International Journal of Safety and Security Engineering
Vol. 13, No. 3, June, 2023, pp. 555-563
Journal homepage: http://iieta.org/journals/ijsse

Security Vulnerabilities and Threats in Robotic Systems: A Comprehensive Review

Mustafa Salah Abed[1*], Qusay F. Al-Doori[1], Afrah Thamer Abdullah[2], Azhaar Akram Abdallah[3]

[1] Department of Control and Systems Engineering, University of Technology-Iraq, Baghdad 10066, Iraq
[2] Department of Electrical Engineering, Mustansiriyah University, Baghdad 14022, Iraq
[3] Department of Computer Sciences, University of Technology-Iraq, Baghdad 10066, Iraq

Corresponding Author Email: cse.19.07@grad.uotechnology.edu.iq

https://doi.org/10.18280/ijsse.130318

Received: 28 March 2023
Accepted: 1 July 2023

Keywords:
attacker, communication system, cyber security, robotic systems, physical system, security vulnerabilities, threats

ABSTRACT

The recent digital revolution has resulted in robots being integrated more than ever into various domains, such as agriculture, healthcare, and the military. Robots are dedicated to serving, facilitating, and improving human life. However, the growing prevalence of robotics has brought to light the need for robust security measures. While unintentional accidents are inevitable, this paper focuses on the increasingly challenging problem of malicious cyber-attacks against robotic systems. One specific incident highlighting the severity of this issue occurred in 2022 when a healthcare robot was hacked, resulting in the misadministration of medication to several patients, leading to severe health complications and unnecessary loss of human lives. Such instances underscore the urgency of understanding the robotics domain's security vulnerabilities, threats, and consequences. In conclusion, this paper highlights the critical aspects of securing robotic systems in today's technologically advanced world. By identifying and analyzing the primary security vulnerabilities, this paper examines the primary security vulnerabilities, the type of application, then the impact of vulnerabilities; we can pave the way for effective security measures and ultimately ensure the safety and reliability of robotic systems.

1. INTRODUCTION

Due to the digital revolution, the evolution of machines, the adoption of artificial intelligence, and the COVID-19 pandemic, intelligent robots have been used to perform various daily tasks [1, 2].

This growth in robotics has also led to the emergence of the Internet of Robotic Things (IoRT) concept within the broader subject of the Internet of Things (IoT) ecosystem [3].

However, with the widespread use of robots in civil, military, industrial, and agricultural fields, concerns about Security, safety, accuracy, and confidence have arisen [4]. Security relates to protecting robots against cyber-attacks, safety focuses on reducing accidents and human injuries, accuracy pertains to flawless task performance, and confidence reflects satisfaction with robotic performance in replacing humans in certain activities [4].

The continuous appearance of security concerns, problems, vulnerabilities, and threats has led to the misuse of robots through cyber-attacks, resulting in severe injuries and even loss of human life [5].

To fully comprehend the gravity of this issue, it is essential to delve deeper into the field's current state. Various sectors have implemented robots to enhance productivity, efficiency, and safety. For example, in the healthcare sector, surgical robots have revolutionized precision surgery, but they also face security threats such as unauthorized access to patient data or manipulation during surgeries. Autonomous robots work alongside human workers in the industrial domain, but their vulnerabilities to cyber-attacks pose potential risks to manufacturing [6].

By examining specific examples of robots in various sectors, such as agriculture, healthcare, manufacturing, and defense, we can gain insights into the types of security threats they encounter. Cyber-attacks targeting robots can result in financial losses, critical infrastructure disruptions, and sensitive information compromised. Furthermore, the implications of these threats are far-reaching, affecting human safety, economic stability, and public trust in the reliability of robotic systems.

Supplementing the introduction with relevant statistics and notable case studies would further highlight the importance and urgency of addressing security concerns in the rapidly evolving field of robotics. Statistical data on the rise of cyber-attacks against robots or case studies of high-profile incidents can offer a more tangible perspective on the risks and consequences of inadequate security measures.

This paper aims to shed light on the critical security challenges faced by intelligent robotic systems as they become increasingly integrated into our daily lives. By exploring specific examples, common security threats, and their implications for various sectors, we can better understand the significance of safeguarding robots from cyber-attacks and the urgency of implementing robust security measures. The findings presented in this paper will contribute to the ongoing discussions on securing the future of robotics and its potential impact on society. Lastly, this paper is organized into five sections: Section 2 presents the real-world applications of robots, Section 3 delves into the building level of robot systems, and Section 4 discusses cyber vulnerabilities and

attacks for each level in Section 3, along with the percentage of incremental attacks in the last five years. The paper concludes with suggestions for future developments.

2. ROBOT APPLICATION FIELD

This section illustrates the primary use of robots in the fields of industry, Healthcare, agriculture, and disaster, as well as police and military ones. Figure 1 demonstrates robotic applications in different operation fields for many tasks [6].

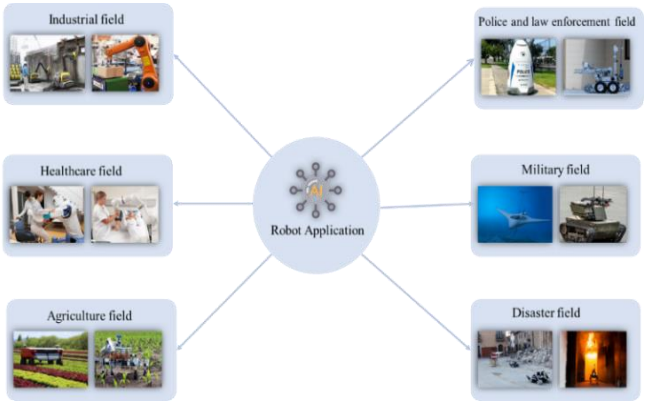

Figure 1. Robots used in specific fields

2.1 Industrial field

Industrial robots are vital automation systems withinside the contemporary-day production industry. They combine advanced technology in several disciplines, including machinery, electronics, control, computers, sensors, and synthetic intelligence. They benefit from completing work faster, safer, extra efficiently, and finishing repetitive tasks with equal accuracy and efficiency, using Industrial robots to reduce the workforce. As a result, welding, distribution, meeting, and coping with robots were extensively utilized in commercial manufacturing activities [7]. However, they come with challenges, including high initial costs, complex programming, limited flexibility, safety concerns, and potential job displacement. Maintenance, integration with existing systems, and cybersecurity risks also pose drawbacks. Striking a balance between automation and human involvement is crucial for maximizing the benefits of industrial robots while addressing these challenges [8].

