Hindawi
Security and Communication Networks
Volume 2022, Article ID 8045874, 9 pages
https://doi.org/10.1155/2022/8045874

Research Article

Cyberattacks on Self-Driving Cars and Surgical and Eldercare Robots

Sultan S. Alshamrani, Bdour A. Alkhudadi, and Sara M. Almtrafi

Department of Computer Engineering, College of Computer and Information Technology, Taif University, P.O. Box 11099, Taif 21994, Saudi Arabia

Correspondence should be addressed to Sultan S. Alshamrani; susamash@tu.edu.sa

Received 26 September 2021; Revised 28 December 2021; Accepted 4 May 2022; Published 12 May 2022

Academic Editor: Konstantinos Rantos

Robots have improved human life and increased the efficiency of performance in tasks that require precision and effort. For example, surgical robots are now used to perform precise surgical procedures and give accurate results. Moreover, robots are also used in elderly care to ease their lives. Perhaps there can even be self-driving cars that could deliver a person to their destination without the need of a driver. So it is very important to mention that these robots should be secure in terms of security for human life. Hence, this paper aims to explore the published studies on robots and their various security vulnerabilities. We review the most prominent weaknesses in the robotic operating system (ROS) and discuss some types of attacks against these robots. Also, this paper discusses the security enhancements to protect ROS that researchers have suggested protecting against some of the attacks and vulnerabilities that may occur on these robots. The primary findings of this work are to generate system copies for backup as well as encryption to protect against information disclosure. Also, a dynamic model is needed to detect and mitigate attacks that may occur in a physical manner, such as injecting malware into robots.

1. Introduction

Robotic systems are cyber-physical systems that interact with the physical environment by combining hardware and software tools, network and communication processes, mechanical actuators, controllers, operating systems, and sensors [1]. These complex systems increasingly interact with humans in professional, public, private, and healthcare settings. They are typically divided into industrial and service robots depending on whether they are "for use in industrial automation applications" or "perform useful tasks for humans" [2]. Industrial robots, warehouse robots, feeding robots, exoskeletons, assistants, socially interactive robots, robotic wheelchairs, and robotic surgeons are just a few examples. These systems are distinguished by the fact that they build an interconnected framework where the virtual and physical worlds collide [3]. Also, the robot enterprise has an outstanding effect on the growth of robots, which focuses particularly on human's daily life activities. Robots can be a useful resource for surgical procedures in hospitals where robots have brought about higher surgical outcomes and quicker recovery. For these, the surgical robots use publicly available networks and satellites to transmit images, video, and sensitive information among surgeons and robots [4]. Additionally, the robots can reach locations where humans cannot, such as in the case of extinguishing fire, war zones, and so on. Moreover, self-driven cars may be useful in lowering the human losses due to accidents. That is, these cars are predicted to quickly replace human drivers and promise significant societal advantages. This is possible due to the vehicular advert on inside networks permitting a conversation with cars via the radio [5]. Yet potential customers continue to be skeptical of how self-driving cars will be managed. This is partly because of the uncertainty related to ethical norms for such cars [6]. Similarly, an eldercare robot is one that is explicitly intended for medical care purposes. Care robots exist in different structures and have different capacities including physical, intellectual,

clinical, and psychosocial upholding [7]. But these robots rely upon the network's connectivity and the program-based operating system (ROS). Basically, robot operating system (ROS) is an open-supply framework for buying robots to perform tasks. The ROS is supposed to function as a software program platform for (among other subsets) the individuals who are constructing and using robots. This software program could help people percentage code and make greater thoughts more readily available [8]. Therefore, the network connectivity and programs behind ROS must be free from security threats and viruses. As ROS-based care robots have the ability to analyze large volumes of data generated in medical and behavioral monitoring, which are known extremely sensitive. So robotic security flaws present serious problems, not just for manufacturers and programmers but also for anyone who interacts with them. Moreover, the more the operations performed across networked systems and devices, the more the chances for system flaws to emerge, and the greater the potential of system failures or malicious attacks. Hence, the given system should not get corrupted at the right time from their functions by the inclusion of intruders. But it comes into notice that many manufacturers and programmers face a lot of security challenges in the building of their robots, particularly for sensitive-based applications and hardly can assure full strength of these robots against all types of security attacks. At present, however, nothing is known about how an attacker may use a robot's computational elements to manipulate the physical surroundings in an industrial setting (social or medical surroundings) [1]. As a result, these systems can be defenseless against the existing security challenges. That is, their software or hardware are easily vulnerable to attacks, and the authentication check can be easily compromised. Thus, the development of these robots should not only focus on the functions of these robots but also make them strong against the different kinds of cybersecurity threats and vulnerabilities. Otherwise, their work can be compromised by the invader attacks and can lead to improper functioning for respective tasks. The published research articles mentioned different vulnerabilities and attacks that the robotic system faced during working [9, 10].

