Design and Architecture of Robotized Unmanned Ground Vehicle (UGV)-Based Intrusion Detection Perimeter Security Systems

Simeon Angelov
Omnitel LTD
Sofia, Bulgaria
s.angelov@omnitel.bg

Abstract **- Perimeter security is critical for protecting military installations, industrial complexes, and critical infrastructure. Recent advances in robotics, sensor technologies, and machine learning have spurred the development of robotized Unmanned Ground Vehicle (UGV)-based intrusion detection systems (IDS) that promise to enhance security by offering autonomous, continuous, and dynamic surveillance capabilities. This paper introduces a novel design and architecture for such systems that emphasizes modularity, advanced sensor fusion, robust autonomous navigation, and integrated cybersecurity measures. Our proposed architecture incorporates an innovative multi-layered design comprising a hardware layer with enhanced UGV platforms and heterogeneous sensor arrays, a perception layer utilizing adaptive sensor fusion, a decision-making layer employing ensemble machine learning techniques for intrusion detection, and a secure communication and integration layer. Extensive experiments conducted in both controlled and real-world environments demonstrate significant improvements in detection accuracy, response time, and operational reliability compared to conventional systems. We discuss the design rationale, detailed implementation, experimental evaluation, and potential future directions for this emerging technology.**

Keywords— Unmanned Ground Vehicle-UGV, Intrusion Detection, Perimeter Security, Sensor Fusion, Autonomous Navigation, Cybersecurity, Machine Learning

I. INTRODUCTION

Traditional perimeter security systems have relied heavily on fixed installations such as closed-circuit television (CCTV) cameras, motion detectors, and human patrols. Although these methods offer baseline surveillance, they are inherently limited by static coverage, high operational costs, and the inability to rapidly adapt to evolving threat landscapes. The advent of unmanned systems [1], [2], [3], [4] has introduced a new paradigm in security operations. In particular, robotized UGVs offer mobility, flexibility, and the capacity to navigate challenging terrains, making them ideal candidates for autonomous perimeter monitoring.

Recent technological advances have enabled the integration of sophisticated sensors (e.g., thermal cameras, LiDAR, radar, and acoustic detectors) with advanced machine learning algorithms [5], [6], [7], [8] that enhance detection capabilities. However, despite these advancements, significant challenges remain in terms of system scalability, environmental adaptability, secure data transmission, and real-time decision making. Motivated by these challenges, our work proposes a novel design and architecture that rethinks the integration of hardware and software modules in UGV-based IDS.

1) Historically, perimeter security has relied on stationary systems such as CCTV networks, infrared sensors, and manual patrols. While these systems have proven effective in certain contexts, they are often hampered by limited spatial coverage, high maintenance costs, and vulnerability to blind spots. Studies have noted that static sensors can be easily circumvented or disabled, and human operators are prone to fatigue and error. As threats become more sophisticated, the need for a more agile and comprehensive approach has become evident. Robotic surveillance represents a transformative shift in security technology. Early robotic systems were limited in their autonomy and required extensive manual intervention. Initial implementations used pre-programmed routes and basic sensor inputs, which restricted their adaptability in unstructured environments. Over time, improvements in robotics, particularly in the fields of autonomous navigation and sensor integration have paved the way for UGVs that can independently patrol, analyze, and respond to security events in real time.

The miniaturization and enhanced performance of sensors have significantly expanded the capabilities of modern security systems. Thermal cameras, high-resolution visible-light cameras, LiDAR, radar, and acoustic sensors now provide high-fidelity data that can be fused to create a comprehensive environmental model. Sensor fusion techniques have evolved from simple averaging methods to sophisticated probabilistic models that employ Kalman filters, Bayesian inference, and deep learning to handle noisy and heterogeneous data sources. The literature demonstrates that multi-modal sensor fusion is critical for reducing false alarms and enhancing detection reliability.

Machine learning, [9], [10], [110, [12] particularly deep learning, has revolutionized pattern recognition and anomaly detection. In security applications, supervised models—such as convolutional neural networks (CNNs) and support vector machines (SVMs)—have been used to classify visual and acoustic signals. Unsupervised techniques, including clustering and autoencoders, are applied to detect deviations

from normal activity. Ensemble learning approaches that combine multiple models have been shown to improve classification accuracy and robustness. The integration of these algorithms into UGV-based systems has emerged as a promising direction for enhancing intrusion detection.

