Journal of Computing Theories and Applications ISSN:3024-9104

Review Article

Comprehensive Review of Security Problems in Mobile Robotic Assistant Systems: Issues, Solutions, and Challenges

Long Q. Dinh [1], Dung T. Nguyen [1], Thang C. Vu [1], Tao V. Nguyen [1], and Minh T. Nguyen [2],*

[1] Faculty of Engineering and Technology, Thai Nguyen University of Information and Communications Technology, Viet Nam; e-mail: dqlong@ictu.edu.vn; ntdungcndt@ictu.edu.vn; vcthang@ictu.edu.vn; nvtao@ictu.edu.vn

[2] Faculty of International Training, Thai Nguyen University of Technology, Thai Nguyen University, Viet Nam; e-mail: nguyentuanminh@tnut.edu.vn

* Corresponding Author : Minh T. Nguyen

Abstract: Nowadays, robots in the modern world are playing an important and increasingly popular role. MRA (Mobile Robotic Assistant) is a type of mobile robot designed to support humans in many different fields, helping to improve efficiency and safety in daily activities, work, or medical treatment. The number of MRAs is increasing and diverse in function, in addition to the ability to collect and process data, MRAs also have the ability to physically interact with users. Therefore, security is one of the important issues to improve the safety and effective operation of MRA. In this paper, through a com-prehensive literature review and detailed analysis of the prominent MRA security attacks in recent years (based on criteria such as: attack targets, technologies used, impact level, feasibility, and contribution to addressing overall MRA security issues), a systematic classification by MRA activity fields is conducted. Security attacks, threats, and vulnerabilities are examined from various perspectives, such as hardware attacks or network/system-level attacks, operating systems/application software. Additionally, corresponding security solutions are proposed, compared, and evaluated to enhance MRA security. The paper also addresses challenges and suggests open research directions for the future.

Keywords: Cryptographic protocols; Hardware attacks; Intrusion detection; Mobile Robotic Assistant; Security attacks.

Received: August, 19th 2024
Revised: September, 5th 2024
Accepted: September, 16th 2024
Published: September, 17th 2024

1. Introduction

Mobile Robotic Assistants (MRAs) are designed to assist humans in many fields such as industry, medicine, services, etc. to replace human labor and improve the quality of life. MRA systems are equipped with advanced technologies, such as artificial intelligence to increase operational efficiency and the ability to perform complex tasks. Modern MRAs allow for close interaction with users, the ability to physically interact highlights the importance of MRAs in today's life.

In addition to the potential benefits of MRAs, there are concerns about privacy and security. MRAs are often designed with many types of sensors that collect different types of data (including important information), and can work in sensitive places[1]. The study by Fosch-Villaronga et al. shows that security attacks on MRA often cause property damage, psychological harm to users, or disrupt the operation of MRA systems[2], [3]. In practice, MRA systems typically have limitations in authorization/ authentication [4], encryption [5], and physical protection [6], which are often the main reasons these systems are vulnerable to security attacks. Fosch-Villaronga [2] conducted research on cybersecurity challenges and their impact on the integrity of MRA systems in the healthcare sector. Dóczi addressed the availability of MRA systems [7] and colleagues, who proposed an application-layer solution to control and protect the data flow between nodes. Staffa's [8] study suggested a security solution based on using safety zones, allowing developers to implement preventive measures during the robot design phase. Moreover, other notable attacks in the MRA field include sensitive information theft [9], interference[6], robot behavior control[10], spoofing, and espionage[5], among others.

DOI : 10.62411/jcta.11408

In MRA systems, implementing robust security measures not only prevents common cyberattacks but also ensures that data exchange, storage, and robot operations are not compromised. The aforementioned studies have highlighted prominent MRA security attacks in recent years, based on criteria such as attack targets, technology used, impact level, feasibility, and contribution to overall MRA security solutions. However, gaps remain in these studies, particularly in thoroughly analyzing attacks from hardware, network, and operating system/application software perspectives. Additionally, corresponding security methods need to be considered holistically based on criteria such as cost optimization, resource efficiency, energy savings, and ensuring system availability.

Given the diversity and complexity of modern attacks, continuously updating and strengthening security measures is essential to ensure that MRA systems operate safely, effectively, and reliably. In this paper, through a comprehensive literature review and detailed analysis of prominent MRA security attacks in recent years, the importance of MRA systems is highlighted based on their applications across various fields. Security issues in MRA systems are examined, and related security attacks are classified into hardware, network, and operating system/application software attacks. From there, corresponding security solutions are proposed, compared, and evaluated to minimize security attacks, threats, and vulnerabilities in MRA systems. The rest of the paper is organized as follows: In Section 2, security issues and the importance of security in MRA systems are described, along with their requirements and constraints. Section 3 classifies the attacks in MRA systems, security solutions and protection of MRA systems are presented and compared and evaluated in Section 4. In Section 5, opening challenges and some future research proposals are specifically mentioned. Finally, conclusions are provided in Section 6.

2. MRA and security issues

2.1. General structure of MRA

Robots play an important role in today's life, including MRA systems, which are mobile robots designed to support people in many different fields, helping to improve their capabilities, efficiency, and safety in daily activities (tour guides, receptionists, health care, etc.)[11].

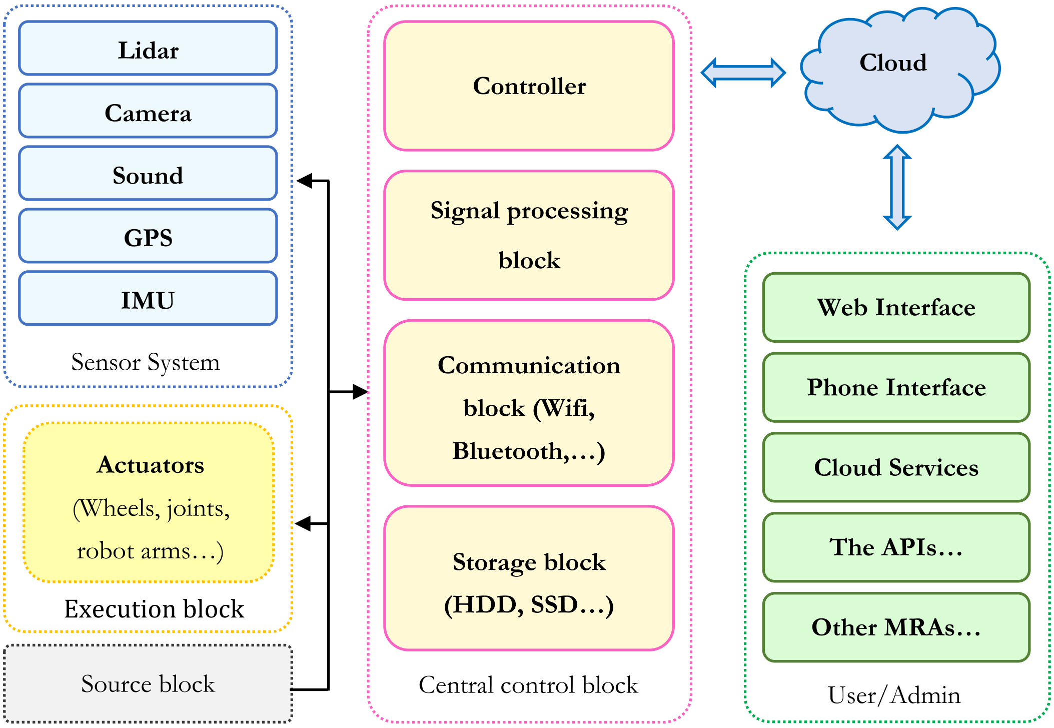

Figure 1. MRA system components

Advances in manufacturing technology: The ability to move flexibly, interact with people, communicate naturally, or integrate with AI makes MRA increasingly intelligent, perform better, and be able to perform many complex tasks. MRA has modern sensors to collect many different types of data, even sensitive information.

The important components of the MRA system are described in Fig. 1. The control system is designed based on the level of automation of the application: MRA can operate according to a pre-set program; or require human intervention in some tasks; MRA can be integrated with AI to be smarter and improve operational efficiency. Physical components (with modern sensors, motors, actuators, movement systems, robotic arms, etc.) and network components use wireless connections, cloud computing, etc. In addition, the MRA system also has functions such as localization and mapping, motion planning, computer vision, and development of field-specific sensors. MRA systems have advantages in data storage capacity, real-time processing speed, or management of heavy computing tasks such as navigation, object recognition, etc[12], [13].

2.2 Classification of assistive robot applications

Nowadays, MRA systems have been implemented, and their applications are very diverse. Fig. 2 illustrates the applications of MRA in different areas.

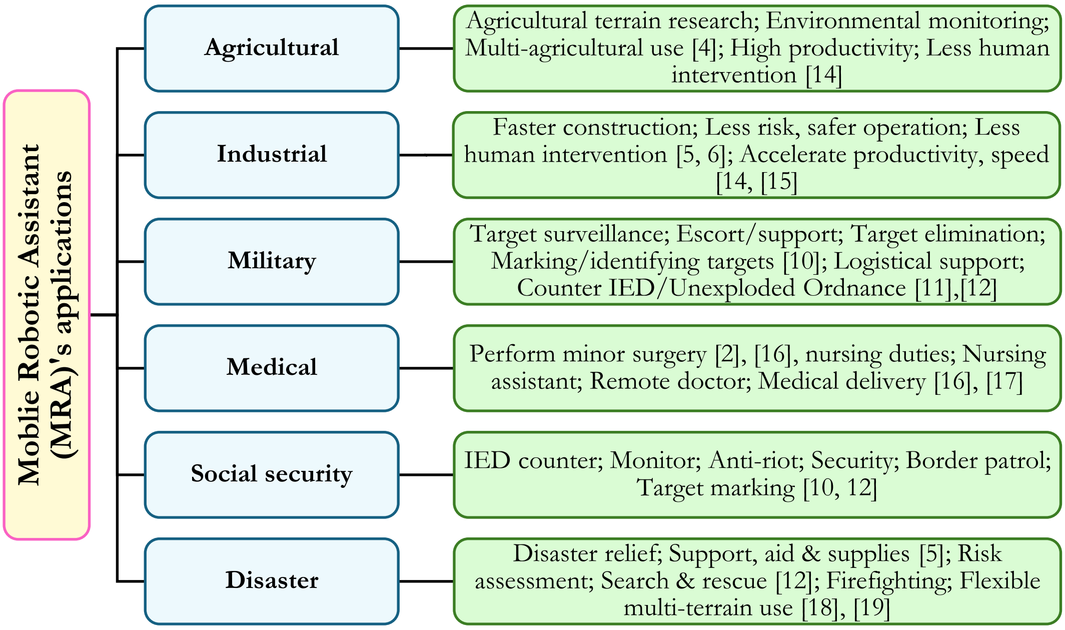
Moblie Robotic Assistant (MRA)'s applications
Agricultural
Agricultural terrain research; Environmental monitoring; Multi-agricultural use [4]; High productivity; Less human intervention [14]
Industrial
Faster construction; Less risk, safer operation; Less human intervention [5, 6]; Accelerate productivity, speed [14, [15]
Military
Target surveillance; Escort/support; Target elimination; Marking/identifying targets [10]; Logistical support; Counter IED/Unexploded Ordnance [11],[12]
Medical
Perform minor surgery [2], [16], nursing duties; Nursing assistant; Remote doctor; Medical delivery [16], [17]
Social security
IED counter; Monitor; Anti-riot; Security; Border patrol; Target marking [10, 12]
Disaster
Disaster relief; Support, aid & supplies [5]; Risk assessment; Search & rescue [12]; Firefighting; Flexible multi-terrain use [18], [19]

