Quantitative impact analysis of application-level attacks on a robotic platform

Khalil M. Ahmad Yousef*, Anas AlMajali, Bassam J. Mohd and Salah Abu Ghalyon

Department of Computer Engineering,
Faculty of Engineering,
The Hashemite University,
P.O. Box 330127, Zarqa 13133, Jordan
Email: khalil@hu.edu.jo
Email: almajali@hu.edu.jo
Email: bassam@hu.edu.jo
Email: salah.g.ghalyon@hu.edu.jo
*Corresponding author

Abstract: Robots are important examples of cyberphysical systems. Typically, robots are battery powered, which are a potential target for cyber-physical attacks to drain batteries and reduce their lifespan. When the battery is drained, the robot is not available and results in denial-of-service. Hence, robotic security and operation duration are fundamental requirements. The main objective of this paper is to provide an impact-based quantitative security risk assessment of three application level attacks targeting a well-known mobile robot platform that is called the PeopleBot^{TM}. The novelty of our work is that we successfully drained a fully-charged robot battery using application level attacks that include exhausting the computing resources of the robot. The attacks cause a reduction in the robot availability time. The average availability time from the performed attacks was reduced by 11.78%. We followed the adversarial risk assessment template provided in NIST. Finally, some mitigation strategies for the performed attacks were suggested.

Keywords: cyber-physical security; robot availability; attacks; vulnerability; risk assessment; PeopleBot.

Reference to this paper should be made as follows: Ahmad Yousef, K.M., AlMajali, A., Mohd, B.J. and Abu Ghalyon, S. (2022) 'Quantitative impact analysis of application-level attacks on a robotic platform', *Int. J. Electronic Security and Digital Forensics*, Vol. 14, No. 4, pp.388–412.

Biographical notes: Khalil M. Ahmad Yousef is an Associate Professor of the Department of Computer Engineering at the Hashemite University, Jordan. He is currently the Faculty of Engineering Dean Assistant for Industrial Affairs and Training for the academic year 2020/2021. He is an IEEE senior member. He is a certified professional engineer from the Jordanian Engineering Association (JEA). He received his PhD in Electrical and Computer Engineering from the Purdue University, West Lafayette, USA, in 2013, his MS in Computer Engineering from the Jordan University of Science and Technology, Jordan, in 2008, and his BS in Electrical

and Computer Engineering from the Hashemite University, in 2005. His research interests include computer vision, sensor fusion, image processing, optimisation, algorithms, cyber-security and robotics.

Anas AlMajali is an Associate Professor at the Department of Computer Engineering at the Hashemite University, Jordan. He is currently the Chair of the Department of Computer Engineering. He received his PhD and MS in Computer Engineering from the University of Southern California in Fall 2014 and Fall 2008 respectively. He also received his BSc in Computer Engineering from the University of Jordan in 2005. His research interests include computer and network security, smart grid security and cyber-physical systems.

Bassam J. Mohd is a Full Professor at the Department of Computer Engineering at the Hashemite University, Jordan. He is currently the Vice Dean of Scientific Research at the Hashemite University. He received his BS in Computer Engineering from the KFUPM of Dhahran-KSA, his MS in Computer Engineering from the University of Louisiana at Lafayette and his PhD from the University of Texas- Austin, in 2008. He has worked for several semiconductor companies including Intel, SUN, Synopsys and Qualcomm. His research interests include hardware security, encryption processors, DSP designs, steganographic processors, image processing, speech recognition and power/energy optimisation.

Salah Abu Ghalyon is currently a lab instructor in the Computer Engineering Department at the Hashemite University, Jordan. He is a certified professional engineer from the Jordanian Engineering Association (JEA). He received his MS in Embedded Systems Engineering/Computer Engineering from the Yarmouk University, Jordan, in 2016, and his BS in Computer Engineering from the Hashemite University, in 2013. His research interests include computer vision, image processing, machine learning, artificial intelligence, cyber-security and robotics.

1 Introduction

Currently, there is a huge work related to protecting embedded systems and cyber-physical systems (CPSs) [e.g., robots, internet of things (IoT) devices, and the industrial internet of things (IIoT) (Al-Sibai et al., 2021)] from cyber-security attacks Bonaci et al. (2015), Bezemskij et al. (2016), Ahmad Yousef et al. (2017), AlMajali et al. (2018), Ahmad Yousef et al. (2018), Mohd et al. (2019), Matellán et al. (2017), Mukhandi et al. (2019), Vilches et al. (2018) and Wang et al. (2021). Such attacks usually target one or more of the following well-known security requirements; the confidentiality, integrity and availability (CIA) triad and possibly others (e.g., authentication, authorisation, accountability, etc.). However, from an industrial perspective where robots are classified or categorised to be called operational technology (OT) systems as opposed to traditional information technology (IT) systems, the availability security requirement is what is being highly emphasised to be the most critical factor, and thus what is being mostly targeted (Srinivas, 2014; Aijaz et al., 2015). This is explained by the fact that OT systems mandate real-time production networks

(e.g., robot used to assemble parts on a production line in a manufacturing company or warehouse) where the acceptable downtime is usually less than 300 ms, whereas for the case of IT systems minutes range might be acceptable (Hingley, 2018).

This imposes several requirements to insure that the robots must be protected against the attacks or threats that are highly to impact their availability. The most dangerous attacks that can impact the availability of the robots are the denial-of-service (DoS) attacks that are specially customised to affect the power system of the robot (Bonaci et al., 2015; Wang et al., 2021). According to the 2020 ENISA threat landscape report (T.E.U.A. for Cybersecurity ENISA, 2020) and the 2019 Verizon Data Breach Investigations Report (2019), DoS is ranked one of the top trending cyber attacks. This includes those attacks that can quickly drain the batteries or the limited power resources of the robot. The most important factor that is being targeted in such attacks is the communication link or the sensing domain between the robot and the user or the operator. The former (i.e., the robot) and the latter (i.e., operator) are usually to be called the server and client respectively, in the robotic network paradigm.

Some important types of the attacks that can impact the availability of the robots are listed below, and tabularly presented in Table 1.

- Vampire attacks, where the attacker utilises different ways (e.g., sending vampire packets in the network) to make the limited battery lifetime devices consume more energy as quickly as possible causing service disruption.
- Denial of sleep attacks, where the attacker tries to prevent devices from switching to sleep mode by possibly sending control signals that affect their duty-cycles. This way the devices will be active for longer durations leading to their slow depletion of their battery life.
- Flooding attacks, where the attacker floods network with dummy packets from several clients and request them to deliver these packets to the server (e.g., robot), where the server wastes energy while receiving and responding to those packets.
- Replay attacks (also known as playback attacks), where the attacker fraudulently repeats valid data transmission through the network consuming more energy.

Table 1 Summary of some important security attacks targeting the sensing domain

Attack type	*Target OSI layer*	*Vulnerability reason*	*Security violation*
Vampire attacks	Data link, and network	Limited battery lifetime	Availability and freshness
Denial of sleep attacks	Physical and network	Limited battery lifetime	Availability
Flooding attacks	Network	Limited transmission capability	Availability
Replay attacks	Network and application	Limited transmission capability	Availability

In this paper, we consider one or more of the attacks listed above to impact the availability security requirement of the PeopleBot^{TM} research mobile robot platform (PeopleBot, https://telepresencerobots.com/robots/adept-mobilerobots-peoplebot). Importantly, in one of the attack types (replay attacks), we utilised certain vulnerability in the PeopleBot's libraries (ARNL and ARIA) and

software (e.g., MobileEyes and arnlServer) (Adept MobileRobots Software, http://www.mobilerobots.com/Software.aspx) as shall be seen later in the paper. It should be mentioned that the vendor of the PeopleBot robot, which is also the vendor for many other similar robotic research platforms (e.g., PowerBot, AmigoBot, etc.) – Omron Adept MobileRobots LLC, the Research and Academic Robotics division of Omron Adept Technologies – was permanently closed effective 31 January 2018, and thus discontinued the support for all of its research robot platform to only focus on their industrial mobile robots. However, fortunately, such robotic platforms are now being supported through robot operating system (ROS), which is considered as a de-facto framework for developing robotic solutions (Mukhandi et al., 2019).