2.2 Healthcare field

Today, the use of robots in medicine and healthcare has evolved far beyond its starting point in the operating room more than 30 years ago. They are now used in clinical settings to help healthcare workers and patients. For instance, hospitals and clinics are deploying robots for various tasks to help reduce pathogen exposure during the COVID-19 pandemic [9].

Nowadays, robots can be found assisting in many medical fields, including robot-assisted surgery and Surgical robots, rehabilitation robots, radiotherapy robots, laboratory robots, robotic prostheses, hospital robots, and social robots are all examples of medical robots [10]. The benefits of robotics in healthcare include reduced physician workload and patient stress [11].

However, their implementation also comes with challenges, including high costs, complexity, ethical considerations, integration issues, limited autonomy, patient acceptance, security risks, job impact, and accessibility. Addressing these challenges requires collaboration and careful consideration of ethical, legal, and social implications to ensure medical robots' responsible and effective integration into healthcare settings [12].

2.3 Agriculture field

Robots work in the agricultural sector to improve productivity, specialization, and environmental sustainability, by automating repetitive, slow, and tedious tasks for workers, allowing them to improve farmers' overall profits, thus reducing the need for human participation in many repetitive tasks. The most common use of agricultural robots is picking and harvesting, self-mowing, weed control, pruning, seeding, phenotyping, spraying and loosening, sorting, and packing. Agricultural robots offer several drawbacks. Agricultural Robots are Costly, Complex, and Require Technical Expertise [13].

2.4 Police and law enforcement field

There is no difference between police and other robots since they use artificial intelligence, machine learning, and IoT to perform assigned tasks. Police robots are designed to allow access to hazardous situations that the police cannot neutralize or may cause the loss of life of policemen; this Robot was used in Dubai in 2017 and was called Robocop [14]. It is also known that the Indian, South African, and Dutch police employed Skunk drones with pepper sprayers. US law enforcement institutions also used “armed drones” with electro-shock weapons, rubber bands, and tear gas [15]. These applications raise concerns about the responsible and ethical use of robotic technology in law enforcement.

To provide a more balanced view, it would be beneficial to discuss the positive and intended uses of robotics in the police and law enforcement field. For instance, robots can assist in dangerous and high-risk situations, reducing the risk to human officers and improving overall safety. Additionally, they can be valuable tools in conducting search and rescue operations, bomb disposal, and surveillance in scenarios where human intervention may be limited or impractical.

2.5 Military field

Military robots are self-contained or remotely controlled machines designed for military use. Unmanned aerial vehicles like the Predator drone can take surveillance photographs and even accurately launch missiles at ground targets. Unmanned Combat Air Vehicles, a subclass, are designed to carry out combat strike missions [16].

The main benefit of military robots is their ability to make quick decisions in fast-paced combat situations. When robots enter the front line of combat, they can save lives. They can navigate through environments that are deadly and dangerous for humans. However, military robots have some drawbacks that can become legitimate users if hacked [17].

Robots' positive and intended uses can aid in reconnaissance and surveillance missions, providing critical information to military personnel and enhancing situational awareness. Additionally, they can be used for bomb disposal, reducing the risk to human bomb disposal teams.

2.6 Disaster field

Disaster response robots that fly, swim, crawl through the rubble, put out fires, or assist first responders have come a long way in the last few decades [18].

The difficult jobs for humans, such as getting to dentures places, are done using disaster. One of the famous applications was when Searching and Rescuing (SAR) robots were used to find lost Thai cave boys safely. Furthermore, robots have been used in the firefighting domain to help save firefighters' lives and access areas rated as too dangerous, too risky, or too small for firefighters [19]. The latest application of disaster robots was in the Beirut port explosion in 2020, where robots and drones were used to kill fires and save human lives [20].

Dissimilar types of robots dependent on their field of operations: Unmanned Aerial Vehicles (UAVs) like Autonomous Unmanned Aircraft Vehicles and drones [21]. Unmanned Ground Vehicles (UGVs) such as Mobile robots and autonomous vehicles [22]. Unmanned Underwater Vehicles like underwater drones [23].

3. ROBOT SYSTEM

Robotic systems, including humans, react with their surrounding parameters to provide smart services and information through their attached actuators, sensors, and human interfaces [24, 25]. Figure 2 presents the general level of the robot system [26, 27].

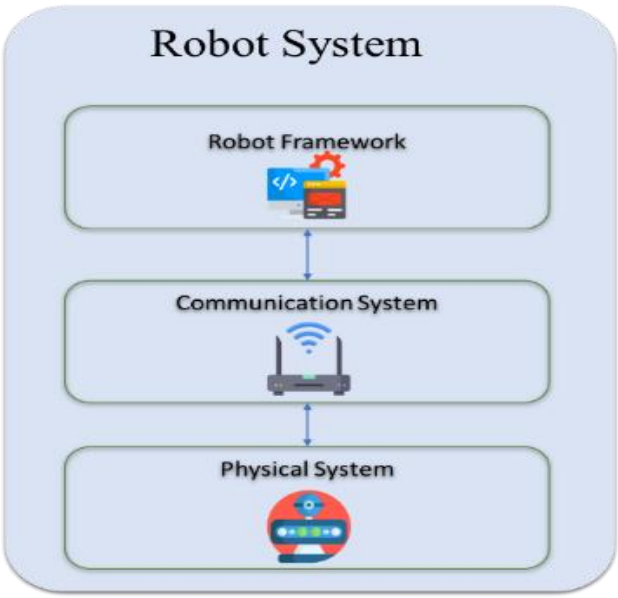

Figure 2. The general level of the robot system

As shown in Figure 2, the level robot system has three levels physical, communication, and software and platform system.

3.1 Physical system

The embodiment philosophy of Rodney Brooks, who famously stated, “The world is its own best model”, is at the heart of Physical Systems [28]. A typical basic robot consists of a movable physical structure, a motor, a sensor system, a power supply, and a computer “brain” that controls all these elements [29]. Figure 3 depicts the general system for a physical robot.

