Jornadas Nacionales de Robótica

Spanish Robotics Conference

8-9 Junio 2017

Valencia

Organizado por:

Universitat Politècnica de València

Instituto Universitario de Automática e Informática Industrial

Comité Español de Automática

Grupo Temático de Robótica

Título: Libro de actas de las Jornadas Nacionales de Robótica 2017

Editores: Martin Mellado Arteche, Antonio Sánchez Salmerón, Enrique J Bernabeu Soler

Editorial CEA-IFAC

ISBN: 978-84-697-3742-2

Jornadas Nacionales de Robótica
Spanish Robotics Conference
8-9 Junio 2017 http://jnr2017.ai2.upv.es

Desarrollo seguro de software para robots y sistemas autónomos

Vicente Matellán [a 1], Ángel Manuel Guerrero-Higueras[b], Jesús Balsa-Comerón[a], Camino Fernández-Llamas[a], Francisco J. Rodríguez-Sedano[b], Miguel Á. Conde[b], Francisco Javier Rodríguez-Lera[c]

[a] *Grupo de Robótica. Depto. de Ingenierías Mecánica, Informática y Aero-espacial. Universidad de León, España.*
[b] *Instituto de Ciencias Aplicadas a la Ciberseguridad (RIASC), Universidad de León, España.*
[c] *AI Robolab. University of Luxembourg, Luxemburgo*

Resumen

Este artículo presenta las actividades en desarrollo en el marco del proyecto sobre ciberseguridad en sistemas con capacidades autónomas que está desarrollando el Grupo de Robótica de la Universidad de León (ULE) en colaboración con el Instituto Nacional de Ciberserguridad (INCIBE). El trabajo realizado hasta la fecha tiene como objetivo principal la mejora de la ciberseguridad en sistemas robóticos. En concreto, durante el primer año de desarrollo se han abordado dos problemáticas diferentes: la primera tiene que ver con el bastionado de los entornos de desarrollo de software para robots. En concreto se ha trabajado sobre el *middleware* ROS (*Robotic Operating System*) analizando sus vulnerabilidades y ofreciendo una solución a nivel de aplicación basado en monitorización y cifrado del entorno desplegado. La segunda tiene que ver con el análisis de los problemas de seguridad en sistemas de localización para interiores. En concreto, se han desarrollado mecanismos de detección de ataques de denegación de servicio (DoS) y de *spoofing* en sistemas de localización para interiores basados en balizas de radio.

Palabras Clave:
Ciber-seguridad, robótica, sistemas autónomos, sistemas de localización
Datos del Proyecto:
Denominación del proyecto: Ciberseguridad en Sistemas Autónomos
Referencia: Adenda 21
Investigador/es responsable/es: Vicente Matellán Olivera
Tipo de proyecto (internacional, nacional, autonómico, transferencia): Nacional
Entidad/es financiadora/s: INCIBE SA y Universidad de León
Fecha de inicio/fin: 17/12/2015 al 17/12/2018

1. Introducción

La preocupación por la ciberseguridad de los sistemas robóticos está creciendo (Morante2015). Cada vez va a ser más frecuente encontrarse con sistemas robóticos fuera de los laboratorios de investigación. Dichos dispositivos deben ser seguros en su interacción con los usuarios y cíber-seguros en su interacción con otros dispositivos computacionales, especialmente si están conectados a Internet.

El plan de trabajo del proyecto identificaba a priori dos líneas de investigación principales: desarrollo de sistemas autónomos para seguridad y la ciberseguridad de los sistemas autónomos, indicando la segunda como la primera a abordar.

En esa línea, un elemento primordial de la ciberseguridad son los *frameworks* de desarrollo de software para robots que se utilizan. En el caso de la robótica existen numerosas alternativas (Magyar2015), algunas desarrolladas por fabricantes, pero muchas originadas en entornos universitarios o de investigación, pero que actualmente se han extendido al entorno comercial.

