Projektvalskatalog

EF112X kandidatexamensarbete inom elektroteknik (15 hp) våren 2024

I denna katalog kan du hitta information om alla valbara projekt inom kursen EF112X kandidat-examensarbete inom elektroteknik (15 hp) som erbjuds våren 2024 vid EECS skolan, KTH. Kursen EF112X pågår hela vårterminen från mitten av januari till slutet av maj. Projekten utförs i grupper om två. I år finns 63 projekt att välja emellan inom ramen av 15 olika kontext.

Kontext inom systemteknik och robotik

- Kontext A: The Dynamics of a sustainable society (*Jonas Mårtensson)*
- Kontext B: Learning in Dynamical Systems (*Cristian Rojas*)

Kontext inom inbyggda system och elkraftteknik

- Kontext C: Electric transportation (*Mats Leksell*)
- Kontext D: Kraftsystemstyrning (*Mehrdad Ghandhari*)
- Kontext E:Hydro power as a balancing resource in the power system (*Mikael Amelin)*
- Kontext F: Predicting the future sustainable power system (*Lars Nordström*)

Kontext inom elektromagnetism, fusion och rymdteknik

- Kontext G: Design and testing of novel microwave/antenna technologies (*Oscar Q.-Teruel*)
- Kontext H: Fusion - solens energikälla på jorden (*Thomas Jonsson*)
- Kontext I: Planetary magnetospheres and aurora (*Tomas Karlsson*)
- Kontext J: Fixed wing UAV for space and environment monitoring (*Nickolay Ivchenko*)

Kontext inom information och nätverksteknik

- Kontext K: Artificial Intelligence for the Internet of Things (*Carlo Fischione*)
- Kontext L: Cyber Security (*Rolf Stadler*)
- Kontext M: Information Engineering: Big Data & AI (*Tobias Oechtering*)

Kontext inom datavetenskap och maskininlärning

- Kontext N: AI, games, and strategy (*Mika Cohen*)
- Kontext O: Computational brain modelling and brain-like computing (*Pawel Herman)*

Viktiga datum

- **Informationsmöte om projektvalet:** Torsdag, 12 okt 2023, kl 9:15-12:00, sal L1
- **Projektval:** 1-15 nov 2023
- **Kursstart:** vecka 3, 2024 (uppstart-möte, i anslutning första träff med handledaren)
- **Kursslut:** vecka 20, 2024 (heldag KEX-presentation)

Kurs-PM

All information om kursens uppbyggnad finns i kurs-PM. En preliminär version kommer att läggas ut senast den 2 november 2023 på kurshemsidan i KTH social: www.kth.se/social/course/EF112X/

Tillgängliga projekt 2024

Alla projekt som erbjuds vårterminen 2024 finns beskrivna i denna pdf-fil. Läs igenom projektbeskrivningarna noggrant. I valet markerar du vilka projekt du helst vill göra. Obs, inom ramen av denna kurs kan man inte "skräddarsy" sitt eget projekt. Du måste välja ett av de tillgängliga projekten som finns beskrivna i denna katalog.

Behörighet

Minst 104 högskolepoäng från kurser i utbildningsplanen, till och med period 1 i årskurs 3, ska vara avklarade senast vid startdatum för period 2 för att studenten ska få påbörja kandidat-examensarbetet.

Anmälan till KEX-kursen

Elektroteknikstudenter: Om du går i årskurs tre (CELTE-3) och ligger i fas med studierna, ska du välja villkorligt valfria, och/eller den helt valfria kursen, och kandidatexjobbskursen EF112X mellan 1-15 november via antagning.se. Logga in med ditt kth.se konto.

Om du antogs till Elektroteknik 300 hp år 2018 eller tidigare sker anmälan till kandidatexjobbskursen EF112X via e-post till svl-celte@kth.se mellan 1-15 november.

Om du är från en annan KTH skola (fysik, farkost, teknisk matematik eller energi och miljö programmet), anmäler du att du vill göra kandidatexjobbskursen EF112X till studievägledaren vid respektive KTH skola.

Val av projekt

Förutom att anmäla dig till kandidatexjobbskursen behöver du (oberoende från vilken skola du kommer) välja på internet själva kandidatexjobbsprojektet du vill jobba med.

När sker valet?
Valet av kandidatexjobbprojekten görs under perioden 1-15 november 2023. Resultatet påverkas ej av när du väljer under valperioden.

Projektgruppen
Kandidatexjobbsprojektet utförs i grupper om två studenter. Om du inte lyckas hitta en projektpartner, tilldelas du en partner med liknande projektönskemål som du.

Gör ditt val
Anmälan görs på kurshemsidan i KTH social (www.kth.se/social/course/EF112X/). Välj de sju mest intressanta projekten ur denna projektvalskatalog. Du kommer kunna ange din prioriteringsordning när du väljer (prio 1= projektet du helst vill ha). Om du redan har hittat en projektpartner, fyll i bådas namn, e-mail och program i samma anmälan. Gör endast **en** anmälan per grupp. Om du inte har en projektpartner än, anmäl dig ensam (du kommer sedan tilldelas en projektpartner).

Lycka till!

Anita Kullen (kullen@kth.se)
Kursledare för kandidatexjobbskursen EF112X
Stockholm, 1 oktober 2023

Context A: The Dynamics of a Sustainable Society

Context Responsible: Jonas Mårtensson, jonas1@kth.se, Matthieu Bareau, barreau@kth.se
Division: Decision and Control Systems

"*Meeting the needs of the present without compromising the ability of future generations to meet their own needs.*"

This is the well-known sustainability definition by the United Nations Brundtland Commission in 1987. Sustainable development is then taking into consideration environmental concerns along with economic development and social aspects. The 17 Sustainable Development Goals is a framework for improving the lives of populations around the world and mitigating the hazardous man-made effects.

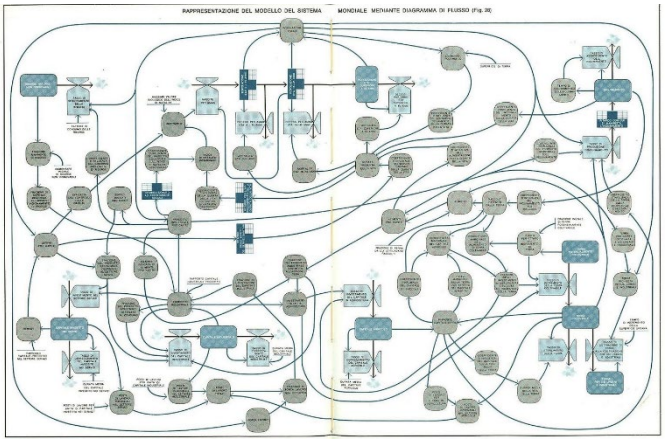
But how is this done? We are dealing with an extremely complex and complicated problem that involves the law of nature, global politics and economics, cultures, human behavior, and technical solutions, to name just a few of the aspects. And we need to deal with long time scales and complex interplay between different domains. In these projects we will approach this problem by dynamical systems modelling.

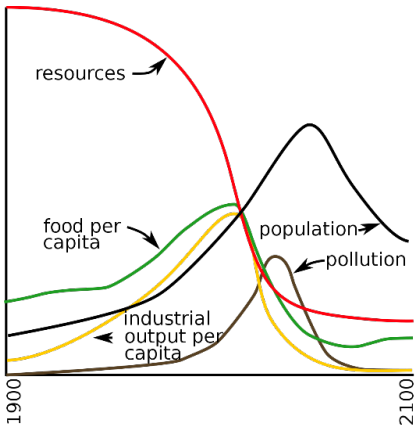
The World3 model, featured prominently in the groundbreaking 1972 book "The Limits to Growth," was a pioneering computer-based system dynamics model that aimed to shed light on the complex interactions between population growth, resource depletion, industrialization, and environmental impacts. The central message of the model was that if left unchecked, human activities such as rapid population growth and excessive resource consumption would eventually lead to ecological and societal challenges.

It generated heated debates and criticism, particularly regarding the assumptions made, predictions capabilities, and policy implications. While the model had its limitations, it played a pivotal role in raising awareness about the challenges of sustainable development and the importance of considering the finite nature of Earth's resources in shaping our future. The ongoing debates surrounding the model continue to shape discussions on environmental and economic policy.

Projects A1 – A3: Modeling the world

This context has three projects. The aim of these three projects is to analyze and experiment with the World3 model. The focus of each project is different but there is a common ground. There will be three independent projects A1 – A3, but you will interact between the groups in multiple workshops, where you will share knowledge and identify connections between the methods.





The World3 model is a dynamic model with interconnected subsystems describing: 1) food production and agriculture, 2) industrial production, 3) human population, 4) non-renewable resources, and 5) pollution. A typical simulation of the model is shown to the right. The initial step will be common for all projects. The students will first make use of a web graphical interface of the World3 model (The World3 Model: Classic World Simulation | Insight Maker), to understand its structure and build some intuitive understanding. In the later phase you will use and modify a Python implementation of the model (GitHub - cvanwynsberghe/pyworld3: The World3 model revisited in Python).

Project A1: Modeling the world – Exploring possible futures with systems thinking

Supervisors: Jonas Mårtensson, jonas1@kth.se, Matthieu Barreau, barreau@kth.se, Division of Decision and Control Systems

In this project you will work with the World3 model to explore possible futures of our world. You will work with one or several submodels of World3. The model contains many variables that are dynamically interconnected in reinforcing and stabilizing loops. You will use systems thinking and control/systems theory to analyze it and to propose and evaluate aspects with an implication on sustainability.

1. Analyze the causal loop diagram to understand its structure. Find the main relations between the variables of the model. Identify important loops. Define the variables and the external inputs.
2. Use a mix of simulation and analysis to understand the behavior of the model. Use sensitivity analysis to identify variables and inputs of importance. Identify important delays and inertia that affect the dynamic response of the model.
3. Based on your systems understanding, explore different possible futures, for example new policies, changed behaviour, technology development, or other important factors. Use simulation and analysis to explain the effects. Experiment with the model and modify it, if necessary, for example by changing parameters or introducing/removing links.

Project A2: Modeling the world – Model identification using physics-informed learning

Supervisors: Jonas Mårtensson, jonas1@kth.se, Matthieu Barreau, barreau@kth.se, Division of Decision and Control Systems

The dynamics of one sector is very complex and not written in a form suitable for control. The tool you will use is Physics Informed Learning.

1. You will first assume no knowledge on the original system and try to find a nonlinear dynamical model using a neural network. You will need to collect data and train the model.
2. The second step is to try to simplify the neural network from the previous part. You can investigate the dimension of the original system but also try to simplify the model by identifying key signals.
3. You will go deeper into the identification by considering submodels and repeting the first step with this new system design.
4. From your understanding of the different variables, you will try to find which ones are measurable. The final identified model should be interpretable and has a physical sense. This model should help you to highlight the most important features and the policies with the most impact.

Project A3: Modeling the world – Optimal policies with reinforcement learning

Supervisors: Jonas Mårtensson, jonas1@kth.se, Matthieu Barreau, barreau@kth.se, Division of Decision and Control Systems

Reinforcement Learning (RL) is a well-known machine learning technique often used to find an optimal policy for controlling a dynamic system in order to maximize a reward cumulated over time. At each time step, the agent takes an action, influencing the system's evolution over time. The agent then observes the updated states and receives a reward based on the transition. RL is often used in uncertain environments where the dynamics of the system need to be learned while interacting with the system itself. Over time, the agent gathers more information, enhancing its understanding of the system dynamics for more informed decisions. RL is used for many applications such as robotics, automation, video games, finance and recommendation systems.

In this thesis, we propose the application of RL techniques to a subsystem of the World3 model, a well-known system dynamics model used for studying global sustainability. Using RL the students should try to derive the optimal control policy with respect to a given cost. Constraints on the measurements (availability of the measure, sampling…) and the control inputs (delayed inputs, quantization…) can be considered. More precisely, the aim is to optimize resource allocation and policy decisions within the selected subsystem, with the overarching goal of contributing to a specific UN sustainability goal. The World3 model provides a comprehensive framework for simulating interactions between population, resources and the environment, making it a good testbed for the students' RL experiments.

This thesis will require a thorough understanding of the structure and dynamics of at least one of the World3 model's subsystems.

1. Identify relevant state variables, actions and their interdependencies.
2. Formulate a reward function that can well quantify the desired system behaviour linked to a specific UN sustainability goal.
3. Train and evaluate the RL agent using appropriate algorithms, in order to derive an optimal control policy.
4. Assess the performance of the obtained control policy with simulation experiments and compare against a baseline approach.

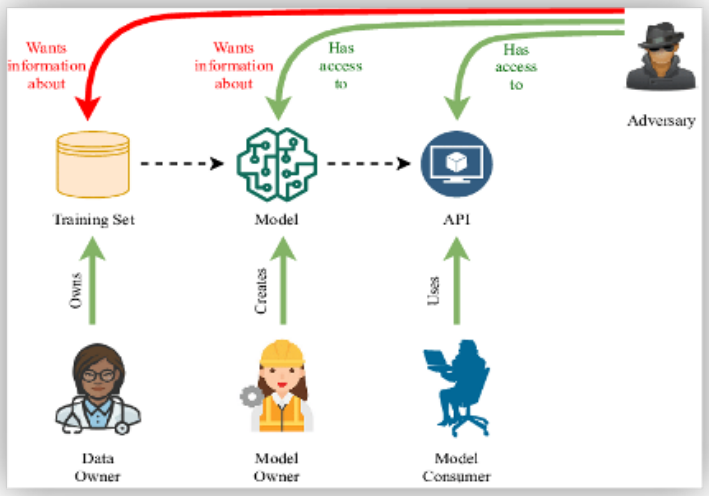
Context B: Learning in Dynamical Systems

Powerful computers, new sensors and high efficiency communication technology have opened the door to the design of technological systems that can learn by themselves. You have probably seen for example how Google's self-taught AlphaGo defeated in 2016 the world champion of Go. The advantage of self-learning systems is that they can adjust themselves according to the behavior they observe from their environments. The development towards such self-learning systems is happening on many fronts, including factories, smart buildings and autonomous vehicles among others. In most of these applications, physical systems or humans interact with a computer system, and the computer is based on a mathematical model of their environment. A complicating factor is that physical bodies and humans have dynamics, that is, their behaviors depend on what has happened before.

In this theme, the projects offered are meant to explore several aspects of the problem of learning dynamical systems. For example, how is it possible to learn from observed data the collective behavior of a large number of independent agents? what have self-learning systems actually learned from their interaction with the world around them? how can one implement efficient self-learning systems, either as single entities or as collaborative autonomous robots learning independently of each other? These questions are considered within important applications such as finance, computer gaming and autonomous robotics, using state-of-the-art machine learning tools.

Project B1: Differentially Private Machine Learning

Supervisor: Cristian R. Rojas, Decision and Control Systems, crro@kth.se



Machine learning (ML) has been growing rapidly in recent years, and especially deep learning has transformed various sub-fields in engineering and science, paving the way for great and improved solutions to some of the most difficult problems in these fields. A recent achievement is Chat-GPT and it needs no introduction about its success, as everyone uses it quite frequently. The ultimate success of deep learning lies in the availability of enormous amount of data that makes its training possible. It is the success of deep learning that attracts various big parties such hospitals, universities and financial markets to deploy these models for their accurate predictions, for example, of whether a particular treatment can cure a patient, or if a bank customer will default on her home loan.

However, data shared by these parties to an ML developer may contain sensitive information. For example, data from a bank may contain the address, gender and race of its customers, or a hospital data set may contain previous diseases of its patients. Hence, it is very important to protect this sensitive information. Differential privacy (DP) is a paradigm that allows this by adding some noise in the data or the output of an ML algorithm so that it is impossible for any eavesdropper to infer this sensitive information.

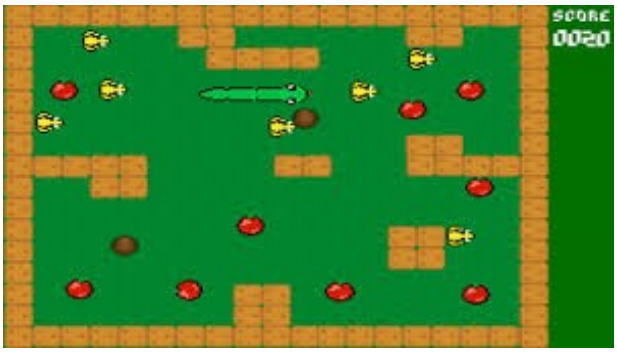
The aim of this project is to implement different approaches to DP and study the impact of DP in the accuracy of standard ML algorithms. In particular, we will apply DP in the context of parameter estimation for dynamical systems.

The main tasks of the project are:

1. Propose various mathematical models for different dynamical systems.
2. Estimate the unknown parameters of these mathematical models and analyse the Cramér-Rao lower bound.
3. Apply DP constraints and numerically analyse their impact on the accuracy of these estimators compared to when there is no DP constraint.

Project B2: Deep Reinforcement Learning for Games

Supervisor: Alexandre Proutiere, Decision and Control Systems, alepro@kth.se



Reinforcement Learning (RL) addresses the problem of controlling a dynamical system so as to maximize a notion of reward cumulated over time. At each time (or round), the agent selects an action, and as a result, the system state evolves. The agent observes the new state and collects a reward associated with the state transition, before deciding on the next action. Unlike classical control tasks where typically the system dynamics are completely predictable, RL is concerned with systems whose dynamics have to be *learnt* or with systems interacting with an uncertain environment. As time evolves, the agent gathers more data, and may improve her knowledge about the system dynamics to make better-informed decisions. RL has found numerous applications, ranging from robotics, control, online services and game playing, and has received an increasing attention. Very recently, RL has solved problems in situations approaching real-world complexity, e.g., in learning human-level control for playing video games. These progresses are mainly due to the use of deep neural networks to speed up classical learning algorithms.

This project aims at developing and implementing reinforcement algorithms to learn to play simple video games optimally. More specifically the main tasks of the project are:

1. Propose a game.
2. Create a mathematical model and a succinct representation and encoding of the game snake.
3. Propose and implement deep reinforcement algorithms.
4. Evaluate the speed at which the algorithms learn optimal moves, depending on the size of the chosen neural network.

Project B3: Distributed Optimization through Deep Reinforcement Learning

Supervisor: Alexandre Proutiere, Decision and Control Systems, alepro@kth.se

Reinforcement Learning (RL) has recently gained popularity through its use in learning to play video and board games. The program AlphaGo developed by Google Deep Mind outperformed the best professional go player and received a lot of media attention. The state-of-the-art algorithms in RL combine classical learning techniques, such as Q-learning, with deep neural networks used to get a succinct representation of the system state and of the reward function. RL algorithms are typically implemented in a single agent whose objective is to optimally interact with her environment. This project is concerned with multiple agents cooperating to learn to interact and to accomplish some tasks optimally. We will focus on a simple warehouse example where multiple robots have to learn to interact with each other (avoid collisions) while repeatedly transporting items from one point to another. These points differ for the various robots, but to perform their tasks, robots must move along common paths. Each robot is assumed to know at any time the positions and velocities of the other robots.

The main tasks of the project include:

1. Model the warehouse and encode the tasks robots have to accomplish.
2. Develop and implement in each robot a deep RL algorithm.
3. Simulate the resulting complex dynamical system.

Project B4: Portfolio Optimization with Predictive Stock Selection Using Machine Learning

Supervisor: Cristian R. Rojas, Decision and Control Systems, crro@kth.se

Portfolio management is the structured process of selecting and distributing various investment assets. The objective is to continually adjust this allocation to optimize expected returns while aligning with an individual's risk tolerance. At the core of portfolio theory lies the Markowitz mean-variance (MV) model, established in 1952, which is widely recognized and utilized in portfolio management.

Recently, machine learning has demonstrated its advantages in the domain of quantitative finance, particularly in the context of portfolio optimization. Traditionally, the MV model relies heavily on historical data to construct the optimal portfolio. However, this approach has limitations due to the static nature of historical data.
Consequently, there has been a growing interest in applying machine learning techniques to forecast future returns and volatility. This research aims to explore the fusion of the MV model with deep learning, yielding a hybrid model that combines a convolutional neural network (CNN) with a bidirectional long short-term memory (BiLSTM) block to predict future stock closing prices.

The primary tasks of this project include:

1. Collecting stock closing prices from sources such as Yahoo!, accessible on the internet.
2. Applying deep learning methodologies to the gathered data to extract meaningful features and predict future prices.
3. Using the Mean-Variance model to minimize the risk of the investor.

Kontext C: Elektriska transportsystem och inbyggda system

Introduktion

Dagens samhälle är starkt beroende av ett fungerande transportsystem för såväl människor som gods. Samtidigt står transporterna för en stor andel av världens koldioxidutsläpp eftersom det är framförallt olja som används som bränsle. Lösningen på det här problemet heter idag elektrifiering. Man behöver elektriska farkoster för såväl på väg, på vatten och i vatten!

I det här kontextet studeras 3 helt olika farkoster som har det gemensamma att de ska utföra en uppgift så effektivt som möjligt. Det är en hyperavancerad racingbil, en flygande elbåt samt en millimeter stor robot som kan övervaka växande grödor. För samtliga farkoster ska utrustning byggas som kan effektivisera deras arbeten.

Tillsammans ska projektdeltagarna även sätta in sina system i det överordnade transportsystemet och reflektera över deras betydelse.

Project C1: Efficiency monitoring of marine electric drivelines

Supervisors: Nicholas Honeth (honeth@kth.se) och Mats Leksell (leksell@kth.se) , Div. Electric power and energy system KTH

This project is part of the FoilCart project, a collaboration of the division of Electric power and energy systems and the division of Naval architecture and solid mechanics. The FoilCart project is investigating the use of compact integrated hydrofoils with electric propulsion to create high performance electric boats.

Measuring the efficiency of a system combining batteries, electric drives, propellers, hulls and hydrofoils requires many simultaneous measurements of the different stages of the driveline and movement of the watercraft. The system taking these measurements needs to be compact and robust in order to be used in the test environments at sea as well as easy to administer and manage the collected data.

In this bachelor's degree project, the participants will design more in detail the energy monitoring system, build it, install it on the FoilCart prototype and present some collected results from sea tests. The project will be practical, challenging, fun and make a useful contribution to a research project.

The following are examples of tasks involved:

- Experiment with measurements of AC and DC voltages and currents
- Experiment with RTK GNSS positioning systems
- Design and implement a data logging system combining the collected measurements
- Install the system in the FoilCart prototype
- Participate in the sea tests with the energy monitoring system
- Present the logged data in real time as well as historical data analysis

Project C2: Wireless Sensor unit for a Formula Student car

Supervisors: Carl-Mikael Zetterling (bellman@kth.se) together with the electronics team at KTH Formula Student Team

The KTH Formula Student vehicle rely on testing for verification and design. In order to get as much data and information possible from every testing session a reliable and extensive sensor setup need to be implemented. Since the car only does a 100-500km of testing each year every session needs to test session needs to collect data for multiple subsystems. Currently there is no way of measuring airspeed and pressure at different points of the car, and the placement of sensors are limited by the cable length. DeV17 has a sophisticated aero kit consisting of venturi tunnels, rear wing, front wing, sidepods, floor and more. The aerodynamic development is heavily dependent on CFD simulations, but to set up accurate simulations real world data is essential and is the difference between guessing and making good assumptions.

The goal of this project is to create a PCB that communicates wirelessly with small sensor units and send the data on CAN. The project will be split into PCB design and Sensor unit design. The PCB should have a wireless transceiver, CAN transceiver and a MCU. The MCU will be programmed by you. The sensor units should be like an AirTag in size and form factor, be powered by a small battery, measure temperature, airspeed or pressure and send the data on CAN. The sensor casing should be designed in CAD and 3D printed. This you can get help with from the KTHFS team. The component selection and design of this sensor unit will be done by you.

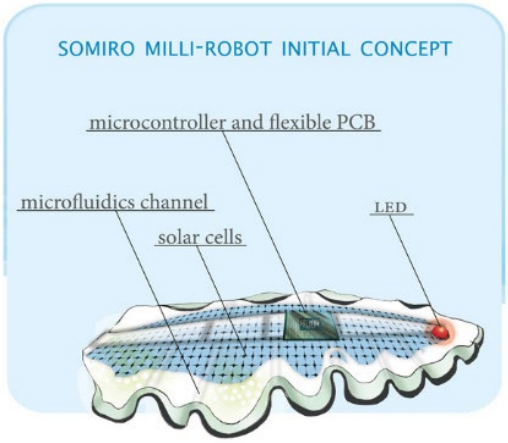
Project C3: Assembly, test design and functionality testing of an energy-autonomous, swimming milli-robot for agricultural monitoring

Supervisor: Gustaf Mårtensson, gustaf.martensson@mycronic.com, Mycronic AB / CBH-KTH

In the Horizon 2020 research project SOMIRO (Soft Millimeter Robot), the world's first energy-autonomous swimming milli-robot with the aim of reducing the environmental impact of farming in terms of carbon footprint, eutrophication and excessive use of pesticides will be designed, built and tested. An important step of this is the assembly and design of testing strategy for the fundamental electronic assembly.