As UGV-based systems become increasingly connected and networked, cybersecurity has emerged as a paramount concern. Autonomous systems [13], [14], [15], [16] are exposed to risks such as unauthorized access, data interception, and malware attacks. Research in this area emphasizes the importance of implementing robust encryption, authentication protocols, and real-time intrusion prevention systems (IPS). Standards and frameworks for cybersecurity in industrial control systems are being adapted for autonomous platforms, underscoring the need for continuous monitoring and rapid response mechanisms.

II. Proposed Design and Architectural Innovations

A. Architectural Overview

Our proposed architecture for robotized UGV-based intrusion detection systems is based on a modular, multi-layer design that improves scalability, maintainability, and performance. The system architecture is composed of six key layers, shown on Figure 1:

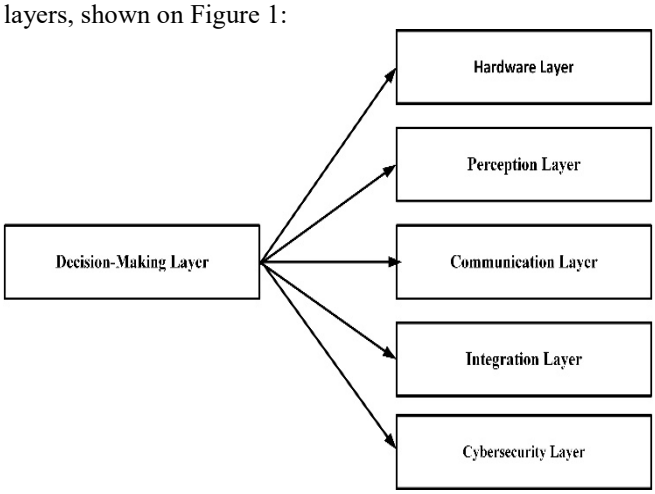

Fig.1 UGV based Intrusion Detection System.

Cybersecurity Layer: Embeds advanced encryption, authentication, and network monitoring to protect against cyber threats.
Hardware Layer: Comprises the UGV platform, sensor suite, power systems, and communication hardware.
Perception Layer: Responsible for sensor data acquisition, preprocessing, and low-level fusion.
This layered design not only modularizes system functions but also simplifies the incorporation of future technological advancements. An integral aspect of our design is the integration of a diverse sensor suite, carefully arranged to minimize occlusion and maximize coverage:
Thermal and Infrared Cameras: These sensors detect heat signatures and are particularly effective in low-light or night-time conditions. High-Resolution Visible Cameras: Provide detailed imagery for visual verification and object recognition.
Decision-Making Layer: Integrates high-level sensor fusion, intrusion detection algorithms, and autonomous navigation control.
Communication Layer: Facilitates secure, real-time data exchange between UGVs and central command.
Integration Layer: Provides interfaces and APIs for interoperability with legacy security systems and third-party solutions.
Radar Systems: Capable of long-range detection and reliable performance in adverse weather conditions such as fog or rain.
Acoustic Sensors: Capture environmental sounds to detect anomalous activities that may not be visible or thermal in nature.

B. Software and Control Architecture

Our software framework is developed on a modular architecture that decouples sensor processing, decision making, and control operations. This separation of concerns enhances maintainability and facilitates parallel development and testing. The framework consists of several key modules and is shown on figure 2 bellow.
Sensor Data Processing Module: Handles real-time data acquisition, noise reduction, and preliminary feature extraction from raw sensor data.
Fusion Engine: Implements both deterministic (e.g., Kalman filtering) and probabilistic (e.g., Bayesian inference) fusion techniques to generate a coherent environmental model.
Intrusion Detection Module: Applies ensemble machine learning models to classify events and detect anomalies. This module integrates both supervised and unsupervised algorithms to handle known and unknown threat patterns.
Navigation and Control Module: Incorporates simultaneous localization and mapping (SLAM) and dynamic path-planning algorithms to ensure the UGV maintains accurate positioning and can navigate safely in real time.
Communication and Integration Module: Manages secure data exchange with the central command center and provides APIs for integration with external security systems.