Estos *middlewares* tienen generalmente origen investigador tradicionalmente no han prestado atención al problema de la ciberseguridad porque no es un requisito fundamental en dichos entornos.

En este contexto surge la necesidad de analizar el estado de la cíber-seguridad de los *frameworks* para el desarrollo de software que más se utilizan en la actualidad. En particular el proyecto establece como prioridad el análisis de la ciber-seguridad de ROS - *Robotic Operating System* - (Quigley2009) por ser el *framework* que se ha convertido en el estándar de facto para el desarrollo de aplicaciones en robots móviles.

Adicionalmente, se ha establecido un segundo objetivo que es el análisis de los ataques a sistemas de localización en interiores porque se trata de sistemas que se utilizan en numerosas aplicaciones, especialmente en entornos de robots móviles industriales. En concreto se ha realizado un análisis de ataques de Denegación de Servicio (DoS) y de *Spoofing* sobre un sistema comercial basado en balizas de radiofrecuencia colocadas en posiciones fijas del entorno y un receptor que se monta en el robot móvil cuya posición se desea conocer.

[1]Autor en correspondencia.
Correos electrónicos: vicente.matellan@unileon.es (Vicente Matellán), am.guerrero@unileon.es (Ángel Manuel), jbalc@unileon.es (Jesús Balsa), camino.fernandez@unileon.es (Camino Fernández), francisco.sedano@unileon.es (Francisco J.R. Sedano), mcong@unileon.es (Miguel A. Conde), francisco.lera@uni.lu (Francisco J.R. Lera)
URL: http://robotica.unileon.es

El resto del artículo se organiza como sigue: La siguiente sección presenta un análisis general de la seguridad en los sistemas autónomos. La tercera sección resume las actividades realizadas en el bastionado de ROS. La cuarta presenta los primeros resultados en la detección de ataques a sistemas de localización. La última sección resume brevemente las conclusiones preliminares que se han obtenido y los trabajos que se espera desarrollar en el marco de este proyecto.

2. Seguridad en sistemas Autónomos

El objetivo del proyecto es la mejora de la cíber-seguridad de los sistemas autónomos. El estado del arte presenta multitud de trabajos relativos a sistemas cíber-físicos industriales. En ellos se analizan generalmente entornos bien definidos, donde es posible acotar los problemas asociados a la seguridad física (de contacto humano-robot) y la seguridad virtual (de los datos) del sistema.

Sin embargo, es muy difícil aplicar los mismos conceptos de seguridad a otros entornos, por ejemplo, los domésticos, ya que presentan unas características muy diferentes, como un dinamismo mayor que los entornos industriales. Ello hace que los productos robóticos que están llegando al mercado de consumo no estén suficientemente maduros en los aspectos de cíber-seguridad. El motivo fundamental a juicio de los autores de este trabajo es que los fabricantes se han centrado más en la usabilidad y en la eficacia en la realización de las tareas que en los aspectos de cíber-seguridad. Sin embargo. se abre una vía potencial de cíber-ataques (Denning2009).

Estos problemas no son exclusivos de los sistemas robóticos domésticos. Otros muchos sistemas autónomos de consumo presentan problemas similares. Por ejemplo, los automóviles sin conductor que están actualmente siendo objeto de gran atención mediática y que se podrían calificar como robots móviles con pasajeros, presentan diferentes tipos de vulnerabilidades (Yağdereli2015) ya conocidas en otros entornos, pero que no dejan de suponer una amenaza.

En el campo de la medicina, existen igualmente robots quirúrgicos que permiten realizar tele-operaciones de manera eficaz, e irán apareciendo más a corto plazo. El personal médico puede manejar a distancia estos robots, realizando las cirugías por control remoto. Sin embargo, la ausencia de ciberseguridad en estos robots también ha sido descrita desde hace tiempo (Bonaci2012).

Por todo ello cabe preguntarse, ¿Qué está realmente comprometido cuando desplegamos un robot en entornos domésticos? Por un lado, la seguridad física del usuario o usuarios con las que comparte el entorno (Mitka2012). Por otro lado, la seguridad del sistema lógico del robot ya que no deja de ser un sistema informático empotrado como sistema de control de un conjunto de sensores y actuadores.