Figure 2. Applications of MRA in a number of fields

- Agriculture field: MRAs perform tasks efficiently, reduce human labor, and increase agricultural productivity, especially when handling large farming areas. MRAs can operate in various agricultural environments, from large fields to greenhouses. MRAs can perform tasks such as sowing and planting, tending crops, harvesting, or monitoring and managing farms.[14];
- Industrial field: MRAs perform tasks faster, safely, and with high efficiency[15]. MRA with flexible mobility can transport goods or move into hard-to-reach areas to inspect and maintain equipment;
- Military field: MRA in the military field is developed to perform reconnaissance, patrol, monitor important areas, bomb disposal, and combat support. In particular, unmanned aerial vehicle applications are researched and developed to perform special missions[20];
- Medical field: MRA is deployed in activities such as telemedicine, patient care, and support [17]. MRA is also used in surgeries that require high precision and minimal invasiveness[16];
- Social security field: MRA plays an important role in enhancing social security and order, especially the ability to respond quickly to emergency situations. These robots are

designed to assist police forces in patrolling, monitoring, handling dangerous situations and protecting the community[18];

- Disaster field: With the ability to operate flexibly on many different terrains, MRA is capable of supporting relief in natural disasters and catastrophes, such as: search and rescue; aid and transportation of supplies, and disaster impact assessment[19].

2.3. Security in the MRA system

2.3.1. Security issues in the MRA system

Security in the MRA system is an important factor to ensure safety and privacy for users, data information is strictly secured against sharing, interference, or changing information content; at the same time, it also prevents MRA from being illegally violated and controlled, distorting operations. This not only maintains the continuous and reliable operation of MRA but also protects the assets and information of organizations and users (see Fig. 3).

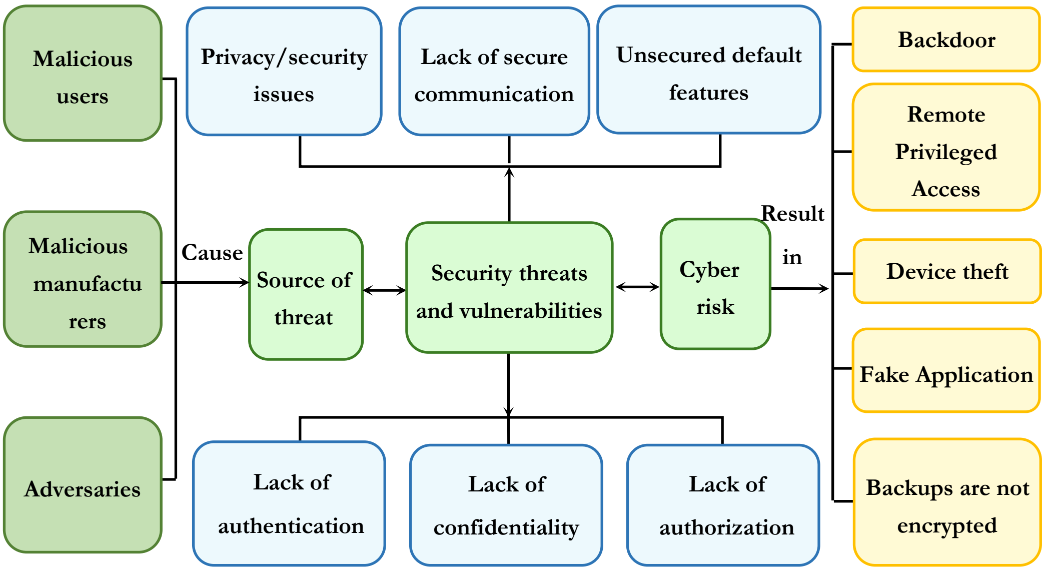

Figure 3. Overview of security issues in the MRA system

Threats to the MRA security system come from adversaries, malicious manufacturers or malicious users. These actors launch attacks to illegally collect information, interfere with the system or manipulate the MRA system to malfunction. Attacks can be carried out through applications masquerading as legitimate applications developed by third parties. Such ap-plications include various types of malware attached, such as Ransomware, backdoors, spyware, botnets, worms, trojans, etc. In addition, MRA devices are also vulnerable to theft or hijacking: Thieves are able to perform de-authentication and disconnect the legitimate owner to regain control of the robot[10].

- Security threats and vulnerabilities: Including issues of privacy, authentication, security, authorization, etc. This affects the processing and performance of the robot. It can even lead to system congestion, blocking, data extraction, and damage to MRA. MRA applications with weak security capabilities are susceptible to user privacy attacks[21];
- Network risks of MRA systems: Unsecured remote access, wireless communication ports, and open communication ports can be used to remotely access a certain robot system to launch a network attack[22]. Some common attacks in MRA systems are: Various wired/wireless connection and communication attacks (including replay attacks, man-in-the-middle attacks, eavesdropping, spoofing, etc.).
- In addition to the issues listed, there are many other threats targeting MRA systems and system security vulnerabilities, such as[23]:
- Threats aimed at analyzing traffic, spoofing, modifying data/information, injecting malicious data or malware, and compromising the hardware of robotic devices. In particular, with the integration of AI technology in MRA, attacks aimed at modifying

information are common threats that affect the performance of AI (ability to distinguish between images, accuracy in performing tasks, etc.);

- Availability threats include service data theft, denial/disruption of service, resource depletion, interference, and various types of malware (Trojans, botnets, etc.). MRA availability threats can cause hardware damage and interference with MRA sensors or actuators. In addition, cyber threats to MRA can be selective replay and forward attacks, wormholes, blackholes, and sinkholes;
- Authentication threats include malicious third-party applications and services, phishing and social engineering (deceiving MRA employees or operators to gain unauthorized access to MRA systems), privilege abuse, information theft, spoofing attacks

2.3.2. The importance of security in MRA systems

The number of attacks on robot systems in general or MRA in particular is increasing, so security in MRA systems is an important factor in protecting assets, information and safety for users:

- For individual users: MRA systems in the civil field often collect data, process personal information of users such as images, surveillance videos, or personal information, health status, etc. Security for MRA systems is to comply with regulations on privacy and protection of user data, avoid illegal data abuse or unauthorized monitoring of users[21];
- In business and industry: MRA support brings significant growth and efficiency due to higher productivity, optimized time and human resource costs[21]. However, MRA attacks in this field will cause loss of customer confidence and economic losses to organizations, businesses and individuals;
- In healthcare: MRA systems in this field are of concern because when the system is compromised, it will be possible to perform hardware attacks (causing loss of control) or logic attacks (modifying/injecting malicious data)[24];
- In social security and military: In this field, MRA can be upgraded to carry lethal weapons [25]. Therefore, without ensuring the deployment of safer and more secure robots, MRA systems can be compromised or reprogrammed to perform actions that are dangerous to humans.

2.3.3. Security requirements and constraints

Some important security requirements that need to be considered in MRA systems are described in Table 1.

Table 1. Security and privacy requirements of MRA systems:

Requirements	Motivation
Transparency	Users will grasp and control the robot's operations
Channel security	Avoid data leakage
Data integrity and availability	Ensure accurate and reliable data. Detect and minimize the impact of attacks to increase data availability.
Access control	Only authenticated users and authorized users have valid access.
Network and storage security	Storage and remote access do not leak user data.
Scalability	MRA system can serve many users, performance is not degraded, low cost and fast response time.

In addition, MRA security solutions need to meet the following constraints:

- Adaptive security: Security solutions in MRA systems must be proactive and adaptive. These adaptive security solutions can be divided into two main types: threat-focused or data-focused to know which data needs to be secured (even AI-resistant)[26];
- Security programs and software: Use firewalls and anti-virus software to protect the system from threats. The system must be periodically assessed for security, penetrated, and regularly updated for software to improve and enhance protection against the latest security attacks. In addition, when attacks occur, the system program needs to identify and respond promptly;

- Low-energy security: To build energy-efficient security services, low-energy security protocols provide an alternative to heavy cryptographic systems that consume many energy resources[27]. However, designing a lightweight, robust, and efficient crypto-graphic protocol for MRA applications is not easy due to the constraints on robot performance, such as communication costs, latency, resource usage, etc., so the balance between security and cost also needs to be considered;
- Authentication and authorization: Use strong authentication methods (such as multifactor authentication) to ensure that only authorized users can access the system. Manage system user permissions to limit unnecessary access.

3. Classification of attacks in MRA system

MRA systems face many different types of attacks, especially when MRA is integrated with IoT technology in fields such as industry, medicine, and the military[28]. In the framework of this article, we focus on common attacks related to MRA, classified as: Hardware attacks, network attacks, and operating system/application software attacks (see Fig. 4).

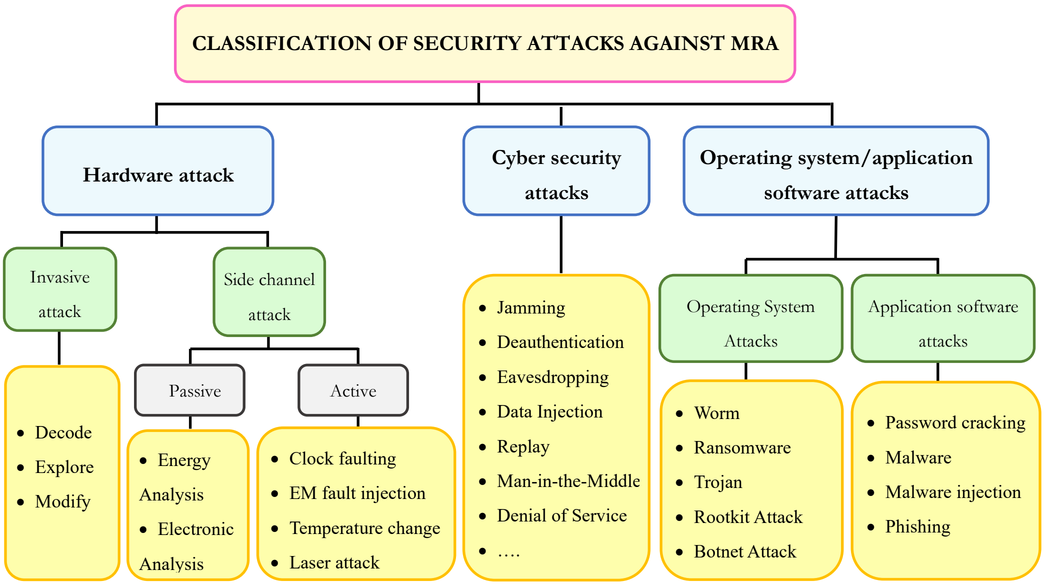

Figure 4. Classification of attacks in MRA

3.1. Hardware attacks

Attacks against the hardware of MRA systems, including invasive attacks and side-channel attacks. Invasive attacks aim at physically interfering with the device, commonly involving probing, decrypting, and modifying the chip's operation. In addition, such attacks often include the insertion of hardware trojans or rogue components[29], from which the attacker can launch another attack by gaining unauthorized access to the MRAs, possibly even gaining full access to the hardware[30]. Hardware attacks can affect the motor or battery's performance, giving incorrect instructions or even causing damage to the MRA's components [31].

