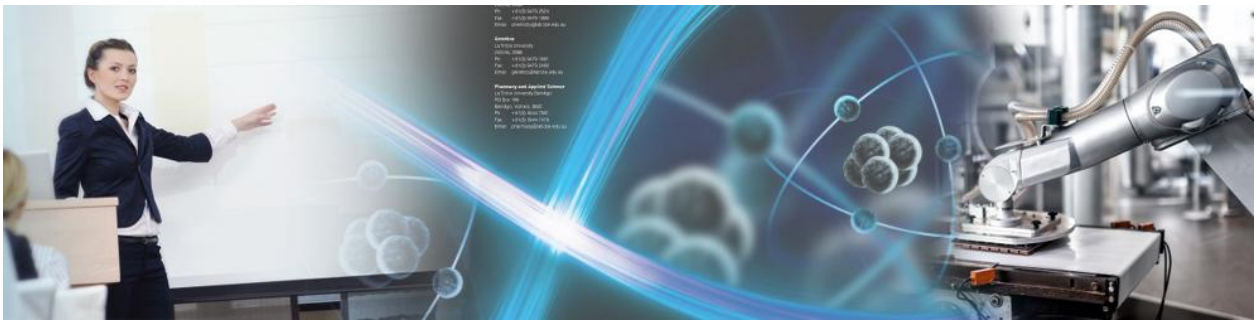
Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Кафедра комп'ютерно-інтегрованих технологій, автоматизації, робототехніки та безпекової інженерії

X Міжнародна Конференція
ВИРОБНИЦТВО
&
МЕХАТРОННІ СИСТЕМИ 2026



X International Conference
MANUFACTURING
&
MECHATRONIC SYSTEMS 2026

M&MS

2026

X International Conference

22-23 October

Kharkiv

УДК: 005:004.896:62-65:338.3

Виробництво & Мехатронні Системи 2026: матеріали X-ої Міжнародної конференції, Харків, 22-23 жовтня 2026 р.: тези доповідей / [редкол. І.Ш. Невлюдов (відповідальний редактор)].-Харків: [електронний друк], 2026. – 87 с.

У збірник включені тези доповідей, які присвячені сучасним тенденціям розвитку технологій та засобів виробництва та мехатронних систем, передовому досвіду та впровадженню їх в галузях систем промислової автоматизації та керування виробництвом; системній інженерії; CAD/CAM/CAE системах; мехатроніці (електро-механічних системах, електронних інструментах систем керування, механічних CAD системах); робототехніці та засобахм інтелектуалізації; MEMS (сучасних матеріалів та технологіях виготовлення MEMS) та компонентах і технологіях автоматизації видобутку, переробки та транспортування нафти та газу.

Редакційна колегія: І.Ш. Невлюдов, В.В. Євсєєв.

Manufacturing & Mechatronic Systems 2026: Proceedings of X st International Conference, Kharkiv, October 22-23, 2026: Thesises of Reports / [Ed. I.Sh. Nevlyudov (chief editor).] .- Kharkiv .: [electronic version], 2026. - 87 p.

The collection includes the thesises of reports on modern trends in the development of technologies and means of production and mechatronic systems, top experience and implementation of them in fields of: industrial automation and production management systems; systems engineering; CAD/CAM/CAE systems; mechatronics (electrical and mechanical systems, electronic control tools, mechanical CAD systems); robotics and intellectual toolls; MEMS (modern materials and manufacturing technologies MEMS) and components and technologies for the automation of oil, gas and oil extraction, processing and transportation.

