Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 04, No. 03, December 2018.

SEMI-QUANTITATIVE SECURITY RISK ASSESSMENT OF ROBOTIC SYSTEMS*

Anas AlMajali[1], Khalil M. Ahmad Yousef[1], Bassam J. Mohd[1], Waleed Dweik[2], Salah Abu Ghalyon[1] and Roa'a Hasan[1]

(Received: 28-Aug.-2018, Revised: 15-Oct.-2018 and 5-Nov.-2018, Accepted: 15-Nov.-2018)

ABSTRACT

Robots are becoming increasingly integrated in our daily lives, providing services in civilian, industrial and military applications. Many of those applications require robots to be remotely operated and controlled through communication channels. This makes the robotic system susceptible to a class of attacks targeting the connection between the controlling client and the robot, which can render the robot unavailable. The objective of our research is to identify, estimate and prioritize the risks associated with attacks targeting the availability of the robotic system. To achieve our objective, we perform an impact oriented semi-quantitative risk assessment of the loss of availability on the well-known PeopleBot™ mobile robot platform. We experimented with several well-known attacks that can target and affect the availability of the robot. To examine the cyber-physical impacts of the attacks on the robotic system, we setup a ten-goal test area and constructed a 2D map. The robot was programmed to tour the test area while being targeted by cyber-attacks. The physical impacts of the attacks are demonstrated in this paper. The results indicate that attacks can potentially lead to loss of availability which may result in serious cyber-physical consequences.

KEYWORDS

Cyber-physical security, Robot, Availability, Threats, Attacks, Vulnerability, Risk, Risk assessment, Mitigation, PeopleBot.

1. INTRODUCTION

Robots have been an essential part in many domains like industry, military, research and health [1]. In the Internet of Things (IoT) era, robots are gaining increasing interest to perform critical and non-critical tasks. For example, robots can be used to clean the house floor [2], which is a non-critical task. On the other hand, robots can be used to remotely perform surgical operations, which is considered critical to human life [3]-[4]. As any Cyber-Physical System (CPS), robotic systems are prone to cyber-physical attacks [5]-[6].

Many robotic applications require remote control and monitoring by an operator like Unmanned Aerial Vehicles (UAVs) [7]-[8]. Such applications require establishing a bidirectional communication path between the robot and the controller. The controller can send direct commands to the robot to perform specific functions (e.g. move forward). Based on the application, the controller receives data from the robot (i.e., sensory data), which may be used to make critical decisions, especially in medical and military applications. The communication between the robot and the controller can be wireless (e.g. WiFi - IEEE 802.11) or wired (e.g. Ethernet - IEEE 802.3), utilizing different standards and protocols [9]–[11].

Robotic systems are susceptible to cyber-physical attacks, especially the ones targeting the communication path between the robot and the controller [1]. Attacks on the communication path causing loss of availability are referred to as Denial of Service (DoS) attacks. DoS leads to the loss of the communication between the robot and the controller, as well as the loss of the control and monitoring services. It is important to mention that losing the monitoring and control abilities while performing

*This paper is an extension to our published paper "K. Ahmad Yousef, A. AlMajali, R. Hasan, W. Dweik and B. Mohd, "Security risk assessment of the PeopleBot mobile robot research platform," in 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), pp. 1–5, 2017".

1. A. AlMajali, K. M. A. Yousef, B. J. Mohd, S. Abu Ghalyon and R. Hasan are with Department of Computer Engineering, The Hashemite University, Zarqa, Jordan. Emails: almajali@hu.edu.jo, khalil@hu.edu.jo, bassam@hu.edu.jo, salah.g.ghalyon@hu.edu.jo and roaa.mamoun@gmail.com
2. W. Dweik is with Department of Computer Engineering, The University of Jordan, Amman, Jordan. Email: w.dweik@ju.edu.jo

critical missions (e.g. surgical operations, defense and space missions) may result in undesirable consequences and harm human lives. This raises the flag and demonstrates the importance of performing risk assessment on robotic platforms, especially if they are responsible for critical missions.

Despite the fact that cyber-physical security is very important, it is usually overlooked. This is evident by the study performed by [12], which indicates that about 30% of the studied robots are accessible from the Internet posing a security threat. The same study also indicates that 76% of the surveyed members did not perform a professional cyber-security assessment on their infrastructure, while more than 50% of the surveyed members did not consider cyber-attacks as a realistic threat. This demonstrates the lack of awareness of the current security posture in the robotic system domain.

The main objective of this paper is to perform cyber-physical security risk assessment on the PeopleBot™ research mobile robot platform [13]. By performing this risk assessment, we raise the awareness of possible threats on the robotic platforms. The robotic system, which is used in this paper as a use-case to perform the risk assessment, consists of the following components (see Figure 1):

- The PeopleBot robot, which runs a server application on its on-board computer to which the client connects. The client then connects to the server (i.e., robot), issues commands and monitors the operation of the robot.
- The client, which is simply a computer machine (e.g. PC or laptop) that runs certain applications to communicate with the robot.
- The network communication medium, which connects the robot and the client. In our case, it is the WiFi access point.
- The attacker, which performs cyber-physical attacks to affect the availability of the robot.

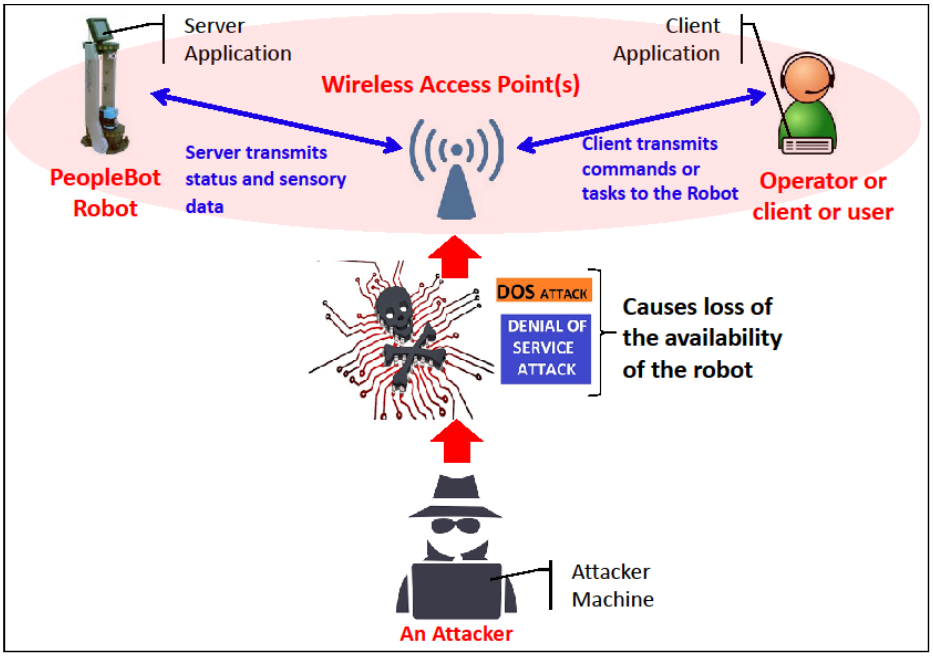

Figure 1. The PeopleBot robotic system under study.