Side-channel attacks exploit information leakage during device operation. These attacks analyze physical characteristics such as power consumption, electromagnetic emissions, or execution time to extract sensitive information such as cryptographic keys. For side-channel attacks, they are usually performed by passive attacks or active attacks:

- Passive attacks are performed by power analysis or electromagnetic analysis. In the power analysis method, the MRA's power consumption depends on the processed data and the actions taken will be collected to infer sensitive information[32]. Cryptographic modules perform encryption or decryption; secret keys can be discovered from the side-channel information. Electromagnetic analysis attacks are typically performed by measuring and analyzing the electromagnetic radiation of the device[33]. Detailed measurements and analysis are performed to detect patterns in the electromagnetic radiation;

- Active attacks are typically performed by Clock/power fault injection; Electromagnetic fault injection (EMFI) using high-energy, short-wavelength (nanosecond range) electromagnetic pulses to change the state of data memory cells; Injecting faults using a focused laser beam to change the state of a transistor on a microcontroller; Changing the operating temperature of the MRA leading to abnormal robot behavior, even causing errors in the memory cells.

3.2. Cyber attacks

Cyber-attacks in MRA are performed by remote connection without direct access to the physical port, further expanding the attacker's modus operandi. Common attacks include eavesdropping, data interference, Man in the Middle (MITM) attacks, spoofing attacks, denial of service, etc[31].

- Jamming attacks disrupt communication between MRA and MRA and between MRA and users;
- Deauthentication attacks aim to temporarily, periodically or disable the ability of MRA devices to reconnect to users or even take control of MRA by gaining control;
- Eavesdropping and traffic analysis attacks target ongoing traffic between MRA and controller and retrieve important information of MRA. In fact, advanced eavesdropping can take the form of "clone and replay" attacks or data recovery through information-gathering processes;
- False data injection attacks by intercepting and modifying packet payloads[34] by injecting false data and information, making it impossible for the MRA to perform its operations correctly;
- Replay attacks replay old messages sent between the MRA and the user to disrupt the ongoing transmission channel and can compromise the location or routing table of devices in the system[35];
- Man-in-the-Middle attacks occur when an attacker is able to eavesdrop and intercept communications between two entities or MRAs, changing the information. Thereby controlling the information transmitted/received between legitimate entities[36];
- Denial of service attacks aim to prevent legitimate users from accessing MRA systems and devices by sending a large number of requests for the network to re-authenticate [37]. Common attacks include DDoS/DoS, volume-based attacks, protocol attacks, application layer attacks, black hole attacks, Zero-day DDoS attacks, etc[24].

3.3. Operating system/application software attacks

Operating system upgrades are performed over a network connection, as the firmware code is typically stored on flash memory[38]. On the other hand, since applications rely on running software programs to perform their tasks, software programs can be exposed to a variety of attacks including viruses, worms, trojans, buffer overflow attacks, and malware injection attacks[24].

- Worm attacks target MRA systems by exploiting vulnerabilities in network-connected devices before propagating and replicating themselves to infect other MRA devices or control systems[39];
- Ransomware attacks aim to encrypt all data associated with MRA systems, devices, and applications, as well as lock down backed-up data. Some of the attacks include: WannaCry (2017), GandCrab (2018), LockerGoga (2019), CovidLock (2020)[40];
- Trojans are often masquerading as a legitimate application. This attack can be linked to Botnets to conduct DDoS attacks. Many trojans include Storm Worm (2006), Zeus (2007), Plug X malware (2008), and Emotet (2018);
- Rootkit attacks allow attackers to gain administrator-level access with the ability to access information and data related to MRA and MRA systems;
- Botnet attacks can rely on malware to infect unprotected MRA devices. Botnets can also be linked to worms, ransomware, and trojans to conduct attacks against the privacy security of MRA systems and data. Some types of botnets include Methbot (2016), Mirai (2016) and Glupteba (2019);

- In addition, other attacks against MRA system application software include: Password cracking attacks aimed at authenticating MRA systems[41]; Attacks via malicious MRA application software (malicious third-party applications disguised as legitimate applications) to spy on users or to gain control and hijack robots[42]; Malicious code injection (MCI) attacks or remote code execution (RCE) attacks via software vulnerabilities[43]. Application software attacks of Linux or ROS-based operating systems[41], [44].

4. Security Protection Schemes in MRA systems

Security not only protects data and personal information but also prevents remote attacks, protects control software, and ensures the physical safety of MRA (Table 2).

Table 2. Evaluation of security criteria in MRA systems

Criteria	Hardware protection	Network Security	Operating System/ Application Software Security
Interest Level	High	High	High
Reliability	High	Medium	High
Implementability	Medium	High	Low
Compatibility	High	High	Low - Average
Cost	High	Low - Average	Medium
Management, Maintenance	Low	Medium	High
Human Resources	Medium	High	High
Technology Used	Physical locks, shielding control techniques.	Firewalls, encryption.	Antivirus software, operating system updates.

In the encryption methods for MRA security discussed in studies[45]–[50], the selected criteria for comparison include reliability, cost, complexity, deployability, scalability, and security features. These criteria play a crucial role in creating an overall and effective security design for MRA systems. Each criterion functions independently and must be closely interconnected to enhance MRA security effectiveness against current threats and provide a solid foundation for future security solutions.

In Table 2, the encryption methods compiled from the literature include AES, ECC, KATAN, KLEIN, mCrypton, Piccolo, and PRESENT. Based on understanding the structure, algorithms, and applicability of security in MRA systems, each encryption method will be evaluated and categorized according to the established criteria. For example, the AES encryption method can be rated as "High" in terms of reliability because AES has been widely used in robotics and has demonstrated its security through numerous studies. The comparison results show that each encryption method has its strengths and weaknesses, making it suitable for specific MRA security applications.

4.1. Hardware Protection

Hardware (physical) protection ensures the overall integrity of MRA systems, as unauthorized physical access can cause damage such as cyber-attacks. Methods for protecting the hardware of MRA are proposed to prevent invasive attacks and side-channel attacks (see Fig. 5).

For invasive attacks, anti-tampering techniques include anti-tampering, tamper detection, tamper feedback, etc. In [51], Bilhan et al. describe a method to measure the resistance change of a conductive grid covering sensitive hardware to protect the hardware.

A random (non-replicable) signal is transmitted through the conductive grid without reaching the receiver. The processor determines the system's response to the detected manipulation. This method can detect attacks using high-frequency EM signals. In Cherukuri et al's [52] study, tampering detection is performed by measuring the change in the resistance difference of the conductive grid. This method is implemented using an amplifier or voltage comparator with multiple inputs.

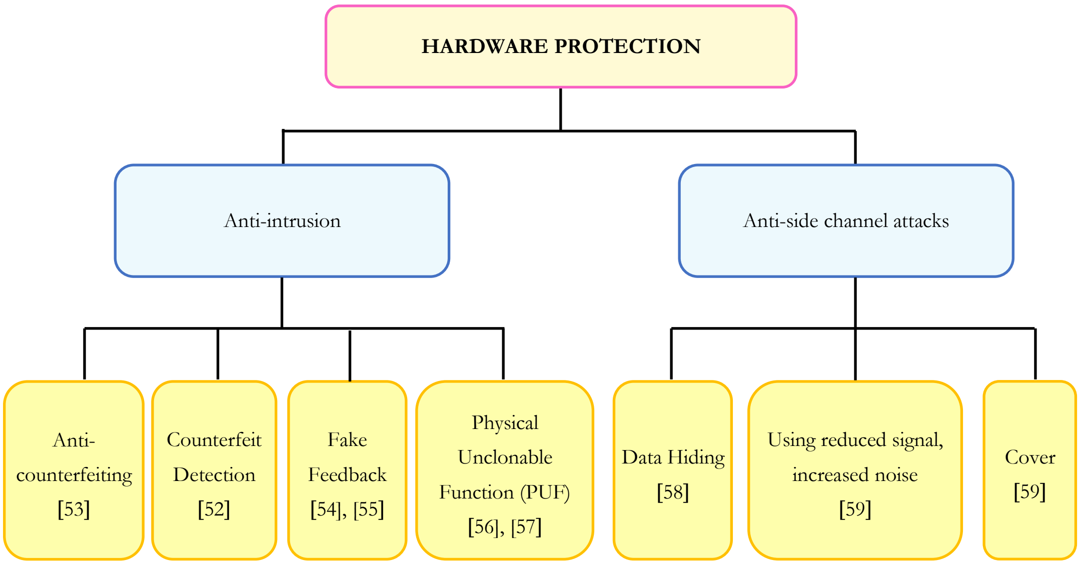
HARDWARE PROTECTION
Anti-intrusion
Anti-side channel attacks
Anti-counterfeiting [53]
Counterfeit Detection [52]
Fake Feedback [54], [55]
Physical Unclonable Function (PUF) [56], [57]
Data Hiding [58]
Using reduced signal, increased noise [59]
Cover [59]

Figure 5. Hardware protection layer

Sion et al.[53] proposed a system with anti-tampering properties and a decoupled architecture. With a device containing sensitive data comprising an enclosure, a cryptographic module, a tamper detection sensor, memory, and an internal IPM detachable configured to provide a link between the tamper protection system and an electronic component within the enclosure, the device is configured to permit replacement of the information processing module or cryptographic module. The disclosure further provides a tamper protection system configured to enable design reuse when interconnected with different modules. In the work of Busby et al.[54] a method of protection against reverse engineering is described. The disclosure describes techniques for hiding conductive connections on a circuit board and using dummy connections that make the circuit layout difficult to determine. These dummy connections are readily visible through X-ray analysis but do not provide a conductive connection between circuit components. In the study of Razaghi [55] described a method of detecting tampering by integrating a conductive grid into the device housing. The tamper detection circuit also detects tampering by monitoring the voltage at the reference points. This method allows for detecting tampering if a short circuit occurs.