The main contributions of this work are as follows:

- Studied the power/energy consumption profile of the PeopleBot robot that is equipped with several sensors or accessories.
- Examined three different security threats on the power system of the PeopleBot robot.
- Designed a specific application-level attack utilising discovered robot's server-client software vulnerability.
- Performed quantitative security risk assessment using the adversarial risk assessment template provided in NIST (Guide for Conducting Risk Assessments, https://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf) extending our previous work, where qualitative risk assessment (Ahmad Yousef et al., 2018, 2017) and semi-quantitative risk assessment (AlMajali et al., 2018) of the PeopleBot robot were presented.
- Conducted numerous experiments and practically demonstrated that it is fairly easy to cause loss of availability to the PeopleBot robot after some period of time from initiating the designed attacks. The average availability time from the performed attacks was reduced by 11.78%.
- Proposed a possible detection system that was inspired by detecting any slope deviation compared to the baseline performance while analysing the consumed power during the operation time of the robot.
- Discussed the possible physical consequences if the PeopleBot becomes unavailable and presented recommendations to mitigate loss of availability and other expected risks.

It is noteworthy to mention that the main focus of this work is on providing a quantitative security risk assessment. Thus, the proposed detection system is an example of a possible detection technique, while other techniques could be designed, implemented, and integrated in this work.

The rest of the paper is organised as follows. In Section 2, related work is discussed. In Section 3, we discuss the power profile of the PeopleBot mobile robot platform. In Section 4, we describe the planned availability-targeted attacks. In Section 5, we present the quantitative risk assessment approach used in this paper. Section 6 presents our discussion on the performed security attacks. Finally, we conclude the paper and provide our future directions in Section 7.

2 Related work

According to many very recent studies including Dudek and Szynkiewicz (2019), Shah (2019), Mukhandi et al. (2019), Wardega et al. (2019), Vilches et al. (2018), Ahmad Yousef et al. (2018) and AlMajali et al. (2018), it is clear that robot security is an emerging challenge that needs to be addressed immediately. Additionally, there are currently few formal documentation, guidelines, standards, and tools to assess robot security. Therefore, robot security is now a major issue and concern in the robotic field that is being studied and discussed extensively. In this section, we present a brief summary about the literature concerning studying the power profile of mobile robots, and that concerning recent robotic or CPSs power attacks and their associated quantitative security risk assessment whenever possible.

Mei et al. (2005) studied the power consumption profile of the well-known mobile robot that is called Pioneer 3DX. The authors analysed the energy consumers of such robot and built experimental-based power models for motion, sonar sensing and control. They introduced two energy-conservation techniques: real-time scheduling (RTS) and dynamic power management (DPM) for energy-efficient designs of mobile robots. The authors showed how motion planning together with the introduced techniques provide greater opportunities to reduce the power consumption and achieve better energy efficiency for mobile robots.

Krishnaswami (2004) investigated sleep deprivation attacks, which are DoS type of attacks that rapidly drain the battery of mobile devices such as laptops. The author implemented and presented three different methods for such attacks: network service request attacks, benign attacks, and malignant attacks. Such methods were then used to derive a battery usage mathematical model to predict the impact of sleep deprivation attacks on the battery life of the device under attack, and thus giving an estimate of its battery lifetime considering its power consumption usage and status. A similar work was described by Martin et al. (2004).

Kundu et al. (2017) quantitatively analysed and studied energy attacks on mobile devices such as smart-phones. Such attacks were used to exploit the hardware, software or communication components of the device in order to drain its battery. As such, the authors designed and implemented several malicious applications and malicious web pages to explore the energy attacks from different aspects: software resources, network communications, and hardware components. The main metric that was used is the energy drain of the battery (percentage) per time.

Vilches et al. (2018) presented the robot security framework (RSF) to be a standardised methodology to perform systematic security assessments in robots. The RSF consisted of four main layers (physical, network, firmware and application). As reported by the authors, RSF is proposed to be used "to identify, classify and report vulnerabilities for robots within a formal operational protocol."

Grooby et al. (2019) provided a quantitative analysis of the academic literature, named as bibliometric analysis, of available academic research articles from 2008 to 2017 in the area of security and access control of the IoT devices. They proposed a classification of research themes in terms of countries, journals, authors, research institutions, most common research areas, most common research keywords, and the most highly cited articles. Based on such analysis, the authors attempt to answer several research questions related to finding the trends in IoT access control research over the last 10 years and extrapolate upon them to predict the possible future trends.

Mohd et al. (2019) presented a scheme to adjust energy consumption of data encryption cipher based on predefined power levels. The scheme adjusts encryption energy by varying design options and operation complexity of the cipher. Implementation results show an energy savings of 35%-39%, as well as facilitating limited-scale encryption at low power levels.

Very recently, AlMajali et al. (2020) performed security risk assessment following the NIST standards and using Bayesian networks targeting one of the CPSs; the smart grids and specifically the circuit breakers within the smart grid environment. Several vulnerabilities in the girds' cyber and physical domains were analysed by the authors manipulating the circuit breakers and thus the power supply of the grid, which successfully resulted in destabilising the power grid. Also, the authors analysed the effect of integrating photovoltaic (PV) systems on the stability of the grid and showed that integrating smart grids with PV systems improved the resilience even if a cyber-attack succeeds.

3 Power profile of the PeopleBot Mobile Robot Platform

To study the power profile of the PeopleBot robot, first it was important to identify all the sensors the robotic platform has, and the power capability of the PeopleBot in terms of the number of batteries it is equipped with and their total charges. To this end, following we list the robot sensors, and batteries/power specifications of the PeopleBot.

The PeopleBot robot platform that we deal with has been customised to have the following sensors (accessories) installed on-board as shown in Figure 1.

- MobileRanger FPGA-accelerated C3D stereo camera
- SICK LMS500 range finder sensor (lidar)
- AXIS PTZ camera
- IR sensors
- lower and upper sonar arrays
- ten bumper elements
- speakers
- buzzers
- touchscreen interface
- gyroscopic sensor.

The PeopleBot robot, which is shown in Figure 1, has three batteries as shown in Figure 2 that are working at one time with the following specifications (PeopleBot, https://telepresencerobots.com/robots/adept-mobilerobots-peoplebot):

- battery nominal voltage: 12 V
- battery nominal capacity: 9 Ah
- chemistry: lead acid

- hot-swappable batteries.

