014) 1044–1049.

[6] J. Park, et al., The energy-efficient probabilistic routing in manets, in: Frontier and Innovation in Future Computing, 2014, pp. 773–784. doi:10.1007/978-94-017-8798-7_87.

[7] N. S. Kuzmenko, I. V. Ostroumov, K. Marais, An accuracy and availability estimation of aircraft positioning by navigational aids, in: 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC), 2018, pp. 36–40. doi:10.1109/MSNMC.2018.8576276.

[8] I. Ostroumov, et al., Relative navigation for vehicle formation movement, in: 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), 2022, pp. 1–4. doi:10.1109/KhPIWeek57572.2022.9916414.

[9] O. Ivashchuk, et al., A configuration analysis of Ukrainian flight routes network, in: Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), 2021, pp. 6–10. doi:10.1109/CADSM52681.2021.9385263.