El sistema lógico deberá implementar mecanismos suficientes para garantizar la seguridad de la información. Para el análisis de la seguridad robóticos hemos utilizado como sistema de referencia el esquema *IAS-Octave* (Cherdantseva2012) basado en ocho elementos: 1) confidencialidad, 2) integridad, 3) disponibilidad, 4) autenticidad, 5) responsabilidad, 6) auditabilidad, 7) privacidad e 8) irrefutabilidad (no repudio). Este esquema teórico abarca todo el ciclo para asegurar la información en una empresa u organización y creemos que es fácilmente trasladarle al proceso de gestión de la información que realizan las plataformas robóticas de forma genérica.

Como resultado de aplicar dicho modelo, la Tabla 1 muestra nuestra valoración de los valores de criticidad para los componentes de seguridad que consideramos más relevantes en el caso de los robots móviles. Una versión más completa de este análisis puede encontrarse en (Lera2017).

Tabla 1: Niveles de criticidad en las componentes de seguridad para diferentes tipos de sistemas

Perfil	Criticidad		
	Confidencialidad	Integridad	Disponibilidad.
Estación de Trabajo	Alta	Alta	Baja
Control Industrial	Media	Media	Muy Alta
Robots Asistenciales	Muy Alta	Muy Alta	Muy Alta
Robots Sociales	Muy Alta	Media	Baja

A partir de estos valores hemos realizado el análisis del *framework* de desarrollo más utilizado en la actualidad (ROS), que describimos en la siguiente sección.

3. Securización del *framework* de desarrollo ROS

ROS (Quigley2009) es un *framework* diseñado para facilitar el desarrollo de software para robots y acelerar su difusión. A pesar de su nombre, no se trata de un sistema operativo, es un *middleware* distribuido que proporciona soporte para procesos, llamados "nodos" en la terminología ROS.

La arquitectura de ROS se basa en un grafo de nodos, donde cada nodo es un proceso independiente, que puede ejecutarse en máquinas diferentes.

Estos procesos se ejecutan en paralelo y se encargan de realizar distintas tareas sobre el robot: procesar datos de los sensores, calcular la localización, conducir al robot por un entorno, etc. Los nodos pueden intercambiar información entre ellos de forma asíncrona suscribiéndose a canales llamados "topics", y de manera síncrona mediante "services".

3.1. Problemas en ROS

El principal problema de seguridad de ROS es que las comunicaciones entre los nodos se realizan en texto plano, sin aplicar ningún mecanismo de protección. En (Pohl2014) se analizan a fondo las vulnerabilidades de ROS. Atendiendo a las tres componentes mencionados, sus principales problemas de seguridad son los siguientes:

Disponibilidad

La disponibilidad se centra en la prevención de fallos en el sistema como resultado de un ataque. Por ejemplo, la anulación de funcionamiento de un componente por medio de un ataque de denegación de servicio.

El sistema de intercambio de datos entre nodos de ROS, está gestionado únicamente por el nodo Máster. Si este nodo se ve comprometido, todo el sistema se vería afectado.

Una posible solución se basaría en implementar varios nodos Máster redundantes.

Integridad

La integridad consiste en garantizar la no modificación en los datos. Los datos enviados entre nodos de ROS situados en equipos diferentes, se transmiten sin cifrar por la red utilizando un protocolo propio llamado TCPROS.

ROS aplica una comprobación de firma MD5 al tipo de mensaje que un nodo espera recibir, para asegurar que el tipo de dato es correcto.

Sin embargo, no aplica ningún método de chequeo a los datos contenidos en el mensaje, con lo que ROS no ofrece integridad en la información intercambiada.

Los mensajes podrían ser manipulados por un atacante que se encuentre conectado a la misma red que el robot.

