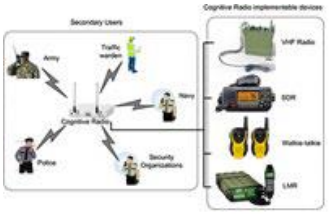
M.Sc. internship projects CWI Stochastics Group

Automatic Signal Recognition with Artificial Intelligence





Supervisors: Arwin Gansekoele M.Sc. and Prof. dr. Rob van der Mei
Key words: Wireless spectrum, modulation techniques, generative deep learning models
Location: CWI, Science Park 123, Amsterdam
Timeframe: Fall 2022 / Spring 2023

Background and problem
The development of new mobile technologies (5G) and the increased number and diversity of internet of things (IoT) devices are just some examples of recent improvements in wireless technologies. The increasing number of connections and sophistication of technologies puts a strain on the wireless spectrum, however. How to handle devices interfering with each other is a constant struggle. In an ideal world, IoT devices would be able to communicate with one another automatically and determine when which parts of the spectrum are available; the cognitive radio.
Radio signals are commonly processed by analog devices, which are very cost-effective at their specific task but not necessarily flexible. An alternative is to use a software-defined radio (SDR), which means that parts of the signal processing are performed using a computer running some software instead. Fueled by recent developments in Artificial Intelligence (AI) and, more specifically, Deep Learning (DL), research into SDR software has increased drastically. The automatic pattern recognition component alongside improved hardware has opened up a whole new avenue of research into achieving the so-called cognitive radio. Some questions are:
1. Can we automatically sense which parts of the spectrum are in use?
2. Can we automatically detect which modulation technique is being used?
3. Can we de-modulate signals using a generative deep learning model?

What we look for
We are looking for a motivated M.Sc. student to work on a research question important in the journey to achieve cognitive radio. The student is otherwise free to choose which topic to investigate as long as it fits within the intersection of math/optimization/AI and cognitive radio. In an ideal scenario, the results of the project are suitable for scientific publication.
More specifically, we look for highly motivated master students, who:
1. take initiative and are driven, inquisitive and independent.
2. are proficient in their topic of choice (e.g. an AI student should have an affinity with Deep Learning); experience in signal processing is a plus.
3. have an average grade of at least 8.0.

Data Stealing and Federated Learning

Supervisors: Arwin Gansekoele M.Sc. and Prof. dr. Rob van der Mei
Key words: federated learning, data/model stealing, sensitive data
Location: CWI, Science Park 123, Amsterdam
Timeframe: Fall 2022 / Spring 2023

Background and problem
Recent years has seen a massive increase in both the amount of data and number of methods that operate on data. The majority of data is private, however, and the consequence of data leaks can range anywhere from being a minor nuisance to being catastrophic for a company or institute. Nevertheless, being able to train using personal data from various sources is ideal in many cases, a notable example being patient data from multiple hospitals. Methods to enable model training from various sources fall under the topic of federated learning.
On the other hand, assuming that everyone working with trained machine learning models is upright is a bit of a stretch. If it is possible to reverse engineer a model from an API, or even the data used to train that model, then we have a whole new dimension of data leakage to deal with. Carlini et al. [1] show that big language models, for example, memorize data to such an extent that they could extract a credit card number out of a trained model.
This project works on the intersection of federated learning and, for example, data stealing. The core question we are trying to answer is to what extent a user in a (perhaps primitive) federated learning scheme can extract potentially sensitive data other users have included in the model. Any kind of model stealing or federated learning topic is within the scope of this project, however.

What we look for
We are looking for a motivated MSc student to work on a research on federated learning and data stealing. The student is otherwise free to choose which topic to investigate as long as it fits within the scope of the project. In an ideal scenario, the results of the project are suitable for scientific publication.
More specifically, we look for highly motivated master students, who:
1. take initiative and are be driven, inquisitive and independent.
2. are proficient in their topic of choice (e.g. an AI student should have an affinity with Deep Learning).
3. have an average grade of at least 8.0.

What we offer our interns:
1. Daily supervision from a Ph.D. student working on the same topic along with access to multiple experts on the topic.
2. An internship position at the CWI, the Dutch research institute for mathematics and computer science.
3. A standard monthly fee for Master internships.
4. A fun and engaging environment with M.Sc. and Ph.D. students that undertake regular activities such as weekly drinks.

About Centrum Wiskunde & Informatica
The CWI, founded in 1946, is an internationally leading research institute in Mathematics and Computer Science. CWI is very active a range of research areas, including stochastic modeling, optimization,

quantum computing, cryptology, database management systems and artificial intelligence. CWI employs some 250 researchers, including M.Sc. and Ph.D. students, postdocs and professors. See the website www.cwi.nl for more details.

Contact: If you are interested, please send a message and your CV to Prof. Rob van der Mei (mei@cwi.nl) or Arwin Gansekoele (Arwin.Gansekoele@cwi.nl). If you have any questions, please send them as well.