Overall, robots had been invented to assist people and facilitate the overall performance of tasks, and these robots must not become sources of problems to people and the environment. Asimov made the following three legal guidelines for robots:

(1) A robot must follow the orders given by people besides when such type of orders would abide by the primary law

(2) A robot will not injure an individual or, through inaction, permit an individual to harm someone

(3) A robot must defend its lifestyle if such safety abides by the primary or second legal guidelines

With robots being slowly developed, researchers have proven that those legal guidelines alone are not enough to manipulate the conduct of robots. These robots have emerged with a supply of challenges for a few products because of their publicity with several assaults that make them pose a danger to people and the environment. Hence, this research work focuses on how to use these robots securely for daily human life tasks.

1.1. Contributions. In this paper, we discussed some types of robots such as self-driving cars, surgery, and eldercare robots. After that, the paper mentioned the weaknesses in the most famous robot operating systems (ROS) that may be the cause of some attacks. Next, some of the attacks that occur in these robots against the security methods as suggested by other researchers in the field are highlighted.

1.2. Organization of Paper. The rest of the paper is organized as follows: Section 2 reviews the related literature of the ROS system. Section 3 discussed the security enhancements to protect ROS and how attacks are prevented. In Section 4, the paper is concluded with a summarization.

2. Related Work

2.1. Security Problems inside ROS. In [4], the authors have discussed several security attacks on robot operating systems (ROS). Some of the prominent attacks discussed are unauthorized publishing, unauthorized data access, and denial-of-service (DOS) cyberattacks. A node in the ROS may announce some data that may be considered not important data and that will be published without proper approval. In such a case, this data may be misused to inject data or some instruction to the robot to disrobe the normal operation of the robot. Every node in ROS may join each subject matter in the software application. After that, the node will receive any data that is posted for this subject matter. These statistics can include important data related to business or can be used to do reverse engineering for the manufacturing process. This attack is particularly difficult to determine due to how a node can also not have any outgoing ROS conversation. In ROS, DoS attacks can be simply started by publishing a considerable amount of bogus data. This message type's subscriber will be bombarded with false communications. This results in a heavy processing burden on all nodes, as well as the probable inability to do meaningful processing. Because there is no way to regulate which node publishes what data, any node in the network can be used to broadcast data on a topic to which a target node has subscribed. This can later be used to launch a targeted DoS attack on that node.

In [11], the authors did a test to evaluate the overall execution of open robot communication (ORC) using the ROS middleware. The test's outcomes showed that ORC can manage the communication switch with expectancy properly under 1 ms with minimal variance. They performed skilled problems with ROS when the message payload was around 1 KB, when the postpone increased considerably and generally stayed at milliseconds. A postpone of that order, mixed with the untrustworthiness of the conversation system, concentrates ROS useless for any high overall performance program in robotics. We have proven that a low-latency conversation allows controllers to be written without delay in better stage languages.

In [12], the authors undertook an empirical observation of the actual time characteristics of ROS 2.0 in comparison to ROS. A conversation overall performance assessment was completed to examine the network's overall performance with appreciation of the actual time, overall performance, and the balance of a ROS. Two metrics were evaluated for message loss, cost, and latency, consistent with the statistics length and conversation frequency. The message loss cost was described because of the ratio of messages that were misplaced by the receiving node at some point in the conversation among the two nodes, and the conversation latency was then described because of the time distinction from when the message was sent to when it was received in a round-experience conversation. Those experiments proved that the actual time overall performance of a ROS 2.0 primarily based on a multiagent system is advanced in actual time, compared to the system using ROS 1.0 in the phrase of the proposed overall performance measures.

2.2. Security Enhancements to Protect ROS. The authors of [13] introduced a software-degree security structure to overcome a few essential security threats, which arise in regular ROS software. The issues are resolved by considering ROS as a black box, which is essentially a noninvasive design, in the sense that no modifications to ROS are made, but security is done solely at the application layer. As a result, ROS was considered a black box with security precautions built-in, such as an authentication server (AS) and specific functionalities in the ROS nodes themselves. As it cannot cowl all security threats, it can protect from a few of the maximum critical security vulnerabilities that are presently found in ROS. It can save unauthorized nodes from recording data, which may be used for the reserve engineering of manufacturing. This is carried out through the subject matter's particular encryption keys that are best when exceeded by legal software modules. Second, the black boxes deal with the danger of unauthorized publishing to protect against injecting false records into the robot software. They achieve this by verifying that every message has been encrypted with a valid key. Still, a few insufficiencies persist that cannot be treated at the software stage alone. They all want ROS itself to be modified. First, even though the message content material is encrypted and cannot be processed through unauthorized nodes, they could nevertheless gather data on which messages were posted in the frequency. This can be solved through end-to-end encryption of complete messages included in the ROS. An alternative action at the software stage is to submit certain kinds of fake messages intended to hide the real publishing frequency. Second, because of their technique, they cannot keep malicious publishers from publishing messages. They can best ensure that those messages are not interpreted through ordinary nodes. However, a denial-of-provider assault with excessive publishing frequency is possible. Third, their technique cannot keep a subscriber from subscribing to arbitrary topics. Thus, all messages of a certain subject matter will be added to it. Their most effective technique guarantees that.

