KIOS
Research and Innovation Center of Excellence

Machine Learning in Wireless Communications

Markos Loizou

Supervisor: Prof. Ioannis Krikidis

University of Cyprus

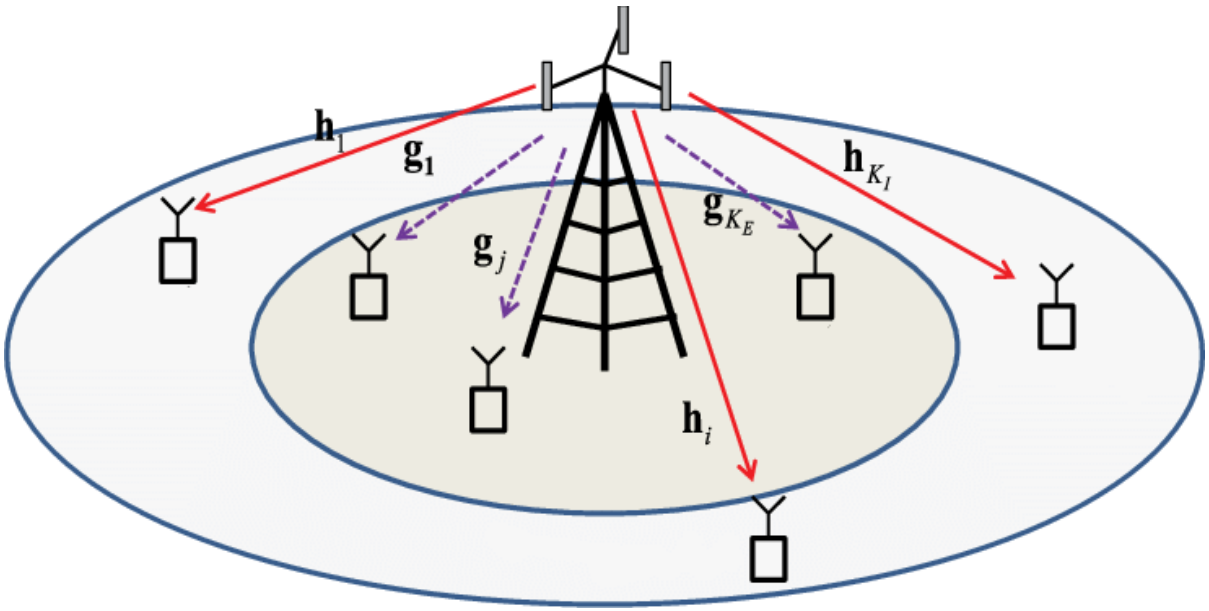
Imperial College London

Funded by:

Case Study 1 - Physical Layer Security

Motivation

- Broadcasting in wireless communications makes it susceptible to eavesdropping.



Case Study 1 - Physical Layer Security

Motivation

- Broadcasting in wireless communications makes it susceptible to eavesdropping.
- Key distribution in dynamic networks used in symmetric crypto-systems.
- High computational complexity of asymmetric crypto-systems.