Editorial board: Igor.Sh. Nevludov, Vladyslav.V. Yevsieiev

© Кафедра комп'ютерно-інтегрованих технологій, автоматизації, робототехніки та безпекової інженерії (КІТАРБІ), ХНУРЕ,2026

Міністерство освіти і науки України (МОНУ)
Харківський національний університет радіоелектроніки (ХНУРЕ)
Варшавський університет сільського господарства (WULS - SGGW)
Азербайджанський державний університет нафти і промисловості
Національний університет «Львівська політехніка»
Festo Didactic Україна
Jabil Circuit Ukraine Limited
ТОВ «Науково-виробниче підприємство «УКРІНТЕХ»»
Факультет автоматизації, комп'ютерно-інтегрованих технологій та систем (АКТС)
Кафедра комп'ютерно-інтегрованих технологій, автоматизації, робототехніки та безпекової інженерії (КІТАРБІ),
Державне підприємство «Харківський науково-дослідний інститут технології машинобудування»
Державне підприємство «Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості»

МАТЕРІАЛИ

X-ої Міжнародної Конференції

ВИРОБНИЦТВО
&
МЕХАТРОННІ СИСТЕМИ 2026

(22-23 жовтня 2026)
Харків, Україна

Ярослав Бєлий, Дмитро Гурін

Аналіз принципів нульової довіри для побудови кіберфізичної системи віддаленого моніторингу та керування промисловим обладнанням …… 49

Olha Shevchenko, Svetlana Sotnik

Comparison of Simulation Environments: Wokwi, Tinkercad, Falstad Circuit Simulator …… 53

Vladyslav Yevsieiv, Kyrylo Luchaninov

EDGE Method for Identification and Prediction of Dynamic Object Trajectories for a Mobile Robot Based on YOLO26n …….. 57

Ростислав Колногузов, Дмитро Гурін

Розроблення автоматизованого модуля орієнтації сонячної панелі з адаптивним керуванням за метеорологічними параметрами …….. 61

Михайло Лазаренко

Структура системи автоматизованого керування автоматичною насосною пневматичною установкою …… 64

Tymofii Cherednichenko, Svetlana Sotnik

Typology of a Mobile Robot's Internal Data and the Threats to Their Security 68

М. С. Черкашин, С. В. Хрустальова

Сучасні підсистеми автоматизованого обліку робочого часу операторів сортувальних ліній на основі RFID-карт …… 73

Artem Shevchenko, Svetlana Sotnik

Review of Methods for Ensuring the Positioning Accuracy of an Industrial Robot During Technological Operations …… 75

Vladyslav Yevsieiv, Svitlana Starikova

Analysis of the Effectiveness of Using a Mobile Robot Digital Twin for Teaching School Students the Fundamentals of Robotics …….. 80

Oleksandr Kolbasa, Svetlana Sotnik

Sensors and Navigation for Energy-Efficient Mobile Robots …… 83

Typology of a Mobile Robot's Internal Data and the Threats to Their Security

Tymofii Cherednichenko, Svetlana Sotnik

Department CITARSE, Kharkiv National University of Radio Electronics, Ukraine,
Kharkiv, av. Nauki. 14., email: tymofii.cherednichenko@nure.ua

Annotation: In this work, the internal data of an autonomous mobile robot is considered an asset to be protected. We propose a classification of data by processing level: raw sensor data (LiDAR, cameras, IMU), odometry and localization data, mapping data (occupancy grids, feature maps), ROS/ROS 2 logs and recordings, control commands, and telemetry. For each level, characteristic message types, communication channels, and storage locations are identified. Three groups of threats are analyzed: attacks on sensor data integrity (spoofing), data interception via insecure DDS middleware, and unauthorized data extraction in cases of physical access or robot compromise. The analysis shows significant risks associated with the propagation of distortions across data levels and with the fact that default ROS 2 security mechanisms are disabled. The proposed typology can serve as a foundation for formulating data protection requirements for mobile robotic platforms. Existing security tools are examined (SROS2, network segmentation, restricting automatic DDS discovery, and data-at-rest encryption), along with their limitations: cryptography secures the transmission channel but not the physical measurements; therefore, mitigating sensor spoofing requires cross-verification of data and anomaly detection.

