ROS Cipherer

Publishing & consuming of encrypted topics

Robotics Group
University of León

Jesús Balsa Comerón
Mª Del Carmen Calvo Olivera
Alexis Gutiérrez Fernández
Ángel Manuel Guerrero Higueras

¿Por qué nosotros?

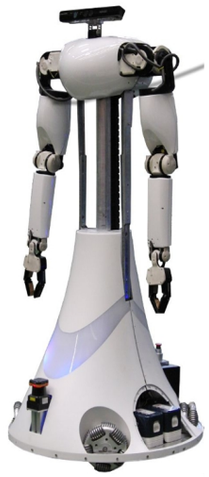
- Robótica asistencial
- Dispositivos hápticos
- **Seguridad en sistemas autónomos**

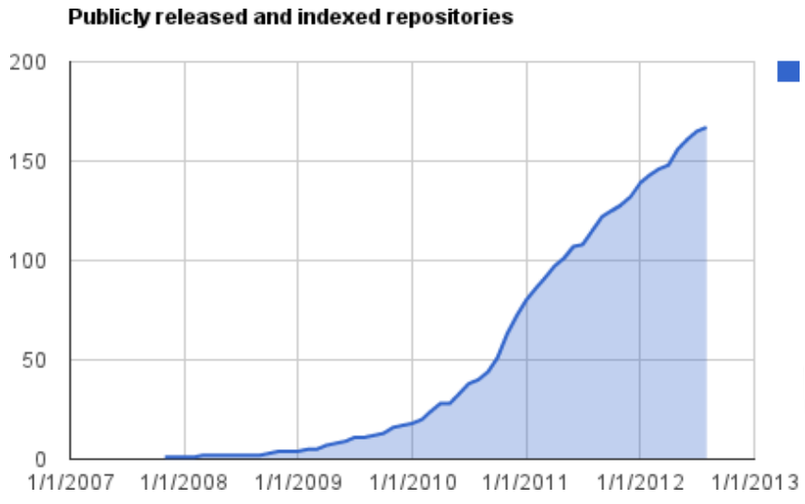
GRUPO DE **ROBÓTICA**

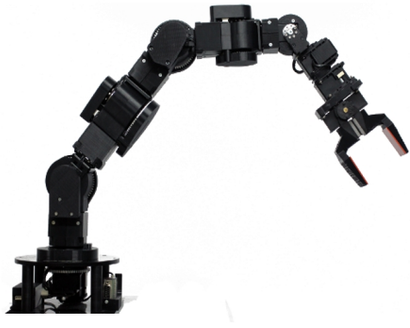
universidad de león

¿Por qué ROS?