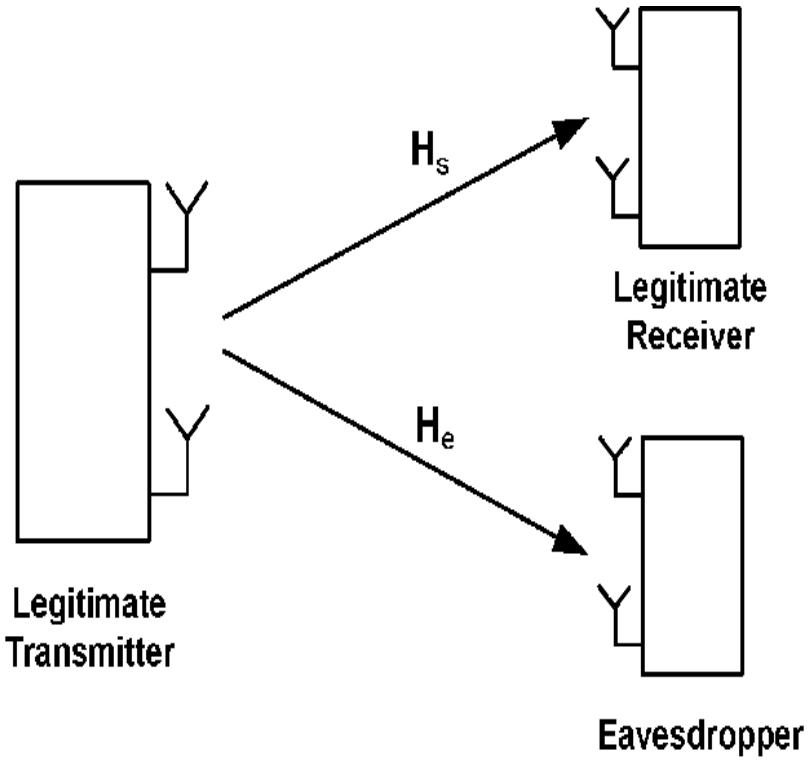
Case Study 1 - Physical Layer Security

Information Theoretic Secrecy

- The secrecy rate, C_s, is the maximum rate which can be transmitted over a communications channel with guaranteed secrecy.

$$C_s = \left[C^U - C^E\right]^+ \qquad (1)$$

- The channel rate of each user is determined by the channel randomness.



Case Study 1 - Physical Layer Security

MIMO Systems

- MIMO is a technique used to exploit or combat multipath scattering environments.
- Exploiting them allows for increased throughput.
- Combating them improves the reliability of communications by exploiting spatial diversity.

Case Study 1 - Physical Layer Security

MIMO Systems

- The increased number of antennas also increases their complexity.
- By choosing a single antenna, or any subset, we can decrease the complexity.
- Antenna Selection can also be used as a way to increase the security of the system.

Case Study 1 - Physical Layer Security

Antenna Selection Techniques

By choosing a single antenna, i, the user receives,

$$y^U = H_i^U x + n^U \tag{2}$$

and their channel rate (when using MRC) is given by

$$R_i = \log_2 \left(1 + \sum_{j=1}^{N_U} \frac{P \left| h_{ij}^U \right|^2}{\sigma_U^2} \right). \tag{3}$$

- If only the channel state information, H, of the user is known we can chose the antenna that maximizes R_i in hope of also maximizing C_s (SAS).
- Another approach is to maximize the smallest singular value of the reduced matrix when selecting a subset of antennas to transmit (MaxMinSV).

Case Study 1 - Physical Layer Security

Antenna Selection Techniques

In the case where the eavesdropper is a member of the network and his channel state information is also known, the secrecy rate can be directly maximized by choosing antenna a, such that,

$$a = \arg\max_i R_s = \left[R_i^U - R_i^E\right]^+ \tag{4}$$

$$= \arg\max_i \frac{1 + \sum_{j=1}^{N_U} \frac{P\left|h_{ij}^U\right|^2}{\sigma_U^2}}{1 + \sum_{j=1}^{N_E} \frac{P\left|h_{ij}^E\right|^2}{\sigma_E^2}} \tag{5}$$

This will be referred to as Optimal Antenna selection (OAS).

Case Study 1 - Physical Layer Security

Computational Complexity

Selection Method	Complexity
MaxMinSV	$\mathcal{O}(2^{N_t}(N_r N_t^2 + \log(2^{N_t}))$
MaxMinNorm	$\mathcal{O}(\binom{N_t}{N_s}(N_t N_r + \log(\binom{N_t}{N_s})) + N_t N_r)$
OAS	$\mathcal{O}(N_t N_r)$
SAS	$\mathcal{O}(N_t N_r)$

- In terms of BER the best Antenna Selection scheme is MaxMinSV which however has a large complexity.