This paper extends our previous work in which we performed qualitative risk assessment of mobile robots [14]. The main contributions of this paper can be summarized as follows:

- We identify possible threats and vulnerabilities that may lead to the loss of availability in the robotic platform using an impact-oriented approach. While those threats and vulnerabilities are not unique to the robotic platform and may apply to any computer network, it is important to study the physical consequences on robotic platforms and the impact on their critical missions.
- We create an experimental test area using the PeopleBot robot. We construct a 2D line and point

map of our research lab environment, identify and localize ten goals within the map for the robot to navigate and tour. We analyze the impact of the attacks on the robot while performing the experimental task of touring the goals. The goals are setup to emulate robotic tasks in a real environment.

- We estimate the risk of each identified threat by following a semi-quantitative approach based on NIST adversarial risk assessment template proposed in [15]. This assessment template was employed in numerous research work, such as the work in [16]–[18]. In this approach, representative numbers are used to estimate the risk of the loss of availability. The main advantage of this approach is that it compromises a middle ground between qualitative and quantitative risk assessments. To the best of our knowledge, this is the first study to perform such a semi-quantitative analysis on vulnerabilities in the robotic platforms.
- We prioritize the risk of each threat based on the risk estimation, so that more severe threats are handled first.
- We discuss the possible physical consequences of the identified threats.

The rest of the paper is organized as follows. In Section 2, related work is discussed. In Section 3, we introduce the PeopleBot mobile robot platform. In Section 4, we present the risk assessment approach used in this paper and the experimental results. Section 5 presents our discussion on the performed security attacks. Finally, we conclude the paper and provide our future directions in Section 6.

2. RELATED WORK

Recently, the security risk assessment on robotic platforms or CPSs has been a very hot research topic. Despite it is a critical issue, the number of publications addressing risk assessment on robotic platforms is limited. In fact, no systemic analysis of industrial robot security was conducted [12]. Further, there is inadequate understanding of what are the actual risks and the affected security goals [19]. In what follows, we present a literature summary for security threat analysis and detection for several robot platforms or CPSs.

Javaid et al. [7] analyzed different security threats to Unmanned Aerial Vehicles (UAVs). The threat model is based on listing vulnerabilities that can affect confidentiality, integrity and availability. The authors followed a typical risk evaluation approach.

Vasconcelos et al. [20] used three DoS attack tools to experimentally evaluate and analyze UAV behavior. The information gathering about the targeted network is performed using a reconnaissance attack that leverages an open source security tool called Network Mapper (Nmap). Next, DoS attacks are launched using Low Orbit Ion Cannon (LOIC), Netwox and Hping3 automated tools. All experiments were conducted in real time on AR.Drone 2.0 UAV while navigating inside a University building. The results show that Hping3 tool causes the highest average network latency of 455.82 milliseconds, which negatively impacts the video streaming application along with other computer vision applications.

Bezzo et al. [21] presented a control-level resiliency estimation technique against security sensor attacks in autonomous robots. The technique is based on a recursive algorithm, which exploits the redundancy in the sensor measurements. Although the proposed approach is generic, the authors used a case study on a vehicle cruise-control, where the latest N velocity measurements are recursively filtered and the variance of the measurements noise is considered to estimate resiliency. In addition, the authors validated the efficacy of their technique through outdoor experiments on two unmanned ground robots.

Bonaci et al. [19] discussed security threats for tele-operated surgical robot Raven II, which is an advanced surgery system. The authors demonstrated that intruders can maliciously control a wide range of the robot functions by performing disruption and manipulation attacks against the surgeon robot communication link that is likely to be wireless. The attacks are based on man-in-the-middle model and they successfully impacted the safety and usability of the surgical robot, which could potentially result in legal and privacy violations. Batson et al. [22] conducted an analysis to identify threats and vulnerabilities in the system's concept for Unmanned Tactical Autonomous Control and Collaboration (UTACC). Jones and Straub [23] presented a two-stage intrusion detection system (IDS) for detecting

network intrusions and malware in autonomous robots. The authors utilized and trained a deep neural network to detect commands that deviate from the expected behavior.

Maggi et al. [24] studied the impacts of system-specific attacks on real industrial robots. The authors analyzed two attacker models: network attacker (i.e., communicates with the robot over the network) and physical attacker (e.g. the robot operator). Five attack scenarios were demonstrated (e.g. altering the control-loop parameters, tampering with calibration parameters, …etc.) and the physical impacts in addition to the compromised requirements (i.e., safety, integrity and accuracy) were discussed. Similarly, Quarta et al. [12] performed an experimental security analysis of an ABB 6-axis IRB140/IRC5 industrial robot controller. The authors exploited several software vulnerabilities in the robot main computer (MC). They mainly exposed and focused on the network services that are essential for the operation of the robot, such as FTP (File Transfer Protocol).

Lera et al. [25] presented a taxonomy that classifies cyber-security attacks, which target safety and security of service robots. For safety threats, the proposed taxonomy differentiates between the risks according to the user type (e.g. domestic, commercial). For each user type, the expected risks are classified according to the level of the physical impact (e.g. destruction, partial damage) and the origin of the risk. On the other hand, security threats are classified according to the robot function (i.e., personal or commercial) and the type of sensors that the robot is equipped with.

Vuong et al. [26] proposed two different approaches for detecting attacks in robotic vehicles. The first approach was based on using decision trees and the second approach was based on using deep learning. Loukas et al. [27] argued that the limited rule-based or lightweight machine learning techniques used for cyber-physical intrusion detection of vehicles can be substituted with more advanced techniques using computational offloading to the cloud. The boosted processing power is used to implement a deep multilayer perception and recurrent neural network architecture, which receives the real-time cyber-physical data captured in the robotic vehicle and analyzes it to detect intrusions. The authors showed that the deep learning technique noticeably improves the detection accuracy; however, the long detection latency and the security of the external network between the vehicle and the cloud must be carefully considered.

Similar to this work, some researchers focused on risk assessment for robotic platforms. Chen et al. [28] assess the cyber security risks in industrial control systems (ICSs) (e.g. SCADA) by quantifying the availability using the concept of mean failure cost (MFC). Various security issues arise as the ICS becomes more integrated with IT networks. Hence, it is important to compare the cost of implementing security counter-measures with the expected losses of cyber-attacks, especially due to the limited resources.