***Ключові слова*:** mobile robots, ROS 2, DDS, data security, sensor spoofing, SROS2, data exfiltration.

I. INTRODUCTION

Autonomous Mobile Robots (AMRs) and Automated Guided Vehicles (AGVs) are widely deployed across logistics, manufacturing, agriculture, as well as service and domestic robotics [1–9]. During operation, a mobile robot continuously generates and processes substantial volumes of data: point cloud streams, video frames, self-pose estimates, environmental maps, event logs, and control commands. A significant portion of this data carries not only technical but also high informational value: a facility map reveals structural layouts, a video stream may capture personnel and confidential documents within the camera's field of view, while event logs and telemetry reflect enterprise operating modes [10–15].

Most research and a significant portion of industrial platforms are built on the Robot Operating System (ROS) and its second version, ROS 2, in which messaging is implemented on top of the Data Distribution Service (DDS) standard [16–18]. ROS 1 was designed for closed laboratory networks and lacked built-in authentication mechanisms. ROS 2 introduced the SROS2 toolset, which utilizes the DDS Security specification; however, these mechanisms are disabled by default and require separate configuration. Threats to robotic systems are no longer purely theoretical: IPv4 address space scanning has revealed publicly accessible ROS nodes, and the analysis of DDS implementations has exposed a number of vulnerabilities, including those present in implementations used within ROS 2 [19–21].

In order to build an effective protection system, it is necessary first and foremost to determine what exactly needs to be protected. Internal data of a mobile robot is heterogeneous in terms of origin, update frequency, volume, lifespan, and the consequences of compromise; thus, a uniform approach to its protection is ineffective. This underscores the relevance of systematizing the robot's internal data and mapping each of its classes to relevant threats.

The objective of this work is to systematize the internal data of a mobile robot by processing levels, analyze key threats to their integrity and confidentiality, and evaluate the capabilities and limitations of existing protection mechanisms as a foundation for formulating data security requirements.

To achieve the set objective, the following tasks were solved:

1. Propose a classification of internal data of a mobile robot by processing levels.
2. Determine typical formats, transmission channels, and storage locations for data at each level within the ROS/ROS 2 ecosystem.
3. Analyze three groups of threats: sensor spoofing, data interception via DDS, and unauthorized extraction of stored data.
4. Outline existing protection mechanisms and their limitations.

II. TYPOLOGY OF INTERNAL DATA OF A MOBILE ROBOT

Internal mobile robot data should be classified by processing level – from physical measurements to control decisions. This approach corresponds to the architecture of a typical navigation stack (for example, Nav2 in ROS 2), in which data sequentially goes through the stages of perception, localization, mapping, planning, and motion execution. Logs and recordings that aggregate data from all other levels are distinguished separately. Table 1 summarizes data levels, characteristic ROS 2 message types, and the main consequences of their compromise.

The presented levels differ significantly in their characteristics. Raw sensor data has the largest volume and frequency: IMUs typically operate at frequencies of hundreds of Hertz, rotating LiDARs – on the order of 10-20 Hz, and image and point cloud streams can reach tens of megabytes per second. At the same time, their relevance is short-lived, so integrity and timeliness are critical for them, rather than long-term confidentiality.

Таблиця 1. Типологія внутрішніх даних мобільного робота

Data level	Typical messages / formats	Transmission channel	Storage place	Consequences of compromise	Priority property
Raw sensor data	LaserScan, PointCloud2, Image, CompressedImage, Imu	ROS 2 topics over DDS/RTPS (UDP)	Mostly not saved; they end up in rosbag2.	False or «missing» obstacles; leakage of images of people, rooms, documents; orientation shift.	Integrity, timeliness.
Odometry and localization	nav_msgs/Odometry, /tf, pose estimation (AMCL)	DDS Topics	RAM; trajectory in rosbag2 and logs.	Accumulated positioning error; trajectory disclosure.	Integrity.
Maps	OccupancyGrid, .pgm + .yaml, feature maps, SLAM graphs	DDS topics; cloud sync (if available)	Onboard computer storage, cloud.	Disclosure of room planning; saved images of the environment.	Confidentiality during storage.
Journals and records	/rosout, ~/.ros/log, rosbag2 (MCAP)	Topic /rosout; DDS	Onboard computer storage, cloud.	Disclosure of configuration, service information, copies of streams.	Confidentiality during storage.
Control teams and telemetry	Twist/TwistStamped (/cmd_vel), navigation goals, /diagnostics, battery status	DDS topics; telemetry channel to the cloud.	Magazines, cloud services.	Unauthorized movement; disclosure of operating mode.	Integrity (team), confidentiality (telemetry).

