# Cybersecurity in Autonomous Systems: Analyzing the ROS Communications Model

David Mañanes, Francisco Javier Rodríguez Lera, Jesús Balsa and Vicente Matellán,

***Abstract*—La ciberseguridad en robtica es importante**
**ROS es esl framework ms extendido**
**Cifrar las comunicaciones, medir rendimiento**

***Index Terms*—autonomous systems, cybersecurity, robotics, performance, cyber-physical**

## I. Introduction

AUTONOMOUS systems are spreading not just in the virtual world (Internet, software systems) or in science-fiction movies, but in our ordinary real world. We can already find driverless cars in the streets, autonomous vacuum cleaners in our homes, museum guides hotel assistants, etc. These cyber-physical systems, as any computer-based system, can suffer different types of vulnerabilities, and the need of cybersecurity [3] is required.

ROS (Robotic Operating System) [4] has become the most popular framework for developing robotic applications. It started in the research environment, but currently most of the current manufacturers of commercial platforms use ROS as the *de facto* standar for building robotic software, from manufacturing robots as Baxter (by Rethink robotics) to service robots as our RB1 (by Robotnik).

Contar nuestra linea de robots asistenciales [**?**]

Comentar problemas de privacidad en entornos domesticos: [**?**]

Organizacion del paper

### A. ROS security assestment

ROS framework is basically a message-passing distributed system. Its architecture is based on processes that publish *messages* to *topics*. For instance, a process (*node*) can be in charge of accessing a sensor, making the basic processing of the information, and publishing it as a structure information on a named topic. Another process can *subscribe* to this topic, that is, it can read that information, make a decision about the movement of the robot. These commands will be sent to the motors in another topic.

These nodes can be running in the same computer or in different computers.

Comentar papers sobre seguridad en ROS

caso del honeypot [2]

## II. Testbed description

We want to evaluate if ciphering the communications would affect the performance of ROS.

All authors are with the Robotics Group at Universidad de León (Spain)
Corresponding author: vicente.matellan@unileon.es

### A. Simulated testedbed

We have installed ROS Jade in two computers connected through a wired Ethernet 10/100 switch (model XXXX). In the first computer we have connected a Xtion camera and a Hokuyo laser. In the second computer have run a node visualizing the information from the sensors. Figure **??** shows this environment.

Then we modified the standard ROS implementation. We changed the TCP/IP sockets based implementation by ciphered ones.

### B. Robotic testbed

In the second experiment we changed the first computer for a RB1 robot and the XXX switch by a wireless one. This robot was also running ROS Jade.

## III. Experimental Measuments

Figure **??** shows the maximum rate that can be reached both in the laser and the camera visualization according to `rviz` information.

The same measurements were made in the second environment to see if the use of wireless systems and a real robot would have any influence.

The absolute values of the frame rates is obviously different, as shown in figure **??**. But the interesting part is the relative different when using clear communications or ciphered ones.

Table **??** compares the relative reduction of speed when using ciphered protocols vs clear ones in both environments as well as the relative increase of CPU usage.

## IV. Conclusion and Futher Work

We have evaluated the influence of cyphering in the performance of ROS based robotic systems.

As we commented in the introduction, we think that securing communications is just one dimension in the cybersecurity of Autonomous Systems. If we want to see autonomous systems working in our homes we need to secure the navigation abilities, the interaction mechanisms, etc.

Some works have been sketched in this area, as for instance in [1].

## Acknowledgment

The authors would like to thank the Spanish Ministry of Economy and Competitiveness for the partial support to this work under grant DPI2013-40534-R and to the Spanish National Institue of CyberSecurity (INCIBE) under grand Adenda21 ULE-INCIBE.

## REFERENCES

[1] Jérémie Guiochet. Hazard analysis of humanrobot interactions with HAZOPUML. *Safety Science*, 84:225–237, 2016.

[2] Jarrod McClean, Christopher Stull, Charles Farrar, and David Mascareñas. A preliminary cyber-physical security assessment of the Robot Operating System (ROS). *SPIE Defense, Security, and Sensing*, 8741:874110, 2013.

[3] Santiago Morante, Juan G Victores, and Carlos Balaguer. Cryptobotics: Why robots need cyber safety. *Frontiers in Robotics and AI*, 2(23):1–4, 2015.

[4] Morgan Quigley, Ken Conley, Brian P. Gerkey, Josh Faust, Tully Foote, Jeremy Leibs, Rob Wheeler, and Andrew Y. Ng. Ros: an open-source robot operating system. In *ICRA Workshop on Open Source Software*, 2009.