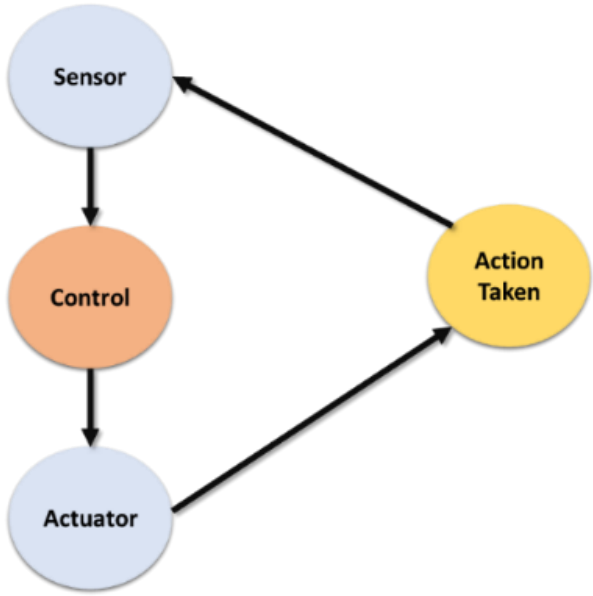

Figure 3. The general system for a physical robot

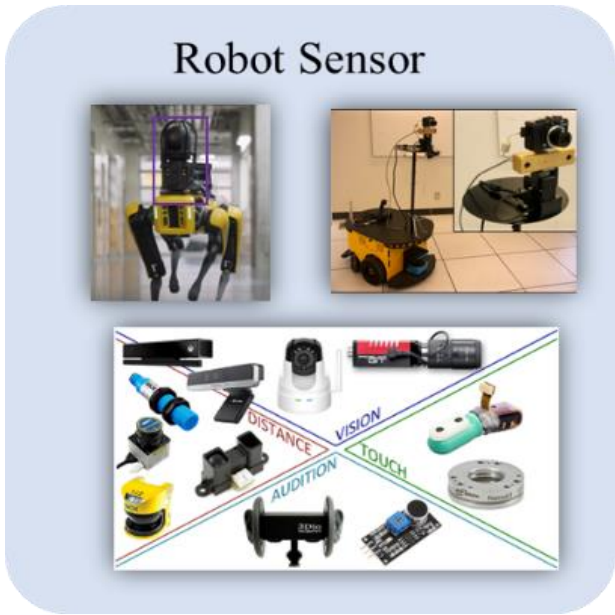

Figure 4. The sensor type of robot

A) Sensor: Robots have to understand their environment through sensors. A typical sensor could be a camera or a managed device (light detector and array finder) which uses a laser scanner to create three-dimensional images. However, robots may also have systems for taste, sound, smell, and even touch. They also include sensors without the boundary of human capabilities, such as chemical detection or night vision. Information gathered by the sensors is sent to a control unit that can operate an arm or other robot functional parts [30]. Figure 4 shows the accurate picture of some sensors.

B) Control: The control system (“the brains”) is the system that allows the robots to move. This system includes the mechanical aspects and the programmable systems that control robots. Robots are controlled in different ways, including by hand, semi-autonomously (a combination of fully automated and wireless control), wirelessly, and fully autonomously (i.e., when it uses AI to move by its understanding of the environment, but there may be options to control it manually), [31, 32].

C) Actuator: A robotic actuator is an electromechanical device that can respond to external stimuli and make autonomous decisions or actions to complete a specific task [33]. The robotic actuator is regarded as the most critical component of the robotic ecosystem because it cannot perform any physical motion without it [34]. Figure 5 presents the classification and uses of the robotic actuator [35].

D) Take Action: Take action means (to do something or to act to get a particular result) for example robot moves to the right and then goes to the goal, which means the action of the Robot at this moment is to move to the right and go to the goal, [36].

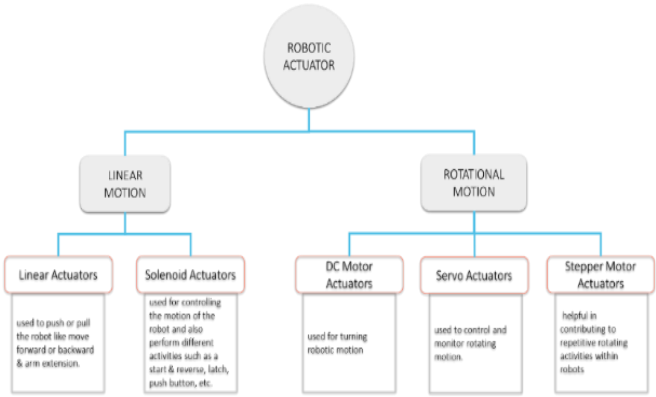

Figure 5. Types of robotic actuators

3.2 Communication system

Many robots rely on user interaction or communication with the outside world. Robots use a variety of communication methods, including:

3.2.1 Short-range connectivity:

Short-range technology has found applications in industrial equipment and household appliances. The transmission channels that include the short-range are presented below:

A) **Bluetooth** is a popular wireless technology that adheres to the IEEE standard 802.15.1. Data can be transferred over short distances, typically 8-10 meters. Users can quickly upload or download huge volumes of data from the mobile phone, computers, or any other controller to the Robot if a Bluetooth module is added. Another advantage is that Bluetooth modules do not require a direct line of sight to communicate, making them an excellent choice for mobile robots [37].

B) **Ultra-WideBand (UWB)** communication protocol uses radio waves to communicate over short distances [38]. According to the FiRa Consortium, UWB can determine the relative position of peer devices with line of sight at up to 200 meters using the IEEE 802.15.4a standard [39]. The Consortium is adding a security extension-specified in IEEE 802.15.4z-to make it a “secure fine-ranging technology” [40]. The benefits of UWB include high-level Security, power consumption, and low cost. In robotics, UWB positioning systems are increasingly being adopted for localizing autonomous ground or aerial robots [41].

C) **Thread, Zigbee, and Z-Wave** are IEEE 802.15.4-based technologies used in the access layer for low-rate wireless personal area networks (WPAN) [42]. These mechanisms are widely used in intelligent home environments because of their low power consumption and data rates [3]. Z-Wave, which the Z-Wave Alliance manages, differs from Thread and Zigbee technologies in that it operates on unlicensed 908 MHz range frequency bands to prevent interference with other wireless technologies. Within the Omnidirectional Ultrasonic Localization robotics field for Mobile Robots [43].

D) **Wi-Fi (802.11 networks):** IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) protocols that are used in wireless local area network (WLAN) computer communication, which is a part of the IEEE 802 set of local area network (LAN) technical standards [44]. This prototype is relatively new in the world of robotics. Can control on Robot via the Internet by using a Wi-Fi adapter in a computer that converts digital data into radio signals, which are then converted back into digital data by the Wi-Fi unit on the Robot (another network adapter) [45].