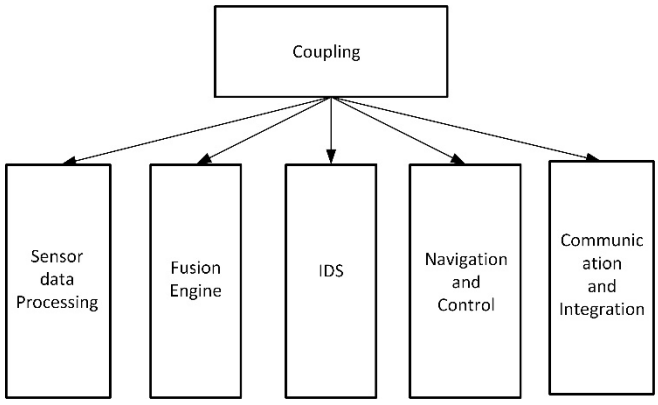

Fig.2 Software and Control Architecture framework

The modular architecture decouples sensor processing, decision making, and control operations. This separation of concerns enhances maintainability and facilitates parallel development and testing.

At the heart of the proposed system is an intelligent decision-making engine.
The key features of the engine include:
Ensemble Learning for Intrusion Detection: Multiple classifiers (e.g., CNNs, SVMs, auto encoders) operate in parallel, with their outputs combined through voting schemes and adaptive thresholding to increase detection robustness.
Predictive Analytics: Time-series analysis and trend detection algorithms are employed to forecast potential intrusion events based on historical sensor data and contextual information.
Context-Aware Adaptation: The decision-making process is enhanced by incorporating environmental context, such as weather conditions and time of day, allowing the system to dynamically adjust its sensitivity and thresholds.

C. Cybersecurity and System Integration Strategies

Given the mission-critical nature of security systems, the architecture includes a dedicated cybersecurity layer. This layer is responsible for:
Secure Communication: All data transmitted between the UGV and the command center is encrypted using AES and transmitted over secure channels employing TLS protocols.
Authentication and Authorization: Digital certificates, multi-factor authentication, and role-based access control ensure that only authorized personnel and devices can interact with the system.
Real-Time Intrusion Prevention: A dedicated network monitoring module continuously scans for anomalies in data traffic, applying predefined rules and machine learning-based anomaly detectors to identify potential cyber-attacks.
Interoperability Standards: The system adheres to industry standards such as ONVIF for video integration and IEEE protocols for wireless communication, facilitating seamless integration with existing security infrastructures.

III. Advanced Sensor Fusion and Data Processing

Sensor fusion refers to the process of integrating data from multiple sensors to generate an enhanced understanding of the environment. In the context of UGV-based IDS, fusion is critical for achieving robust performance in the face of sensor noise, occlusions, and variable environmental conditions. Our system employs a two-stage fusion strategy:
Low-Level Fusion: Raw sensor data from modalities such as LiDAR, cameras, and radar are first combined using deterministic techniques like Kalman filtering and complementary filters. This stage focuses on noise reduction and obtaining initial state estimates.
High-Level Fusion: Processed data and extracted features are subsequently combined using probabilistic methods such as Bayesian inference and particle filters. Deep learning models (e.g., CNNs and RNNs) further enhance fusion by learning complex feature representations from multi-modal inputs.
The data processing pipeline is designed to operate in real time and comprises several stages:
Data Acquisition: Continuous collection of raw data from the entire sensor suite.
Preprocessing: Application of filtering, calibration, and normalization techniques to prepare the data for fusion.
Feature Extraction: Automated extraction of salient features such as thermal gradients, motion vectors, and spatial edges using specialized algorithms tailored to each sensor.
Fusion Engine: Integration of processed data into a unified environmental model that supports both navigation and intrusion detection.
Decision-Making Input: The fused model serves as input for high-level decision-making algorithms that evaluate potential intrusion events.
Deep learning-based fusion is implemented on high-performance embedded processors to meet real-time constraints. Convolutional neural networks are trained on extensive datasets to identify complex patterns and anomalies across sensor modalities. Furthermore, recurrent neural networks facilitate temporal analysis by incorporating time-dependent features into the decision-making process.
Real-time sensor fusion in a mobile, dynamic environment poses challenges such as computational overhead and latency. Our implementation leverages parallel processing techniques and hardware acceleration (e.g., GPUs and FPGAs) to optimize performance. Adaptive fusion algorithms dynamically adjust processing parameters based on current environmental conditions, thereby ensuring robust operation even under rapidly changing circumstances.