In this project, this goal will be attained by

- Assembling the swimming milli-robot in a proof-of-concept configuration consisting of swimming module, drive electronics and photovoltaic (PV) cell.
- Designing a test of experiment to evaluate the chosen electronic design. The parameters to be tested may include robot's power consumption and / or PCB's electrical characteristics.
- Performing test of proposed design of experiment.
- Collecting and analysing test data and presenting results.
- The swimming module and the PV cell were designed and manufactured by SOMIRO project partners. The drive electronics PCB was co-designed by former KTH students in collaboration with Mycronic AB and the other SOMIRO project partners.



Kontext D: Kraftsystemstyrning

Framtidens kraftsystem ställer helt nya krav på mätning, automation och styrning

På svenska

Som ett svar på utmaningen med klimatförändringarna elektrifieras allt fler delar av samhället, och elproduktionen ställs om till att inkludera stora mängder förnybar och delvis distribuerad kraftproduktion. Dessa förnybara kraftkällor ersätter de större centrala synkronkopplade produktionsenheter som tidigare utgjort ryggraden i systemet. De förnybara kraftkällorna (t.ex. vind och solkraft) är dock kopplade till elkraftsystemet via omriktarstyrda enheter, dvs de är inte synkronkopplade produktionsenheter. Storskalig integrering av dessa förnybara kraftkällor kan påverka elkraftsystemets stabilitet. Dessutom är de förnybara kraftkällorna inte lokaliserade i närheten av stora last-centra, ex vis. städer, vilket gör att kraven på överföring av elenergi förändras. De senaste åren har dessa frågor blivit alltmer aktualiserat i samhällsdebatten.

De nya kraven finns både på transmissions och distributionsnivå. Det inkluderar nya gränser för stabilitet i systemet på grund av minskad rotationsenergi i systemet och ökade variationer gällande spänning, effektflöden och frekvens. Dessa nya krav möts effektivast med nya kontroll- och automationssystem och även nya styrbara kraftsystemkomponenter, vilka blir allt viktigare för ett välfungerande elkraftsystem. För att dessa kontrollsystem ska fungera krävs mer omfattande mätning och insamling mätvärden från större delar av systemet.

Denna kontext behandlar nya metoder och tekniker för styrning av elkraftsystem med stora mängder förnybar kraftproduktion. Projekten i kontexten inkluderar både traditionella elkrafttekniska frågor såväl som utmaningar inom automation och reglerteknik samt de informations och kommunikationssystem som är nödvändiga för denna automation.

In English

For several reasons, the power system is currently developing to include large amounts of renewable and distributed generation that in part replaces the large central synchronously connected production units that previously formed the backbone of the system. However, these renewable energy sources (such as wind power and solar power) are connected to the system via power-electronic-based devices (convertors), i.e. they are not synchronously connected to the system and they are also known as non-synchronous generation. High penetration of renewable energy may affect the power system stability. Furthermore, they are not always located near large loads.

These changes place new requirements on the power system, both at transmission and distribution level. These new requirements include new limits on the stability of the system due to reduced stored kinetic energy in the system and increased variations of voltage, power flow and frequency. These new requirements are in turn met most efficiently with new control and automation systems and new controllable power system components, which are becoming increasingly important for an efficient power system.

This context deals with new methods and techniques for the control of power systems with large amounts of renewable power generation. The projects in the context include both the traditional electric power issues as well as challenges in automation and control technology and information and communication systems necessary for this automation.

Project D1: The impact of high penetration of renewable energy on system inertia and frequency

Supervisor: Mehrdad Ghandhari, mehrdad@kth.se , Electric Power and Energy Systems

Power system frequency is an appropriate measure on the active power balance in a power system. The frequency is constant when the same amount of electrical power is produced as consumed by the loads, including system losses. If this is not the case, frequency changes will occur. The frequency is reduced when a load increase or a loss of production is not compensated by a corresponding increase of the turbine power of the connected generators. The power deficit decelerates the generator rotors and consequently the frequency is reduced. Too large reductions of the frequency can trigger protection system which may result in system separation, loss of load and costumer outages, since many equipments in a power system, e.g. power supply systems, do not tolerate too low frequencies.
Today's power systems have been designed and developed based on conventional power plants (i.e. those that are synchronously connected to the system). These power plants provide synchronizing power (or torque) and inertia which have crucial roles on power system dynamical response, on setting of rotor angle, voltage and frequency stability limits, and also on setting of protection systems. However, renewable energy sources (non-synchronous generation) do not contribute in providing synchronizing power and inertia. Replacing some of the conventional power plants with the non-synchronous generation will result in less system inertia and synchronizing power. The high penetration of non-synchronous generation (mostly wind power, but it can also include solar power and other renewable energy) can therefore result in new challenges to operate the system in a secure and cost-effective manner.
The aim of this project is to study how the system inertia and frequency will be affected once replacing conventional power plants with renewable energy sources via convertors in a test system (the Nordic test system). Also, how to minimize the Instantaneous Frequency Deviation (IFD) after a disturbance in the system.

This study will involve power system stability, frequency control and basic control theory.

The students will be provided with appropriate literature and also simulation models/files.

Project D2: The impact of high penetration of renewable energy on power system stability and damping

Supervisor: Mehrdad Ghandhari, mehrdad@kth.se , Electric Power and Energy Systems

Traditionally, large power systems have mainly been comprised of synchronous forms of generation. Due to concerns of climate change as well as the decrease in cost of wind and solar generation, it is predicted that the widespread integration of power electronics based forms of generation such as solar and wind will occur in the near future. However, the large-scale introduction of power electronics

based generation will have significant impacts on the stability of electrical power systems. First, the frequency of the power system will more rapidly decrease after a disturbance. Additionally, power electronics based devices are not able to provide the same level of reactive power when a fault occurs in the system. The initial objective of this project is to understand the stability issues that arise when renewable generation is introduced into the system. This project will first analyze a small power system. The students will then incorporate wind generation into the power system, decreasing the amount of power provided by the synchronous generators. The response of the two systems will be compared, identifying the differences after the integration of renewable generation. The second portion of the project is to improve the stability of the system and the power system oscillations that arise after a disturbance is applied. This will be done by tuning the supplementary form of excitation control in the synchronous generators or introducing supplementary control in the power electronics based devices.

This study will involve control theory and its application to power system stability.

The students will be provided with appropriate literature and also simulation models/files.

Project D3: Design of a future residential microgrid

Supervisor: Qianwen Xu, qianwenx@kth.se , Electric Power and Energy Systems

Driven by environmental concern and sustainable requirement, development of residential microgrids attracts much attention around the world, as a forward step towards future carbon-neutral society. A residential microgrid is a small power system for a house/building, which consists of a solar photovoltaic (PV) source, a battery storage, and residential loads, and can operate either in isolation or in connection to the main grid. In the daylight, the solar PV source can generate electricity to supply the loads, and the extra electricity can be stored in the battery to be used in the evening, or even sold back to the main grid. Thus a residential microgrid can reduce the energy cost and reduce CO2 emission. To make it works, each component of the microgrid should be properly designed and they should be controlled in a coordinated manner to provide stable and sustainable electricity

This project will develop a residential microgrid and its control scheme to achieve stable and sustainable electricity supply. The PV converter system will be designed to maximize its power generation in the daylight; the battery converter system will be designed to be charged when there is surplus electricity, and discharged when there is insufficient electricity. A coordinated control scheme will be developed for the whole system with high reliability and stability.

Context E: Hydro power as a balancing resource in the power system

A fundamental property of a power system is that the generation and consumption of electric power must always be in balance. It is therefore necessary to have enough flexible resources (i.e., generation or demand that can be adjusted to help maintain the balance of the power system) available. The amount of weather dependent, continuously varying generation (for example wind or solar power) is expected to continue increase in the future, which means that the need for flexible resources will also continue to increase.

An individual hydro power plant is very flexible and can very rapidly increase or decrease the generation. However, the operation of multiple hydro power plants in the same river system will be most efficient if coordinated, as water released from an upstream reservoir will eventually reach the next reservoir in the river and if that reservoir is full then water will have to be spilled. The operation planning of a river system can be formulated as an optimisation problem, where the objective is to maximise the value of the total hydro generation in the river system, while taking into account the hydrological coupling between the hydro power plants as well as other operational limitations.

Hydro power has been one of the main sources of flexibility in the Nordic power system. However, to fulfil EU-wide goals for water environment, Sweden has a national plan for revision of the hydro power plant licences, which determine how the owners of the hydro power plants are allowed to schedule generation. The revision of the licenses will need to balance conflicting environment goals and energy goals. For example, requirements on keeping water flows through the natural riverbeds will promote biodiversity and provide ecosystem services, but will result in lower hydro power generation and may influence the flexibility of the concerned hydro power plants.

The aim of this context is to study how much flexibility different hydro power systems can provide under various conditions. The operation planning of the studied systems will be studied using the open-source energy system modelling tool Spine [1].

[1] https://github.com/Spine-tools

Project E1: Impact of environment restrictions on hydro power flexibility

Supervisor: Mikael Amelin, amelin@kth.se, Electric Power and Energy Systems

The revision of hydro power plant licenses in Sweden will be a process that take several years to complete and it is not yet certain what kind of environment restrictions that will be imposed by the court decisions and to which extent hydro power plants that are important to the power system can be exempted from strict requirements.

The objective of this project is to set up a model of a larger Swedish river system and investigate the consequences of different possible environment restrictions.

Project E2: Comparison of flexibility factor and extreme load following capacity

Supervisor: Mikael Amelin, amelin@kth.se, Electric Power and Energy Systems

The flexibility of a power plant is generally understood as the capability of the power plant to generate electricity when it is needed by the system. However, there is no common definition of how to estimate the flexibility of a power plant. Two possible measures of flexibility are *flexibility factors* and *extreme load following capacity*. The former represents the average income of sold electricity during a test period divided by the average electricity price during the same period, whereas the latter represents the capability of the power plants to follow a load that is periodically varying between a low level and a high level.

The objective of this project is to set up one or more models of Swedish or fictitious river systems and compare the results of the two flexibility measures for each system.

Project E3: Coordinated versus greedy planning of small-scale hydro power

Supervisor: Mikael Amelin, amelin@kth.se, Electric Power and Energy Systems

The hydro power plants in one river system may in many cases have different owners. In practice, companies are not allowed to cooperate when bidding to the electricity market. However, in the ideal case, there would be one single entity that is responsible for planning the entire river (coordinated planning). The opposite extreme would be planning where the most upstream hydro power plant decides their own schedule, without consideration of the other power plants, and the downstream power plants will simply have to adjust (greedy planning). This will obviously lead to less optimal results compared to the coordinated planning. The question is how much worse greedy planning would be?

The objective of this project is to set up several fictitious systems of small-scale hydro power plants and to carry out a sensitivity analysis of which factors that influences the difference between coordinated and greedy planning the most.

Context F: Predicting the future sustainable power system

To help mitigate climate change, it will be necessary to significantly reduce CO_2 emissions. These efforts will in turn have a major influence on power systems and electricity markets, both because power generation is in itself a large source of CO_2 emissions, but also because electricity is necessary to facilitate eliminations of CO_2 emissions in other parts of society. In short, there will be an increased demand for CO_2-free electricity generation in the future. Two main sources of such electricity is of course wind and solar power, which is being introduced in a wide scale across most electric power systems on the planet.

One important characteristic of wind and solar power is that it is non-dispatchable, i.e. the output cannot be controlled but depends on weather. As can be observed on the electricity market recently, the volatility of electricity prices has increased due to the varying inflow of power from these sources[1]. Similarly, the non-disptachable nature of the renewable sources are creating futheer challenges for stable operation of the power system in real-time. To improve functioning of the electricity markets and faciliatate cost-efficient and reliable planning and operation of electric power systems, there is a need for better prediction of the impact of renewable sources on the power grid. This inludes several aspects of this problem including forecasting electricity prices as well as renewable generation but also load, which is also trending towards increased volatility due to new types of consumers e.g. electric vehicles, electrolysers and battery storage systems.

The aim of this context is to explore data science based methods for improved forecasting of electricity price (F1), Renewable generation (F2) and Load (F3).

(1) https://www.di.se/nyheter/svenska-kraftnat-varnar-for-mer-volatila-elpriser-och-okad-risk-for-akut-effektbrist/

Project F1: Estimation and forecasting of the electricity prices

Supervisor: Mohammad Reza Hesamzadeh, mrhesa@kth.se,
Electric Power and Energy Systems

In this project we focus on estimating and forecasting electricity prices in the wholesale electricity markets. We mainly focus on the electricity spot markets which are day-ahead, intra-day, and real-time markets. Due to competitive forces in the today's electricity markets, electricity-price estimation and forecasting has become a fundamental tool which provides input to the decision-making mechanisms.

The electricity as a tradable commodity is notoriously volatile. This is partly because electricity is not economically storable and what is produced at a moment must be consumed at that moment. Also, electricity demand depends on hard-to-predict parameters such as weather or the intensity of everyday activities. These characteristics of electricity make the electricity prices to have a very complex dynamic. It often depends on several driving factors.

Besides, the current push from governments in many jurisdictions to increase the share of renewable CO2 free generating technology (mainly wind and solar generation) has added extra level of complexity to electricity price estimation and forecasting models. These renewable generation sources are intermittent, and they make the electricity spot prices more volatile than before.

At this background, the area of price estimation and forecasting has been quite active over the last few years. Various estimation-and-forecasting techniques are suggested in the academic literature with various degrees of success. Also, competition events such as Global Energy Forecasting Competition (GEFcom) are organized to attract the innovative forecasting techniques.

Broadly speaking, the estimation-and-forecasting techniques can be categorized as regression models and intelligent models. Linear and nonlinear regression are examples of regression models and the Neural network models are examples of intelligent models. The estimation and forecasting models can be static (without considering time) and dynamic (with time consideration). References [1] and [2] below provide very good information about different estimation-and-farecasting techniques.

At this background, this project has the following aims:

(1) A review of different recent techniques developed and suggested in the literature for electricity spot-price estimation and forecasting; In this review, the strengths and weaknesses of these reviewed techniques are clarified.
(2) To select three promising forecasting techniques and justify why these technique are suitable for forecasting; These three techniques can be selected between the regression and intelligent techniques.
(3) To apply the selected three forecasting techniques to estimate-and-forecast the spot prices in the Nordic electricity market. You can select two markets out of three following markets: day-ahead market, intra-day market, and real-time market. For your application, you may use the following software packages: Julia/Python, R, Eviews or Matlab.
(4) To interpret and explain the estimation-and-forecasting results that you have obtained for your selected spot markets and your forecasting technique.

References:
[1] https://en.wikipedia.org/wiki/Electricity_price_forecasting
[2] Bunn, Derek W. "Modelling prices in competitive electricity markets." (2004).

Project F2: Estimation and forecasting of the renewable generation

Supervisors: Lars Nordström, larsno@kth.se, and Xavier Weiss xavierw@kth.se
Electric Power and Energy Systems

Wind generation in Sweden has gone through an enormous expansion the last 5-10 years and is expected to see even larger expansion with the growth of off-shore wind power [1]. Presently (2022) the total wind energy production amounted to 33TWh, approximately 20% of the total Swedish electric energy generation. Similarly, Solar power is seeing a similar expansion, albeit from lower numbers, both in terms of PV-farms in the MW scale to household level PV on roof-tops. With the size and scale of PV being smaller, and more distributed in the grid, the observability of PV is lower than that of wind generation but can during situations of low load, e.g. a warm day in July, still amount to a large proportion of the total generation.

Given the variability in in-feed from renewable sources both in time and space, there is a need to forecast the production so that planning of the operation of the power grid can be facilitated. As an example, upcoming changes in production from wind may necessitate activation of reserves and systems services. Similarly, the location of generation in the grid may cause congestion if the production is concentrated to specific areas far from load-centers. Overall, the need to predict the production from renewable generation both in space (price area) and time (hours and days) is growing.

1) A review of different recent techniques developed and suggested in the literature for renewable generation (wind, solar or both) estimation and forecasting; In this review, the strengths and weaknesses of these reviewed techniques should be clarified. https://transparency.entsoe.eu https://transparency.entsoe.eu
2) Develop one forecasting application for renewable generation based on suitable approach identified above, using data from the ENTSO-E Transparency portal[1] applied to one or several price areas in the Nordic power system. For your application, you are encouraged to use: Python or Matlab.
3) To apply the developed forecasting technique to estimate-and-forecast the renewable generation. The forecasts shall be benchmarked with the forecasts available on the ENTSO-E transparency platform.
4) To interpret and explain the estimation and forecasting results that you have obtained

References:

1. https://www.energimyndigheten.se/statistik/den-officiella-statistiken/statistikprodukter/vindkraftsstatistik/
2. https://transparency.entsoe.eu

Project F3: Estimation and forecasting of load

Supervisors: Lars Nordström, larsno@kth.se, and Arvid Rolander arvidro@kth.se
Electric Power and Energy Systems

The electric load has in Sweden for a long period remained relatively stable. The share of residential load remaining constant with some changes in industrial and commercial load as society has moved from heavy industry in 1980s to a service based economy centered on larger cities[1]. Present forecasts [2] indicate a doubling of the electricity load, mainly due to electrification of heavy industries in mining and steel manufacturing, but other sectors such as transportation are also contributing to this growth.

Similar to the development within renewables (see project 2) the changes in load happen both in time and space. E.g. data centers are built outside municipalities or steel mills are redesigned to use electricity and Hydrogen instead of fossil fuels. Given this, there is a need to forecast the load so that planning of the operation of the power grid can be facilitated. As an example, the location of loads in

the grid may cause congestion if the production is concentrated to specific areas far from these load-centers. Overall, the need to predict the loads both in space (price area) and time (hours and days) is growing.

1) A review of different recent techniques developed and suggested in the literature for electricity load both residential, commercial and industrial; In this review, the strengths and weaknesses of these reviewed techniques should be clarified.
2) Develop one forecasting application based on suitable approach identified above, using data from the ENTSO-E Transparency portal[1] applied to one or several price areas in the Nordic power system. For your application, you are encouraged to use: Python or Matlab.
3) To apply the developed forecasting technique to estimate-and-forecast the total electricity load. The forecasts shall be benchmarked with the forecasts available on the ENTSO-E transparency platform.
4) To interpret and explain the estimation and forecasting results that you have obtained

References:

1. https://www.energimyndigheten.se/statistik/den-officiella-statistiken/statistikprodukter/manatlig-elstatistik-och-byten-av-elleverantor/
2. https://www.svk.se/siteassets/om-oss/rapporter/2021/langsiktig-marknadsanalys-2021.pdf
3. https://transparency.entsoe.eu

Context G: Design and testing of novel microwave/antenna technologies

Today, microwave technology is employed in many of our technological devices, and they fulfil an essential function in communication systems, intelligent cities, surveillance, medical diagnosis and space observation.

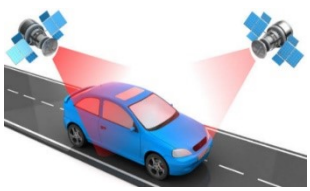
Innovative microwave designs are required daily in the products of technology-driven companies. These companies require efficient and multi-functional antennas and microwave devices that can enable:

- High data rate communications for future 5G and 6G networks.
- Efficient satellite communications with the newly deployed low-Earth-orbit satellites.
- High resolution radars to detect people, vehicles and objects in smart cities.
- Non-invasive imaging of patients for early detection of health issues.
- Highly precise airport scanners that maximize the location of concealed objects.
- Precise detection of stars and planets in the outer space.

Within the projects of this Context, you will be able to acquire the fundamental knowledge for designing advanced microwave devices and antennas. You will learn how to use commercial software of simulation, which is commonly employed in the industry. Finally, you will manufacture and measure a proof-of-concept. After the project, you will be able to reproduce the usual steps followed in a microwave or antenna design process.

Examples of challenges which require innovative microwave/antenna technologies





Picture 1. Artistic rendition of 5G communications.
Picture 2. Autonomous car inter-connected with wireless systems.
Picture 3. Patient inside a high-resolution medical scanner.
Picture 4. Car communicating with low-Earth-orbit *satellites.*

Project G1: Characterization of 3D printing microwave dielectric materials for space communications

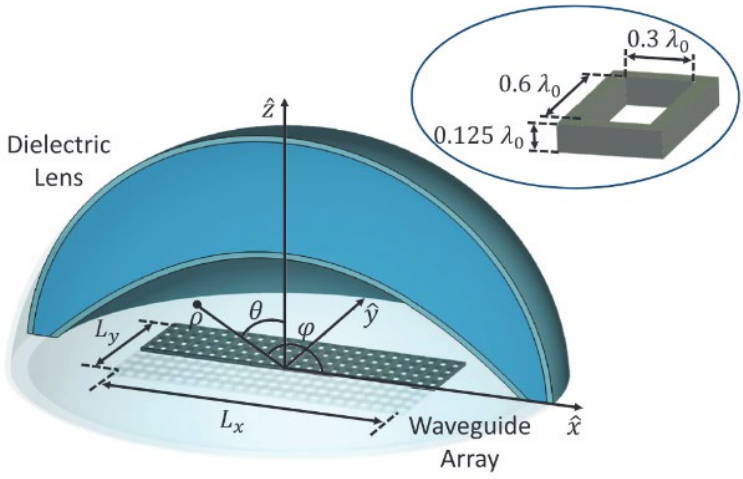
Supervisors: Oscar Quevedo-Teruel, oscarqt@kth.se, Jose Rico-Fernandez jrfe@kth.se, *Division of Electromagnetic Engineering and Fusion Science*

In the ever-evolving landscape of communication systems, the demand for efficient antennas capable of handling higher frequency bands is on the rise. This project aims to explore the potential of 3D printed dielectric microwave unit cells as essential building blocks for next-generation space communication systems. These unit cells will be designed, manufactured using Fused Deposition Modeling (FDM) additive manufacturing technology, i.e. 3D printing, and thoroughly characterized to assess their electromagnetic properties. The ultimate goal is to contribute to the development of advanced components for space communication applications.

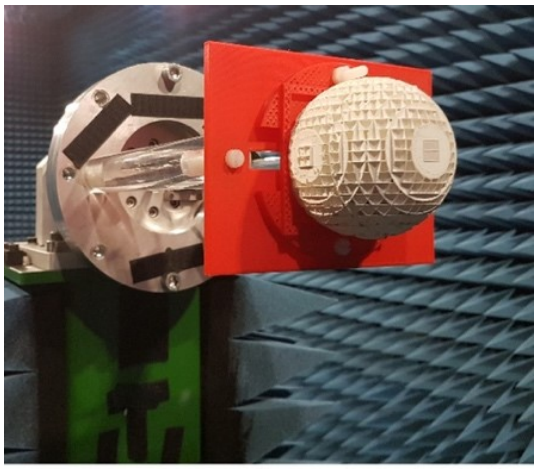
Along the project the student will develop various microwave unit cell designs tailored to specific communication system requirements. This will include exploring different geometries and configurations to optimize unit cell performance. Secondly, FDM 3D printing technology will be used to manufacture the designed unit cells, which will mean experimenting with different printing parameters and materials to achieve optimal results. After manufacturing, the student will conduct comprehensive measurements and testing of the 3D printed unit cells to characterize their electromagnetic properties.

As a student, you will learn:

- How to design microwave unit cells tailored to specific communication system needs. Learn how different geometries and configurations can impact unit cell performance.
- How to use FDM 3D printers to manufacture complex microwave unit cells. Understand the importance of selecting appropriate printing parameters and materials for optimal results.
- How is the influence of dielectric materials on unit cell behavior. Understand the trade-offs between different materials and their suitability for space communication system



Three-dimensional configuration with a dielectric lens antenna and 24×8waveguides as array feeds.



3D printed Gutman lens at KTH anechoic chamber.

Project G2: Higher-symmetric microwave device based on anten'it kits

Supervisors: Oscar Quevedo-Teruel, oscarqt@kth.se, Núria Flores-Espinosa, nuriafe@kth.se, Pilar Castillo-Tapia, pilarct@kth.se, *Division of Electromagnetic Engineering and Fusion Science*

With the development of modern society, there is a high demand for high-performance yet low-cost microwave devices for the applications of terrestrial and satellite communications, automotive radars, surveillance systems and so on. Recently, periodic structures have been widely used to design a wide range of microwave devices, such as lenses, leaky-wave antennas, flanges with low leakage, and filters. A periodic structure is said to possess a higher symmetry if it is invariant after a transition and additional geometrical operation. Mainly, two types of higher symmetries have been investigated for electromagnetic purposes: glide- and twist-symmetries. Higher symmetries are capable of increasing the bandwidth, isotropy, and equivalent refractive index of conventional periodic structures.

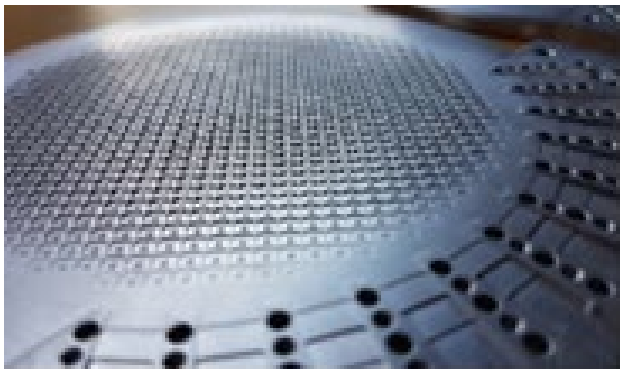
Anten'it is an antenna & microwave design and training hardware, which offers a new approach to antenna & microwave component design. The brick-based design methodology lets the users have reusable building blocks and iterate directly on the hardware. Aside from direct design in hardware environment, Anten'it also supplies 3D CAD files that can be imported to electromagnetic simulation tools, such as the CST studio.