3.2.2 Long-range connectivity:

Long-range technology has found applications in mobile car communication. The transmission channels that include the long-range are presented below:

A) Satellite communication (GPS controlled)

The Global Positioning System, or GPS, is a navigation system that relies on satellites to provide coordinates for objects on Earth equipped with a GPS receiver. This technology is used by robots, which use signals sent by orbiting satellites to calculate their position accurately. GPS devices can also provide data on the speed and direction of the Robot. GPS is a satellite-based system and is particularly useful for outdoor robots. However, the accuracy of GPS is limited to a few meters [46].

B) Cellular networks and service

Cell phone-controlled robots are the latest buzzwords in mobile robots. A cell phone can control a robot using DTMF control [47].

The idea behind DTMF control is simple: Two phones are connected, one of which is mounted on a robot. The call is automatically answered. During the call, pressing a specific button produces a tone decoded by the Robot's decoder, which outputs its binary value. This binary value can be used to control the Robot. This setup offers a wide coverage area limited only by the service provider's network and ease of construction [48].

Few other robots use GPRS and 3G/4G/5G services on the cell phone. A combination of services available in different generations can aid in developing a mobile robot capable of transmitting video and audio [49].

3.3 Robot framework

The Robot Framework is an open-source test automation framework widely used in acceptance testing and test-driven development. It provides an easy-to-understand and use format for writing test cases, including keyword-driven, behavior-driven, and data-driven formats. The test cases are organized in a tabular format using keywords, making them efficient and effective [50].

One of the main benefits of the Robot Framework is its flexibility in test case creation, as it allows collaboration between technical and non-technical team members. The framework's keyword-driven approach promotes test case reusability, simplifying maintenance and scalability [51].

Additionally, Robot Framework's compatibility with external libraries and open-source tools enhances its automation capabilities. Popular libraries like Selenium can be

integrated to expand the framework's usability in various domains and technologies [52].

The Robot Framework's cross-platform support is another advantage, allowing it to run on multiple platforms such as Jython (JVM) and IronPython (.NET) [53].

However, it is essential to acknowledge that the Robot Framework may not be suitable for all testing scenarios, and newcomers might face a learning curve, particularly if unfamiliar with automation or Python programming [54].

Finally, integrating the Robot Framework into the robot system empowers testers and developers with an accessible, flexible, and efficient automation tool. It excels in readability, reusability, and cross-platform compatibility. Careful consideration of its strengths and limitations will aid organizations in making informed decisions about its implementation for their specific automation needs.

4. CYBER ATTACK

This section will illustrate, with an explanation, the primary attacks targeting the robotic field.

4.1 Robotics cyber-physical system (CPS)

Physical access or connection to the Robot leads to exploiting the physical vulnerability. It thus lies the control of the device, reprogramming the components of the Robot and exploiting them. Two methods of privacy leakage in CPS were presented in this study [55]:

A) Physical: This privacy attack directly interferes with the system's physical properties. For example, we are changing the capabilities of an implantable healthcare chip.

B) Cyber: CPS cyber-attacks include computer viruses, software, and network-based attacks, for example, forged sensor data [56].

Moreover, one of the most famous physical devices infected by attacks are sensors susceptible to signals the opponent manipulates for an instant for sensor attack, sensor spoof, and A Denial-of-Service (DoS) [57]. Figure 6 presents the sensor attack.

Table 1 shows the cyber-physical attack summary of recent previous work.

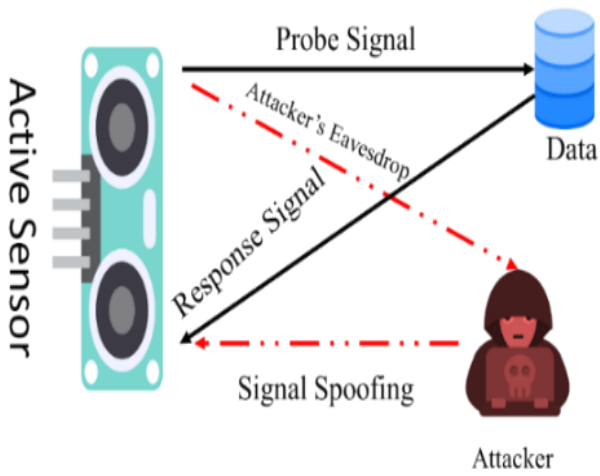

Figure 6. Sensor spoof attack

Table 1. Recent cyber-physical attack

No	Ref	Year	Type of Attack	Application	Impact
1	[58]	2019	Spoofing	Wheel Mobile Robot	Moderate
2	[59]	2019	Spoofing	Unmanned Aerial Vehicles	High
3	[60]	2020	Spoofing	Dron	High
4	[61]	2020	Spoofing	Unmanned Aerial Vehicles	High
5	[62]	2021	Spoofing	Wheel Mobile Robot	Moderate
6	[63]	2021	DoS	Mobile Robot	Moderate
7	[64]	2022	DoS	Industrial robots	High
8	[65]	2022	Spoofing	Robotic Vehicles	High
9	[66]	2022	Spoofing	UAVs	High

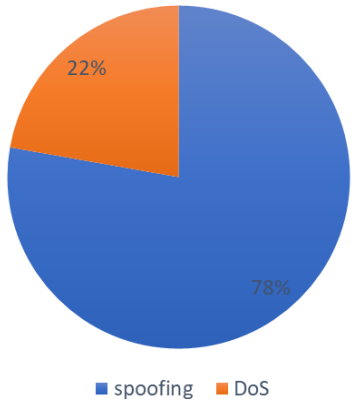

Figure 7. Percentage of spoofing Vs DoS

Table 1 noted that most attacks are spoofing and in an increased state in the last two years. In contrast, Figure 7 represents the percentage of attacks in the last four years, and the severity of these attacks was also classified depending on the work environment.

Finally, Robotics Cyber-Physical Systems (CPS) can be safeguarded against cyber-attacks through various countermeasures and prevention strategies. These include strong access controls, secure communication protocols, regular updates, network segmentation, intrusion detection, continuous monitoring, security awareness training, hardware security measures, and isolating critical systems. Implementing these strategies ensures the safety and Security of Robotics CPS in diverse environments.