Similar approaches were proposed in [14], which focused on an unauthorized user trying to reach the video display unit; however, they used a physical system referred to as the cyber-physical security "honeypot." The cyber-physical security honeypot is designed in such a way that its video display units' nodes request for a translated message to be verified, which means that the messages that exceed beyond the physical system could cause unintentional damage to the robot or its environment. Researchers in [15] created a new version of security for ROS systems. They proposed SROS, a library for the ROS ecosystem to guide modern cryptography as a security measure to address the present vulnerabilities. In SROS, all network conversation was encrypted by using a secure sockets layer (SSL) or a greater transport layer security (TLS). Furthermore, a researcher in [16] progressed the ROS security functions with encrypted communication and semantic policies to ensure accurate behavior. To encrypt communications, an advanced encryption standard set of rules was created. The ROS framework was proven to perhaps be hardened through using symmetric encryption algorithms and semantic policies to be certain of particular properties in ROS messages. Eduardo, Thomas, and Marco in [17] suggested a unique version to encapsulate cooperative robot missions in Merkle trees. Swarm operators can offer the "blueprint" of the swarm's project without disclosing its raw data. In other words, fact verification may be separated from the data itself. We suggest a system in which robots within the swarm must "prove" their integrity to their peers by replacing cryptographic proofs. Merkle trees are binary hash tree structures with primary properties: correctness and security. These properties can obtain stable and mystery robotic cooperation and consequently make robotic swarms resistant to tampered participants and physical seize attacks.

In [18], the authors provided a real-time scheduling framework for ROS, known as ROSCH, that meets the real-time necessities taking place in ROS. ROS now no longer guarantees real-time performance; hence, a ROS primarily based on self-reliant using vehicle could cause a site visitor's accident. Therefore, ROSCH contains three functionalities that do not exist within the ROS to guarantee real-time performance: (1) a synchronization system; (2) a fixed-priority scheduling framework primarily based on directed acyclic graph (DAG); and (3) a fail-secure function. In particular, the synchronization system guarantees that the timestamp gap between sensor measurements could be much less than or the same as the calculated value. The fixed-precedence scheduling framework primarily based on DAG guarantees that stop-to-stop latency is much less than or identical to a predicted value. Operating each mechanism simultaneously guarantees the final output topic frequency.

In robot operating systems (ROS), messages can be transmitted without encryption, which encourages eavesdropping. In [19], they suggested integrating data distribution service (DDS) as a delivery layer that allows plug-ins to be set up to ensure authentication, access management, and cryptography. Table 1 summarizes the ROS security issues and enhancements.

Table 1: Weaknesses and enhancements in ROS.

Reference	ROS security issues	Enhancements
Application-level security for ROS-based applications [14]	Unauthorized nodes from recording data	Application-level security architecture
A preliminary cyber-physical security assessment of the robot operating system (ROS) [15]	Unauthorized publishing unauthorized use	Cyber-physical security "honeypot"
ROSploit: cybersecurity tool for ROS [16]	Cryptography issues in ROS	SROS
Cybersecurity in autonomous systems: hardening ROS using encrypted communications and semantic rules [17]	Cryptography issues in ROS	Encrypted communications
Secure and secret cooperation of robotic swarms by using Merkle trees [18]	Secure and secret robot	Merkle trees
Rosch: real-time scheduling framework for ROS [19]	ROS does not guarantee real-time performance	ROSCH
Detecting and mitigating robotic cybersecurity risks (IGI Global [20])	Eavesdropping	Data distribution service (DDS)

2.3. Threat and Attacks on Surgical and Eldercare Robots. The use of humanoid robots is increasing exponentially; therefore, the risks associated with robotics have also increased. Cybersecurity breaches in robots will harm robotics [20]. There is a possible risk involved in operating on patients by giving commands to robots. The system is vulnerable to a man-in-the-middle attack if no encryption or authentication method is in place. When an illegal party gains control of a surgical robot, the results could be disastrous [20] and are illustrated in Figure 1. Due to the reliance on network connectivity to provide surgical robots at a distance, the robots are vulnerable to cyberattacks and critical data spills. Although end-to-end encryption protects against data leaks, backup systems are required in the event of a cyberattack during an operation, to either fully block the communication or change the command. This has the potential to be dangerous [21]. The researchers conducted surgical robot attacks in [22]. These cyber-physical assaults on the surgical robot's control system exploited flaws in the robot's control system to infer a critical period during surgery and insert malicious control orders into the robot. Malware can be installed to strategically introduce defects into the control system by an attacker. A faulty or inaccurate motor command might cause the robot arm to travel to an undesirable place, causing damage to the system or injury to the patient. They employed dynamic model-based detection and robot safety procedures to predict the negative effects of the assault on physical robots in [22].

In [23], they showed a new form of threat. They exploited ROS vulnerabilities and introduced intelligent self-learning malware so that when the robot was in a crucial stage of the proposed medical operation, they could monitor the actions of the robot's arms and activate the attack payload. The most commonly used ROS contains vulnerabilities that leak data and can become the basis for intelligent malware to learn about the device's behavior and use that information to decide when to trigger an attack. The ROS enables a master (core) node to register any new node/process; hence, without being detected, an attacker can register its malicious node to the robotic application. The study indicated that the applications were secured in the implementation phase.