Figure 1 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. (see online version for colours)

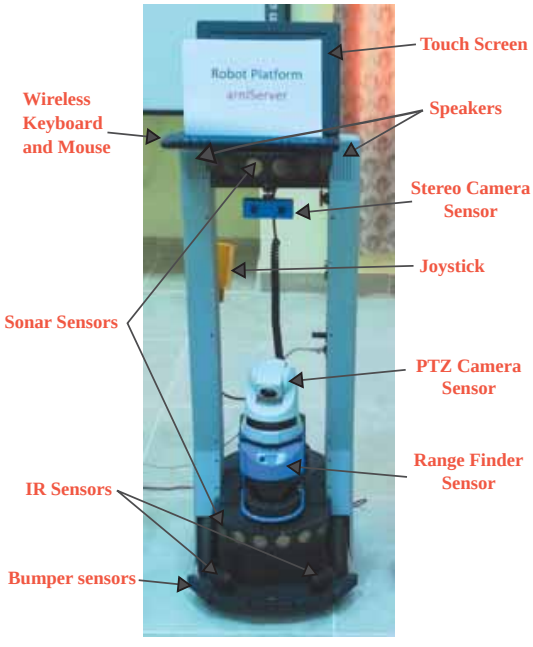
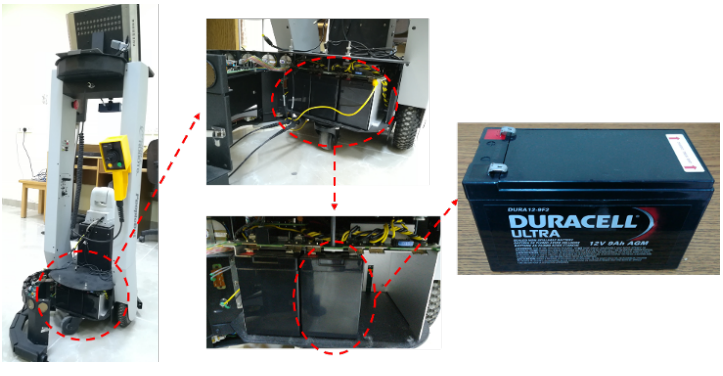


Figure 2 PeoplebBot batteries (see online version for colours)



The power specifications of the PeopleBot (https://telepresencerobots.com/robots/adept-mobilerobots-peoplebot) are as follows:

- run time: 8 hours with three batteries (with no accessories)
- charge time: 2.4 hours
- available power supplies:

a 5 V @ 1.5 A switched

b 12 V @ 2.5 A switched.

The robot on-board computer specifications are as follows, which were obtained using the 'phoronix-test-suite' software utility with the option 'system-info' (Larabel and Tippett, 2011):

- Processor: Intel Core 2 Duo P8400 @ 2.34 GHz (2 Cores).
- Motherboard: Intel Montevina Development Board.
- Chipset: Intel Mobile 4 MCH + ICH9M.
- Memory: 8,192 MB.
- Disk: 480 GB INTEL SSDSC2BW48 + 160 GB INTEL SSDSC2BB16.
- Graphics: Intel Mobile 4 IGP.
- Audio: IDT 92HD87B1/3.
- Network: Intel 82574L Gigabit Connection + Qualcomm Atheros AR928X Wireless.
- Software: OS: Ubuntu 12.04, Kernel: 3.13.0-107-generic (i686), desktop: GNOME 3.2.1, display server: X Server 1.13.0, display driver: Intel 2.20.9, compiler: GCC 4.6, file-system: ext4 and screen resolution: 1,024 × 768.

Each sensor on the robot is being used by the different applications or software running on the robot to add certain context by which the robot can better understand its environment and thus effectively performs its assigned job(s). As such, depending upon the application or software that is being run on the robot, different number of sensors might be turned-on or active and others might be turned-off or inactive.

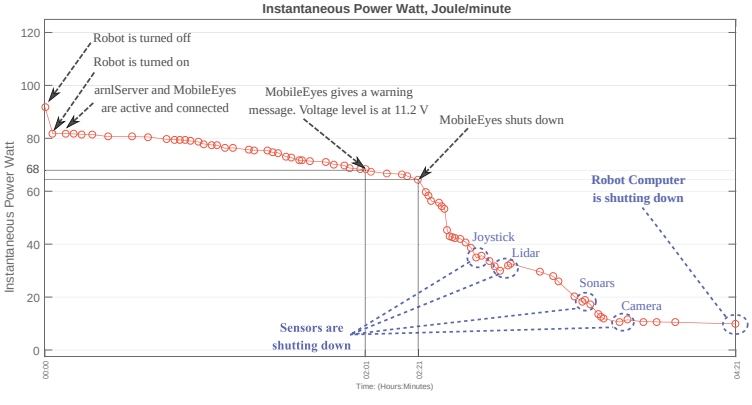
One of the most important PeopleBot robot software that can control, set and enable the use of the robot sensors is called 'arnlServer'. 'arnlServer' is a program from the 'ARIA' and 'ARNL' middleware libraries that comes installed with the robot [currently available through ROS: 'ROSARIA' and 'ROS-ARNL' (ROS Adept MobileRobots Pioneer and Pioneer-Compatible Platforms, http://wiki.ros.org/Robots/AMR_Pioneer_Compatible)]. According to the PeobleBot (https://www.generationrobots.com/media/PeopleBot-PPLB-RevA.pdf) manual and ROS Adept MobileRobots Pioneer and Pioneer-Compatible Platforms (http://wiki.ros.org/Robots/AMR_Pioneer_Compatible), "ARIA provides a framework for controlling and receiving data from all MobileRobots platforms, as well as most accessories, includes open source infrastructures and utilities useful for writing robot control software, provides support for network sockets, and finally provides support for an extensible framework for client-server network programming." On the other hand, ARNL enables the robot to "perform robust, laser-based autonomous localisation and navigation" (PeopleBot, https://www.generationrobots.com/media/PeopleBot-PPLB-RevA.pdf).

To perform our PeopleBot power profile analysis, we have modified the 'arnlServer' software so that all of the sensors/accessories that we previously mentioned (except for the stereo camera) were turned on and in active use. There is another software that we

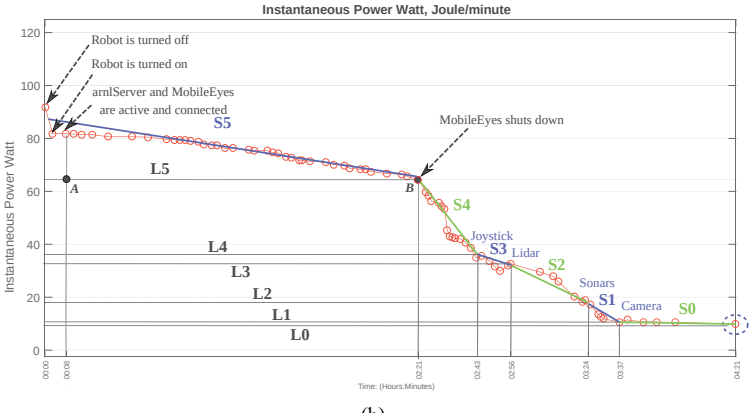
used to connect to the robot server, which is called 'MobileEyes' (or 'rqt' as known in ROS). MobileEyes is a graphical user interface (GUI) client for remote operation and monitoring of the robot.

Figure 3 Connected oscilloscope probes (two channels) on the positive/negative terminals of the batteries of the PeopleBot robot (see online version for colours)

Figure 4 Power profile of the PeopleBot robot; the time axis is formatted as HOURS:MINUTES, (a) power profile plot (b) power profile with levels (see online version for colours)



(a)



(b)

Therefore, when the robot is initially turned-on and started to be monitored for its power consumption to analyse its power/energy profile, we first connected oscilloscope probes (two channels) on the positive/negative terminals of the batteries (the power supply unit) as shown in Figure 3 to record the electrical voltage and current changes/variations of the robot and thus its power level variations. Additionally, we run arnlServer on the robot and MobileEyes on a client computer (laptop). When the robot is turned-on, its batteries were fully charged. We analysed the power/energy profile of the PeopleBot robot for about 4 hours and 21 minutes till the robot completely stopped with an average sampling period of one minute. The resulted analysis is shown in Figure 4(a). The zero time 00:00 (hours:minutes) represents the starting time of the analysis.

