Inception Report – 18/11/2019

## Aims & background material (student)

The project aims to research into the field of wireless Federated Learning (FL). We can define wireless FL as privacy-preserving Machine Learning performed over a wireless communication channel.

The definition points towards the different subtopics of wireless FL: Machine Learning, Distributed Algorithms, Communications, Information Theory, Security and Privacy.

My personal aim for this first phase of the project is to:

1. Research into how the topics listed above combine together into wireless FL
2. Research on the current state-of-the-art wireless FL
3. Understand the challenges that each subtopic poses to wireless FL
4. Decide, together with my supervisor Dr Gunduz and his research group (IPC), the main focus of my subsequent work
5. Familiarize with the existing codebase on wireless FL created by the IPC research group

I have already got in contact with Dr Gunduz and the IPC group to get support and pointers in this first research phase.

## Student Summary of project deliverables, fallbacks & extensions (student)

My main intuition and interest about this research topic are to create a modular software simulator that can recreate a wireless FL system. The behaviour of all the different parts of the system (i.e. base station, clients, communication channel, model to be trained and dataset to use) should be fully configurable and the performance metric analysed would be training time (for the model to converge to a certain threshold)

The simulator will have for each component an abstract base class which will be then overridden by the different class implementations related to different behaviours and protocols.

The software architecture of the simulator, the exact list of deliverables that I intend to submit, and their associated fallbacks and extensions, will be one of the outcomes that I aim to generate from the initial background research that I am conducting at the moment.

If the time allows it, it would be interesting to do a real-world experiment of a simple wireless FL system on devices such as mobile phones and/or IoT microcontrollers (e.g. Raspberry PI) to test how the theoretical results apply in a real scenario.

## Summary of Risks (student)

The main risk that I can foresee at this stage is to set an overwhelming deliverables plan in terms of time available considering the workload of the modules that I have chosen.

This risk can be mitigated by carefully designing the deliverables plan after an attentive research phase.