© 2026 International Conference on Multidisciplinary Sciences and Innovations . All Rights Reserved.

INTRUSION DETECTION SYSTEM (IDS) FOR SELF-ORGANIZING WHEELED ROBOT NETWORKS AGAINST BLACKHOLE AND SYBIL ATTACKS

Axmedov Jasur Rajab o‘g‘li
Master’s Student, ISMA University, Riga, Latvia

Abstract: This thesis investigates the development of an Intrusion Detection System (IDS) for improving the cybersecurity of self-organizing wheeled robot networks against Blackhole and Sybil attacks. The proposed approach analyzes network traffic, node behavior, routing information, and communication patterns to detect malicious activities and maintain the availability, reliability, and integrity of communication among autonomous robots.

Keywords: Intrusion Detection System, IDS, self-organizing networks, wheeled robots, cybersecurity, Blackhole attack, Sybil attack, malicious nodes, network security, autonomous robot communication.

The rapid development of autonomous systems, robotics, artificial intelligence, and wireless communication technologies has increased the use of groups of autonomous wheeled robots in various fields. Such robotic systems can be applied in industrial automation, logistics, environmental monitoring, disaster response, agriculture, and intelligent transportation systems. In many situations, a group of robots must communicate and cooperate without relying on a fixed communication infrastructure.

Self-organizing robot networks are characterized by dynamic network topology, autonomous communication, and decentralized decision-making. Each robot can act as an independent network node while simultaneously participating in the transmission and forwarding of information. Although this architecture provides flexibility and scalability, it also introduces significant cybersecurity challenges.

One of the major security problems in self-organizing robot networks is the presence of malicious nodes. An attacker may compromise a robot or introduce a malicious node into the network to disrupt communication, manipulate routing information, or impersonate multiple network identities. Blackhole and Sybil attacks are among the most dangerous attacks that can affect the reliability and stability of such networks.

Therefore, the development of an effective Intrusion Detection System is important for identifying suspicious and malicious activities before they cause significant damage to the robot network.

A Blackhole attack occurs when a malicious node falsely advertises that it has the most efficient or shortest route to a particular destination. Other nodes may therefore select the malicious node as an intermediate communication node and forward their data through it.

After receiving the data, the malicious node can intentionally drop packets instead of forwarding them to their intended destination. As a result, communication between robots can be disrupted, important control commands may be lost, and the overall performance of the robot network may decrease.

In a self-organizing wheeled robot network, the consequences of a Blackhole attack can be particularly serious. Robots may depend on communication links to exchange information about their position, movement direction, tasks, and environmental conditions. If critical information is lost because of a malicious node, robots may fail to coordinate their activities effectively.

© 2026 International Conference on Multidisciplinary Sciences and Innovations . All Rights Reserved.

An IDS can detect Blackhole attacks by monitoring packet forwarding behavior and comparing the number of packets received and transmitted by each network node. A node that receives a large number of packets but forwards only a small number may be identified as suspicious. Additional indicators such as abnormal routing advertisements and unusually attractive route claims can also be analyzed.

A Sybil attack occurs when a malicious entity creates or uses multiple false identities within a network. Instead of appearing as a single network participant, the attacker may pretend to be several independent robots or nodes.

This attack can significantly affect decentralized robot networks because many network protocols assume that each network identity represents a unique physical node. By creating multiple identities, an attacker may manipulate network routing, influence distributed decision-making processes, and gain an unfair advantage in communication protocols.

For example, a malicious robot may generate several fake identities and appear to represent multiple robots in the same communication area. This can create false information about the network topology and lead legitimate robots to make incorrect routing or coordination decisions.

An Intrusion Detection System can help detect Sybil attacks by analyzing identity-related behavior. The system may compare communication patterns, physical location information, signal characteristics, and behavioral similarities among network identities. If several identities demonstrate highly similar communication behavior or appear to originate from the same physical location, they can be classified as suspicious.

The proposed IDS for self-organizing wheeled robot networks consists of several functional stages. The first stage is data collection. During this stage, the system gathers information related to network traffic, packet transmission, routing messages, node identities, and communication behavior.

The second stage is behavior analysis. The IDS analyzes the collected information to identify normal and abnormal network activities. Parameters such as packet delivery ratio, packet forwarding behavior, routing response time, node identity frequency, and communication patterns can be used as detection features.

The third stage is attack detection. The system compares the observed behavior of network nodes with predefined security rules or learned behavioral patterns. Suspicious activities are classified according to their characteristics. For example, a node that continuously receives packets but fails to forward them may be associated with a potential Blackhole attack.

Similarly, multiple network identities demonstrating identical communication patterns or physical characteristics may indicate the presence of a Sybil attack.

The final stage is response and mitigation. After detecting a malicious node, the IDS can inform other robots about the potential threat. The suspicious node may then be isolated from routing operations, and other robots can avoid forwarding critical information through that node.