Dominic et al. [29] proposed a risk assessment framework for autonomous and cooperative automated driving. The authors started by describing the recent attack surfaces and then discussing the proposed application-based threat enumeration and analysis framework. For each threat, model parameters are specified and accordingly the result vector which characterizes the risk level of the threat is computed. The result vector reflects attack potential, motivation and impact.

Very recently, the authors in [30] performed qualitative risk assessment of several vulnerabilities identified specifically to the Adept mobile robots (e.g. the PeopleBot [13]); namely, the MobileEyes/arnlServer client/server robotic applications. Such applications are necessary to establish the network connection between the Adebt robots and their clients or users. In contrast to this work, this paper proposes a semi-quantitative security risk assessment, where representative numbers are used to estimate the risk of the loss of availability. The main advantage of this approach is that it compromises a middle ground between qualitative and quantitative risk assessments. Additionally, the focus of this paper is mainly on identifying and raising awareness of possible threats and vulnerabilities that may lead to the loss of availability in the robotic platform under study, the PeopleBot.

3. THE PEOPLEBOT MOBILE ROBOT PLATFORM

Figure 2 shows the PeopleBot mobile robot from Adept company[13], which is used as a case study for our proposed security risk assessment. The PeopleBot robot is a research platform that can be used in service and human robot interaction (HRI) projects and in other projects as well [31]. It consists of

Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 04, No. 03, December 2018.

multiple hardware and software components: main computer, mechanical actuators, controllers, sensors such as lidars (or laser range finders) and cameras, human-interaction devices, control logic, firmware and operating systems (either Windows 7 or Ubuntu 12.04). The main computer of the PeopleBot is connected to the sensors either through controllers or isolated subnet *via* an on-board network access point. There are various interfaces or ports on the robot that include-but are not limited to: serial port, Ethernet RJ45 port, USB ports and wireless adapter.

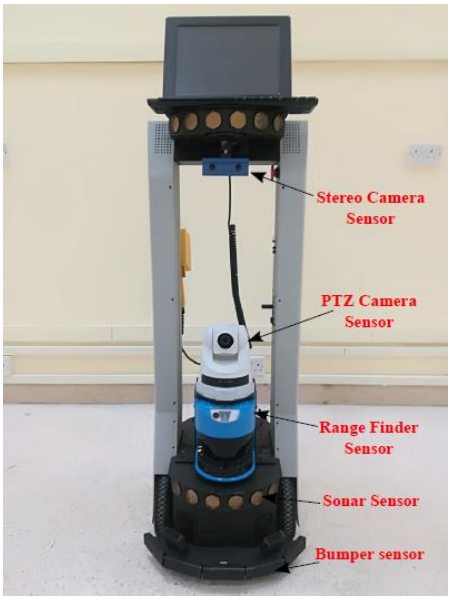

Figure 2. The PeopleBot mobile robot platform, where several sensors are attached to the robot (e.g. pan-tilt-zoom (PTZ) camera, laser range finder, sonars, stereo camera, …etc.).

Several software packages [13] are pre-installed on the robot main computer, such as ARIA, ARNL, MobileEyes, Mapper3, …etc., that enable the control of the robot, its sensors and accessories. In many applications, the robot is often required to be remotely accessible either through a connection to the Internet, or *via* dedicated wireless access points. Some of those applications include:

- Museum robotic guide application [32].
- Map building and robot self-localization [33]-[34].
- Robotic assistant for healthcare applications [35].
- Gesture-based multi-robot control application and robotic desk clerk application using face recognition [10].
- Application of Myo Armband System to control a robot interface [36].
- Extrinsic calibration of camera and 2D laser sensors without overlap [37].

As it can be seen, all of the above applications of the PeobleBot are very important, critical and thus must be protected against cyber-physical attacks. Consequently, this is one of the main goals of this research.

3.1 Experimental Setup

The experimental setup used to perform the impact-oriented risk assessment on the PeopleBot robotic system (shown in Figure 1) assumes the following components:

- The robot runs a server application on its on-board computer. Such an application is assumed to communicate and access all the sensors pre-installed on the robot, fully control the robot movement, have already established a network connection to a certain network and allow (single or multiple) connections from authorized clients to connect to the robot to access/ monitor all of its features, sensors and movement.
- An operator or a client runs certain applications to communicate with the server on his/her own computer.
- The robot network to represent a wireless access point, in which the client can connect to the

server in a client-server mode.

- Only cyber-attacks that can result in the loss of availability on the robot are considered. The attacks target one or more of the following:
  - Application resources; e.g. server application.
  - System resources; e.g. network handling software.
  - Network bandwidth.

To evaluate the impact of the attacks, we created an experimental test area using the PeopleBot robot. We created a 2D line and point map of our research lab environment (6×9 m^2 area). We identified and localized ten goals within the created map of our lab as shown in Figure 3 for the robot to navigate and tour. These goals may emulate important stops for the robot within an industrial workplace application or other applications. The goals are 60 cm spaced apart. The number of goals and separating distances were chosen based on initial feasibility trials to provide adequate accuracy. When a "tour goals" command is issued, the robot tours the goals one by one starting from goal 1. The robot sends its real-time coordinates to the client so that it monitors the physical location of the robot on the map.

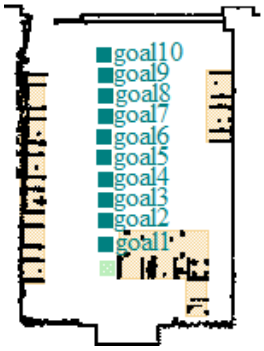

Figure 3. Ten identified and localized goals within the 2D line and point map of our research lab.

4. Risk Assessment of the PeopleBot Robot

Risk is usually defined as the expected impact of an event on a system or organization [15]. Within the context of this paper, an event refers to a cyber-attack and a system refers to the robotic system. Therefore, the risk determination is a function of the impact of an attack and the probability that this attack occurs and succeeds. The impact of an attack measures the loss of one or more of the main security requirements: confidentiality, integrity and availability. The main focus of this research is only on the availability security requirement. The probability that an attack occurs and succeeds depends on the vulnerabilities and threats of the system under study (i.e., the robot). Hence, the risk determination of a given attack can be expressed as follows:

$$Risk = Vulnerability \times Threat \times Impact \quad (1)$$

Risk assessment is the process of identifying, estimating and prioritizing risks to a system or organization [15]. The flow chart in Figure 4 is adopted from NIST risk assessments [15] and shows the main steps of the assessment process. Next, we present the details of the risk assessment process for the attacks under study.

Figure 4. Risk assessment process [15].