Methods based on PUF (Physically Unclonable Functions) to prevent physical tampering have also been developed and mentioned in various studies. A system for tamper detection includes a device in a telecommunications network and an apparatus secured to the device, the apparatus including: a fastener, an adhesive secured to the fastener, and an electric circuit con-figured to measure a property value, wherein the property value is stored on the device, wherein the apparatus is configured to: measure a reference property value of the circuit; store the reference property value of the circuit in the device; measure a current property value of the circuit; compare the reference property value of the circuit to the current property value of the circuit; and initiate an alarm at the device if the current property value does not match the reference property value [56]. Falk et al. [57] proposed a distributed memory protection method by continuously recording new values and checking previously recorded values. The tamper protection device includes a carrier and at least one electronic memory, wherein the at least one electronic memory is disposed of in at least one partial area on the carrier, and the at least one electronic memory stores at least one definable security information item. The at least one electronic memory is configured to modify the pre definable security information item in the event of at least partial damage to the tamper protection device. The disclosure further relates to a method for producing a field device with a tamper protection device, to a field device comprising a tamper protection device, to a tamper protection system, and to use a tamper protection device.

Another solution to protect the hardware of MRA is proposed by Mazzeo et al. [60] with the solution combined with the ROS operating system, the hardware-assisted Trusted-ROS (TROS) to protect the data managed by ROS, which would otherwise reside in the robot's memory unencrypted.

Table 3. Comparison of hardware protection solutions for MRA systems

Method	Complexity	Estimated price	Protection	Applicability	Battery required	Memory required
Bilhan [51]	Low	Low	Low	Medium	Medium	Medium
Cherukuri[52]	Low/Average	Low	Low/ Average	Medium	Medium	Medium
Sion[53]	High	High	High	Medium	Medium	Medium
Busby [54]	Medium/high	Medium	Low	Medium/high	Low	Low
Razaghi [55]	Low/ Average	Low/ Average	Low	Medium	Medium	Medium
Hasan [56]	Low	Low	Low	High	Low	High
Falk[57]	Medium/high	Medium/high	Medium	Low	Low	High

For side-channel attacks, the proposed techniques are based on data obfuscation to hide sensitive information, using reduced signal amplitude and injecting noise into the power analysis data (power analysis protection) [58], [59]. These mechanisms provide tamper resistance by increasing the number of samples required for a power analysis attack, which generates a large number of samples that reduce the feasibility of attacks. Active shielding techniques and methods that disrupt the chip layout and allow components on the chip to be distributed over the entire surface of the chip.

Hardware protection in MRA systems prevents unauthorized physical access from the outside. However, physical security methods often require high costs (purchase, installation, and maintenance of security devices), and maintenance, updating, and upgrading of hardware protection measures also require costs and resources (Table 3).

4.2. Network Security

The network security solutions of the MRA system are described in Fig. 6.

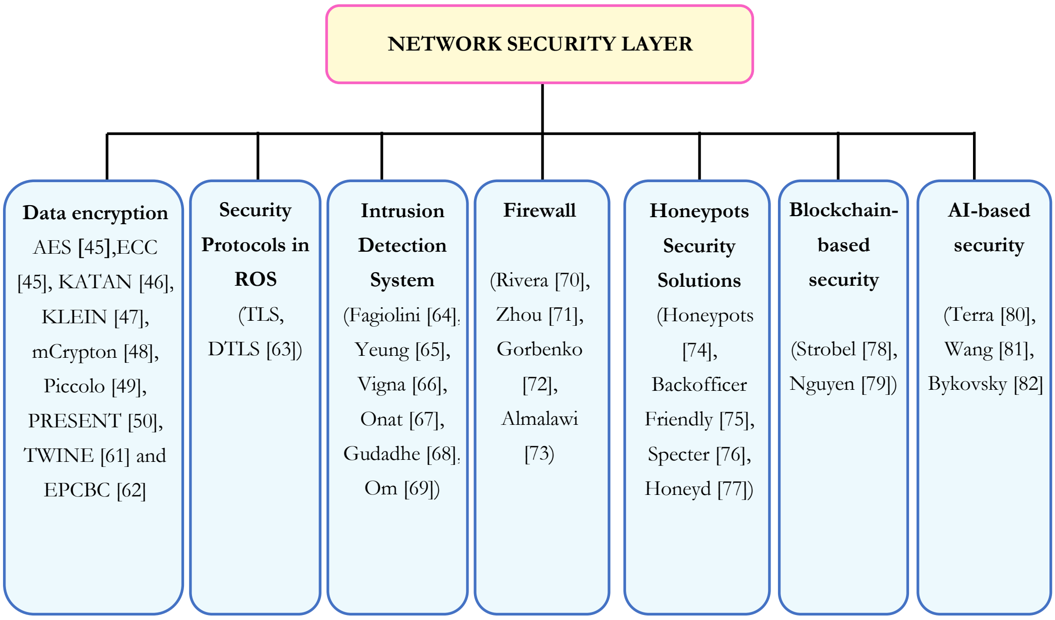
NETWORK SECURITY LAYER
Data encryption AES [45],ECC [45], KATAN [46], KLEIN [47], mCrypton [48], Piccolo [49], PRESENT [50], TWINE [61] and EPCBC [62]
Security Protocols in ROS (TLS, DTLS [63])
Intrusion Detection System (Fagiolini [64]. Yeung [65], Vigna [66], Onat [67], Gudadhe [68]. Om [69])
Firewall (Rivera [70], Zhou [71], Gorbenko [72], Almalawi [73)
Honeypots Security Solutions (Honeypots [74], Backofficer Friendly [75], Specter [76], Honeyd [77])
Blockchain-based security (Strobel [78], Nguyen [79])
AI-based security (Terra [80], Wang [81], Bykovsky [82]

Figure 5. Network security layer

4.2.1. Encryption protocols and solutions

Cryptographic protocols used for user authentication or MRA typically use cryptographic algorithms. Designing an efficient cryptographic algorithm will help reduce latency, communication overhead, and required resources. Therefore, improving key management techniques and ROS management layer security in MRA systems can help achieve better security. Symmetric cryptographic protocols are more suitable because they are lighter than asymmetric cryptography, especially with the Advanced Encryption Standard (AES), which is faster than the Elliptic Curve Cryptography (ECC) standard [45]. Furthermore, symmetric protocols are more energy efficient, especially when using optimized AES block ciphers. Some popular crypto-graphic methods include KATAN [46], KLEIN [47], mCryptton[48], Piccolo[49], PRESENT[50], TWINE[61], and EPCBC[62].

Breiling[83] presented a solution to secure the communication channels of the MRA operating system (ROS) using encryption to mitigate DoS attacks. In [63], Hussein introduced the transport layer security (TLS) and transport layer security (DTLS) methods in the ROS core to secure the communication of MRA.

Hussaini proposed a security model to enhance the level of network security [84] along with the optimal key selection. First, the secret information is grouped using the K-Mediod group algorithm based on the data distance measure. Then, the grouped data is encrypted using Blowfish Encryption (BE) and stored in the cloud to improve network security. Elfaki [85] presented a Cloud-Based framework for enhancing the intelligence and autonomy of MRA system, enabling flexible and compliant feedback control for MRA's physical interactions with humans. This solution is tested on various MRAs to minimize network latency. Another encryption and authentication mechanism is also presented by Chavhan [86] to implement access to MRA services hosted on a secure server. The proposed solution uses the Kerberos module and the Elliptic Curve Integrated Encryption Scheme (ECIES) to encrypt data.

Encryption protocols and solutions play an important role in ensuring the security of MRA systems, and security in MRA networks. The choice of encryption solutions depends on many factors, especially the MRA's computing, processing and resource capabilities. In this study, some management protocols and encryption solutions are proposed, the analysis and comparison results are presented as in Table 4.

Table 4. Comparison and evaluation of encryption methods for MRA systems

Encryption Method	Type	Key size (bits)	Trust level	Cost	Complexity	Implementation	Scalability	Features
AES [45]	Symmetric Key	128, 192, 256	High	High	Medium	High	High	Data, Network, Software Security
ECC [45]	Public Key	-	High	Medium	High	Medium	High	Network, Communication Security, Embedded Systems
KATAN [46]	Light Symmetric Key	80	Medium	Low	Low	Medium	Medium	Embedded Systems with Limited Resources
KLEIN[47]	Light Symmetric Key	64, 80, 96	Medium	Low	Low	Medium	Medium	Embedded Systems with Limited Resources
mCrypton [48]	Light Symmetric Key	96	Medium	Low	Medium	Medium	Medium	Embedded Systems with Limited Resources
Piccolo [49]	Light Symmetric Key	80, 128	Medium	Low	Low	High	Medium	Embedded Systems with Limited Resources
PRESENT [50]	Light Symmetric Key	80, 128	Medium	Low	Low	High	Medium	Embedded Systems with Limited Resources
AES [45]	Light Symmetric Key	80, 128	Medium	Low	Medium	Medium	Medium	Embedded Systems with Limited Resources

4.2.2. Intrusion Detection Systems and Firewalls

Intrusion detection systems provide a level of protection and response to known or unknown threats around the MRA domain. Network-level MRA protection can be implemented early by detecting anomalies and intrusions. Machine Learning (ML) and statistical methods are techniques used to secure MRA at the network level. In addition, Bayesian network-based techniques can also be used to detect security attacks against MRA[87].

Fagiolini [64] proposed a synthesis technique used to build a distributed IDS to secure a multi-agent MRA layer. This IDS model includes a decentralized monitoring mechanism and a consensus mechanism. Another IDS model was implemented by Yeung [65] using the PMRAzen window estimator with Gaussian multiplication to build an intrusion detection system using only regular data. Vigna [66] proposed a WebSTAT solution, a new intrusion detection system based on analyzing web requests and searching for evidence of malicious behavior. WebSTAT showed effectiveness with a low false positive rate. An anomaly-based IDS solution was proposed by Nguyen [67] using a binary logistic regression (BLR) statistical tool to classify local sensor activities and detect malicious behavior of MRA. Another IDS approach was implemented by Gudadhe [68] using enhanced decision tree. The results were compared with other algorithms such as Naive Bayes, k-Nearest Neighbor (kNN) showing superiority. Om [69] proposed a hybrid IDS solution to overcome the false alarm rate when detecting anomalies. This hybrid IDS combines k-Means, kNN, and Naive Bayes to detect anomalies.

Develop an intrusion detection system to detect anomalous behavior and prevent malicious intrusions. The comparison and evaluation results of network security methods in MRA are presented in Table 5.

Rivera [70] presented the ROS-Immunity solution that allows ROS users to harden the system against attacks with low cost, automatic rule generation, and distributed defense with firewalls. Zhou [71] proposed a new overall system based on a modified adaptive boosting algorithm with area under the curve (M-AdaBoost-A) to detect network intrusions more effectively. Additionally, some other studies by Gorbenko [72] proposed an IDS model to detect zero-day phishing attacks. Almalawi [73] proposed an additional anomaly threshold to identify any anomalous deviations and improve the performance of unsupervised IDS methods.

