ISSN:2308-5703
Impact factor:13.5 *International Multidisciplinary Online Journal* September, 2026

RESILIENCE OF AI-BASED ROUTING PROTOCOLS IN AUTONOMOUS WHEELED ROBOT SWARMS TO CYBERATTACKS AND MANIPULATIONS

Jasur Rajab o'g'li Ahmedov
Master's Student, ISMA University
(Riga, Latvia)
doi:https://doi.org/10.5281/zenodo.22822837

Abstract: This article investigates the issue of ensuring the resilience of artificial intelligence-based routing protocols in autonomous wheeled robot swarms against cyberattacks, false data, and adversarial manipulations. The study takes into account the dynamic characteristics of inter-robot networks and proposes a multi-stage protection approach aimed at developing a threat model, an AI-based routing mechanism, and improving its security.

Keywords: autonomous robots, robot swarm, artificial intelligence, routing protocol, cybersecurity, adversarial attack, machine learning, network resilience.

In recent years, the development of autonomous robotic systems has significantly increased scientific interest in robot swarms, which enable multiple robots to cooperate toward a common goal in a decentralized manner. The effective operation of a robot swarm depends not only on the movement capabilities of individual robots, but also on information exchange between robots, network stability, and the reliability of routing mechanisms. In swarm systems, communication and routing protocols are considered fundamental components for coordination and data exchange.

The connectivity of robots to a network, together with their ability to perform real physical movement in the environment, makes cybersecurity issues more complex than those encountered in traditional computer networks. In robotic systems, vulnerabilities can arise at the network, software, data, and hardware component levels; practical studies have extensively discussed attacks such as DoS, MITM, and attacks targeting robotic software environments.[1,34-p.]

The introduction of artificial intelligence-based routing protocols creates a new layer of this problem. On the one hand, AI enables the analysis of dynamic network conditions, selection of optimal routes, and adaptation to changing circumstances. On the other hand, the AI model itself may become a target of adversarial manipulation. In the adversarial machine learning taxonomy published by NIST in 2025, evasion, poisoning, and other attacks are classified as important risks associated with the life cycle of AI systems.[2,13-p.]

Therefore, routing in autonomous wheeled robot swarms should be considered not only from the perspective of network efficiency, but also from the perspectives of security, reliability, and adversarial resilience.

Problem Statement.A robot swarm is represented as a dynamic graph in the form of G=(V,E)G=(V,E). Here, V=v1,v2,…,vnV={v_1,v_2,\ldots,v_n} represents the set of robots, while EE represents the available communication channels between them. Each robot forms a routing decision based on parameters such as network status, neighboring robots, signal quality, latency, and packet loss.

In conventional routing mechanisms, route selection may be based on distance, connectivity, or other predefined metrics. In an AI-based approach, decisions are formed based on relationships learned from the current state of the network. As a result, the system can adapt to dynamic environments; however, incorrect or manipulated input data may lead to the disruption of routing decisions.

The main problem addressed in this study can be formulated as follows: how can an AI-based routing protocol maintain reliable communication and optimal routing between robots in the presence

of false, corrupted, or intentionally modified information provided by an adversarial party within the network?

This question is particularly important for robot swarms because an incorrect routing decision made by a single robot may affect the decisions of other robots and amplify errors throughout the system. Modern studies in swarm robotics identify communication, security, and real-time requirements as closely interconnected issues.[4,56-p.]

Scientific and Theoretical Foundations of the Topic. Adversarial machine learning studies attacks that cause AI models to make incorrect decisions through specially prepared or modified data. The NIST 2025 taxonomy proposes a systematic classification of adversarial threats based on the attacker's objective, level of knowledge, stage of the attack, and machine learning method being used.

In the context of robot swarms, such attacks may manifest themselves in the following forms.

False Data Injection Attack. An attacker sends false information to a robot or its routing module regarding signal quality, distance, the status of neighboring robots, or channel load. If the AI accepts this information as legitimate, it may select an unsafe or inefficient route.

Data Poisoning Attack. Malicious or incorrect samples are inserted into the dataset used during the training of an AI model. As a result, the model may become prone to incorrect generalization even under normal conditions. Data poisoning is identified as one of the major types of attacks within the field of adversarial machine learning.

Evasion Attack. After the model has been deployed, its input data are modified in such a way that causes the model to produce an incorrect classification or an incorrect decision. Such an approach can also be applied to AI-based security mechanisms.