In [5], a robot attack tool (RAT) was created to direct one-of-a-kind security assaults. To assess the attacks' impacts in a simulated environment, an impact-oriented approach was approved. Tests and attack tests were done physically on the robot. The simulated environment depends on Mobile Sim, a software tool utilized on mobile robots/antimedia platforms and their environments to simulate, debug, and explore. For physical tests, the robot platform People BotTM was utilized. The study's results and testing proposed indicated that a few attacks were effective in violating the robot's protection. Integrity attacks changed the guidelines and controlled the robot's activities. Availability attacks were able to trigger denial-of-service (DoS), and mobile eye orders were not available to the robot. Integrity and availability attacks made the robot seize confidential details. To limit the dangers to security in integrity hazards, having end-to-end encryption of the traffic is an effective way to resolve these threats. With respect to the peril of availability, which is centered around the corruption of configuration data, there are some standards for a mitigation technique to decrease the danger of availability loss: replacing the insecure MD5 hashing algorithm used to authenticate the password between client and server is essential.

In [24], researchers suggested viable assaults in eldercare robots. They stated that the aim of this assault was to benefit the manipulation of the eldercare robotic to display its consumer's information by searching for data such as credit scorecard facts for identification theft. A financially inspired attacker may want to carry out a utility degree assault by infiltrating the home network and searching for the robotics' IP deal to attain the username/password login access. In a buffer overflow assault, the attacker accesses the login to the overflow stack with malicious code and inserts a go-back to deal with those factors with the malicious code. Once this is accomplished, the attacker may want to completely manage the robotic and is then lose to display the aged victim through a camera or microphone, looking for data, which includes credit scorecard data, to use for financial advantage.

The researchers of [25] advised viable countermeasures for robotic producers to implement to save the victim from such assaults. They advised that robotic producers pass on adopting a not unusual place standardized running system.

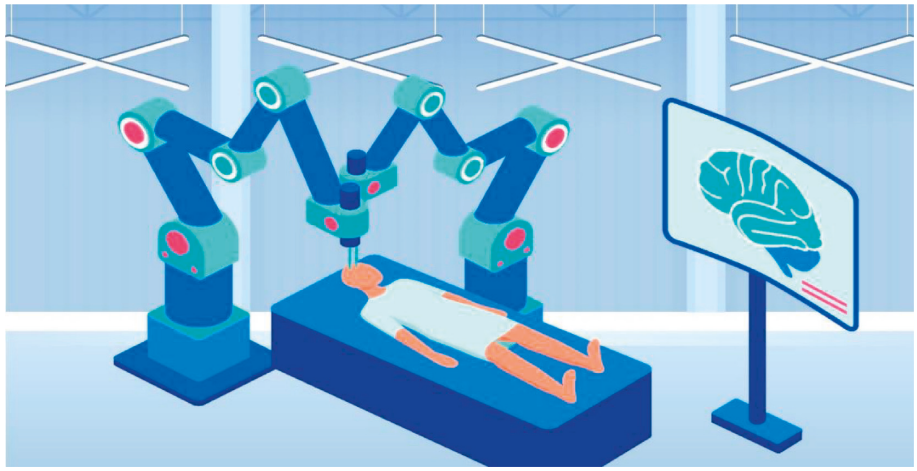

Figure 1: Medical surgery robots.

To assist in protecting the victim from firmware and OS assaults, producers may want to standardize on a not unusual place OS consisting of the open supply NuttX OS. Through standardization, robotic producers may want to create a conglomerate to supervise the platform and be liable for obtaining the OS, reporting security issues, and releasing security updates.

2.4. Threat and Attacks on Self-Driving Cars. Self-reliant cars, robotic cars, or self-driving cars massively affect road safety by using excessive skill in both hardware and software programs to lessen injuries because of numerous forms of human error. The view of self-driven cars is shown in Figure 2. However, there have been many accidents with self-driving cars [26]. In another case, a self-driving car from a Ford-backed business named Argo was carrying four people when it jumped a red light and collided with a vehicle in Pittsburgh, less than a mile from its starting position. Four people in the passenger compartment were injured and sent to the hospital [27]. Vehicular cybersecurity has traditionally targeted passive assault, especially by shielding the confidentiality of communications among cars or other motorized vehicles and smart infrastructures. However, over the past couple of years, self-driving cars have ended up as especially vulnerable to experimental cyber-assault [28]. Assaults on self-driving cars can permit attackers to manage, manipulate, or suppress the facts being routed within the network. This management of the facts of the customers may be used for their advantage or to disrupt the network [29].

Security and privateers' issues with self-driving cars and different self-reliant cars are still prevalent. The authors of [30] provided a new viable assault trajectory privacy attack on autonomous driving (T-PAAD) that was aimed at privateers in AVs, in which an adversary deanonymizes the usage trajectories of the present course, making different planning techniques.