Case Study 1 - Physical Layer Security

Machine Learning Algorithms

- K-Nearest Neighbors (KNN)
  - Memory-based with no model to fit
  - Classifies each point by majority among the k neighbors
- Support Vector Machines (SVM)
  - Find hyper-planes that give the maximum class separation
  - Only a *small* subset of the training data is required for classifying new inputs
- Multi-Layer Perception Classifier (MLPC)
  - Neural network trained using Adam's Stochastic Optimizer.
  - Significantly faster training on large data-sets

Case Study 1 - Physical Layer Security

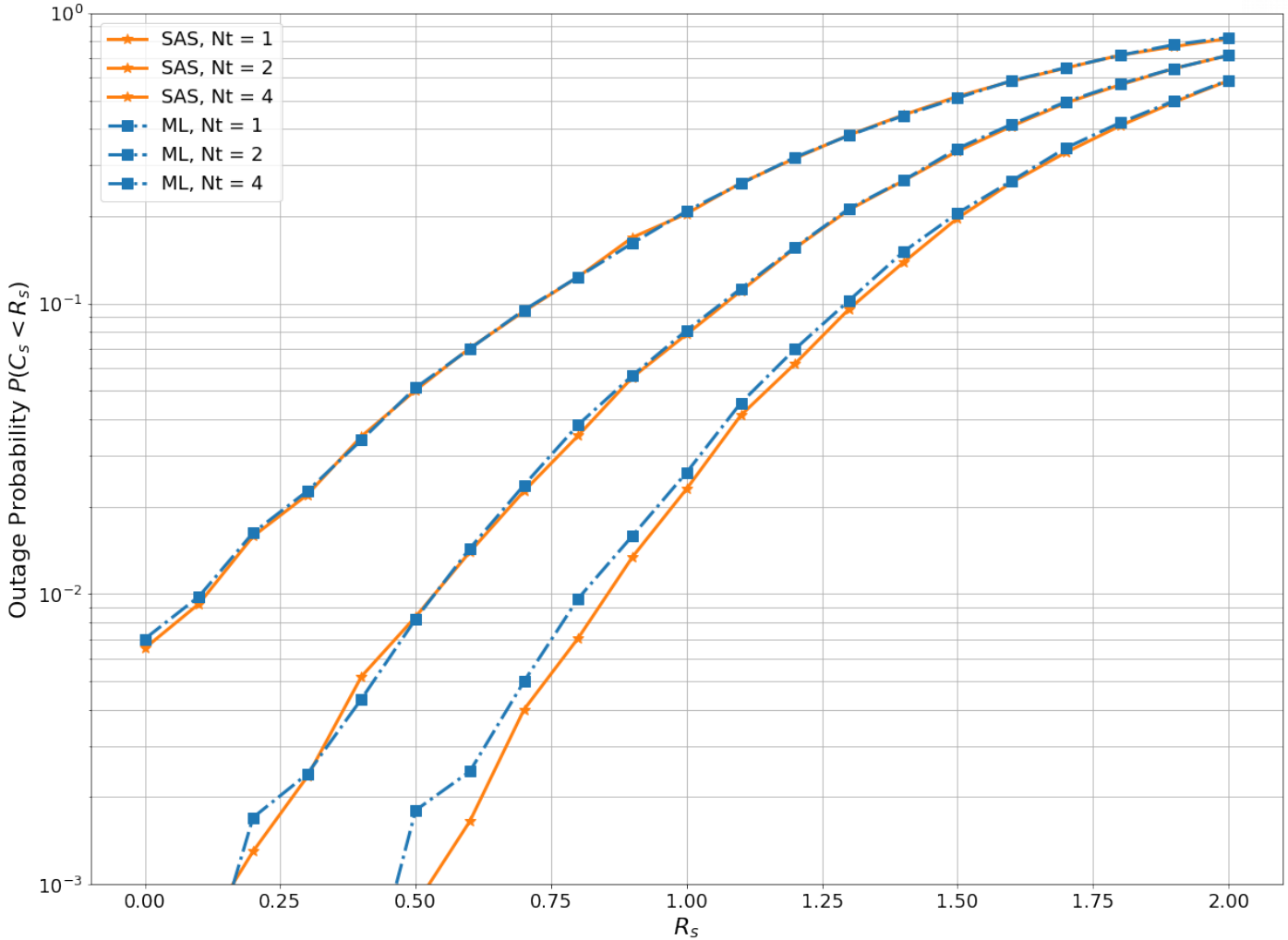
Machine Learning Computational Complexity