4.2 Cyber attacks on a robotic communication system

Robotic communications are not immune to attacks that could disrupt various security services; for example, **Jamming attacks** are one of the most severe threats to wireless sensor networks (WSNs) that use the IEEE 802.15.4 standard. This attack interrupts and disrupts robot-to-robot and robot-to-human communication to suspend further robotic activities and jam any communication and control. **A Man in the Middle attack** happens when an intruder can eavesdrop on and intercept the communication between two robotic entities or nodes, modify the information, and insert it without being detected**. A Meet in Middle attack,** also referred to as a plaintext attack, happens when robotic communication is encrypted using a 2-DES and 3-DES (168-bit) key. A brute-force technique is then employed to break the encrypted communication channel, which enables the attacker to eavesdrop actively or passively [67].

Table 2 shows the cyber-communication attack summary of

recent previous work.

Table 2. Recent cyber-communication attack

No	Ref	Year	Type of Attack	Application	Impact
1	[68]	2019	Man in the Middle attack	Robot	High
2	[69]	2020	Man in the Middle attack	Industry Robot	High
3	[70]	2020	Man in the Middle attack	Mobile Robot	Moderate
4	[71]	2020	Jamming attacks	Drones	High
5	[72]	2020	Meet in the Middle attacks	Healthcare	High
6	[73]	2021	Man in the Middle attack	Robot	Moderate
7	[74]	2021	Man in the Middle attack	Industry Robot	High
8	[75]	2022	Man in the Middle attack	Drones	High
9	[76]	2022	Jamming attacks	Autonomous ground vehicle	High

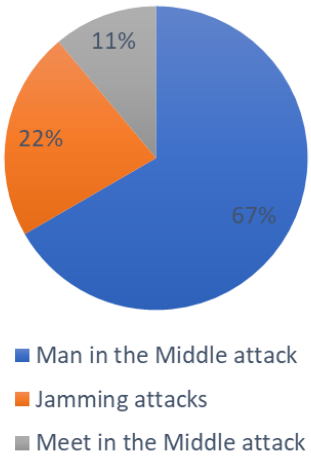

Figure 8. Percentage of man in the middle attack vs meet in the middle attacks vs jamming attacks

Table 2 noted that most attacks are Man in the Middle attack and an increased state in the last few years. Figure 8 represents the percentage of attacks in the last four years, and the severity of these attacks was also classified depending on the work environment.

Finally, potential countermeasures and prevention strategies to protect a robotic communication system against cyber attacks include encryption, secure authentication, firewalls, regular updates, network segmentation, secure protocols, user training, penetration testing, secure configuration, and an incident response plan. Implementing these measures enhances the system's Security and safeguards robotic operations from potential cyber threats.

4.3 Cyber attacks on robotics framework

The objective of the operating system framework is to provide a unified and open-source software framework for controlling robots in various actual and simulated environments. The most attack is Information leakage [77]. In the study [78], data leakage with high impact. In the study [79], apply attack on indoor robot navigation where policies can leak private information requires.

In the context of the operating system framework for robot control, 'Information leakage' refers to the unintentional or unauthorized divulgence of sensitive or confidential data. This can occur as a result of security vulnerabilities within the framework or due to cyber attacks. When confidential information is exposed to unauthorized parties, it poses substantial risks to the overall integrity, privacy, and Security of robot operations [80].

Lastly, protecting robotics frameworks against cyber attacks requires implementing several countermeasures. These include secure coding practices, regular security updates, security audits, access controls, encryption, intrusion detection systems, firewalls, network segmentation, user training, secure communication protocols, and secure supply chain management. These measures enhance the resilience of robotics frameworks, ensuring the safety and Security of robotic systems.

5. CONCLUSION

Automated systems are now being deployed and used in various fields that rely on critical infrastructure. However, botnets have numerous security flaws that can be used to launch dangerous attacks. These attacks could lead to significant economic losses and pose serious risks to human life and critical infrastructure. Specific examples, such as the NotPetya ransomware attack's global impact on businesses or the Triton malware attack's potential danger to a petrochemical plant, illustrate the gravity of these threats. Healthcare disruptions and power grid outages caused by cyber-attacks further underscore the need for robust security measures in automated systems. Understanding the real-world implications emphasizes the urgency of enhancing cybersecurity to protect data, public safety, and essential services reliant on robotic systems. At the end of the paper, the most recent attacks in the last five years are listed, along with the impact of each vulnerability, as shown in Table 1 and Table 2.

In the future, we intend to cover additional topics, such as machine learning and AI, to detect vulnerabilities.

REFERENCES

[1] Saeed, R.S., Oleiwi, B.K. (2022). A survey of deep learning applications for covid-19 detection techniques based on medical images. Ingénierie des Systèmes d'Information, 27(3): 399-408. https://doi.org/10.18280/isi.270305

[2] Abed, M.S., Lutfy, O.F., Al-Doori, Q.F. (2021). A review on path planning algorithms for mobile robots. Engineering and Technology Journal, 39(5): 804-820. https://doi.org/10.30684/etj.v39i5A.1941

[3] Vermesan, O., Bahr, R., Ottella, M., Serrano, M., Karlsen, T., Wahlstrøm, T., Sand, H.E., Ashwathnarayan, M., Gamba, M.T. (2020). Internet of robotic things intelligent connectivity and platforms. Frontiers in Robotics and AI, 7: 104. https://doi.org/10.3389/frobt.2020.00104

[4] von Braun, J., Archer, M.S., Reichberg, G.M., Sánchez Sorondo, M. (2021). AI, robotics, and humanity: Opportunities, risks, and implications for ethics and policy. Robotics, AI, and Humanity: Science, Ethics, and Policy, 1-13. https://doi.org/10.1007/978-3-030-54173-