Control commands are small in size but directly affect the robot's physical movement, so their authenticity is a matter not only of information security but also of functional safety.

Maps, logs, and rosbag2 recordings have the opposite profile: they update infrequently, are stored for a long time on the onboard computer or in the cloud, and concentrate information about the environment. The occupancy grid is basically a floor plan, while a rosbag2 recording can contain a complete copy of sensor streams, movement trajectory, and commands for the entire session. That’s why, for this data, privacy during storage is a top priority.

An important feature is the hierarchical link between levels: distortions at the lower level spread upwards. False LiDAR points end up in the costmap, change the planning outcome, and eventually the control commands. Similarly, odometry errors accumulate in position estimates and distort the constructed map. So, protecting the robot's data should be seen as protecting the entire processing chain, not just individual messages.

III. THREATS TO THE SECURITY OF INTERNAL DATA

Of the three classical security properties (confidentiality, integrity, availability), this paper focuses primarily on the first two; threats to internal data of a mobile robot are divided into three groups: sensor data integrity attacks, data interception in communication channels, and unauthorized extraction of stored data. Since the subject of consideration is data protection, main attention is given to integrity and confidentiality; availability (denial of service) is considered only as a consequence of integrity attacks. These groups differ in their attack vectors and the data levels they primarily target.

Sensor data integrity attacks (spoofing) aim to force the robot to perceive plausible yet false measurements. A distinct feature of such attacks is that they are implemented via a physical channel and bypass network defense mechanisms, including encryption. For cameras, blinding by light sources has been demonstrated, while for LiDAR, relaying and injection of false reflected pulses using inexpensive equipment have been shown [22]. Subsequent studies revealed that direct point injection by itself is ineffective at deceiving machine learning-based object detection algorithms; however, formulating the attack as an optimization problem allowed the creation of false obstacles in front of a vehicle with a success rate of about 75% [23]. For inertial sensors, it was demonstrated that an acoustic signal at the resonant frequency of a MEMS gyroscope can disrupt stabilization and cause a drone to fall, while acoustic injection into MEMS accelerometers allows controlled manipulation of their readings [24, 25]. For robots operating outdoors, GNSS signal spoofing presents an additional threat.

For a mobile robot, the consequences of attacks depend on the direction of distortion: the injection of a false obstacle leads to a stop or a detour, resulting in a denial of service, whereas hiding a real obstacle creates a collision risk [30–33]. A distinct class comprises integrity attacks at the message level: with SROS2 disabled, any participant in the same DDS domain can publish data to arbitrary topics, for example, sending speed commands to /cmd_vel or a false initial pose to /initialpose, which resets the localization estimate.

Data interception (eavesdropping) is tied to the DDS architecture. Domain participants automatically discover each other via the Simple Participant Discovery Protocol (SPDP), which uses UDP multicast by default. During discovery, information about nodes, topic names, and

message types is transmitted, and without DDS Security enabled, the data itself is sent over the RTPS protocol in plaintext. Consequently, any device in the same network segment and domain can subscribe to camera, LiDAR, odometry, or map streams without authentication. Implementation vulnerabilities amplify this risk: in 2021, researchers reported 13 vulnerabilities across six DDS implementations (RTI Connext DDS, CoreDX DDS, Cyclone DDS, Fast DDS, GurumDDS, OpenDDS) and in the specification itself, including reflection and amplification traffic attacks, as well as buffer overflows during XML configuration parsing; an IPv4 scan revealed 643 nodes responding to RTPS discovery requests [21].