Prediction Method	Complexity
KNN	$\mathcal{O}(N_t N_r)$
SVM	$\mathcal{O}(N_t^2 N_r^2)$
MLPC	$\mathcal{O}(N_t^2 N_r^2)$

- All the Machine Learning algorithms have a lower computational complexity for prediction than MaxMinNorm and MaxMinEV

Case Study 1 - Physical Layer Security

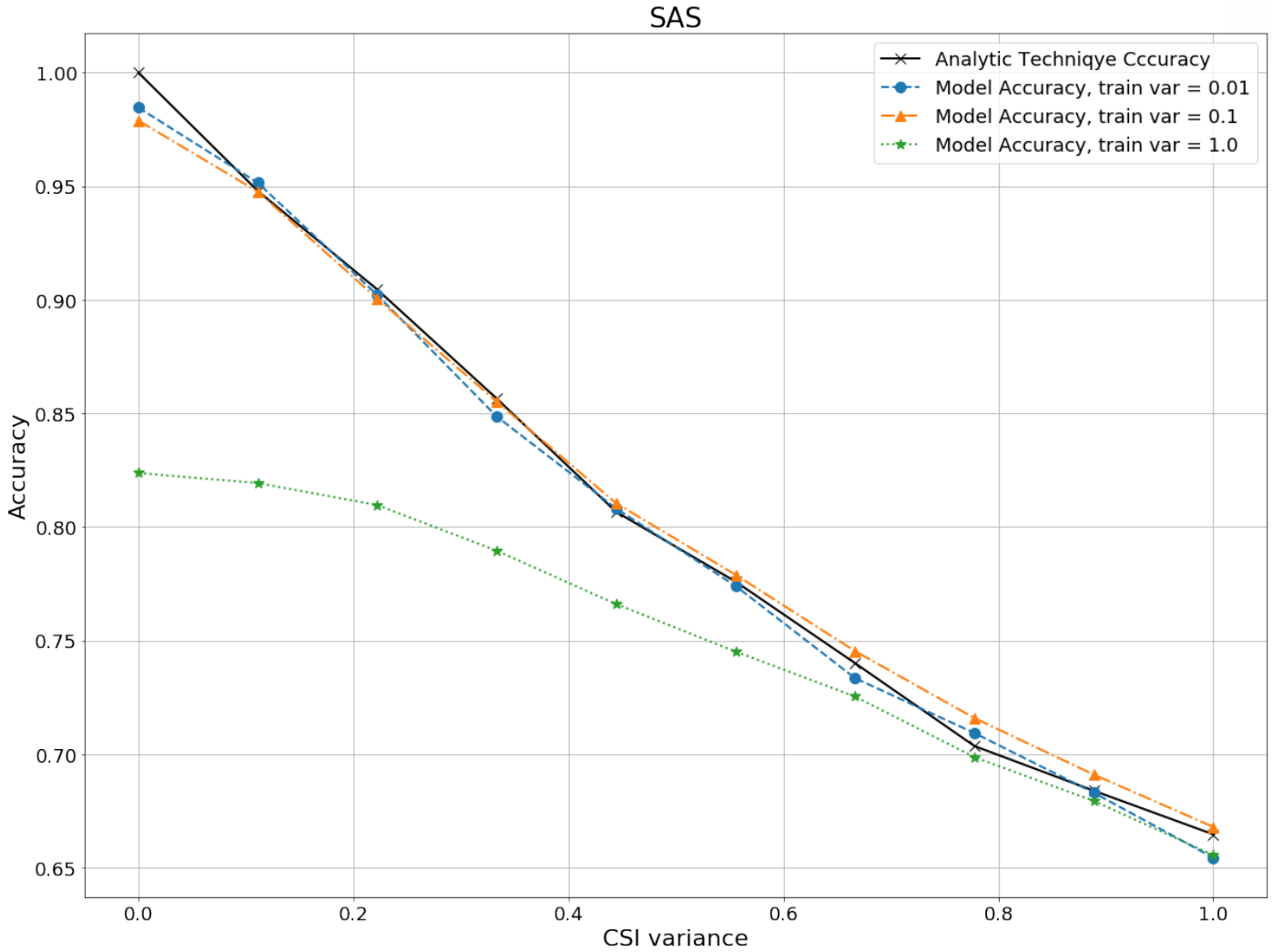
Results - Probability of Outage Comparison