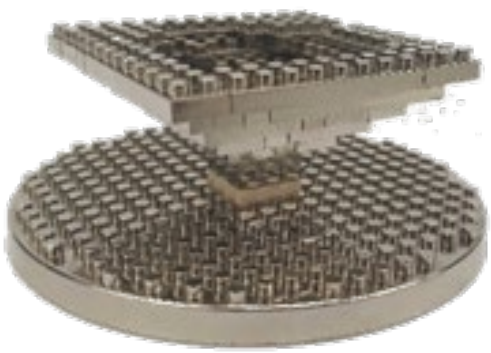
The main goal of this project is to design, build and measure a higher-symmetric microwave device based on Anten'it kits. As a student, you will learn:

- The electromagnetic operation of higher-symmetric structures.
- How to simulate higher-symmetric structures with commercial software.
- How to design and build microwave devices with the Anten'it kits.
- How to measure a microwave device in our microwave laboratory.

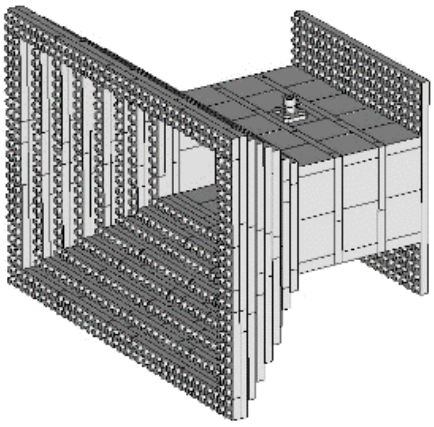
A holey glide-symmetric filter

A glide-symmetric Luneburg lens





A discone antenna built by anten'it kits



A discone antenna with building bricks in CST

Project G3: Design of a linear to circular polarization converter for satellite communication applications

Supervisors: Oscar Quevedo-Teruel, oscarqt@kth.se, Freysteinn Viðarsson, fvvi@kth.se, *Division of Electromagnetic Engineering and Fusion Science*

Satellite communications from ground to Earth typically require circularly polarized (CP) waves to mitigate the effect of Faraday rotation. However, the advantage of circularly polarized waves comes at the cost of added complexity in designs.

One method of achieving CP is through the integration of an appropriate polarization converter with a linearly polarized (LP) source. This is achieved by advancing or delaying the phase of each of the components of the LP signal, so that when they are transmitted from the converter, they add vectorially to form a CP wave.

With 3D printers becoming relatively cheap and commercially available they offer new and low-cost solutions. Complex geometries can be realized without any waste of material and with good repeatability.

The purpose of this project is to simulate, design and test a linear-to-circular polarization converter that can be manufactured using 3D printing, with intended use for satellite communication.

In this project, the student will learn:

- The operation linear to circular polarization converters and their implementation in satellite antennas.
- How to simulate periodic structures using commercial simulation software.
- How to design a linear to circular polarization converter with the desired bandwidth and angular performance capabilities.
- How 3D print microwave compatible materials.
- How to do antenna measurements in the antenna laboratory.

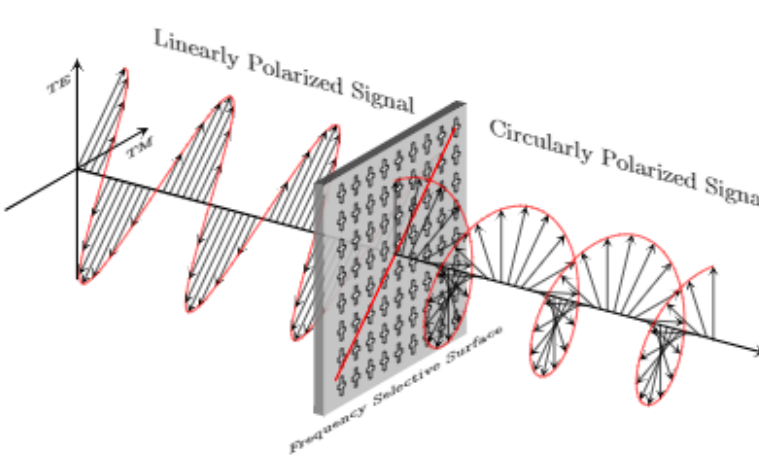


Illustration showing the conversion of a linearly polarized wave to a circularly polarized one after incidence on an appropriate converter.

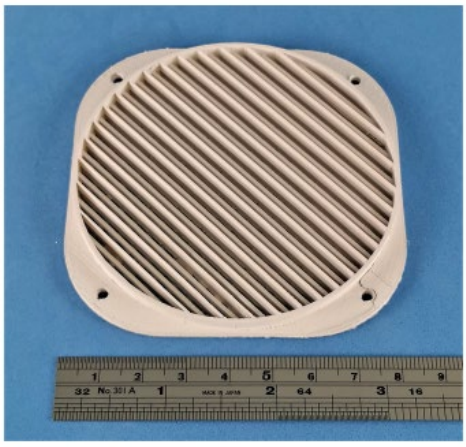


Image of a 3D-printed polarizer converter.

Project G4: Microwave heating of nanoparticles in human tissue

Supervisors: Mariana Dalarsson, mardal@kth.se, Brage Bøe Svendsen, bragebs@kth.se *Division for Electromagnetic Engineering and Fusion Science*

Conventional radiation treatment of cancer uses high doses of x-ray radiation to kill cancer cells and shrink tumors. However, high doses of x-ray radiation does not only kill or slow the growth of cancer cells, they also affect the nearby healthy cells. Damage to healthy cells can cause various side effects. It is therefore of interest to potentially replace the damaging x-ray radiation treatment with treatment using non-ionizing microwave radiation.

The idea relies on the unique property of cancer cells to attract inserted gold nanoparticles (GNPs) when the GNPs are attached with nutrients targeting the bio-markers or antigens that are specific to cancer tissue. Once the electrically charged GNPs have been taken up by the cancer cells, an electromagnetic (EM) field is applied, which indirectly destroys the cancer through heating without damaging the surrounding tissue. This can only be achieved provided that the suspension of GNPs can be designed to be plasmonically resonant, and have a sufficiently large absorption cross-section in contrast to the surrounding medium.

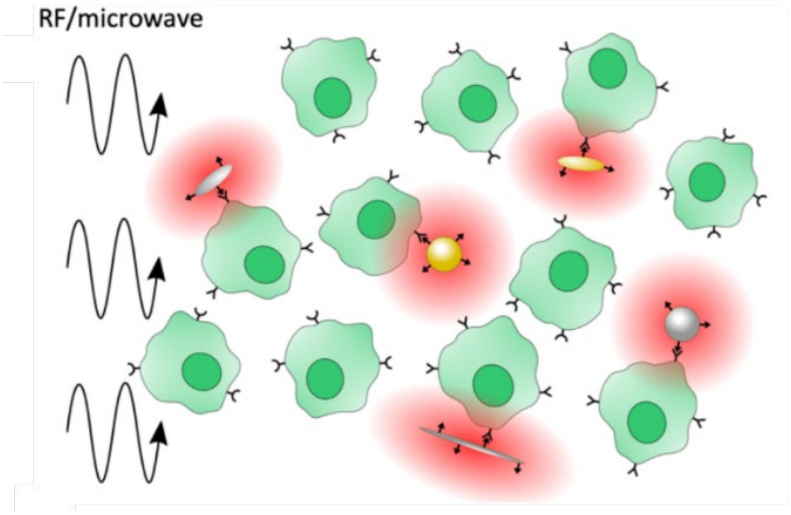


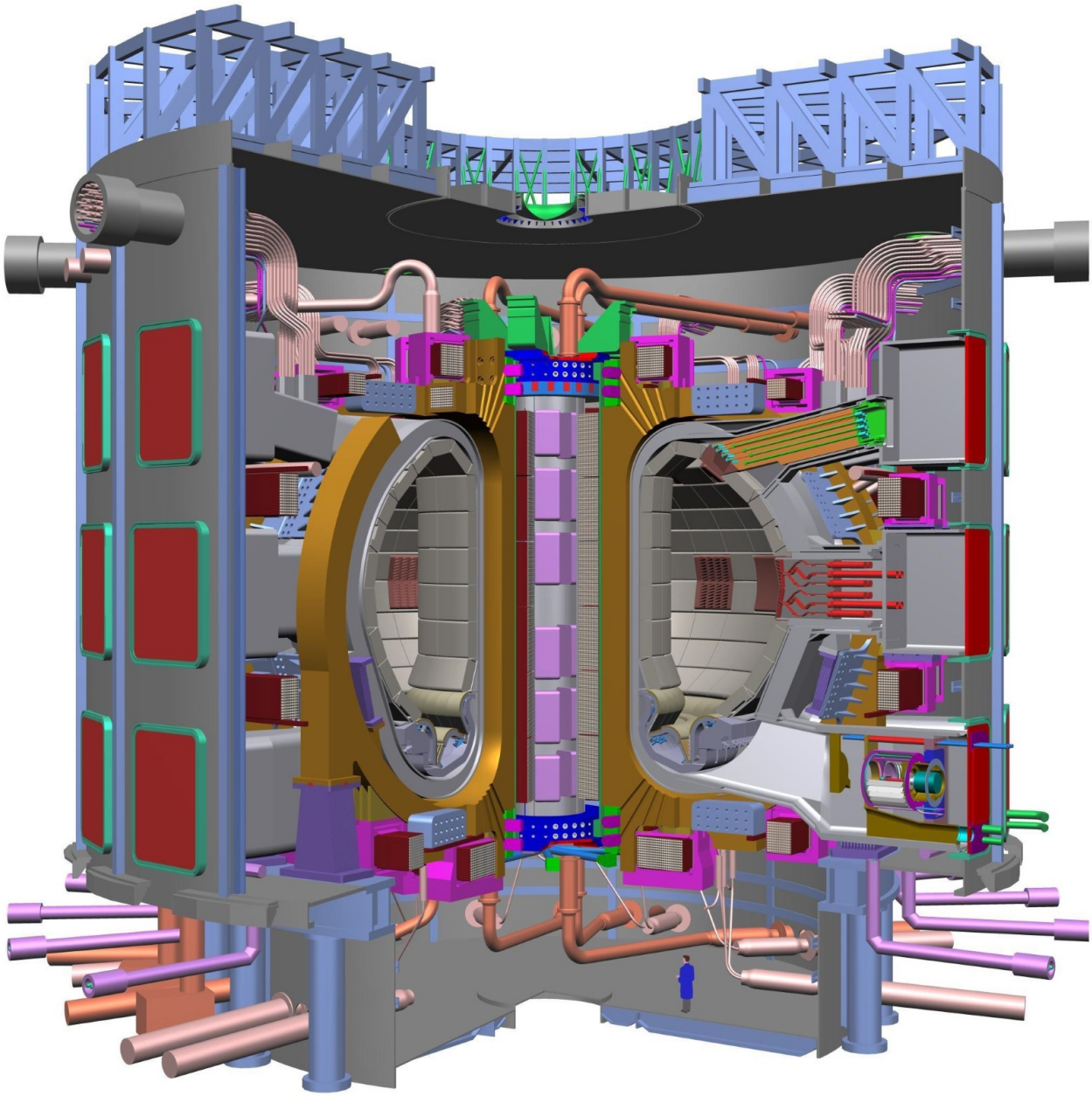
Figure: GNPs of various shapes near cancer cells are heated due to the applied field.

The purpose of this student project is to investigate the theory behind the heating mechanisms involved for GNPs in biological tissue exposed to applied radiofrequency fields. The project is theoretical, with numerical simulations in COMSOL to verify the theory.

In this project, the student will learn:

- About the heating mechanisms at play between the EM field, GNPs, and tissue.
- About the bio-markers attached to the GNPs and the side-effect they have on heating.
- How to model the EM properties of the relevant biological tissue.
- How to evaluate the EM absorption in GNPs using scattering theory.
- How to use effective medium theory to approximate properties of inhomogeneous materials.
- How to develop relevant numerical models using commercial software (COMSOL).

Context H: Fusion, solens energikälla på jorden



Den 73m höga fusionsreaktorn ITER som nu byggs i södra Frankrike och som ska stå klar 2020. ITER väntas kunna producera 10 gånger mer energi än den förbrukar.

Introduktion

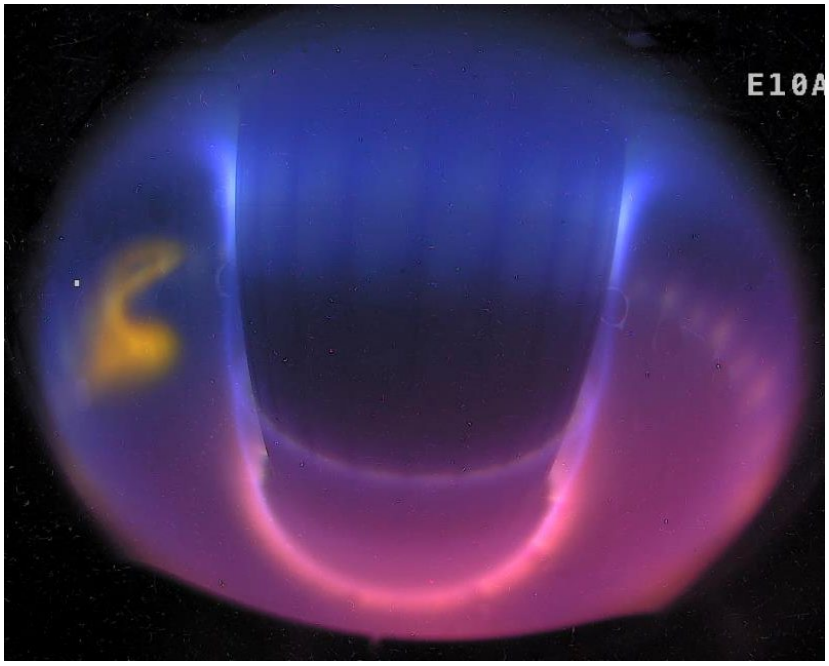
Fusionsforskningen arbetar för att kunna konstruera ett kraftverk som genererar energi från kärnreaktioner mellan olika väteisotoper. Dessa fusionsreaktioner avger ungefär en miljon gånger mer energi än kemiska reaktioner och är den process som värmer solen. Om fusionskraften kan bemästras på jorden har vi en i princip i outtömlig energikälla utan växthuseffekter och med relativt lite radioaktiva restprodukter. Dessa reaktioner sker dagligen i fusionsexperiment världen över, men man har aldrig lyckats producera mer än 65% av den inmatade effekten. För att producera nettoeffekt krävs större experiment och just nu byggs en experimentanläggning, ITER, i södra Frankrike som väntas producera tio gånger högre effekt än vad man stoppar in. ITER är det andra mest påkostade vetenskapliga projektet i mänsklighetens historia, efter den internationella rymdstationen (ISS). Om fusion fungerar, som många forskare tror, kan det ha stor betydelse för vår framtida energiförsörjning.

Varför behövs så stora experiment? För att fusionsreaktionen ska komma i gång måste man uppnå en temperatur på över 200 miljoner grader, samtidigt som man behöver en tillräckligt hög täthet (~10^{20} m^{-3}), vilket är svårt att åstadkomma i mindre maskiner. Så hur kan man bygga en reaktor som innesluter en 200 miljoner grader varm gas (eller plasma som gasen kallas vid dessa temperaturer)? Det finns inga material som klarar att värmas till över 3 000 grader utan att smälta, så i en fusionsreaktor måste det varma plasmat hållas borta från väggarna. Detta sker med hjälp av magnetfält. Men även med starka magnetfält "läcker" värmen ut, och väggarna i en fusionsreaktor utsätts för stora påfrestningar. Dessutom måste plasmat ständigt värmas upp för att kompensera för värmeförluster till väggen. Denna uppvärmning kommer dels från fusionsreaktionerna, dels från injektion av radiovågor och av högenergetiska partiklar, samt resistiv uppvärmning.
Projekten i den här kontexten ingår både experimentella och teoretiska projekt. Här får man möta forskning vid frontlinjen och man får en inblick i möjligheterna och utmaningarna kring fusionskraften. Dessutom ska vi besöka fusionsexperimentet Extrap-T2R på KTH, samt diskutera etiska och politiska frågor kring vår framtida elförsörjning.

Projekt H1: Strålande relativistiska bananer i fusionsplasmor

Handledare: Mathias Hoppe, mhop@kth.se, EMF

Framtidens fusionsreaktorer av typen tokamak – den hittills mest framgångsrika sortens fusionsmaskin – står inför ett svårt problem. Om det svårkontrollerade plasma som utgör fusionsreaktorns bränsle plötsligt kyls ner (exempelvis på grund av att föroreningar från väggarna tar sig in i plasmat eller på grund av att plasmat försöker slita sig loss från det magnetfält som håller det på plats) kan fusionsreaktions väggar ta skada och plasmats elektroner kan accelereras till relativistiska energier och skena iväg. Den här sortens skenande elektroner kan i sin tur orsaka speciellt djup skada på väggarna vilket kan kräva lång reparationer och öka kostnaden för att driva en fusionsreaktor.



För att utveckla metoder att bli av med, eller helt förhindra uppkomsten av, skenande elektroner görs idag olika typer av experiment vid existerande fusionsanläggningar för att bättre förstå hur de skenande elektronerna uppstår och beter sig. Eftersom plasmat är extremt känsligt går det inte att göra mätningar på elektronerna direkt, utan deras egenskaper måste mätas indirekt, dvs på avstånd från plasmat. En av de mest kraftfulla metoderna för att göra mätningar på skenande elektroner går ut på att detektera det så kallade synkrotronljus de strålar ut med hjälp av synligt ljus- och IR-kameror. Synkrotronljuset varierar nämligen när elektronernas hastighetsvektor varierar, vilket gör det möjligt att bestämma både position och hastighet för elektronerna med en synkrotronkamera.

Modeller har utvecklats för att beräkna synkrotronljuset från skenande elektroner, men på grund av svårigheter i de numeriska implementationerna av modellerna är det fortfarande oklart hur synkrotronljus från vissa typer av skenande elektroner ser ut. Framförallt rör detta skenande elektroner som rör sig längs så kallade fångade banor, ibland även kallade banan-banor med hänvisning till den form partikelbanorna tar. Målet med detta projekt är därför att ta fram och implementera en modell som undviker tidigare modellers numeriska brister och en gång för alla ger svar på hur synkrotronljus från relativistiska elektroner som följer banan-banor faktiskt borde se ut!

Projektet kommer kräva en del analytiska beräkningar och en större del programmering för att lösa ekvationerna som formuleras.

Projektet kommer genomföras i följande steg:

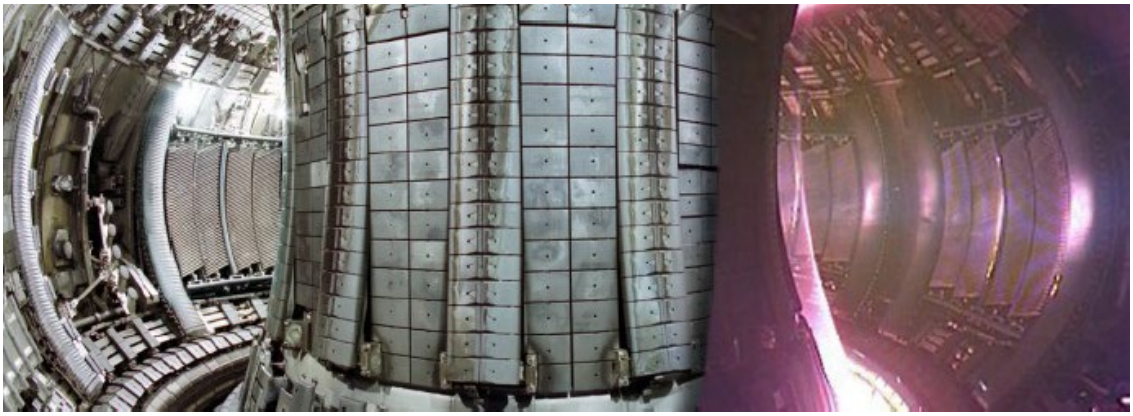
1. Läs relevant litteratur om skenande elektroner, synkrotronljus och den matematiska beskrivningen av en tokamaks geometri
2. Utgående från existerande modeller för synkrotronljuset, formulera en ny, förenklad modell.
3. Skriv en kod som löser ekvationerna för den nya modellen i valfritt programspråk (t.ex. Python)
4. Med hjälp av den nya koden, studera hur synkrotronljus från olika typer av skenande elektroner ser ut och betrakta speciellt de elektroner som följer banan-banor.
5. Skriv en rapport och gör en presentation som beskriver projektets metod och resultat.

Project H2: Automatic interpretation of ion beam measurements of walls in fusion machines

Supervisors: Per Petersson, per.petersson@ee.kth.se, EMF; Laura Dittrich, lauradi@kth.se, EMF

The hot fusion plasmas (200 million degrees) must be surrounded by walls of a vacuum vessel and confined by strong magnetic forces. The heat necessary for fusion reactions poses very severe requirements on the selection of wall materials for a thermonuclear fusion reactor.
In future reactor devices, such as the International Thermonuclear Experimental Reactor (ITER), the interaction of the plasma with surrounding materials in the vacuum vessel constitutes one of the main remaining engineering problems.

As access to the walls of large-scale fusion devices is extremely limited one method to gain knowledge about the impact of the plasma on the wall of fusion devices is to perform small scale experiments. Such small-scale experiments can be performed by producing samples with relevant combination of materials and expose these samples to directions plasma conditions.



JET tokamak in Culham, England - with and without plasma.

The main goal of this project is to investigate the effects of combing different materials compared to simulate deposits on plasma facing components with a focus on the effect of combining Tungsten and

Boron with further elements. The results can then be compared with samples of without the included elements and by simulations of the interaction.

The work will be of practical and interdisciplinary character with elements of material science, data processing, atomic physics and plasma physics. Depending on the interests and selection of samples, the project may be developed in several directions.

It will include visits to the Tandem Accelerator Laboratory of Uppsala University that houses equipment for both production of samples and for material analysis by to accelerator-based material analysis techniques.

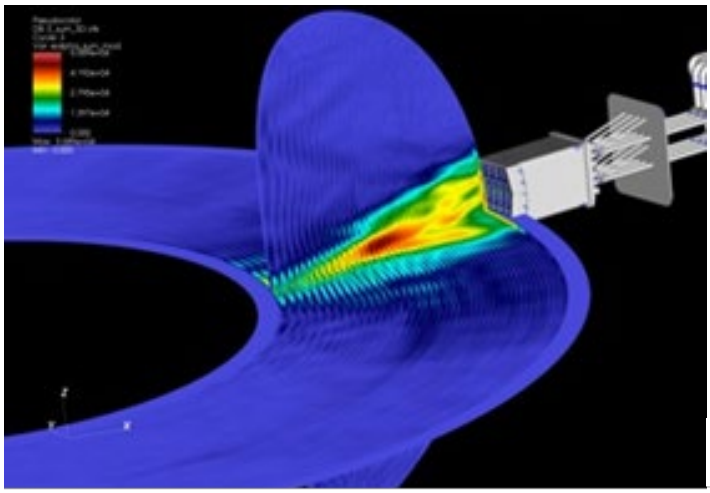
Main Tasks

1. Selection of materials for studies and simulations
2. Production of materials
3. Surface studies of the selected materials.
4. Exposure of the materials
5. Further surface studies of the selected materials for comparisons
6. Possible comparison to simulations of the interaction
7. Report and presentation

Projekt H3: Modellering av radiovågsuppvärmning för fusion

Handledare: Thomas Jonsson, johnso@kth.se, EMF; Lukas Bähner, bahner@kth.se, EMF; Björn Zaar, bzaar@kth.se, EMF

Fusionsreaktioner kräver mycket höga temperaturer. För att producera stora mängder energi i ett fusionskraftverk krävs cirka 200 miljoner grader, temperaturer som kan skapas med hjälp av radiovågsuppvärmning. I det här projektet kommer vi studera radiovågsuppvärmning genom simuleringar med det nya kodpaketet Femic-Foppler. Målet med projektet är att få en djupare förståelse för vad som händer när man kopplar mer och mer effekt. Denna förståelse är av stor vikt för framtida studier med Femic-Foppler.



Elektrisk fältstyrka från en numerisk simulering av radiovågsuppvärmning i ett fusionsplasma.

Modellering av radiovågsuppvärmning kräver att man beräknar både hur vågen propagerar, samt hur partiklar accelereras av vågorna. För att göra den här typen av beräkningar har forskare på KTH utvecklat två koder: Femic, som beräknar vågfält, samt Foppler, som beräknar accelerationen av partiklar. Men, de två koderna beror på varandra - accelerationen beror på vågfältet, samtidigt som vågfältets påverkas av hastigheten på de accelererade partiklarna. Därför har de två koderna nyligen kopplats ihop så att man på ett konsistent sätt kan beräkna både vågens utbredningen och accelerationen av partiklar.

I detta projekt kommer vi köra simuleringar med Femic-Foppler för att studera de ickelinjära effekterna som uppkommer när man kopplar vågutbredning och partikelacceleration. Vi kommer framför allt att studera vad som händer när man ökar den inmatade effekten och därmed accelererar partiklarna till högre och högre energi. Studien ska jämföra ett par olika uppvärmningsscenarier, d.v.s. olika frekvenser och acceleration av olika partikelslag.

