7MR10070: Software and Robotic Integration

Semester 2

Assignment 3

Written by Alexandros Megalemos

# ROS slicer integration and robotic control

# Introduction

### Application Program Interface (API)

An API is an interface/toolset whose purpose is to provide developers/users with useful functionality in a simple manner. An API glues together / connects different pieces of software. A few examples of APIs are libraries such as numpy (for python), or more web-based APIs such as SOAP and REST.

One of the reasons to develop an API is so that other developers (or you), won’t have to develop the same piece of code again. By simply “encapsulating” a piece of software/algorithm within an API, you can then reuse it without having to know how it works, just that it works.

Another reason to develop an API is security. For example, a company could give users free access to their database (not recommended) but that could lead to many problems, such as security breaches and loss of data (either on purpose or by mistake). What they could do instead is develop an API with (for example) a function called *getAvailableProducts()* which will handle all security issues as well as ensure that the correct data is returned.

A final reason to develop an API is automation and integration. For example, a certain third-party website could use the APIs of various airline websites to alert a user that a flight they’re interested in has reached a certain price by a certain airline.

This leads to the next point which is that APIs should be treated as products and not as random collections of code to be forgotten.

Pros of an API:

* Automation – Allows computers to manage work instead of people
* Efficiency/Reusability – Developers do not have to develop the same functionality repeatedly
* Integration – Allows content from various parties to be connected into one
* Security – By allowing access only through the API, the provider makes sure that all necessary security measures are enforced (assuming they did a good job)

Cons of an API:

* Relying too much on an API could cause major issues. A publisher of an API could decide to change their implementation without warning, rendering your application useless
* Security – Trusting that you or the publisher of the API have/has taken all the necessary security precautions can be risky
* Loss of control – Once you have deployed an API, it is harder to make changes to it as you may mess up with other people’s applications

### Transfer Communication Protocol (TCP)

TCP is a transmission standard whose purpose is to connect different devices within network (which can be either private or public). It works with the Internet Protocol (IP) which defines how computers send data to each other. TCP is responsible for organising the data that is being transferred in a secure manner and it guarantees the integrity of the data.

TCP is connection-oriented which means that a connection needs to be established between the devices (server-client) before any data is sent. In order to establish this connection, a three-way handshake is used. The way this works is as follows:

1. A Source Machine sends an initial request by sending a message to a Destination Machine (SYN)
2. The Destination Machine acknowledges this request and agrees or disagrees to establish a connection by sending a message back (ACK)
3. The Source Machine acknowledges the Destination’s agreement, and establishes the connection (SYN-ACK)

TCP/IP works by breaking the message/data into smaller parts called packets, and then sending them one by one between the devices. Each packet carries information to help the devices identify which part of the message it is, from whom it was sent, when it was sent and so on. The TCP part is responsible for assembling the packets into the complete message once the transfer is finished. If for any reason a packet is missing, it is responsible for requesting it again.

TCP is important because it establishes a standard for how information is communicated over a network. This means that anyone using TCP knows the format in which the data will arrive, making it easier to interpret it.

Pros of TCP:

1. Reliability – Since it is a standard adopted by the whole industry, transferring data using TCP means that we can expect how the data is transferred.
2. Cross Platform – It works across different/heterogeneous networks
3. Open Protocol – No one owns TCP and therefore can be used by anyone
4. Scalable – Networks can be added without disruption to current services
5. Data integrity – TCP can detect if data is lost or damaged and can therefore be discarded and requested again

Cons of TCP:

1. Strict Protocol – It is not generic by design
2. Bad for small networks – It is designed to be used by wide networks
3. Vulnerable to Denial of Service attacks – Attackers can abuse the handshake process to send many requests to establish a connection with the server, thus overloading it and rendering it unable to establish legit connections
4. Vulnerable to Connection Hijacking – Eavesdroppers can redirect packets if they can learn the sequence number from an ongoing communication
5. It is not a network – TCP is just a protocol. It only describes how a connection should be established.

# Code / Git Repository

# Appendix