DoS and DDoS Attacks. As a result of excessive occupation of network resources, communication between robots may be delayed or interrupted. For robots, this represents not only a reduction in data transmission quality, but may also have negative consequences for coordination and motion control. Reviews of robotic cybersecurity identify DoS and DDoS attacks as important network threats.

Sybil Attack. A single malicious device may appear within the network using multiple false robot identities. As a result, the routing algorithm may develop an incorrect perception of the available nodes and their reliability. This is particularly dangerous in decentralized robot swarms where decisions regarding nodes are made solely on the basis of local information.

AI-Based Secure Routing Model. In the proposed approach, the feature vector representing the state of the robot network is expressed as follows:[5,67-p.]

Xi=[di,ri,li,pi,ei,ti]X_i=[d_i,r_i,l_i,p_i,e_i,t_i]

where:

- did_i — distance to the neighboring robot;
- rir_i — communication signal quality;
- lil_i — channel load;
- pip_i — packet loss rate;
- eie_i — robot energy status;
- tit_i — latency indicator.

Based on these parameters, the AI model calculates the security and efficiency value for each possible route. The overall route score can be expressed as follows:

S(R)=αQ(R)+βC(R)−γL(R)−δA(R)S(R)=\alpha Q(R)+\beta C(R)-\gamma L(R)-\delta A(R)

where Q(R)Q(R) represents communication quality, C(R)C(R) represents the reliability indicator of the route, L(R)L(R) represents latency and resource cost, and A(R)A(R) represents the detected level of risk.

The important feature of this model is that the routing decision is not directed solely toward selecting the fastest and shortest path, but toward selecting a secure and stable path.

Proposed Protection Mechanism. To increase the adversarial resilience of the AI-based routing protocol, it is appropriate to use a multi-stage protection architecture. At the first stage, data verification is performed. Data received from a robot are compared using a timestamp, source identifier, physical plausibility of the value, and information from neighboring nodes.

At the second stage, an anomaly detection model is applied. This module learns the normal state of the network and identifies sudden changes, repeated abnormal values, or contradictory messages.

At the third stage, an adversarially robust AI model is used. During the model training process, manipulated samples are used together with normal data in order to increase the model's resilience to attacks. Protection mechanisms such as adversarial training and anomaly detection are discussed in the scientific literature as promising measures for strengthening the security of AI-based robotic systems.[3,49-p.]

At the fourth stage, reliability-based route selection is performed. A dynamic trust score is generated for each robot or communication channel, and nodes with low reliability are restricted during the route selection process.

At the fifth stage, a secure rerouting mechanism is activated. When a threat is detected on the primary route, the system automatically selects an alternative route with a lower level of risk.

Algorithmic Operating Principle of the Model. The proposed algorithm can be organized according to the following sequence:

1. Robots collect local information about the network state.
2. The collected data undergo preliminary verification.
3. The AI model calculates efficiency and security indicators for the routes within the network.
4. The anomaly detection module identifies suspicious nodes or connections.
5. Routes are re-evaluated based on the reliability indicator.
6. The most appropriate and secure route is selected.
7. When the network state changes, the decision is recalculated.

The advantage of this approach is that routing and security are not considered as separate modules, but rather as an integrated decision-making mechanism.

Experimental Evaluation Methodology of the Study. To experimentally validate the model proposed in the article, a simulation environment representing a robot swarm can be developed. During the simulation, parameters such as the number of robots, communication radius, movement speed, packet transmission frequency, network density, and number of attackers are varied.

The following indicators can be used to evaluate the effectiveness of the model:

PDR=NreceivedNsent×100%PDR=\frac{N_{received}}{N_{sent}}\times100\% where PDRPDR represents the packet delivery ratio.

In addition, average end-to-end latency, route stability, attack detection accuracy, false positive rate, false negative rate, rerouting time, and robot energy consumption should also be evaluated.

It is particularly important to compare the security performance of the AI model with that of a conventional routing algorithm. In this case, the main question should not only be “How quickly can the model find a route?”, but also “How effectively can the model maintain its functionality under attack conditions?”