In a maximum embedded system, the firmware that controls the functionality is saved within the flash, reminiscent of the chip [31]. The cap has the potential to replace cars' on-board software programs over the air and allows acquiring security patches and new functions without going to the service center. However, this kind of channel, if managed through an attacker, may be used to manipulate the motors. The OS is recognized to be at risk of DoS assault. In October 2016, a primary distributed denial-of-service (DDoS) assault caused an internet outage in essential metropolitan regions within the United States. The botnet foot soldiers within the cyberwarfare are managed through malicious malware; in a good deal of identical way, a contemporary-day electric-powered vehicle with self-reliant riding skills can be hacked remotely. In September 2016, the Keen Security Lab of Tencent, a tech massive in China, proved a vulnerability in taking advantage of the whole management system of a brand-new Tesla Model S with cutting-edge unmodified firmware and security patches [32].

With the advent of autonomous driving and modern vehicle technologies, cars are more powerful and connected than ever. Cars might suffer from a hijacked infrastructure or services that lead to a malfunction of their autonomous driving capability. Only this time, hackers and artificial intelligence might be able to harm someone from miles away by spoofing GPS. Although currently there are no complete standards of how cars will communicate in the future, the network that unmanned aerial vehicles (UAVs) currently use could shed some light on how an attack targeting the infrastructure could severely damage the functionality of an autonomous car. Cars will have the ability to communicate with each other and with satellite and ground stations. The autonomous driving feature of the vehicle will rely heavily on GPS and vehicle-to-vehicle communication, both of which can be manipulated by the attacker to tamper with the vehicle and injure the passengers. By spoofing GPS, attackers can cause traffic jams so that the police will not be able to catch up with any possible criminal activities, such as robbing a bank. Furthermore, attackers might hijack the technology to kidnap a person. The image recognition technology can be manipulated by changing the landscape of traffic signs or lanes so that the vehicle will be stopped or hijacked. The microphone installed on the vehicle's voice

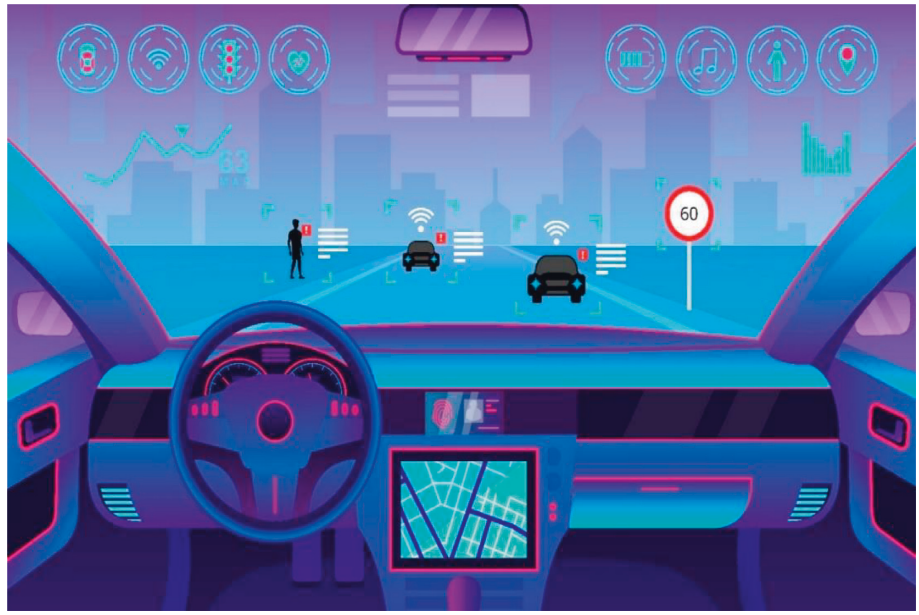

Figure 2: Self-driving cars.

recognition system might be used to eavesdrop on sensitive political/financial information. The need for autonomous cars is apparent in terms of the world's population. Since it is not sustainable to control all cars manually, a stable and secure way to organize autonomous cars is necessary. From a safety point of view, the World Health Organization stated that every year, 85,000 road traffic deaths occur in Europe and 34,000 occur in the United States [33].

To improve street security and driving encounters, recent self-driving cars can detect their environments and explore them without human interaction. These cars' dependability must be analyzed before they can be generally adopted on the road. Self-driving cars depend intensely on the use of the sensory ability of their environments to make driving decisions, which acquires a security risk from sensors. Accordingly, in [34], they analyzed independent cars' sensors' security and researched the reliability of the cars' "eyes." They examined sensors whose estimations were utilized for direct driving, ultrasonic sensors, and forward-looking cameras. They presented contactless attacks on these sensors and gathered the results in both a lab setting and outside of a Tesla Model S car. Results showed that using other shelf hardware could cause jamming and spoofing attacks, which then caused Tesla's visual deficiency and breakdown, all of which might prompt crashes and impede the well-being of self-driving cars. To reduce these issues, they recommended software and hardware countermeasures that would strength the sensor's resistance to these attacks. Table 2 summarizes the robot's assaults and how to foresee them.

