Contents lists available at ScienceDirect

Intelligent Systems with Applications

journal homepage: www.journals.elsevier.com/intelligent-systems-with-applications

Cyber security of robots: A comprehensive survey

Alessio Botta [*], Sayna Rotbei, Stefania Zinno, Giorgio Ventre

Department of Electrical Engineering and Information Technology University of Napoli Federico II, Napoli, Italy

ARTICLE INFO

Keywords:
Cyber security
ROS
Robot forensics
DoS

ABSTRACT

The use of robots in the modern world is widespread, not only in medicine and automated vehicles, but also in national security, defense, and industry. Together with the growing number of robots there is also an increase of cyber attacks against robots and in general of their security issues. Thus, we consider cyber security and related issues such as robots vulnerabilities from different perspectives that need to be investigated in order to understand strengths and weaknesses of robots. The aim of this paper is to cover the topic of cyber security in robots in a more focused and comprehensive way with respect to what has been done previously in literature. Throughout our comprehensive survey, we discuss also different aspects related to threats, attacks, and available methods for preventing malicious behavior from robots. As a result of our investigation, it has been found that robots' data, software, network, and hardware are the most vulnerable components. During this review, eventually current approaches to protect robots are discussed in order to maintain their integrity, availability, and confidentiality. Furthermore, we demonstrate that the likelihood of cyber security risks on robotic platforms can be significantly reduced through improvements in encryption, authorization/authentication, and physical security. Security level of different robotic systems is analyzed in different fields so as to determine whether the security needs to be upgraded or rectified. We also present and describe open challenges that can arise in the next few years. This paper aims at being a starting point for researchers and practitioners to understand and upgrade the cyber security of robots.

List of Acronyms

AA	Authentication and Authorization
AI	Artificial Intelligence
CPS	Cyber Physical System
CUSUM	Cumulative Summation
DDS	Data Distribution Service
DoS	Denial of Service
DDoS	Distributed Denial of Service
IDS	Intrusion Detection System
MITM	Man in the Middle
RAS	Robots and Autonomous Systems
ROS	Robotic Operating System
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicles
IC	Intelligent Checker

1. Introduction

In recent years, security of computers and IoT devices became a crucial issue: not only robots deal with critical information but they also can be located in vital locations. Robots of today and tomorrow will be in closer contact with humans and being aware of their vulnerabilities and potential threats is fundamental to guarantee the safety of humans and robots. Although their main role is being a facility for improving human life quality, many unfortunate and harmful events can occur. Therefore the consequences of security issues of the robots can be dramatic in many aspects. It is also necessary to protect costly, sophisticated robots against such threats.

According to papers that were reviewed in this work, Fig. 1 simplifies main cyber security issues of robots. Security risks can emerge accidentally during the development of robot platform, applications, hardware and sensors while even untrained users, can cause unwanted security problems for robots accidentally (Yaacoub et al., 2020, Fosch-Villaronga & Mahler, 2021). On the other hand, cyber security problems can be caused by attackers (Wang et al., 2021). Hackers aim at

[*] Corresponding author.
E-mail addresses: a.botta@unina.it (A. Botta), sayna.rotbei@unina.it (S. Rotbei), stefania.zinno@unina.it (S. Zinno), giorgio.ventre@unina.it (G. Ventre).

https://doi.org/10.1016/j.iswa.2023.200237
Received 3 August 2022; Received in revised form 9 March 2023; Accepted 19 May 2023
Available online 26 May 2023

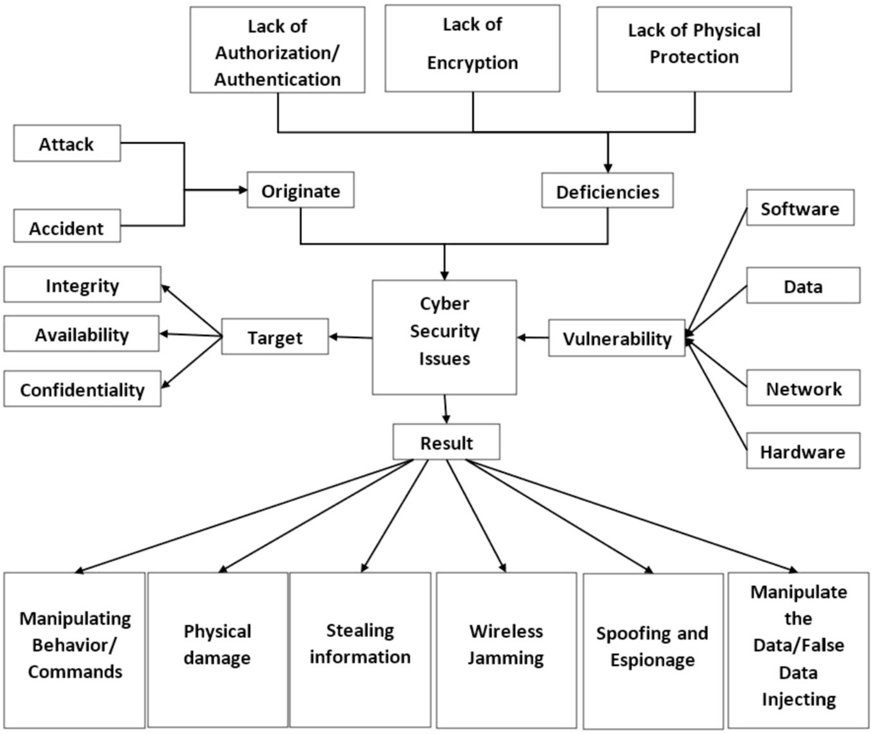

Fig. 1. Origin, reason, target vulnerability and results of cyber security issues.

being able to spy or use critical data of robots and information to damage or even to destroy robots. Some limitations in fact as lack of authorization/authentication (Jain & Doriya, 2019), encryption (Petit & Shladover, 2015), and physical protection (Khalid et al., 2018) play a critical role in making the robots weak against cyber security issues and their implementation needs to be upgraded. Related work shows that the main target of attackers are robots integrity (Jain & Doriya, 2019, Fosch-Villaronga & Mahler, 2021), availability (Dóczi et al., 2016), and confidentiality (Staffa et al., 2018). According to the reviewed papers for this research, attacks can have different consequences like stealing information (Pogliani et al., 2019), wireless jamming (Khalid et al., 2018), manipulating robots behavior or commands (Yaacoub et al., 2020), manipulation data (Sabaliauskaite et al., 2017), physical damage (Cornelius et al., 2018, Alemzadeh et al., 2016), and spoofing and espionage (Petit & Shladover, 2015).

Table 1 mentions some of the papers that refer to the origin of threats against the cyber security of robots. Such table divides issues related to the robot cyber security into intentional and unintentional actions causing malfunctioning. The number of literature works concerning attacks proved the importance of investigation on cyber security attacks in fact, the number of security problems arising from malicious actions is much higher than the number of such problems caused by accidental causes.

There are several surveys in literature related to the robots and their security issues. Yaacoub et al. have investigated and evaluated the robots-related security issues in different fields like security attacks, vulnerabilities and associated risks (Yaacoub et al., 2021). The authors also provided a set of recommendations and requirements, and some suggestions in order to protect robots from malicious attackers, with the aim of minimizing damages and making deployment and use of robots every day safer. However, such paper also covers aspects that are not specific for robots, while our work focus only on robot-related ones. Main threats, literature and open challenges in the field of safety-critical robots are also explored linking up the concept of dependability and robots (Guiochet et al., 2017). Dudek et al. in their research (Dudek & Szynkiewicz, 2019) reviewed the known and new threats for cyber-physical robotic systems caused by cybernetic attacks.

Table 1
Attacks as the most common origin of cyber security issues.

Paper	Origin	
	Accident	Attack
Yaacoub et al. (2020)	X	X
Fosch-Villaronga and Mahler (2021)	X	X
Jain and Doriya (2019)		X
Petit and Shladover (2015)		X
Wang et al. (2021)		X
Staffa et al. (2018)		X
Mazzeo and Staffa (2020)		X
Giaretta et al. (2018)		X
Alemzadeh et al. (2016)		X
Dóczi et al. (2016)		X
Fosch-Villaronga and Mahler (2021)		X
Pogliani et al. (2019)		X
Quarta et al. (2017)		X
Khalid et al. (2018)		X
Vuong et al. (2014)		X
Ahmad Yousef et al. (2018)		X
Cornelius et al. (2018)		X
Sabaliauskaite et al. (2017)		X

The authors of “Potential cyber attacks on automated vehicles” (Petit & Shladover, 2015) specifically analyzed the threats on Unmanned Aerial Vehicles (UAV) and cooperative automated vehicles extensively describing of their specific threats and attacks as well as (Yaacoub et al., 2020). In other research the authors depicted the most common vulnerabilities and attack vectors together with several approaches to secure Robotic Operating System (ROS) and similar systems (Dieber et al., 2017). According to Cottrell et al. (2021) 92.6% of vulnerabilities are software-related, in fact, a much higher percentage when compared to ones posed by hardware only components. In another research authors only classified modern Intrusion Detection System (IDS) based on detection technique and audit material and only for Cyber Physical System (CPS) (Mitchell & Chen, 2014).

Although some works related to cyber security of robots have been presented, challenges like threats, vulnerabilities and consequences on

Table 2
Inclusion criteria and exclusion criteria.

Inclusion criteria	Exclusion criteria
Studies that describe the challenges of cyber security of robots	Articles not in English language
Studies that describe different kinds of cyber security attacks	Studies those are not relevant to the research questions
Studies that describe different kinds of attacks and related issues	Articles outside the domain of Robots cyber security
Studies that describe the vulnerability of robots	Books
Studies that describe the effect of cyber security attacks	Irrelevant articles obtained from ineffective search engines

robots and their environment have still to be extensively studied and investigated (Ahmad Yousef et al., 2018). The main goal of our work is to cover the gap of knowing challenges of robotics, related to cyber security in more detail, by reviewing other related papers and classifying the issues that others covered and worked on. As aforementioned there is a necessity to have a comprehensive but also focused work, which is our approach for this paper. This work in fact, focuses on all aspects of both threats, attacks, and available frameworks to prevent malicious actions only related to the robotics field and in addition to being comprehensive, is also focused, which is its essence. Such focus allows us to concentrate on issues that are only relate to such platforms and therefore to go much deeper into the cyber security of robots with respect to what has been done previously. Previous surveys (Yaacoub et al., 2021, 2020) analyzed broader topics, which not only included robots but also other platforms while the aim of our paper, instead, is to go into the specific details of robot cyber security. Specifically, our work covers challenges related to robot cyber security, as types of attacks that can be launched at each component of the robot platform. Prior review papers have seldom looked at robot cyber security challenges from this perspective. As a result of this classification and analysis of the cyber security of robots, it was possible to determine which components need more attention and investigation to address weaknesses. Another important issue was the lack of a focused and comprehensive study about analyzing the current methods and strategies for protecting robots. By reviewing existing methods and finding their weaknesses and possible solutions, the current paper examines how to protect different robot components. Also, the consequences of specific attacks on robots are investigated with a focused study as well following the cause-effect attacks-consequences relationship, which has not been explored by other works in this field. All of the above mentioned are thoroughly discussed in this paper in order to demonstrate the risk that robots face everyday. Moreover, we examined robots working in different fields as industrial or medical. Taking into account this information is crucial since according to their work environment the rate and kind of risks and threats greatly vary. Finally, during the analysis and reviews, topics that need more attention and investigation in future works have been found, which nobody mentioned in their study.

Paper is structured as follows: in Section 3 major attacks and how they are performed are described, in Section 4 solutions to secure and protect robots are shown, in Section 5 all possible results of attacks are presented. Section 6 presented in order to know different types of available robots in the real world. Section 7 presents possible application scenarios for robots and cyber-security implications. Also in Section 8 we addressed the current open challenges for the next few years.

2. Materials and methods

This survey provides a review of the papers related to robot cyber security and tries to make a comprehensive insight into the topic.

In the first step of the review plan, the research questions and targets are identified. The context of the study is set for the cyber security of robots and the issues related to that. Based on the motivation and requirements of this topic the research questions focused on:

- What are the different types of attacks targeting the robotic platform?