En (Lera2016b) analizamos una posible solución a este problema consistente en cifrar los datos intercambiados. En ese mismo trabajo analizados el rendimiento de alternativas basadas en diferentes algoritmos de cifrado (AES, *Blowfish*, etc.) para diferentes tipos de datos (lecturas de láser, imágenes, etc.) y en CPUs diferentes.

Confidencialidad

Esta propiedad se refiere a la protección de los datos contra accesos no autorizados. Debido a la transmisión en claro de los mensajes a través de la red, ROS no proporciona confidencialidad. En este sentido, un atacante podría leer y guardar en su equipo los datos de un sensor (por ejemplo, las imágenes de una cámara).

Los puertos TCP que usan los nodos para la conexión por red desde otros equipos, no tienen ninguna protección. Realizando un simple escaneo de puertos, es posible saber el puerto de un nodo.

Además de estas tres componentes, ROS presenta problemas en otras dimensiones del modelo IAS-Octave. Por ejemplo, en ROS no hay mecanismos de autentificación, por lo que es posible realizar ataques de suplantación de nodos. Es decir, un atacante podría crear nodos "falsos" con los mismos nombres y engañar al resto de componentes. En realidad, ROS casi favorece este ataque, puesto que cuando en ROS se lanza un nuevo nodo con el mismo nombre que otro que se está ejecutando, el "Master" finaliza la ejecución del primer nodo y da paso al segundo, ya que no puede haber dos nodos con en ROS con el mismo nombre.

Este funcionamiento del Master de ROS se implementó para facilitar el despliegue de nuevas versiones de software sin tener que detener la ejecución, pero como se comentó anteriormente, es el tipo de *feature* que es muy apreciada en entornos de investigación y desarrollo, pero que incorpora graves problemas de seguridad en sistemas comerciales.

Una vez analizados los problemas de forma sistemática, se han propuesto diferentes soluciones.

3.2. Bastionado de ROS

En primer lugar, puesto que ROS se basa en XML-RPC, la primera medida es reducir los problemas debidos a las vulnerabilidades conocidas de dicho protocolo. Por ejemplo, proponemos actualizar el *parser* de Python utilizado en ROS incorporando la librería `python-defusedxml` que proporciona un módulo para proteger de bombas XML en los módulos de Python `stdlib` (Python 2). Esto nos permitiría solventar problemas a ataques de tipo DoS que buscan explotar las vulnerabilidades del análisis de documentos XML utilizado por Python.

La siguiente propuesta que hemos realizado plantea la utilización de cifrado a nivel de aplicación para solventar los problemas de confidencialidad asociados al uso del paradigma de publicación-subscripción sin cifrar que usa ROS. Los detalles de esta propuesta se pueden encontrar en (Lera2016a).

Para valorar la influencia del cifrado en el rendimiento general de las plataformas hemos realizado una comparativa del desempeño de dos plataformas robóticas con diferentes CPUs, (Lera2016b).

Para ello se han realizado una serie de experimentos que han implicado la instalación de ROS en varios robots (Orbi-One y Karen) y en diferentes computadores del grupo de robótica de la Universidad de León, tanto equipos i7 de alta gama como Atom).

Además, se ha generado un *dataset* de prueba en forma de `rosbags`, el formato estándar de log de ROS, que permite la reproducción off-line o en simulador. Este *dataset* está disponibles en la web del grupo de robótica de la universidad de León[2].

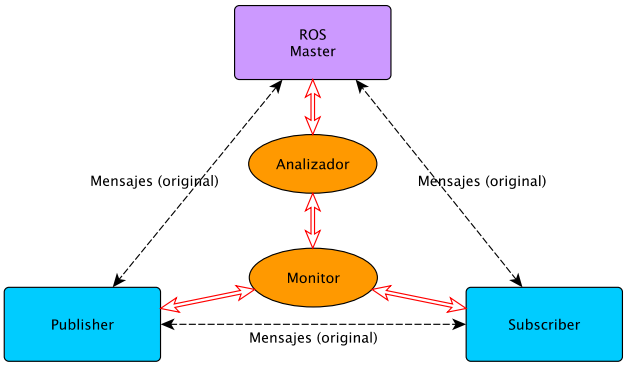

Figura 1: Propuesta de arquitectura para el análisis semántico de riesgos de ciber-ataques a plataformas basadas en ROS

En la actualidad se está trabajando en la implementación de una arquitectura (resumida en la Figura 1) que permite realizar el análisis del estado del sistema mediante la inclusión de uno nodo ROS de monitorización (Monitor) y el análisis mediante reglas semánticas en otro nodo adicional (Analizador).

