Detecting Robot Operations Using Statistical Traffic Analysis

Scott Gibb
Dr Shishir Nagaraja

University of Strathclyde Glasgow

Abstract

Teleoperated surgical robots enable surgeons to participate remotely in surgeries. We developed traffic analysis techniques to study network traffic between the surgeon's controller and the arm-robot itself. We studied a real-world robot called the uArm Swift Pro robot arm. We found that a passive attacker using our techniques might be able to identify some surgical procedures with 100% accuracy, without access to packet contents.

The Robot Patient Privacy Problem

Robot operations can leak sensitive information
- Captured operation data + patient information can violate patient privacy
- The threat model here is that an adversary (insider or otherwise) will passively analyse the network link (Fig. 1)

In order to prevent information leakage, we must first answer the following:
- How can the operations be detected?
- Can we detect the type of operation?
- How much information about the operation can be detected?

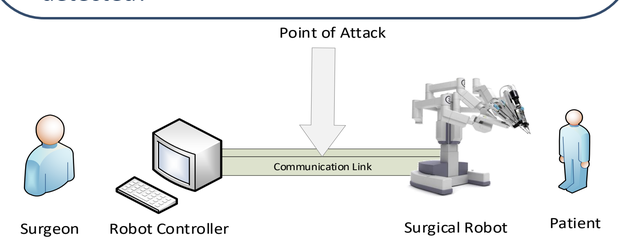

Figure 1: Robot Patient Privacy Threat Model[1]

Detecting Robot Operations

For robot operations (i.e. removing a circular growth), we:
- Used WireShark to capture data between controller and robot
- Observed **Packet Length** and **Packet Throughput**
- Analysed data using histograms, boxplots and time-series

These complex operations were mimicked by simpler operations such as drawing a circle and rectangle.

Figure 2: Circle S100 Packet Length Box Plot Histogram(10 Runs)

Figure 3: Rectangle S200-100 Packet Length Box Plot Histogram(10 Runs)

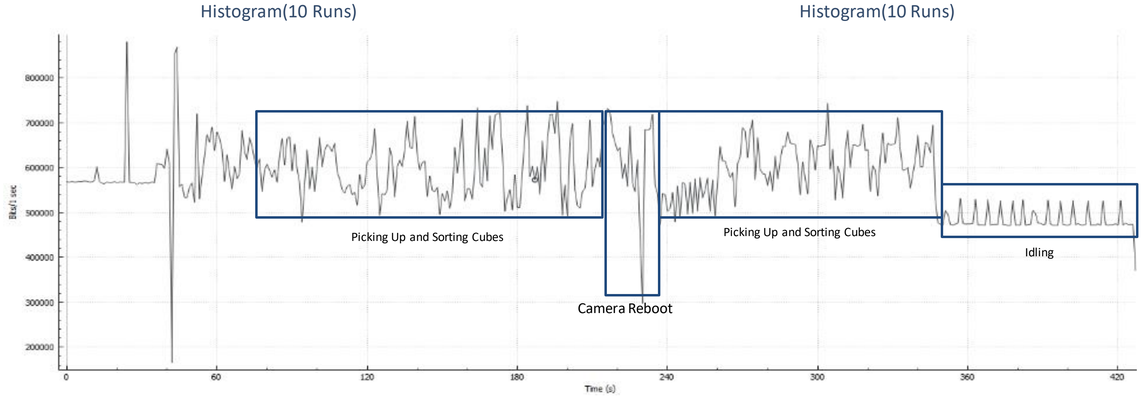

Figure 4: Sorting Colours Network Packet Throughput Diagram

References: [1] - https://pixfeeds.com/images/technology/artificial-intelligence/1280-527676755-surgical-robot.jpg

Evaluation

Analysing just the **packet lengths** of the captured data, we were able to predict what operation the robot was carrying out (Fig. 2 and 3)
- For growths, the volume of packets associated with certain packet lengths are somewhat constant and show a particular histogram throughout the process.
- For selecting a rectangular region, a different pattern emerged with the packet length histogram.

Results:
The degree in difficulty in comparing the motions was monitored, it was found that certain shapes were harder to distinguish than others. (Table 1)

Table 1: Distinguishing Different Robot Motions Comparison Table

Motion Comparison		Difficulty in Distinguishing	Packet Length Box Plot Histogram	
Motion A	Motion B		Motion A	Motion B
Square	Circle	Moderate	Fig. 7	Fig. 5
	Rectangle	Easy		Fig. 6
	Triangle	Moderate	Fig. 8	Fig. 8
Circle	Rectangle		Fig. 5	Fig. 6
	Triangle			Fig. 8
Rectangle		Easy	Fig. 8	

Analysing the **traffic throughput** allowed us to find when the robot was operating (Fig. 4).
- Spike patterns correlate to robot activity (i.e. idle status, operation and camera)

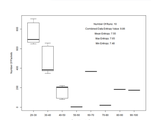

Figure 5: Circle S50 Packet Length Box Plot Histogram(10 Runs)

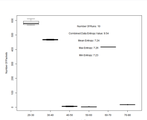

Figure 6: Rectangle S100-50 Packet Length Box Plot Histogram(10 Runs)

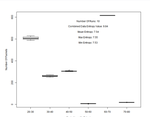

Figure 7: Square S100 Packet Length Box Plot Histogram(10 Runs)

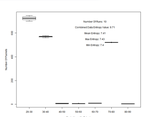

Figure 8: Triangle S100 Packet Length Box Plot Histogram(10 Runs)

Future Work

- Make operations more realistic by adding complexity (i.e. rotations to estimate roundness of bones)
- Use **TLS/SSL** between controller and robot for security of the network link
- Integrate **Tor** to provide some level of anonymity of the controller and the robot
- Incorporate a **Mixed Router** into the network, thus making the network traffic unidentifiable