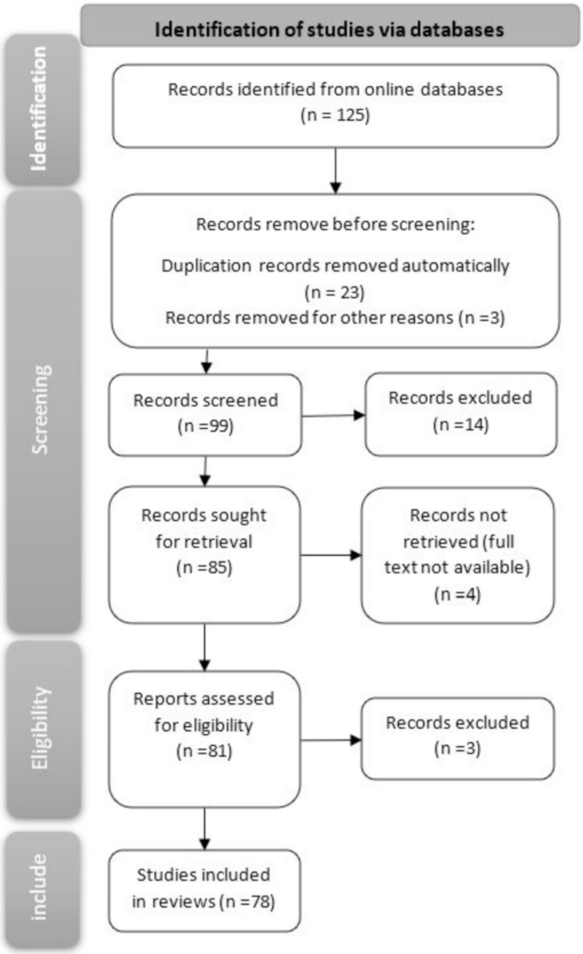
Identification of studies via databases
Identification
Records identified from online databases (n = 125)
Screening
Records remove before screening:
Duplication records removed automatically (n = 23)
Records removed for other reasons (n =3)
Records screened (n =99)
Records excluded (n =14)
Records sought for retrieval (n =85)
Records not retrieved (full text not available) (n =4)
Eligibility
Reports assessed for eligibility (n =81)
Records excluded (n =3)
include
Studies included in reviews (n =78)

Fig. 2. All phases of a systematic review.

- Which kinds of techniques and strategies are provided in this field?
- How the cyber security attacks on the robots can affect them?
- What are the common cyber security issues of each type of robot?
- Which issues related to cyber security of robots have not been enough covered and counted as an open challenge in this field?

In the next step, seven related online databases including ACM, Emeralds, Springer, Taylor and Francis, IEEE, SAGE, and IGI were selected. Then, the combination of the search terms was used for searching the related studies from online databases between 2011 to 2021. In this study, various combinations of “robots cybersecurity”, “security of the robots”, and “cyber-physical system” were used. Only studies in English language were selected for screening. The full search strategy is reported in the Prisma Fig. 2. In the next step, a linear reference search was conducted by checking the identified papers, to recognize if they met the inclusion criteria, Table 2 shows the inclusion and exclusion criteria. Two researchers, who were blinded to the author information of the articles, independently screened all identified records for inclusion. In case of disagreements, a third author was consulted.

Table 3
Majority of cyber robotics attacks at different level of the stack.

Paper	Hardware	DoS	Spoofing	Eavsdrop	MITM	ARP	Data	ROS Node
Network								
Sabaliauskaite et al. (2017)							X	
Raval et al. (2018)	X			X	X		X	
Guerrero-Higueras et al. (2017)		X	X					
Guerrero-Higueras et al. (2018)		X	X					
Vuong et al. (2014)		X						
Ahmad Yousef et al. (2018)		X						
Trabelsi et al. (2021)		X				X		
Soe et al. (2020)		X						
Wang et al. (2021)								X
Giaretta et al. (2018)					X	X		
Gorbenko and Popov (2020)							X	
OS/Network								
Dieber et al. (2020)					X			X
Teixeira et al. (2020)					X			
Rivera, Lagraa, & State (2019)		X					X	X
OS								
Toris et al. (2014)								X
Goerke et al. (2021)					X			X
Sandoval and Thulasiraman (2019)							X	X
Breiling et al. (2017)		X					X	X
Dieber et al. (2016)								X
Mukhandi et al. (2019)					X			
Physical/Network/OS								
Quarta et al. (2017)							X	
Alemzadeh et al. (2016)	X			X				
Bonaci et al. (2015)	X			X				

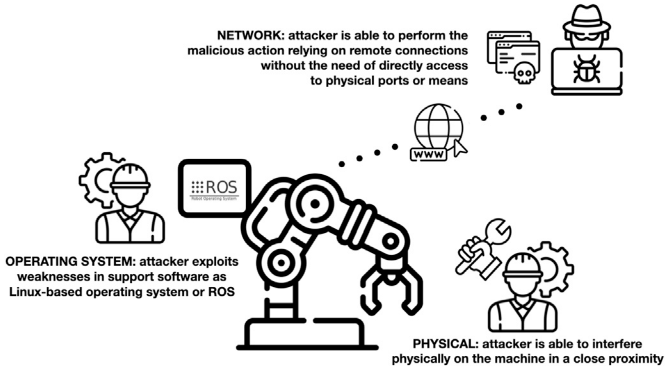
NETWORK: attacker is able to perform the malicious action relying on remote connections without the need of directly access to physical ports or means
WWW
ROS
OPERATING SYSTEM: attacker exploits weaknesses in support software as Linux-based operating system or ROS
PHYSICAL: attacker is able to interfere physically on the machine in a close proximity

Fig. 3. Hacking Robots at physical network and/or operating system level.

2.1. Data extraction

In the first step, two review authors performed the screening of the title and abstract from included studies, and the third author checked the extracted data. The extracted data was: a) title, b) if they are journal or conference paper, c) the name of journal or conference, d) keywords, e) main goal of the studies that mentioned in the abstract. Then, the quality of the papers reviewed by checking all the details extracted in the previous step. Finally, all studies reviewed in details and all related data and information were extracted from studies according to the main target of this research.

3. Types of attacks on robotic platforms

All available literature on attacking robots is presented in this section: first all physical attacks are discussed, then networking- and software-based ones are illustrated as also presented in Fig. 3.[1]

Table 3 provides an overview of several attacks we found in literature. Most papers deal with DoS, MITM and attacks to ROS nodes. Papers in Table 3 are divided by area of the attacks which can be physical, network and OS and some of them are cross area. Almost the same division is here reported in the Section 3. Most papers of each area deal only with one or two types of attacks while only few of them worked on all three kinds.

3.1. Physical

Physical layer attack means the hardware-based attacks. A review of possible threats for CPSs systems is presented in Dudek and Szynkiewicz (2019). Due to the variety of CPS components and systems it is very difficult to approach security following one generalized model (Humayed et al., 2017). Therefore, Humayed et al. explored this issue from the security perspective, starting, from the perspective of CPS components and also from the CPS systems (Humayed et al., 2017). The physical layer of CPSs exposes a number of possibilities in terms of vulnerabilities and attacks, so due to the extent of threats, being aware of possible profiles of attackers could be useful to prevent them. By classifying and comparing attacker models on CPSs, it has been proved that there are no commonly used attacker models for focusing to tackle, so the physical attacks can be really threatening to CPSs (Rocchetto & Tippenhauer, 2016). The hardware-based attacks may target code controlling microcontrollers for a robotic car, impacting the performance of motors or battery, giving false instructions and even damaging the robots' components. Such results are easily achieved through commands that drain the battery of the car or using the operator interface to gain a full set of vulnerable protocols (Raval et al., 2018).

3.2. Networking

Performing malicious actions by remote connections without the need to directly access to physical ports is called a “Network Attack”, which expands the attacker's possibilities of actions effectively.

In general, sensors are one of the most sensitive and important parts of robots in terms of network attacks that can be easily exploited with

[1] All icons are created by Freepik, BabyCorn, Eucalyp, Torskaya from Flaticon.

cyber attacks. According to Sabaliauskaite et al. (2017), “Three types of cyber attacks on sensor measurements were implemented and investigated: false data injection, scaling, and stealthy attacks”. In the injection attacks, sensor measurements were biased through addition, while in scaling attacks the bias was through multiplication. Different unique scenarios related to CPSs have been explored where NFC and Wi-Fi are the wireless technology for operating and controlling. Each technology showed its risk profile and known weaknesses that are associated with attacks including eavesdropping, data corruption, data modification and Man in the Middle (MITM) (Raval et al., 2018). Rivera et al. tested attacks such as Denial of Service (DoS) and spoofing attacks on Real Time Location Systems. DoS was able to interfere with the signal emitted by beacons. Spoofing, on the other hand, changed the signal emitted by beacons introducing errors and resulting in incorrect calculating of the tag location (Guerrero-Higueras et al., 2017).

Both CPSs and complex robots such as humanoid robots can be targets of traditional network attacks.

About the humanoid robots, APIs of Pepper are particularly vulnerable and prone to accept TCP packets from any untrusted sources, following the assumption that only legitimate users will call the APIs. Therefore, such humanoid robots can be abused by using security threats like spoofing login credentials, stealing data stored in robots and hacking the devices; they can even be forced to harm humans around the robot physically (Giaretta et al., 2018).

Through hands-on activities, NAO a popular humanoid robot has been evaluated in terms of resilience, and robustness against common DoS attacks. The test proved that NAO is very vulnerable to DoS attacks and is not equipped with features of security defense in order to limit external malicious attacks (Trabelsi et al., 2021). About the DoS attacks, they have clear effects on the movement of rescue robots (Vuong et al., 2014), and can cause robots as PeopleBot to not respond to proper commands. Also, a Robot Attack Tool (RAT) was developed in order to perform attacks on the robot platform PeopleBot. Attacks against availability were able to cause DoS and the robot was not responsive to MobileEyes commands. Attacks against integrity and availability caused sensitive information on the robot to be hijacked (Ahmad Yousef et al., 2018).

3.3. Operating system

Operating system attacks exploit weaknesses in support software such as Linux-based operating systems or ROS which constitute the heart of several robots. Analyzing a total of 176 threats collected from the robot vulnerability database showed that 92.6% are mainly software-related and proved that software in robotics systems poses a more critical threat in comparison with hardware components (Cottrell et al., 2021).

To identify realistic profiles for attackers that pose a threat specifically to ROS based robotic systems, an exemplary networking setup is created by Goerke et al., where ten existing protection mechanisms are compared. Results for both ROS 1 and ROS 2 provided useful insights and guidelines to help experts of the field choose the most effective protection solutions for their scenario for ROS node attacks and MITM (Goerke et al., 2021). When dealing with multi-robot active surveillance systems, an attacker inside the network can easily send shutdown commands to manipulate or destroy any ROS node and publish adulterated messages manipulating velocity commands to misdirect a robot (Portugal et al., 2017). Another example of ROS attack is the use of unsecured ports for ROS-to-ROS, node-to-node, communication in plain text (Toris et al., 2014).

To better facilitate penetration testing for ROS, ROSPenTo and ROSchaos appear to be powerful tools that make use of the vulnerabilities of ROS and demonstrate how ROS applications can be sabotaged by an attacker targeting APIs (Dieber et al., 2020). Another tool that can intercept, manipulate and completely disrupt the communication between two ROS nodes is presented in Teixeira et al. (2020). The tool was tested on a robot called DoRIS, a domestic robot, showing the ability to completely compromise its functionalities by loosing control of the communication channel, its implementation is also briefly compared to ROSspent. Another tool for assisting researchers in testing exploitation for ROS is ROSploit, a tool designed for this goal (Rivera, Lagraa, & State, 2019).

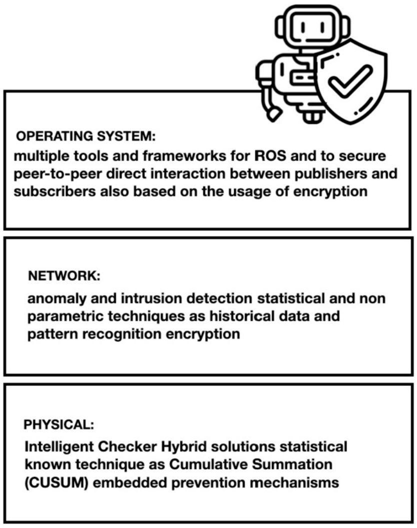
OPERATING SYSTEM:
multiple tools and frameworks for ROS and to secure peer-to-peer direct interaction between publishers and subscribers also based on the usage of encryption
NETWORK:
anomaly and intrusion detection statistical and non parametric techniques as historical data and pattern recognition encryption
PHYSICAL:
Intelligent Checker Hybrid solutions statistical known technique as Cumulative Summation (CUSUM) embedded prevention mechanisms

Fig. 4. Main techniques adopted to protect robots.