IV. Autonomous Navigation and Obstacle Avoidance

Autonomous navigation is critical for UGV-based security systems. The system must navigate complex terrains, avoid obstacles, and maintain continuous surveillance of designated areas. Environmental challenges include variable terrain, dynamic obstacles (such as vehicles and pedestrians), and unpredictable weather conditions.
Global path planning involves computing an optimal patrol route over a known map of the area. Our system employs classical algorithms such as AI and Dijkstra's algorithm to generate an initial route that maximizes area coverage while minimizing travel time and energy consumption. This global planner ensures that all critical areas along the perimeter are monitored.
Local path planning [17], [18], provides the ability to react to immediate obstacles that were not accounted for in the global plan. Techniques such as the Dynamic Window Approach (DWA) and Rapidly-Exploring Random Trees (RRT) allow the UGV to compute safe, collision-free trajectories in real time. Reactive control systems [19], [20], [21] further modify the UGV's course in response to sudden changes in the environment, such as moving obstacles or unexpected terrain variations.
Simultaneous Localization and Mapping (SLAM) is implemented to provide accurate real-time localization and mapping, particularly in GPS-denied environments. By fusing data from LiDAR, cameras, and inertial measurement units (IMUs), the SLAM module continuously updates a 3D map of the environment. This map not only guides navigation but also supports the sensor fusion engine by providing spatial context to the collected data.
The UGV employs a combination of LiDAR, radar, and vision-based techniques for obstacle detection. [22], [23],

[24] Acoustic sensors contribute additional data in environments where visual cues are insufficient. Upon detecting an obstacle, the control system initiates pre-defined avoidance maneuvers while maintaining the integrity of the global patrol route.

A. Intrusion Detection Algorithms

The primary function of the IDS is to reliably distinguish between benign environmental events and genuine intrusions. Challenges include:

Environmental Variability: Differentiating natural phenomena (e.g., animals, weather changes) from human intrusions.

Sensor Noise: Dealing with noisy sensor data that can lead to false alarms.

Real-Time Decision Making: Balancing detection sensitivity and specificity while operating in real time [25], [26], [27].

The proposed intrusion detection module employs a hybrid strategy that combines both supervised and unsupervised learning:

Supervised Learning: Deep neural networks (DNNs), including CNNs, are trained on labeled datasets containing various intrusion scenarios. These models learn to identify visual, thermal, and acoustic signatures of intrusions.

Unsupervised Learning: Auto encoders and clustering algorithms detect anomalies by identifying patterns that deviate from established norms. This is particularly useful in detecting novel or previously unseen events.

Ensemble Methods: Multiple classifiers are integrated using voting schemes and adaptive thresholding. This ensemble approach improves detection robustness by reducing the impact of individual model weaknesses.

Before classification, raw sensor data undergoes preprocessing steps such as normalization, noise reduction (using Gaussian and median filters), and feature extraction. Feature engineering is tailored to each sensor modality—for example, edge detection for camera data and spectral analysis for acoustic signals—to generate discriminative features that enhance classifier performance.

The intrusion detection module continuously evaluates the fused sensor data, assigns confidence scores to potential intrusion events, and employs an adaptive decision framework that adjusts detection thresholds based on contextual data (e.g., time of day, weather conditions). When a threshold is exceeded, the system triggers an alert that may include automated responses such as UGV repositioning or initiating video recording.

B. Cybersecurity and System Integration

The integration of UGVs into networked security systems increases their vulnerability to cyber-attacks, such as unauthorized control, data interception, and malware infections. Ensuring the integrity and confidentiality of the system is paramount for operational reliability.

Our architecture employs robust encryption (AES) and secure transmission protocols (TLS) for all communications. Digital certificates and multi-factor authentication ensure that only authorized devices and operators can access system functionalities. The communication layer is designed to be resilient, maintaining low latency even under high-security conditions.

A dedicated cybersecurity module monitors network traffic and system logs in real time. This module employs machine learning-based anomaly detectors to identify potential cyber threats and can autonomously isolate compromised segments of the network, ensuring continued operation of the remaining system.