All these challenges arise because there is no unified legislative framework for robot cybersecurity; multiple legal instruments addressing various sectors of applications including medical device regulation provide criteria that are applicable to care robots [1]. For example, consider the usage of a ROS-based care robot in the household of a lonely elderly person. The robot's purpose would be to allow the user's family to monitor and find him/her remotely in the event of a medical or health emergency. The robot is connected to the Internet via the home's wireless network and comes with a video camera, microphone, and speaker so that the family can see and talk to the user. An application-level attack might be carried out by infiltrating the home network and probing for the robot's IP address in order to reach the username/password login entry. The attacker exploits the login to overrun the stack with malicious code and inserts a return address that links to the malicious code via a buffer overflow attack. Once the attacker has complete control of the robot, he or she is free to watch the elderly victim using a camera or microphone, looking for information such as credit card numbers that may be exploited to make money. Hence, there is a necessity for security enhancement in care robot to protect ROS from day-to-day security attacks of intruders.

3. Discussion

In this section, the authors are discussing security enhancements that are required to protect ROS in Section 3.1.

Various attacks and their prevention are discussed in Section 3.2. The various security performance benefits of ROS-integrated robots are discussed in Section 3.3.

3.1. Security Enhancements to Protect ROS. For the manufacturer, the ROS is the backbone for the development of robotic technology. But it lacks many security enhancements that would not make these suitable for use. In this paper, we reviewed a set of enhancements suggested by multiple researchers that the manufacturers keep in mind in the development of robots for different kinds of applications. That is, the developed robots should be strong enough resistant to

Table 2: Robots attacks and their prevention methods.

Reference	Robots	Attacks	Prevention method
Analyzing cyber physical threats on robotic platforms [5]	Surgical robots	DOS attack – integrity attacks	Providing an end-to-end encryption
Targeted attacks on teleoperated surgical robots [22]	Surgical robots	Injection of malicious control commands to the robot	Dynamic model-based detection and robot safety mechanisms
In the case of Raven-II surgical robots [23]	Surgical robots	Exploitation of ROS vulnerabilities and implement smart self-learning malware	Suggesting that the applications can be secured in the implementation phase
Cybersecurity issues in robotics [24]	Eldercare robots	Gaining control of the eldercare robot to monitor its user looking for data	Standardized operating system
Trajectory privacy attack on autonomous driving [30]	Self-driving cars	Trajectory privacy attack	—
Cybersecurity in autonomous cars [31]	Self-driving cars	OS upgrade attack	—
Risk and opportunity governance of autonomous cars [33]	Self-driving cars	Services attack	—
Contactless attacks against sensors of self-driving [34]	Self-driving cars	Sensor attacks	Software and hardware countermeasures that will improve sensor resilience against these attacks

any kind of attacks and vulnerabilities during their use. So that is the reason that some researchers suggested using an authentication server to ensure that all nodes were valid. They also used encryption to achieve confidentiality and data accuracy. There may be unauthorized access to the encryption keys, so it is assumed that the keys were stored securely. There are also researchers who used a physical tool. This tool is good in terms of monitoring the connection as it is not allowed to pass any unauthorized messages. Researchers have also proposed a new security model for ROS systems that supports modern encryption. They also developed a tool (Rospolit) that simulates possible attacks on a ROS system. We think it is good to develop such tools that simulate attacks to make it easier for researchers to study these possible attacks and find solutions to prevent them.

Researchers have also made improvements to ROS using encrypted communication and semantic rules to ensure correct behavior. They did two experiments to test their suggestion. The encryption used symmetric encryption, where every node must know the key, but we believe that the process of exchanging the key will be difficult. As for the Markle tree model, which some researchers suggested using, it did achieve confidentiality and data integrity. ROS does not guarantee real-time performance, so it was a good idea to introduce work such as this, where real-time scheduling is done by the ROS. Thus, the transition time from one party to another is either less than or equal to the calculated value. Researchers also suggested data distribution service (DDS). It ensures authentication and access control and prevents modification and eavesdropping attacks by using encryption. We believe that this approach fulfills many of the security requirements.

3.2. Attacks and Prevention. Some of the mechanisms that researchers have suggested to protect against some of the attacks that may occur on these robots. Some researchers suggested having system copies for backup as well as encryption to protect against information disclosure. Other researchers have proposed a dynamic model to detect and mitigate attacks that may occur in a physical manner, such as injecting malware into robots. Furthermore, some researchers have suggested encrypting traffic to prevent safety threats to surgical robots. Moreover, some of them suggested countermeasures that robotics manufacturers could implement as a common operating system that standardized a system to report security problems and issue updates.

3.3. Prospective Benefits. This paper aims to enhance the security performance of ROS-integrated Robots and ensure safe human-robot interaction particularly in sensitive case applications. Hence, make the sensitive information exchange scenario fearless from the threats of invaders. An attempt is made in this research work by discussing some types of robots such as self-driving cars, surgery, and eldercare robots. After that, the paper outlined the weaknesses in the most famous robot operating systems (ROS) that may be the cause of some attacks. This paper also discussed the attacks that occur in these robots against the security methods as suggested by other researchers.