I detta projekt kommer man lära sig mycket fysik. Man kommer få prova på att göra ett forskningsprojekt och dessutom göra att viktigt bidrag till forskningen kring Femic-Foppler. I projektet kommer vi arbeta med både COMSOL Multiphysics och MATLAB.

Målen med detta projekt är:

1. Läsa relevant litteratur om fusionsplasmafysik och radiovågsuppvärmning.
2. Lära sig den grundläggande fysiken som finns beskriven i Femic-Foppler, samt att lära sig köra koden och analysera resultaten.
3. Identifiera och beskriva de ickelinjära fenomen som vi kan förvänta oss i Femic-Foppler modellen.
4. Designa och utföra simuleringar av uppvärmning i fusionsanläggningen ASDEX som både är experimentellt relevanta och som illustrerar de olika ickelinjära fenomenen.
5. En kvalitativ och kvantitativ analys av simuleringsresultaten som besvarar frågorna;
    a. När är de olika ickelinjära effekterna viktiga?
    b. Hur skiljer sig dessa effekter mellan olika uppvärmningsscenarier?
6. Skriva en rapport och hålla en presentation.

Context I: Solar wind and planetary magnetospheres

Context responsible: Tomas Karlsson (tomas@kth.se)

INTRODUCTION

Space Physics encompasses the physics of the open space in our solar system, mainly the environments of the Earth, other planets, and the Sun. The neutral gas and plasma (charged gas) environments of the Sun, the planets (including Earth's magnetosphere) and smaller bodies like moons and asteroids are studied with help of space probes that are in high-altitude orbit around the Earth or visit other planets. Observations are also made by space-based telescopes Hubble and the James Webb observatory. The space plasma physics research group SPP at KTH is involved in various projects that utilize direct in-situ measurement by space probes from both, NASA and ESA space missions as well as the observatories mentions. In this context, students have the possibility to participate in real research projects within observational space physics.

In the first project of this context, the focus is on how the generation mechanism of auroral arcs can be studied by observing the space above the aurora by two satellites simultaneously. The project work will be based on data from Earth orbiting research satellites MMS, Cluster and DMSP. MMS and Cluster both consist of four identical spacecraft and orbit through vast regions of the Earth's magnetosphere. The science instruments of MMS can take more precise measurements of the mirco-physics of plasma (charged gas) than any space probe before.

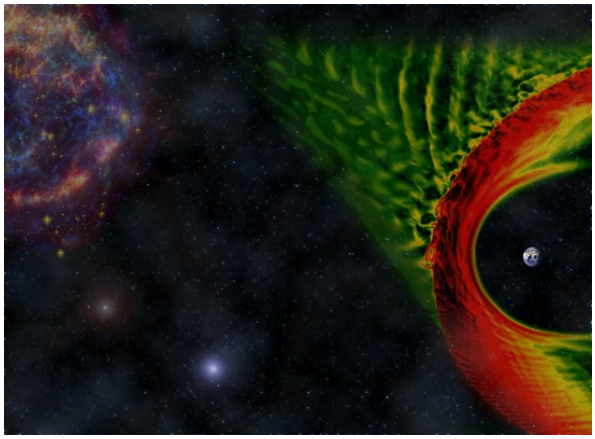
The second project in this context is about the gas giant Saturn. The focus is on the bow shock region created by the interaction between the solar wind and Saturn's large magnetosphere. It uses data from ESA's Cassini spacecraft mission.

Projects 3 and 4 relate to remote observations of the Jupiter system, and include modelling of the Jupiter moons Io and Europa, and their interaction with the Jupiter magnetospheric plasma, and observations of the moon Ganymede and its possible atmosphere. In Project 5 the Hubble space telescope is used to study the outer parts of Earth's atmosphere, the hydrogen-rich geocorona.

In projects 6 and 7 the solar wind (the stream of plasma continuously emitted by the Sun) and its turbulence is studied by the NASA and ESA spacecraft Parker Solar Probe and Solar Orbiter.

Project I1: Search for satellite conjunctions in the magnetospheric source region of auroral arcs

Supervisor: Anita Kullen, kullen@kth.se, Space and Plasma Physics



Aurora forms due to high energy electrons from space hitting the Earth's atmosphere and exciting atoms and molecules there. The high energy electrons are accelerated far out in space on the magnetic flux tubes where strong currents are flowing in plasma (gas of charged particles filling the outer space). Experimentally it has been difficult to identify the exact physical processes far out in space driving the strong currents that later create aurora. However, with the launch of the European Space Agency mission Cluster in 2000 and the NASA MMS mission in 2015 finally, there can be a good possibility to address this question.

Identifying experimentally excellent time periods for deeper studies requires several conditions to be satisfied:

- Cluster and MMS have to be located close to the same flux tube,
- MMS has to be far out in space in the Earth magnetotail where the strongest currents are generated,
- Cluster has to be significantly closer to the Earth to observe the currents driving the aurora,
- all the payload on both MMS and Cluster
- should be operating,
- significant auroral activity should be ongoing.

In this project, the students will analyze Cluster and MMS data and positions to identify the time periods satisfying the conditions above. For the best events, additional work will be carried out to characterize the properties of the current and aurora.

The tasks in this project are:

- Learn Cluster and MMS orbits, magnetic field models, and how to identify time periods when satellites are close to the same field line.
- Learn the payload of Cluster and MMS and how to identify in which mode they are operated.
- Construct a database of events satisfying the conditions above.
- Rank the events based on quality factors defined within the project.
- Characterize a few best events in detail.

In this project, the students will acquire knowledge about space plasma and physical processes in near-Earth space. In addition, the students will learn about spacecraft payload, spacecraft operations, and spacecraft data. The data analysis will be done in MATLAB. The results of the work will be of high importance for further studies by scientists in the space and plasma physics division.

Project I2: Ultralow frequency electromagnetic waves at and behind the Saturn bow shock

Supervisor: Tomas Karlsson, tomask@kth.se, Space and Plasma Physics

The Sun continuously emits a not only light, but also a plasma, containing electrons and protons. This solar wind is highly supersonic, and interacts strongly with planets in the solar system, and their magnetic fields. In this interaction, the solar wind is braked down and forms a shock, similar to that in front of a supersonic airplane. Saturn, one of the outermost planets in the solar system has such a bow shock (Figure 1). During some circumstances strong ultra-low frequency (ULF) electromagnetic waves are formed in front of the bow shock. Figure 2 shows such waves in front of Earth's bow shock. For Saturn this type of ULF waves have been detected, but many of their properties are unknown.

You will use magnetic field measurements from the Cassini spacecraft (https://www.esa.int/Science_Exploration/Space_Science/Cassini-Huygens), which orbited Saturn for over ten years, to identify such ULF waves.

In this project we are primarily interested in answering the following question: can these ULF waves cross the bow shock and also be observed behind it?

In this project you will acquire knowledge about the solar wind and how it interacts with planets. The data analysis will take place in Matlab, partially by using existing programs. The data is readily available from KTH or directly from an international repository (The Planetary Data System). The results will be very useful for future scientific investigations by researchers at KTH and elsewhere in the world.

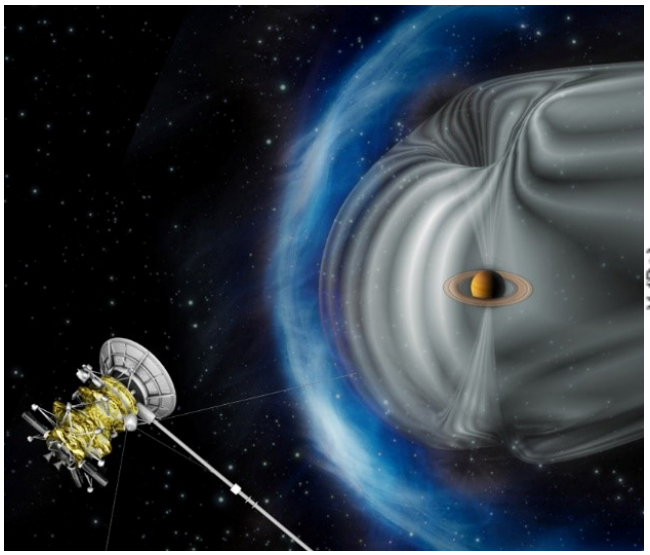


Figure 1. The Cassini spacecraft in front of Saturns's bow shock (Image: ESA).

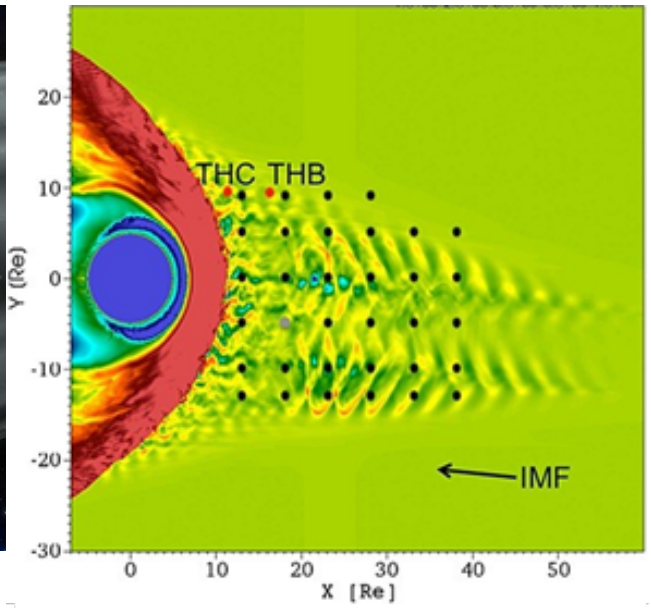


Figure 2. Simulation of ULF waves in front of Earth's bow shock [Turc, 2020]. Also here Earth is at the origin of the plot.

Project I3: Using Jupiter's moons Io and Europa as probes to the plasma torus

Supervisor: Lorenz Roth, lorenzr@kth.se, Space and Plasma Physics

Jupiter is not only the largest planet in the Solar System, but it also possesses the by far strongest magnetic field. Jupiter's vast magnetosphere, i.e., the region dominated by the planet's magnetic field, extends over several astronomical units (AU, distance between Earth and Sun) in the tail and provides a variety of interesting physical phenomena. The magnetosphere is loaded with plasma that stems from the volcanically active moon Io and rotates with the magnetic field in only 10 hours around the planet.

The four large Galilean moons of Jupiter – Io, Europa, Ganymede, and Callisto – revolve around the planet on Keplerian orbits embedded in the fast flow of plasma. When colliding with the moons' atmosphere the plasma particles excite auroral emissions that are often observed from Earth with the Hubble Space Telescope. The brightness of the auroral emissions is a diagnostic for the plasma environment at the time of the observation.

In this project, you will create a model the of the fast-rotating plasma environment of Jupiter and predict the brightness of the aurora at the moons Io and Europa. The predicted brightness is compared to Hubble Space Telescope observations.

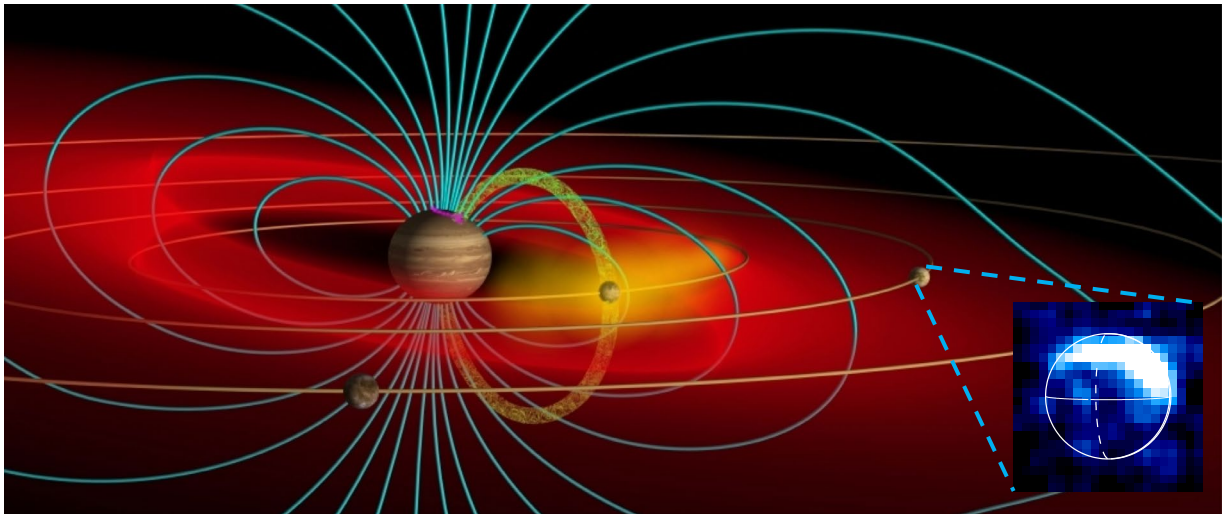


Figure 1. Jupiter is surrounded by a dense sheet of charged particles (plasma, shown in red). The auroral lights from the moons (small picture, Hubble Space Telescope image) can be used to "probe" the plasma (Image credit: J. Spencer).

Steps include:

- Use and improve a code in that describes the distribution of the plasma around Jupiter
- Calculate the plasma density at the moons Io and Europa specific times and geometries
- Relate the density to aurora brightness and compare to Hubble Space Telescope observations

The project is directly related to the NASA *Juno* mission. The *Juno* probe will take several measurements of the plasma near the moon in the coming months!

Project I4: James Webb Space Telescope observations of Jupiter moon Ganymede

Supervisor: Lorenz Roth, lorenzr@kth.se, Space and Plasma Physics

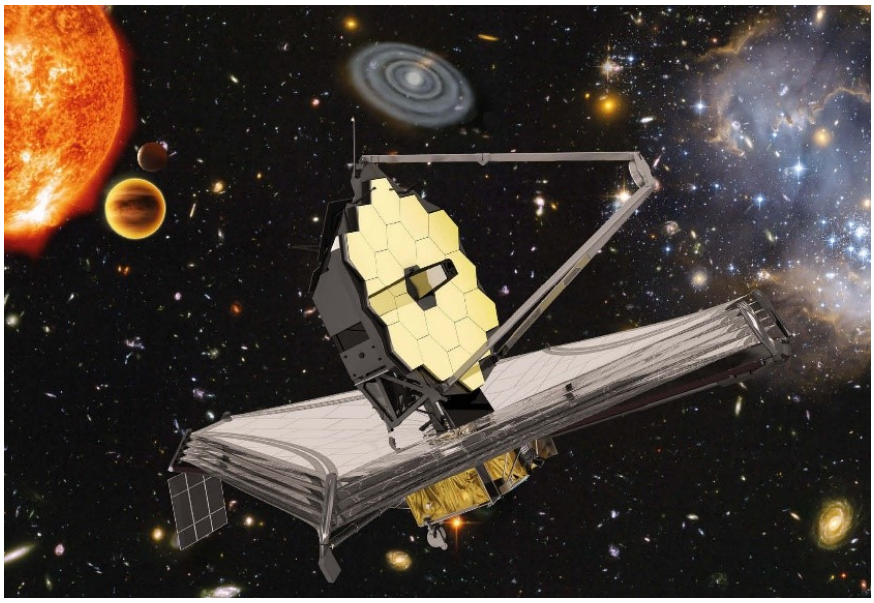


Figure 1.James Webb Space Telescope

The NASA/ESA James Webb Space Telescope (JWST) was successfully launched on Christmas Day last year (2021). After commissioning of the telescope, science observations are taken since July and the large moons of Jupiter are among the first targets for JWST!

The Space and Plasma Physics group at KTH has been involved in an observing program for moon Ganymede. JWST has the unique capabilities to take spectral images with information on wavelength (color) in infrared light (IR) in each pixel (Figure 2). The Ganymede observations have provided many insights into the material of Ganymede's surface in different places. However, so far signals from Ganymede's atmosphere were not found in the data. In this project, you will search for atmosphere signals in the JWST data and calculate what signal might be expected theoretically.

The tasks in this project include:

- Download JWST observations from one of the moons from the NASA data archive
- Read and process the data "cubes" extract infrared spectra and images of the moon
- Interpret the spectra using reference spectra and simple models
- Compare the spectra to previous observations from spacecraft

Doing this project, you will be among the first people actively working with this milestone telescope in the world.

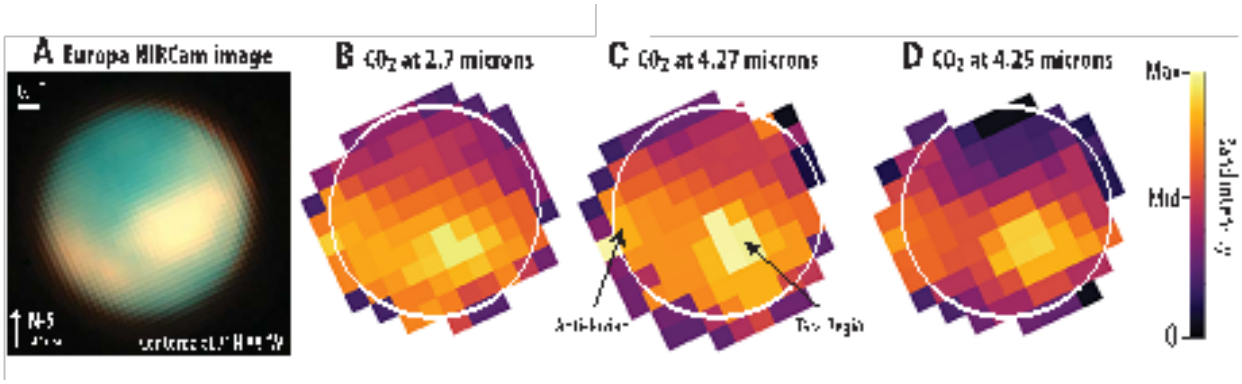


Figure 2. JWST observations of Europa showing CO2 in a special region

Project I5: Investigation of hydrogen corona around Earth with HST

Supervisors: Nickolay Ivchenko, nickolay@kth.se / Lorenz Roth, lorenzr@kth.se, Space and Plasma Physics

The geocorona is the outermost layer of the neutral atmosphere of Earth (labeled “exopshere” in Figure 1). It consists of hydrogen atoms, the lightest of all elements. A recent study has claimed that the top of this outermost layer contains extremely hot hydrogen atoms that populate an even wider space around Earth than thought before. The existence of this hot outer geocorona has however not been independently confirmed yet.

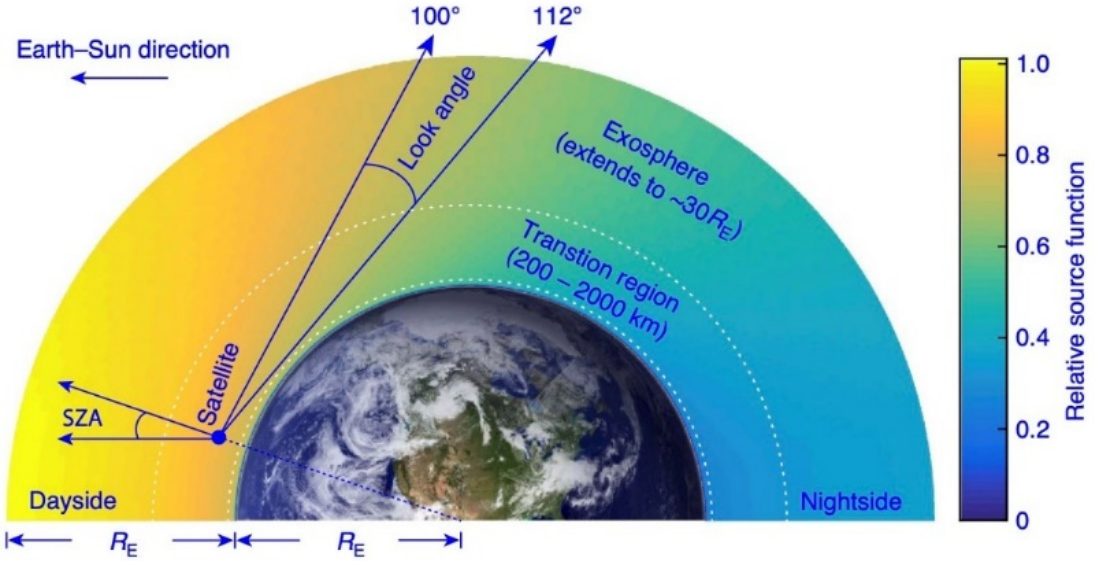


Figure 1: Sketch of the Earth’s upper atmosphere as observed from a space telescope

The Hubble Space Telescope is orbiting the Earth at about 600 km for over 30 years now. In every single observations, HST is looking through the hydrogen geocorona of Earth. Interestingly, the hydrogen geocorona is automatically measured in all far-UV spectral observations that include the wavelength 121.6 nm. In the spectra with highest resolution, the hottest outermost part of the geocorona should appear in the data, separable from the main cooler geocorona.

In this project, you will systematically go through the archive of the Hubble Space Telescope and identify observations that are suitable to search for the geocorona signatures. You will then process the identified observations to extract the relevant signals. Finally, you convert the signal to the values of density and temperature of hydrogen.

Steps include:

- Search the HST archive, identify and download the HST data containing geocorona emissions.
- Process the data and extract the geocorona signal.
- Convert the geocorona signal to hydrogen densities and temperature and compare to the previous detections of the hot outer geocorona.

The project deals with the acclaimed but debated existence of a very hot outer part of our atmosphere. If the hot geocorona is detectable in the HST data, it would constitute an important confirmation of this phenomenon.

Project I6: Radial evolution of solar wind turbulence using multi-spacecraft alignments in the inner heliosphere

Supervisor: Luca Sorriso-Valvo, lucsv@kth.se, Space and Plasma Physics

The inner heliosphere is currently sampled by several spacecraft, whose orbits occasionally result in the alignment of two or more of them along the radial direction from the Sun. Such configurations provide samples of expanding solar wind at different distances from the Sun, enabling us to evaluate the radial evolution of various properties. For this project, the student will use measurements collected during one or more radial alignments of spacecraft in the inner heliosphere, such as Solar Orbiter, Parker Solar Probe, BepiColombo or missions near the Earth (Wind). The accurate determination of the solar source region will be used to convalidate the effective radial alignment.

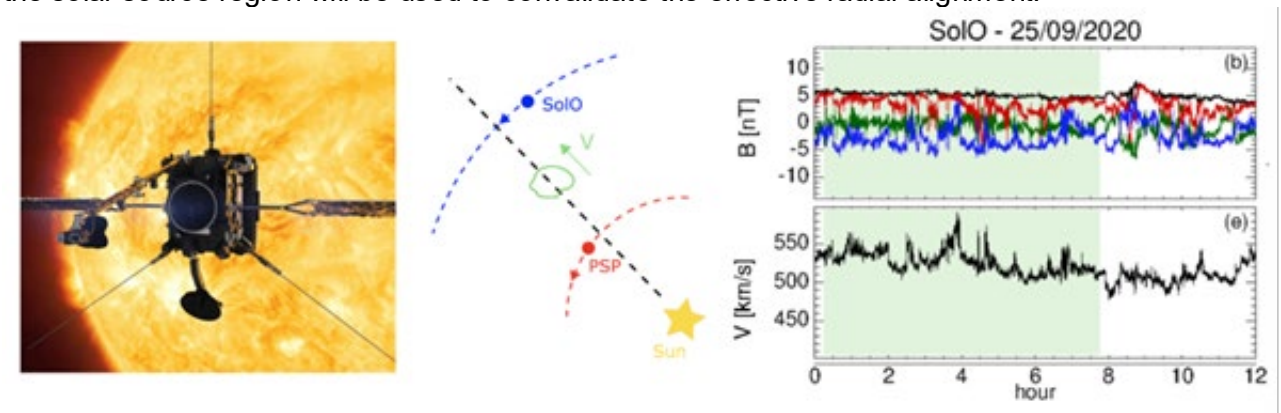


Figure 1. Left: representation of Solar Orbiter facing the Sun. Center: schematics of radial alignment between Solar Orbiter and Parker Solar Probe measuring the same wind parcel. Right: velocity (bottom) and magnetic field (top) by Solar Orbiter.

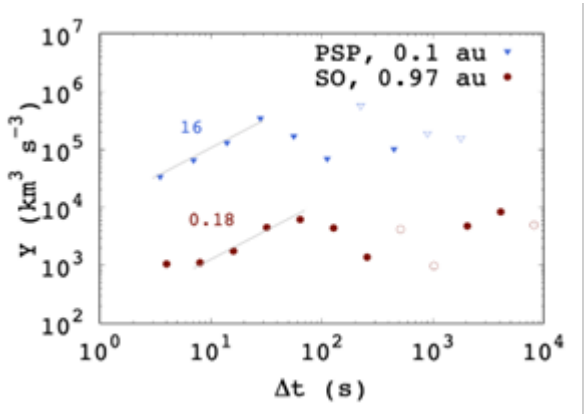


Figure 2. Scaling laws for the total energy at Solar Orbiter and at Parker Solar Probe during a radial alignment

A comprehensive analysis of the turbulent statistical properties of the fields and plasma fluctuations will be complemented with estimates of the turbulent energy transfer rate, based on different versions of the third-order moment scaling laws. The radial decay of the turbulent energy will be thus determined and compared with the measured solar wind heating, providing crucial information about the global energy budget of the solar wind in its expansion in the heliosphere.