Discussion. Existing scientific studies on robotic cybersecurity demonstrate that security problems are not limited to the physical components of a robot, but also encompass network, software, and data layers. The deeper integration of AI technologies into robotic systems additionally introduces the requirement to protect the model itself. A 2024 IEEE study notes the existence of scientific gaps related to the development of AI-assisted cybersecurity in robotics and autonomous systems.

From this perspective, optimizing the routing protocol in autonomous wheeled robot swarms solely on the basis of conventional network parameters is not sufficient. The security value of a route, the reliability of a node, and the integrity of the data provided to the AI model should also be incorporated into the decision function.

In the proposed approach, three objectives are optimized simultaneously: network efficiency, resilience to attacks, and continuity of system operation. However, there is a trade-off between these objectives. Excessively strict security checks may increase network latency, while overly rapid decision-making may reduce the level of security. Modern reviews of swarm robotic systems identify the balance between real-time requirements, security, and efficiency as an important open issue.

Scientific Novelty. The main scientific novelty of this article lies in considering AI-based routing for autonomous wheeled robot swarms in combination with a security metric.

In the proposed model, the following factors are taken into account within a unified decision-making process:

- network efficiency of the route;
- reliability level of the node;
- data anomaly;
- adversarial risk;
- necessity for rerouting.[7,85-p.]

Furthermore, the integration of adversarial training, anomaly detection, and trust-based routing mechanisms aimed at protecting the model itself can be considered a promising conceptual foundation for increasing the resilience of robot swarms against cyberattacks. This direction is also consistent with international taxonomies of adversarial machine learning.

Conclusion. Autonomous wheeled robot swarms may become an important component of future intelligent transportation, monitoring, search and rescue, logistics, and many other autonomous systems. However, the effectiveness of such systems is determined not only by their ability to make autonomous decisions, but also by the cybersecurity of their network and AI components.

The study proposes a multi-stage approach to protecting AI-based routing protocols against adversarial attacks, data manipulation, false data injection, and attempts to disrupt network services. This approach integrates data verification, anomaly detection, an adversarially resilient AI model, node reliability assessment, and secure rerouting mechanisms into a unified system.

Future research should involve implementing this model in ROS 2 or another robotics simulation environment, testing it with different numbers of robots and network densities, developing several scenarios of adversarial attacks, and statistically comparing protected and unprotected routing algorithms. Empirical testing is necessary to quantitatively substantiate the performance of the proposed model in terms of security, latency, packet delivery, and energy efficiency.

REFERENCES

1. Vassilev, A., Oprea, A., Fordyce, A., Anderson, H., Davies, X., & Hamin, M. (2025). Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. NIST AI 100-2e2025. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-2e2025. (NIST Computer Security Resource Center)
2. Santoso, F., & Finn, A. (2024). An in-depth examination of artificial intelligence-enhanced cybersecurity in robotics, autonomous systems, and critical infrastructures. IEEE Transactions on Services Computing, 17(3), 1293–1310. https://doi.org/10.1109/TSC.2023.3331083. (Digital Library Adelaide)

3. Yan, Y., Xie, Y., Tang, J., Li, Y., & Jin, Y. (2025). Reliability and security: from swarm robots to AI agents. Journal of Reliability Science and Engineering, 1, 032001. https://doi.org/10.1088/3050-2454/adea7a. (DOI)
4. Macas, M., Wu, C., & Fuertes, W. (2024). Adversarial examples: A survey of attacks and defenses in deep learning-enabled cybersecurity systems. Expert Systems with Applications, 238, 122223. (ScienceDirect)
5. Chen, X., Tang, J., & Lao, S. (2020). Review of unmanned aerial vehicle swarm communication architectures and routing protocols. Applied Sciences, 10(10), 3661. https://doi.org/10.3390/app10103661. (MDPI)
6. Grigorescu, S., Trasnea, B., Cocias, T., & Macesanu, G. (2021). Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. International Journal of Information Security, 20, 819–838. https://doi.org/10.1007/s10207-021-00545-8. (PubMed)
7. Diab, A., et al. (2023). Cyber security of robots: A comprehensive survey. Intelligent Systems with Applications, 18, 200237. https://doi.org/10.1016/j.iswa.2023.200237. (DOI)
8. Altun, V. C., Ata, B., & Canbay, Y. (2026). Threats, vulnerabilities and measures in robot communication security: A review. Kahramanmaraş Sütçü İmam Üniversitesi Mühendislik Bilimleri Dergisi, 29(1). (jes.ksu.edu.tr)