4. Open Challenges and Issues

Based on the discussion in Section 3, the various challenges and issues that exist in the security of robotic operating systems are highlighted below:

(i) The robots can reach locations where humans cannot, such as in the case of extinguishing fire, war zones, and so on. Moreover, self-driven cars may be useful in lowering the human losses due to accidents. Hence, efficient enhancements in robot

operating systems (ROS) will be beneficial in these application areas.

(ii) Robot operating systems (ROS) in the future need to be networked in environments where they can communicate with cloud services and industrial-based control systems from remote locations.

(iii) With the expansion of robot operating systems (ROS), it is very important to counter threats of cybersecurity before products based on them will reach mass markets.

(iv) Some of the mechanisms are needed to protect robot operating systems (ROS) that could benefit the reader as well as the manufacturers of robots to obtain a deeper understating of the robots' threats and security.

5. Conclusion

The robotics industry has increased and has become an important part of humans' lives. Robots have been involved in many fields such as surgery and healthcare. Self-driving cars have also contributed to reducing the number of accidents. However, these robots, like any other computer device, may be exposed to various cyberattacks. Our concept pays special attention to security and antitampering. We discussed three types of robots that are important for human life: self-driving cars, surgical robots, and eldercare robots. We mentioned the weaknesses and enhancements of the most famous robot operating systems (ROS) that may be the cause of some attacks, according to several researchers. In addition to the attacks that occur on these robots and some of the mechanisms to protect them, this could benefit the reader as well as the manufacturers of robots to obtain a deeper understating of the robots' threats and security.

Data Availability

The data will be available upon request from the corresponding author.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This research was supported by Taif University Researchers supporting project number: TURSP-2020/215, Taif University, Taif, Saudi Arabia.

References

[1] D. Quarta, M. Pogliani, M. Polino, F. Maggi, A. M. Zanchettin, and S. Zanero, "An experimental security analysis of an industrial robot controller," in *Proceedings of the 2017 IEEE symposium on security and privacy (SP)*, pp. 268–286, San Jose, CA, USA, May 2017.

[2] ISO 8373:2012 Robots and robotic devices –vocabulary, S. D. Johnson, J. M. Blythe, M. Manning, and G. T. W. Wong, "The impact of IoT security labelling on consumer product choice and willingness to pay," *PLoS One*, vol. 15, no. 1, Article ID e0227800, 2020.

[3] E. Fosch-Villaronga and C. Millard, "Cloud robotics law and regulation," *Robotics and Autonomous Systems*, vol. 119, pp. 77–91, 2019.

[4] B. Dieber, B. Breiling, S. Taurer, S. Kacianka, S. Rass, and P. Schartner, "Security for the robot operating system," *Robotics and Autonomous Systems*, vol. 98, pp. 192–203, 2017.

[5] K. A. Yousef, A. AlMajali, S. Ghalyon, W. Dweik, and B. Mohd, "Analyzing cyber-physical threats on robotic platforms," *Sensors*, vol. 18, no. 5, pp. 21–23, 2018.

[6] T. Gill, "Blame it on the self-driving car: how autonomous vehicles can alter consumer morality," *Journal of Consumer Research*, vol. 47, no. 2, pp. 272–291, 2020.

[7] S. Frennert, H. Aminoff, and B. Östlund, "Technological frames and care robots in eldercare," *International Journal of Social Robotics*, vol. 13, no. 2, pp. 311–325, 2020.

[8] M. Quigley, B. Gerkey, and W. D. Smart, *Programming Robots with ROS: A Practical Introduction to the Robot Operating System*, O'Reilly Media, Inc, Sebastopol, CA, USA, 2015.

[9] K. M. A. Alheeti, A. Gruebler, and K. McDonald-Maier, "Using discriminant analysis to detect intrusions in external communication for self-driving vehicles," *Digital Communications and Networks*, vol. 3, no. 3, pp. 180–187, 2017.

[10] C. Ekenna and B. Acharya, "Clustering and analysis of vulnerabilities present in different robot types," 2020, https://arxiv.org/abs/2008.08166.

[11] F. Frank, A. Paraschos, and P. Smagt, "ORC—a lightweight, lightning-fast middleware," in *Proceedings of the 2019 Third IEEE International Conference on Robotic Computing (IRC)*, pp. 337–343, IEEE, Naples, Italy, February 2019.

[12] J. Park, R. Delgado, and B. W. Choi, "Real-time characteristics of ROS 2.0 in multiagent robot systems: an empirical study," *IEEE Access*, vol. 8, pp. 154637–154651, 2020.

[13] B. Dieber, S. Kacianka, S. Rass, and P. Schartner, "Application-level security for ROS-based applications," in *Proceedings of the 2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 4477–4482, IEEE, Daejeon, Korea (South), October 2016.

[14] J. McClean, C. Stull, C. Farrar, and D. Mascarenas, "A preliminary cyber-physical security assessment of the robot operating system (ROS)," *Unmanned Systems Technology XV International Society for Optics and Photonics*, vol. 8741, Article ID 874110, 2013.