Possible questions to be addressed include:

1. Do the selected intervals show typical and measurable characteristics of turbulence?
2. Does the solar wind turbulence evolve as it expands from the Sun?
3. Is the energy dissipated by the turbulence sufficient to heat the solar wind to the observed temperature?

In this project, the students will learn basic concepts of space plasma turbulence. They will acquire competences in obtaining, managing and analyzing spacecraft data, and interpreting the observations of statistical analysis. The analysis will be performed using a programming language of choice. The work will be a preliminary study for further research by KTH scientists.

Project I7: Scaling law for the cross-helicity in solar wind turbulence

Supervisor: Luca Sorriso-Valvo, lucsv@kth.se, Space and Plasma Physics

The turbulent dynamics of the solar wind plasmas at fluid scales conserves the total energy and the global cross-helicity, namely, the degree of correlation between magnetic and velocity fluctuations, typical of space plasmas. Both quantities are important ingredients of the dynamical expansion of the solar wind, and their radial evolutions are key parameters of heliospheric models.
Exact mathematical scaling relations describe the transfer of such conserved quantities from large-scale to small-scale fluctuations, which is the result of the turbulent nonlinear interactions. The theoretical predictions for the energy transfer scaling laws have been validated in numerical simulations and in solar wind data, obtaining estimates of the rate of turbulent energy dissipation. However, the cross-helicity scaling laws has been only validated in numerical simulations, but never in solar wind data.

For this project, the students will use intervals of solar wind parameters measurements from spacecraft such as Solar Orbiter and/or Parker Solar Probe to validate the turbulence scaling law for the cross-helicity, estimate the cross-helicity dissipation rate, and compare samples with different wind characteristics. The students will select some intervals from one or more spacecraft databases, determine the solar wind characteristics (in particular the wind speed and the degree of correlation between magnetic field and velocity), and perform statistical analysis of the data.

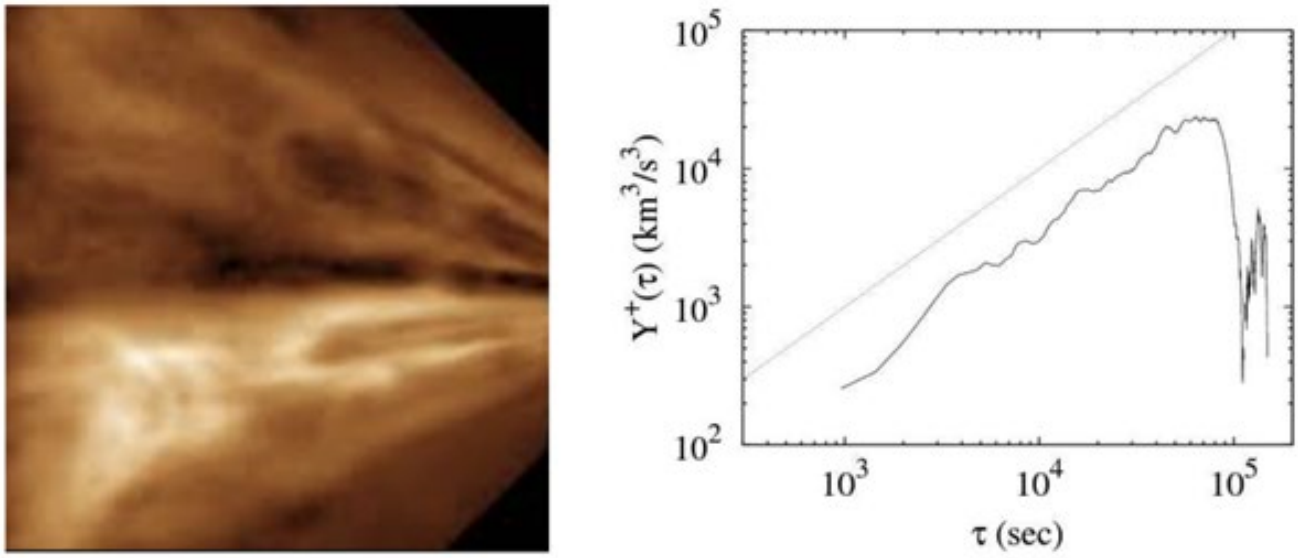


Figure 1. Left: an image of the solar wind in the proximity of the Sun, obtained by the THEMIS spacecraft. Right: linear scaling law for the total energy in fast solar wind turbulence using Ulysses measurements.

The main questions that will be addressed are:

1. Is the cross-helicity scaling law valid in solar wind plasmas?
2. What is the cross-helicity dissipation rate in the solar wind?
3. How does the cross-helicity scaling and dissipation depend on the solar wind parameters?

In this project, the students will learn basic concepts of space plasma turbulence. They will acquire competences in obtaining, managing and analyzing spacecraft data, and interpreting the observations of statistical analysis. The analysis will be performed using a programming language of choice. The work will be a preliminary study for further research by KTH scientists.

Context J: Fixed wing UAV for space and environment monitoring

Figure: ALPHA UAV developed and built at KTH in 2022.

Introduction

Our understanding of the environment of the Earth, with its upper atmosphere and the space beyond, comes from observations from the ground, satellites, sounding rockets and, more recently, unmanned vehicles (UAVs). Several projects aimed at development and validation of custom-designed fixed wing UAVs for various applications (to observe the upper atmosphere and the terrain on the ground) are ongoing at KTH (see https://www.kthaero.com/). This context takes up engineering projects related to the UAV development.

Four projects are offered in this context, all relating to ongoing activities at KTH.

Project J1: Flight testing of fixed wing UAVs

Supervisors: Nickolay Ivchenko, nickolay@kth.se, Space and Plasma Physics
Raffaello Mariani, rmariani@kth.se, Aeronautics and Vehicle Engineering.

In this project you will focus on the autonomous flight control system for the fixed wing UAVs. Today a number of open source “autopilot” software solutions are available, that use multiple sensors onboard the UAV together with a control loop to steer the main engines and control surfaces. This way a “stabilized” flight – or even fully autonomous mission – can be achieved. In order to reliably use the UAVs a substantial amount of flight testing is required, to characterize the aerodynamical performance of UAV and validate the function of the autopilot (including response to non-nominal situations). Several different UAVs at KTH use similar approach, with Ardupilot used as the flight software. This project aims at developing a systematic process of flight testing of the UAVs, that can be applied across the platforms.

The tasks in this project include:

- Getting familiar with the basics of flight
- Understanding the basics of the fixed wing UAV control
- Getting familiar with the open source autopilot (Ardupilot)
- Flying the UAVs in various modes
- Analyzing the flight data to determine the performance of the UAV.

Figure J1. Early flight testing of a fixed wing UAV by KTH students.

Project J2: Optimisatino of a UAV solar power system

Supervisor: Nickolay Ivchenko, nickolay@kth.se , Space and Plasma Physics

Integration of solar power in a UAV system promises significant increase of the flight duration, up to perpetual flight. The new project, in which a dedicated UAV is being custom designed for forest fire detection aims at being able to fly during the daytime (i.e. when illuminated by the sun).
Integration of the solar cells with the electrical power system of the UAV requires addressing a number of issues. To harvest maximum power from the solar panels with varying illumination conditions, a dynamically adjusted maximum power point tracker (MPPT) is needed. It should also be seamlessly integrated with the battery management system (charging/discharging). Integrated measurement of currents/voltages allows for a more advanced and intelligent power handling system. Considering that the system is to be implemented on a flying platform, the solution should be mechanically and thermally robust, and lightweight. A prototype system was developed within a BSc thesis during 2023, which needs to be optimised for performance and integration with the UAV.

The tasks in this project include:

- Getting familiar with the prototype system
- Optimising the design of the system
- Implementing the design in a PCB
- Conducting the tests of the design

Project J3: Thermal control for the ALPHA UAV

Supervisor: Nickolay Ivchenko, nickolay@kth.se , Space and Plasma Physics

In this project you will consider the challenge of maintaining the subsystems and the payload of the ALPHA UAV within their designated operational temperature range during high-altitude flight.

The tasks in this project include:

- Understanding the thermal requirements of various subsystems of the ALPHA UAV
- Understanding the heat transfer processes at work in the system
- Constructing a simple thermal model of the UAV
- Designing a prototype of the thermal control system and experimentally validating it.

Project J4: Detecting smoke plumes from airborne images

Supervisor: Nickolay Ivchenko, nickolay@kth.se, Space and Plasma Physics

This project focuses on the analysis of the images acquired from the UAV. The detection of the smoke plumes relies both on the morphology/appearance and the motion of the plume between subsequent images. While the partner company, EVSolutions, has an extensive experience with the stationary vantage point imaging, the UAV imaging poses a number of challenges. Due to the motion of the UAV, the view of the scene is changing related to the perspective change.

The tasks in this project include:

- Generating a model perspective view with terrain lines (horizon/ridge lines) from the position and look direction of the camera
- Aligning the actual image with the model image, with the purpose of being able to georeferenced each pixel in the image
- Determining the errors in the alignment above, and finding whether more accurate alignment can be achieved from the image itself
- Determining whether the motion within the scene can be detected within a moving scene (due to the UAV motion)

The EVSolution can provide sample imaging from their system, either from ground towers or from airplane tests.

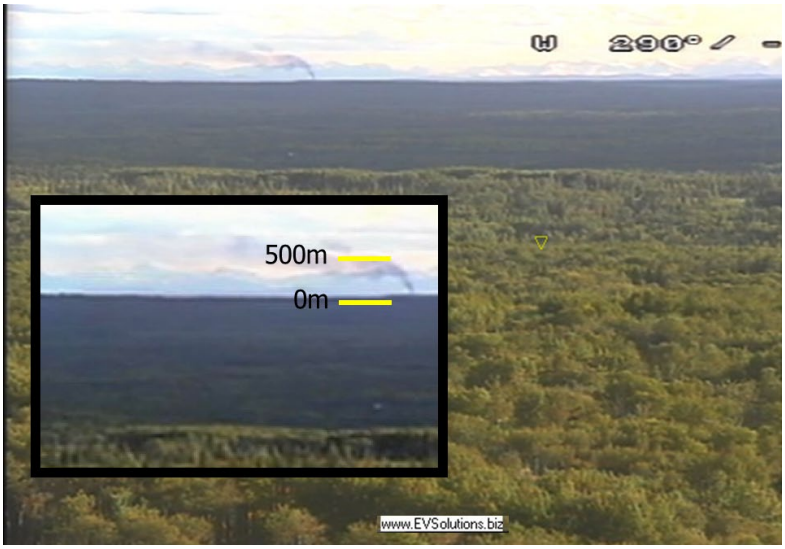


Figure J4 . An example of the smoke plume from a forest fire [EVSolutions].

Context K: Artificial Intelligence and the Internet of Things

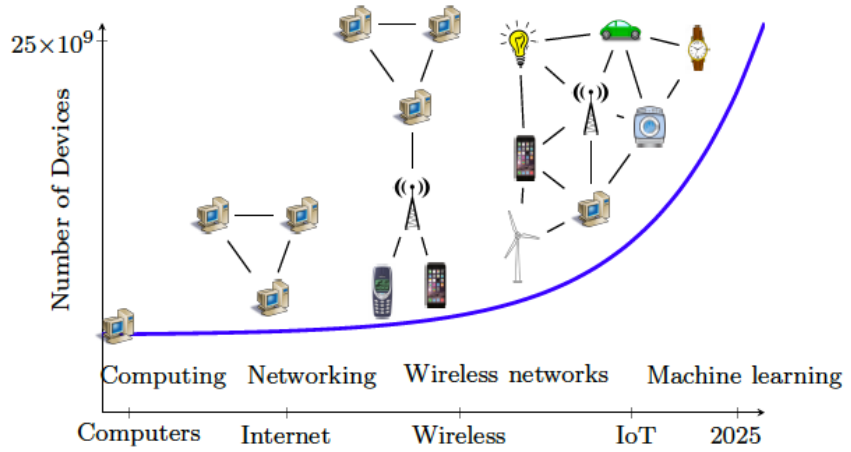


Figure 1: *Four technological revolutions: Computers, Internet, Wireless Phones, and Internet of Things (IoT) or "the all-connected and digitalized world". With future wireless networks and IoT, any system or object that can be connected via communication networks will become "intelligent". An essential part of the "intelligence" is machine learning.*

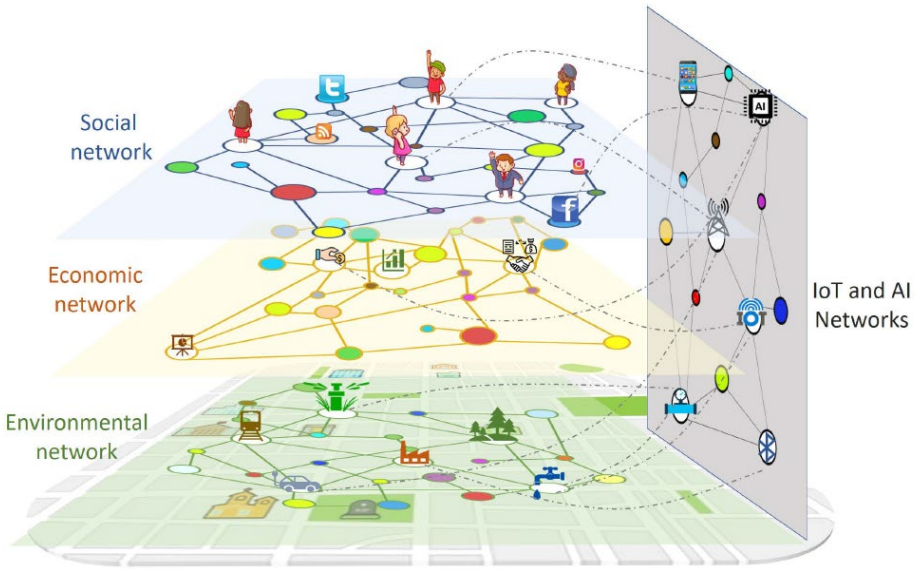


Figure 2: *Machine learning in communication networks with distributed nodes and data sets will face formidable challenges, due to the size of local data sets, limited computation and energy and narrow bandwidth of the nodes, heterogeneity of communication protocols, privacy, and security. Distributed machine learning is conceived for high performing networks of processors (often in data centres), and not for "the connected world".*

In the past decades, we have seen a series of computing–information-communication revolutions that started with computers, followed by computer networking, and up to wireless networks (see Figure 1). We are now at the onset of the fourth revolution: "the all-connected and digitalized world", where networks will bring automatic data analysis and decision making in any object, transforming it into an "intelligent" system (see Figure 2). Current predictions specify that, around 2030, the number of networked objects will be around 100 billions and that the fourth revolution has the potentiality to create a new multi-trillion economy. One of the main characteristics of the fourth revolution is the huge data generation. It appears that the last recent years have produced 90% of the world's data available up to now, especially due to devices such as sensors in Internet of Things (IoT) or smart phones.

Such wealth of data is forcefully motivating the development of intelligent data analysis methods, namely Machine Learning (ML) and Artificial Intelligence (AI). Thanks to AI, speech recognition and automatic text entry can be performed, or good photos are automatically selected by smart phones, or cars see and avoid obstacles. To achieve such impressive results, machine learning needs big datasets and very huge computational and communication resources. For example, the Google AlphaGo has been trained with around 30 million possible moves to beat a Go grand champion. However, in the fourth technological revolution, data sets of any size will be distributed among several networked nodes (people, devices, objects, or machines) that might not be able to perform the computations and to share data. Existing AI methods are mostly intended for proprietary or high performing networks (e.g., in data centres), and would greatly stress communication networks such as IoT and 5-6G wireless networks. When we perform AI over IoT, we have fundamentally new technological challenges in terms of **distributed data sets, bandwidth, or heterogeneous protocols.**

One major issue to apply AI over communication networks is **the fundamental bandwidth limitations**. The huge number of nodes and their data sets transmissions may congest the practically available bandwidth. The emerging technology of extremely low latency communications, will rely on short packets that carry few bits. Techno-economical forecasts indicate that, in the coming years, IoT systems such as smart grids or smart cities will be mostly served by narrow band IoT. For example, to monitor and control water distribution lines, an IoT network will be underground and underwater, where the nature of the communication channels gives low data rates with unreliable links and delays. Communications within the human body can rely only on few bits per second. The nodes generating data may not have enough communication bandwidth to transmit data where it has to be analyzed, or simply not enough computational power to perform local analysis.

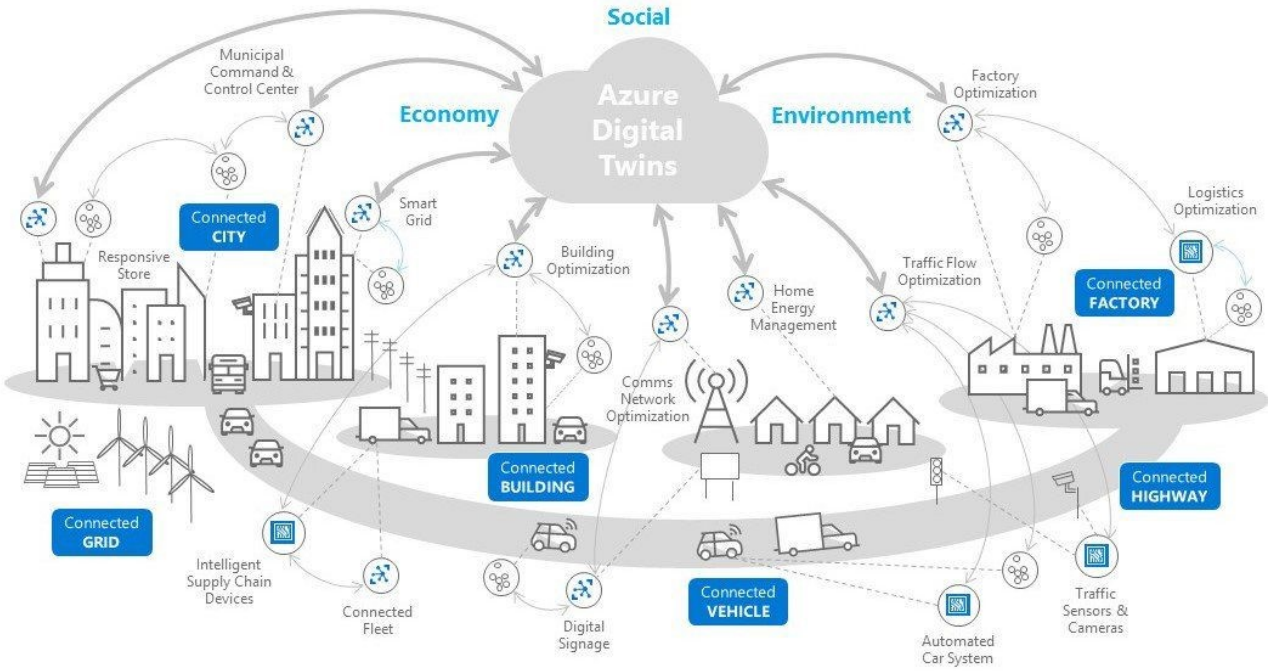
In this Bachelor Thesis context, you will study a subset of exciting topics within Artificial Intelligence and IoT (AIoT):

- Communication-Efficient Federated Learning over IoT Systems
- Distributed Computing Using Matrix Factorization
- Distributed Machine Learning over Time-Varying Channels
- Model Drift in Federated Learning
- Machine Learning for Fast Beam Alignment in Intelligent Reflecting Surface-Aided Communications
- Enhancing Edge Computing Through Over-the-Air Computation
- Enhancing Security and Privacy in Over-the-Air Computation
- Distributed Machine Learning over IoT
- Proximal Gradient Methods with Dual Decomposition for Distributed Consensus Optimization

We describe in the projects in the detail in the following pages.

Project K1: Communication-Efficient Federated Learning over IoT Systems

Supervisors: Seyedsaeed Razavikia (sraz@kth.se), Carlo Fischione (carlofi@kth.se)



In federated learning, deepening our understanding of distributed and decentralized algorithms is vital, especially when compared to their centralized counterparts. There is a lack of detailed knowledge about these algorithms, especially when considering the communication delays that occur in distributed datasets within IoT networks.

This project proposes a detailed study of the ML training algorithms used across IoT nodes. The focus will be on understanding the relationship between the convergence rates of these algorithms and the communication dynamics between nodes. The study will involve a thorough review of recent literature, along with simulations of different scenarios and possible theoretical analyses.

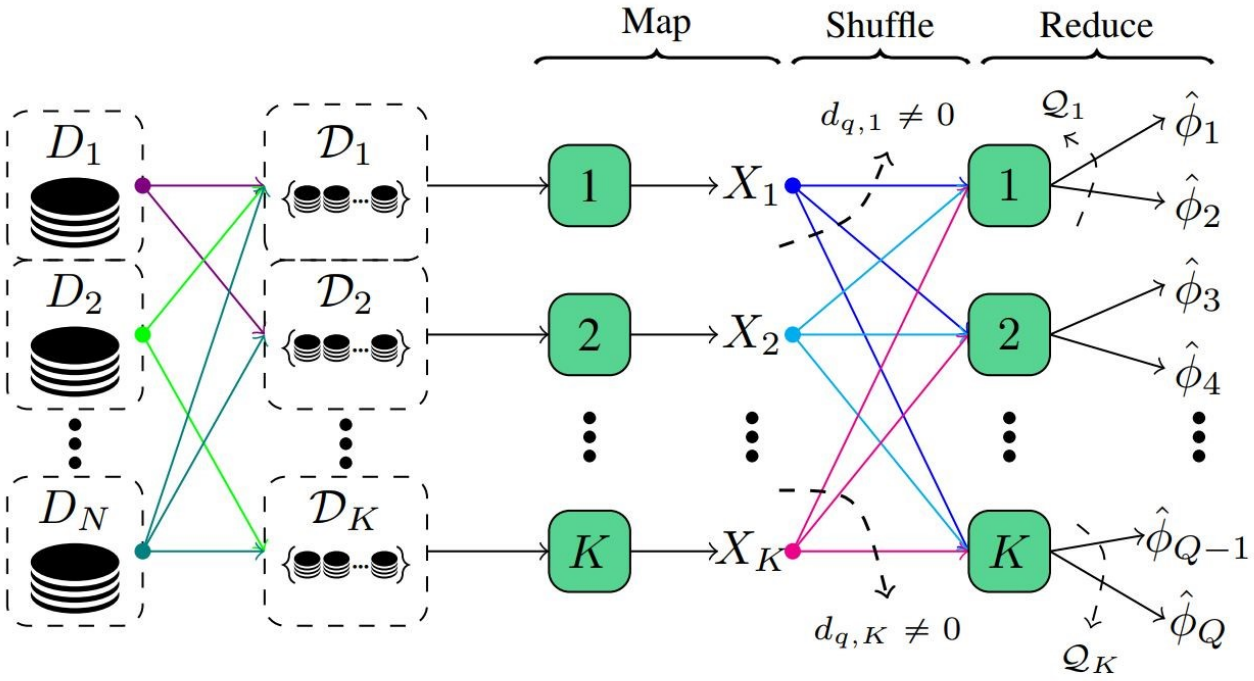
One of the main challenges to address is the varied data types across nodes, which can lead to unbalanced learning models. Developing advanced algorithms that can effectively combine different data sets is essential. At the same time, improving communication efficiency is a critical requirement. This involves updating current communication protocols to allow quicker data transmission and reduce delays, optimizing the federated learning process.

Furthermore, the project requires the development of an algorithm that aligns with existing communication system protocols. This step is necessary to ensure the solutions are practically applicable and scalable, allowing for easy integration with current infrastructures and speeding up real-world deployment.

In conclusion, this research aims to explore the effects of communication networks on the performance of distributed optimization algorithms used in ML training. The anticipated results will offer insights into the opportunities and challenges of using ML over real-life communication networks, promoting significant improvements in federated learning approaches.