Figure 4(a) shows the PeopleBot power profile, which provides the power level of the batteries for the robot and its operated sensors. This is an indication of the stored energy at which robot and its sensors can operate. It is noteworthy to mention that, first, there are some sources of errors in the measurements that may be due to one or more of the following, however, we believe the measurements are still representative.

- Human errors while performing the manual steps in recording the data entries (current and voltages from the oscilloscope machine).
- Aging problem of the batteries and sensors that may affect their reading accuracies.
- The oscilloscope machine measurement resolution.

And, second, certain sensors cannot operate below a particular power level.

Examining the power profile in Figure 4(a), we can notice and observe the following:

- Initially the power level is at about 81.79 watt.
- The entire robot system shuts down when the power level reaches 9.86 watt.
- The supplied power initially declines slowly, then decline accelerates after 68.2 watt. At this power level, the voltage of the robot system is at 11.2 volts, and MobileEyes gives a warning message (text and a high buzzer sound) that it will shutdown when the voltage level becomes 10.8 volts.
- As the power declines, when the power level is at 64.41 watt (the voltage level is at 10.8 volts), MobileEyes client and arnlServer are completely disconnected from each other, but the robot sensors are all still on. The time it took MobileEyes to shutdown after triggering the buzzer sound at 11.2 Volts was observed to be 53 minutes.
- As the power continues to decline, certain sensors/components start to shut down. In Figure 4(a), shutting down event of a component/sensor is indicated by a slight increase in the supplied power. For example, this is highlighted in blue dashed circles for the joystick, lidar, sonars, and camera, respectively.

The power profile curve in Figure 4(b) demonstrates different regions, where each region has a distinct slope. In Figure 4(b), we roughly identified regions with different slopes S5-S0. We mapped such regions to the power axis (Y-axis), and designated several power levels L5-L0, as described below:

- L5 is the level, where the power ends to decline slightly from the state when the battery is initially charged to (almost) maximum. In this region, the robot and its components/sensors operate with no issues. The average duration for this region is about 133 minutes [time difference between point A and B in Figure 4(b)].
- L0 is the level where the robot completely shuts down. The average time to reach this level is about 260 minutes.
- L1-L4: these are intermediate power levels, where the power curve declines faster and various components/sensors in the robot system start to shut down because supplied power is not sufficient to operate stopped components/sensors.

4 Planned attacks

In this section, we describe the planned availability attacks. By looking at Figure 4(b), we can observe that L5 is the most critical power level that affects the software operation and availability of the robot. For example, at level L5, MobileEyes client software shuts down and is completely disconnected from the robot (i.e., arnlServer). In this case, the robot becomes unavailable (i.e., software (client and server applications) is no longer running to control and monitor the robot). Subsequently, this can be considered as a possible vulnerability that can be utilised by an attacker, who will try to look for different ways to force the robot system to reach L5 power level as soon possible to shorten the availability and thus productivity time of the robot. Toward achieving this goal, we planned and plotted three different attacks to exhaust the computing resources of the robot (CPU, network bandwidth, sensors, and storage) as follows:

1 Running and connecting multiple clients (MobileEyes) to the robot server (arnlServer) exhausting the computing resources of the robot: network bandwidth and CPU. This attack was plotted after we carefully studied and analysed the robot software (specifically MobileEyes and arnlServer). Our analysis showed that arnlServer allows for several client connections at the same time, which represents a serious and sever vulnerability in the robot system. Subsequently, we tried to utilise this vulnerability by running several instances of the MobileEyes client software at the same time both on the same client machine and also on different client machines.

2 Running a malware to exhaust and fully utilise the two cores of the robot processor. We used and run two threads, where each thread contains the following piece of code:

```
int *p;
while (p == p){
(*p++)+1;
}
```

The above piece of code contains one declared pointer variable p that simply causes the two cores of the robot processor to enter an infinite loop while

performing simple arithmetic pointer operations (post-increment and an increment operations simultaneously).

Figure 5 Robot power profile based on running the first attack; simultaneously connecting multiple clients to the robot (server) (see online version for colours)

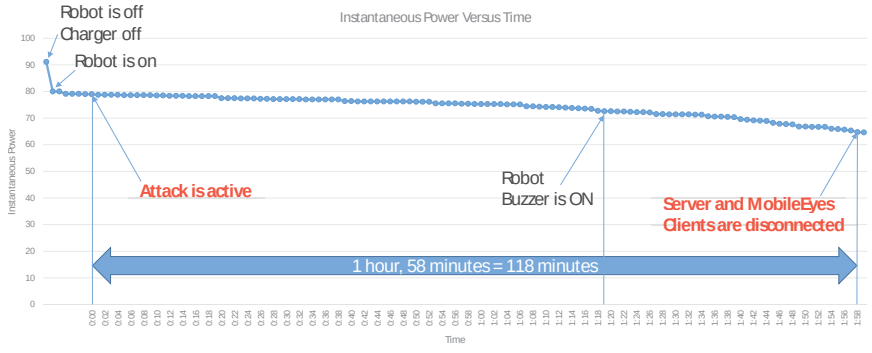


Figure 6 Robot power profile based on running the second attack; exhausting the processing power of the robot (see online version for colours)

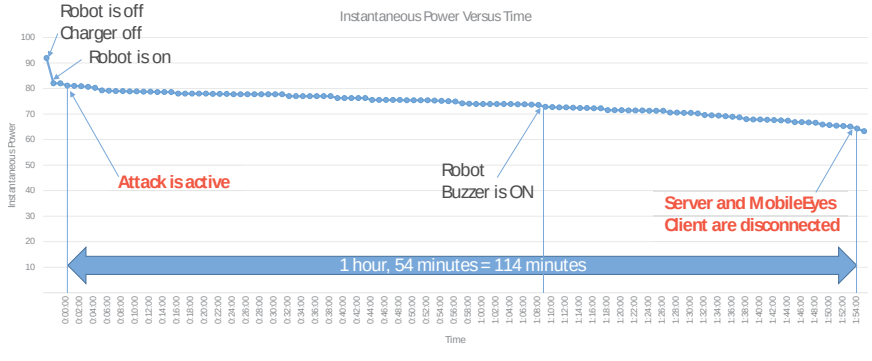
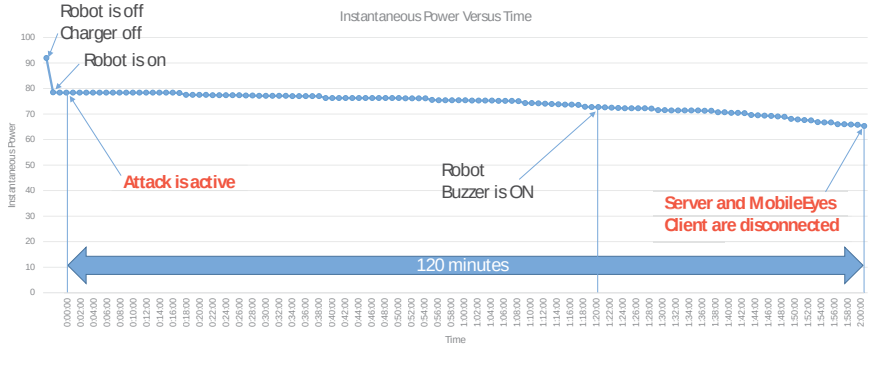


Figure 7 Robot power profile based on running the third attack; exhausting the processing power of the robot (see online version for colours)



3 Activating and running additional sensor on the robot that was not considered in the conducted base-line power profile analysis of the robot. This attack tries to exhaust the computing resources of the robot (CPU, sensors, and storage). In our

case, we utilised the MobileRanger FPGA-accelerated C3D stereo camera, and continuously logged stereo images (two black and white images with a resolution of 752 × 480 pixels stored in '.JPG' format) to the robot hard-drive until the server and MobileEyes client were disconnected. It is noteworthy to mention that the MobileRanger stereo vision sensory system provides depth range sensing, with no or very minimal software processing required. The system performs initial depth calculations on the FPGA card (PC104+), reserving the robot's computing resources for other tasks.