Yankson et al. proved how challenging is to develop a fully secure environment for the robot by testing the vulnerabilities of Zenbo which runs on the Android platform with automated tools such as Drozer, MobSF and Androbugs on the robot Zenbo. Android OS appears to be subject to attacks due to some vulnerable applications installed on it and internal storage can be easily accessed. Also stored information is easily manipulated during penetration testing and users' personal information could be easily accessed and retrieved, exposing the user to a dangerous breach (Yankson et al., 2021). Even when using simple interfaces as SeeedStudio BeagleBone[2] Green Wireless, attacks can have devastating effects on robots. An attacker that successfully gains control of BeagleBone when adopted for a robotic car can: modify operator command behavior of moving forward, disable Wi-Fi access to the car, severing the operator's command and control communication channel, reduce the speed of the car or stop it all of a sudden (Raval et al., 2018).

3.4. Discussion

Papers analyzed in this section show that most of the researchers dealt with one or maximum two kinds of attacks in their work, which means that they had the opportunity to study them more in details. On the other side, this paper shows that there are several topics in the robot cyber security attack field that need more attention like ARP, Spoofing, and Eavsdrop. Moreover, it seems that physical attacks have less importance for the researchers and most of them studied attacks that targeted networks and operating systems.

4. Techniques and strategies to protect robots

In this section, available literature on protecting robots is presented: first all physical solutions are discussed, then the ones related to network and operating system are analyzed, as shown in Fig. 4.

[2] BeagleBone is an open-source hardware design that includes a high-performance flexible WiFi-Bluetooth module.

Table 4
Hardware solutions applied to protect humanoid robots.

Paper	Robot
Sabaliauskaite et al. (2017)	Amigobot
Sabaliauskaite et al. (2016)	Amigobot
Staffa et al. (2018)	NAO
Mazzeo and Staffa (2020)	NAO
Zhao et al. (2020)	Gazebo

4.1. Physical

Protecting robots at physical levels starts with early detection of attacks. When a cyber attack is conducted against a rescue robot it is accompanied by physical effects, that can help detect it. More specifically, two are the main significant physical indicators related to a cyber attack: the robot halting and delay in responding to navigation commands (Vuong et al., 2014). Solutions are mostly implemented in humanoid robots as depicted in Table 4. To detect the possible effects of false data injection, scaling, and stealthy attacks a hybrid solution was implemented with an Intelligent Checker (IC) and used with an Amigobot Robot. The Intelligent Checker (IC) has a sensor and a decision logic, the sensor able to measure parameters of the process and the decision logic compares measurements against constraints. The decision logic element is connected to an alarm, which is activated if there are any violation. Solutions show to outperform statistical known technique as Cumulative Summation (CUSUM), in detecting cyber attacks (Sabaliauskaite et al., 2016, 2017). Another solution for protecting robots is proposed by Staffa et al. Authors presented a testbed for robots equipped with Intel SGX systems that can be easily integrated with ROS components to improve the overall robot security in a hardware-assisted trusted execution environment (Staffa et al., 2018). To protect and secure ROS (Mazzeo & Staffa, 2020), a patched ROS solution called Trusted-ROS demonstrates also how to take advantage of hardware-assisted computing to protect data handled by the operating system, which on the other side would be stored in the memory unencrypted. TROS is implemented on NAO through Intel SGX as well (Mazzeo & Staffa, 2020).

Again Gazebo, another humanoid robots adopting ROS, is equipped with a controller that constrains the robot behavior with the aim to prevent security problems and to put forward protective measures against false information induction and DoS attacks (Zhao et al., 2020).

4.2. Networking

Protecting robots at network level starts as early as possible with anomaly and intrusion detection. Different techniques are shown in Table 5. Machine Learning (ML) and statistical methods represent the two main used techniques while two papers deal with pattern recognition.

ML is widely used as in an effective criminal detection system based on face recognition. Based on facial recognition data, algorithms such as principle component analysis (PCA) and linear discriminant analysis (LDA) can be used to identify criminals. Quality, illumination, and vision are all factors that influence system efficiency (Jujjuri et al., 2022). Concerning geographical and temporal data forecasting with machine learning techniques as an example 68 various crime keywords are explored to figure out what kind of crime investigators are dealing with (Prathap, 2022). Anomaly detection in sensor networks can be explored with misuse detection or signature-based detection. With misuse detection attacks signatures are matched against monitored ones, this kind of detection technique is able to detect known attacks but acts inefficiently with new ones. Anomaly detection on the other hands acts when anomalies are identified as deviation from normal data profiles.

Attacks that can be easily detected and discovered are: jamming, tampering, sinkhole attack, DoS, Sybil attack, wormholes, spoofing, selective forwarding, eavesdropping (Mitchell & Chen, 2014). Modern CPS IDS techniques can be also classified in detection technique and audit material. Advantages and drawbacks of each category are depicted in Mitchell and Chen (2014). Industrial robots lately can be equipped with an innovative intrusion detection technology called PIDS (Power-based Intrusion Detection System), which is delivered as a bump-in-the-wire module put at the powerline of commodity robots (Pu et al., 2021). The particle swarm optimization algorithm (PSO-H-SVM) is also used with industrial robots and is able to classify the operation state of robotic arms, predicting the operation state in real time and determining whether the state transfer meets the logical requirements. Whether the requirement appears to be met or not it determines if an intrusion occurred reaching 96.02% in accuracy (Zhou et al., 2022).

Bayesian network-based techniques for attack detection can also be used to determine whether an autonomous vehicle is under threat as well as whether the attack originated in the physical or cyber worlds (Bezemskij et al., 2017).

Other approaches for IDS are based on statistical techniques and non-parametric techniques as rule based Approaches, CUSUM-Based Approaches, data clustering approaches, density-based approaches and support vector machine approaches (Rajasegarar et al., 2008). A lightweight machine learning-based intrusion detection system using a new feature selection algorithm is designed and implemented on Raspberry Pi, and its performance is verified using a public dataset collected from an IoT environment in Soe et al. (2020). In the other research authors (Sabaliauskaite et al., 2016, 2017), in particular, explored detection methods based on CUSUM methodology and compared those to an attack detection method based on retrieval of sensor values. Tests were conducted on an Amigobot Robot. Four different methods were compared: the Average Distance Method, the Average Distance Change Method, the Average Distance Traveled Method, the Estimated Distance Change Method. Methods were implemented to detect false data injection, scaling, and stealthy attacks. In particular, the average distance method proved to be effective for detecting attacks on Amigobot and could be used as a valid alternative to CUSUM-based methods when paired with a controller based solution. When cyber attacks on real time location systems occur, statistically meaningful differences appear in the data provided by beacon-based real time localization systems comparing the case when there is an attack or none (Guerrero-Higueras et al., 2017). Also attacks can be spotted easily, specifically DoS and Spoofing, when detected by a system built using machine learning techniques (Guerrero-Higueras et al., 2018).

In order to provide the fundamental understanding of the problem needed to create elegant Distributed Denial of Service (DDoS) defensive systems, many detection approaches are surveyed by Singh and Gupta in their paper (Singh & Gupta, 2022). Another approach to the development of an intrusion detection system is based on an abnormal behavioral pattern detection. The system can be used for detection of zero-day deceptive attacks (Gorbenko & Popov, 2020).

In “Classification based machine learning for detection of DDos attack in cloud computing”, the author used a classification-based machine learning approach for finding the DDoS attacks in cloud computing by using three ML classification methods, including K Nearest Neighbor, Random Forest, and Naive Bayes. The provided result proved that the DDoS attacks can be detected with 99.76% accuracy (Mishra et al., 2021). For reducing the risk of attacks from network, the researchers used a white-hat worm launcher based on machine learning adaptable to a large-scale IoT network for Botnet Defense System (BDS), and the results showed a 30-40% of reduction in infected devices (Pan et al., 2022).

A service-oriented software architecture (SOA) for big data analytics based on fog computing in Intelligent Transportation System (ITS) applications appears to be quite useful to reduce the risk of a network attack. Hussain and Beg (2019) proposed a method based on SOA after studying the so called “mission-critical computing needs of the next generation ITS applications” and while reviewing scenarios related to underutilized communication and computational resources which are

Table 5
Detection techniques and methodologies to prevent cyber attacks.

Paper	Machine Learning	Statistical Methods	Pattern Recognition
Rajasegarar et al. (2008)		X	
Sabaliauskaite et al. (2016)		X	
Sabaliauskaite et al. (2017)		X	
Guerrero-Higueras et al. (2017)	X	X	
Soe et al. (2020)	X		
Guerrero-Higueras et al. (2018)	X		
Chen et al. (2020)	X		
Gorbenko and Popov (2020)			X
Olivato et al. (2019)			X

available in connected vehicles and can be used to play the role of Fog Computing infrastructures.

Other major detection techniques rely on historical data and pattern recognition. With autonomous boats and social robots detecting anomalies can be improved extracting system logs from a set of internal parameters of the robotic system and transforming them into images, while auto-encoder architectures are able to classify behaviors (Olivato et al., 2019). Experimental results confirm that adopting RoboFuzz as a detection and mitigation algorithms shows a success rate of up to 93.3% taking advantage of historical records of obstacles to detect inconsistency in obstacle appearances allowing robot to continue to move (Wang et al., 2021). Analysis based on logs using ML methods is also able to detect robots instances online and crucial to prevent possible exploitation from malicious attacks. Web robot detection methods are offline web-log mining with machine learning, honeypot, and online web robot detection. Offline analyses appear to achieve high accuracy in some scenarios while honeypots play an important role in collecting information from websites, however, robots can be tricked by them so that eventually they could be used as a data collector rather than as a classifier (Chen et al., 2020).

Another web related threat is posed by ROS instances that are open and exposed to the public, allowing to access robotic sensors and malicious users to read images and information from sensors (DeMarinis et al., 2019). Eventually adopting RSA (Rivest Shamir Andelmen), AES (Advanced Encryption Standard), ECC (Elliptic Curve Cryptography) can relieve cloud robotics suffering from network based attacks, data storage based attacks, virtualization based attacks (Jain & Doriya, 2019).

During the COVID pandemic, to encourage uptake of learning cyber security skills a new approach to security is presented by Legg et al. (2021). The traditional approach that uses *Capture-The-Flag* routine widely used in cyber security education, has been replaced by interactive sessions made possible via video conferencing platforms along with the possibility of exploiting home IoT environments (Legg et al., 2021).

4.3. Operating system

Most robots equipped with operating systems as Linux or ROS suffer from a variety of vulnerabilities and are exposed to well known attacks as previously discussed. As an example, if exploited using data distributed services security extension, ROS 2 security vulnerabilities arise (Sandoval & Thulasiraman, 2019). Several approaches are already available to secure ROS showing that the best way to secure it is the application level with a solution integrated directly into the ROS core (Dieber et al., 2017).

When two popular middleware used in robotics solution as Ice and Fast-RTPS are adopted, the security capabilities of the standard ROS transport system of some analyzed communication solutions have an acceptable impact in latency and loss terms (Martín et al., 2018).

When dealing with UAV, the ability of ROS to detect and prevent malicious attackers is almost a requirement. Basic attacks in a naval fleet can be tested against the security enhancements of ROS 2 APIs. Results demonstrate that ROS bridged with security features/plugins is capable of mitigating attacks against a UAV swarm and are effective at the cost of some delay to the drone. A trade-off can be achieved eventually between the use of ROS 2 and the latency overhead that is induced (Sandoval & Thulasiraman, 2019). To analyze the impact that humans have on the security of CPS, extendable virtual platforms such as RESCHU-SA are available. The platform is an extension of the research environment for supervisory control of heterogeneous uncrewed vehicles simulation environment, already implemented when supervising UAVs and evaluating interface usability (Elfar et al., 2017). Real-time experiments showed also that the Unmanned Aerial System (UAS) are unable to function properly when cyber attacks occur potentially harming board computer. To demonstrate system security through practical experimentation an UAV system was equipped with a security framework and defended against attacks that inject abnormal data into UAV flight by granting only access control and integrity (Lee et al., 2021).