4.1 Risk Identification

To identify the risk, we follow an impact-oriented analysis approach to assess the risk of the attacks on the robot. We focus on the loss of availability as the impact, because this could lead to devastating consequences. As mentioned earlier, the user can connect in a client-server mode to the robot at the

application level to perform certain functions (e.g. transferring medical equipment) and retrieve data (e.g. geographical coordinates). The client and the server have to be available in order to perform the required functions of the robot. Losing availability may have physical impacts, like human injury or physical damage of the robot itself.

4.2 Risk Estimation

To estimate the risk, we have to assess the vulnerabilities and threats that may cause loss of availability. We follow a semi-quantitative risk assessment approach to estimate the risk. In this approach, representative numbers are used to estimate the level of each risk factor, like the severity of a certain vulnerability. The semi-quantitative assessment approach represents a middle-ground between qualitative and quantitative approaches. The semi-quantitative assessment facilitates better comparison and prioritization compared to the qualitative assessment approaches, which rely on non-numerical levels (e.g. low, moderate, high). On the other hand, the semi-quantitative assessment is easier to implement than the quantitative assessment, which requires using specific metrics to measure different risk factors in the assessment process (e.g. the impact of the attack) [15]. Identifying those metrics is challenging in the cyber security domain.

4.3 Risk Prioritization

After estimating the risk level for the attacks under study, the associated threats can be prioritized based on the numerical values calculated to each threat. Next, we present our risk assessment of the loss of availability of the robot.

4.4 Attack Analysis

Figure 5 demonstrates the attack tree for the loss of availability. The root of the attack tree represents the ultimate goal of the attacker, which is causing the loss of availability. In addition, the loss of availability may lead to cyber-physical threats depending on the task that is performed by the robot. The branches of the tree represent the ways and techniques through which the attacker can achieve the ultimate goal. There are three main ways to perform a Denial-of-Service (DoS) attack: attacking the network bandwidth, attacking system resources or attacking the application resources. The next level of the tree represents the techniques that can be used to perform a DoS attack. This attack tree is not inclusive, as it does not cover all possible ways to achieve the loss of availability.

In our assessment, we focus on vulnerabilities that exist in the system itself, especially the network stack. In what follows, we discuss various attacks that target the client, the server or the access point and present the associated experimental results. We want to emphasize that those attacks are not unique to the robotic system. A group of those attacks can target any device that is connected through a network (e.g. SYN flood). On the other hand, another group of those attacks can target devices that are connected through WiFi (e.g. de-authentication attack).

4.4.1 Application Layer Attack

This attack can be implemented on a wireless or wired network. It targets certain application on the server. The attacker sends a large number of requests to the target application on the server, overwhelming its processing and network resources. Typically, HTTP requests are used to exhaust the server. However, the robot does not run a web server, it runs an ARNL server on port 7272 and waits for connections from the client (MobileEyes). An attacker can exploit the ARNL server by initiating a large number of connections at the application level.

Experimental results: we performed a Distributed DoS (DDoS) attack, where seven adversary machines sent application level requests to the server. Initially the robot completed the ten-goal tour. However, after 15 minutes (on average) of the attack, the robot server freezes, old connections are lost and no new connections could be established.

4.4.2 TCP SYN Flood

This attack can be implemented on a wired or wireless network. A TCP SYN flood attack usually targets the operating system's network handling capability of any server that is listening on a certain port. The

"Semi-quantitative Security Risk Assessment of Robotic Systems", A. AlMajali, K. M. A. Yousef, B. J. Mohd, W. Dweik, S. Abu Ghalyon and R. Hasan.

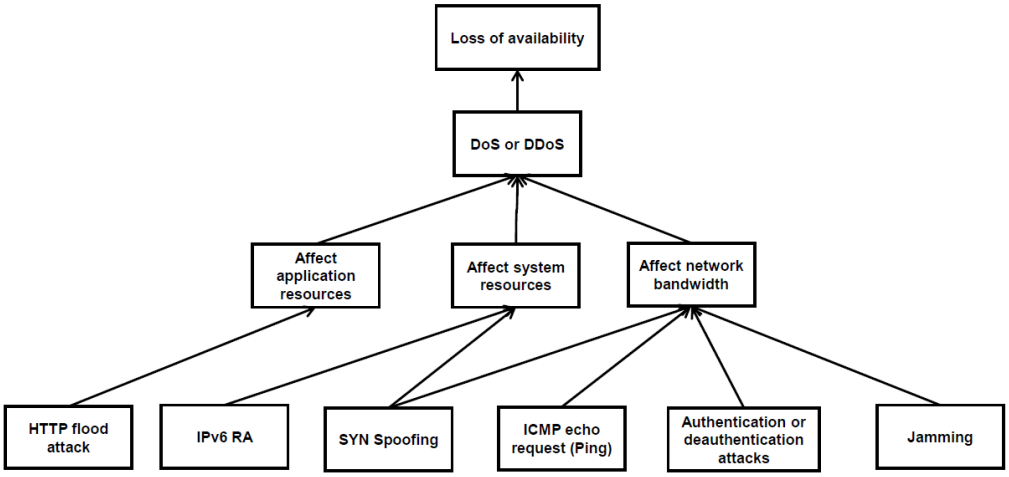

Figure 5. Attack tree with the loss of availability as the ultimate goal of the attacker.

attacker attempts to initiate a large number of TCP connections with the server, where each initiated TCP connection requires what is known as the three-way handshake process (SYN, SYN-ACK, ACK). The server allocates system resources to handle those connections. By overwhelming the server with the attacker's connections, the server will not have enough resources to handle legitimate connections with the client machine. Hence, the connection with the server can be lost, resulting in the loss of availability of the robot. However, this attack can be easily mitigated by blocking the attacker's IP address.

On the other hand, the attacker can use IP source address spoofing to improve the attack. In this case, the attacker uses spoofed IP addresses, so that the server responses are sent to devices that are unreachable (i.e., did not initiate the connection). This way, blocking the attacker's IP does not mitigate the attack. In summary, this kind of attack can result in overwhelming both the operating system of the robot and the robot network.

Experimental results: we performed this attack by sending spoofed TCP SYN flood targeting the robot on port 7272 (ARNL server). Whenever this attack is active, legitimate new connections could not be established from the client to the robot, so no commands could have been issued. Therefore, we could not evaluate the location of the robot as the command could not be issued in the first place. If the connection had already been established before the attack, then the attack fails.

4.4.3 IPv6 Router Advertisement Floods

In IPv6 Router Advertisement (RA) floods, the adversary floods the robot network with fake IPv6 RA packets or messages. Any computer, including the robot, running a vulnerable operating system (on which IPv6 routing is enabled), will be overwhelmed with those fake IPv6 RA packets. In order to perform this attack, the adversary should be connected to the same network of the victims (i.e., the robot network).