Table 2 Performance evaluation metrics and results

Availability time evaluation metrics (in minutes)	*Without any attack*	Attack 1		*Attack 2*		*Attack 3*	
		Time	*%*	*Time*	*%*	*Time*	*%*
Metric (1): 'robot ON' or 'attack activated' to 'software disconnected'	133	118	*11.28%*	114	*14.29%*	120	*9.77%*
Metric (2): 'robot ON' or 'attack activated' to 'robot warning buzzer beeps'	80	79	1.25%	69	13.75%	80	0%
Metric (3): 'robot warning buzzer beeps' to 'software disconnected'	53	39	26.42%	45	15.09%	40	24.53%

For the first attack, the obtained analysis results were as shown in Figure 5. Subsequently, we have the following facts and observations:

- This sort of an attack can be considered as legitimate or benign. We performed a benign attack, where the robot is made to execute a valid but energy-hungry application (MobileEyes and arnlServer) without modifying the application.
- We used 20 personal computers (PCs), where each PC runs 100 MobileEyes clients. The total number of clients tried to connect to the server was 2,000 in total. It is noteworthy to mention that it was found that the maximum number of simultaneous clients that the server could handle was 1,077. After reaching this limit, the server started to stop or drop a few old or early established client connections before allowing to accept new client requests. However, this pattern did not stay for long, where the server then will be overwhelmed and no more connections will be accepted at all unless one of the clients was explicitly closed from its initiating machine.
- Based on the experimental results from this attack as shown in Figure 5, it was observed that the availability time of the robot (since the attack started or the first MobileEyes client successfully connected to the server) was reduced to 118 minutes, with 11.28% drop in power compared to the baseline performance shown in Figure 4(b).
- The availability time of the robot since the robot buzzer started to beep was observed to be 39 minutes.
- It does not matter (i.e., there is no observable change in the results in the devised conclusions above) whether the MobileEyes instances run on the same client machine or on different client machines.

For the second attack, the obtained analysis results were as shown in Figure 6 with the following facts and observations:

- This sort of an attack is considered malignant. We assume that an attacker (insider or outsider) is somehow able to force a connected client to the robot to somehow execute a malware such as the simple code described above or a very similar script (e.g., through social engineering, trojan, virus, etc.). For example, the malware, which caused the Ukraine power outage in 2015 was delivered through spear phishing emails with malicious Microsoft Office attachments (CISA, 2016).
- Based on the experimental results from this attack as shown in Figure 6, it was observed that the availability time of the robot was reduced to 114 minutes, with 14.29% drop in power compared to the baseline performance shown in Figure 4(b) (i.e., 133 minutes).
- The availability time of the robot since the robot buzzer started to beep was observed to be 45 minutes.

For the third attack, the obtained analysis results were as shown in Figure 7. Subsequently, we have the following facts and observations:

- This sort of an attack is considered benign. We assume that an attacker (insider or outsider) is somehow able to activate an additional sensor to run on the robot (a stereo camera in our attack) from a client machine.
- Based on the experimental results from this attack as shown in Figure 7, it was observed that the availability time of the robot was reduced to 120 minutes, with 9.77% drop in power compared to the 133 minutes baseline performance shown in Figure 4(b).
- The availability time of the robot since the robot buzzer started to beep was observed to be 40 minutes.

Table 2 summarises the results stated above. The rows of Table 2 represent three performance evaluation metrics computed in terms of the robot availability time as a function of three unique states. These states are identified during the analysis of the attacks: attack is started and active, robot buzzer sound for the low battery state is triggered ON or started to beep, and lastly the robot software is disconnected. These metrics were found to be useful to compute the impact of the attacks and thus their associated risks as shall be discussed and seen in Section 6. The percentage numbers in the table represents the availability time reduction percentages R as compared to the base performance without attacks, which are computed using the following equation:

$$R = \frac{\text{Availability time}_{\text{no attack}} - \text{Availability time}_{\text{with attack}}}{\text{Availability time}_{\text{no attack}}} \times 100\% \quad (1)$$

In the next section, we present our impact-based quantitative risk assessment of the PeopleBot based on the three attacks described and discussed above.

5 Quantitative impact risk assessment of the PeopleBot robot

Risk assessment is one of the main components in the risk management process. Usually, risk management starts by assessing risk. However, risk assessment is a continuous process that should be maintained during system development. Risk itself is function of vulnerability, threat and impact (harm) of an adverse event (a successful cyber-attack in this case). Vulnerabilities and threats indicate the likelihood of the adverse event (Blank and Gallagher, 2012). To estimate the impact of an attack, we use the quantitative analysis discussed in Section 4 and shown in Table 2. However, to estimate the likelihood of an attack, we follow a semi-quantitative approach similar to the analysis done in AlMajali et al. (2018). In AlMajali et al. (2018) and as shown in Table 3, the qualitative levels (very high, high, moderate, low and very low) are mapped to the semi-quantitative levels (10, 8, 5, 2, and 0), respectively. Then, the overall likelihood of an attack is assigned a value between 0 and 1 based on the average of both the likelihood of attack initiation and the likelihood of success of the initiated attack. The likelihood of attack initiation depends on adversary intent, capability and targeting (Guide for Conducting Risk Assessments, https://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf). Where each of these three factors is assigned a semi-quantitative value (10, 8, 5, 2, and 0) based on experts' opinion. Hence the likelihood of attack initiation was computed as normalised average of these three values, where the normalised factor is 10 (i.e., the semi-quantitative level that is associated with the qualitative level 'very high'). Whereas, the likelihood of success of the initiated attack depends on the threat source capability, severity of the vulnerability, and predisposing conditions. Therefore, it was computed as normalised average of such three factors.

In this work, we are interested in the impacts of cyber-attacks on the availability of the PeopleBot robot. More precisely, we are interested in attacks that drain the power of the robot and consequently make it unavailable. Hence, an impact-oriented analysis is adopted and only vulnerabilities that drain the power of the robot were investigated as discussed in the previous section.

Table 3 Mapping of qualitative levels to semi-qualitative levels

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

5.1 Quantitative risk assessment determination

In this subsection, we discuss how to generate the risk table, which summarises the assessment process. We used the adversarial risk assessment template proposed in Blank and Gallagher (2012). First, Table 3 demonstrates the mapping of the qualitative severity level to its corresponding semi-quantitative level. Table 4 presents the end result of the risk assessment process for the three threats under study. Following, each item in Table 4 is discussed [for more details about those items, the reader is advised to refer to Blank and Gallagher (2012)]:

1 *Threat event:* Refers to the threat that is currently being analysed. In this work, there are three attacks which were discussed in Section 4.

2 *Threat sources:* Refer to the threat source, which can be an insider, outsider, trusted insider, or privileged insider (Blank and Gallagher, 2012). The first attack requires that the attacker establishes multiple client-server connections with the robot. This means that the attacker should be an insider within the local network of the robot (unless the robot can be accessed publicly which is highly unlikely). For the second and third attacks, a malware is injected in the robot by one of the famous means like trojan horses, worms and social engineering. This means that the attacker may be of any type.