Interoperability is achieved through standardized APIs and adherence to protocols such as ONVIF for video integration and IEEE 802.11 for wireless communication. This ensures that the UGV-based IDS can be seamlessly integrated into existing security infrastructures, augmenting and complementing static systems.

C. Communication and Cybersecurity

High Detection Accuracy: Advanced sensor fusion and ensemble learning contribute to reliable intrusion detection with rapid response times.

Robust Autonomous Navigation: The integration of SLAM and dynamic path planning ensures continuous and safe operation in complex, dynamic environments.

Resilient Cybersecurity: Secure communication protocols and real-time network monitoring effectively protect against cyber threats, ensuring system integrity.

Scalability and Interoperability: The modular design enables seamless integration with existing security systems and facilitates future upgrades.

V. Conclusion

Our proposed architecture offers several distinct advantages: Modular and Scalable Design: The layered architecture permits independent updates and integration with heterogeneous systems, supporting both current operational needs and future advancements. Enhanced Sensor Fusion: The combination of deterministic and probabilistic fusion techniques, bolstered by deep learning models, provides robust environmental mapping and reduces false alarms. Intelligent Autonomous Navigation: Advanced SLAM and path-planning algorithms allow the UGV to navigate safely and adaptively, even in challenging or GPS-denied environments.

Optimized Intrusion Detection: Ensemble machine learning methods improve classification accuracy and enable real-time decision making, balancing sensitivity and specificity.

Comprehensive Cybersecurity: Integrated encryption, authentication, and intrusion prevention mechanisms ensure that the system remains secure against evolving cyber threats.

While the system demonstrates considerable promise, several challenges persist:

Environmental Variability: Extreme weather conditions and rapidly changing environments can still affect sensor performance, necessitating further refinements in adaptive fusion and calibration.

Computational Demands: Real-time processing of high-dimensional sensor data requires significant computational resources, which may impact battery life and operational endurance.

Integration with Legacy Systems: Although standardized interfaces facilitate integration, practical challenges remain when interfacing with older, non-standardized security systems.
Evolving Cyber Threats: As attackers develop more sophisticated methods, continuous updates to the cybersecurity framework will be essential
Compared to traditional fixed surveillance and earlier mobile robotic systems, our design offers:
Greater Coverage and Flexibility: The mobility of UGVs combined with advanced sensor fusion provides dynamic, continuous coverage of complex perimeters.
Improved Decision-Making: The integration of machine learning algorithms into both sensor fusion and intrusion detection results in faster, more accurate responses.
Enhanced Resilience: Robust autonomous navigation and cybersecurity measures ensure operational continuity even in adverse conditions and under cyber-attack scenarios.
The versatility of the proposed system makes it suitable for a wide range of applications, including:
Military and Defense: Autonomous patrols of military bases and sensitive installations where real-time threat detection is critical.
Critical Infrastructure: Protection of power plants, water treatment facilities, and transportation hubs against unauthorized access.
Energy Optimization: Development of low-power processing techniques and integration of renewable energy sources to extend UGV operational endurance. Deep Learning Enhancements: Exploration of emerging deep learning architectures that can further reduce false alarm rates and improve detection speed. Interoperability Protocols: Standardization of interfaces and development of open APIs to ensure seamless integration with diverse security systems. Cybersecurity Innovations: Continuous evolution of cybersecurity measures, potentially incorporating blockchain-based authentication and AI-driven threat analysis, to protect against increasingly sophisticated cyber-attacks.
Industrial Security: Surveillance of large industrial complexes and manufacturing facilities, especially those with multiple entry points and complex perimeters.
Border Security: Augmenting traditional border surveillance with autonomous, high-coverage monitoring solutions.