More in general multiple tools and frameworks are proposed to secure ROS:

- ROSRV, an open-source runtime verification framework for robotic applications aimed at addressing safety and security issues. It provides a transparent monitoring infrastructure that monitors commands passing through the system integrating seamlessly with ROS and requiring no changes in the OS architecture (Huang et al., 2014).
- ROS-Defender, a holistic approach integrating a security event management system, an intrusion prevention system and a firewall. The solution brings anomaly detection systems to the application and network level, with dynamic policy enforcement. The solution also adopts software defined networking to protect against malicious attacks (Rivera, Lagraa, Nita-Rotaru, et al., 2019).
- ROS-Immunity, a collection of tools, aimed at developing a modular, secure framework for ROS, which presents internal system defense, external system verification, and automated vulnerability detection in a unique tool that works efficiently together with Secure-ROS (Rivera & State, 2021).
- ROS-FM, an extended version of Berkely Packet Filters and eXpress Data Path to build a network-monitoring framework for ROS. When comparing the overhead of these tools to the existing one, with more than 10 running processes the tool appears to be causing only 4% of overhead with respect to other solutions (Rivera et al., 2020).

In ROS based system a crucial vulnerability is represented by securing peer-to-peer direct interaction between publishers and subscribers. Many solutions have been proposed in literature as:

- A Transport Layer Security and Datagram Transport Layer Security to be included in the ROS core to secure the communication. Few changes were made to the ROS system and the overhead introduced by the security functions was assessed (Breiling et al., 2017).
- An application layer for data flow control and protection between ROS nodes. An extra Authentication and Authorization (AA) node

is supposed to handle authorization and authentication processes within a ROS vl.x based system. With no further slow down in the communication the AA node solves many of authentication and authorization issues just knowing the rules, which node can communicate with which other node. Also nodes at startup can ask the AA node about these rules and accept the messages from nodes to communicate with trusty ones (Dóczi et al., 2016).

- A cross-layer approach dealing with both physical and cyber layers. Due to the delay caused by the security mechanism, a time-delay controller for the ROS agent is placed in the physical layer. In the cyber layer, cyber states and the usage of the Markov decision process are adopted to evaluate the trade offs between physical and security performance. Due to the uncertainty of the cyber state, the method was extended to a partially observed Markov decision process (Xu & Zhu, 2018).
- A security platform that supports secure communication among autonomous systems of robots as TurtleBots, trying to guarantee the security of communication, the integrity of the information, secured availability of the data, and access to services. The solution provides seamless security in heterogeneous collaborative autonomous entities adopting public key encryption (Chauhan et al., 2021).
- A new standard for security logs that enable to build all the library functions and call-back not covered by a usual log system. The result is achieved from a more accurate and defined structure together with a standard syntax for the definition of the policy profiles based on the well-known AppArmor syntax. Also, static and dynamic solutions for certificate and attribute distribution are discussed (Caiazza et al., 2019).
- A data distribution service standard as a middleware to ensure security and QoS policies analyzing costs linked to varying QoS and security settings (Fernandez et al., 2020).
- A robot application security process, a lightweight process that remarks the role of the security engineer as an important actor in robot design. The solution enables the engineer to verify the completeness of his work and allows him to discuss security with other stakeholders (Hochgeschwender et al., 2019).

Multiple solutions to secure ROS are based on the usage of encryption techniques aimed at securing communications between ROS nodes. Examples are reported below:

- CryptoROS, an architecture to secure ROS that makes no changes to software libraries and no tools are required. It works with all ROS client libraries as rospy and roscpp, and rebuilding nodes is not necessary (Amini et al., 2018).
- SROS1 a support for ROS1 APIs aimed at supporting encryption and security precautions as: over-the-wire encryption, namespaced access control enforcing graph policies-restrictions, and process profiles using Linux Security Modules to strengthen nodes resource access (White et al., 2019).
- A solution based on both encryption and ROSRV where an advanced encryption standard algorithm has been used in combination with the framework to define semantic rules for ROS messages. The solution has been tested when plain-text messages are not allowed and must be blocked. Rules for detecting DoS are put in place against attacks tested on a real time locating system, used to estimate location of a mobile robot (Balsa-Comerón et al., 2018).
- A novel approach integrating ROS with the message queuing telemetry transport protocol. Real-world experiments on a robotic surveillance system demonstrate it is possible to prevent man-in-the-middle and hijacking attacks and to secure network communications of robots by providing authentication and data encryption (Mukhandi et al., 2019).
- A dedicated authorization server to ensure that only trusted nodes interact with the application. Cryptographic methods ensure data confidentiality and integrity (Dieber et al., 2016).
- An encryption-powered distributed infrastructure is implemented to preserve robot workflows when a client composes a robot program and once it is accepted a separate entity provides a digital signature for it, which can be verified by the robot before executing it (Breiling et al., 2021).
- The use of web tokens to ensure secure authentication for remote, non-native clients in the ROS middleware. The use has been tested with applications for securing clients within the popular *rosbridge* protocol (Toris et al., 2014).

4.4. Discussion

Summarizing this section, different methods have been used and applied in literature for protecting robots against attacks. Some of them have been tested on robots like NAO, Amigobot, Gazebo. The papers reviewed showed that protecting robots at the operating systems and network levels is more important than protecting robots at the physical levels. They also show that protecting robots at the physical level needs more attention in order to know its cyber security issues and solve them. Cyber security of robots needs a parallel study at all levels and layers to make reliable robots that can survive the different kinds of attacks possible against them.

5. How attacks affect robots

In this section, all available literature on how attacks affect robots is presented: malicious attacks can, in fact, affect robots in different ways. They can harm robots physically and damage them and those around them, they can alter the robot from a networking perspective and defeat the operating system as well, as shown in Fig. 5.

5.1. Physical

When CPSs are under attack, they can be physically damaged together with objects within the environment. Also, injuries or death of humans around appear to be possible (Dudek & Szynkiewicz, 2019). Attacks to micro-controllers for a robotic car can efficiently impact the performance of motors and batteries, give false instructions, and even damage the components of the robots (Raval et al., 2018). Attacks can have a robot crashes into the wall, not reaching the destination, come closer to the wall than expected, move out of limits in opposite direction, and could possibly crash (Sabaliauskaite et al., 2017).

PeopleBot as an example was not responsive to Mobile Eyes commands during DoS attacks (Ahmad Yousef et al., 2018). Also, Pepper appears to be able to physically harm humans around him (Giaretta et al., 2018). Clear effects on the movement of a rescue robot are shown also in Vuong et al. (2014).

One example of an attack occurring in the presence of an intrusion detection system is when eight RV systems, including three vehicles themselves, were attacked. Control-based techniques were unable to identify stealthy attacks, which could have a major impact on the RV's mission (i.e., cause it to deviate significantly from its target) (Dash et al., 2021). Even the environment around us can be dangerous: hacking a smart home can result in physical adjustment of the home settings from switching off and on lights, playing music, controlling a remote robot (Legg et al., 2021). When discussing about ROS, any attacked ROS node can publish adulterated messages and it can easily manipulate velocity commands to misdirect a robot (Portugal et al., 2017). NAO after being attacked with DoS appears to become slow while speaking and doing tasks, changing its voice and eye color (Trabelsi et al., 2021).

Table 6
Manipulation, physical damage, stealing data, wireless jamming, spoofing and data injection as effects of attacks on robots.

Paper	Manipulation	Physical Damage	Stealing Information	Wireless Jamming	Spoofing	Data Injection
Petit and Shladover (2015)	X	X	X		X	X
Yaacoub et al. (2020)	X	X	X	X	X	X
Staffa et al. (2018)	X	X	X		X	X
Mazzeo and Staffa (2020)	X	X	X		X	X
Giaretta et al. (2018)	X	X	X		X	
Alemzadeh et al. (2016)	X	X			X	X
Quarta et al. (2017)	X	X	X		X	X
Khalid et al. (2018)	X			X	X	X
Ahmad Yousef et al. (2018)	X	X	X			X
Cornelius et al. (2018)	X	X	X		X	X
Fosch-Villaronga and Mahler (2021)	X	X				X
Vuong et al. (2014)	X					
Sabaliauskaite et al. (2017)		X				X
Pogliani et al. (2019)			X		X	X
Jain and Doriya (2019)					X	X
Guerrero-Higueras et al. (2018)					X	
Wang et al. (2021)						X
Sandoval and Thulasiraman (2019)	X	X				X

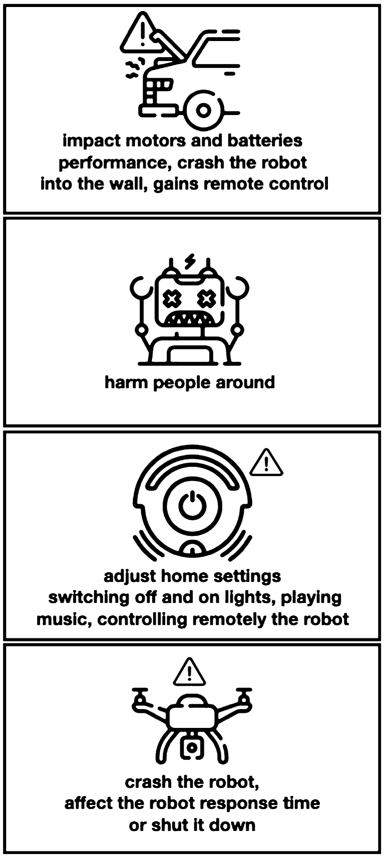
impact motors and batteries
performance, crash the robot
into the wall, gains remote control
harm people around
adjust home settings
switching off and on lights, playing
music, controlling remotely the robot
crash the robot,
affect the robot response time
or shut it down

Fig. 5. Attacks on different types of robots and their effects.

5.2. Networking

When CPSs are under attack financial and image-related losses of the user can happen (Dudek & Szynkiewicz, 2019). An attacker that successfully gains control of it can disable the Wi-Fi access to the car, severing the operator command and control communication channel (Raval et al., 2018). With humanoid robots, a physical attack toward RAVEN allows to log USB communication and forward information to an attacker located remotely (Alemzadeh et al., 2016, Bonaci et al., 2015). Peppers easily grabs login credentials, steals data stored in the robot, hacks connected devices and even physically harms humans around him (Giaretta et al., 2018). PeopleBot integrity and availability attacks also caused sensitive information on the robot to be hijacked (Ahmad Yousef et al., 2018). Real time location systems were hacked with the signal emitted by beacons thus making the tag unable to compute distances from objects and changing the signal emitted by beacons introducing errors and resulting in incorrect calculating of the tag location (Guerrero-Higueras et al., 2017).

5.3. Operating system

The author of “Security of controlled manufacturing systems in the connected factory: the case of industrial robots” mentioned that (Pogliani et al., 2019)

> “A recent Internet-wide scan performed between December 2017 and January 2018 revealed that over 100 instances of ROS master nodes are accessible from the public Internet.”

The robot operating system can be under the control of attackers when malicious operators have access to important files, passwords and can manipulate them (Pogliani et al., 2019), or when the attacker breaks into the kernel of an OS, demonstrating that it can bypass any software level access control mechanism (Cornelius et al., 2018). Therefore, attacks have the potential to leak sensitive information exchanging data also from one application to another (Cornelius et al., 2018). Table 6 summarizes the effect of attacks on robots: most attacks result in data injection and spoofing but in physical damage affecting profoundly the security of robots. When attackers access ROS, a malicious node can change both the commands and a robot behavior. According to Sandoval and Thulasiraman (2019) when a UAV is faced with a rogue node/malicious node, the rogue node the attacker can run malicious commands and can even affect the robot response time or shut it down. Android OS appears to be subject to attacks where stored information is easily manipulated during penetration testing and user personal informations could be easily accessed and retrieved, exposing to a dangerous breach (Yankson et al., 2021).