Table 5. Comparison and evaluation of IDS approaches in network security

IDS method	Reliability	Cost	Complexity	Imple-mentablity	Scalability	Ability to detect new attacks	Features
Fagiolini [64]	High	High	High	Medium	High	High	Distributed Networks, Parallel Processing
Yeung [65]	High	Medium	Medium	High	Low	Medium	Statistical Analytics, Machine Learning
Vigna [66]	Medium	Medium	Medium	High	High	Low	Web Security, Traffic Analytics
Nguyen [67]	High	High	High	High	Medium	High	Behavioral Analytics
Gudadhe [68]	High	Medium	High	Medium	High	High	Machine Learning
Om [69]	High	Medium	High	Medium	Medium	High	Network Traffic Analytics, Network Monitoring

4.2.3. Honeypots Security Solutions

Honeypots are tools that can be used as a standalone system to complement security technologies. Honeypots can be used in conjunction with IDSs and firewalls to detect, prevent, and respond to attacks. Sacrificing an unnecessary or unwanted system to a decoy host allows the system to trap attackers[88]. Some honeypot system solutions are used to improve MRA's security effectiveness. Irvene [74] proposed the HoneyBot solution based on a hybrid interactive honeypot designed specifically for MRA systems. HoneyBot can accurately deceive intelligent attackers by relying on HoneyPhy and traditional honeypot techniques. Based on a freely distributed lightweight honeypot, Hecker [75] proposed Backofficer Friendly, which ensures accurate extraction of log information, sends alerts to identify attacks clearly, and can also respond with fake responses whenever a user connects to HTTP, FTP, and Telnet ports. Another honeypot-based solution is Spectre [76], which can simulate about 13 different operating systems (including Windows and Linux) and provide about 14 different network services and traps. This provides the opportunity to collect information about attackers actively. Another honeypot approach called "Honeyd" [77] uses a mixed defense strategy to keep the attacker's attack success rate low.

The advantage of these approaches on Honeypots is the ability to reduce the false positive and false negative rates; while ensuring high dynamism and flexibility to respond to various types of attacks. The comparison results of honeypot-based security solutions are presented in Table 6.

Table 6. Comparison of evaluation of Honeypots approaches

Honeypots methods	Reliablity	Cost	Complexity	Implementablity	Scalability
Honeypots [74]	Medium	Low	Medium	Medium	Medium
Backofficer Friendly[75]	Medium	Low	Low	High	Low
Specter [76]	Medium	Low	Low	High	Low
Honeyd [77]	High	Medium	High	High	High

4.2.4. Some other network security solutions

Blockchain technology provides an effective solution to the challenges faced by MRA systems. This technique establishes a distributed network capable of performing peer-to-peer network operations, distributed file distribution, and independent coordinating devices that allow the system to monitor multiple nodes in the network. Transactions between nodes in the network are conducted cooperatively, improving security and reliability. Studies have performed cryptanalytic testing on their solution using the Proverif tool, showing the ability of the system to overcome various security threats and attacks. Strobel [78] compares the consensus protocols used in swarm MRA. However, the presence of malfunctioning and malicious robots can make it impossible to reach consensus using classical consensus protocols. With the ARGoS-blockchain solution, it is possible to provide secure coordination for the MRA swarm through blockchain-based smart contracts. Nguyen [79] proposed specific secure nodes in the network based on integrated blockchain security technology to mitigate hacker attacks from outside the network. Authentication is performed by public blockchain and private blockchain. This method identifies the most secure nodes in the network system.

Some advantages of blockchain technology when integrated with the MRA network system: allows peer-to-peer communication, allowing faster information transmission/ reception (instead of communication through a centralized server); data information is tamper-proof, ensuring reliability (because transaction history is stored in a distributed ledger); self-executing processes through smart contracts and a distributed file distribution system (eliminating the dependence on a single centralized server).

Selecting AI-based solutions to ensure a highly secure MRA environment with high accuracy and less cost. Terra [80] deployed fuzzy logic system (FLS) and reinforcement learning (RL) to build risk mitigation modules for user-MRA collaboration scenarios. Wang presented the main security threats to autonomous mobile MRA and their mitigations [81], implemented a directed fuzzing method, and designed RoboFuzz to study the critical environmental parameters affecting the state transition of MRA and inject the robot control program with reasonable but harmful sensor values to compromise MRA. In a study by Nguyen [82] further provides secret encryption, data aggregation, data protection, and communication for network addressing and target control of MRA devices. The method implements Minimized Multi-Valued Logic (MVL) functions to analyze aggregated objects. To ensure full utilization of MVL, a heterogeneous network architecture is also presented using three levels of distributed AI as logic models for discrete multi-valued, Boolean, and fuzzy logic.

The application of artificial intelligence in MRA system security brings many benefits, such as the speed of detection through abnormal behavior and the ability to respond quickly to threats to minimize losses. The ability to continuously learn and improve to detect new threats, enhance analysis and monitoring capabilities, and optimize resources and costs. However, the cost of implementing AI in MRA systems is a challenge that needs to be considered during the design process.

4.3. Operating system/application software security

The operating system is the system software that manages the hardware and application software, providing services for the applications to operate. The robot's application software is the program developed to perform specific tasks. Some methods to improve the security of operating systems and software are described in Fig. 7.

4.3.1. ROS Operating System Security

Most MRAs equipped with operating systems such as Linux or ROS are exposed to various vulnerabilities. Some proposed solutions to overcome ROS are as follows:

ROS-Immunity solution consists of a set of tools proposed [89] by Rivera, aiming to develop a modular security framework for ROS, providing internal system protection, external system verification, and automatic security vulnerability detection. Next, the extended version of ROS-FM is proposed[90] with Berkely packet filter and fast data path to build a network monitoring framework for ROS. Also in a study by Rivera [91], ROS-Defender proposed integrating a security event management system, intrusion prevention system, and firewall. A security framework supporting secure communication between autonomous MRA systems such as TurtleBots is proposed by Chauhan [92] to ensure confidentiality of communication, integrity of information, secure availability of data, and access to services. Data distribution service standard proposals are implemented by Fernandez [93] as a middleware to ensure security and QoS policies, analyzing the costs associated with security and QoS settings.

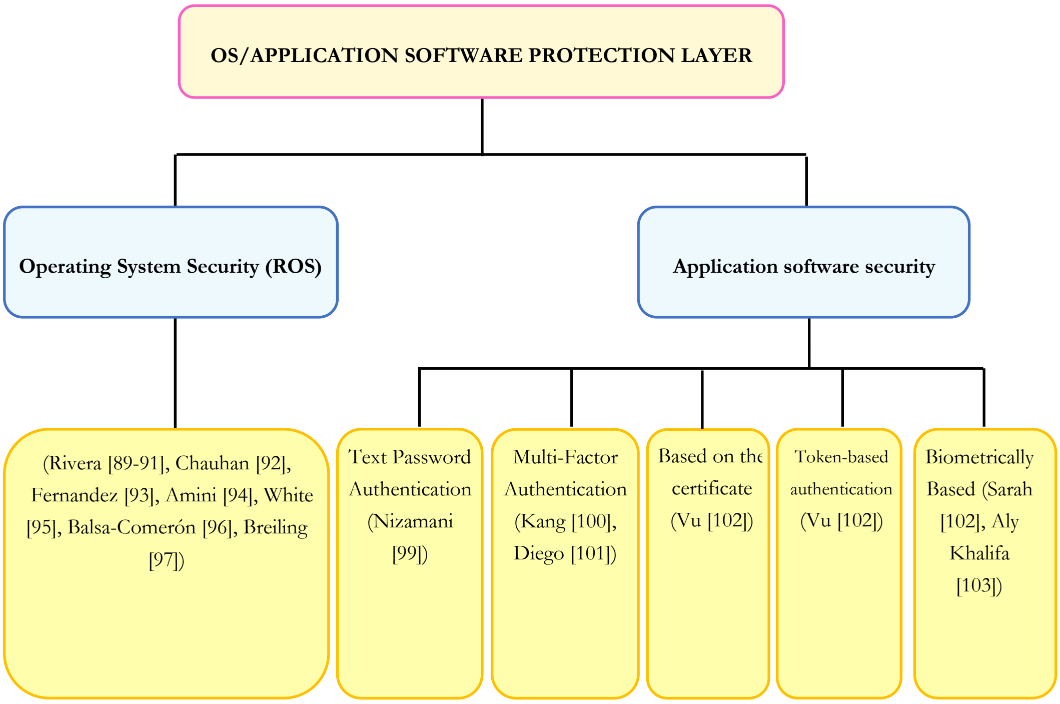
OS/APPLICATION SOFTWARE PROTECTION LAYER
Operating System Security (ROS)
Application software security
(Rivera [89-91], Chauhan [92], Fernandez [93], Amini [94], White [95], Balsa-Comerón [96], Breiling [97])
Text Password Authentication (Nizamani [99])
Multi-Factor Authentication (Kang [100], Diego [101])
Based on the certificate (Vu [102])
Token-based authentication (Vu [102])
Biometrically Based (Sarah [102], Aly Khalifa [103])

Figure 7. Operating system/application software protection layer

Some solutions to secure ROS based on the use of cryptographic techniques to secure communications between ROS nodes are as follows:

A study proposed by White [95] is SROS1 with ROS1 APIs to support encryption and security precautions such as: over-the-wire encryption, zero access control, and record handling using Linux security modules to enhance resource access. A solution based on both encryption and ROSRV was proposed by Balsa-Comerón[96], in which the Advanced Cryptographic Standard algorithm was used in conjunction with a framework to define semantic rules for ROS messages. DoS detection rules were introduced to counter the attacks tested on a real-time positioning system. A cryptographically-based distributed infrastructure is deployed to maintain the MRA workflow proposed by Breiling [97], a separate entity will provide a digital signature, which can be verified by the MRA before executing the task.

4.3.2. Application software security

MRA's application software must undergo a security testing phase to identify security vulnerabilities and minimize and prevent exploitation and attacks. In addition, access control methods [98] aim to establish clear authorization mechanisms for authorized users to access software parts, especially by limiting access to essential programs and sensitive data.

A text-based user authentication technique proposed by Nizamani[99] enhances security by changing the password input mechanism and adding a password conversion layer. Alphanumeric password characters are represented by random decimal values to resist online security attacks such as keyloggers.

Table 7. Applied authentication and analysis mechanisms.

Authentication Mechanism		**Reliability**	**Cost**	**Complexity**	**Implement ability**	**Scalability**	**Features**
Password		Low/ Average	Low	Low	High	Medium	Depends on the strength of the password
Multifactor		Medium/ High	Medium/ High	Medium/ High	Medium	High	Depends on the integration factors
Certificate		High	Low	Medium	Medium	Medium	Requirements on the management system
Token		High	Medium/ High	Medium	High	High	Depends on each type of code
Biometrics	Face	High	Medium	Medium/ High	Medium	Depends on the environmental conditions	Dependent on environmental conditions
	Fingerprint	High	Medium/ High	Medium/ High	Medium/ High	Device and software requirements	Equipment and software requirements
	Voice	High	Medium	Medium/ High	Medium/ High	Device and software requirements	Equipment and software requirements
	Retina	High	High	High	Low/ Average	Device and software requirements	Equipment and software requirements
	ECG	High	High	High	Low	Device and software requirements	Equipment and software requirements

Multifactor authentication techniques based on different factors can be combined to enhance security. Kang's study proposes the method of combining face authentication and password[100]. In addition, Diego's study [101] proposed a multifactor authentication method that requires the user to identify specific images in a set of randomly selected images, and then the user is required to establish a pre-configured relationship between two specific images to complete the authentication.

