engineering proceedings

MDPI

Proceeding Paper

Robotic Sensor Network Security: Threat Analysis and Enhancement Strategies †

Shukun Wu [1,2,*], Deshinta Arrova Dewi [1] and Chunling Lang [3]

[1] Faculty of Data Science and Information Technology, INTI International University, Nilai 71800, Malaysia
[2] Smart Agriculture College (Internet of Things Engineering College), Guangxi Science & Technology Normal University, Laibin 546199, China
[3] College of Mathematics and Computer Engineering, Guangxi Science & Technology Normal University, Laibin 546199, China
* Correspondence: i25031823@student.newinti.edu.my
† Presented at 8th International Conference on Knowledge Innovation and Invention 2025 (ICKII 2025), Fukuoka, Japan, 22–24 August 2025.

Abstract

Robots and diverse sensors constitute a self-contained network. The integration of the Internet and the IoT extends this network, enabling seamless interconnection and information exchange between robotic sensors and external systems. Given that cybersecurity breaches cause significant losses, strengthening the security defenses of autonomous robots and sensor networks is critical. To enhance cybersecurity within robotic sensor networks, we examined strategies, objectives, frameworks, and methods for security improvement in this study. Through case-based analysis, recommendations and references were suggested to advance the cybersecurity capabilities of robotic sensor networks.

Keywords: sensor networks; robotics; cybersecurity architecture; threat analysis; countermeasures

1. Introduction

Robotic technology represents an inevitable trend and an essential tool for future development. Robots relieve humans from arduous and repetitive physical labor, focusing on innovative, creative, and emotionally engaging tasks. This transformation enhances labor efficiency [1] and ultimately reshapes human life. A key factor allowing robots to perform relatively complex tasks is their capacity for autonomous environmental perception. By independently observing their surroundings, robots establish the foundation for decision-making and action by using sensors. Drawing an analogy with humans, sensors are equivalent to human senses and skin [2]. To fulfill their roles, multi-sensor integration is indispensable, as a single sensor cannot provide sufficient data. For multiple sensors, specialized networks known as robotic sensor networks are necessary [3], which represent a distinct application of the Internet incorporated into IoT [4].

The internet and IoT have profoundly transformed the world. Since the 21st century, the network era has begun, in which networks have reshaped production and lifestyles, driven economic growth, and defined future development trajectories. Emerging technologies, particularly networking, are prioritized as a strategic focus to advance traditional industries.

In such a trend, cybersecurity is essential [5]. Once regarded as relevant only to isolated information systems with limited impact, cybersecurity encompasses interconnected infrastructures where failures in a single system cascade into households through the IoT,

check for updates

Academic Editors: Teen-Hang Meen, Chun-Yen Chang and Cheng-Fu Yang

Published: 25 February 2026

Citation: Wu, S.; Dewi, D.A.; Lang, C. Robotic Sensor Network Security: Threat Analysis and Enhancement Strategies. *Eng. Proc.* **2025**, *120*, 70. https://doi.org/10.3390/engproc2025120070

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

disrupt modern factories through smart manufacturing, or generate societal and military consequences through cyberattacks. Robots, connecting networks and operating through coordinated sensor systems, become integral components of the broader internet framework, extending beyond independent sensor networks. For autonomous robots, the critical importance of cybersecurity is therefore unequivocally underscored.

2. Robotic Sensor Network System Architecture

A robotic sensor network is a comprehensive system architecture that integrates a robotic operating platform, multiple sensors, communication networks, and computation and control units. Its objective is to achieve the acquisition, transmission, and processing of environmental information through networked operation. Although the functional units are logically independent, they operate cooperatively to support perception, decision-making, and execution in complex environments.

To illustrate the overall composition and functional relationships of a robotic sensor network, a system architecture diagram is presented in Figure 1. From a functional perspective, the diagram abstracts the system into four main components: the physical platform, sensor layer, communication and network layer, and computation and control unit, and depicts their relative positions and interactions. It should be noted that this hierarchical division does not represent a physical separation, but rather clarifies the functional roles of different components and provides a structural basis for subsequent analysis. Figure 1 is intended to describe the overall system structure, while detailed technical implementations are beyond the scope of this paper.