Experimental results: the results of this attack varied based on the vulnerabilities of the underlining operating system of the robot. We performed an IPv6 attack while running Windows 7 on the robot. Windows 7 is vulnerable to this attack. First, we issue a "tour goals" command from the client machine and immediately start the attack. Subsequently, after starting the attack, the robot operating system freezes, the robot stops before reaching goal 2 and the client loses connection with the robot. To restart the robot, it requires hard reset. Ubuntu operating system is not vulnerable to this type of attack. If client machine is also running a vulnerable operating system, then it will also freeze.

4.4.4 ICMP Echo Request

This attack works in the network layer. The attacker floods the robot or the client with ICMP echo request (ping) packets overwhelming the network of the robot. This degrades the network performance and causes legitimate traffic to be lost rendering the robot unavailable. To improve the attack, the attacker can use IP source address spoofing.

Experimental results: we performed a DDoS attack, where seven adversary machines sent spoofed ICMP echo requests to the server. Initially, the robot completed the-ten goal tour. However, after 45 minutes (on average) of the attack, the robot server freezes, old connections are lost and no new connections could be established.

4.4.5 De-authentication Attack

In a de-authentication attack, the attacker sends a de-authentication frame to the victim machine with a spoofed source address of the access point to terminate the victim's connection with the access point. This results in losing the WiFi connection and disconnecting the client from the server. This attack does not require encryption, so it can be performed by an outsider who can sniff the WiFi connection to get the MAC address of the victims and the access point [38].

Experimental results: we performed this attack after issuing a "tour goals" command from the client. The robot and client were immediately disconnected from the network. The client's map showed that the robot did not reach goal 2. However, this attack did not stop the robot from physically touring all the goals.

4.4.6 Jamming Attack

If the robot and client are connected using WiFi (IEEE 802.11), then they are susceptible to jamming attacks. This kind of attack requires that the attacker be in close proximity to the network under attack. The jammer has to operate in the 2.4 GHz or 5 GHz radio frequency which is used by the WiFi technology. This attack was not performed in our research, as it is a pure physical layer test which is beyond the scope of this paper.

4.4.7 Attack Summary

We specifically chose the previous attacks, because they demonstrate various ways to cause loss of availability (DoS). With the exception of the jamming attack, no special equipment is necessary and script kiddies can implement those attacks (e.g. using Kali Linux [39]). Table 1 summarizes attack characteristics and results. It demonstrates the physical domain of the attack (wired/wireless) and the targeted resources by the attack. Furthermore, Table 1 lists the impact of the attacks on the robot.

4.5 Semi-quantitative Risk Assessment Determination

As mentioned earlier in this section, it is convenient to use a semi-quantitative risk assessment approach. Table 2 represents the mapping between the qualitative and semi-quantitative values [15]. Following [15], we choose to use the semi-quantitative values in the range between 0 and 10, where 10 represents the maximum severity of vulnerability or impact.

The overall likelihood of any threat is assigned a value between 0 and 1 based on the likelihood of attack initiation and the likelihood of success of the initiated attack. Consequently, the risk level is the product of the overall likelihood and the impact of the attack, as demonstrated in Equation 2.

$$Risk = Overall\ Likelihood \times Impact; \quad (2)$$

where the overall likelihood of a threat is computed as a function of the likelihood of attack initiation and the likelihood of success of the initiated attack.

Now, we discuss how to generate the risk table, which summarizes the risk assessment process. We used the adversarial risk assessment template proposed in [15]. Table 3 presents the end result of the risk assessment process for the threat events under study. Following, each item in Table 3 is discussed (for more details about those items please refer to tables D-3, D-4, D-5, E-4, F-2, F-5 and H-3 in [15]):

Threat Event: refers to the threat that is currently being analyzed.

1) *Threat Sources*: refer to the threat source, which can be an insider, outsider, trusted insider or privileged insider [15]. Some attacks require the attacker to communicate with the robot, client or access point. This implies that the attacker has to be on the same network of those devices (unless the robot is configured to be remotely accessed, like having a public IP address). This applies to application level attacks, TCP SYN floods, IPv6 RA floods and ICMP echo requests.

Table 1. Summary of threat characteristics and experimental results

Threat	**Wireless or wired**	**Target resources**	**Impact on the robot**
Application level attack	Wireless	Application resources	Connection with the robot is lost. No new connections could be established.
TCP SYN flood attack	Both	System resources and/or network bandwidth	No new legitimate client connections could be established with the robot.
IPv6 RA attack	Both	System resources	OS (Widows 7) freezes, robot stops before goal 2 and robot disconnected from client.
ICMP echo request flood	Both	Network bandwidth	Connection with the robot is lost. No new connections could be established.
De-authentication attack	Wireless	System resources	Robot disconnected from client before reaching goal 2 and robot is moving without supervision.
Jamming attack	Wireless	Network bandwidth	No connection between the client and the robot.

Table 2. Mapping of the qualitative levels to the semi-quantitative levels

Qualitative level	Very High	High	Moderate	Low	Very Low
Semi-quantitative level	10	8	5	2	0

On the other hand, de-authentication and jamming attacks can be conducted by outsiders with close proximity to the target machines.

2) *Capability*: this is one of the characteristics of the threat source. An attacker with high capability is one with high level of expertise and is well-resourced. Because of the increasing interest in cyber-security, there is an increasing number of highly capable threat sources, especially in a scientific and research environment. The reader should note that the attacks we are implementing can be implemented by a person with moderate or low capabilities.

3) *Intent*: this is one of the characteristics of the threat source. The adversary seeks to undermine critical functions of the system and may result in physical damage by causing loss of availability.

4) *Targeting*: this is one of the characteristics of the threat source. The adversary targets a specific mission or function within an organization (i.e., the target of the attack is not random; however, the threats discussed in this work are not unique to the robots).

5) *Relevance*: indicates how relevant the threat event is to the system under study. For example, if the threat event already happened in the system, then it is confirmed. As we do not have evidence that those threats happened (i.e., reported in the literature as real attack) on a PeopleBot robot, we rank them as possible.

6) *Likelihood of attack initiation*: refers to the likelihood that the adversary will initiate the attack. Hence, it depends on adversary intend, capability and targeting [15]. To find this likelihood, we compute the normalized average of those three values as shown in Equation 3.

$$normalized\ average = \frac{computed\ average}{10} \tag{3}$$

7) *Severity of vulnerabilities*: all of our implemented attacks make use of the vulnerabilities in the communication link with the robot, which are exploitable and exposed. Application level, TCP SYN floods and ICMP echo request can be mitigated by blocking the source IP address of the attacker. However, if IP address spoofing is used, then protecting against those attacks will be difficult. As such, the severity of the attacks is ranked high. IPv6 RA floods can be easily mitigated by disabling IPv6 routing, so it is ranked as moderate. In addition, Windows operating

systems are highly affected by this attack, while Linux operating systems are moderately affected, because they only take the first 15 route advertisements and ignore the remaining. De-authentication and jamming attacks are very difficult to be stopped [40], [41].