- The machine learning algorithms perform as well as the analytic techniques (Nr = 10 for this example).

Case Study 1 - Physical Layer Security

Results - Imperfect CSI Antenna Selection



- Machine learning algorithms are as robust to noise as the traditional techniques.

Case Study 2 - RF for Detection

- Traditionally Radio Frequency waves have only been used for transmitting information.
- More recently, RF waves have also been investigated to transmit power for energy harvesting devices.
- A new application of RF is for detection and classification of objects and events.
- The received signal carries information about the channel (environment) the waves propagated through. This information can be used for detection.

Case Study 2 - RF for Detection

- Traditionally Radio Frequency waves have only been used for transmitting information.
- More recently, RF waves have also been investigated to transmit power for energy harvesting devices.
- A new application of RF is for detection and classification of objects and events.
- The received signal carries information about the channel (environment) the waves propagated through. This information can be used for detection.

A recent paper used two WiFi modules connected on two laptops to identify with high accuracy the quality of wheat. Traditional techniques require expensive equipment, trained personnel while having similar accuracy.

Related work has also been done on WiFire and WiMetal, where RF waves were used to detect fire events and metal object respectively.

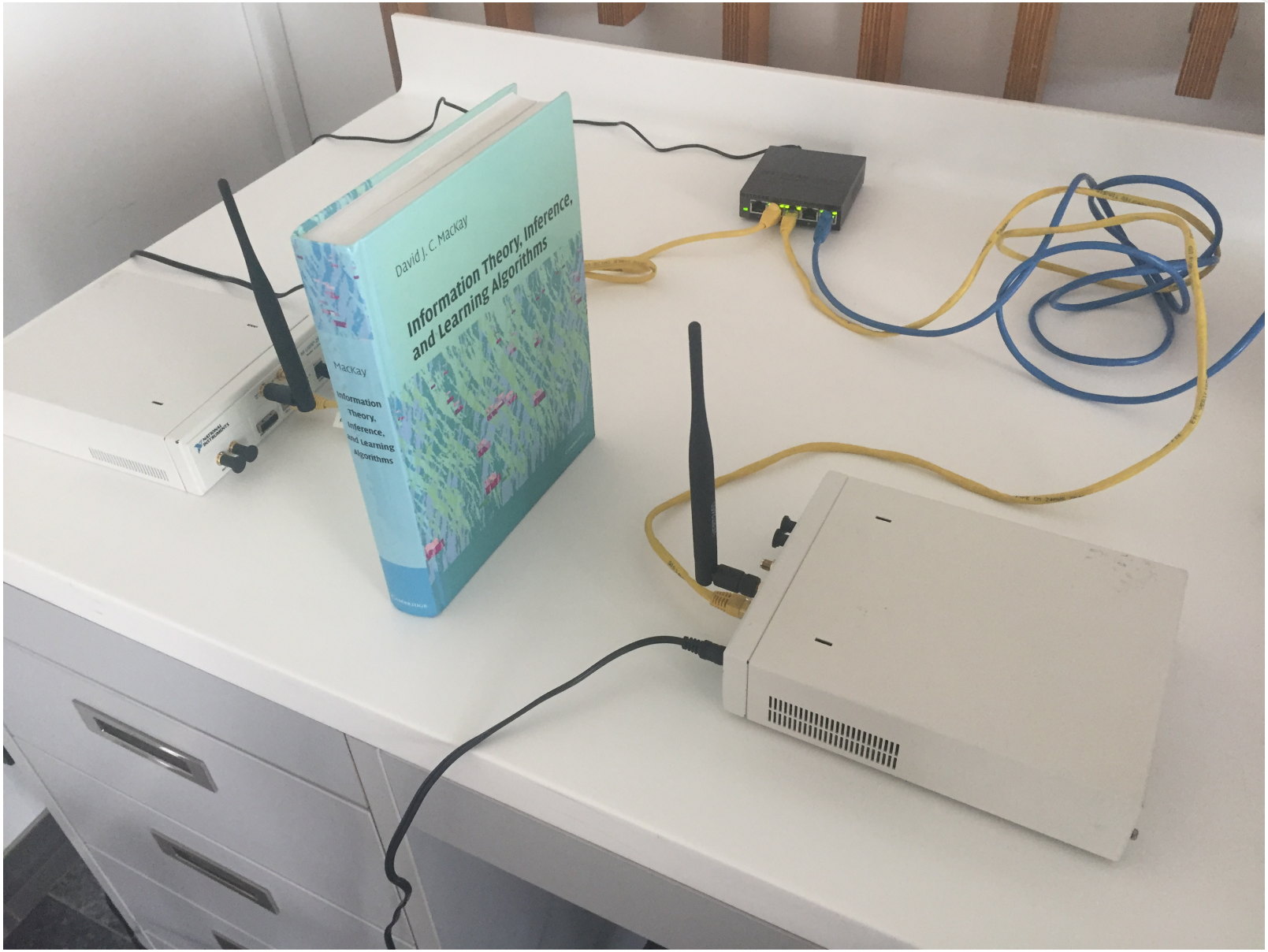
Case Study 2 - RF for Detection

Method

- A USRP was used to transmit a sine wave.
- An object was placed between the transmitter and the receiver (at 3 locations).
- The receiver recorded the amplitude and phase of the received signal.
- The received signal was used to classify the two objects.
- The two objects used were glasses(glass, plastic and metal) and planar objects (mirror, plastic, metallic, wooden).
- We then classified the objects into glasses and planar objects.

Case Study 2 - RF for Detection

Setup



Case Study 2 - RF for Detection

Data Preparation and Training

- The start and end of the signal were discarded since no signal was transmitted at those times.
- Each measurement(12000 sample points) was broken into smaller ones, each one containing about 1 period of the wave(200 sample points)
- Complex data was transformed into magnitude and phase.
- The data was then normalized to lie in $[0, 1]$.
- The data was then labeled with class 0 for glasses and 1 for the planar objects.
- The same supervised learning algorithms as before were trained using part of the labeled dataset.
- The most promising model was then tested on the remaining dataset.