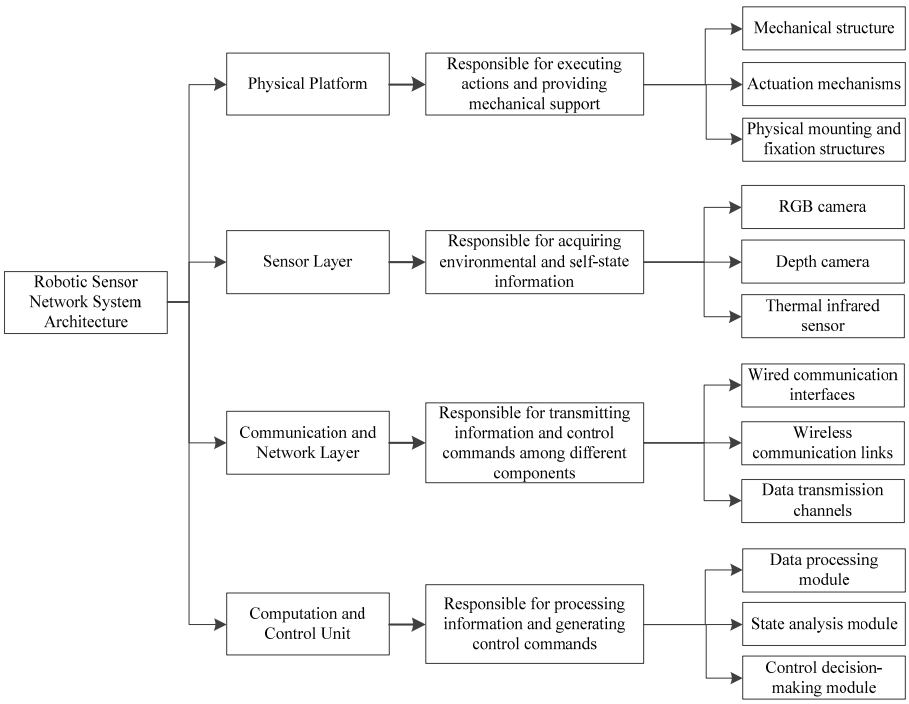

Figure 1. Robotic Sensor Network System Diagram.

The physical platform provides mechanical structure and actuation capability and serves as the physical foundation of the system, without performing information acquisition, transmission, or decision-making tasks. The sensor layer is responsible for acquiring environmental and self-state information and acts as the primary information source of the system. The communication and network layer enables data transmission and connectivity among functional components, playing a key role in supporting stable system operation.

The computation and control unit processes sensor data and generates control commands, serving as the decision-making core of the robotic sensor network, and its reliability is closely related to system security and controllability.

Overall, the robotic sensor network achieves environmental perception and robot behavior control through the coordinated operation of these functional components. Due to its multi-layered, networked, and highly cooperative nature, the system involves extensive data interaction and remote communication, which introduces significant security challenges. Therefore, analyzing security threats based on this system architecture is of great importance.

3. Risks in Sensor Network

Common threats and risks to robots and their sensor networks are illustrated in Figure 2.

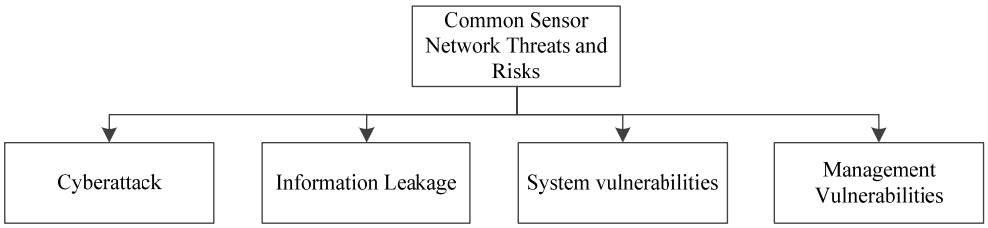

Figure 2. Diagram of common threats and risks to sensor networks.

Cyberattacks represent a prevalent cybersecurity threat, in which hackers remotely target robotic systems and frameworks to disrupt operations, compromise functionality, steal specialized operational data, or pursue illicit financial gain. For example, unauthorized individuals might deploy malware within a robot's sensor network, interfering with system performance or exploiting vulnerabilities to infringe upon broader rights.