Project K2: Distributed Computing Using Matrix Factorization

Supervisors: Seyedsaeed Razavikia (sraz@kth.se), Carlo Fischione (carlofi@kth.se)



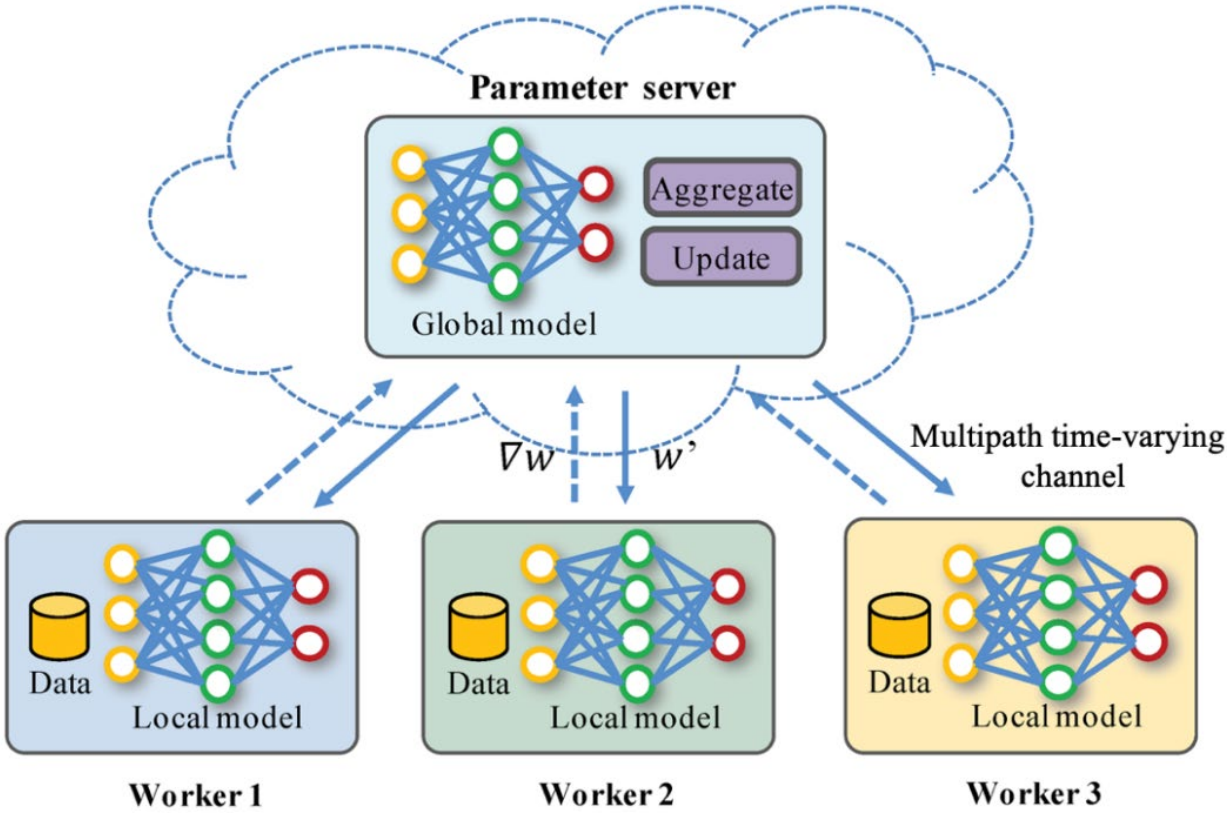
Distributed computing, which divides large-scale computations into subtasks assigned to various computing nodes, has reduced computation time, notably in machine learning and deep learning domains. MapReduce is a prevalent framework facilitating this, which operates through three stages: Map, Shuffle, and Reduce. This framework has applications in diverse fields, including machine learning and bioinformatics.

However, the existing frameworks encounter bottlenecks, particularly during the Shuffle step, where communication costs can significantly impede system performance, especially when communication resources are limited. Current solutions, primarily coding schemes, have been developed to address this, but they often increase computation costs, creating another bottleneck in the system. Moreover, straggler nodes, which take longer to complete tasks, add to the latency in total computation time.

This proposal explores and addresses these challenges by focusing on the trade-off between computation and communication costs in distributed systems. It intends to delve into the computation of linearly separable functions over finite fields, a concept that is central to various computation schemes including distributed gradient coding and matrix multiplication. The goal is to optimize the network layout for computing linearly separable functions, considering matrix factorization over finite fields and beyond, to enhance communication and computation efficiency in distributed computing frameworks. This initiative aims to foster advancements in distributed computing, paving the way for more efficient and scalable systems.

Project K3: Distributed Machine Learning Over Time-Varying Channels

Supervisors: Xinyu Huang (xinyh@kth.se), Carlo Fischione (carlofi@kth.se)



The Internet of Things (IoT) revolution promises a future with an extensive array of mobile devices working together to drive applications like smart cities and edge artificial intelligence (AI). With this surge in IoT integration, a very large amount of data is generated and the computing is spread from the cloud toward the network edge, which enables the deployment of machine learning (ML) algorithms in the proximity of edge devices. This paradigm shift means that the classical centralized ML approach requiring large training datasets is no longer dominant. There is a growing need for novel distributed ML solutions that can leverage rich distributed data and computation resources at the edge without the need for transporting data across the network. Under data privacy considerations, edge devices train the network locally and only forward local network parameters to the cloud.

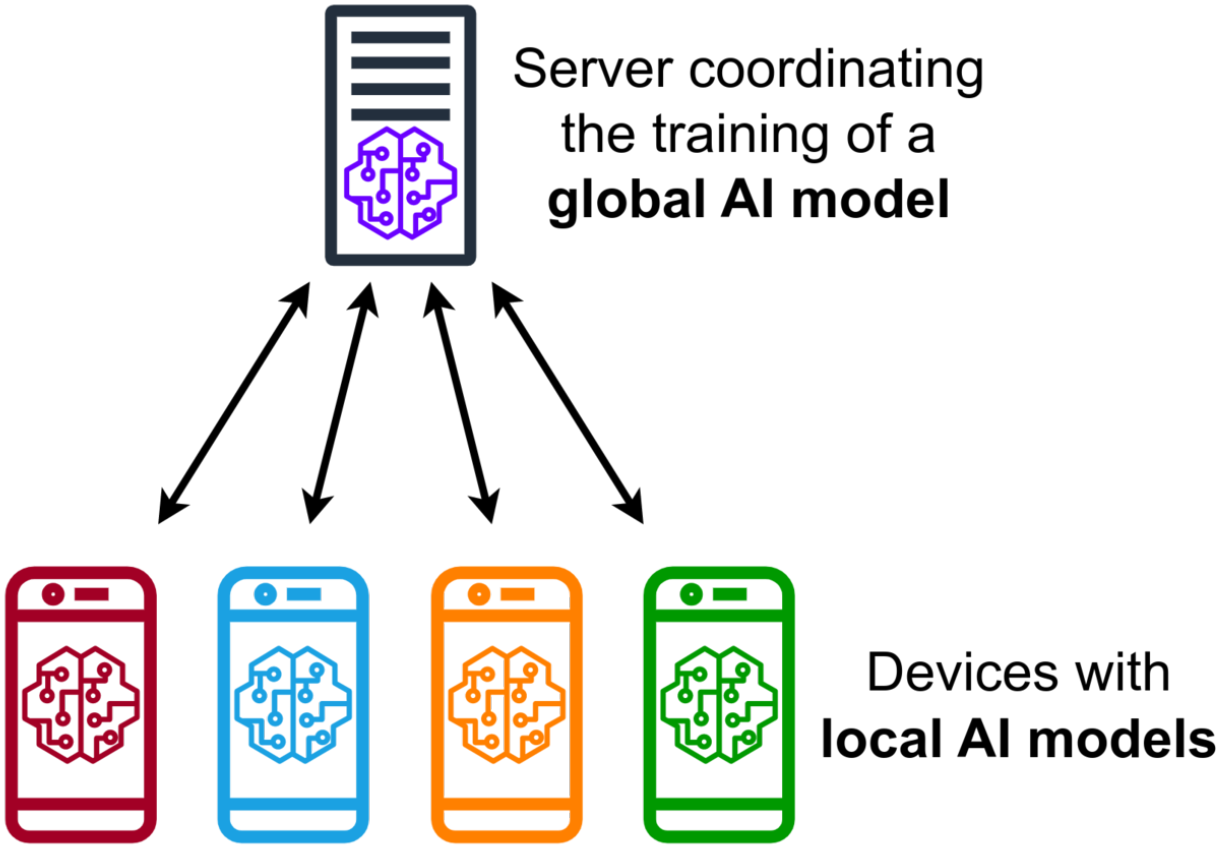
Integrating distributed ML into the next-generation of wireless networks not only challenges us to develop efficient learning algorithms but also to create robust wireless transmission methods, especially for time-varying channels in high-mobility scenarios, such as high-speed trains or unmanned aerial vehicles. These scenarios introduce inter-carrier interference, negatively impacting distributed ML's performance.

In this project, first, we will consider a noise-free channel and train algorithms of ML with distributed data sets across the nodes of the IoT. Second, we will consider a high-mobility channel and investigate how the time-varying channel would impact the convergence rate of distributed ML algorithms. This project includes a study of the latest literature, combined with simulations of different scenarios and possibly theoretical studies.

This project aims at understanding double-selective time-varying channels and the effects of communication networks on the performance of distributed ML algorithms. The results can help to understand the potential and difficulties of deploying ML over real-life communication networks.

Project K4: Model Drift in Federated Learning

Supervisors: Henrik Hellström (hhells@kth.se, hhells@stanford.edu), Carlo Fischione (carlofi@kth.se)



Federated Learning (FL) is a distributed machine learning approach, which was first proposed in 2016 by researchers at Google. Since then, the approach has quickly gained popularity for training deep neural networks using decentralized data. In fact, your smartphone is likely running an FL algorithm to predict traffic patterns for Google Maps or to offer word suggestions when you use text-based applications.

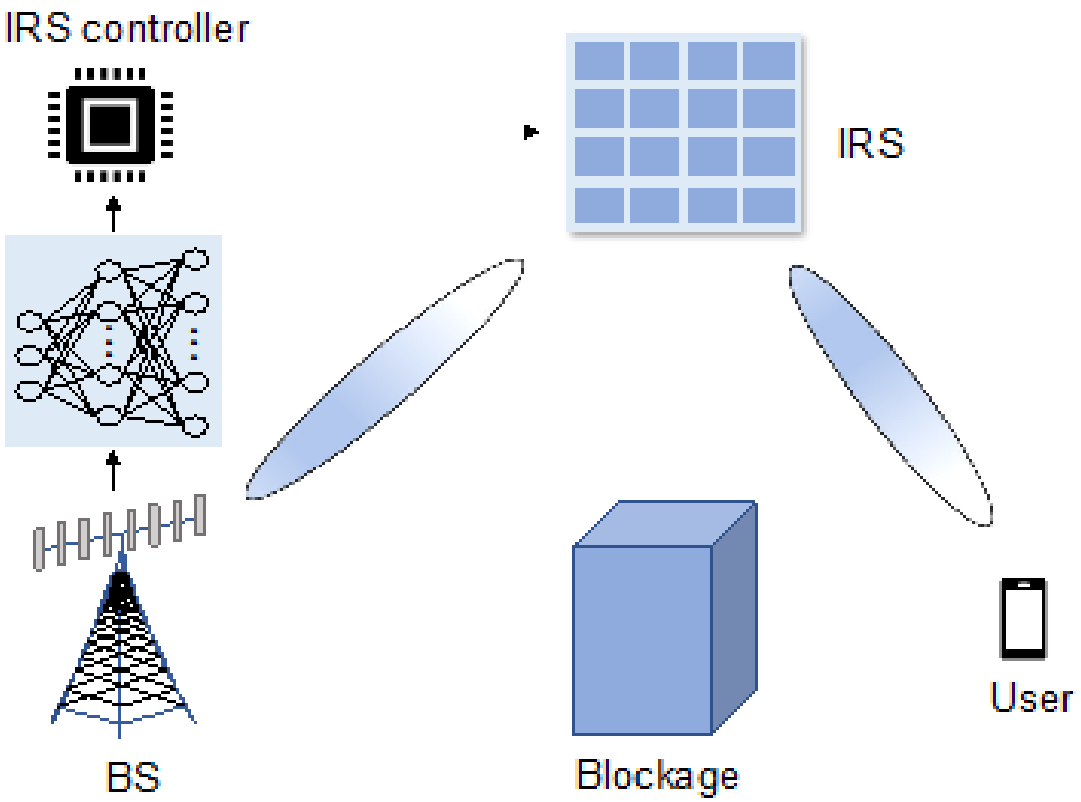
Compared to more traditional distributed methods, such as distributed gradient descent, FL offers significantly higher communication efficiency. The workhorse behind this efficiency is the concept of a communication round. Rather than communicating every gradient to the server, devices operating under FL perform many local iterations of gradient descent before communicating the cumulative result to the server. While efficient, this process also causes a problem known as model drift. In particular, as the devices are running multiple local iterations, their models are becoming increasingly specialized for their dataset. This is not desired, since we are interested in training a model that work for the global dataset of all participating devices. In this bachelor thesis, we wish to evaluate the performance impact of performance drift.

To perform this evaluation, the student(s) will simulate a complete Federated Learning system that trains an image classifier using image data distributed over many devices. In the simulation, the "devices" will be present in the same machine, i.e., the simulator should be able to run on one PC or, preferably, on Google Colab. Once the simulator is complete, the student(s) will perform experiments to evaluate model drift.

Image source:
https://commons.wikimedia.org/wiki/File:Centralized_federated_learning_protocol.png

Project K5: Machine Learning for Fast Beam Alignment in Intelligent Reflecting Surface-Aided Communications

Supervisors: Chen Chen (C.Chen77@liverpool.ac.uk), Carlo Fischione (carlofi@kth.se)



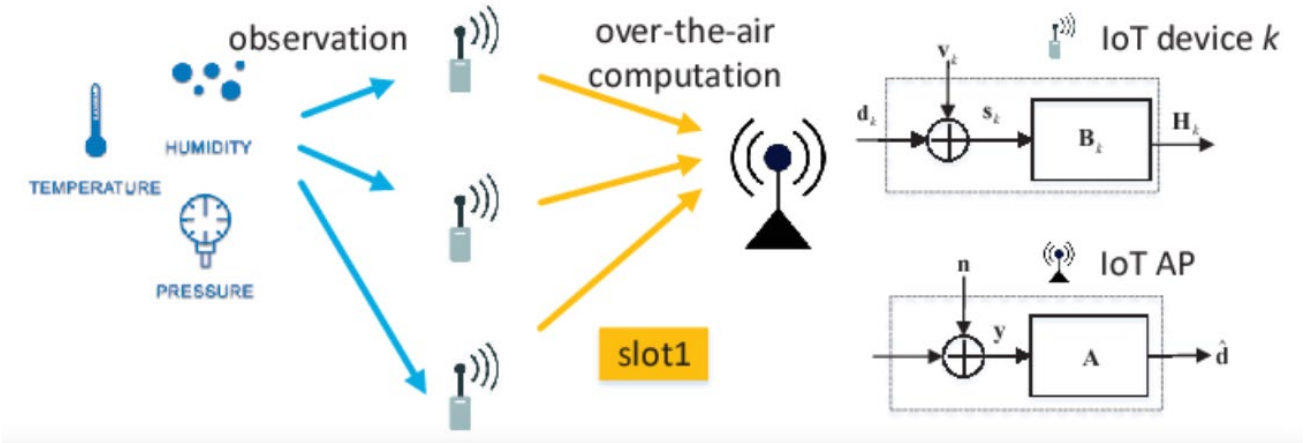
Future data-hungry 6G applications such as holographic telepresence, wireless extended reality, and autonomous vehicles are expected to be supported by higher frequency bands, e.g., millimeter wave and terahertz bands. However, these bands suffer from high penetration loss through blockages. To this end, intelligent reflecting surface (IRS) can be used to establish line-of-sight reflection links, thereby ensuring reliable communications. This requires efficient beam alignment to identify the optimal beams at the base station (BS) and the IRS to maximize the achievable communication rate.

Conventional beam alignment methods require a large beam training overhead, especially in IRS-aided communication systems with a large number of IRS elements. The challenge of this project is to consider the trade-off between communication rate and beam training overhead, and understand the impact of different system parameters on beam alignment. This would include a study of the state-of-art work, combined with simulations of different scenarios and various machine learning algorithms.

This project aims at developing a novel machine learning-based scheme to achieve a good beam alignment performance with a small amount of beam training overhead in IRS-aided communications.

Project K6: Enhancing Edge Computing Through Over-the-Air Computation

Supervisors: Xiaojing Yan (xiay@kth.se), Carlo Fischione (carlofi@kth.se)



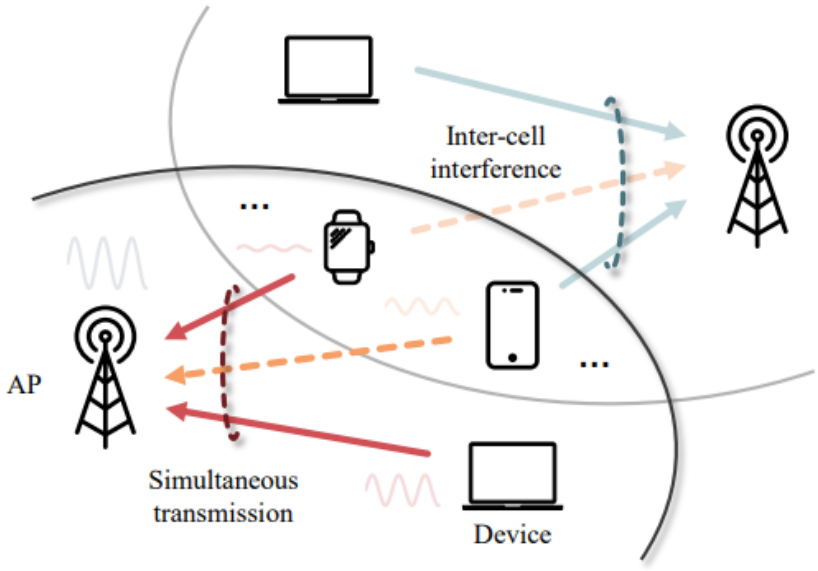
In the current landscape of the Internet of Things (IoT) and the escalating reliance on edge computing, the effective utilization of computing resources at the network's periphery has assumed paramount importance. A nascent paradigm known as over-the-air computation has emerged, enabling devices to delegate computation tasks to proximate edge nodes or interconnected devices.

While over-the-air computation holds great promise for revolutionizing edge computing in IoT environments, several critical challenges need to be addressed to fully unlock its potential. The central query that propels this research forward is: How can over-the-air computation be harnessed to elevate the efficiency and performance of edge computing in IoT and other decentralized environments?

Addressing these challenges requires a multidisciplinary approach that combines expertise in wireless communication, optimization theory, security protocols, real-time systems, and distributed computing. Additionally, practical implementations and extensive experimental validation will be essential to demonstrate the viability and effectiveness of proposed solutions in real-world scenarios. This project aims to tackle these challenges head-on, contributing to the advancement of over-the-air computation for edge computing in IoT environments.

Project K7: Enhancing Security and Privacy in Over-the-Air Computation

Supervisors: Xiaojing Yan (xiay@kth.se), Carlo Fischione (carlofi@kth.se)



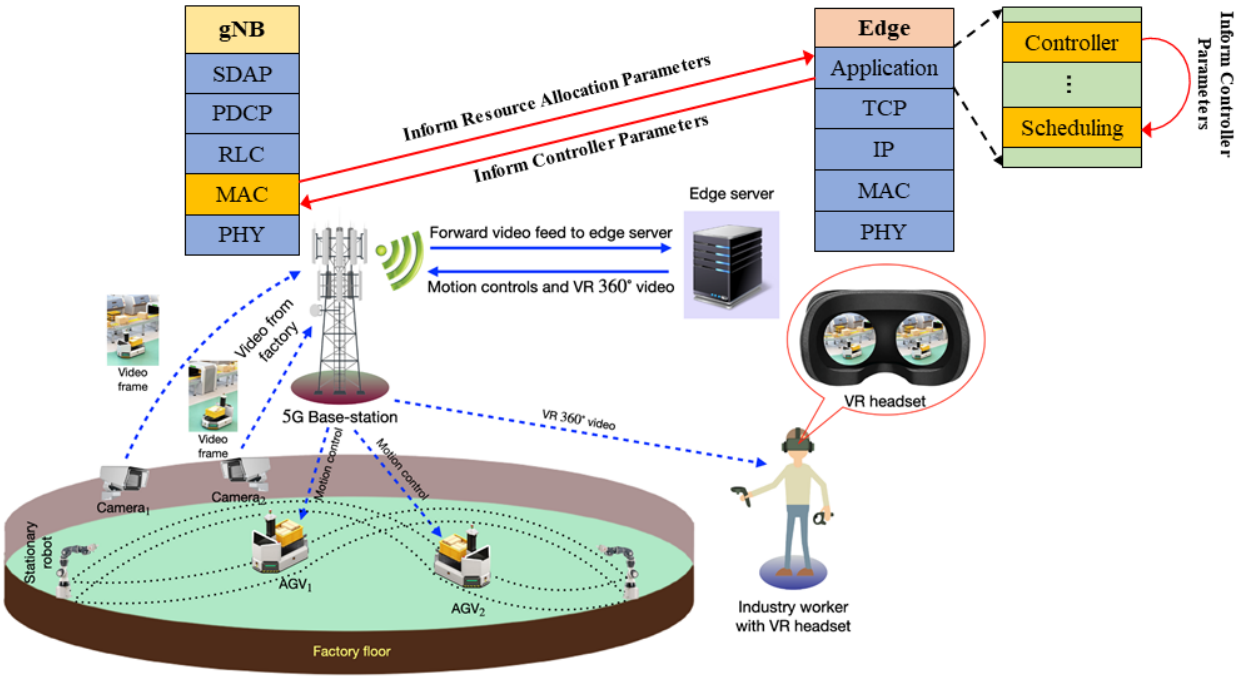
The emergence of Over-the-Air Computation marks a significant leap in distributed computing. However, this progress brings forth critical concerns surrounding security and privacy. Preserving the confidentiality and integrity of data throughout computation processes stands as a paramount objective.

The central inquiry guiding this research endeavor is: How can security and privacy be fortified in over-the-air computation environments to safeguard sensitive information during distributed computations? Developing robust security measures to mitigate these risks is imperative.

The project aims at conducting a thorough analysis of security vulnerabilities specific to over-the-air computation systems. This includes identifying potential attack vectors and formulating mitigation strategies. By addressing these challenges and achieving the stated objectives, this research project can significantly advance the field of over-the-air computation while ensuring robust security and privacy measures are in place for its practical implementation in IoT and distributed computing environments.

Project K8: Distributed Machine Learning over IoT

Supervisors: Sourav Dutta (sourav.dutta.iitkgp@gamil.com), Carlo Fischione (carlofi@kth.se)



Schematic diagram of our system

Industry 4.0 is one of the important application for 6G. In Industry 4.0, three crucial components determine its functionality: application layer scheduling for data generation, the edge server controller function, and the communication system linking them. Traditionally, the IoT devices generates, network schedulers allocate resources to send this traffic to the edge server based on QoS, and the edge server controller uses received data to control the automated industry floor. However, these processes are highly interdependent and require joint execution for optimal industrial IoT leveraging in a 6G network. Existing studies have analyzed network-controlled systems with communication constraints, but haven't explored this interdependency.

The challenge of this project is to solve the resource allocation of 6G networks, traffic generation by the IoT device, and network control system at the edge. This would include a study of the latest literature, combined with simulations of different scenarios and possibly theoretical solution using machine learning.

The overarching goal of this project is to gain a comprehensive understanding of the interdependencies among resource allocation in 6G networks, data traffic generation by IoT devices, and the network control systems at the edge, particularly in the context of Industry 4.0. The outcomes of this research allows enhancing supportability of Industry 4.0 applications and devices within the 6G networks.

Project K9: Proximal Gradient Methods with Dual Decomposition for Distributed Consensus Optimization

Supervisors: Hansi Abeynanda (hkab@kth.se), Carlo Fischione (carlofi@kth.se)

Distributed optimization plays an important role in many application domains, including signal processing, machine learning, robotics, and telecommunications, among others [1] [2] [3] [4]. The challenges, such as existing large data sets, huge problem dimensionality, and geographical distribution of data have created revived interest in the development of novel distributed optimization techniques. One commonly used class of distributed algorithms involves dual decomposition methods coupled with standard gradient descent. However, it is worth exploring alternative approaches that might yield better convergence rates.
This project aims to develop distributed algorithms based on proximal methods [5] with dual decomposition. More importantly, we aim to analyze the algorithms in solving the distributed consensus optimization problem that is commonly used in many types of large-scale signal processing and machine learning applications.

Specifically, the main objectives of this study are as follows:

- Analyze the existing distributed optimization techniques that are widely used in distributed optimization settings.
- Propose distributed algorithms based on the proximal methods with dual decomposition.
- Analyze the convergence properties of proposed algorithms.

[1] D. P. Palomar and Y. C. Eldar, Convex Optimization in Signal Processing and Communications, Cambridge University Press, 2010.
[2] H. Hellström, J. M. B. da Silva Jr., M. M. Amiri, M. Chen, V. Fodor, H. V. Poor and C. Fischione, Wireless for Machine Learning: A Survey, Now Foundations and Trends, 2022.
[3] T. Yang, X. Yi, J. Wu, Y. Yuan, D. Wu, Z. Meng, Y. Hong, H. Wang, Z. Lin and K. H. Johansson, "A survey of distributed optimization," Annual Reviews in Control, vol. 47, p. 278–305, 2019.
[4] A. Nedić and A. Ozdaglar, "Distributed Subgradient Methods for Multi-Agent Optimization," IEEE Transactions on Automatic Control, vol. 54, no. 1, pp. 48-61, 2009.
[5] N. Parikh and S. Boyd, "Proximal Algorithms," Foundations and Trends in Optimization, vol. 1, no. 3, p. 127–239, 2014.

Context L: Cybersecurity

Cybersecurity includes a collection of methods designed to protect systems, networks, and services from external threats. Businesses and organizations employ cybersecurity professionals to protect their confidential information, maintain employee productivity, and enhance confidence in products and services.

Key properties of cybersecurity are privacy, integrity, and availability. Privacy means data can be accessed only by authorized parties; integrity means information can be added, altered, or removed only by authorized users; and availability means systems, functions, and data must be available on-demand according to agreed-upon parameters. An important element of cybersecurity is the use of authentication mechanisms, which allow to securely identify users or processes.