5.4. Discussion

Affecting robots is one of the important subjects of cyber security that deals with consequences of cyber security issues and shows which parts of robots are more vulnerable to attacks and need more investigation. While many research teams work on issues related to robots, trying to solve their problems, this paper illustrates that attackers can create various kinds of challenges for robots like data injection, spoofing, physical damage, and stealing information. To improve robots with

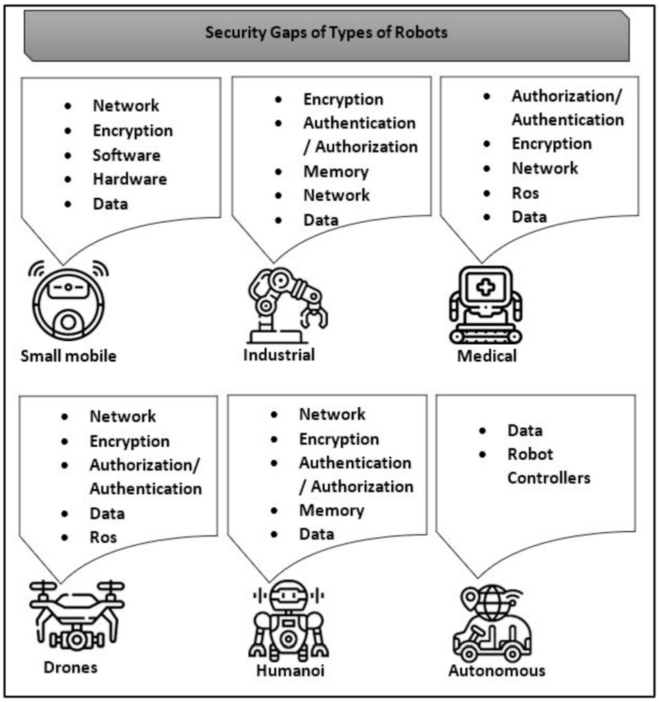

Fig. 6. Security gaps of different typologies of robots.

Table 7
Items vulnerable to cyber security threats.

Paper	Vulnerable Items			
	Data	Network	Hardware	Software
Jain and Doriya (2019)	X			X
Petit and Shladover (2015)	X	X	X	X
Wang et al. (2021)	X	X	X	
Yaacoub et al. (2020)	X	X	X	
Staffa et al. (2018)	X			
Mazzeo and Staffa (2020)	X		X	
Giaretta et al. (2018)	X	X	X	
Alemzadeh et al. (2016)		X		
Fosch-Villaronga and Mahler (2021)	X	X		
Ahmad Yousef et al. (2018)	X	X		
Khalid et al. (2018)	X	X	X	
Sabaliauskaite et al. (2017)	X			
Pogliani et al. (2019)		X	X	
Quarta et al. (2017)		X		
Cornelius et al. (2018)	X	X	X	X
Sandoval and Thulasiraman (2019)				X
Dóczi et al. (2016)		X		

respect to all mentioned weaknesses and vulnerabilities, this field of research surely needs more attention and study.

6. Security for specific types of robots

In this section, cyber security for different types of robots is reviewed and specific security gaps are depicted in Fig. 6. In recent years, robots are increasingly being used for different purposes, in different aspects of human life, as medicine, automated vehicles, national security, defense, and industry. Each robot has its own usability and according to the fields that it is employed in, its operation, tasks, and purposes are different. Therefore, some robots will be more sensitive with respect to others and in some cases, some of their components can be more critical to handle securely.

Robots-related issues must be extensively studied and investigated from different points of view. One of the major issues is represented by cyber security and reviewing their ability in the real world when they are faced with different kinds of attacks. Table 7 mentions four sensitive and vulnerable items of robots that manufacturers and scientists should pay more attention to, in order to improve security of robots. Most of the presented papers discussed integrity, availability, and confidentiality as the main target of attackers that need to be protected strongly by using different methods as depicted in Table 8. By reviewing different kinds of robots, it is obvious that although there are some methods for protecting robots from cyber attacks like encryption, authorization/authentication, and physical protections, those are simple enough to be broken and bypassed by hackers and attackers. Table 9 mentions some of the papers that refer to those methods as the critical issues of robotics cyber security that need to be investigated and improved.

Table 8
Cyber attacks against integrity, availability and confidentiality.

Paper	Threats Target		
	Integrity	Availability	Confidentiality
Jain and Doriya (2019)	X	X	
Staffa et al. (2018)	X		X
Mazzeo and Staffa (2020)	X		X
Fosch-Villaronga and Mahler (2021)	X	X	X
Pogliani et al. (2019)	X		
Quarta et al. (2017)	X		
Ahmad Yousef et al. (2018)	X	X	
Giaretta et al. (2018)		X	
Alemzadeh et al. (2016)		X	
Dóczi et al. (2016)		X	
Khalid et al. (2018)		X	
Toris et al. (2014)			X
Mukhandi et al. (2019)			X

6.1. Sensors, CPSs and small size mobile robots

Cornelius et al. (2018) introduced four main sensitive targets of attacks on mobile robots including: sensor data, hardware, software, and infrastructure. Authors showed that by hacking these vulnerabilities the attackers not only can theft important data but also can cause physical damage and psychological problem to humans (Cornelius et al., 2018). Also, increasing the efficiency of the sensing and network layers of IoT in order to improve cyber security is a critical aspect (Kumar et al., 2022).

Small size robotics is currently a fast-moving sector in the robotics field. According to Ahmad Yousef et al. (2018) the vulnerability of small sized robots is the availability of the IP address when they are connected to a network. Another issue appeared to be weak encryption for the required login credentials: username information was not strongly encrypted and the password was hashed by using vulnerable methods. Moreover, an attacker was able to connect to the robot remotely and pretend that the robot was experiencing network connection problem. Attacks as DoS and the previous ones can manipulate behavior, steal important information and have a serious impact on integrity, availability, and confidentiality of robots (Ahmad Yousef et al., 2018).

Also, Vuong et al. in their paper showed that the impact of a DoS attack on a four drive wheeled (4WD) rescue robot was remarkable on the physical aspect and the most significant effect was on robot movement and reaction time to navigation commands (Vuong et al., 2014).

In another work (McClean et al., 2013), the authors' primary goal was finding the unknown vulnerabilities in the cyber-physical systems based on the ROS framework. They mentioned “plain-text communications”, “unprotected TCP ports”, and “unencrypted data storage” as the vulnerabilities. In the same work, the researchers mentioned authentication as a critical method for reducing the risk of attacks.

The main concentration of “A comprehensive approach, and a case study, for conducting attack detection experiments in cyber physical systems” (Sabaliauskaite et al., 2017) was an attack on sensor data by false data injection, scaling and stealthy attacks that can be dangerous for robots in terms of physical damage.

Table 9
Encryption, authorization, authentication, physical protection as weak points of robots.

Paper	Reason/Lack of		
	encryption	Authorization/Authentication	Physical/Protection
Petit and Shladover (2015)	X	X	X
Yaacoub et al. (2020)	X	X	
Giaretta et al. (2018)	X	X	
Dóczi et al. (2016)	X	X	
Pogliani et al. (2019)	X	X	X
Quarta et al. (2017)	X	X	X
Khalid et al. (2018)	X	X	X
Ahmad Yousef et al. (2018)	X		
Cornelius et al. (2018)	X	X	X
Jain and Doriya (2019)		X	
Staffa et al. (2018)		X	X
Mazzeo and Staffa (2020)		X	X

6.2. *Industrial robots*

Industrial robots usually work in manufacturing sectors and have multi-axis arms to perform automated tasks (Quarta et al., 2017), a control system, an operator interface, and a hardware and software interface (Pogliani et al., 2019).

Khalid et al. (2018) divided cyber attacks of robots into two main groups: the ones coming from internal resources and the others coming from external ones. The attacks of external resources are carried out via communication channels and networks, whereas the internal attacks are the ones where the attacker has physical access to the robots and their data port by working in the near robot's environment. Some attacks are considered passive attacks since they are performed just to spy on the target, others instead aim to destroy specific part of the large scale of robots. Attacks can also be categorized in three levels, *low* as losing control for the short period, *medium* effects on sensor node efficiency, and *high* data of sensor is false (Khalid et al., 2018). The main target of attacks on industrial robots is the production process and the goal of attackers can be causing defects on the products, to damage machines or even hurt people who work around them (Quarta et al., 2017, Pogliani et al., 2019). Another possible effect of cyber security attacks on industrial robots can be halting the whole or part of the manufacture, for a long time or temporary, depending on the size and level of the target of the attackers (Quarta et al., 2017, Pogliani et al., 2019). Moreover, the attackers can have spying goal and want to steal important information and data.

An insecure network is one of the places where attackers can control industrial robots directly or in directly via the company LAN network or internet (Pogliani et al., 2019). Network connections can pose real problems for industrial robots, for example, spying file systems and exposing them may cause serious consequences (Quarta et al., 2017). As mentioned, another gap for industrial robots is their weak authentication and authorization system (Pogliani et al., 2019): in some cases no authentication system for default users is provided, while some other users can work directly with data. The consequences of all mentioned issues contribute to the ability for attackers to have access to the system (Quarta et al., 2017). It is possible that the robots are faced with physical attacks when an operator interacts with robots physically via USB devices (Pogliani et al., 2019, Quarta et al., 2017).

Simple encryption is another weak point for industrial robots, since robots need sufficient encryption in order to protect integrity and files with important information. Without it attackers can access to critical file and information and manipulate them (Quarta et al., 2017). Memory corruption is another weak point that attackers can use, for overflowing the buffer by DoS attack and either lead to remote code execution or forcing system booting (Quarta et al., 2017). The applications of robots play a critical role in their security as well, for example, injecting and executing malicious code can originate easily malicious attacks (Pogliani et al., 2019).

In a robotic delivery setup with TurtleBot3, an authentication system, which includes the client, the server and the robot, a cooperative authentication protocol is implemented and the security of the system has been formally analyzed using ProVerif proving that the setup mitigates various threats (Yang et al., 2021, Wang et al., 2022).

6.3. *Medical robots*

Robots currently used in the health field as service providers for humans play a critical role for people who work with them. Robots in fact have access to personal and sensitive data and have direct interaction with humans. Security vulnerabilities are indeed a vital issue and need significant concern, so not only manufacturers and programmers but also policy makers and everybody who is involved in this field should try to produce really reliable robots (Fosch-Villaronga & Mahler, 2021). The need of implementing security measures to increase the resilience to cyber attacks of Cloud-Based medical IoT is strongly emphasized by Gaurav et al. (2022). One of most critical issues in the medical field is the authorization process that allows to access the network and the software interface. Therefore before giving access to users and services they should be checked carefully, and all the unknown and suspect requests should be denied (Dóczi et al., 2016). Also all communications should have efficient encryption, and ROS plays an important role to reach all these goals since it handles authorization and authentication tasks (Dóczi et al., 2016).

In another paper authors (Alemzadeh et al., 2016) focused on two scenarios that may have occurred for the RAVEN II surgical robot, which was unable to identify the attacks and protect itself from them. The first scenario that caused hijacking of the robot was the result of injecting unwanted input. In this situation the robot would not be under control and behavior like jumping, halting, and unavailability were possible. The second scenario had the same consequences and was the result of injecting unintended commands to the motor torque.

6.4. *Humanoid robot*

In "Adding salt to pepper: A structured security assessment over a humanoid robot" (Giaretta et al., 2018), authors evaluated the security of Pepper, a commercial human-shaped social robot. Attackers appeared to easily retrieve the robot credentials, to login and steal or spy on sensitive data and were also able to harm humans physically. Vulnerabilities of Pepper were mostly open network ports, weak encryption, and MAC algorithms, also the humanoid robot appears to accept TCP packets from any unauthenticated source. In order to spy, hurt people, shut down and reset the robot, attackers can write a simple script and Pepper will run it without knowing the source of it (Giaretta et al., 2018).

Another well-known humanoid robot is NAO. NAO showed an obvious weakness in protecting itself against DoS attacks. An experiment

(Trabelsi et al., 2021) showed that when NAO was faced with DoS attacks it became slow in terms of speaking and doing tasks, also its voice and color of eyes changed and it appeared to look angry. NAO was not able to manage the ping requests, its engine became hot and the robot started to request to rest. Therefore NAO needs a better firewall code for protecting itself without showing issues in the robot behavior (Trabelsi et al., 2021).

For detecting spoofing and DoS attacks researchers developed a model based on the beacons of a commercial Real Time Location Systems (RTLS)s used by an autonomous robot to estimate its position, and showed that supervised learning algorithms can be used for detecting these attacks (Guerrero-Higueras et al., 2018).

Humanoid robots implement complicated operating system like ROS to interconnect hardware components. The adoption of ROS appears to be quite hard on manufacturers since it is necessary to support actuators and sensors interaction and interconnection (Mazzeo & Staffa, 2020, Staffa et al., 2018). The weak point of humanoid robots implementing ROS has been assessed (Staffa et al., 2018, Mazzeo & Staffa, 2020), mentioning that these robots are easily accessible physically and attackers can attack them by using one of current vulnerability or installing a vulnerable software, in order to access critical data for spying a target. Also, the attacker can run a script or DoS attacks to destroy a ROS node, publishing unauthorized data, harming people, or even other equipment and devices (Staffa et al., 2018, Mazzeo & Staffa, 2020). Moreover, the attacker can change the ROS entities' URIs which are stored by environmental elements. In this scenario, the attacker can easily change the address of the master node to a malicious one. Overall, although the security of ROS poses some difficulties for attackers, it is still vulnerable, and an attacker can find new bugs for destroying the confidentiality and integrity of robots, and get access to sensitive data (Mazzeo & Staffa, 2020, Staffa et al., 2018).