8) *Pervasiveness of predisposing conditions*: vulnerabilities that apply to all robots running the same setup are ranked high.

9) *Likelihood Initiated Attack Succeeds*: This item depends on the threat source capability, severity of the vulnerability and predisposing conditions. To compute the probability of a successful initiated attack, we average those three factors and then normalize them.

10) *Overall Likelihood*: this is a combination of the likelihood of attack initiation and the likelihood of the successful initiated attack. In order to capture the effect of both likelihoods, we average the two values.

11) *Level of impact on the robot*: severe or catastrophic effect on the robot system means high impact. All the attacks discussed in this paper cause high impact, which is the loss of availability of the robot.

12) *Risk*: this is the final risk assessment measure, which is the product of the overall likelihood and the level of impact (Equation 2). The risk value represents an estimation of the risk of each threat and can be used to prioritize risk handling; for example, (application level attack):

- The threat source characteristics are all ranked high and hence they were assigned a value of 8 based on Table 2.
- The likelihood of attack initiation is computed based on Equation 3 using the threat source characteristics values (i.e., $\frac{\frac{8+8+8}{3}}{10} = 0.8$).
- The severity of vulnerabilities and the pervasiveness of predisposing conditions were all ranked high and hence they are assigned a value of 8.
- The likelihood that the initiated attack succeeds is computed based on Equation 3 using the threat source capability, severity of vulnerabilities and the pervasiveness of predisposing conditions values (i.e., $\frac{\frac{8+8+8}{3}}{10} = 0.8$).
- The overall likelihood is computed by taking the average of the likelihood of attack initiations and the likelihood that the initiated attack succeeds (i.e.,$\frac{0.8+0.8}{2} = 0.8$).
- The level of impact on the robot is ranked high and thus is assigned a value of 8.
- The risk level is computed based on Equation 2 (i.e., $0.8 \times 8 = 6.4$).

In the following section, we discuss the physical consequences for the loss of availability on the robot.

5. DISCUSSION

In this section, we discuss the physical consequences of the loss of availability on the robot. Since this is an application-specific process, we consider several applications of the robot. We consider the loss of availability as the impact of the attack in the risk assessment process. The impact values in the risk assessment process can be assigned based on the specific robotic application. For example, if the robot freezes in a high traffic area (e.g. airport application), then this may cause more damage than if it continues with the current task. On the other hand, it may be safer for the robot to stop and abort its current task if moving with precise supervision is required (e.g. industrial applications).

5.1 Hospital Application

This application is for the case when the robot is operated in a hospital that is fully covered by a wireless LAN. In this application, the robot is assumed to be used in two critical missions: creating a 2D map of the hospital and performing time-sensitive tasks (e.g. delivering medical supplies and equipment) [42]. Both missions require the robot to be remotely controlled and monitored by a human operator through the wireless LAN. Creating a map requires logging lots of data generated from the 2D laser range finder sensor and the wheel encoders of the robot [33]. The operator connects to the robot through an SSH

Table 3. Risk Assessment Table of the PeopleBot robot

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	**Threat Sources**	**Threat Source Characteristics**			**Relevance**	**Likelihood of attack initiation**	**Severity of vulnerabilities**	**Pervasiveness of predisposing conditions**	**Likelihood of Initiated Attack Success**	**Overall Likelihood**	**Level of impact on robot**	**Risk**
		Capability	**Intent**	**Targeting**								
Application level attack	Insider	8	8	8	Possible	0.80	8	8	0.80	0.80	8	6.40
TCP SYN flood attack	Insider	8	8	8	Possible	0.80	8	8	0.80	0.80	8	6.40
IPv6 RA floods	Insider	8	8	8	Possible	0.80	2	8	0.60	0.70	8	5.60
ICMP echo request attack	Insider	8	8	8	Possible	0.80	8	8	0.80	0.80	8	6.40
De-authentication attack	Insider or outsider	8	8	8	Possible	0.80	10	8	0.87	0.84	8	6.72
Jamming attack	Insider or outsider	8	8	8	Possible	0.80	10	8	0.87	0.84	8	6.72

session and runs a data logging program, such as “sickLogger”[43]. Moreover, the operator runs a monitoring program to control the robot movement using image sequences from the camera sensor. While running these applications, multiple physical consequences are possible if the robot becomes unavailable as a result of exploiting the attacks discussed in Subsection 4.4. First, the robot may get physically damaged due to open stairs in the hospital environment. Second, sudden accidents may cause human injuries or damage critical equipment.

On the other hand, performing time-sensitive delivery tasks requires the operator and the robot to connect using client-server programs; “MobileEyes” and “arnlServer”[43]. The robot runs the ARNLServer program which loads the hospital map in the robot’s memory then waits for commands from the client program. The client runs the MobileEyes program, which connects to the ARNLServer and navigates the robot to destinations within the map using IR, bumpers, camera, sonars and laser range finder sensors. One critical physical consequence of loss of availability in this scenario is delaying or preventing the robot delivering urgent medical supplies to the hospital operation room. Another critical consequence is that the robot may get physically hijacked.

5.2 Airport Application

This application considers the case when the robot is operated at airports to perform two critical tasks: delivering passengers’ luggage to their respective terminals [44] and carrying out security checks for travelers [45]. To achieve the first task, the robot needs to create an airport map for luggage delivery. Creating the airport map can be done exactly the same fashion in the hospital scenario; hence, similar physical consequences might occur after a successful attack that leads to loss of availability. Once the map is constructed, the “MobileEyes” and “ARNLServer” client-server applications are used to load the map in the robot’s memory and send navigation commands to the robot for delivery purposes. Losing availability while delivering passengers’ luggage might result in luggage being delayed, which causes customer dissatisfaction and impacts the airline public image. More severely, the luggage might maliciously get stolen, replaced or delivered to incorrect terminals.

To achieve the second task (i.e., performing security checks for travelers), the robot uses its high-definition cameras and facial recognition software probably running on the operator's computer. Losing availability while carrying out such critical task has the dire consequence of allowing suspects to escape the security check.