Case Study 2 - RF for Detection

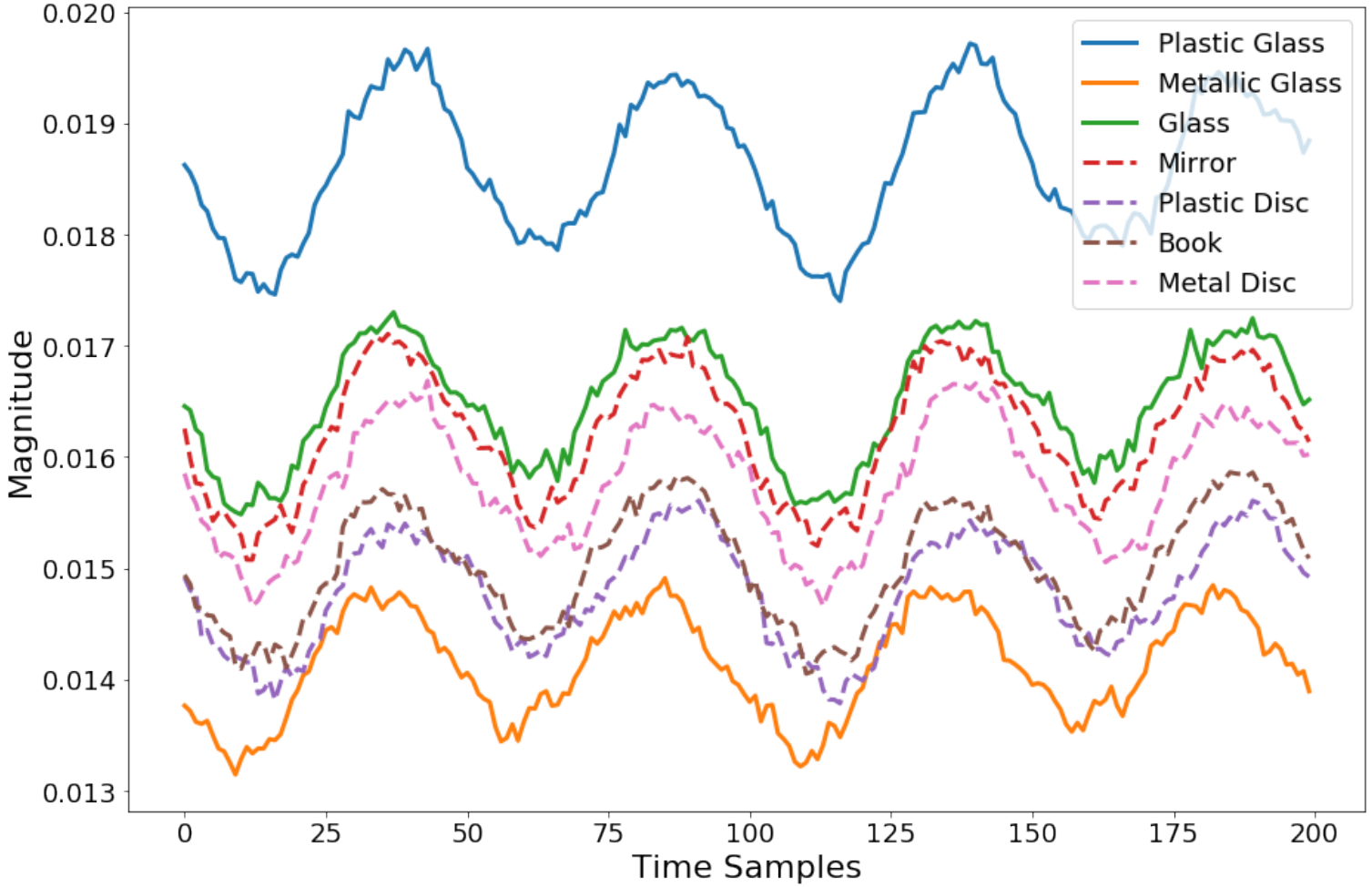
Results

- *The MLPC achieved 95% accuracy*

Case Study 2 - RF for Detection

Results

- *The MLPC achieved 95% accuracy*



Further Work

- Use Reinforcement Learning for antenna selection.
- Use Reinforcement Learning for jamming as well as selecting the transmit antenna.
- Classify materials as well as objects.
- Make the predictions in real time.

Conclusions

- Machine Learning can be useful in Wireless Communications for:
  - Lowering computational complexity.
  - Tackling problems with no known solutions.
  - Tackling problems with no models.

Thank You!