6.5. Drones and unmanned vehicles

Drones became common only during recent years, due to their ability to offer a remote live-stream, real-time video and image capture. On the other side their real-time wireless communication channels makes them vulnerable to a variety of cyber attacks (Yaacoub et al., 2020).

Several scenarios have been reviewed where Drone-To-Drone communication that adopts a peer to peer communication model, would make drones weak against attacks like DDoS and Sybil attacks (Yaacoub et al., 2020). Although drones use IDS to discover malicious activities and probable attacks, their adoption is not efficient enough against security threats. Moreover, all gathered data should be minimized in order to use the minimum amount of traffic possible, which would help reduce security problems. Current threats for drones are represented by being prone to spoofing and interception because of weak encryption algorithms (Yaacoub et al., 2020). Data can be captured or changed simply, malicious code can be injected. Also, by using malware infection over wireless communication, other devices like laptops and mobile phones would have access remotely to drones. Hackers also can use a vulnerability of the network for manipulating the drone behavior and sending its information or high-value cargo to wherever they want.

ROS is another crucial component for drones and should be reinforced to protect them from attacks. ROS has a weak authorization procedure, a weak authentication system, and also connecting to a ROS node is easy for injecting false or malicious data (Lee et al., 2021). All mentioned vulnerabilities let attacker control or destroy drones easily. ROS2 and its Data Distribution Service (DDS) security architecture can be useful for protecting drones especially against injecting unauthorized data and accessing services (Sandoval & Thulasiraman, 2019).

Some reasons for all mentioned attacks are linked to problems in designing and testing phase, in fact there is no strict policy for authorization and authentication (Yaacoub et al., 2020). Also, they noted that there is a requirement for controlling drones manually by disconnecting or turning them off, since they do not have enough methods for protecting themselves from probable attacks. Authors believe that drones suffering from vulnerable encryption, and their limited frequency would make them weak.

6.6. Autonomous robots

A cyber attack on automated vehicles probably would target the information source for knowing the location of the vehicles and its route (Petit & Shladover, 2015). In this scenario, the software of the vehicle plays a critical role in terms of protecting it. On the other side, sensors are key component of robots, and attackers can prevent them from sending information out to confuse the robot. Hackers can provide false information and send it to the robot's controller and the consequence of these attacks would range from wrong decision to physical damages (Wang et al., 2021). The most successful attacks on autonomous vehicles were performed using blinding cameras and spoofing or jamming of GPS (Petit & Shladover, 2015). In terms of successful attack, other minor threats were related to electromagnetic pulse, map poisoning, radar confusion, lidar confusion, infection of in-vehicle devices, and manipulation of in-vehicle sensors. The attacks with a higher success rate are related to injection of false safety messages and malicious map, followed by DoS attacks, where the system would be unable to process due to overloading messages (Petit & Shladover, 2015).

7. Cyber security for robot applications

Many different applications for robots are available today and it is important to consider security implications for each application and robot category. For instance, looking at application field of (Yaacoub et al., 2021) specific considerations for each category are necessary, as reported below.

- Agriculture robots mainly perform tasks outdoor and can be easily physically attacked, so they should be protected with a physical shield, and physical buttons and controls should be covered or even hidden. Most robots in this field are drones which are quite exposed to vulnerabilities as mention in Subsection 6.5 and can be very easily exploited.
- Industrial robots can potentially be a threat to humans surrounding them in factories. Robots can be physically as well as remotely attacked causing damages to the working environment as well as to people interacting with them.
- In the medical field, robots are often exposed to unwanted input injection resulting in behavior like jumping, halting, and being unavailable. This possible outcome, result of network attacks, is quite critical if the scenario where it takes place is like a hospital or an ambulance.
- Military field and police robots on the other hand can easily be attacked over the network so encryption is a necessary solution to preserve data and allow forensic to be performed and lives to be saved.
- Disaster field robots are more susceptible of wireless jamming robotic communications and of network attacks in general. On the other hand, it is crucial to have a clear communication with whoever is piloting a drone saving lives in an emergency.

8. Open challenges

In this section open challenges for robot cyber security are presented. There are in fact, available tools and technologies not covered enough by previous sections that can guarantee higher levels of security when robots are involved with people. Fig. 7 named these topics and their main goal in the robotic field. Trust in a robot for example, can lead to the disclosure of personal information to it and the acceptance of its recommendations (Aroyo et al., 2018). Furthermore, trust

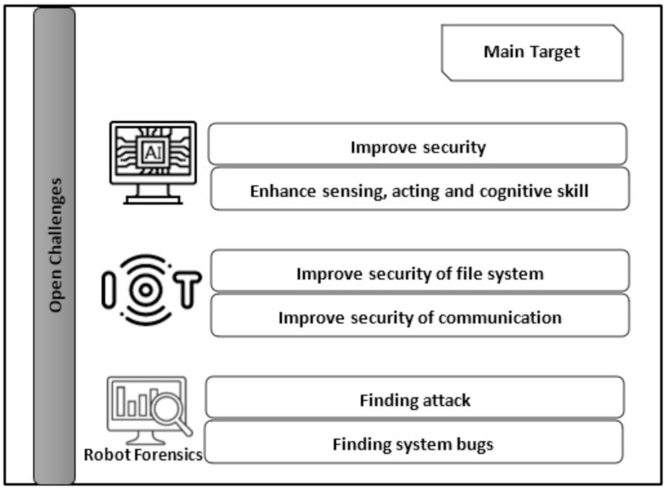
Main Target
Open Challenges
Improve security
Enhance sensing, acting and cognitive skill
Improve security of file system
Improve security of communication
Finding attack
Finding system bugs
Robot Forensics

Fig. 7. Novel approaches in the field of cyber security.

and cooperation can develop quickly during an interaction often considering the influence that a robot displaying emotional behaviors has when persuading people (Saunderson & Nejat, 2022).

8.1. Artificial Intelligence and Machine Learning

The main goal of Artificial Intelligence (AI) in the robotic field is increasing its performance in terms of scalability, flexibility, and robustness to failures also enhancing the sensing, acting skills, and cognitive capabilities of robotics devices (Dutta & Zielińska, 2021).

The power of AI has been proved in different fields. Intelligent solutions for cyber security should have the ability to protect systems from complicated attacks which probably will have different kinds of targets (He et al., 2020). Component should be integrated into the architecture of Robots and Autonomous Systems (RAS) in order to make self-learning and the autonomous ability for the systems and RAS should be accurate, reduce false alarm's rate and detect unknown attacks (He et al., 2020). The adaptive IDS are also needed for facing attack techniques progress and changes and they could passively operate at the network level to prevent impact on RAS (He et al., 2020). Recently, network intrusion detection systems are adopting ML: labeled data is crucial to the supervised learning process and harder to implement while unsupervised learning frequently produces unsatisfactory results. To overcome these issues in a cloud-based robotic system, a unique fuzziness-based semi-supervised learning strategy via ensemble learning has been used (Gao et al., 2018). Offloading the endless and constant task of intrusion detection to a cloud-based solution based on deep learning can potentially lift resource-constrained mobile devices from the task (Loukas et al., 2018).

8.2. Internet of Robotic Things and Cloud Computing

Last years developments in the field of robotics, IoT, and cloud computing can not be ignored (Horton et al., 2017). Cloud Robotics in fact, has indeed become a new important trend in the IoT and Cloud Computing research field. Researchers (Botta et al., 2019, 2021, Stanco et al., 2020) for example, proposed the use of Dew Computing and the term Dew Robotics for this aim. The architecture allows to satisfy the requirements of modern robots, exploiting Cloud and fog infrastructures when possible, and relying on local computation for important tasks that cannot be offloaded or may be offloaded but with a decrease of the overall system performance.

In order to provide a combined set of security best practices for robotic file systems and communications, it is needed to examine and enhance the security between IoT-enabled robots especially in the field of TurtleBots, and the cloud infrastructure for supporting them (Horton et al., 2017). In the communication between robots and clouds, there are several vulnerabilities during the authentication caused mainly by DoS, spoofing attacks or attackers able to find user passwords (Jain & Doriya, 2019). A secure mutual authentication scheme between robots and cloud servers using elliptic curve encryption with key agreement has been presented as a defense mechanism against these attacks for robots that access cloud resources (Jain et al., 2021). Moreover, robot operating systems suffer from vulnerabilities as communication between authorization nodes, unauthorized data access, injection of data without authorization, false information injection, and having unauthorized nodes (Jain & Doriya, 2019).

8.2.1. Robot forensics

Along with the increasing usage of robots, cybercrime-related to them is already growing. Robots will be targets of hackers more and more and therefore, forensics investigations appear to be an important topic to investigate. Although there are some studies about for ROS forensics, a particular methodology or a standard for robot forensics has not been defined, yet.

Some challenges about the ROS include real-time investigation because of communication between the robot components and ROS which add some additional data during this process (Abeykoon & Feng, 2019). A novel challenge for investigators is to acquire accurate evidence from ROS. Moreover, ROS can keep and save a huge amount of data that is difficult for investigators to gain through the network. Also, if researchers want to have a ROS device in their lab, the size of the robot, poses a new challenge when the robot has a bigger size or human form (Abeykoon & Feng, 2019). Having a huge amount of data during analyzing and evaluating of ROS forensics poses a challenge for investigators (Abeykoon & Feng, 2017). The Forensic Toolkit Imager tool, which is a platform for digital investigations can be used for getting access to digital media and helping to reduce the analyses time of evidence of an investigation (Abeykoon & Feng, 2017). In another study about ROS (Basheer & Varol, 2019), authors presented an overview on “Robot Operating System Forensics”, and mentioned some results. One of the issues that the paper refers to is the difficulty of separating the effect of system bugs from ongoing attacks since forensic goal is to identify possible attacks and their consequences. Authors also mentioned issues about performing memory acquisition in ROS systems. A study about “further uttered ROS investigation, where they also applied volatile memory forensics for ROS” is carried out (Basheer & Varol, 2019), moreover a review of papers that studied ROS security is presented in order to answer questions as “if ROS instances are connected to the internet, will they be secure?”

8.3. Discussion

Robots-related issues must be extensively studied and investigated from different points of view. One of the important issues of robots is their cyber security and reviewing their ability in the real world when they are faced with different kinds of attacks. The network layer is one of the most attacked by malicious users, and data should be protected from stealing, manipulating, and spying. Also hacking both robots' software and hardware could be very harmful from a security perspective. Robots' hardware can be expensive and complicated so the consequence of harming them can be irreparable in some situations and from some aspects. Table 7 mentioned four sensitive and vulnerable items of robots that manufactures and scientists should pay more attention to, in order to improve robots security.

Most of the papers discussed Integrity, Availability, and Confidentiality as the main target of attackers and robots should be strongly protected from them by using different methods. The consequence of attacking robot integrity, availability, and confidentiality can make serious to low risks for robots according to attacks domain and target, like manipulating the robot behavior, stealing it, spying sensitive information, physical damage, injecting false data, and so on. Table 8 depicted some of them.

By reviewing literature some methods for protecting robots from cyber attacks are encryption, Authorization/Authentication, and Physical protection. By overcoming the mentioned challenges of these methods the robot performance can be increased in various aspects. Table 9 mentioned some of the papers that refer to those methods as the critical issues of robotics cyber security that need to be investigated and improved.

9. Conclusions

The amount of robots in different fields has grown day by day and they have become an integral part of our daily lives. While they continue to evolve and become more sophisticated, cyber security risks associated with them have also increased, having serious consequences from financial problems to losing human life.

In this paper, the cyber security of robots was reviewed from several aspects. By analyzing the existing attacks and risks for the platform of robots, in three important parts of robots including operating systems, networks, and physical, in order to tackle the consequence of them. It has been found that the methods of authentication, authorization, encryption and physical protection should be improved in order to reduce spying on information, unwanted access to robots, even injecting and installing unknowing data and software, and so on.