3 *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 first attack requires high level of expertise and what makes it easier is that there is a vulnerability in the server side that allows establishing a connection with the robot without authentication. The second and third attack require very high level of expertise as the binaries to execute the code have to be injected first in the robot then executed.

4 *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.

5 *Targeting:* This is one of the characteristics of the threat source. The adversary targets a specific mission or function within an organisation (i.e., the target of the attack is not random).

6 *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 on a PeopleBot robot, we rank them as possible.

7 *Likelihood of attack initiation:* Refers to the likelihood that the adversary will initiate the attack. This value is computed using the normalised average of capability, intent and targeting.

8 *Severity of the vulnerabilities:* The first attack is exposed and exploitable, so its severity level is very high. However, the second and third attacks require an infection mechanism so their exploitability is not high. So, they are ranked as moderate.

9 *Pervasiveness of predisposing conditions:* Vulnerabilities that apply to all robots running the same setup are ranked high.

10 *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 normalise them.

Table 4 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 the vulnerabilities*	*Pervasiveness of predisposing conditions*	*Likelihood initiated attack succeeds*	*Overall likelihood*	*Level of impact*	*Risk*
		Capability	*Intent*	*Targeting*								
Attack 1: running and connecting multiple clients	Insider	8	8	8	Possible	0.80	10	8	0.87	0.84	11.28%	*9.48*
Attack 2: running processor intensive malware	Any type	10	8	8	Possible	0.87	5	8	0.77	0.82	14.29%	*11.72*
Attack 3: running sensor intensive malware	Any type	10	8	8	Possible	0.87	5	8	0.77	0.82	9.77%	*8.01*

11 *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.

12 *Level of impact:* The impact of the attack is quantified based on the power drained by the attack. Table 2 demonstrates the impact of the three attack scenarios on the robot.

13 *Risk:* This is the final risk assessment measure, which is the product of the overall likelihood and the level of impact as shown in equation (2). The risk value represents an estimation of the risk of each threat and can be used to prioritise risk handling (Blank and Gallagher, 2012).

$$Risk = Overall\ likelihood \times Impact \tag{2}$$

Table 5 Risk values for the three attacks based on the possible evaluation metrics as stated in Table 2

Availability time evaluation metrics	*Risk of attack 1*			*Risk of attack 2*			*Risk of attack 3*		
	Overall likelihood	*Impact*	*Risk*	*Overall likelihood*	*Impact*	*Risk*	*Overall likelihood*	*Impact*	*Risk*
Metric (1): 'robot ON' or 'attack activated' to 'software disconnected'	0.84	11.28%	*9.48*	0.82	14.29%	*11.72*	0.82	9.77%	*8.01*
Metric (2): 'robot ON' or 'attack activated' to 'robot warning buzzer beeps'	0.84	1.25%	*1.05*	0.82	13.75%	*11.28*	0.82	0%	*0*
Metric (3): 'robot warning buzzer beeps' to 'software disconnected'	0.84	26.42%	*22.19*	0.82	15.09%	*12.37*	0.82	24.53%	*20.11*

6 Discussion

In this section, we discuss the physical consequences of the loss of availability of the robots, the possibility of detecting the attacks, and some mitigation strategies. However, robots can operate in multiple environments and for the sake of facilitating our discussion in this section, we chose to consider industrial environments as was motivated in Section 1 when we talked about OT. We assume the following setup and only focus on mobile robots as opposed to stationary ones.

Generally speaking in industrial environments, in order to allow higher mobility and long operation time, mobile robots are used, where they are self powered through batteries with known docking stations for auto charging. When the power levels of the batteries become low or fall under established limits, robots will automatically use the docking stations for charging. Thus, when robots are assigned specific tasks to be performed such as stock delivery or helping in the production of expensive instruments and equipment, losing their availability (e.g., become out of batteries) could result in a financial impact, which can lead to catastrophic results. For example, what if a robot

in an industrial workhouse was attacked and resulted in fully drained its batteries while on its way to the docking station. The result is that one of the working task force of the warehouse is lost. Therefore, assuring the robots availability all the time is indeed a major concern. Motivated by this fact, security experts need to carefully consider taking well-studied countermeasures to reduce or even prevent attacks that can target the availability of the robots.

6.1 Cyberphysical impact

Considering the risk analysis of the PeopleBot robot that we carried out in this paper and the computed risk results of the performed attacks in Table 4, it was clear that attack 2 had the highest risk (11.72) followed by attack 1 and lastly attack 3. Indeed, this was expected as attack 2 relied on the ability to inject a malware to the robot system to exhaust the computing resources of the robot, which is a very dangerous and harmful thing to have. However, in order to give further insight and perspective of the risk associated with rest of the attacks (specifically attack 1 and attack 3), we carefully analysed the running path of all the attacks and used the rest of the availability time metrics listed in the last two rows of Table 2 to compute the risk values. The results are shown in Table 5.

The computed risk values listed in the second row of Table 5 are the same to those listed in the last column of Table 4, which were computed based on metric (1) in Table 2. The last two rows of Table 5 list the computed risk values based on metric (2) and metric (3) of Table 2. Looking carefully about these risk values, the following can be observed and noted:

- Based on the risk values associated with metric (2), attack 2 has the highest risk, where attack 1 and attack 3 are associated with very minimal risk (almost have same risk values; around zero or zero values). This indicates that attacks 1 and 3 have almost no effect during the time period where the robot software are ON (or attack is active) until the robot buzzer started to beep. However, attack 2 has the highest impact and thus risk.
- Based on the risk values associated with metric (3), attack 1 has the highest risk, followed by attack 3 and then attack 2. It should also be noted that attacks 1 and 3 are both associated with high risk values (22.19 and 20.11 respectively) in comparable to attack 2 (risk value = 12.37). Thus, the use of metric (3) indicates that attacks 1 and 3 are very critical and have the greatest impact on making the robot unavailable during the time period where the robot buzzer started to beep until the robot software is disconnected. Additionally, the use of metric (3) indicates that attack 2 has a good impact, but not as good as that of attacks 1 and 3.
- The impact and risk associated with attack 2 are almost consistent and very comparable based on all of the used metrics.
- Based on the previous observations and from an attacker point of view, an attacker can utilise attack 2 during the time period associated with metric (2) and then can utilise either attack 1 or attack 3 during the time period associated with metric (3) to cause a DoS to the robot and its software in order to quickly render

the robot unavailable. However, the use of metric (1) indicates that an attacker can just rely on attack 2 in order to render the robot unavailable as it is associated with the highest risk value compared to the rest of the attacks, and has almost consistent effect during the entire period when the attack is started until robot software is disconnected (the computed risk value are almost same or comparable based on all metrics).

6.2 Proposed attack detection system

Obviously, a lack of security in robotic systems is unnerving due to the high risk associated with the many threats that can target the robots. This was clear and demonstrated with the three presented attacks as discussed above. Therefore, a threat detection system or what is known as intrusion detection system (IDS) is indeed something that must be deployed and utilised on the robotic systems. However, the use of IDS is a trade-off between gaining a more secured system on the account of consuming more power as a result of running the IDS system. Discussing this trade-off is very important, but it is considered out of the scope of the paper. In this subsection, we just would like to suggest a possible IDS system for the three attacks presented in the paper. The main idea came up after we further analysed the power profile associated with the attacks as shown in Figures 8, 9 and 10.