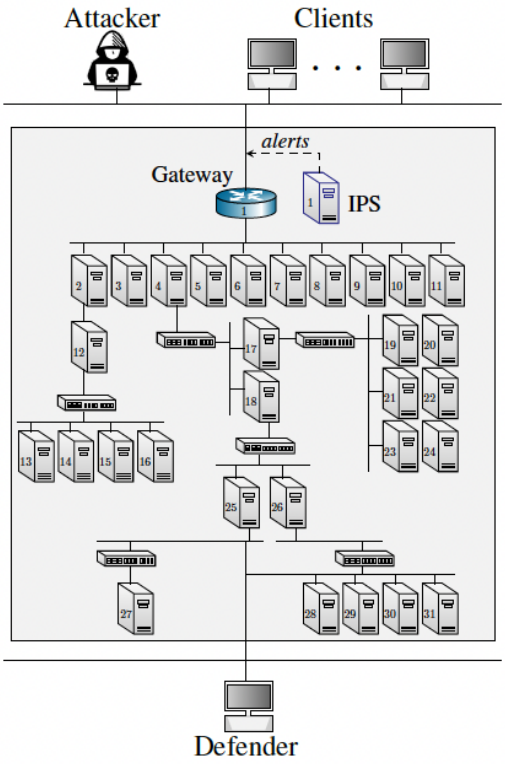
Well-known attacks that compromise the protect systems, networks, and services of an organization include Denial of Service (DOS), installation of malware, man-in-the-middle attack, and phishing. Other types of cyberattacks include cross-site scripting attacks, password attacks, eavesdropping attacks (which can also be physical), SQL-injection attacks, and birthday attacks.

From an engineering point of view, a variety of scientific methods can be used to protect a system or to identify and repel an attack. These include cryptography, formal methods, statistical techniques, and AI. We offer projects where students develop and evaluate state-of-the art approaches to securing systems and preventing attacks:

- Intrusion detection and intrusion prevention
- Active learning for intrusion detection and response
- Human-in-the-loop AI for Intrusion Detection and Response
- Trustworthy Autonomy in Cyber-physical Systems
- Internet of Thing Hacking

Project L1: Intrusion detection and intrusion prevention

Supervisor: Rolf Stadler (stadler@kth.se)



We consider an intrusion prevention use case which involves the IT infrastructure of an organization (see figure). The infrastructure includes a set of servers that run client applications and an Intrusion Prevention System (IPS), which logs events in real-time. Clients access the applications through a public gateway, which also is open to an attacker. The attacker intrudes on the infrastructure and compromises a set of its servers. The defender continuously monitors the infrastructure through accessing IPS and other statistics.

In this project, the students study and evaluate intrusion detection methods of the defender. The methods are based on statistical techniques, e.g. Hidden Markov Models (HMM). They allow a defender to train models based on observations offline and to predict a sequence of observation statistics online. The predictions allow a defender to estimate whether an attack is occurring and in which attack stage it is.

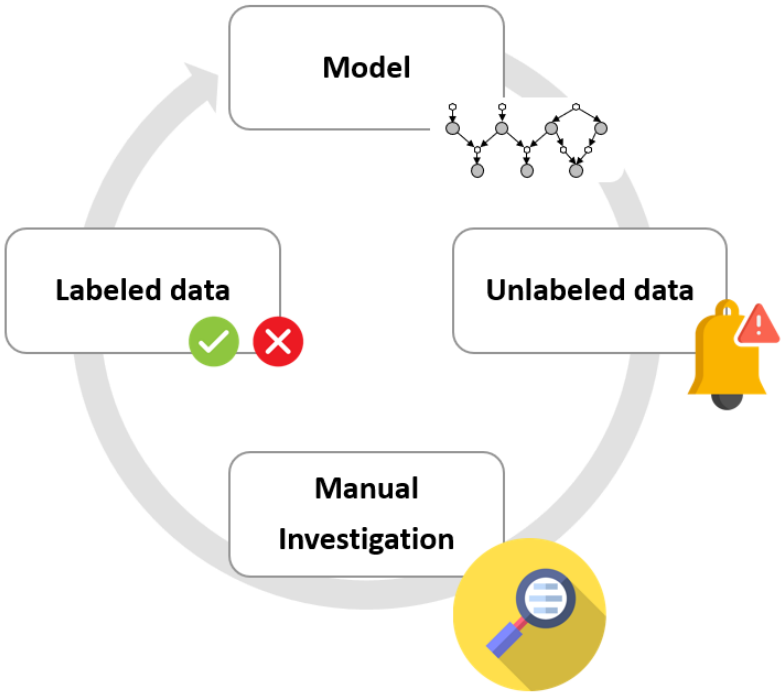
An important part of the project is the experimental evaluation of the studied methods based on measurement traces from a KTH testbed and published data sets.

For the project, the students will use the Anaconda environment (anaconda.com), including Jupyter notebook, and the scikit-learn machine learning packages (scikit-learn.org).
Prerequisites: statistics, applied probability, basic programming skills in Python; basic concepts of machine learning.

Literature: will be made available at the beginning of the project.

Project L2: Active learning for intrusion detection and response

Supervisors: Yeongwoo Kim (yeongwoo@kth.se), György Dán (gyuri@kth.se)



Cyber security has become a major concern in modern society as mobile and wired communication networks provide ubiquitous connectivity, and an ever increasing part of processes and industries become digitalized. Cyber defense is thus becoming fundamental for protecting our digital infrastructures from cyber-attacks and to mitigate the impact of attacks through timely incident response. Mitigation and response typically involve taking defensive actions in response to observations, often in the form of alerts generated by intrusion detection systems, but they come at a certain cost. E.g., a security analyst would have to investigate whether an alert is a false positive, hence spending working hours. Thus, it is important for a defender to choose defensive actions that are optimal, e.g., in the sense that they involve minimal cost while being effective. A fundamental prerequisite for taking an optimal choice is accurate real-time situational awareness (SA), but accurate SA is challenging to obtain due to the high false positive rate of alerts from intrusion detection systems.

A promising framework to address the problem of choosing defensive actions is that of Hidden Markov Models, i.e., modelling alerts as observations triggered by attacker activity from an underlying hidden security state. In order to improve the accuracy of the state estimate, a promising approach is to formulate the problem of the defender as an active learning problem, i.e., a machine learning problem where the defender can perform queries about observed alerts and can choose to execute mitigation actions at a certain cost [1]. Choosing the most informative alerts and the best actions is, however, challenging. In this project the goal is to develop a formulation of the problem faced by the defender and to propose algorithmic solutions for solving the formulated problem, relying on state of the art results in the area of active learning.

[1] Yeongwoo Kim and György Dán, "An Active Learning Approach to Dynamic Alert Prioritization for Real-time Situational Awareness." *Proc. of IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2022.

Project L3: Human-in-the-loop AI for intrusion detection and response

Supervisors: Yeongwoo Kim (yeongwoo@kth.se), György Dán (gyuri@kth.se)

Cyber-attacks pose a significant threat to our digitalized society, and have in the recent past caused major financial loss in critical infrastructures, such as power grids, healthcare, retail, etc. Timely detection and response to cyber-attacks is essential for minimizing their impact, but it is extremely challenging.

The detection of cyber threats involves intrusion sensors that monitor the behavior of processes and network protocols in real-time for generating alerts. The alerts are then investigated by security analysts in a so-called security operations center (SOC). It is the security analysts that decide whether an alert is a sign of an ongoing attack based on log data they can access and based on past alerts observed in the system. The task of security analysts is extremely challenging, as they must decide what alerts to investigate and when, without knowing exactly what a potential attacker is doing in the system [1]. Decision support for security analysts is thus a topic of immense interest worldwide.

In this project our aim is to develop decision support for accelerating the detection of attacks. The approach we follow is to model attack detection as a human-in-the-loop AI problem, i.e., a machine learning problem where the machine and human interact to achieve an objective. The main tasks of the project include:

1. Model the progression of a cyber-attack and the task of a security analyst
2. Develop and implement an algorithm for decision support for security analysts
3. Simulate the resulting human-in-the-loop AI system

[1] Yeongwoo Kim and György Dán, "An Active Learning Approach to Dynamic Alert Prioritization for Real-time Situational Awareness." *Proc. of IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2022.

Project L4: Trustworthy Autonomy in Cyber-physical Systems

Supervisors: Mauricio Byrd Victorica (mbv@kth.se), György Dán (gyuri@kth.se)

Automation and autonomous operation are considered fundamental for future manufacturing and transportation systems, and are expected to be based to a large extent on recent progress in artificial intelligence (AI) and machine learning (ML). They will depend on new generations of sensing equipment providing information for situational awareness. The accuracy and the reliability of the resulting system will depend on the accuracy of the sensed information and on that of the AI/ML algorithms used for processing the information. Along the tremendous benefits come, however, significant risks in terms of new vulnerabilities. State-of-the-art ML algorithms have been shown to be vulnerable to a variety of adversarial attacks, essentially minor manipulations of sensory input, with potentially incorrect operational decisions – and potential safety implications - as a consequence. The situation is aggravated by the fact that there is a lack of understanding of how to mitigate such attacks at the level of individual ML algorithms, and of the severity of these vulnerabilities at a system level.

Existing works in the area of trustworthy machine learning have focused on adversarial attacks against various deep neural network (DNN) classifiers used for detection and classification, e.g., recent work has shown that DNNs are sensitive to small, imperceptible perturbations of visual input [1] as well as to physically realistic attacks, such as patches [2], and have also explored the vulnerability of LIDAR based detection systems to adversarial attacks [3]. The focus of these works is on the automotive domain, and they focus on attacks against individual sensing modalities. They do not, however, consider whether the vulnerabilities could be used for constructing attacks with actual physical impact. Key to addressing this important question is to understand the sensing modalities, their vulnerabilities, and how they are related to each other. In this project we explore this fundamental issue with the objective of developing algorithms for improving the trustworthiness of cyber-physical systems that contain ML components for data processing and inference.

[1] Huang et al, “Adversarial Attacks on Neural Network Policies” in Proc. of ICLR workshops, 2017
[2] Eykholt et al, “Physical Adversarial Examples for Object Detectors,” in Proc. of WEET, 2018
[3] Tu et al, “Physically Realizable Adversarial Examples for LiDAR Object Detection”, Proc. of CVPR 2020

Project L5: Internet of Thing Hacking

Supervisor: Pontus Johnson (pontusj@kth.se)

The Internet of Things entails that a plethora of things become connected to the Internet and fitted with sensors and actuators. Many of these things will be low-cost. However, historically, low production cost has not been conducive to high information security. Sayings such as “The S in IoT stands for Security” reflect the feelings of many observers of the field. The pervasiveness of insecure IoT in smart cities presents a serious risk to society, as more and more critical functions of the city are controlled by automated IoT solutions.

In recent decades, the information security community has come to the realization that white hat hacking is an important activity in the security process. White hat hackers find and responsibly disclose vulnerabilities before malicious actors exploit them.

The main objective of this project is to select and explore the information security of a specific IoT device, and to attempt to hack it.

1. What are typical weaknesses in common Smart City IoT devices?
2. Which devices appear to feature the most easily exploitable vulnerabilities, with the potentially gravest consequences?
3. What methods of penetration appear to explore the most promising attack surfaces? Are access controls flawed? Are there weaknesses in the cryptographic implementations?
4. Is it possible to create a proof-of-concept exploit of a device?

Context M: Big Data & AI

Big data and artificial intelligence are broad topics with huge technological and economical potentials and therefore is of interest in many areas. From an engineering point of view, it is mostly related on how to process data. Currently, information and communication technology is penetrating all systems to make them *smart,* e.g. we envision smart cities, smart homes, smart grids, etc. or Internet of things in general. The smartness of the systems is built on the principle to sense the system environment and then draw smart decisions on it. However without algorithms that extract information from the data, the information is buried in the data and cannot be exploited. Thus, the process of extracting information will be the key ingredient of many future technologies and is the main objective of technologies nowadays known as artificial intelligence (AI), machine learning, data mining, pattern recognition, data analytics, adaptive signal processing etc. which are all instances of information engineering.

In general, we can say that the more data we have, the smarter the system will be. Thus, advanced smart systems sooner or later face the big data problem, which commonly means that the amount of the data is *too big* to be processed e.g. with standard tools. Therefore, there are huge research efforts developing novel information processing and data analytic methods, which enable future systems to deal with larger and larger data sets.

Innovative information processing and data analytic methods are traditional topics of the Information Science and Engineering Division. Thus, the sub-projects offered in this course will address fundamental topics and problems in the area with a strong engagement of the department's teachers. Accordingly, all offered Bachelor projects are closely related to some of the on-going research projects in the division. In particular, we offer project that deal with the classification of ECG data, optimization in decentralized networks, outlier detection and imputation in health-care data, explainability problems of machine learning algorithms, data-driven positioning of a radio source, data minimisation methods for privacy, and data driven state estimation problems.

Since information processing is quite abstract, all projects require a good mathematical background and solid programming skills.

Project M1: Classification of ECG data

Supervisor: Joakim Jaldén, jalden@kth.se, Information Science and Engineering Division

Problem Statement:
The electrocardiogram (ECG) is vital for identifying heart issues like heart attacks and irregular heartbeats. Its non-intrusive nature makes it an ideal early screening tool for guiding medical decisions. Nowadays, ECGs are predominantly digital, enabling automated data analysis. The realm of computerized ECG analysis is rapidly progressing.

KTH is collaborating on a novel project with Region Stockholm, AISAB (Ambulanssjukvården i Storstockholm AB – The ambulance service in Stockholm), and Karolinska Institutet (KI). This endeavor will explore the effectiveness of automated ECG analysis within a decision support system. This system, in turn, could aid ambulance staff in making challenging decisions about patient care. Within this project, we are now developing in-house expertise in designing optimal automated ECG classification algorithms. This is where the proposed bachelor project comes into play.

Your project's specific task involves designing and assessing deep neural networks for categorizing 12-lead, 10-second digital ECG traces of the same form as those collected in Stockholm's ambulances. This encompasses identifying the best network structure and dimensions, as well as exploring potential data augmentation techniques to deal with the relative scarcity of training data. However, the bachelor thesis will only employ publicly available ECG datasets due to ethical guidelines for handling patient data. This approach fosters flexibility in project execution by simplifying data access and eliminates potential constraints on the project report's contents. Nonetheless, the collaboration with KI and AISAB researchers will provide guidance throughout the project and guarantees the project's relevance.

Prior experience constructing deep neural networks isn't necessary, but proficiency in Python programming is essential. Basic familiarity with the Unix shell environment will also be advantageous, especially if you wish to use our computational infrastructure to train the neural networks.
Part (ii) would most likely require basic knowledge of modelling and machine learning and hence kept optional depending on the student’s interest and available time.

Project M2: Decentralized ADMM

Supervisors: Jeannie He, jeannie@kth.se, Ming Xiao, mingx@kth.se, Information Science and Engineering Division

Background description:
Thanks to its simplicity and applicability to various optimization problems, the alternating direction method of multiplier (ADMM) has been a hot topic in both academia and industries. To provide an example, ADMM can be used to solve consensus optimization problems where a global optimal solution is found by letting several workers compute and send a set of primal and dual variable values to a central unit, where a corresponding global variable value will be computed and sent back to the workers. After receiving the global variable value, the workers will then trigger the next iteration by computing and sending the next set of primal and dual variable values to the central unit until the global variable value converges [1]. Nevertheless, such an approach is often discouraged due to the disadvantages of centralized methods, such as the high dependency on the location, availability, and capacity of the central unit. The task of the project is to first make a survey on decentralized implementations of ADMM; implement the ones that you identify as state-of-the-art implementations in a somewhat realistic simulation environment and compare them.

Detailed project goal:
The primary goal is to identify the state-of-the-art decentralized ADMM implementations. After this project, students should be able to explain the core of ADMM and some of the state-of-the-art decentralized ADMM implementations. The student should also have implemented and evaluated the performance of a few the state-of-the-art decentralized ADMM implementations in terms of convergence rate, accuracy throughout the time, and computational/communication cost.

Coarse Task Planning

1. Make a survey on decentralized implementations of ADMM
2. Set up a realistic simulation environment for the implementation of ADMM with connected computing units - if implemented on the same machine, communication delays should be simulated based on adequate assumptions.
3. Implement the ones that you identify as state-of-the-art implementations and compare them in terms of convergence rate, accuracy throughout the time, and computational/communication cost.
4. Propose improvement to the implementations - optional.

Require skills
Coding skills

Recommended prerequisites:
SF1811 Optimization, DD2352 Algorithms and Complexity, SF1624 Algebra and Geometry, DD1389 Internet Programming.

References
[1] S. Boyd, N. Parikh, E. Chu, B. Peleato, J. Eckstein, et al., “Distributed optimization and statistical learning via the alternating direction method of multipliers,” Foundations and Trends® in Machine learning, vol. 3, no. 1, pp 1-122, 2011
[2] P. Singh, M. Masud, M. S. Hossain, A. Kaur, G. Muhammad, and A. Ghoneim, “Privacy-preserving serverless computing using federated learning for smart grids,” IEEE Transactions on Industrial Informatics, 2021

Project M3: Machine Learning for Outlier Detection and Imputation in Health-Care Data

Supervisor: Ragnar Thobaben (ragnart@kth.se), Division of Information Science and Engineering (ISE)

In the last decade, a large amount of health care data has been collected in hospitals world-wide, which is now partially made available for research purposes in public data bases to foster the development of new data-driven approaches to health care and to take advantage of the recent progress in the field of machine learning. Typical applications for machine learning in health care include pre-processing steps (e.g., outlier detection, missing-data imputation), decision support systems, (e.g., diagnostics, outcome prediction, and treatment recommendations), treatment automation (e.g., glucose, ventilation, circulatory and cardiovascular management), and data analysis (e.g., identification of patient- and treatment-specific risk factors). A fundamental challenge in using data-driven approaches in health-care data is that data is inherently noisy as a side effect of the care environment, interventions, treatment, and patient-specific factors; for example, time stamps may be inaccurate for lab measurement, manually documented data can be false or incomplete (e.g., shifted decimal separator, data ends up in the wrong field), time-series measurements can be interrupted (e.g., due to treatment and interventions), the condition of a patient makes certain measurements difficult, and measurement noise in general. Pre-processing of clinical data is therefore an important step that if done manually, consumes a lot of resources (i.e., a specialist has to review the data and make corrections by hand) that could be better used in other ways to offload the burden and stress of care staff, and hence, may contribute to improved patient safety. The goal of this project is therefore to explore the use of machine learning algorithms for outlier detection and data imputation in clinical data by developing a suitable machine learning method in a relevant use case (e.g., based on publicly available data sets and following recent trends in the related research literature).

The steps in the project are as follows:

- In self-studies, the students are expected to acquire the required machine learning background and skills to execute the work in this project. Following publicly available online lectures has been a successful approach to this in previous years.
- Together with the supervisor, you will identify a few suitable problems and data sets (e.g., outlier detection, data imputation, data correction), for which you will train at least two different machine learning models using different methods.
- Next, you will adopt strategies from the literature and possibly develop new strategies to further analyse the models to explain their responses to the data.
- You will summarize your findings and present the results of a comparison of the different approaches investigated in this project in the final report and the final presentation. The final report will also include a brief survey of recent approaches to outlier detection and data imputation in clinical data.

The project is fairly open and leaves students with a lot of space to develop and pursue own ideas. Since this freedom also can be a burden, this project is only recommended for creative students with strong mathematical and programming background. Students working in this project will be supported by Ragnar Thobaben.

Project M4: Explainable Machine Learning for Health Care

Supervisor: Ragnar Thobaben (ragnart@kth.se), Division of Information Science and Engineering (ISE)

In the last decade, a large amount of health care data has been collected in hospitals world-wide, which is now partially made available for research purposes in public data bases to foster the development of new data-driven approaches to health care and to take advantage of the recent progress in the field of machine learning. Typical applications for machine learning in health care include pre-processing steps (e.g., outlier detection, missing-data imputation), decision support systems, (e.g., diagnostics, outcome prediction, and treatment recommendations), treatment automation (e.g., glucose, ventilation, circulatory and cardiovascular management), and data analysis (e.g., identification of patient- and treatment-specific risk factors). One of the biggest obstacles though that hinders the wide acceptance of machine learning models in health care, is lack of interpretability of such models. For example, in a clinical context, a decision support system needs to be able to provide an explanation for its recommendation in order to be trusted by the medical staff, and in the case of data analysis (e.g., identification of risk factors), it is important to understand which signal components are responsible for triggering a certain response of the learned model. In this project, we will investigate this issue by studying machine learning models trained from health-care data (e.g., models for detecting cardiovascular disease and/or pre-diabetes, mortality prediction) and by extending these models to yield interpretability and explainability. This can be achieved, e.g., by considering models that are inherently well interpretable like, e.g., logistic regression, random forests and clustering, or by performing a sensitivity analysis of trained models with known parameters.

The steps in the project are as follows:

- In self-studies, the students are expected to acquire the required machine learning background and skills to execute the work in this project. Following publicly available online lectures has been a successful approach to this in previous years.
- Together with the supervisor, you will identify a few suitable problems (e.g., detection of cardiovascular disease and/or pre-diabetes, mortality prediction) and data sets, for which you will train at least two different machine learning models using different methods.
- Next, you will adopt strategies from the literature and possibly develop new strategies to further analyse the models to explain their responses to the data.
- You will summarize your findings and present the results of a comparison of the different approaches investigated in this project in the final report and the final presentation. The final report will also include a brief survey of recent approaches to explainable machine learning.

The project is fairly open and leaves students with a lot of space to develop and pursue own ideas. Since this freedom also can be a burden, this project is only recommended for creative students with strong mathematical and programming background. Students working in this project will be supported by Ragnar Thobaben.

Project M5: Learning to find a radio source

Supervisor: Mats Bengtsson matben@kth.se, Division of Information Science and Engineering (ISE)

Problem Statement:
In 5G wireless systems and in the plans for next generation (6G), the possibility to localize a phone or a gadget is getting more and more focus, and the number of positioning based services is growing. Most smart phones are already equipped with GPS receivers, but since GPS cannot be used reliably indoors or other places where the satellite signals are blocked by buildings or tunnels, other complementary solutions are needed, preferably exploiting the same radio signal that anyway is transmitted between the base stations and users. In particular, most modern base stations are equipped with multiple antenna elements, which can be used to determine the direction of an incoming signal, just as we humans can exploit our two ears to determine the direction of sound.
Such direction finding using multiple antennas (so-called MIMO or antenna arrays) has been used for a long time in RADARs and a number of different algorithms have been developed over the years to efficiently compute an accurate estimate of the direction, based on the vector of received signals. However, these algorithms require highly accurate calibration of the radio hardware and often they require a very specific layout of the antenna placements. It would therefore be interesting to use machine learning techniques that can learn to solve the direction finding problem in an efficient way for arbitrary antenna arrays.

In this project, you will get access to wideband radio propagation measurements from a test vehicle that was driving around in Kista collecting frequency responses of the radio propagation from a base station equipped with an antenna array. The calibration and even the layout of the antenna array is partly unknown, but we have reliable information on the position of the test vehicle, meaning that we have ground truth data on the directions.

Your task will be to train different forms of machine learning solutions (using standard toolboxes in Matlab or Python) based on a subset of the measurement data and evaluate the resulting performance using the rest of the data. The goal is to find a solution that requires as low computational complexity as possible to determine the direction (once the training is finished) and uses as little training data as possible, and at the same time achieves a good accuracy. Many possible extensions of the project are possible, such as trying the approach on simulated data corresponding to a well-calibrated array and compare the estimation accuracy to that of existing state-of-the-art algorithms, or learning to estimate several directions in scenarios where there are multiple transmitting signals (which easily can be emulated by superposing different samples of the measurement data).

Project M6: Information Bottleneck for Data Minimization

Supervisors: Mengyuan Zhao, mzhao@kth.se, Tobias Oechtering, oech@kth.se, Information Science and Engineering Division

The Information Bottleneck is a fundamental concept in information theory and machine learning, serving as a powerful framework for understanding the trade-off between simplicity and accuracy in data compression and representation learning. The Information Bottleneck Method is a computational approach derived from this concept, aimed at extracting the most essential and relevant information from a complex dataset while discarding extraneous details. By constraining the information flow through a bottleneck, this method enables the creation of compact and informative representations that are particularly valuable for tasks like feature selection, dimensionality reduction, and deep learning, where balancing the preservation of vital information and the reduction of noise is critical for effective data analysis and model generalization.

In this project the information bottleneck method should be studied to enhance the privacy of structured data. The information bottleneck formulation can be seen as a relaxation of a sufficient statistic requirement. A data representation based on sufficient statistic that cannot be reduced further reduced is desirable since it meets GDPRs data minimization principle [3]. Thus, we will study how the information bottleneck method can used to obtain a privacy-preserving representation that also provides sufficient accuracy for the inference task.

The steps in the project are as follows: The students are expected to acquire the required background and skills to execute the work in this project in mostly self-studies. Together with the supervisor, you will identify a few suitable information bottleneck-based approaches, privacy measures and data sets for which a privacy-enhancing data compression can be done. Next, you will adopt information bottleneck method strategies from the literature and possibly develop new strategies to create representations that achieve a good utility and privacy leakage can be assessed. Lastly, you will summarize your findings and present the results comparing different approaches investigated in this project in a final report and final presentation. The report will also include a brief survey of recent information bottleneck method approaches.