5.3 Industrial Application

This application considers the case when the robot is operated at an industrial warehouse for helping in the production of expensive instruments and equipment. This is one of the critical scenarios, as the robot needs to make precise movements and actions. Losing availability of the robot could result in a financial impact. In this case, financial losses can be huge due to production halt, business disruption and replacement or remediation costs. It is clear that the physical consequences described above can lead to catastrophic results. Security experts need to carefully consider taking well-studied countermeasures to reduce or even prevent attacks. Surely this needs to be considered per each application of the robotic platform.

5.4 Mitigating Robot Cyber-Security

In this subsection, we suggest some recommendations as possible mitigation techniques for the loss of availability of the robot. It is important to mention that building a secure robot is not a simple task. However, considering and implementing the following recommendations can highly improve the cyber-security of the robot.

- Encrypt the robot communications.
- Assure that only authorized users have access to the robot network, on-board computer, services and functionality.
- Install operating systems updates to fix known vulnerabilities.
- Invest in cyber-security education for everyone using the robot.
- Enforce a backup plan policy in case the robot becomes unavailable.
- Enable SYN Cookies to protect against TCP SYN floods [46].

5.5 Limitations

The main limitation of this approach is the dependency on identifying the vulnerabilities of the system. This requires deep knowledge of all the systems integrated to operate the robot, including hardware, software, operating systems, communications, …etc.

6. CONCLUSIONS

In this paper, we identified, estimated and prioritized the risks associated with attacks targeting the availability of the robotic system.

The paper discussed several attacks that can result in losing the availability of the PeobleBot robot. We setup a ten-goal test area in our research lab. The robot is commanded to tour the ten goals while being attacked. We discussed the experimental results from each attack. The paper presented an impact-oriented analysis approach to assess the risk of these attacks as demonstrated in Table 3. We discussed the physical impacts for losing the availability of the robot while performing several critical applications. The severity of the physical impacts raises the flag of the requirement of considering effective cyber-security countermeasures.

Future work could focus on extending the semi-quantitative risk assessment to a quantitative assessment. In addition, one area of research is to examine attacks on integrity and confidentiality of robotic systems. We also plan to analyze the resilience of robotic systems to cyber-physical attacks. By analyzing the resilience, we investigate how the robotic system responds and recovers from failures that are caused by cyber-physical attacks.

ACKNOWLEDGEMENTS

This research was supported by a grant from the Deanship of Scientific Research at the Hashemite University, Zarqa, Jordan.

REFERENCES

[1] I. Priyadarshini, "Cyber Security Risks in Robotics," Detecting and Mitigating Robotic Cyber Security Risks, IGI Global, pp. 333–348, 2017.

[2] J. L. Jones, N. E. Mack, D. M. Nugent and P. E. Sandin, Autonomous Floor-cleaning Robot, 2009.

[3] B. Hannaford et al., "Raven-II: An Open Platform for Surgical Robotics Research," IEEE Transactions on Biomedical Engineering, vol. 60, no. 4, pp. 954–959, 2013.

[4] 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," Proc. of the 46th Annual IEEE/IFIP Inter. Conf. on Dependable Systems and Networks (DSN), pp. 395–406, 2016.

[5] C. Cerrudo and L. Apa, "Hacking Robots before Skynet1," IOActive Website, 2017.

[6] A. Khalid, P. Kirisci, Z. H. Khan, Z. Ghrairi, K.-D. Thoben and J. Pannek, "Security Framework for Industrial Collaborative Robotic Cyber-physical Systems," Computers in Industry, vol. 97, pp. 132–145, 2018.

[7] A. Y. Javaid, W. Sun, V. K. Devabhaktuni and M. Alam, "Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System,", Proc. of the IEEE Conference on Technologies for Homeland Security (HST), pp. 585–590, 2012.

[8] A. J. Kornecki and Z. Janusz, "Threat Modeling for Aviation Computer Security," CrossTalk, vol. 21, 2015.

[9] A. Sanfeliu Cortés, "URUS: Ubiquitous Networking Robotics for Urban Settings," Cognitive Systems Industry Day (CSID), 2008.

[10] T. Jason, S. C. Chan, G. Ngai, J. C. Cheung and V. T. Ng, "Dynamic Collaborative Robotic Platform-A Brief Introduction," Proc. of the 13th International Conference on Computer Supported Cooperative Work in Design (CSCWD 2009), pp. 125–130, 2009.

[11] Y.-H. Wei, Q. Leng, S. Han, A. K. Mok, W. Zhang and M. Tomizuka, "RT-WiFi: Real-time High-speed Communication Protocol for Wireless Cyber-physical Control Applications," Proc. of the 34th IEEE on Real-Time Systems Symposium (RTSS), pp. 140–149, 2013.

[12] D. Quarta, M. Pogliani, M. Polino, F. Maggi, A. M. Zanchettin and S. Zanero, "An Experimental Security Analysis of an Industrial Robot Controller," IEEE Symposium on Security and Privacy (SP), pp. 268–286, 2017.

[13] "PeopleBot," [Online], Available: http://www.mobilerobots.com/ResearchRobots/PeopleBot.aspx.

[14] K. Ahmad Yousef, A. AlMajali, R. Hasan, W. Dweik and B. Mohd, "Security Risk Assessment of the PeopleBot Mobile Robot Research Platform," Proc. of the International Conference on Electrical and Computing Technologies and Applications (ICECTA), pp. 1–5, 2017.

[15] R. Blank and P. Gallagher, "NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments," National Institute of Standards and Technology, 2012.

[16] J. Holliman, M. Zhivich, R. Khazan, A. Swiston and B. Telfer, "Building Low-power Trustworthy Systems: Cyber-security Considerations for Real-time Physiological Status Monitoring," Proc. of the IEEE Military Communications Conference (MILCOM 2016), pp. 1083–1089, 2016.

[17] I. Kateeb and M. Almadallah, "Risk Management Framework in Cloud Computing Security in Business and Organizations," IAJC/ISAM Joint International Conference, 2014.

[18] E. Moradian and M. Kalinina, "Decision Support for Assessment of IT-Security Risks," Proceedings of the International Conference on Security and Management (SAM), p. 1, 2013.

[19] T. Bonaci, J. Herron, T. Yusuf, J. Yan, T. Kohno and H. J. Chizeck, "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots," arXiv preprint arXiv:1504.04339, 2015.

[20] G. Vasconcelos, G. Carrijo, R. Miani, J. Souza and V. Guizilini, "The Impact of DoS Attacks on the AR.Drone 2.0," 2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR), pp. 127–132, 2016.

[21] N. Bezzo, J. Weimer, M. Pajic, O. Sokolsky, G. J. Pappas and I. Lee, "Attack Resilient State Estimation for Autonomous Robotic Systems," Proc. of the IEEE/RSJ Inter. Conf. on Intelligent Robots and

Systems, pp. 3692–3698, 2014.