Robotic operations inherently involve substantial volumes of critical data related to security, privacy, and finance. If compromised, such data leakage leads to consequences ranging from minor privacy breaches or exposure of sensitive personal information to severe incidents that undermine operational integrity. For instance, cybercriminals may infiltrate a robot's camera system through the internet, co-opting its cameras for illicit purposes and thereby causing privacy violations, financial losses, or psychological harm.

System vulnerabilities further exacerbate these risks. Robotic networks are not established in a single phase, and earlier systems often lack robust cybersecurity measures, rendering them more susceptible to exploitation. Recent systems typically incorporate stronger protections as technologies advance. However, within a single operational environment, robots manufactured across different periods may coexist, and disparities among their systems can create weak points in data interfaces that expose them to attack.

Management vulnerabilities also play a critical role. Robotic systems remain human-dependent, requiring personnel for both establishment and maintenance. Human involvement, while indispensable, introduces systemic risks through operational errors, whether deliberate or inadvertent. For example, an engineer responsible for maintaining robot data might temporarily disable a firewall to facilitate program or data updates. Such actions enable unauthorized individuals to infiltrate sensor networks.

4. Sensor Network Security

Strategies represent the concrete implementation of principles, while objectives embody aims and aspirations. In cybersecurity, strategic and objective security is indispensable. Without secure protocols and clearly defined objectives, neither robust systems nor effec-

tive operations can be achieved. Accordingly, specific mechanisms must be employed to safeguard both regulatory security and purpose-driven security.

The first security mechanism involves establishing policy and objective review protocols. Effective progress requires inspection systems to monitor operational status through manual spot checks and big data anomaly analysis. These measures provide timely feedback and corrective action, ensuring that security objectives are realized. The second mechanism is policy and objective re-examination. Unlike initial reviews, re-examination constitutes a follow-up assessment of improvements, reinforcing focus and enhancing the security of policies and objectives. For example, the first inspection of a child's homework represents review, while subsequent verification of task completion represents re-examination. This process enables an understanding of rules and goals while strengthening assurance. The third mechanism is the implementation of non-periodic spot checks. By assessing subjects and content in their most authentic state, non-periodic checks facilitate improvement and support, while reducing inspection costs and improving efficiency. Together, these mechanisms form the foundation of the policy and objective assurance framework, illustrated in Figure 3.

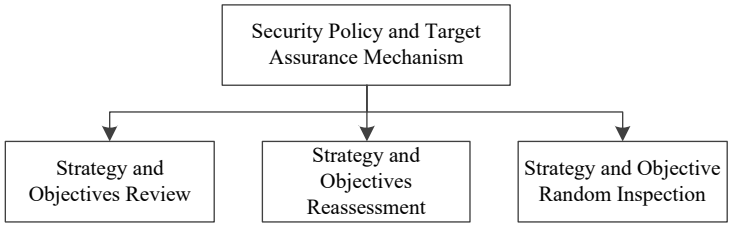

Figure 3. Security strategy and objective assurance mechanism diagram.

Beyond policy assurance, appropriate business strategies and principles are equally critical. Sound strategies streamline operations, while principles are needed to define the purpose of requirements. The business strategy and principle framework is illustrated in Figure 4. The framework is user-centric. Robots enhance user experience and convenience. Therefore, cybersecurity policies must not only strengthen the security of robots and their sensor networks but also accommodate reasonable user requirements. Functionality must remain intact, as strategies that compromise usability risk prioritizing means over ends.

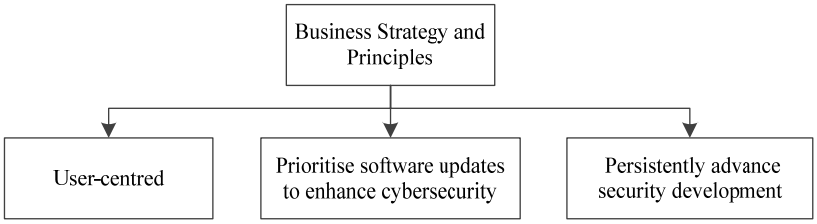

Figure 4. Business strategy and principle framework diagram.