[15] S. Rivera, S. Lagraa, and R. State, "ROSploit: cybersecurity tool for ROS," in *Proceedings of the 2019 Third IEEE International Conference on Robotic Computing (IRC)*, pp. 415-416, IEEE, Naples, Italy, February 2019.

[16] J. Balsa-Comerón, Á. M. Guerrero-Higueras, F. J. Rodríguez-Lera, C. Fernández-Llamas, and V. Matellán-Olivera, "Cybersecurity in autonomous systems: hardening ROS using encrypted communications and semantic rules," in *Proceedings of the Iberian Robotics Conference*, pp. 67–78, Springer, Seville, Spain, November 2017.

[17] E. C. Ferrer, T. Hardjono, M. Dorigo, and A. S. Pentland, "Secure and secret cooperation of robotic swarms by using merkle trees," 2019, https://arxiv.org/abs/1904.09266.

[18] Y. Saito, F. Sato, T. Azumi, S. Kato, and N. Nishio, "Rosch: real-time scheduling framework for ROS," in *Proceedings of the 2018 IEEE 24th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA)*, pp. 52–58, IEEE, Hakodate, Japan, August 2018.

[19] R. Kumar, P. K. Pattnaik, and P. Pandey, *Detecting and Mitigating Robotic Cyber Security Risks*, IGI Global, Hershey, PA, USA, 2017.

[20] I. Priyadarshini, "Cyber security risks in robotics, in cyber security and threats: Concepts, methodologies, tools, and applications," *IGI Global*, vol. 61, pp. 1235–1250, 2018.

[21] N. Shahzad, T. Chawla, and T. Gala, "Telesurgery prospects in delivering healthcare in remote areas," *The Journal of the Pakistan Medical Association*, vol. 69, p. S69, 2019.

[22] H. Alemzadeh, D. Chen, X. Li, T. Kesavadas, Z. T. Kalbarczyk, and R. K. Iyer, "Targeted attacks on teleoperated surgical robots: dynamic model-based detection and mitigation," in *Proceedings of the 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 395–406, IEEE, Toulouse, France, July 2016.

[23] K. Chung, X. Li, P. Tang et al., "Smart malware that uses leaked control data of robotic applications: in the case of Raven-II surgical robots," in *Proceedings of the 22nd International Symposium on Research in Attacks, Intrusions and Defenses ({RAID} 2019)*, pp. 337–351, Beijing, China, September 2019.

[24] G. W. Clark, M. V. Doran, and T. R. Andel, "Cybersecurity issues in robotics," in *Proceedings of the 2017 IEEE conference on cognitive and computational aspects of situation management (CogSIMA)*, pp. 1–5, IEEE, Savannah, GA, USA, March 2017.

[25] T. Sahashi, A. Sahashi, H. Uchiyama, and I. Fukumoto, "A study of operational liability of the medical rescue robot under disaster," in *Proceedings of the 2011 IEEE/SICE International Symposium on System Integration (SII)*, pp. 1281–1286, IEEE, Kyoto, Japan, December 2011.

[26] A. A. Mokhtarzadeh and Z. J. Yangqing, "Human-robot interaction and self-driving cars safety integration of dispositif networks," in *Proceedings of the 2018 IEEE International Conference on Intelligence and Safety for Robotics (ISR)*, pp. 494–499, IEEE, Shenyang, China, August 2018.

[27] S. Gibbs, "Ford-backed self-driving car in crash that sent two to hospital," 2018, https://www.theguardian.com/technology/2018/jan/11/fordselfdriving-car-crash-hospital-argo-ai-pittsburgh.

[28] A. Bezemskij, G. Loukas, R. J. Anthony, and D. Gan, "Behaviour based anomaly detection of cyber-physical attacks on a robotic vehicle," in *Proceedings of the 2016 15th International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security (IUCC-CSS)*, pp. 61–68, IEEE, Granada, Spain, December 2016.

[29] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolafaei, and R. Das, "Attacks on self-driving cars and their countermeasures: a survey," *IEEE Access*, vol. 8, pp. 207308–207342, 2020.

[30] A. Banihani, A. Alzahrani, R. Alharthi, H. Fu, and G. P. Corser, "T-PAAD: trajectory privacy attack on autonomous driving," in *Proceedings of the 2018 IEEE Conference on Communications and Network Security (CNS)*, pp. 1-2, IEEE, Beijing, China, June 2018.

[31] S. Morimoto, F. Wang, R. Zhang, and J. Zhu, *Cybersecurity in Autonomous Vehicles, Introduction to Applied Informatics*, University of Hyogo, Kobe, Japan, 2017.

[32] Keen Security Lab, *Car Hacking Research: Remote Attack Tesla Motors*, keen security lab blog, Shenzhen,China, 2016.

[33] M. V. Florin, *Risk and Opportunity Governance of Autonomous Cars*, international risk governance center, Lausanne, Switzerland, 2016.

[34] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: contactless attacks against sensors of self-driving vehicle," *DEF CON*, vol. 24, no. 8, pp. 1–13, Article ID 109, 2016.