Unauthorized data exfiltration targets primarily long-term data: maps, rosbag2 recordings, logs, and credentials. Given physical access, an attacker can obtain the contents of the onboard computer drive, exploit debugging interfaces, or take advantage of unprotected initial setup procedures. If SROS2 private keys are stored on disk without additional protection, stealing them allows an attacker to impersonate a legitimate node. A notable example is the study of the Unitree G1 humanoid robot (2025): shared hardcoded AES keys across all devices in the Bluetooth Low Energy setup procedure enabled remote code execution with root privileges, while the robot itself sent telemetry every five minutes to external servers – including battery status, joint torques, and motion states – without explicit notification to the user [34]. In Ecovacs robot vacuums (2024), access to Wi-Fi credentials, indoor maps, cameras, and microphones could be obtained via Bluetooth from a distance of about 130 m, and account deletion did not remove data or authentication tokens in the cloud [18]. These examples demonstrate that the telemetry channel and cloud services themselves constitute a data leakage channel, and the robot's lifecycle, including resale and disposal, must be factored into the threat model.

IV. PROTECTION MECHANISMS AND THEIR LIMITATIONS

The fundamental data protection mechanism in ROS 2 is SROS2, which utilizes three built-in DDS Security plugins: X.509 certificate-based authentication (DDS:Auth:PKI-DH), access control based on signed governance and permissions files (DDS:Access:Permissions), and cryptographic protection using AES-GCM/GMAC (DDS:Crypto:AES-GCM-GMAC). Security is enabled via the ROS_SECURITY_ENABLE environment variable, and under the Enforce strategy, a node without valid security artifacts will fail to launch [7, 8]. When properly configured, SROS2 prevents passive eavesdropping and data publishing by unauthorized nodes. At the same time, protection effectiveness depends on policy quality: overly broad permissions effectively negate access control, while managing certificates for a robot fleet requires a dedicated infrastructure.

Network-level measures complement SROS2: network segmentation, firewall filtering of DDS traffic, limiting the automatic discovery range (via the ROS_AUTOMATIC_DISCOVERY_RANGE variable starting in ROS 2 Iron), and timely updates of DDS implementations. It should be noted that the domain identifier ROS_DOMAIN_ID merely segregates logical networks and is not a security mechanism.

For stored data (maps, rosbag2, logs, keys), drive encryption, filesystem access control, data retention, and guaranteed wiping policies are required; for telemetry, data minimization, channel encryption, and user transparency are essential.

A fundamental limitation is that cryptographic tools protect the transmission channel, but not the physical measurement itself: a signed message containing a point cloud distorted by laser spoofing remains authentic. Therefore, defending against sensor attacks requires alternative approaches: cross-consistency validation across different sensors (LiDAR, cameras, odometry, IMU), anomaly detection, and physical countermeasures at the sensor hardware level. Furthermore, encrypting high-rate image streams and point clouds increases computational load and latency, which, for embedded platforms, demands a differentiated approach: prioritizing integrity protection for control commands and localization data, and confidentiality for long-term data.

V. CONCLUSIONS

This paper proposes a typology of internal mobile robot data covering five levels: raw sensor data, odometry and localization data, maps, ROS/ROS 2 logs and recordings, control commands, and telemetry. It is demonstrated that these levels differ in frequency, volume, and lifespan, and consequently in their primary security priority: integrity is critical for sensor data and commands, whereas confidentiality during storage is paramount for maps, logs, and recordings.

The threat analysis showed that sensor attacks are executed via the physical channel and cannot be mitigated by cryptography; data interception in ROS 2 is made possible by the plaintext DDS exchange used by default and vulnerabilities in its implementations; data exfiltration poses the greatest risk to long-term data and is exacerbated by weak setup procedures and unmonitored cloud telemetry channels. A significant risk factor is the propagation of distortions from lower data levels up to control commands.

The resulting typology can serve as a foundation for threat modeling and establishing differentiated security requirements for mobile robotic platforms – combining SROS2, network isolation, data-at-rest protection, and sensor data consistency validation.