Artificial intelligence and machine learning techniques can improve the effectiveness of intrusion detection systems. Traditional IDS approaches often depend on predefined rules, which may be ineffective against new or modified attack strategies.

Machine learning algorithms can analyze large amounts of network data and identify unusual behavior automatically. By learning the characteristics of normal robot communication, an AI-based IDS can detect deviations that may indicate malicious activity.

Supervised learning algorithms can be trained using labeled datasets containing normal network behavior and different types of cyberattacks. Unsupervised learning methods can also be useful when labeled attack data are limited. These algorithms can identify abnormal patterns without requiring detailed information about every possible attack.

© 2026 International Conference on Multidisciplinary Sciences and Innovations . All Rights Reserved.

In the proposed system, artificial intelligence can be used to continuously analyze the behavior of robots and network nodes. This makes the IDS more adaptive to changes in network topology and robot movement.

The proposed IDS provides several advantages for self-organizing wheeled robot networks. First, it can improve the security and reliability of communication between autonomous robots. Second, the system can detect malicious activities before they significantly affect the network.

Another important advantage is adaptability. Since wheeled robots can move continuously, the network topology may change frequently. An intelligent IDS can analyze these changes and distinguish between normal topology changes and suspicious activities.

The system can also support decentralized security mechanisms. Instead of relying entirely on a central server, robots can participate in monitoring the security of the network. This approach is particularly useful in environments where fixed communication infrastructure is unavailable.

In conclusion, self-organizing wheeled robot networks require effective cybersecurity mechanisms to ensure secure and reliable communication. Blackhole and Sybil attacks represent significant threats because they can disrupt data transmission, manipulate routing information, and create false network identities.

The development of an Intrusion Detection System can provide an effective solution for monitoring network behavior and identifying malicious activities. By combining traffic analysis, node behavior monitoring, identity verification, and artificial intelligence techniques, the proposed IDS can improve the security, availability, and reliability of autonomous robot communication. Future research may focus on implementing the proposed system in a real or simulated robot network environment and evaluating its performance under different attack scenarios.

REFERENCES

1. Ganiev, S. K. (2017). Axborot xavfsizligi [Information Security]. Tashkent: Fan va texnologiya.
2. Djurayeva, R. Kh., Jabbarov, Sh. Yu., & Umirzakov, B. M. (2019). Setevaya bezopasnost [Network Security]. Tashkent: Aloqachi.
3. Mamatov, I., Galety, M. G., & Natarajan, A. K. (2026). Hands-On Computer Networks and AI-Driven Cybersecurity: A Comprehensive Student Guide. Cham: Springer.
4. Khanna, N., & Sachdeva, M. (2019). A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in mobile ad hoc networks. Computer Science Review, 32, 24–44.
5. Conti, M., Willemsen, J., & Crispo, B. (2013). Providing security and privacy in wireless and mobile networks. IEEE Communications Surveys and Tutorials.
6. Nuriddinova, N. N. (2025). Sun'iy intellekt asosida kiberxavfsizlikni ta'minlash: yangi yondashuvlar va texnologiyalar. Yosh olimlar, 3(22), 88–91.
7. Temirbekov, S. F. (2025). Sun'iy intellekt va kiberxavfsizlik: ilm-fan rivojlanishida raqamli inqilob va yangi imkoniyatlar. Ilmiy tadqiqotlar va ularning yechimlari jurnali.
8. Piro, C., Shields, C., & Levine, B. N. (2007). Detecting the Sybil attack in mobile ad hoc networks. In Proceedings of the IEEE International Conference on Security and Privacy in Communication Networks. IEEE.
9. Tseng, F.-H., Chou, L.-D., & Chao, H.-C. (2011). A survey of black hole attacks in wireless mobile ad hoc networks. Human-Centric Computing and Information Sciences, 1(4), 1–16.
10. Mitchell, R., & Chen, I.-R. (2014). A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Surveys, 46(4), 1–29.
11. Butun, I., Morgera, S. D., & Sankar, R. (2014). A survey of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys and Tutorials, 16(1), 266–282.

© 2026 International Conference on Multidisciplinary Sciences and Innovations . All Rights Reserved.

12. Stallings, W. (2023). Network Security Essentials: Applications and Standards. Pearson.
13. Qodirov, F., & Xolmurodova, A. (2025). Tarmoq xavfsizligini ta'minlashda sun'iy intellekt imkoniyatlari. Fan va innovatsiya.
14. Ulug'bekov, A. U., Qurbonazarov, F. F., & To'rayev, R. N. (2025). Sun'iy intellekt asosidagi kiberxavfsizlik tizimlari: zamonaviy yondashuvlar, jahon tajribasi va O'zbekiston uchun istiqbollar. Ustozlar uchun.
15. Forouzan, B. A. (2021). Data Communications and Networking. McGraw-Hill Education.