6_1
[5] Djenna, A., Harous, S., Saidouni, D.E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences, 11(10): 4580. https://doi.org/10.3390/app11104580
[6] Taylor, R.H., Menciassi, A., Fichtinger, G., Fiorini, P., Dario, P. (2016). Medical robotics and computer-integrated surgery. Springer Handbook of Robotics, 1657-1684. https://doi.org/10.1007/978-3-319-32552-1_63
[7] Li, Z.B., Li, S., Luo, X. (2021). An overview of calibration technology of industrial robots. IEEE/CAA Journal of Automatica Sinica, 8(1): 23-36. https://doi.org/10.1109/JAS.2020.1003381
[8] Buerkle, A., Eaton, W., Al-Yacoub, A., Zimmer, M., Kinnell, P., Henshaw, M., Coombes, M., . Chen, W.H., Lohse, N. (2023). Towards industrial robots as a service (IRaaS): flexibility, usability, safety and business models. Robotics and Computer-Integrated Manufacturing, 81: 102484. https://doi.org/10.1016/j.rcim.2022.102484
[9] Quazi, S., Saha, R.P., Singh, M.K. (2022). Applications of artificial intelligence in healthcare. Journal of Experimental Biology and Agricultural Science, 10(1): 211-226. https://doi.org/10.18006/2022.10(1).211.226
[10] Williams, A., Sebastian, B., Ben-Tzvi, P. (2019). Review and analysis of search, extraction, evacuation, and medical field treatment robots. Journal of Intelligent & Robotic Systems, 96: 401-418. https://doi.org/10.1007/s10846-019-00991-6
[11] Hassan, M.Y., Karam, Z.A. (2014). Modeling and force-position controller design of rehabilitation robot for human arm movements. Engineering and Technology Journal, 32(8): 2079-2095. https://doi.org/10.30684/etj.32.8A15
[12] Verma, G., Shahi, A.P., Prakash, S. (2022). A study towards recent trends, issues and research challenges of intelligent IoT healthcare techniques: IoMT and CIoMT. Proceedings of Trends in Electronics and Health Informatics, 177-190. https://doi.org/10.1007/978-981-16-8826-3_16
[13] Xie, D.B., Chen, L., Liu, L.C., Chen, L.Q., Wang, H. (2022). Actuators and sensors for application in agricultural robots: a review. Machines, 10(10): 913. https://doi.org/10.3390/machines10100913
[14] While, A.H., Marvin, S., Kovacic, M. (2021). Urban robotic experimentation: San Francisco, Tokyo and Dubai. Urban Studies, 58(4): 769-786. https://doi.org/10.1177/0042098020917790
[15] Engberts, B., Gillissen, E. (2016). Policing from above: drone use by the police. The Future of Drone Use: Opportunities and Threats from Ethical and Legal perspectives, 93-113. https://doi.org/10.1007/978-94-6265-132-6_5
[16] Valavanis, K.P., Vachtsevanos, G.J. (2015). Handbook of unmanned aerial vehicles. Springer Dordrecht, 1. https://doi.org/10.1007/978-90-481-9707-1
[17] Tlili, F., Fourati, L.C., Ayed, S., Ouni, B. (2022). Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: Assessments & countermeasures. Ad Hoc Networks, 129: 102805. https://doi.org/10.1016/j.adhoc.2022.102805
[18] Murphy, R.R., Tadokoro, S., Kleiner, A. (2016). Disaster robotics. Springer Handbook of Robotics, 1577-1604. https://doi.org/10.1007/978-3-319-32552-1_60
[19] Jorge, V.A., Granada, R., Maidana, R.G., Jurak, D.A., Heck, G., Negreiros, A.P.F., dos Santos, D.H., Gonçalves, L.M.G., Amory, A.M. (2019). A survey on unmanned surface vehicles for disaster robotics: Main challenges and directions. Sensors, 19(3): 702. https://doi.org/10.3390/s19030702
[20] Cheaito, M.A., Al-Hajj, S. (2020). A brief report on the Beirut port explosion. Mediterranean Journal of Emergency Medicine & Acute Care, 1(4): 22-24. https://doi.org/10.52544/2642-7184(1)4001
[21] Shakhatreh, H., Sawalmeh, A.H., Al-Fuqaha, A., Dou, Z.C., Almaita, E., Khalil, I., Othman, N.S., Khreishah, A., Guizani, M. (2019). Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges. IEEE Access, 7: 48572-48634. https://doi.org/10.1109/ACCESS.2019.2909530
[22] Bonadies, S., Gadsden, S.A. (2019). An overview of autonomous crop row navigation strategies for unmanned ground vehicles. Engineering in Agriculture, Environment and Food, 12(1): 24-31. https://doi.org/10.1016/j.eaef.2018.09.001
[23] Wang, G.H., Yang, Y.N., Wang, S.X. (2020). Ocean thermal energy application technologies for unmanned underwater vehicles: A comprehensive review. Applied Energy, 278: 115752. https://doi.org/10.1016/j.apenergy.2020.115752
[24] Abed, M.S., Lutfy, O.F., Al-Doori, Q.F. (2022). Online path planning of mobile robots based on African vultures optimization algorithm in unknown environments. Journal Européen des Systèmes Automatisés, 55(3): 405-412. https://doi.org/10.18280/jesa.550313
[25] Abed, M.S., Lutfy, O.F., Al-Doori, Q.F. (2022). Adaptive weight grey wolf algorithm application on path planning in unknown environments. Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), 27(3): 1375-1387. http://doi.org/10.11591/ijeecs.v27.i3
[26] Švec, J., Neduchal, P., Hrúz, M. (2022). Multi-modal communication system for mobile robot. IFAC-PapersOnLine, 55(4): 133-138. https://doi.org/10.1016/j.ifacol.2022.06.022
[27] Rácz, M., Noboa, E., Détár, B., Nemes, Á., Galambos, P., Szűcs, L., Márton, G., Eigner, G., Haidegger, T. (2022). PlatypOUs-a mobile robot platform and demonstration tool supporting STEM education. Sensors, 22(6): 2284. https://doi.org/10.3390/s22062284
[28] Rieffel, J., Mouret, J.B., Bredeche, N., Haasdijk, E. (2017). Introduction to the evolution of physical systems special issue. Artificial Life, 23(2): 119-123. https://doi.org/10.1162/ARTL_e_00232
[29] Mikolajczyk, T., Mikołajewska, E., Al-Shuka, H.F.N., Malinowski, T., Kłodowski, A., Pimenov, D.Y., Paczkowski, T., Hu, F.W., Giasin, K., Mikołajewski, D., Macko, M. (2022). Recent advances in bipedal walking robots: Review of gait, drive, sensors and control systems. Sensors, 22(12): 4440. https://doi.org/10.3390/s22124440
[30] Li, P., Liu, X.P. (2019). Common sensors in industrial robots: a review. In Journal of Physics: Conference Series, IOP Publishing, 1267(1): 012036. https://doi.org/10.1088/1742-6596/1267/1/012036
[31] Waheed, Z.A., Humaidi, A.J. (2022). Design of optimal

sliding mode control of elbow wearable exoskeleton system based on whale optimization algorithm. Journal Européen des Systèmes Automatisés, 55(4): 459-466. https://doi.org/10.18280/jesa.550404

[32] Ibrahim Majeed, A. . (2020). Mobile robot motion control based on chaotic trajectory generation. Journal of Engineering and Sustainable Development, 24(4), 48–55. https://doi.org/10.31272/jeasd.24.4.6