Estos nodos se encargarán tanto de verificar la seguridad física, es decir, que el robot no incumple una serie de reglas (velocidad máxima, distancia a humanos, etc.) así como de cíber-seguridad (accesos remotos, etc.).

4. Detección de ataques en sistemas de localización

Los sistemas de localización para sistemas autónomos, el GPS por ejemplo, son elementos críticos para determinadas aplicaciones, y como tales han sido objeto de diversos ataques. Incluso en sus versiones militares han sufrido ataques (Psiaki2016).

Los sistemas de localización no son sólo útiles en robots de exteriores, también existen numerosas aplicaciones para robots de interiores. Especialmente en entornos industriales (logística, seguridad, etc.).

También los robots de servicios hacen uso de estos sistemas en lugar de utilizar mecanismos de auto-localización como las diferentes técnicas de SLAM. El motivo es que los sistemas de posicionamiento son más baratos y fiables que los sistemas de auto-localización, aunque estos sean mucho más interesantes desde el punto de vista de la investigación.

[2] http://niebla.unileon.es/proyectos/publications/dataset-kio-rtls.git

Por ello, la segunda línea de trabajo se ha centrado en los problemas de seguridad de los sistemas de posicionamiento para robots de servicios en entornos de interiores.

Para ello se ha instalado en los laboratorios del grupo de robótica una maqueta de un sistema de localización para interiores basada en tecnología *Ultra-WideBand* (UWB). Concretamente se ha utilizado el producto comercial KIO-RTLS (ver figura 2) de Eliko Tehnoloogia (Estonia).

Este sistema se basa en un conjunto de balizas que se colocan en el edificio (círculo rojo marcado como 1 en la Figura 2) y un receptor que se coloca en el robot e informa de la posición (círculo marcado como 2 en la Figura 2).

Figura 2: Izquierda: Balizas del sistema de localización KIO-RTLS y derecha robot Karen equipado con el sistema

En la Figura 3 se muestra la distribución de las antenas en los Laboratorios del grupo de Robótica de la Universidad de León. En esta maqueta se han simulado diferentes tipos de ataques, como la denegación de servicio (eliminando diferentes tipos de antenas) o de *spoofing* (cambiando su localización) y se están diseñando diferentes tipos de algoritmos que permiten a un sistema robótico detectar este tipo de ataques.

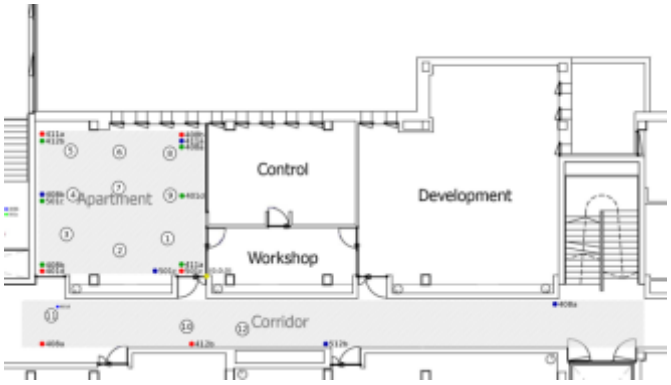

Figura 3: Diferentes distribuciones (colores) de antenas del RTLS-KIO

Además, los primeros resultados de estos experimentos permitirán también establecer guías de buenas prácticas para la instalación de estos equipos, indican por ejemplo qué tipo de distribución de las antenas es más aconsejable para la instalación de RTLS desde el punto de vista de la ciberseguridad.