For keeping integrity, availability, and confidentiality under protection, three layers of robots, namely operating systems, networks, and physical were studied during the current paper. Analysis showed that machine learning, statistical methods and pattern recognition are the common techniques and strategies for detecting attacks and their consequences. Attacks on robots can have significant consequences, they can manipulate and affect robots functioning and cause harm to humans and the environment. Hence it is crucial to know their effects of them. Our work showed that prevalent ones are manipulating the behavior of robots, physical damage, stealing information, wireless jamming, spoofing and espionage, and manipulating the data.

Another important subject that has been investigated in this work is studying robots in the real world, in order to make a clear attitude about the weaknesses and vulnerabilities of robots. It is important to ensure that they are secure and free from cyber threats. Therefore, in this paper, we mentioned some important topics which are highly recommended for protecting robots and keeping them safe which are yet to be covered enough.

We gave a baseline for future works and researchers to start building new defensive mechanisms for securing robots, presenting open challenges as artificial intelligence in robotics, cloud robotics and robot forensics. AI should be explored thoroughly since it is increasing robots performance in terms of scalability, flexibility, and robustness to failures also enhancing the sensing, acting skills, and cognitive capabilities of robotics devices. Cloud Robotics also is a paradigm to investigate since it has indeed become a new important trend in the IoT and Cloud Computing research field. Lastly since robots will be targets of hackers more and more, forensics investigations applied to robots appear to be an important topic to explore in the next future. We believe that this paper sheds lights on robot cyber security, which is a topic of paramount importance in current and future scenarios.

CRediT authorship contribution statement

Alessio Botta: Conceptualization, Writing – review & editing. **Sayna Rotbei:** Methodology, Writing – original draft. **Stefania Zinno:** Writing – original draft, Writing – review & editing. **Giorgio Ventre:** Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

Abeykoon, I., & Feng, X. (2017). A forensic investigation of the robot operating system. 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)* (pp. 851–857).

Abeykoon, I., & Feng, X. (2019). Challenges in ros forensics. In *2019 IEEE SmartWorld, ubiquitous intelligence computing, advanced trusted computing, scalable computing communications, cloud big data computing, Internet of People and smart city innovation* (pp. 1677–1682).

Ahmad Yousef, K. M., AlMajali, A., Ghalyon, S. A., Dweik, W., & Mohd, B. J. (2018). Analyzing cyber-physical threats on robotic platforms. *Sensors*, *18*. https://doi.org/10.3390/s18051643.

Alemzadeh, H., Chen, D., Li, X., Kesavadas, T., Kalbarczyk, Z. T., & Iyer, R. K. (2016). Targeted attacks on teleoperated surgical robots: Dynamic model-based detection and mitigation. In *2016 46th annual IEEE/IFIP international conference on dependable systems and networks (DSN)* (pp. 395–406).

Amini, R., Sulaiman, R., & Kurais, A. H. A. R. (2018). Cryptoros: A secure communication architecture for ros-based applications. *International Journal of Advanced Computer Science and Applications*, *9*. https://doi.org/10.14569/IJACSA.2018.091022.

Aroyo, A. M., Rea, F., Sandini, G., & Sciutti, A. (2018). Trust and social engineering in human robot interaction: Will a robot make you disclose sensitive information, conform to its recommendations or gamble? *IEEE Robotics and Automation Letters*, *3*, 3701–3708. https://doi.org/10.1109/LRA.2018.2856272.

Balsa-Comerón, J., Guerrero-Higueras, Á. M., Rodríguez-Lera, F. J., Fernández-Llamas, C., & Matellán-Olivera, V. (2018). Cybersecurity in autonomous systems: Hardening ros using encrypted communications and semantic rules. In A. Ollero, A. Sanfeliu, L. Montano, N. Lau, & C. Cardeira (Eds.), *ROBOT 2017: Third Iberian robotics conference* (pp. 67–78). Cham: Springer International Publishing.

Basheer, M. M., & Varol, A. (2019). An overview of robot operating system forensics. In *2019 1st international informatics and software engineering conference (UBMYK)* (pp. 1–4).

Bezemskij, A., Loukas, G., Gan, D., & Anthony, R. J. (2017). 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)* (pp. 98–103).

Bonaci, T., Herron, J., Yusuf, T., Yan, J., Kohno, T., & Chizeck, H. J. (2015). To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots. arXiv:1504.04339.

Botta, A., Cacace, J., De Vivo, R., Siciliano, B., & Ventre, G. (2021). Networking for cloud robotics: The DewROS platform and its application. *Journal of Sensor and Actuator Networks*, *10*. https://doi.org/10.3390/jsan10020034.

Botta, A., Gallo, L., & Ventre, G. (2019). Cloud, fog, and dew robotics: Architectures for next generation applications. In *2019 7th IEEE international conference on mobile cloud computing, services, and engineering (MobileCloud)* (pp. 16–23).

Breiling, B., Dieber, B., Pinzger, M., & Rass, S. (2021). A cryptography-powered infrastructure to ensure the integrity of robot workflows. *Journal of Cybersecurity and Privacy*, *1*, 93–118. https://doi.org/10.3390/jcp1010006.

Breiling, B., Dieber, B., & Schartner, P. (2017). Secure communication for the robot operating system. In *2017 annual IEEE international systems conference (SysCon)* (pp. 1–6).

Caiazza, G., White, R., & Cortesi, A. (2019). *Enhancing security in ROS*. Singapore: Springer Singapore (pp. 3–15). Chapter vol. 883.

Chauhan, M. A., Babar, M. A., & Grainger, S. (2021). Designing a security platform for collaborating autonomous systems - an experience report. In *2021 IEEE 18th international conference on software architecture companion (ICSA-C)* (pp. 1–7).

Chen, H., He, H., & Starr, A. (2020). An overview of web robots detection techniques. In *2020 international conference on cyber security and protection of digital services (Cyber Security)* (pp. 1–6).

Cornelius, G., Caire, P., Hochgeschwender, N., Olivares-Mendez, M. A., Esteves-Verissimo, P., Völp, M., & Voos, H. (2018). A perspective of security for mobile service robots. In A. Ollero, A. Sanfeliu, L. Montano, N. Lau, & C. Cardeira (Eds.), *ROBOT 2017: Third Iberian robotics conference* (pp. 88–100). Cham: Springer International Publishing.

Cottrell, K., Bose, D. B., Shahriar, H., & Rahman, A. (2021). An empirical study of vulnerabilities in robotics. In *2021 IEEE 45th annual computers, software, and applications conference (COMPSAC)* (pp. 735–744).

Dash, P., Karimibiuki, M., & Pattabiraman, K. (2021). Stealthy attacks against robotic vehicles protected by control-based intrusion detection techniques. *Digital Threats: Research and Practice*, *2*. https://doi.org/10.1145/3419474.

DeMarinis, N., Tellex, S., Kemerlis, V. P., Konidaris, G., & Fonseca, R. (2019). Scanning the internet for ros: A view of security in robotics research. In *2019 international conference on robotics and automation (ICRA)* (pp. 8514–8521).

Dieber, B., Breiling, B., Taurer, S., Kacianka, S., Rass, S., & Schartner, P. (2017). Security for the robot operating system. *Robotics and Autonomous Systems*, *98*, 192–203. https://doi.org/10.1016/j.robot.2017.09.017.

Dieber, B., Kacianka, S., Rass, S., & Schartner, P. (2016). Application-level security for ros-based applications. In *2016 IEEE/RSJ international conference on intelligent robots and systems (IROS)* (pp. 4477–4482).

Dieber, B., White, R., Taurer, S., Breiling, B., Caiazza, G., Christensen, H., & Cortesi, A. (2020). *Penetration testing ROS*. Cham: Springer International Publishing (pp. 183–225). Chapter Volume 4.

Dóczi, R., Kis, F., Sütő, B., Póser, V., Kronreif, G., Jósvai, E., & Kozlovszky, M. (2016). Increasing ros 1.x communication security for medical surgery robot. In *2016 IEEE international conference on systems, man, and cybernetics (SMC)* (pp. 004444–004449).

Dudek, W., & Szynkiewicz, W. (2019). Cyber-security for mobile service robots – challenges for cyber-physical system safety. *Journal of Telecommunications and Information Technology*, *2*, 29–36. https://doi.org/10.26636/jtit.2019.131019.

Dutta, V., & Zielińska, T. (2021). Cybersecurity of robotic systems: Leading challenges and robotic system design methodology. *Electronics*, *10*. https://doi.org/10.3390/electronics10222850.

Elfar, M., Zhu, H., Raghunathan, A., Tay, Y. Y., Wubbenhorst, J., Cummings, M. L., & Pajic, M. (2017). Wip abstract: Platform for security-aware design of human-on-the-loop cyber-physical systems. In *2017 ACM/IEEE 8th international conference on cyber-physical systems (ICCPS)* (pp. 93–94).

Fernandez, J., Allen, B., Thulasiraman, P., & Bingham, B. (2020). Performance study of the robot operating system 2 with qos and cyber security settings. In *2020 IEEE international systems conference (SysCon)* (pp. 1–6).

Fosch-Villaronga, E., & Mahler, T. (2021). Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Computer Law & Security Review*, *41*, Article 105528. https://doi.org/10.1016/j.clsr.2021.105528.

Gao, Y., Liu, Y., Jin, Y., Chen, J., & Wu, H. (2018). A novel semi-supervised learning approach for network intrusion detection on cloud-based robotic system. *IEEE Access*, *6*, 50927–50938. https://doi.org/10.1109/ACCESS.2018.2868171.

Gaurav, A., Psannis, K., & Peraković, D. (2022). Security of cloud-based Medical Internet of Things (MIoTs). *International Journal of Software Science and Computational Intelligence*, *14*, 1–16. https://doi.org/10.4018/IJSSCI.285593.

Giaretta, A., De Donno, M., & Dragoni, N. (2018). Adding salt to pepper: A structured security assessment over a humanoid robot. In *Proceedings of the 13th international conference on availability, reliability and security* (pp. 1–8). New York, NY, USA: Association for Computing Machinery.

Goerke, N., Timmermann, D., & Baumgart, I. (2021). Who controls your robot? An evaluation of ros security mechanisms. In *2021 7th international conference on automation, robotics and applications (ICARA)* (pp. 60–66).

Gorbenko, A., & Popov, V. (2020). 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)* (pp. 1–6).

Guerrero-Higueras, Á. M., DeCastro-García, N., & Matellán, V. (2018). Detection of cyber-attacks to indoor real time localization systems for autonomous robots. *Robotics and Autonomous Systems*, *99*, 75–83. https://doi.org/10.1016/j.robot.2017.10.006.

Guerrero-Higueras, Á. M., DeCastro-García, N., Rodríguez-Lera, F. J., & Matellán, V. (2017). Empirical analysis of cyber-attacks to an indoor real time localization system for autonomous robots. *Computers & Security*, *70*, 422–435. https://doi.org/10.1016/j.cose.2017.06.013.

Guiochet, J., Machin, M., & Waeselynck, H. (2017). Safety-critical advanced robots: A survey. *Robotics and Autonomous Systems*, *94*, 43–52. https://doi.org/10.1016/j.robot.2017.04.004.

He, H., Gray, J., Cangelosi, A., Meng, Q., McGinnity, T. M., & Mehnen, J. (2020). The challenges and opportunities of artificial intelligence for trustworthy robots and autonomous systems. In *2020 3rd international conference on intelligent robotic and control engineering (IRCE)* (pp. 68–74).

Hochgeschwender, N., Cornelius, G., & Voos, H. (2019). Arguing security of autonomous robots. In *2019 IEEE/RSJ international conference on intelligent robots and systems (IROS)* (pp. 7791–7797).

Horton, M., Chen, L., & Samanta, B. (2017). Enhancing the security of iot enabled robotics: Protecting turtlebot file system and communication. In *2017 international conference on computing, networking and communications (ICNC)* (pp. 662–666).

Huang, J., Erdogan, C., Zhang, Y., Moore, B., Luo, Q., Sundaresan, A., & Rosu, G. (2014). Rosrv: Runtime verification for robots. In B. Bonakdarpour, & S. A. Smolka (Eds.), *Runtime verification* (pp. 247–254). Cham: Springer International Publishing.

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, *4*, 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172.

Hussain, M., & Beg, M. (2019). Using vehicles as fog infrastructures for transportation cyber-physical systems (t-cps): Fog computing for vehicular networks. *International Journal of Software Science and Computational Intelligence*, *11*, 47–69. https://doi.org/10.4018/IJSSCI.2019010104.