LIST OF REFERENCES

[1] I. Nevliudov, Sh. Omarov, and S. Sotnik, "Evolution of physical ai in humanoid robotics: from Atlas locomotion to Optimus neural networks," in *Proc. Int. Sci.-Pract. Conf. "Towards the Fifth Industrial Revolution – the Role of Universities, Challenges and Opportunities"*, 2026, pp. 393-395

[2] A. Yakimenko, et al., "Robotics in logistics – From autonomous trucks to Amazon's picking robots," in *All-Ukrainian Conference "Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations" (ICSTRO-2026)*, Feb. 2026, pp. 86–90

[3] S. V. Sotnik, Y. S. Usenko, and P. V. Shakhov, "Safe cobots in development of industrial robotics," in *European Scientific Congress: Proceedings of the 8th International Scientific and Practical Conference*, Barca Academy Publishing, Sep. 2023, pp. 80–84

[4] S. V. Sotnik, "Support systems for robotics: principles, algorithms and development prospects," *Journal of natural sciences and technologies*, vol. 4, no. 2, pp. 419-430, 2025

[5] D. A. Sukhomlinova, et al., "Analysis of main tasks and challenges in drone remote control," in *Proc. 18th Int. Sci.-Pract. Conf. "Information Technologies and Automation – 2025"*, Odesa, Ukraine, Oct. 30-31, 2025, pp. 1059-1061

[6] T. A. Lykho, et al., "Pattern recognition and computer vision technologies in decision support systems of robotic systems," in *Proc. 17th Int. Sci.-Pract. Conf. "Information Technologies and Automation – 2024"*, 2024, pp. 645-648

[7] D. Sukhomlinova, et al., "Optimization of drone trajectory algorithms," in *Proc. 9th Int. Conf. Manufacturing & Mechatronic Systems (MMS 2025)*, Kharkiv, Ukraine, Oct. 25-26, 2025, pp. 46-49

[8] M. O. Ivanov, et al., "Features of drone application in emergency situations," in *II All-Ukrainian Conference "Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations" (ICSTRO-2026)*, Kharkiv, Ukraine, Sep. 2026, pp. 55–59

[9] M. S. Bielik, et al., "Analysis of the structures of mobile platforms for promoter robots," in *Proc. 5th Int. Sci.-Pract. Conf. "Global Trends in Science and Education"*, Kyiv, Ukraine, June 2-4, 2025, pp. 319-325

[10] A. D. Yechevskyi, et al., "Research of orientation methods of autonomous mobile robots in industrial conditions," in *Proc. Conf. "Computer-Integrated Technologies, Automation and Robotics" (CITAR-2025)*, 2025, pp. 115-119

[11] D. A. Sukhomlinova, et al., "Aerial robot in urban environments," in *Proc. 1st Int. Conf. Sustainable Smart Cities Communities: Business Innovation Solutions*, Kharkiv, Ukraine, Apr. 21, 2025, pp. 45-46

[12] A. S. Andreiev, et al., "Methods for improving the energy efficiency of small language models for autonomous robotics," in *Proc. 3rd All-Ukr. Conf. Computer-Integrated Tech., Automation Robotics (CITAR 2026)*, Kharkiv, Ukraine, May 14-15, 2026, pp. 6-10

[13] A. Andreiev, et al., "Comparative analysis of robotics platform: Webots, CoppeliaSim and Gazebo," in *Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: Тези доповідей XII Міжнародної науково-практичної конференції*, Запоріжжя, Україна, Dec. 2024, pp. 96–100

[14] A. D. Yechevskyi, et al., "Research of orientation methods of autonomous mobile robots in industrial conditions," in *Proc. Conf. "Computer-Integrated Technologies, Automation and Robotics" (CITAR-2025)*, 2025, pp. 115-119

2025", Odesa, Ukraine, Oct. 30-31, 2025, pp. 1059-1061

[15] Y. Floru, et al., "Robotic process automation and integration systems for SMBS: priority processes and software comparison," in *Proc. 3rd All-Ukr. Conf. Computer-Integrated Tech., Automation Robotics (CITAR 2026)*, Kharkiv, Ukraine, May 14-15, 2026, pp. 11-15