Certificate-based authentication methods use digital certificates with keys (public and private)[98] to authenticate the user or system that holds this certificate. In addition, another technique, token-based authentication, is used to allow the user to enter their credentials into the server, and the server provides a unique encrypted random string (token) that the system recognizes [98]. However, anyone with this token can compromise the system, and this method is also vulnerable to various types of password-based attacks.

Biometric-based authentication uses the user's biometric data to identify the person uniquely. Sarah proposed an offline authentication method that uses biometric data to authenticate users on a mobile robot[102]. This method uses a smart card to authenticate authorized people on a mobile robot. The smart card is equipped with a fingerprint reader, and only valid users can pass the authentication. In order to enhance human-robot interactions, Aly Khalifa [103] proposed a lightweight CNN-based authentication solution for all stages of face recognition, including face detection, alignment, and feature extraction, to achieve higher accuracy. In addition, biometric-based authentication methods can use factors such as voice, retina, gait, heart signals, and electroencephalogram[98], but the disadvantage of these methods is the requirement for the stability of the biometric factor (stable parameters, normal body, etc.). The positive aspect of biometric authentication is the ability to combine multiple factors to enhance security or be combined with technologies such as AI to enhance the accuracy and reliability of the authentication process. Different techniques for user authentication are compared in Table 7 to consider the feasibility of applying authentication mechanisms.

5. Some challenges and future research directions

While the proposed solutions have addressed some urgent issues regarding data security, user information protection, and defenses against attacks on MRA operations, several limitations remain in the research. These include:

- Lack of empirical deployment data: Many studies are based on theoretical analysis or simulations, which may reduce the feasibility of comprehensive security solutions for MRA systems.
- Compatibility and integration of security solutions: The studies do not address the compatibility between various security solutions and their simultaneous integration, likely due to the lack of experimental data.
- Looking ahead, several challenges must be addressed:
- Privacy and data protection in multimodal MRA systems: Ensuring privacy and protecting user data is challenging, as there are multiple alternative interaction channels (e.g., audio, video, gesture actions) that could be exploited to access personal information. These channels often have few or no security mechanisms.
- Lightweight Intrusion Detection Systems (IDS): There is a need to develop efficient, lightweight IDS using anomaly-based techniques as part of detecting unknown attacks in MRA contexts. These lightweight IDS techniques can enable quick decision-making in resource-constrained environments or real-time applications like MRA. Therefore, the focus should be on designing effective anomaly classifiers to balance performance and detection accuracy.
- Authentication processes for MRA systems: These should aim for the highest security level by using mutual multifactor authentication programs. This would reduce the risk of unauthorized access to MRA systems or users. Lightweight cryptographic algorithms and protocols at the network or physical layer are essential to ensure secure wireless com-munication with minimal latency and resource usage. Furthermore, non-cryptographic solutions, such as lightweight intrusion detection or prevention systems, should be designed for better protection of MRA applications.

6. Conclusions

This article classifies firstly MRA by applications and fields of operation. Security issues for the MRA system are analyzed and determined in details with the security requirements and constraints. All the attacks, threats, and security vulnerabilities are also classified in aspects such as: hardware, network system, operating system/application software. The authors compare and evaluate corresponding security methods to improve the security capabilities of MRA. Most of challenging issues in MRA system security are considered including open research directions in the future. In the future work, the authors continue to develop new security methods to respond to the changing threat landscape, and to focus on adaptive, model-based, resource-optimized strategies that would be the key to secure and effective MRA systems.

Author Contributions: Conceptualization: Long Q. Dinh and Minh T. Nguyen; methodology: Long Q. Dinh; software: Dung T. Nguyen and Minh T. Nguyen.; validation: Thang C. Vu, Tao V. Nguyen; formal analysis: Tao V. Nguyen, Dung T. Nguyen; investigation: Minh T. Nguyen; resources: Dung T. Nguyen; data curation: Thang C. Vu.; writing—original draft preparation: Long Q. Dinh; writing—review and editing: Minh T. Nguyen; visualization: Thang C. Vu, Dung T. Nguyen; supervision: Thang C. Vu; project administration: Tao V. Nguyen; funding acquisi-tion: Minh T. Nguyen.

Funding: This research received no external funding.

Data Availability Statement: Data can be shared based on any requests to the corresponding authors.

Acknowledgments: The authors would like to thank Thai Nguyen University of Technology, Thai Nguyen University, Ministry of Education and Training (Project B2023-TNA-16), Viet Nam for the support.

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

References

[1] M. T. Nguyen and H. R. Boveiri, "Energy-efficient sensing in robotic networks," *Measurement*, vol. 158, p. 107708, Jul. 2020, doi: 10.1016/j.measurement.2020.107708.

[2] E. Fosch-Villaronga and T. Mahler, "Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots," *Comput. Law Secur. Rev.*, vol. 41, p. 105528, Jul. 2021, doi: 10.1016/j.clsr.2021.105528.

[3] M. D. Nguyen, M. T. Nguyen, T. C. Vu, T. M. Ta, Q. A. Tran, and D. T. Nguyen, "A Comprehensive Study on Applications of Blockchain in Wireless Sensor Networks for Security Purposes," *J. Comput. Theor. Appl.*, vol. 2, no. 1, pp. 102–117, Jul. 2024, doi: 10.62411/jcta.10486.

[4] S. Jain and R. Doriya, "Security Issues and Solutions in Cloud Robotics: A Survey," in *Next Generation Computing Technologies on Computational Intelligence*, Springer Singapore, 2019, pp. 64–76. doi: 10.1007/978-981-15-1718-1_6.

[5] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 1–11, 2014, doi: 10.1109/TITS.2014.2342271.

[6] A. Khalid, P. Kirisci, Z. H. Khan, Z. Ghrairi, K.-D. Thoben, and J. Pannek, "Security framework for industrial collaborative robotic cyber-physical systems," *Comput. Ind.*, vol. 97, pp. 132–145, May 2018, doi: 10.1016/j.compind.2018.02.009.

[7] R. Doczi *et al.*, "Increasing ROS 1.x communication security for medical surgery robot," in *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Oct. 2016, pp. 004444–004449. doi: 10.1109/SMC.2016.7844931.

[8] M. Staffa, G. Mazzeo, and L. Sgaglione, "Hardening ROS via Hardware-assisted Trusted Execution Environment," in *2018 27th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN)*, Aug. 2018, pp. 491–494. doi: 10.1109/RO-MAN.2018.8525696.

[9] M. Pogliani, D. Quarta, M. Polino, M. Vittone, F. Maggi, and S. Zanero, "Security of controlled manufacturing systems in the connected factory: the case of industrial robots," *J. Comput. Virol. Hacking Tech.*, vol. 15, no. 3, pp. 161–175, Sep. 2019, doi: 10.1007/s11416-019-00329-8.

[10] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things*, vol. 11, p. 100218, Sep. 2020, doi: 10.1016/j.iot.2020.100218.

[11] M. T. Nguyen, H. M. La, and K. A. Teague, "Compressive and collaborative mobile sensing for scalar field mapping in robotic networks," in *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sep. 2015, pp. 873–880. doi: 10.1109/ALLERTON.2015.7447098.

[12] D. L. T. Tran, H. T. Do, H. T. Tran, T. Hoang, and M. T. Nguyen, "A Design and Implement of Fuzzy Controller for Taking-off and Landing for Unmanned Aerial Vehicles," in *Advances in Engineering Research and Application*, 2023, pp. 13–22. doi: 10.1007/978-3-031-22200-9_2.

[13] H. T. Do, H. T. Hua, H. T. T. Nguyen, M. T. Nguyen, and H. T. Tran, "Cooperative Tracking Framework for Multiple Unmanned Aerial Vehicles (UAVs)," in *Advances in Engineering Research and Application*, 2022, pp. 276–285. doi: 10.1007/978-3-030-92574-1_29.

[14] V. C. Thanh, N. N. A. Quan, T. Le Thang Dong, T. T. Hoang, and M. T. Nguyen, "Fusion of Inertial and Magnetic Sensors for Autonomous Vehicle Navigation and Freight in Distinctive Environment," in *Advances in Engineering Research and Application*, 2022, pp. 431–439. doi: 10.1007/978-3-030-92574-1_45.

[15] A. Q. Pham, H. M. La, K. T. La, and M. T. Nguyen, "A Magnetic Wheeled Robot for Steel Bridge Inspection," in *Advances in Engineering Research and Application*, 2020, pp. 11–17. doi: 10.1007/978-3-030-37497-6_2.

[16] R. A. Beasley, "Medical Robots: Current Systems and Research Directions," *J. Robot.*, vol. 2012, pp. 1–14, 2012, doi: 10.1155/2012/401613.

[17] H. T. Tran, D. L. T. Tran, and M. T. Nguyen, "Design of a robotic system to assist in the treatment of severe COVID‐19 patients," *Adv. Control Appl.*, vol. 6, no. 1, Mar. 2024, doi: 10.1002/adc2.193.

[18] H. T. Tran *et al.*, "Field programmable gate array based moving object tracking system for robot navigation," *Bull. Electr. Eng. Informatics*, vol. 12, no. 2, pp. 771–781, Apr. 2023, doi: 10.11591/eei.v12i2.4538.

[19] Đ. Q. Long, N. H. Công, D. P. Tuấn, N. Q. Vịnh, and N. T. Minh, "A Comprehensive Study of Mobile Robot Navigation and Obstacle Avoidance Schemes," *TNU J. Sci. Technol.*, vol. 228, no. 14, pp. 302–312, Nov. 2023, doi: 10.34238/tnu-jst.8978.

[20] M. T. Nguyen, K. A. Teague, and S. Bui, "Compressive wireless mobile sensing for data collection in sensor networks," in *2016 International Conference on Advanced Technologies for Communications (ATC)*, Oct. 2016, pp. 437–441. doi: 10.1109/ATC.2016.7764822.

[21] H. T. Tran *et al.*, "A novel design of a smart interactive guiding robot for busy airports," *Int. J. Smart Sens. Intell. Syst.*, vol. 15, no. 1, Jan. 2022, doi: 10.2478/ijssis-2022-0017.

[22] H. Noura, T. Hatoum, O. Salman, J.-P. Yaacoub, and A. Chehab, "LoRaWAN security survey: Issues, threats and possible mitigation techniques," *Internet of Things*, vol. 12, p. 100303, Dec. 2020, doi: 10.1016/j.iot.2020.100303.