[33] Walker, J., Zidek, T., Harbel, C., Yoon, S., Strickland, F.S., Kumar, S., Shin, M. (2020). Soft robotics: A review of recent developments of pneumatic soft actuators. Actuators, MDPI, 9(1): 3. https://doi.org/10.3390/act9010003

[34] Crispel, S., García, P.L., Saerens, E., Varadharajan, A., Verstraten, T., Vanderborght, B., Lefeber, D. (2021). A novel wolfrom-based gearbox for robotic actuators. IEEE/ASME Transactions on Mechatronics, 26(4): 1980-1988. https://doi.org/10.1109/TMECH.2021.3079471

[35] Lomas, M., Chevalier, R., Cross, E.V., Garrett, R.C., Hoare, J., Kopack, M. (2012). Explaining robot actions. In Proceedings of the Seventh Annual ACM/IEEE International Conference on Human-Robot Interaction, 187-188. https://doi.org/10.1145/2157689.2157748

[36] Top, A., Gökbulut, M. (2022). Android application design with MIT app inventor for bluetooth based mobile robot control. Wireless Personal Communications, 126(2): 1403-1429. https://doi.org/10.1007/s11277-022-09797-6

[37] Rasool, J.M. (2019). Ultra wide band antenna design for robotics & sensors environment. In 2019 12th International Conference on Developments in eSystems Engineering (DeSE), IEEE, 668-672. https://doi.org/10.1109/DeSE.2019.00125

[38] Gigl, T., Troesch, F., Preishuber-Pfluegl, J., Witrisal, K. (2012). Ranging performance of the IEEE 802.15. 4a UWB standard under FCC/CEPT regulations. Journal of Electrical and Computer Engineering, 2012: 1-9. https://doi.org/10.1155/2012/218930

[39] Zignani, A., Tomsett, S. (2021). Ultra-wideband (UWB) for the IoT-a fine ranging revolution. ABI Research.

[40] Morón, P.T., Salimi, S., Queralta, J.P., Westerlund, T. (2022). UWB role allocation with distributed ledger technologies for scalable relative localization in multi-robot systems. In 2022 IEEE International Symposium on Robotic and Sensors Environments (ROSE), IEEE, 1-8. https://doi.org/10.1109/ROSE56499.2022.9977431

[41] K. Hassan, S., H. Sallomi, A., H. Wali, M. (2022). Design of a dual-band rejection planar ultra-wideband (UWB) antenna. Journal of Engineering and Sustainable Development, 26(4), 30–35. https://doi.org/10.31272/jeasd.26.4.3

[42] Nassir, R.B., Jassim, A.K. (2022). Design of mimo antenna for wireless communication applications. Journal of Engineering and Sustainable Development, 26(4): 36-43. https://doi.org/10.31272/jeasd.26.4.4

[43] Menegatti, E., Zanella, A., Zilli, S., Zorzi, F., Pagello, E. (2009). Range-only slam with a mobile robot and a wireless sensor networks. In 2009 IEEE International Conference on Robotics and Automation, IEEE, 8-14. https://doi.org/10.1109/ROBOT.2009.5152449.

[44] Mahmood, S.H., Salih, A.M. (2019). Study of the most important factors affecting on efficiency of power line communication systems. Journal of Engineering and Sustainable Development, 23(5): 55-70. https://doi.org/10.31272/jeasd.23.5.5

[45] Haxhibeqiri, J., Jarchlo, E.A., Moerman, I., Hoebeke, J. (2018). Flexible Wi-Fi communication among mobile robots in indoor industrial environments. Mobile Information Systems, 2018. https://doi.org/10.1155/2018/3918302

[46] Gharajeh, M.S., Jond, H.B. (2020). Hybrid global positioning system-adaptive neuro-fuzzy inference system based autonomous mobile robot navigation. Robotics and Autonomous Systems, 134: 103669. https://doi.org/10.1016/j.robot.2020.103669

[47] Kumar, M., Kaushal, N., Bhute, H., Sharma, M.K. (2013). Design of cell phone operated robot using DTMF for object research. In 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), IEEE, 1-5. https://doi.org/10.1109/WOCN.2013.6616244

[48] Naveena, M., Madhavi, P., Meghana, M., Badashah, S.J. (2022). Remote vehicle control through cell phone using DTMF. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 10: 1169-1177. https://doi.org/10.22214/ijraset.2022.43972

[49] Hamzeh, O., Elnagar, A. (2015). A kinect-based indoor mobile robot localization. In 2015 10th International Symposium on Mechatronics and its Applications (ISMA), IEEE, 1-6. https://doi.org/10.1109/ISMA.2015.7373469

[50] Al-Omair, O.M., Huang, S. (2022). An emotional support robot framework using emotion recognition as nonverbal communication for human-robot co-adaptation. In Proceedings of the Future Technologies Conference, Cham: Springer International Publishing, 451-462. https://doi.org/10.1007/978-3-031-18344-7_30

[51] Shahria, M.T., Sunny, M.S.H., Zarif, M.I.I., Khan, M.M.R., Modi, P.P., Ahamed, S.I., Rahman, M.H. (2022). A novel framework for mixed reality-based control of collaborative robot: development study. JMIR Biomedical Engineering, 7(1): e36734. https://doi.org/10.2196/36734

[52] Ahmed, Z.A., Raafat, S.M. (2023). An extensive analysis and fine-tuning of gmapping's initialization parameters. International Journal of Intelligent Engineering & Systems, 16(3): 126-138. https://doi.org/10.22266/ijies2023.0630.10

[53] Tsardoulias, E., Mitkas, P. (2017). Robotic frameworks, architectures and middleware comparison. arXiv Preprint arXiv: 1711.06842. https://doi.org/10.48550/arXiv.1711.06842

[54] Atiyah, H.A., Hassan, M.Y. (2023). Outdoor localization for a mobile robot under different weather conditions using a deep learning algorithm. Journal Européen des Systèmes Automatisés, 56(1): 1-9. https://doi.org/10.18280/jesa.560101

[55] Newaz, A.I., Sikder, A.K., Rahman, M.A., Uluagac, A.S. (2021). A survey on security and privacy issues in modern healthcare systems: attacks and defenses. ACM Transactions on Computing for Healthcare, 2(3): 1-44. https://doi.org/10.1145/3453176

[56] Umer, M., Sadiq, S., Karamti, H., Alhebshi, R.M., Alnowaiser, K., Eshmawi, A.A., Song, H.B., Ashraf, I. (2022). Deep learning-based intrusion detection methods in cyber-physical systems: Challenges and future trends. Electronics, 11(20): 3326.