Figure 8 combines and shows all the power profiles of the attacks and the baseline performance [A-B region of Figure 4(a)]. In Figure 8, we identified two region of interests (ROI's) or bounding boxes which are very much related to the used metrics presented in Table 2:

- ROI_1: Outer dotted box, which is highlighted in Figure 9. This ROI is identified based on the following time instants

  a The time instant at which any of the performed attacks first causes the robot buzzer to beep.

  b The time instant at which any of the performed attacks first causes the robot software to be fully disconnected.

- ROI_2: Inner shaded box, which is highlighted in Figure 10. This region is identified to be about the 50th percentile of ROI_1. It should be mentioned that the linear least squares curve fitting method is what used to fit the data points in this region of interest. Additionally, as highlighted underneath each linearly fitted curve in Figure 10, the squared correlation coefficients R^2 are included, which demonstrate that the linear model is indeed an excellent model in fitting the data.

The main motivation of identifying the above ROI's is that we wanted to see if we can design a detection system of the attacks based on observing the slopes of the attacks over certain period of the operation time of the robot while being attacked. Thus, we wanted to possibly see if there is any possible and clearly identified slope deviations or variations that are unique to the performed attacks as compared to the base line performance without any attack. If such variations do exist, then we can possibly use them to uniquely detect each attack type. It turned out that:

- ROI_1 does not possess or show any clear slope deviations to detect the attacks.

Figure 8 Performance evaluation: comparison (see online version for colours)

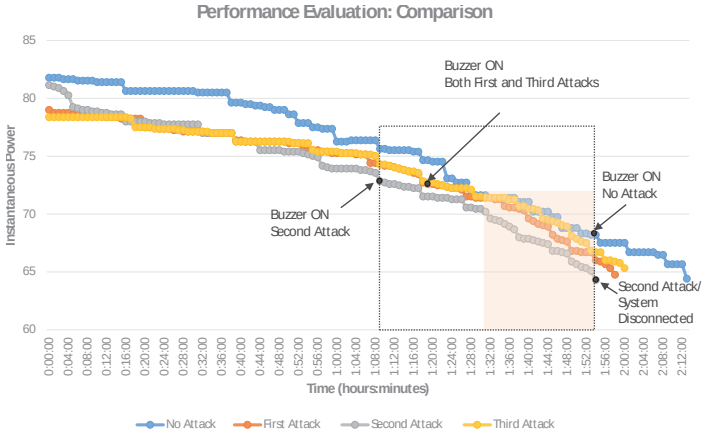


Figure 9 Performance evaluation: comparison [zoomed view – ROI_1 (outerbox) of Figure 8] (see online version for colours)

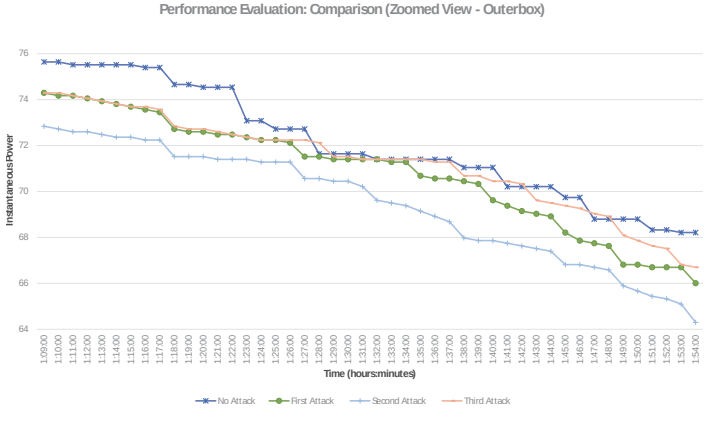
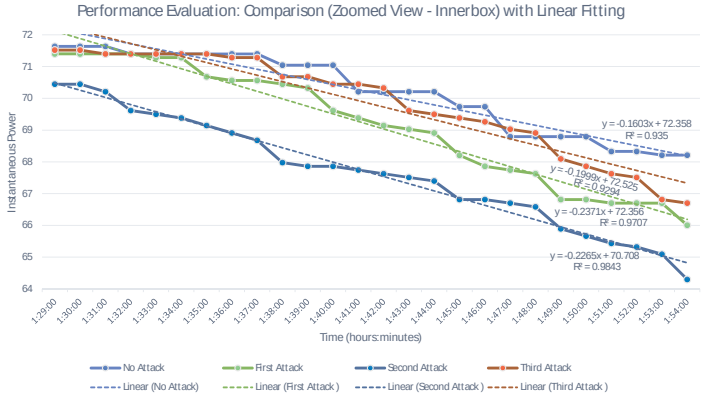


Figure 10 Performance evaluation: comparison [zoomed view – ROI_2 (innerbox) of Figure 8 with linear fitting]



- ROI_2 clearly possesses noticeable slope deviations. Consequently, the linear fitting curves of the power profiles of the attacks as depicted in Figure 10 indicate that the no-attack, attack 1, attack 2, and attack 3 have the following slopes –0.1603 $\pm$ 0.0086, –0.2371 $\pm$ 0.0084, –0.2265 $\pm$ 0.0058, and –0.1999 $\pm$ 0.0112, respectively, where these slope values were normalised to 24 hours by dividing the time values (x-axis) by 60 $*$ 24 or 1,440.

The slope values above suggest that we can design an IDS system that operates on the ROI_2 region to detect the types of the attacks if presented. When the detected slope value becomes very close to –0.2 or smaller then that means the robot system is indeed under one of the attacks, otherwise there is no attack. This proposed IDS system might be a starting point to design a more robust IDS, which is planned to be done as a future work.

6.3 Mitigation

It is vital to consider the battery of robotic systems as a vulnerability and hence, methodologies should be devised to protect it from the various attacks. Therefore, for the first attack, one possible mitigation is to limit the number of active connections to the server (i.e., robot). Usually, the operators of the robot are known and there is no need to allow too many active connections. This mitigation can be configured through the firewall of the operating system (OS) running the robot. For the second and third attacks, application whitelisting (AWL) can be used to detect and prevent execution of malware delivered by threat agents (CISA, 2016; Solutions, 2015). Lastly, adopting a robust low-power IDS system is a good thing to have. An important question to be answered regarding the use of IDS is that: what level of security is required? as typically the more security needed means more power to consume.

Given the suggested mitigations above, it is important to be realised that enforcing and implementing security policies as part of the robotic system design, may not imply that the entire system is safe or available. Therefore, in order to have a comprehensive security approach, we need to employ three steps: assess security, implement security [e.g., anomaly detection, security monitoring, firewalls and VPN, system hardening, patch management, security zones and demilitarised zone (DMZ), etc.], and manage security (Hingley, 2018; Solutions, 2015).

7 Conclusions and future directions

In this paper, we analysed the power profile of the PeopleBot mobile robot platform, an embedded system, without and with attacks. Three possible attacks were analysed and discussed, which targeted the computing resources of the robot (CPU, network bandwidth, sensors, and storage). We showed that such attacks resulted in reducing the availability time of the robot by 11.78% on average using metric (1) that was presented in Table 2. We followed the adversarial risk assessment template provided in NIST and presented an impact-oriented quantitative analysis approach to assess the risk of these attacks as was shown quantitatively in Table 5. To the best of our knowledge, we believe that this is the first paper to quantitatively perform such risk assessment for the PeopleBot robot. A possible detection system for the performed attacks was suggested

and some mitigations were provided. All in all, it was clear that it is now imperative to raise awareness and increase understanding of the emerging attacks for mobile robots and other CPSs in general; especially those operated in industrial environments.