[23] K. Ahmad Yousef, A. AlMajali, S. Ghalyon, W. Dweik, and B. Mohd, "Analyzing Cyber-Physical Threats on Robotic Platforms," *Sensors*, vol. 18, no. 5, p. 1643, May 2018, doi: 10.3390/s18051643.

[24] G. W. Clark, M. V. Doran, and T. R. Andel, "Cybersecurity issues in robotics," in *2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, Mar. 2017, pp. 1–5. doi: 10.1109/COGSIMA.2017.7929597.

[25] J. Block, "A laws of war review of contemporary land-based missile defence system 'Iron Dome,'" *Sci. Mil.*, vol. 45, no. 2, Dec. 2017, doi: 10.5787/45-2-1207.

[26] H. T. Tran, D. T. Tran, M. T. Nguyen, and T. C. Vu, “Intelligent mobile robot for contagious disease treatments in hospitals,” *MethodsX*, vol. 13, p. 102941, Dec. 2024, doi: 10.1016/j.mex.2024.102941.

[27] N. Campagna, V. Castiglia, R. Miceli, F. Viola, A. Busacca, and M. T. Nguyen, “Hybrid Energy Storage Systems: A Brief Overview,” in *Advances in Engineering Research and Application*, 2023, pp. 573–579. doi: 10.1007/978-3-031-22200-9_62.

[28] M. T. Nguyen, “An energy-efficient framework for multimedia data routing in Internet of Things (IoTs),” *EAI Endorsed Trans. Ind. Networks Intell. Syst.*, vol. 6, no. 19, p. 159120, Jun. 2019, doi: 10.4108/eai.13-6-2019.159120.

[29] M. Tehranipoor and F. Koushanfar, “A Survey of Hardware Trojan Taxonomy and Detection,” *IEEE Des. Test Comput.*, vol. 27, no. 1, pp. 10–25, Jan. 2010, doi: 10.1109/MDT.2010.7.

[30] X. Wang, T. Mal-Sarkar, A. Krishna, S. Narasimhan, and S. Bhunia, “Software exploitable hardware Trojans in embedded processor,” in *2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, Oct. 2012, pp. 55–58. doi: 10.1109/DFT.2012.6378199.

[31] S. Bhunia and M. M. Tehranipoor, Eds., *The Hardware Trojan War*. Cham: Springer International Publishing, 2018. doi: 10.1007/978-3-319-68511-3.

[32] M. Safta, P. Svasta, M. Dima, A. Marghescu, and M.-N. Costiuc, “Design and setup of Power Analysis attacks,” in *2016 IEEE 22nd International Symposium for Design and Technology in Electronic Packaging (SIITME)*, Oct. 2016, pp. 110–113. doi: 10.1109/SIITME.2016.7777256.

[33] Y. Hayashi *et al.*, “Efficient Evaluation of EM Radiation Associated With Information Leakage From Cryptographic Devices,” *IEEE Trans. Electromagn. Compat.*, vol. 55, no. 3, pp. 555–563, Jun. 2013, doi: 10.1109/TEMC.2012.2222890.

[34] M. T. Nguyen, C. V. Nguyen, and H. N. Nguyen, “Visualization-based monitoring in early warning systems with wireless sensor networks,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 31, no. 1, p. 281, Jul. 2023, doi: 10.11591/ijeecs.v31.i1.pp281-289.

[35] T. Vuong, A. Filippoupolitis, G. Loukas, and D. Gan, “Physical indicators of cyber attacks against a rescue robot,” in *2014 IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM WORKSHOPS)*, Mar. 2014, pp. 338–343. doi: 10.1109/PerComW.2014.6815228.

[36] R. E. Navas, H. Le Bouder, N. Cuppens, F. Cuppens, and G. Z. Papadopoulos, “Demo: Do Not Trust Your Neighbors! A Small IoT Platform Illustrating a Man-in-the-Middle Attack,” in *Ad-hoc, Mobile, and Wireless Networks*, 2018, pp. 120–125. doi: 10.1007/978-3-030-00247-3_11.

[37] P. Ferguson and D. Senie, “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing,” Jan. 1998. doi: 10.17487/rfc2267.

[38] H. Elmiligi, F. Gebali, and M. W. El-Kharashi, “Multi-dimensional analysis of embedded systems security,” *Microprocess. Microsyst.*, vol. 41, pp. 29–36, Mar. 2016, doi: 10.1016/j.micpro.2015.12.005.

[39] H. Kabir, M.-L. Tham, and Y. C. Chang, “Internet of robotic things for mobile robots: Concepts, technologies, challenges, applications, and future directions,” *Digit. Commun. Networks*, vol. 9, no. 6, pp. 1265–1290, Dec. 2023, doi: 10.1016/j.dcan.2023.05.006.

[40] M. Benmalek, “Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges,” *Internet Things Cyber-Physical Syst.*, vol. 4, pp. 186–202, 2024, doi: 10.1016/j.iotcps.2023.12.001.

[41] K. Cottrell, D. B. Bose, H. Shahriar, and A. Rahman, “An Empirical Study of Vulnerabilities in Robotics,” in *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, Jul. 2021, pp. 735–744. doi: 10.1109/COMPSAC51774.2021.00105.

[42] M. H. Khan and M. Ali Shah, “Survey on security threats of smartphones in Internet of Things,” in *2016 22nd International Conference on Automation and Computing (ICAC)*, Sep. 2016, pp. 560–566. doi: 10.1109/IConAC.2016.7604979.

[43] G. S. Kc, A. D. Keromytis, and V. Prevelakis, “Countering code-injection attacks with instruction-set randomization,” in *Proceedings of the 10th ACM conference on Computer and communications security*, Oct. 2003, pp. 272–280. doi: 10.1145/948109.948146.

[44] H. Shahbaznezhad, F. Kolini, and M. Rashidirad, “Employees’ Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter?,” *J. Comput. Inf. Syst.*, vol. 61, no. 6, pp. 539–550, Nov. 2021, doi: 10.1080/08874417.2020.1812134.

[45] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, “A Survey of Lightweight-Cryptography Implementations,” *IEEE Des. Test Comput.*, vol. 24, no. 6, pp. 522–533, Nov. 2007, doi: 10.1109/MDT.2007.178.

[46] C. De Cannière, O. Dunkelman, and M. Knežević, “KATAN and KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers,” in *Cryptographic Hardware and Embedded Systems - CHES 2009*, 2009, pp. 272–288. doi: 10.1007/978-3-642-04138-9_20.

[47] Z. Gong, S. Nikova, and Y. W. Law, “KLEIN: A New Family of Lightweight Block Ciphers,” in *RFID. Security and Privacy*, 2012, pp. 1–18. doi: 10.1007/978-3-642-25286-0_1.

[48] C. H. Lim and T. Korkishko, “mCrypton – A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors,” in *Information Security Applications*, 2006, pp. 243–258. doi: 10.1007/11604938_19.

[49] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, “Piccolo: An Ultra-Lightweight Blockcipher,” in *Cryptographic Hardware and Embedded Systems – CHES 2011*, 2011, pp. 342–357. doi: 10.1007/978-3-642-23951-9_23.

[50] A. Bogdanov *et al.*, “PRESENT: An Ultra-Lightweight Block Cipher,” in *Cryptographic Hardware and Embedded Systems - CHES 2007*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 450–466. doi: 10.1007/978-3-540-74735-2_31.

[51] E. Bilhan, R. Padakanti, and A. S. Mundra, “Tamper detection,” 2021 [Online]. Available: https://patents.justia.com/patent/11132659

[52] V. N. Cherukuri, S. Balakrishnan, and C. L. Rao, “Tamper detection techniques,” 2024 [Online]. Available: https://patents.justia.com/patent/11893146

[53] R. Sion, “Anti-tamper system,” 2018 [Online]. Available: https://patents.justia.com/patent/10007811

[54] J. A. Busby, J. R. Dangler, M. J. Fisher, and D. C. Long, “Tamper-respondent assembly with interconnect characteristic(s) obscuring circuit layout,” 2020 [Online]. Available: https://patents.justia.com/patent/10575398

[55] M. Razaghi, “Secure electronic circuitry with tamper detection,” 2023 [Online]. Available: https://patents.justia.com/patent/11681833

[56] A. R. Hasan and R. Rezaian, “Method and apparatus for tamper detection,” 2018 [Online]. Available: https://patents.justia.com/patent/9898909

[57] R. Falk, “Tamper protection device for protecting a field device against tampering,” 2018 [Online]. Available: https://patents.justia.com/patent/9858446

[58] S. Jog, V. Bhatnagar, T. Chinchore, D. Chinchalkar, and R. Chidrawar, “Design and Implementation of Stainless Steel EMI Compliant Enclosure for Wireless Communication System,” in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, Aug. 2018, pp. 1–5. doi: 10.1109/ICCUBEA.2018.8697398.

[59] I. Frieslaar and B. Irwin, “Developing an Electromagnetic Noise Generator to Protect a Raspberry PI from Side Channel Analysis,” *SAIEE Africa Res. J.*, vol. 109, no. 2, pp. 85–101, Jun. 2018, doi: 10.23919/SAIEE.2018.8531950.

[60] G. Mazzeo and M. Staffa, “TROS: Protecting Humanoids ROS from Privileged Attackers,” *Int. J. Soc. Robot.*, vol. 12, no. 3, pp. 827–841, Jul. 2020, doi: 10.1007/s12369-019-00581-4.

[61] T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi, “TWINE: A Lightweight Block Cipher for Multiple Platforms,” in *Selected Areas in Cryptography*, 2013, pp. 339–354. doi: 10.1007/978-3-642-35999-6_22.

[62] H. Yap, K. Khoo, A. Poschmann, and M. Henricksen, “EPCBC - A Block Cipher Suitable for Electronic Product Code Encryption,” in *Cryptology and Network Security*, 2011, pp. 76–97. doi: 10.1007/978-3-642-25513-7_7.

[63] A. Hussein, I. H. Elhajj, A. Chehab, and A. Kayssi, “Securing Diameter: Comparing TLS, DTLS, and IPSec,” in *2016 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*, Nov. 2016, pp. 1–8. doi: 10.1109/IMCET.2016.7777417.

[64] A. Fagiolini, M. Pellinacci, G. Valenti, G. Dini, and A. Bicchi, “Consensus-based Distributed Intrusion Detection for Multi-Robot Systems,” in *2008 IEEE International Conference on Robotics and Automation*, May 2008, pp. 120–127. doi: 10.1109/ROBOT.2008.4543196.

[65] Dit-Yan Yeung and C. Chow, “Parzen-window network intrusion detectors,” in *Object recognition supported by user interaction for service robots*, 2002, vol. 4, pp. 385–388. doi: 10.1109/ICPR.2002.1047476.