[16] S. Macenski, et al., Lalancette, and W. Woodall, "Robot operating system 2: Design, architecture, and uses in the wild," *Science Robotics*, vol. 7, no. 66, eabm6074, May 2022

[17] G. Deng, et al., "On the (in) security of secure ROS2," in *Proc. 2022 ACM SIGSAC Conf. Comput. Commun. Secur.*, Los Angeles, CA, USA, Nov. 2022, pp. 739-753

[18] V. Mayoral-Vilches, *et al.*, "Sros2: Usable cyber security tools for ROS 2," in *Proc. 2022 IEEE/RSJ Int. Conf. Intell. Robots Syst. (IROS)*, Kyoto, Japan, Oct. 2022, pp. 11253-11259

[19] N. DeMarinis, et al., "Scanning the internet for ROS: A view of security in robotics research," in *Proc. 2019 Int. Conf. Robotics Automation (ICRA)*, Montreal, QC, Canada, May 2019, pp. 8514-8521

[20] L. Hanenko, et al., "Creation of navigation system for autonomous mobile robot using ROS 2," *Cybersecurity: Educ., Sci., Tech.*, vol. 4, no. 28, pp. 498-510, 2025

[21] F. Maggi, et al., "A security analysis of the Data Distribution Service (DDS) protocol," Trend Micro Research, Inc., Tokyo, Japan, Tech. Rep., 2022, pp. 15-20

[22] J. Petit, et al., "Remote attacks on automated vehicles sensors," in *Proc. Black Hat Eur.*, London, UK, Nov. 2015, pp. 1-11

[23] Y. Cao, et al., "Adversarial sensor attack on LiDAR-based perception in autonomous driving," in *Proc. 2019 ACM SIGSAC Conf. Comput. Commun. Secur.*, London, UK, Nov. 2019, pp. 2267-2281

[24] Y. Son, et al., "Rocking drones with intentional sound noise on gyroscopic sensors," in *Proc. 24th USENIX Secur. Symp. (USENIX Security 15)*, Washington, D.C., USA, Aug. 2015, pp. 881-896

[25] T. Trippel, *et al.*, "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," in *Proc. 2017 IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Paris, France, Apr. 2017, pp. 3-18

[30] A. Taran, et al., "Impact of 5G/6G networks on the development of IoT, robotics, and autonomous systems. Low latency and mass connection of devices," in *All-Ukrainian Conference "Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations" (ICSTRO-2026)*, Feb. 2026, pp. 114–118

[31] I. S. Nevliudov, et al., "Design of the structure and motion control system of a stationary robot manipulator for construction work," *Нові технології в будівництві*, no. 47, pp. 37-45, 2025

[31] I. Zarubin, et al., "Basic principles of building aerial robots," in *Manufacturing & Mechatronic Systems 2024: Proceedings of VIII International Conference*, Kharkiv, Ukraine, Oct. 2024, pp. 32–36

[32] С. Сотник, "Розробка автоматизованої інформаційно-пошукової системи вибору маніпулятора промислових роботів," *Електромеханічні і енергозберігаючі системи*, 1 (68), pp. 52-58, 2025

[33] H. Attar, A. T. Abu-Jassar, V. Lyashenko, A. Al-qerem, S. Sotnik, N. Alharbi, et al.,, "Proposed synchronous electric motor simulation with built-in permanent magnets for robotic systems," *SN Applied Sciences*, vol. 5, no. 6, p. 160, Jun. 2023

[34] V. Mayoral-Vilches, "The cybersecurity of a humanoid robot," *arXiv preprint arXiv:2509.14096*, 2025
[35] D. Giese, et al., "Reverse engineering and hacking Ecovacs robots," in *Proc. DEF CON 32*, Las Vegas, NV, USA, Aug. 2024, pp. 9-11