Por ejemplo, en la Figura 3 se muestran tres alternativas para distribuir 6 balizas. La primera distribución intenta maximizar el área cubierta por el sistema (en azul). La segunda distribución trata de maximizar la precisión (en verde), en este caso sobre la zona del apartamento. La tercera distribución (en rojo) representa el compromiso entre cobertura y precisión.

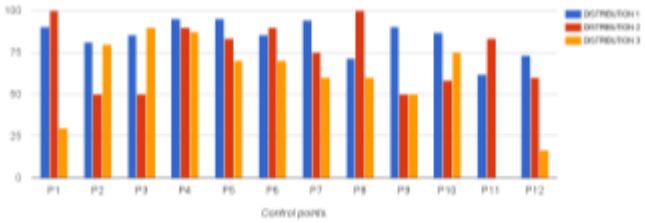

Figura 4: Grado de significación

Los resultados preliminares muestran que la distribución de antenas que persigue maximizar la precisión es también la que permite detectar mejor los ataques de DoS y de Spoofing.

Además, los experimentos realizados nos permiten determinar qué puntos (marcados como círculos negros numerados en la Figura 3) son más discriminantes a la hora de detectar esos ataques.

La figura 4 resume el grado de significación para los 12 puntos de control marcados en la Figura 3 y para cada una de las tres distribuciones mencionadas anteriormente. Como se puede apreciar en dicha figura el punto 4 es el que proporciona más información de forma combinada, mientras que el 1 lo sería para la distribución 2.

5. Conclusión

La primera conclusión que se puede extraer del trabajo realizado en este proyecto hasta la fecha es que la preocupación por la seguridad de los sistemas robóticos está creciendo y hay razones para ello. Cada vez va a ser más frecuente encontrarse con sistemas robóticos fuera de los laboratorios de investigación y dichos dispositivos deben ser seguros en la interacción con los usuarios y cíber-seguros en su interacción con otros dispositivos, especialmente si están conectados a Internet.

Un elemento primordial de la ciberseguridad de los robots de servicio son los *frameworks* de desarrollo. En el caso particular de ROS son bien conocidos sus problemas de seguridad, que se están tratando de resolver en la versión 2 con el cambio de TCPROS por DDS. Sin embargo, la disponibilidad de esa versión se nos antoja aún lejana en el tiempo y además habrá numerosos sistemas ya desplegados que no serán capaces de implementarla. Por ello hemos propuesto soluciones alternativas basadas en cifrado y en la incorporación de nodos de monitorización que permitirán mejorar la seguridad de los robots que usan actualmente ROS.

Otra aportación realizada en este proyecto es el análisis de la seguridad en sistemas de posicionamiento para interiores y la propuesta de mecanismos estadísticos para detectar ataques de DoS y de *Spoofing* en este tipo de entornos. Las técnicas que estamos desarrollando, además de detectar ataques, creemos que servirán para establecer guías de instalación que hagan más robustos estos sistemas.

Además de continuar con los trabajos de cíber-seguridad en robots de servicios, en el *roadmap* de este proyecto está ampliar el tipo de sistemas autónomos cuya cíber-seguridad se tratará de mejorar; así como extenderlo a los diferentes subsistemas de los robots móviles (sensores, cámaras, etc.) más alla de los sistemas de localización.

English Summary

Cybersecurity in Autonomous Systems.

Abstract

This paper presents the activities of the Robotics Group from Universidad de León (ULE) on cyber-security of systems with autonomous capabilities. This work has been carried out in collaboration with the "Instituto Nacional de Ciberserguridad" (INCIBE). The goal of the work carried out up to now has to do with the improvement of cyber-security of robotic systems. It has dealt with two major issues: the first one has to do with the hardening of software development frameworks for robots. In particular, we have analyzed the vulnerabilities of ROS (*Robotic Operating System*) middleware and have developed a proposal to detect attacks and to improve its cyber-security. The second one has to do with the problems in real-time indoor positioning systems. We have developed a method for detecting DoS (Denial of Service) and Spoofing attacks in radio-beacon based systems.