[66] G. Vigna, W. Robertson, V. Kher, and R. A. Kemmerer, “A stateful intrusion detection system for world-wide web servers,” in *19th Annual Computer Security Applications Conference, 2003. Proceedings.*, 2003, pp. 34–43. doi: 10.1109/CSAC.2003.1254308.

[67] M. T. Nguyen and K. A. Teague, “Neighborhood based data collection in Wireless Sensor Networks employing Compressive Sensing,” in *2014 International Conference on Advanced Technologies for Communications (ATC 2014)*, Oct. 2014, pp. 198–203. doi: 10.1109/ATC.2014.7043383.

[68] M. Gudadhe, P. Prasad, and L. Kapil Wankhade, “A new data mining based network Intrusion Detection model,” in *2010 International Conference on Computer and Communication Technology (ICCCT)*, Sep. 2010, pp. 731–735. doi: 10.1109/ICCCT.2010.5640375.

[69] H. Om and A. Kundu, “A hybrid system for reducing the false alarm rate of anomaly intrusion detection system,” in *2012 1st International Conference on Recent Advances in Information Technology (RAIT)*, Mar. 2012, pp. 131–136. doi: 10.1109/RAIT.2012.6194493.

[70] R. Sean, I. A. Ken, and others, “Ros-immunity: Integrated approach for the security of ros-enabled robotic systems,” *TechRciv*. 2023. doi: 10.36227/techrxiv.13013336.

[71] Y. Zhou, T. A. Mazzuchi, and S. Sarkani, “M-AdaBoost-A based ensemble system for network intrusion detection,” *Expert Syst. Appl.*, vol. 162, p. 113864, Dec. 2020, doi: 10.1016/j.eswa.2020.113864.

[72] A. Gorbenko and V. Popov, “Abnormal Behavioral Pattern Detection in Closed-Loop Robotic Systems for Zero-Day Deceptive Threats,” in *2020 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, May 2020, pp. 1–6. doi: 10.1109/ICIEAM48468.2020.9112054.

[73] A. Almalawi *et al.*, “Add-On Anomaly Threshold Technique for Improving Unsupervised Intrusion Detection on SCADA Data,” *Electronics*, vol. 9, no. 6, p. 1017, Jun. 2020, doi: 10.3390/electronics9061017.

[74] C. Irvene, D. Formby, S. Litchfield, and R. Beyah, “HoneyBot: A Honeypot for Robotic Systems,” *Proc. IEEE*, vol. 106, no. 1, pp. 61–70, Jan. 2018, doi: 10.1109/JPROC.2017.2748421.

[75] C. Hecker and B. Hay, “Automated Honeynet Deployment for Dynamic Network Environment,” in *2013 46th Hawaii International Conference on System Sciences*, Jan. 2013, pp. 4880–4889. doi: 10.1109/HICSS.2013.110.

[76] N. Ilg, P. Duplys, D. Sisejkovic, and M. Menth, “A survey of contemporary open-source honeypots, frameworks, and tools,” *J. Netw. Comput. Appl.*, vol. 220, p. 103737, Nov. 2023, doi: 10.1016/j.jnca.2023.103737.

[77] N. Bhagat and B. Arora, “Intrusion Detection Using Honeypots,” in *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Dec. 2018, pp. 412–417. doi: 10.1109/PDGC.2018.8745761.

[78] V. Strobel, E. Castelló Ferrer, and M. Dorigo, “Blockchain Technology Secures Robot Swarms: A Comparison of Consensus Protocols and Their Resilience to Byzantine Robots,” *Front. Robot. AI*, vol. 7, May 2020, doi: 10.3389/frobt.2020.00054.

[79] M. Nguyen, C. Nguyen, and H. T. Tran, “A Framework of Deploying Blockchain in Wireless Sensor Networks,” *EAI Endorsed Trans. Ind. Networks Intell. Syst.*, vol. 9, no. 32, p. e3, Aug. 2022, doi: 10.4108/eetinis.v9i32.1125.

[80] A. Terra, H. Riaz, K. Raizer, A. Hata, and R. Inam, “Safety vs. Efficiency: AI-Based Risk Mitigation in Collaborative Robotics,” in *2020 6th International Conference on Control, Automation and Robotics (ICCAR)*, Apr. 2020, pp. 151–160. doi: 10.1109/ICCAR49639.2020.9108037.

[81] C. Wang, Y. C. Tok, R. Poolat, S. Chattopadhyay, and M. R. Elara, “How to secure autonomous mobile robots? An approach with fuzzing, detection and mitigation,” *J. Syst. Archit.*, vol. 112, p. 101838, Jan. 2021, doi: 10.1016/j.sysarc.2020.101838.

[82] M. T. Nguyen, H. M. La, and K. A. Teague, “Collaborative and Compressed Mobile Sensing for Data Collection in Distributed Robotic Networks,” *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 4, pp. 1729–1740, Dec. 2018, doi: 10.1109/TCNS.2017.2754364.

[83] B. Breiling, B. Dieber, and P. Schartner, “Secure communication for the robot operating system,” in *2017 Annual IEEE International Systems Conference (SysCon)*, Apr. 2017, pp. 1–6. doi: 10.1109/SYSCON.2017.7934755.

[84] S. Hussaini, “Cyber Security in Cloud Using Blowfish Encryption,” *Int. J. Inf. Technol.*, vol. 6, no. 5, 2020, [Online]. Available: https://api.semanticscholar.org/CorpusID:224430049

[85] A. O. Elfaki *et al.*, “Revolutionizing Social Robotics: A Cloud-Based Framework for Enhancing the Intelligence and Autonomy of Social Robots,” *Robotics*, vol. 12, no. 2, p. 48, Mar. 2023, doi: 10.3390/robotics12020048.

[86] S. Chavhan and R. Doriya, "Secured Map Building using Elliptic Curve Integrated Encryption Scheme and Kerberos for Cloud-based Robots," in *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*, Mar. 2020, pp. 157–164. doi: 10.1109/ICCMC48092.2020.ICCMC-00032.

[87] A. Bezemskij, G. Loukas, D. Gan, and R. J. Anthony, "Detecting Cyber-Physical Threats in an Autonomous Robotic Vehicle Using Bayesian Networks," in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Jun. 2017, pp. 98–103. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.20.

[88] Feng Zhang, Shijie Zhou, Zhiguang Qin, and Jinde Liu, "Honeypot: a supplemented active defense system for network security," in *Proceedings of the 8th International Scientific and Practical Conference of Students, Post-graduates and Young Scientists. Modern Technique and Technologies. MTT'2002 (Cat. No.02EX550)*, pp. 231–235. doi: 10.1109/PDCAT.2003.1236295.

[89] S. Rivera and R. State, "Securing Robots: An Integrated Approach for Security Challenges and Monitoring for the Robotic Operating System (ROS)," in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9463965

[90] S. Rivera, A. K. Iannillo, S. Lagraa, C. Joly, and R. State, "ROS-FM: Fast Monitoring for the Robotic Operating System(ROS)," in *2020 25th International Conference on Engineering of Complex Computer Systems (ICECCS)*, Oct. 2020, pp. 187–196. doi: 10.1109/ICECCS51672.2020.00029.

[91] S. Rivera, S. Lagraa, C. Nita-Rotaru, S. Becker, and R. State, "ROS-Defender: SDN-Based Security Policy Enforcement for Robotic Applications," in *2019 IEEE Security and Privacy Workshops (SPW)*, May 2019, pp. 114–119. doi: 10.1109/SPW.2019.00030.

[92] M. A. Chauhan, M. A. Babar, and S. Grainger, "Designing a Security Platform for Collaborating Autonomous Systems - An Experience Report," in *2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C)*, Mar. 2021, pp. 1–7. doi: 10.1109/ICSA-C52384.2021.00018.

[93] J. Fernandez, B. Allen, P. Thulasiraman, and B. Bingham, "Performance Study of the Robot Operating System 2 with QoS and Cyber Security Settings," in *2020 IEEE International Systems Conference (SysCon)*, Aug. 2020, pp. 1–6. doi: 10.1109/SysCon47679.2020.9275872.

[94] R. Amini, R. Sulaiman, and A. Hadi, "CryptoROS: A Secure Communication Architecture for ROS-Based Applications," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 10, 2018, doi: 10.14569/IJACSA.2018.091022.

[95] R. White, G. Caiazza, H. Christensen, and A. Cortesi, "SROS1: Using and Developing Secure ROS1 Systems," in *Robot Operating System (ROS)*, 2019, pp. 373–405. doi: 10.1007/978-3-319-91590-6_11.

[96] J. Balsa-Comerón, Á. M. Guerrero-Higueras, F. J. Rodríguez-Lera, C. Fernández-Llamas, and V. Matellán-Olivera, "Cybersecurity in Autonomous Systems: Hardening ROS Using Encrypted Communications and Semantic Rules," in *ROBOT 2017: Third Iberian Robotics Conference*, 2018, pp. 67–78. doi: 10.1007/978-3-319-70836-2_6.

[97] B. Breiling, B. Dieber, M. Pinzger, and S. Rass, "A Cryptography-Powered Infrastructure to Ensure the Integrity of Robot Workflows," *J. Cybersecurity Priv.*, vol. 1, no. 1, pp. 93–118, Jan. 2021, doi: 10.3390/jcp1010006.

[98] T. C. Vu, M. T. Nguyen, V. T. Nguyen, and Q. C. Le, "Approach New Framework of Compressive Sensing Based Secret Sharing in Wireless Sensor Network: Theory and Applications," in *Advances in Information and Communication Technology*, 2024, pp. 26–34. doi: 10.1007/978-3-031-50818-9_4.

[99] S. Zaman, S. Raheel, T. Jamil, and M. Zalisham, "A Text based Authentication Scheme for Improving Security of Textual Passwords," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 7, 2017, doi: 10.14569/IJACSA.2017.080771.

[100]J. Kang, D. Nyang, and K. Lee, "Two-factor face authentication using matrix permutation transformation and a user password," *Inf. Sci. (Ny).*, vol. 269, pp. 1–20, Jun. 2014, doi: 10.1016/j.ins.2014.02.011.

[101]D. Carrillo-Torres, J. A. Pérez-Díaz, J. A. Cantoral-Ceballos, and C. Vargas-Rosales, "A Novel Multifactor Authentication Algorithm Based on Image Recognition and User Established Relations," *Appl. Sci.*, vol. 13, no. 3, p. 1374, Jan. 2023, doi: 10.3390/app13031374.

[102]S. Haas, T. Ulz, and C. Steger, "Secured Offline Authentication on Industrial Mobile Robots Using Biometric Data," in *RoboCup 2017: Robot World Cup XXI*, 2018, pp. 143–155. doi: 10.1007/978-3-030-00308-1_12.

[103]A. Khalifa, A. A. Abdelrahman, D. Strazdas, J. Hintz, T. Hempel, and A. Al-Hamadi, "Face Recognition and Tracking Framework for Human–Robot Interaction," *Appl. Sci.*, vol. 12, no. 11, p. 5568, May 2022, doi: 10.3390/app12115568.