- Open source
- Popular
- Estándar de facto





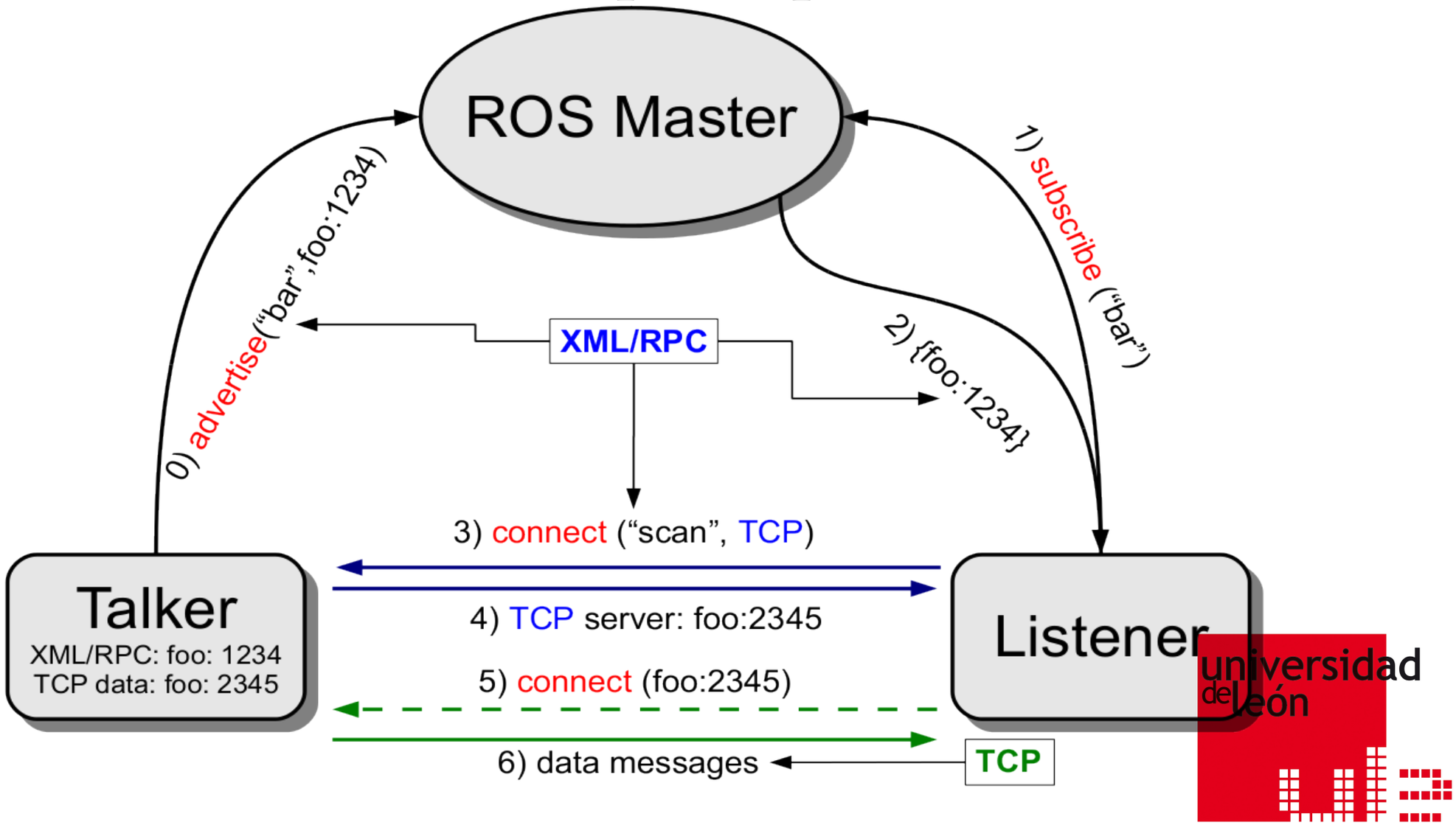


GRUPO DE **ROBÓTICA**

universidad de león

¿Como funciona ROS?

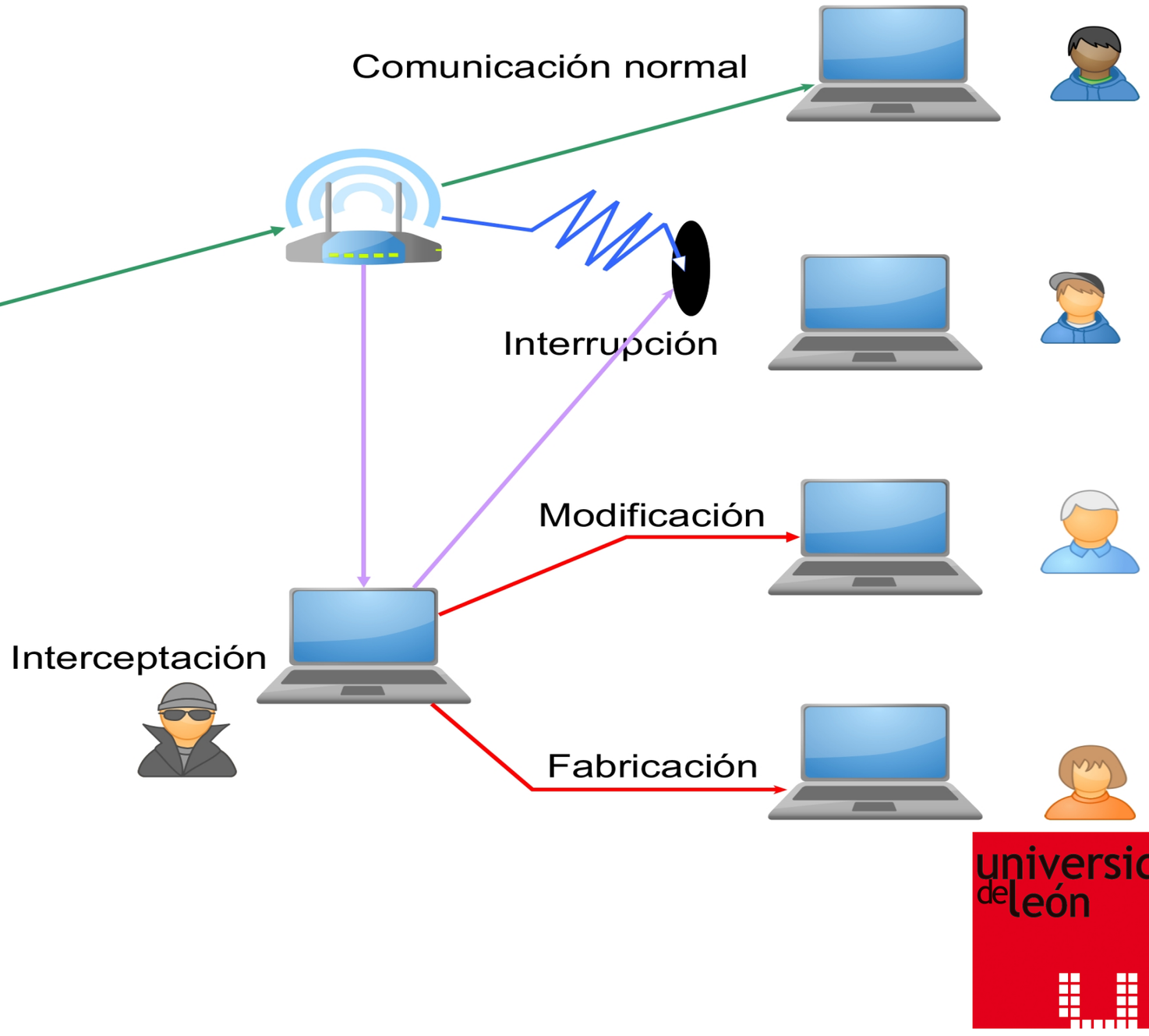
- Framework distribuido donde unos procesos (nodos) publican información (topics) que otros consumen



GRUPO DE ROBÓTICA

universidad de león

Seguridad en ROS



GRUPO DE **ROBÓTICA**

universidad de león

¿Que aporta ROS Ciphered?

- Topics cifrados con **AES** o **3DES** (**PyCrypto**)
- Cada mensaje tiene su propio IV que viaja junto al mensaje cifrado
- La cola de mensajes solamente tiene capacidad para 1 mensaje
- El nodo **publisher** cifra el mensaje junto a un número de secuencia
- El nodo **suscriber** descifra y comprueba la validez del número de secuencia

GRUPO DE **ROBÓTICA**

universidad de león

¿Trabajos futuros?

- Intercambio de clave segura
- Paquete startup que permita eligir que topic cifrar

GRUPO DE **ROBÓTICA**

universidad de león