Keywords:

Cyber-security, robotics, autonomous systems, real-time localization systems

Agradecimientos

Este trabajo ha sido financiado parcialmente por el Instituto Nacional de Ciberseguridad (INCIBE) mediante un convenio con la Universidad de León.

Referencias

(Bonaci2012) Bonaci, Tamara; Chizeck, Howard Jay. On potential security threats against rescue robotic systems. 2012 IEEE International Symposium on Safety, Security, and Rescue Robotics, SSRR 2012.

(Cherdantseva2012) Cherdantseva, Y., & Hilton, J. (2012, February). The Evolution of Information Security Goals from the 1960s to today. https://users.cs.cf.ac.uk/Y.V.Cherdantseva/LectureEvolutionInfoSecGOALS.pdf.

(Denning2009) Denning, Tamara, Matuszek, Cynthia, Koscher, Karl; Smith, Joshua R. Kohno, Tadayoshi. A spotlight on security and privacy risks with future household robots. Proceedings of the 11th International Conference on Ubiquitous Computing - Ubicomp '09 pp. 105-114.

(Lera2016a) Lera, F.J., Matellán, V. Casado, F. and Balsa, J. Ciberseguridad en robots autónomos: Análisis y evaluación multiplataforma del bastionado de ROS. Jornada SARTECO, pp. 571-578, dentro del Congreso Español de Informática (CEDI 2016) Salamanca.

(Lera2016b) Lera, F.J., Balsa, J. Casado, F. Fernández, C. Martín, F. and Matellán, V. Casado, F. Cybersecurity in Autonomous Systems: Evaluating the performance of hardening ROS. XVII Workshop en Agentes Físicos, pp. 47-54. Málaga.

(Lera2017) Lera, F.J., Fernández, C. Guerrero, A.M. Matellán, V. Cyber-Security of Robotics and Autonomous Systems: Privacy and Safety. In Robotics - Legal, Ethical and Socioeconomic Impacts, ISBN 978-953-51-5511-9 (No Publicado – En impresión).

(Magyar2015) Magyar, G. Sincak, P. Krizsan, Z. Comparison study of robotic middleware for robotic applications. In Emergent Trends in Robotics and Intelligent Systems. Springer International Publishing, pp. 121–128. 2015. DOI: 10.1007/978-3-319-10783-7_13

(Mitka2012) Mitka, E., Gasteratos, A., Kyriakoulis, N., & Mouroutsos, S. G. (2012). Safety certification requirements for domestic robots. Safety Science, 50(9), pp. 1888–1897. http://doi.org/10.1016/j.ssci.2012.05.009

(Morante2015) Morante S., Victores J.G., Balaguer C. Cryptobotics: Why robots need cyber safety. Frontiers in Robotics and Artificial Intelligence. 2015;2(23):1–4. DOI: 10.3389/frobt.2015.00023

(Psiaki2016) Psiaki, M.L. and Humphreys, T.E. (2016) Protecting fGPS from Spoofers Is Critical to the Future of Navigation. IEEE Spectrum, Vol 10.

(Pohl2014) Pohl, H. (2014). Robot Operating System (ROS): Safe & Insecure. Automationspraxis, 9. Retrieved from http://www.generationrobots.com/en/content/55-ros-robot-operating-system

(Quigley2009) Quigley, M., Conley, K., Gerkey, B., Faust, J., Foote, T., Leibs, J., ... & Ng, A. Y. (2009). ROS: an open-source Robot Operating System. In ICRA workshop on open source software (Vol. 3, No. 3.2, p. 5).

(Yağdereli2015) Yağdereli, E., Gemci, C., & Aktaş, A. Z. (2015). A study on cyber-security of autonomous and unmanned vehicles. The Journal of Defense Modeling and Simulation, 12(4), 369-381.