In this work, we just focused on quantitatively studying the availability security requirement of the PeopleBot robot, which is considered an indoor robot platform. Thus, for our future directions, we plan to extend our quantitative risk assessment to study other security functions of the robot such as integrity, confidentiality or others that seem to be more unique to the robotic systems. Additionally, we would like to consider studying other robotic platforms such as outdoor ones. Also, we would like to design a robust low-power IDS system. Moreover, we would like to study and analyse the case of adding an energy harvesting module for robots (specifically for outdoor ones) as we believe this may provide another source of energy. Hence, it becomes harder to drain the battery and consequently increases the resilience of the robot from power-drain attacks.

Acknowledgements

We would like to acknowledge that this research was supported by a grant (its number is 26/2015) from the Deanship of Scientific Research at the Hashemite University, Zarqa, Jordan.

References

2019 Verizon Data Breach Investigations Report (2019) [online] https://enterprise.verizon.com/resources/reports/2019/2019-data-breach-investigations-report-emea.pdf (accessed April 2021).

Adept MobileRobots Software [online] http://www.mobilerobots.com/Software.aspx (accessed January 2017).

Ahmad Yousef, K, AlMajali, A., Hasan, R., Dweik, W. and Mohd, B. (2017) 'Security risk assessment of the PeopleBot mobile robot research platform', in *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, IEEE, November, pp.1–5.

Ahmad Yousef, K., AlMajali, A., Ghalyon, S., Dweik, W. and Mohd, B. (2018) 'Analyzing cyber-physical threats on robotic platforms', *Sensors*, Vol. 18, No. 5, p.1643.

Aijaz, L., Aslam, B. and Khalid, U. (2015) 'Security operations center – a need for an academic environment', in *2015 World Symposium on Computer Networks and Information Security (WSCNIS)*, IEEE, pp.1–7.

AlMajali, A., Yousef, K.M.A., Mohd, B.J., Dweik, W., Ghalyon, S.A. and Hasan, R. (2018) 'Semi-quantitative security risk assessment of robotic systems', *Jordanian Journal of Computers and Information Technology*, Vol. 4, No. 3, pp.185–200.

AlMajali, A., Wadhawan, Y., Saadeh, M.S., Shalalfeh, L. and Neuman, C. (2020) 'Risk assessment of smart grids under cyber-physical attacks using Bayesian networks', *International Journal of Electronic Security and Digital Forensics*, Vol. 12, No. 4, pp.357–385.

Al-Sibai, H.S., Alrubaie, T. and Elmedany, W.M. (2021) 'IoT cybersecurity threats mitigation via integrated technical and non-technical solutions', *International Journal of Electronic Security and Digital Forensics*, Vol. 13, No. 3, pp.298–333.

Bezemskij, A., Loukas, G., Anthony, R.J. and Gan, D. (2016) 'Behaviour-based anomaly detection of cyber-physical attacks on a robotic vehicle', in *International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security (IUCC-CSS)*, IEEE, pp.61–68.

Blank, R. and Gallagher, P. (2012) *NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments*, Tech. Rep., National Institute of Standards and Technology.

Bonaci, T., Yan, J., Herron, J., Kohno, T. and Chizeck, H.J. (2015) 'Experimental analysis of denial-of-service attacks on teleoperated robotic systems', in *Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems*, ACM, pp.11–20.

CISA (2016) *Cyber-Attack Against Ukrainian Critical Infrastructure*, Technical Report ICS Alert (IR-ALERT-H-16-056-01), February, Cybersecurity and Infrastructure Security Agency, Washington, DC, USA.

Dudek, W. and Szynkiewicz, W. (2019) 'Cyber-security for mobile service robots-challenges for cyber-physical system safety', *Journal of Telecommunications and Information Technology*, Vol. 2, No. 2, pp.29–36.

Grooby, S., Dargahi, T. and Dehghantanha, A. (2019) 'A bibliometric analysis of authentication and access control in IoT devices', in *Handbook of Big Data and IoT Security*, pp.25–51, Springer.

Guide for Conducting Risk Assessments [online] https://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf (accessed April 2021).

Hingley, P. (2018) 'IIot... Ind 4.0... a thirst for data...', *EU Cyber Summit*, Siemens.

Krishnaswami, J. (2004) *Denial-of-Service Attacks on Battery-Powered Mobile Computers*, PhD thesis, Virginia Tech.

Kundu, A., Lin, Z. and Hammond, J. (2017) *Energy Attacks on Mobile Devices*, arXiv preprint arXiv:1704.04464.

Larabel, M. and Tippett, M. (2011) *Phoronix Test Suite*, Phoronix Media [online] http://www.phoronix-test-suite.com/ (accessed January 2020).

Martin, T., Hsiao, M., Ha, D. and Krishnaswami, J. (2004) 'Denial-of-service attacks on battery-powered mobile computers', in *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications, PerCom 2004*, IEEE, pp.309–318.

Matellán, V., Bonaci, T. and Sabaliauskaite, G. (2017) 'Cyber-security in robotics and autonomous systems', *Robotics and Autonomous Systems*, Vol. 100, pp.41–42, Elsevier.

Mei, Y., Lu, Y-H., Hu, Y.C. and Lee, C.G. (2005) 'A case study of mobile robot's energy consumption and conservation techniques', in *ICAR'05, Proceedings, 12th International Conference on Advanced Robotics*, IEEE, pp.492–497.

Mohd, B.J., Yousef, K.M.A., AlMajali, A. and Hayajneh, T. (2019) 'Power-aware adaptive encryption', in *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology*, April, pp.711–716.

Mukhandi, M., Portugal, D., Pereira, S. and Couceiro, M.S. (2019) 'A novel solution for securing robot communications based on the MQTT protocol and ROS', in *2019 IEEE/SICE International Symposium on System Integration (SII)*, IEEE, pp.608–613.

PeopleBot [online] https://telepresencerobots.com/robots/adept-mobilerobots-peoplebot (accessed April 2021).

PeopleBot [online] https://www.generationrobots.com/media/PeopleBot-PPLB-RevA.pdf (accessed April 2021).

ROS Adept MobileRobots Pioneer and Pioneer-Compatible Platforms [online] http://wiki.ros.org/Robots/AMR_Pioneer_Compatible (accessed April 2021).

Shah, R. (2019) *Security Landscape for Robotics*, arXiv preprint arXiv:1904.03033.

Solutions, V. (2015) *Seven Steps to Effectively Defend Industrial Control Systems* [online] https://us-cert.cisa.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf (accessed April 2021).

Srinivas, B.V. (2014) *Security Operations Centre (SOC) in a Utility Organization* [online] https://www.sans.org/white-papers/35502/ (accessed April 2021).

T.E.U.A. for Cybersecurity ENISA (2020) *ENISA Threat Landscape Report 2020* [online] https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020 (accessed April 2021).

Vilches, V.M., Kirschgens, L.A., Calvo, A.B., Cordero, A.H., Pisón, R.I., Vilches, D.M., Rosas, A.M., Mendia, G.O., Juan, L.U.S., Ugarte, I.Z. et al. (2018) *Introducing the Robot Security Framework (RSF), A Standardized Methodology to Perform Security Assessments in Robotics*, arXiv preprint arXiv:1806.04042.

Wang, C., Tok, Y.C., Poolat, R., Chattopadhyay, S. and Elara, M.R. (2021) 'How to secure autonomous mobile robots? An approach with fuzzing, detection and mitigation', *Journal of Systems Architecture*, Vol. 112, p.101838, ISSN: 1383-7621.

Wardega, K., Tron, R. and Li, W. (2019) 'Masquerade attack detection through observation planning for multi-robot systems', in *Proceedings of the 18th International Conference on Autonomous Agents and MultiAgent Systems*, International Foundation for Autonomous Agents and Multiagent Systems, pp.2262–2264.