Another essential strategy is prioritizing software updates to enhance cybersecurity. Once manufactured, robots undergo prolonged user engagement, during which users become accustomed to their operation and sensitive to modifications or associated costs. Extensive retrofitting of long-term robotic assets is unlikely to be accepted, and hardware upgrades for unsold robots may incur significant costs in mechanical structures and design. For sold units, users are generally unwilling to pay additional fees for cybersecurity enhancements. By contrast, software updates are cost-effective, feasible, and widely accepted. While hardware upgrades may occasionally be necessary, they must be carefully balanced against cost and update frequency.

5. Framework and Methods

Secure networks support secure applications and environments. It is necessary to prioritize the actual security needs of individuals within the network, as people constitute the essence of cybersecurity. Achieving cybersecurity requires sustainable measures that avoid short-sighted solutions, which sacrifice long-term benefits. It cannot be a permanent solution. Rather, continuous development and improvement are required. The framework and methods for enhancing sensor network security are illustrated in Figure 5.

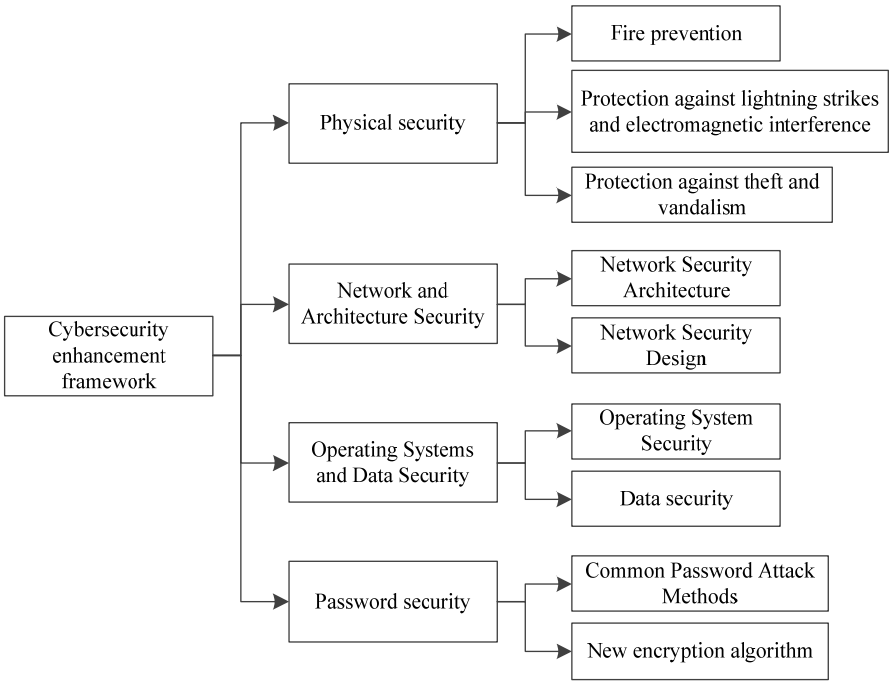

Figure 5. Diagram of the sensor network security enhancement framework and methods.

5.1. Physical Security

Domestic and industrial robotic data are obtained from networked equipment. The conversion of electrical energy and operation of appliances generate significant heat, and air conditioning alone cannot guarantee protection against overheating. Fire safety requires the effective use of sensors and equipment. Where such equipment is absent, environmental monitoring devices, such as temperature and smoke sensors, must be installed, with alarms connected to the control room. In addition, fire safety equipment and facilities must be regularly inspected to ensure immediate response and suppression. Lightning strikes and electromagnetic interference also pose risks, potentially damaging equipment or disrupting operations. Protection depends on building structure and hardware installations. Daily manual safety inspections are essential to promptly identify and rectify issues, while quarterly checks of both network equipment and building facilities help uncover hidden hazards. Robots are valuable assets, making theft and vandalism prevention difficult. Although rare, deliberate damage occurs in heightened emotion. Addressing these risks requires strengthening awareness campaigns to emphasize equipment importance and safety requirements, alongside deploying security personnel patrols to detect potential problems.

5.2. Network and Architectural Security

Network security architecture encompasses cloud, network, and data security domains. At the server level, dedicated personnel should oversee each domain, although in smaller-scale operations, a single individual may supervise all. Robust backup and isolation measures must be integrated into the design framework. Backups safeguard critical

data against temporary failures, while isolation mechanisms limit the impact of viruses or other threats to a contained scope. Network security design requires the integration of multiple technologies across the system. Firewalls, as mature and widely deployed products, prevent unauthorized access to application and data servers. Their flexibility allows deployment across both local and cloud environments, supported by specialized cloud products and policies provided by infrastructure-as-a-service (IaaS) providers. Intrusion prevention systems (IPS) are used to protect unpatched servers by blocking attacks on vulnerabilities. IPS functionality can be integrated into other security products or deployed as standalone solutions, with particular emphasis on intrusion detection in publicly accessible network segments.