Jain, S., & Doriya, R. (2019). Security issues and solutions in cloud robotics: A survey. In M. Prateek, D. Sharma, R. Tiwari, R. Sharma, K. Kumar, & N. Kumar (Eds.), *Next generation computing technologies on computational intelligence* (pp. 64–76). Singapore: Springer Singapore.

Jain, S., Nandhini, C., & Doriya, R. (2021). ECC-based authentication scheme for cloud-based robots. *Wireless Personal Communications*, *117*, 1557–1576. https://doi.org/10.1007/s11277-020-07935-6.

Jujjuri, R., Tripathi, A. K., V. S., C., Majji, S., Prathap, B. R., & Patnala, T. R. (2022). Detection of cyber crime based on facial pattern enhancement using machine learning and image processing techniques. In *Using computational intelligence for the dark web and illicit behavior detection* (pp. 150–165).

Khalid, A., Kirisci, P., Khan, Z. H., Ghrairi, Z., Thoben, K. D., & Pannek, J. (2018). Security framework for industrial collaborative robotic cyber-physical systems. *Computers in Industry*, *97*, 132–145. https://doi.org/10.1016/j.compind.2018.02.009.

Kumar, A., Rahmath, M., Raju, Y., Reddy Vulapula, S., Prathap, B. R., Hassan, M. M., Mohamed, M. A., & Asakipaam, S. A. (2022). Enhanced secure technique for detecting cyber attacks using artificial intelligence and optimal IoT. *Security and Communication Networks*, *2022*, Article 8024518. https://doi.org/10.1155/2022/8024518.

Lee, H., Yoon, J., Jang, M. S., & Park, K. J. (2021). A robot operating system framework for secure uav communications. *Sensors*, *21*. https://doi.org/10.3390/s21041369.

Legg, P., Higgs, T., Spruhan, P., White, J., & Johnson, I. (2021). "Hacking an IoT home": New opportunities for cyber security education combining remote learning with cyber-physical systems. In *2021 international conference on cyber situational awareness, data analytics and assessment (CyberSA)* (pp. 1–4).

Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., & Gan, D. (2018). Cloud-based cyber-physical intrusion detection for vehicles using deep learning. *IEEE Access*, *6*, 3491–3508. https://doi.org/10.1109/ACCESS.2017.2782159.

Martín, F., Soriano, E., & Cañas, J. M. (2018). Quantitative analysis of security in distributed robotic frameworks. *Robotics and Autonomous Systems*, *100*, 95–107. https://doi.org/10.1016/j.robot.2017.11.002.

Mazzeo, G., & Staffa, M. (2020). TROS: Protecting humanoids ROS from privileged attackers. *International Journal of Social Robotics*, *12*, 827–841. https://doi.org/10.1007/s12369-019-00581-4.

McClean, J., Stull, C., Farrar, C., & Mascarenas, D. (2013). A preliminary cyber-physical security assessment of the robot operating system (ros). In *Unmanned systems technology XV* (pp. 341–348). SPIE.

Mishra, A., Gupta, B. B., Peraković, D., Peñalvo, F. J. G., & Hsu, C. H. (2021). Classification based machine learning for detection of ddos attack in cloud computing. In *2021 IEEE international conference on consumer electronics (ICCE)* (pp. 1–4). IEEE.

Mitchell, R., & Chen, I. R. (2014). A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys*, *46*. https://doi.org/10.1145/2542049.

Mukhandi, M., Portugal, D., Pereira, S., & Couceiro, M. S. (2019). A novel solution for securing robot communications based on the mqtt protocol and ros. In *2019 IEEE/SICE international symposium on system integration (SII)* (pp. 608–613).

Olivato, M., Cotugno, O., Brigato, L., Bloisi, D., Farinelli, A., & Iocchi, L. (2019). A comparative analysis on the use of autoencoders for robot security anomaly detection. In *2019 IEEE/RSJ international conference on intelligent robots and systems (IROS)* (pp. 984–989).

Pan, X., Yamaguchi, S., Kageyama, T., & Kamilin, M. H. B. (2022). Machine-learning-based white-hat worm launcher in botnet defense system. *International Journal of Software Science and Computational Intelligence*, *14*, 1–14.

Petit, J., & Shladover, S. E. (2015). Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *16*, 546–556. https://doi.org/10.1109/TITS.2014.2342271.

Pogliani, M., Quarta, D., Polino, M., Vittone, M., Maggi, F., & Zanero, S. (2019). Security of controlled manufacturing systems in the connected factory: The case of industrial robots. *Journal of Computer Virology and Hacking Techniques*, *15*, 161–175. https://doi.org/10.1007/s11416-019-00329-8.

Portugal, D., Pereira, S., & Couceiro, M. S. (2017). The role of security in human-robot shared environments: A case study in ros-based surveillance robots. In *2017 26th IEEE international symposium on robot and human interactive communication (RO-MAN)* (pp. 981–986).

Prathap, B. R. (2022). Chapter 7 - Geospatial crime analysis and forecasting with machine learning techniques. In R. Pandey, S. K. Khatri, N. kumar Singh, & P. Verma (Eds.), *Artificial intelligence and machine learning for EDGE computing* (pp. 87–102). Academic Press.

Pu, H., He, L., Zhao, C., Yau, D. K. Y., Cheng, P., & Chen, J. (2021). Fingerprinting movements of industrial robots for replay attack detection. *IEEE Transactions on Mobile Computing*, 1. https://doi.org/10.1109/TMC.2021.3059796.

Quarta, D., Pogliani, M., Polino, M., Maggi, F., Zanchettin, A. M., & Zanero, S. (2017). An experimental security analysis of an industrial robot controller. In *2017 IEEE symposium on security and privacy (SP)* (pp. 268–286).

Rajasegarar, S., Leckie, C., & Palaniswami, M. (2008). Anomaly detection in wireless sensor networks. *IEEE Wireless Communications*, *15*, 34–40. https://doi.org/10.1109/MWC.2008.4599219.

Raval, R., Maskus, A., Saltmiras, B., Dunn, M., Hawrylak, P. J., & Hale, J. (2018). Competitive learning environment for cyber-physical system security experimentation. In *2018 1st international conference on data intelligence and security (ICDIS)* (pp. 211–218).

Rivera, S., Iannillo, A. K., Lagraa, S., Joly, C., & State, R. (2020). Ros-fm: Fast monitoring for the robotic operating system(ros). In *2020 25th international conference on engineering of complex computer systems (ICECCS)* (pp. 187–196).

Rivera, S., Lagraa, S., Nita-Rotaru, C., Becker, S., & State, R. (2019). Ros-defender: Sdn-based security policy enforcement for robotic applications. In *2019 IEEE security and privacy workshops (SPW)* (pp. 114–119).

Rivera, S., Lagraa, S., & State, R. (2019). Rosploit: Cybersecurity tool for ros. In *2019 third IEEE international conference on robotic computing (IRC)* (pp. 415–416).

Rivera, S., & State, R. (2021). 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)* (pp. 754–759).

Rocchetto, M., & Tippenhauer, N. O. (2016). On attacker models and profiles for cyber-physical systems. In *European symposium on research in computer security* (pp. 427–449). Springer.

Sabaliauskaite, G., Ng, G. S., Ruths, J., & Mathur, A. P. (2016). Empirical assessment of methods to detect cyber attacks on a robot. In *2016 IEEE 17th international symposium on high assurance systems engineering (HASE)* (pp. 248–251).

Sabaliauskaite, G., Ng, G., Ruths, J., & Mathur, A. (2017). A comprehensive approach, and a case study, for conducting attack detection experiments in cyber–physical systems. *Robotics and Autonomous Systems*, *98*, 174–191. https://doi.org/10.1016/j.robot.2017.09.018.

Sandoval, S., & Thulasiraman, P. (2019). Cyber security assessment of the robot operating system 2 for aerial networks. In *2019 IEEE international systems conference (SysCon)* (pp. 1–8).

Saunderson, S., & Nejat, G. (2022). Investigating strategies for robot persuasion in social human–robot interaction. *IEEE Transactions on Cybernetics*, *52*, 641–653. https://doi.org/10.1109/TCYB.2020.2987463.

Singh, A., & Gupta, B. B. (2022). Distributed Denial-of-Service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms. *International Journal on Semantic Web and Information Systems*, *18*, 1–43. https://doi.org/10.4018/IJSWIS.297143.

Soe, Y. N., Feng, Y., Santosa, P. I., Hartanto, R., & Sakurai, K. (2020). Towards a lightweight detection system for cyber attacks in the iot environment using corresponding features. *Electronics*, *9*. https://doi.org/10.3390/electronics9010144.

Staffa, M., Mazzeo, G., & Sgaglione, L. (2018). Hardening ros via hardware-assisted trusted execution environment. In *2018 27th IEEE international symposium on robot and human interactive communication (RO-MAN)* (pp. 491–494).

Stanco, G., Botta, A., & Ventre, G. (2020). Dewros: A platform for informed dew robotics in ros. In *2020 8th IEEE international conference on mobile cloud computing, services, and engineering (MobileCloud)* (pp. 9–16).

Teixeira, R. R., Maurell, I. P., & Drews, P. L. (2020). Security on ros: Analyzing and exploiting vulnerabilities of ros-based systems. In *2020 Latin American robotics symposium (LARS), 2020 Brazilian symposium on robotics (SBR) and 2020 workshop on robotics in education (WRE)* (pp. 1–6).

Toris, R., Shue, C., & Chernova, S. (2014). Message authentication codes for secure remote non-native client connections to ros enabled robots. In *2014 IEEE international conference on technologies for practical robot applications (TePRA)* (pp. 1–6).

Trabelsi, Z., Alnajjar, F., Aljaberi, M., Aldhaheri, S., Alkhateri, H., & Alkhateri, F. (2021). Robot security education: Hands-on lab activities based teaching approach. In W. Lepuschitz, M. Merdan, G. Koppensteiner, R. Balogh, & D. Obdržálek (Eds.), *Robotics in education* (pp. 61–75). Cham: Springer International Publishing.

Vuong, T., Filippoupolitis, A., Loukas, G., & Gan, D. (2014). Physical indicators of cyber attacks against a rescue robot. In *2014 IEEE international conference on pervasive computing and communication workshops (PERCOM WORKSHOPS)* (pp. 338–343).

Wang, W., Gope, P., & Cheng, Y. (2022). An AI-driven secure and intelligent robotic delivery system. *IEEE Transactions on Engineering Management*, 1–16. https://doi.org/10.1109/TEM.2022.3142282.

Wang, C., Tok, Y. C., Poolat, R., Chattopadhyay, S., & Elara, M. R. (2021). How to secure autonomous mobile robots? An approach with fuzzing, detection and mitigation. *Journal of Systems Architecture*, *112*, Article 101838. https://doi.org/10.1016/j.sysarc.2020.101838.

White, R., Caiazza, G., Christensen, H., & Cortesi, A. (2019). *SROS1: Using and developing secure ROS1 systems*. Cham: Springer International Publishing (pp. 373–405). Chapter Volume 3.

Xu, Z., & Zhu, Q. (2018). Cross-layer secure and resilient control of delay-sensitive networked robot operating systems. In *2018 IEEE conference on control technology and applications (CCTA)* (pp. 1712–1717).

Yaacoub, J. P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*, *11*, Article 100218. https://doi.org/10.1016/j.iot.2020.100218.

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*. https://doi.org/10.1007/s10207-021-00545-8.

Yang, J., Gope, P., Cheng, Y., & Sun, L. (2021). Design, analysis and implementation of a smart next generation secure shipping infrastructure using autonomous robot. *Computer Networks*, *187*, Article 107779. https://doi.org/10.1016/j.comnet.2020.107779.

Yankson, B., K, J. V., Hung, P. C. K., Iqbal, F., & Ali, L. (2021). Security assessment for zenbo robot using drozer and mobsf frameworks. In *2021 11th IFIP international conference on new technologies, mobility and security (NTMS)* (pp. 1–7).

Zhao, X., Shu, S., Lan, Y., Feng, H., & Dong, W. (2020). Security controller synthesis for ros-based robot. In *2020 IEEE 20th international conference on software quality, reliability and security companion (QRS-C)* (pp. 472–477).

Zhou, Y., Xie, L., & Pan, H. (2022). Research on a PSO-H-SVM-based intrusion detection method for industrial robotic arms. *Applied Sciences*, *12*. https://doi.org/10.3390/app12062765.