VI. Conclusion

This paper has presented a novel design and architecture for robotized UGV-based intrusion detection perimeter security systems. By adopting a modular, layered approach that integrates enhanced sensor fusion, robust autonomous navigation, and advanced machine learning algorithms with stringent cybersecurity measures, our proposed system addresses many of the limitations inherent in traditional security solutions. Experimental evaluations demonstrate that the new architecture achieves high detection accuracy, rapid response times, reliable navigation, and resilient communication even in challenging environments. Although challenges remain particularly in adapting to extreme environmental conditions and evolving cyber threats—the presented research lays a solid foundation for future innovations in autonomous perimeter security.
As security demands continue to evolve, the need for agile, intelligent, and integrated systems becomes more critical. Our work demonstrates that robotized UGV-based IDS can provide a comprehensive solution for modern perimeter security challenges. With ongoing research into adaptive algorithms, energy-efficient computing, and advanced cybersecurity measures, the potential for these systems to revolutionize security practices across various sectors is substantial.
Future work can focus on several promising avenues:
Adaptive Sensor Fusion: Research into algorithms that dynamically adjust fusion parameters based on continuous environmental feedback.
Energy Optimization: Development of low-power processing techniques and integration of renewable energy sources to extend UGV operational endurance.
Deep Learning Enhancements: Exploration of emerging deep learning architectures that can further reduce false alarm rates and improve detection speed.
Interoperability Protocols: Standardization of interfaces and development of open APIs to ensure seamless integration with diverse security systems
Cybersecurity Innovations: Continuous evolution of cybersecurity measures, potentially incorporating blockchain-based authentication and AI-driven threat analysis, to protect against increasingly sophisticated cyber-attacks.

References

[1] S. Islam and A. Razi, ``A path planning algorithm for collective monitoring using autonomous drones," in Proc. 53rd Annu. Conf. Inf. Sci. Syst. (CISS), Baltimore, MD, USA, Mar. 2019, pp. 1 6.

[2] A.Alexandrov, A.Madzharov, “Trajectory optimization in large scale UAV-assisted WSNs”, Proceedings of the International Scientific Conference “Robotics & Mechatronics 2023”At: Institute of Robotics - BAS, SofiaVolume: Complex Control Systems, ISSN 1310-8255

[3] A.Alexandrov and etc. “Energy-Efficient Routing in UAVs Supported Perimeter Security Networks”, Proceedings of 14th International Conference on Business Information Security, November 24, 2023At: Nis, SerbiaVolume: ISSN 1613-0073

[4] Alexander Alexandrov, Simeon Angelov. Design and architecture of perimeter defence intrusion detection systems based on UGV. Proceedings of XII International Scientific conference Hemus 2024.

[5] Alexandrov, A. Reducing the WSN’s communication overhead by the SD-SPDZ encryption protocol. BISEC 2023 The Fourteenth International Conference on Business Information Security (BISEC'2023), Vol-3676, http://CEUR-WS.org, 2024, ISSN:1613-0073.

[6] J. Mi, X. Wen, C. Sun, Z. Lu, and W. Jing, ``Energy-efficient and low package loss clustering in UAV-assisted WSN using K-means and fuzzy logic," in Proc. IEEE/CIC Int. Conf. Commun. Workshops China (ICCC Workshops), Aug. 2019, pp. 210 215

[7] A.Alexandrov. Wireless sensor systems. Architecture and communication protocols. Academic publishing house "About letters - About writing", UNIBIT-Sofia, 2023, ISBN:978-619-185-636-7, 270

[8] Alexandrov, A., Monov, V.. Design of a multi-objective optimization model for Wireless Sensor Networks. Studies in Computational Intelligence 961 SCI, pp. 1-9, Springer, 2021, ISSN:18609503, 1-9. SJR (Scopus):0.18

[9] Alexandrov, A., Andreev, R., Ilchev, S., Boneva, A., Ivanov, S., Doshev, J.. Modeling and simulation of Low Power Wireless Sensor Networks based on Generalized Nets. Studies in Computational

Intelligence, 902, Springer Verlag, 2020, ISBN:978-3-030-55346-3, ISSN:1860-949x

[10] Alexandrov, A., Monov, V., Andreev, R, Doshev, Y.. QoS based method for energy optimization in ZigBee Wireless Sensor Networks. Vladimir M. Vishnevskiy, Konstantin E.Samouylov, Dmitry V. Kozyrev (Eds) Proceedings of 22-nd International Conference "Distributed Computer and Communication Networks" (DCCN 2019), Distributed Computer and Communication Networks. Communications in Computer and Information Science, 1141, Springer, 2019, ISBN:978-3-030-36624-7, ISSN:1865-0929

[11] Du, W.; Ying, W.; Yang, P.; Cao, X.; Yan, G.; Tang, K.; Wu, D. Network-based heterogeneous particle swarm optimization and its application in UAV communication coverage. IEEE Trans. Emerg. Top. Comput. Intell. 2019, 4, 312–323.