https://doi.org/10.3390/electronics11203326
[57] Shin, J., Baek, Y., Eun, Y., Son, S.H. (2017). Intelligent sensor attack detection and identification for automotive cyber-physical systems. In 2017 IEEE Symposium Series on Computational Intelligence (SSCI), IEEE, 1-8. https://doi.org/10.1109/SSCI.2017.8280915
[58] Varshosaz, M., Afary, A., Mojaradi, B., Saadatseresht, M., Ghanbari Parmehr, E. (2019). Spoofing detection of civilian UAVs using visual odometry. ISPRS International Journal of Geo-Information, 9(1): 6. https://doi.org/10.3390/ijgi9010006
[59] Liang, C., Miao, M.X., Ma, J.F., Yan, H.Y., Zhang, Q., Li, X.H., Li, T. (2019). Detection of GPS spoofing attack on unmanned aerial vehicle system. In Machine Learning for Cyber Security: Second International Conference, Springer International Publishing, 123-139. https://doi.org/10.1007/978-3-030-30619-9_10
[60] Gluck, T., Kravchik, M., Chocron, S., Elovici, Y., Shabtai, A. (2020). Spoofing attack on ultrasonic distance sensors using a continuous signal. Sensors, 20(21): 6157. https://doi.org/10.3390/s20216157
[61] Guo, R.X., Tian, J.W., Wang, B.H., Shang, F.T. (2020). Cyber-physical attack threats analysis for UAVs from CPS perspective. In 2020 International Conference on Computer Engineering and Application (ICCEA), IEEE, 259-263. https://doi.org/10.1109/ICCEA50009.2020.00063
[62] Kamal, M., Barua, A., Vitale, C., Laoudias, C., Ellinas, G. (2021). GPS location spoofing attack detection for enhancing the security of autonomous vehicles. In 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), IEEE, 1-7. https://doi.org/10.1109/VTC2021-Fall52928.2021.9625567
[63] Lee, S., Min, B.C. (2021). Distributed control of multi-robot systems in the presence of deception and denial of service attacks. arXiv Preprint arXiv: 2102.00098. https://doi.org/10.48550/arXiv.2102.00098
[64] Li, N.N., Wang, Y., Shen, P.F., Li, S.F., Zhou, L. (2022). A dos attacks detection aglorithm based on snort-base for robotic arm control systems. Journal of Computer and Communications, 10(04): 1-13. https://doi.org/10.4236/jcc.2022.104001
[65] Xu, Y., Han, X.S., Deng, G.L., Li, J.W., Liu, Y., Zhang, T.W. (2022). SoK: Rethinking sensor spoofing attacks against robotic vehicles from a systematic view. arXiv Preprint arXiv: 2205.04662. https://doi.org/10.48550/arXiv.2205.04662
[66] Wei, X.M., Sun, C., Lyu, M.J., Song, Q.P., Li, Y. (2022). ConstDet: control semantics-based detection for GPS spoofing attacks on UAVs. Remote Sensing, 14(21): 5587. https://doi.org/10.3390/rs14215587
[67] Ackoski, J. (2020). Man in the middle attacks. International Journal of Science and Arts-IDEA, 4(8).
[68] Mohammad, A.F., Almeida, P., Soliman, Y., Sadhu, A., Kata, K., Straub, J. (2019). Secure satellite database transmission. In 2019 IEEE Aerospace Conference, IEEE, 1-6. https://doi.org/10.1109/AERO.2019.8741992
[69] Gaba, G.S., Kumar, G., Monga, H., Kim, T.H., Liyanage, M., Kumar, P. (2020). Robust and lightweight key exchange (LKE) protocol for industry 4.0. IEEE Access, 8: 132808-132824. https://doi.org/10.1109/ACCESS.2020.3010302
[70] Levshun, D., Chevalier, Y., Kotenko, I., Chechulin, A. (2020). Design and verification of a mobile robot based on the integrated model of cyber-physical systems. Simulation Modelling Practice and Theory, 105: 102151. https://doi.org/10.1016/j.simpat.2020.102151
[71] Garg, N., Roy, N. (2020). Enabling self-defense in small drones. In Proceedings of the 21st International Workshop on Mobile Computing Systems and Applications, 15-20. https://doi.org/10.1145/3376897.3377866
[72] Pandey, P., Pandey, S.C., Kumar, U. (2020). Security issues of Internet of Things in health-care sector: an analytical approach. Advancement of Machine Intelligence in Interactive Medical Image Analysis, 307-329. https://doi.org/10.1007/978-981-15-1100-4_15
[73] Vulpe, A., Crăciunescu, R., Drăgulinescu, A.M., Kyriazakos, S., Paikan, A., Ziafati, P. (2021). Enabling security services in socially assistive robot scenarios for healthcare applications. Sensors, 21(20): 6912. https://doi.org/10.3390/s21206912
[74] Clark, G.W., Doran, M.V., Andel, T.R. (2017). Cybersecurity issues in robotics. In 2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), IEEE, 1-5. https://doi.org/10.1109/COGSIMA.2017.7929597
[75] Li, L., Lian, X.F., Wang, Y.L., Tan, L. (2022). CSECMAS: An efficient and secure certificate signing based elliptic curve multiple authentication scheme for drone communication networks. Applied Sciences, 12(18): 9203. https://doi.org/10.3390/app12189203
[76] Cheung, C., Rawashdeh, S., Mohammadi, A. (2022). Jam mitigation for autonomous convoys via behavior-based robotics. Applied Sciences, 12(19): 9863. https://doi.org/10.3390/app12199863
[77] Dutta, V., Zielińska, T. (2021). Cybersecurity of robotic systems: Leading challenges and robotic system design methodology. Electronics, 10(22): 2850. https://doi.org/10.3390/electronics10222850
[78] Değirmenci, E., Kirca, Y.S., Yolaçan, E.N., Yazici, A. (2023). An analysis of DoS attack on robot operating system. Gazi University Journal of Science, 1-1. https://doi.org/10.35378/gujs.976496
[79] Pan, X.L., Wang, W.Y., Zhang, X.S., Li, B., Yi, J.F., Song, D. (2019). How you act tells a lot: Privacy-leakage attack on deep reinforcement learning. arXiv Preprint arXiv:1904.11082.https://doi.org/10.48550/arXiv.1904.11082
[80] Tariq, U., Ahmed, I., Bashir, A.K., Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review. Sensors, 23(8): 4117. https://doi.org/10.3390/s23084117