[22] L. T. Batson, D. R. Wimmer Jr et al., Unmanned Tactical Autonomous Control and Collaboration Threat and Vulnerability Assessment, PhD Thesis, Monterey, California: Naval Postgraduate School, 2015.

[23] A. Jones and J. Straub, "Using deep learning to detect network intrusions and malware in autonomous robots," SPIE Defense+ Security, pp. 1018505–1018505, 2017.

[24] F. Maggi, D. Quarta, M. Pogliani, M. Polino, A. M. Zanchettin and S. Zanero, "Rogue Robots: Testing the Limits of an Industrial Robot's Security," Technical Report, Trend Micro, Politecnico di Milano, 2017.

[25] F. J. R. Lera, C. F. Llamas, Á. M. Guerrero and V. M. Olivera, "Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety," Robotics-Legal, Ethical and Socioeconomic Impacts, InTech, 2017.

[26] T. Vuong et al., Cyber-physical Intrusion Detection for Robotic Vehicles, PhD Thesis, University of Greenwich, 2017.

[27] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon and D. Gan, "Cloud-based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning," IEEE Access, vol. 6, pp. 3491–3508, 2018.

[28] Q. Chen, R. K. Abercrombie and F. T. Sheldon, "Risk Assessment for Industrial Control Systems Quantifying Availability Using Mean Failure Cost (MFC)," Journal of Artificial Intelligence and Soft Computing Research, vol. 5, no. 3, pp. 205–220, 2015.

[29] D. Dominic, S. Chhawri, R. M. Eustice, D. Ma and A. Weimerskirch, "Risk Assessment for Cooperative Automated Driving," Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, pp. 47–58, 2016.

[30] K. M. Ahmad Yousef, A. AlMajali, S. A. Ghalyon, W. Dweik and B. J. Mohd, "Analyzing Cyber-Physical Threats on Robotic Platforms," Sensors, vol. 18, no. 5, p. 1643, 2018.

[31] H. Hüttenrauch, K. S. Eklundh, A. Green and E. A. Topp, "Investigating Spatial Relationships in Human-robot Interaction," Proc. of the IEEE/RSJ International Conference on Intelligent Robots and Systems, pp. 5052–5059, 2006.

[32] A. Chella et al., "A BCI Teleoperated Museum Robotic Guide," Proc. of the International Conference on Complex, Intelligent and Software Intensive Systems (CISIS'09), pp. 783–788, 2009.

[33] H. Kwon, K. M. A. Yousef and A. C. Kak, "Building 3D Visual Maps of Interior Space with a New Hierarchical Sensor Fusion Architecture," Robotics and Autonomous Systems, vol. 61, no. 8, pp. 749–767, 2013.

[34] K. M. Ahmad Yousef, J. Park and A. C. Kak, "Place Recognition and Self-localization in Interior Hallways by Indoor Mobile Robots: A Signature-based Cascaded Filtering Framework," Proc. of the IEEE/RSJ Inter. Conf. on Intelligent Robots and Systems (IROS 2014), pp. 4989–4996, 2014.

[35] I.-H. Kuo, E. Broadbent and B. MacDonald, "Designing a Robotic Assistant for Healthcare Applications," Proc. of the 7th Conference of Health Informatics, New Zealand, Rotorua, 2008.

[36] G. D. Morais, L. C. Neves, A. A. Masiero and M. C. F. de Castro, "Application of Myo Armband System to Control a Robot Interface, " Biosignals, pp. 227–231, 2016.

[37] K. M. Ahmad Yousef, B. J. Mohd, K. Al-Widyan and T. Hayajneh, "Extrinsic Calibration of Camera and 2D Laser Sensors without Overlap," Sensors, vol. 17, no. 10, p. 2346, 2017.

[38] "Deauthentication Attack," [Online], Available: https://www.aircrack-ng.org/doku.php?id= deauthentication.

[39] "Kali Linux," [Online], Available: https://www.kali.org/.

[40] M. J. Handley and E. Rescorla, "Internet Denial-of-service Considerations," 2006.

[41] V. Dey, V. Pudi, A. Chattopadhyay and Y. Elovici, "Security Vulnerabilities of Unmanned Aerial

Vehicles and Countermeasures: An Experimental Study," Proc. of the 17th Inter. Conf. on Embedded Systems (VLSID) and the 31st Inter. Conf. on VLSI Design, pp. 398–403, 2018.

[42] A. G. Ozkil, Z. Fan, S. Dawids, H. Aanes, J. K. Kristensen and K. H. Christensen, "Service Robots for Hospitals: A Case Study of Transportation Tasks in a Hospital," Proc. of the IEEE International Conference on Automation and Logistics (ICAL'09), pp. 289–294, 2009.

"Semi-quantitative Security Risk Assessment of Robotic Systems", A. AlMajali, K. M. A. Yousef, B. J. Mohd, W. Dweik, S. Abu Ghalyon and R. Hasan.

[43] "Creating A Laser Map for ARNL," [Online], Available: http://robots.mobilerobots.com/wiki/Creating _A_Laser_Map_for_ARNL.

[44] "This is Real Life: Robotics Company Cyberdyne Introducing 'Service' Robots with Artificial Intelligence," [Online], Available: http://nationalpost.com/news/world/this-is-real-life-robotics-company-cyberdyne-introducing-service-robots-with-artificial-intelligence.

[45] "Rise of the Airport Robots," [Online], Available: https://www.aerosociety.com/news/rise-of-the-airport-robots/.

[46] D. J. Bernstein, "SYN cookies," [Online], Available: http://cr.yp.to/syncookies.html.

ملخص البحث:

أصبحت الروبوتات تتكامل بشكل متزايد في حياتنا اليومية، حيث تقدم الخدمات في التطبيقات المدنية والصناعية والعسكرية. العديد من هذه التطبيقات تتطلب أن يتم تشغيل الروبوتات والتحكم فيها عن بعد من خلال قنوات الاتصال. وهذا يجعل نظام الروبوت عرضة لطبقة من الهجمات التي تستهدف الاتصال بين العميل المسيطر والروبوت، مما يجعل الروبوت غير متوفر. الهدف من هذه الدراسة هو تحديد وتقييم المخاطر المرتبطة بالهجمات التي تستهدف توفر الروبوت. من أجل تحقيق هدفنا، قمنا بإجراء تقييم مخاطر شبه كمي موجه نحو تأثير فقدان توفر الروبوت (PeopleBot™). قمنا بإجراء مجموعة من التجارب التي استخدمنا فيها العديد من الهجمات المعروفة التي يمكن أن تستهدف وتؤثر على توافر الروبوت. وقد أثبتت النتائج أن الهجمات يمكن أن تؤدي إلى فقدان توفر الروبوت، الأمر الذي يؤدي بدوره إلى عواقب خطيرة.