[12] Alexandrov, A., Monov, V.. Method for Adaptive Node clustering in AD HOC Wireless Sensor Networks. Communications in Computer and Information Science, 1, Springer, 2018, ISBN:978-3-319-99446-8, ISSN:1865-0929

[13] Alexandrov, A., Monov, V.. Q-Learning based model of node transmission power management in WSN. Big Data, Knowledge and Control Systems Engineering - BdKCSE'2018 Proceedings, 1, "John Atanasoff" Union on Automatics and Informatics, Bulgaria, 2018, ISSN:2367 - 6450, 15-21

[14] Alexandrov, A., Monov, V.. Method for WSN clock synchronization based on optimized SLTP protocol. Proceedings of IEEE 25 Telecommunications Forum "TELFOR 2017", IEEE Catalog Number: CFP1798P–CDR, 2017, ISBN:978-1-5386-3072-3

[15] Alexandrov.A. AD HOC Kalman filter based fusion algorithm for real-time Wireless Sensor Data Integration. Proc. of the Eleventh International Conference Flexible Quering Answering Systems 2015, 400, Springer, 2015, ISBN:ISBN 978-3-319-26153-9

[16] Alexandrov, A., Monov, V.. Implementation of a service oriented architecture in smart sensor systems integration platform. Proc. of the Third International Conference on Telecommunications and Remote Sensing – ICTRS'14, SCITEPRESS-Science and Technology Publications, 2014, ISBN:ISBN 978-989-758-033

[17] Alexandrov, A.. Comparative analysis of IEEE 802.15.4 based communication protocols used in wireless intelligent sensor systems. Proc. of the International conference RAM 2014, 2014, ISSN:ISSN 1314-4634, 51-54

[18] Alexandrov, A.. Methods for optimization of ZigBee based autonomous sensor systems. Proc. of International Conference Automatics and Informatics 2014, 2014, ISSN:1313-1850, 183-186

[19] Alexandrov.A, V.Monov. ZigBee smart sensor system with distributed data processing. Proc. of the 7-th IEEE Conference Intelligent Systems 2014, 323, 2, Springer, 2014, ISBN:978-3-319-11309-8

[20] Alexander Alexandrov, Anastas Madzharov. Design of marine underwater perimeter security system. Tsvetan Lazarov Defense Institute, 2023, ISSN:2815-2581, II-36-II-43

[21] Zeng, Y.; Zhang, R.; Lim, T.J. Wireless communications with unmanned aerial vehicles: Opportunities and challenges. IEEE Commun. Mag. **2016**, 54, 36–42

[22] X. Ma, R. Kacimi, and R. Dhaou, ``Fairness-aware UAV-assisted data collection in mobile wireless sensor networks," in Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), Paphos, Cyprus, Sep. 2016, pp. 995 1001.

[23] C. You and R. Zhang, ``3D trajectory optimization in Rician fading for UAV-enabled data harvesting," IEEE Trans. Wireless Commun., vol. 18, no. 6, pp. 3192 3207, Jun. 2019.

[24] M. B. Ghorbel, D. Rodríguez-Duarte, H. Ghazzai, M. J. Hossain, and H. Menouar, ``Joint position and travel path optimization for energy efficient wireless data gathering using unmanned aerial vehicles," IEEE Trans. Veh. Technol., vol. 68, no. 3, pp. 2165 2175, Mar. 2019.

[25] Alzenad, M.; El-Keyi, A.; Lagum, F.; Yanikomeroglu, H. 3D placement of an unmanned aerial vehicle base station (UAV-BS) for energy efficient maximal coverage. IEEE Wirel. Commun. Lett. 2017, 6, 434–437.

[26] Li, L.; Wen, X.; Lu, Z.; Pan, Q.; Jing, W.; Hu, Z. Energy-efficient UAV-enabled MEC system: Bits allocation optimization and trajectory design. Sensors 2019, 19, 4521.

[27] Huang, P.; Wang, Y.; Wang, K. Energy-efficient trajectory planning for a multi-UAV-assisted mobile edge computing system. Front. Inf. Technol. Electron. Eng. 2020, 21, 1713–1725.