5.3. Operating System (OS) and Data Security

OS security ensures the integrity and stable operation of programs, protecting them from external attacks or disruptions. As the bridge between hardware and applications, OS failures can cause widespread disruption, underscoring the need to prioritize OS security. Key considerations include (1) employing genuine, officially released systems to mitigate risks of unauthorized backdoor programs, and (2) conducting thorough compatibility testing before bulk updates to ensure operational requirements remain intact. Data security safeguards network information and system reliability. Compromised data results in severe commercial repercussions and privacy breaches. Enhancing data security requires robust classification management and isolation measures.

Data must be categorized into four levels of importance: extremely critical, significantly important, generally important, and publicly accessible. Permissions for creation, viewing, modification, and verification must correspond to classification levels. For important data, physical isolation is required, with devices disconnected from external networks and copying permitted only with senior approval. Critical data must be transmitted internally but must remain isolated from external networks, requiring mid-level approval. Moderately important data may allow external access but must employ multi-layered encryption and locking, with copying subject to standard approval. Publicly accessible data must be clearly distinguished, with controlled access duration.

5.4. Password Security

The most prevalent encryption method in contemporary society ranges from financial transactions to everyday services. Common cryptographic attack methods include ciphertext-only attacks, known-plaintext attacks, ciphertext-or-plaintext attacks, and chosen ciphertext attacks [6]. To counter these threats, diverse encryption algorithms must be employed. Emerging techniques include key agreement protocols, blockchain-based encryption, dynamic password systems, chaotic cryptographic algorithms, and quantum cryptography [7]. Configuring passwords with multiple encryption methods in tandem enhances the reliability and confidentiality of network security measures.

6. Conclusions

Robotic sensor networks, comprising robots, their embedded sensors, and internet connectivity, have evolved into critical components of the internet and IoT. The autonomous capabilities of robots highlight the importance of these networks. Security breaches within robotic sensor networks may lead to privacy violations, financial losses, or the compromise of sensitive information, underscoring the need for rigorous attention to their protection. We proposed recommendations and countermeasures to strengthen cybersecurity and enhance frameworks and methodologies encompassing physical security, network security, operating system and data security, and cryptographic security.

Author Contributions: Conceptualization, S.W. and D.A.D.; methodology and investigation, S.W.; writing—original draft preparation, S.W.; writing—review and editing, D.A.D. and C.L.; supervision, D.A.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wang, W.; Siau, K. Artificial Intelligence, Machine Learning, Automation, Robotics, Future of Work and Future of Humanity: A Review and Research Agenda. *J. Database Manag.* **2019**, *30*, 61–79. [CrossRef]
2. Roychoudhury, A.; Khorshidi, S.; Agrawal, S.; Bennewitz, M. Perception for Humanoid Robots. *Curr. Robot. Rep.* **2023**, *4*, 127–140. [CrossRef]
3. Ryu, J.H.; Irfan, M.; Reyaz, A. A Review on Sensor Network Issues and Robotics. *J. Sens.* **2015**, *2015*, 140217. [CrossRef]
4. Pradhan, B.; Bharti, D.; Chakravarty, S.; Ray, S.S.; Voinova, V.V.; Bonartsev, A.P.; Pal, K. Internet of Things and Robotics in Transforming Current-Day Healthcare Services. *J. Healthc. Eng.* **2021**, *2021*, 9999504. [CrossRef] [PubMed]
5. Kamilaris, A.; Botteghi, N. The Penetration of Internet of Things in Robotics: Towards a Web of Robotic Things. *arXiv* **2020**, arXiv:2001.05514. [CrossRef]
6. Bellare, M.; Rogaway, P. *Introduction to Modern Cryptography*; Course Notes; University of California: Davis, CA, USA, 2005.
7. Zhang, B.; Liu, L. Chaos-Based Image Encryption: Review, Application, and Challenges. *Mathematics* **2023**, *11*, 2585. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.