The project is fairly open and leaves students with a lot of space to develop and pursue own ideas. Since this freedom also can be a burden, this project is only recommended for creative students with strong mathematical and programming background. Students working in this project will be supported by Mengyuan and Tobias.

References

[1] N. Tishby, F. C. Pereira, W. Bialy, “The Information Bottleneck Method”, in Proc. 37th Allerton Conf. on Communication, Control and Computing, Sept 1999.

[2] N. Tishby and N. Zaslavsky, "Deep learning and the information bottleneck principle," *2015 IEEE Information Theory Workshop (ITW)*, Jerusalem, Israel, 2015.

[3] T.J. Oechtering, S. Saeidian and C.M. Sjöberg, "Calculated Privacy: Tech Meets Law & Law Meets Tech," *FIU Law Review (to apprear)*.

Project M7: Unsupervised learning for tracking and classification of sequences

Supervisors: Anubhab Ghosh (anubhabg@kth.se), Saikat Chatterjee (sach@kth.se)

Large Language Models (LLMs), ChatGPTs are examples of deep learning-based data-driven sequencing methods (modelling processes over time). In the background of multi-dimensional sequence models, the proposed project will investigate two questions where the assumptions are: we have no knowledge of process (model-free process) and we do not have labelled data. That means we must work with unsupervised learning. Unsupervised learning is a true essence of how intelligence works, for example, human mainly learns in unsupervised ways.

The project will investigate two main questions (1) Can we track a car / robot / drone / or any other agent from noisy measurements? In another application context, can we track state of health conditions, like human heart condition, using noisy measurements of heart? (2) Can we classify model-free processes from noisy measurements? How do we design an intelligent classifier that can act on noisy measurement sequences?

Technical Background: Recently Recurrent Neural Nets (RNNs), such as LSTM, GRU, etc. have been widely used in the field of state estimation, i.e. estimating the underlying hidden state of a dynamical system given only noisy observations. This task has been largely catered to by classical methods in the past e.g. Kalman filters, particle filters, etc. Recently there have been data-driven methods as well as hybrid methods (a combination of data-driven and classical approaches). We recently proposed a method named as DANSE (Data-driven Nonlinear State Estimation) and is powered by RNNs. The project will be based on DANSE [1].

Pre-requisites: This project requires that

- Students have a solid background in Linear Algebra, Probability
- Students are quite comfortable with coding in Python and in particular toolkits such as PyTorch [12] or Tensorflow.
- Motivated, dedicated, and a willingness to learn new, complicated but interesting concepts :).
- (Bonus) Knowledge regarding Machine learning (basic feed-forward networks, recurrent neural networks, training of neural networks)

Tasks: The steps of the project are as follows:

- Understanding the existing scheme of DANSE and its Python implementation, including data generation (NOTE: implementation of DANSE already exists, the task is to learn how to use this tool mainly, of course, students with more curiosity are welcome to learn further).
- Implement a classification software platform on Python to do unsupervised binary classification using DANSE via a maximum-likelihood principle (this includes coding the classification testing part, integrating the DANSE model, and tabulating performance metrics e.g. accuracy, F1-score, etc.). The datasets used will be nonlinear state space models which can be simulated, i.e. synthetically generated data.

References

[1] A. Ghosh, A. Honor´e, and S. Chatterjee, “DANSE: Data-driven Non-linear State Estimation of Model-free Process in Unsupervised Bayesian Setup,” in European Signal Processing Conference (EUSIPCO), 2023 (To appear).

CONTEXT N: AI, games, and strategy

Top: The very first AI-program was a computer program that played Checkers (www.chessprogramming.org/Christopher_Strachey). Bottom: The strategy game SIGNAL is used to study nuclear escalation dynamics (pong.berkeley.edu/e-game/).

AI and strategy games have been intimately connected since the very inception of AI. Classic strategy games such as Checkers, Chess, Go, and Poker have served as shared research goals within the AI-community and as benchmarks for evaluating AI-algorithms.
The interest in strategy games within AI has also been motivated by the prospect of supporting real world decision making and strategy. In the social sciences and elsewhere, there is a long tradition of analyzing human interactions of various kinds as strategy games – from relatively peaceful interactions such as business negotiations or stock trading to directly hostile interactions such as dogfights in air combat.

Given a model of a conflict as a strategy game, the strategy space can be explored systematically. However, exploring the strategy space manually, e.g., by repeatedly playing the game, requires considerably time and effort. The recent advances in AI for strategy games have opened up for the possibility of automating decision making and strategy development. Application areas range from security and defence to finance.

.

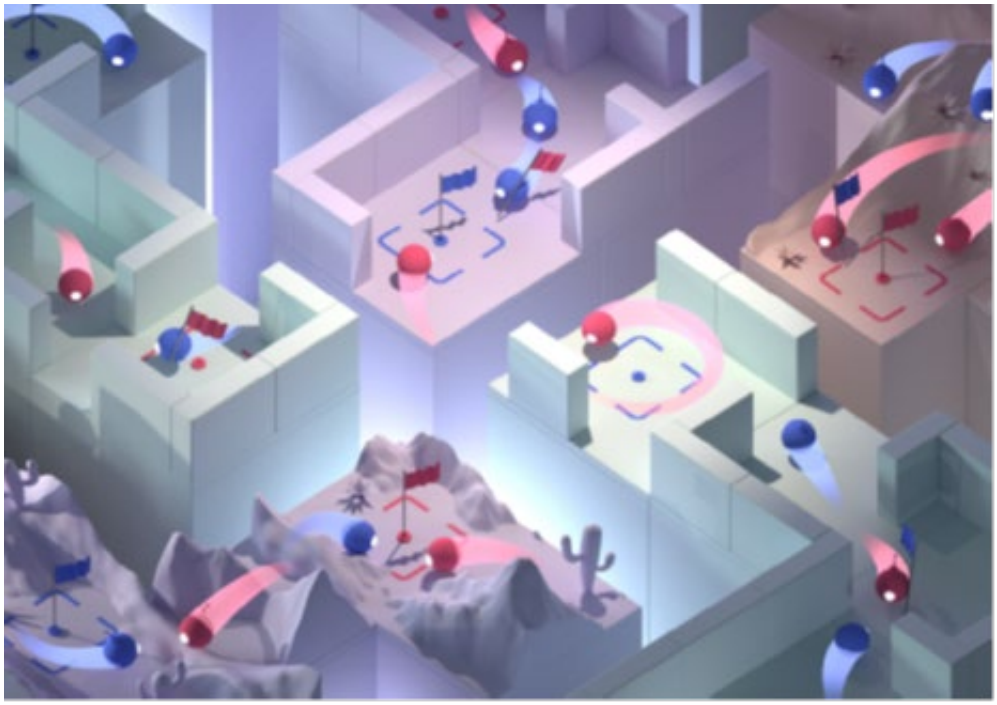
Project N1: Knowledge in Multi-Agent Games

Supervisor: Dilian Gurov (dilian@kth.se), Division of Theoretical Computer Science

Key Words: Multi-Agent Systems, Game Theory, Knowledge-Based Strategies

In a multi-player game, a coalition of **players** (also called agents) is attempting to achieve an **objective** within a (potentially hostile) environment, considered to be the opponent. Solving such a game means to find a **strategy** that achieves the objective regardless of the moves of the environment. Rescue missions involving robots and humans or pursuit-evasion games are examples of such games, often called multi-agent systems.

An interesting, but complicating circumstance is when the players have limited information about the current state of affairs, say due to limited observation capabilities. Such games are called games of **imperfect information**. A related aspect is posed by the communication capabilities between players. The problem of strategy synthesis under imperfect information and limited communication is known to be hard, and is an active research area. The present project investigates the modelling of such games, as well as algorithmic and machine learning-based techniques for strategy synthesis. In particular, the project focuses on strategies based on the notion of **knowledge**. In the context of this project, knowledge refers to information, structured suitably, stored and updated during the course of a play, for deciding on a course of action. Especially interesting is **higher-order knowledge**, where players maintain and use during play knowledge about the other players' knowledge.



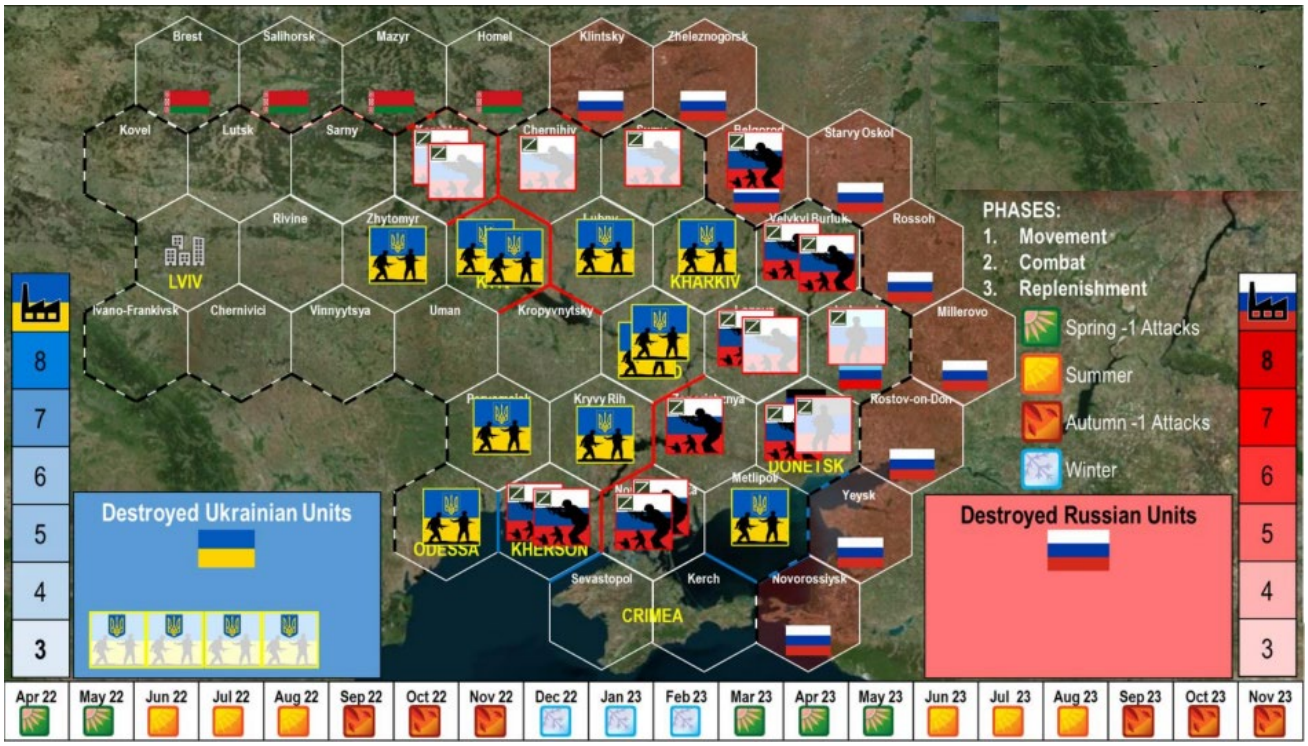
Inspirational Reading:

[1] Gurov, D., Goranko, V., Lundberg, E.: *Knowledge-Based Strategies for Multi-Agent Teams Playing Against Nature*. Artificial Intelligence, vol.309, 2022, DOI: 10.1016/j.artint.2022.103728
[2] Doyen, L., Raskin, J.F.: *Games with imperfect information: Theory and algorithms*. Lectures in Game Theory for Computer Scientists pp. 185–212 (2011)
[3] Berwanger, D., Kaiser, L., Puchala, B.: A *perfect-information construction for coordination in games*. In: Foundations of Software Technology and Theoretical Computer Science (FSTTCS'11). LIPIcs, vol. 13, pp. 387–398 (2011)
[4] Huang, X., van der Meyden, R.: *Synthesizing strategies for epistemic goals by epistemic model checking: An application to pursuit evasion games*. In: Proceedings of AAAI 2012 (2012)

Projekt N2: Ukrainas motoffensiv med AlphaZero

Handledare: Mika Cohen (mikac@kth.se), Farzad Kamrani (farzad.kamrani@foi.se), Daniel Oskarsson (daniel.oskarsson@foi.se)

Sammanfattning: I det här projektet analyserar du en väpnad konflikt med hjälp av en självlärande AI från DeepMind.



Bakgrund
I början av 1941 förstörde tyska ubåtar allierad sjöfart i en förödande takt. Winston Churchill beordrade att den brittiska flottan skulle "Ta reda på vad som händer och sänka U-båtarna!". En ny taktikutvecklingsenhet skapades, Western Approaches Tactical Unit (WATU), där man simulerade ubåtsattacker och utvecklade motåtgärder med hjälp av krigsspel. Krigsspelens spelregler speglade kända fysikaliska egenskaper hos handelsfartyg, eskorter och ubåtar vad gäller hastighet, vändcirkel, synlighet, beväpning och så vidare, men spelreglerna lämnade taktiska beslut kring formation, m.m. öppna för spelarna att välja fritt. Spelarna tilläts därvid att experimentera med taktiken och pröva sig fram och på så vis – genom trial-and-error – nå fram till den bästa taktiken för att skydda konvojerna. Denna taktikutveckling anses ha varit avgörande för utvecklingen i kriget i stort.
Idag är det rimligt att tänka sig att ”Liknande utmaningar i framtiden skulle kunna hanteras ännu snabbare och mer effektivt med hjälp av AI-program som AlphaZero” (Edward Stringer, generaldirektör för försvarshögskolan i Storbritannien).

AlphaZero. För fem år sedan förlorade Lee Sedol, legendarisk 18-faldig världsmästare i Go, mot AlphaGo, en AI från DeepMind. Händelsen väckte stor uppmärksamhet – att bemästra Go sågs av många som det yttersta inom mänsklig intelligens och kreativitet. DeepMind förenklade och generaliserade sedermera AlphaGo till en generell algoritm, AlphaZero, som kan lära sig godtyckliga strategispel (av ett visst slag) till övermänsklig skicklighet. AlphaZero lär sig ett spel genom att spela mot sig själv om och om igen (self-play) i en process av försök-och-misstag inte helt olik mänsklig inlärning i t.ex. WATU. AlphaZero har i grunden förändrat förståelsen av klassiska strategispel som Go och Schack med nydanande, bitvis revolutionerande taktik som århundraden av omfattande, heroisk mänsklig ansträngning inte lyckats upptäcka.

Mikrokrigsspel med AlphaZero. Ubåtsspelen i WATU tillhör en typ av mycket småskaliga krigsspel, ibland kallade mikrokrigsspel, som i mångt och mycket påminner om klassiska strategispel som Go och Schack. Den avgörande skillnaden är att spelreglerna syftar till att korrekt spegla dynamiken i en viss verklig militär konfliktsituation, om än på en hög abstraktionsnivå. Eftersom AlphaZero har visat sig kunna bemästra klassiska strategispel och ge ett fönster mot optimalt spelande kan AphaZero förväntas att på liknande sätt kunna ge ett fönster mot optimalt spelande även i mikrokrigsspel.

Syfte
Projektet syftar till att analysera en mikrokrigsspelssimulering av Ukrainakriget, alternativt flygdueller i Blitzen, med hjälp av AlphaZero:

- Glory to the Heroes, en simulering av Ukrainakriget på strategisk nivå. (https://paxsims.wordpress.com/2023/09/03/glory-to-the-heroes-a-simple-grand-strategic-simulation-of-the-russo-ukrainian-war/)
- Fighter Duel Lite, en simulering av Blitzen på lägre taktisk nivå. (https://www.wargamevault.com/product/446605/Fighter-Duel-Lite)

Metod
Det valda mikrokrigsspelet analyseras med AlphaZero i OpenSpiel, en fullskalig implementation av AlphaZero som nyligen blivit publik (https://github.com/deepmind/open_spiel). Lite grovt kan arbetet delas in i tre steg:

1. Spelreglerna implementeras i OpenSpiel. GUI är ett bonus, men inte ett krav.
2. AlphaZero (som medföljer OpenSpiel) konfigureras för det specifika spelet.
3. Spelbalans (eng: game balance) och strategi/taktik undersöks med AlphaZero.

Nytta
Projektet bedrivs i anslutning till forskningsprojekt om taktisk AI på FOI.

Vidare läsning

- *Krigsspel med AlphaZero*, FOI 2021, https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--5057--SE
- *Patrullering* med poker-AI, FOI 2022, https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--5291--SE

Tidigare kursomgångar
Projektet är det tredje i en rad projekt kring taktisk AI inom samma kurskontext.

- *Exploring Game Balance in the Scandinavian Fox Game with Monte-Carlo Tree Search*, Anton Janshagen och Olof Mattsson, Workshop on Tabletop Games, 2022
- *Monte-Carlo Tree Search for Risk*, Erik Kalmer och Christoffer Limer, 14th NATO Operations Research and Analysis (OR&A) Conference, 2020

Projekt N3: Design och jämförelse av strategier för oförutsägbar utplacering av honungsfällor

Handledare: Joel Brynielsson (joel@kth.se), Edward Tjörnhammar (edward.tjornhammar@foi.se).

Sammanfattning: I det här projektet studeras cybervilseledning genom oförutsägbar utplacering av honungsfällor.

Bakgrund
All krigföring baserar sig på bluffspel. -- Sun Zi

Av alla mänskliga aktiviteter påminner krig mest om ett kortspel. -- Carl von Clausewitz

Runt om i världen använder numera säkerhetsoperatörer AI-algoritmer för att planera ett optimalt oförutsägbart försvar inom olika arenor – tillämpningarna handlar om övervakning av allt från flygplatser och hamnar till kust och hav. För att göra försvarsinsatser oförutsägbara i en konfliktsituation (exempelvis bekämpningen av tjuvjakt i ett naturreservat) tillförs ett element av slumpmässighet i hur försvarsresurserna (såsom fotpatruller) agerar. Men försvarsresurserna agerar inte helt godtyckligt utan algoritmerna slumpar agerandet på ett sätt som maximerar den avskräckande effekten i konfliktsituationen. Cyberförsvar utgör ett exempel på en sådan konfliktsituation som är asymmetrisk såtillvida att angriparen har möjlighet att skanna av och testa olika attacker över tid, samtidigt som försvararen utför motåtgärder i form av att placera ut olika typer av skyddsåtgärder såsom honungsfällor – falska servrar som placeras ut i en organisation i syfte att locka till sig angripare och kartlägga dem.

Nyligen genomförda experimentella studier har undersökt hur väl adaptiva strategier för utplacering av honungsfällor klarar att försvara sig mot mänskliga angripare. Men eftersom försökspersonerna hämtades från en okänd population av försökspersoner via Amazon Mechanical Turk,1 är relevansen för försvar mot verkliga hackers oklar. I en studie som genomfördes 2023 i samband med förra årets kandidatexjobbskurs replikerades därför experimenten med mer relevanta försökspersoner. De erhållna resultaten tyder på att strategierna är mindre effektiva mot angripare i den studerade populationen, och att algoritmernas förmåga att förutsäga nästa attack stadigt minskar över tid: de mänskliga försökspersonerna lärde sig att attackera allt mindre förutsägbart.

Syfte
Projektet syftar till att designa och jämföra algoritmer för oförutsägbar utplacering av honungsfällor i en organisations datornätverk.

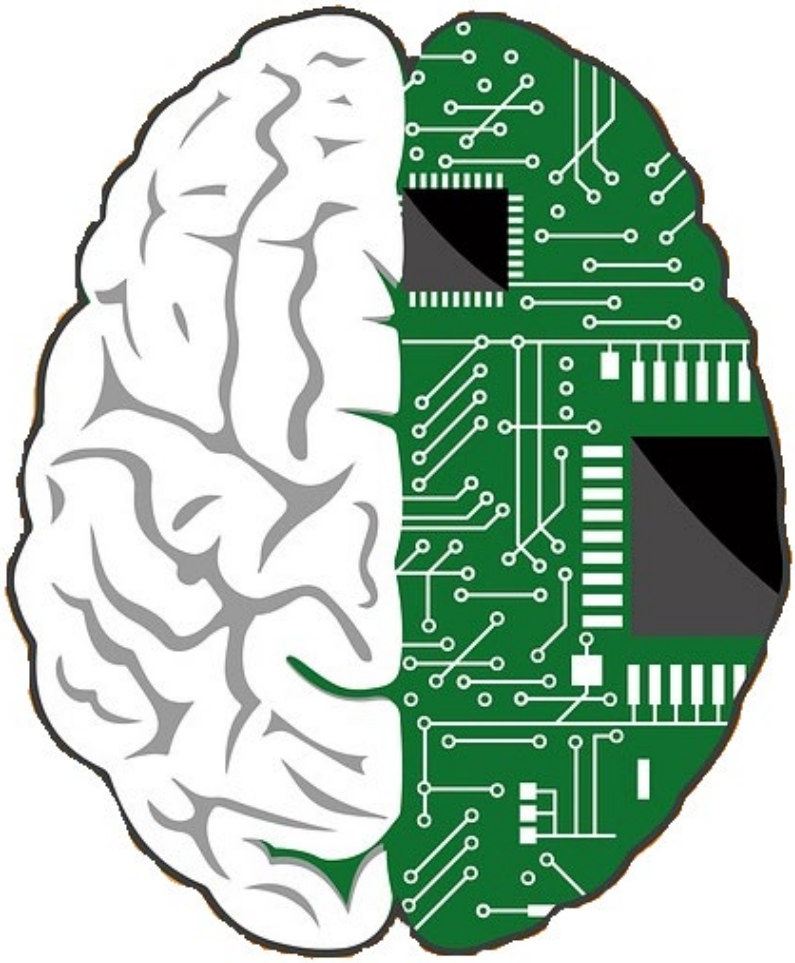
Metod
Projektet kan beroende på exjobbsgruppens intressen och bakgrund ges en i olika utsträckning utforskande, jämförande eller implementerande karaktär. Ett grovt utkast till metodologiskt upplägg skulle kunna vara följande:

- Studera vad som hittills är gjort med fokus på inläsning på tidigare strategier för slumpvis utplacering, och välj sedan en delmängd av följande approacher för att designa strategier:
    - klura ut en helt ny strategi som skulle kunna spöa de som redan finns
    - skapa en ensemble-strategi som kombinerar bra egenskaper hos tidigare strategier
    - ta del av FOI:s idéer kring nya alternativa strategier och konkretisera dessa.
- Överväg att antingen använda det befintliga abstrakta spelet för honungsfällautplacering, eller att hitta på ett nytt spelproblem som bättre fångar/efterliknar en organisations datornätverkstopologi.
- Implementera de nya strategierna och stoppa in dem i det redan utvecklade FOI-systemet för experimentella studier.
- Genomför försök med en relevant population (gör som förra årets studenter som genomförde sina försök med en årskurs F-studenter som fick FOI-sponsrad choklad som pris då de spelade, eller genomför tillsammans med FOI försök med en relevant cybersäkerhetspopulation).

Nytta
Projektet bedrivs i anslutning till flera olika forskningsprojekt på FOI med bäring på AI för optimalt oförutsägbar allokering i cyberrymden.

Vidare läsning
J. Brynielsson, M. Cohen, P. Hansen, S. Lavebrink, M. Lindström, E. Tjörnhammar, ”Comparison of Strategies for Honeypot Deployment”, i Proceedings of the 2023 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2023). ACM, New York, NY, 2023.
J. Brynielsson, M. Cohen, F. Kamrani, D. Oskarsson. Patrullering med poker-AI: Systematiskt oförutsägbar patrullering i sjö, mark och cyberrymd. Teknisk rapport FOI-R--5291--SE. Totalförsvarets forskningsinstitut, Stockholm, 2022.

Context O: Computational brain modelling and brain-like computing



The general focus is here on developing, studying and/or applying connectionist (network based) brain models. The proposed topics range from simulating detailed spiking neural networks to investigating and validating more abstract brain-like computing architectures. Projects can be formulated to either address theoretical questions or test the networks' functionality in applications.

Please bear in mind that project details and specific research questions within the proposed themes are discussed individually with students depending on their interests. There is also a lot of flexibility in defining the scope and size of these projects. Some project ideas at the cross-sections of the following themes can be proposed/found. Students will have an opportunity to learn to use dedicated simulation software (with a possibility to rely on Python interface) or exploit their programming competence to build their own computational tools for theoretical or applied research. The focus however is on the scientific essence of the project, not on the methodology used.

The suggested projects are organized in three main themes, each of which describes a set of proposed topics. The lists of topics and some project ideas are not meant to be limiting in any sense and can therefore be easily expanded by students' own ideas.

Project O1: Simulations of attractor neural networks as models for human memory

Supervisor: Pawel Herman (paherman@kth.se), Department of Computational Science and Technology (CST)

General theme

There have been a range of theoretical concepts of brain computations proposed in computational neuroscience. Among the connectionist (network-based) approaches to modelling brain function, an attractor theory of neural computations has recently received particular attention. The functionality of attractor networks has been found helpful in explaining various perceptual and memory phenomena. Consequently, these models can be considered as fundamental components of systems level approach to modelling brain function within the framework of network-of-networks architecture. An implementation of attractor memory models can range from a more biologically plausible networks of spiking neurons to more abstract networks of units with continuous rate-based input/output.

More biophysically detailed models with spiking neurons and synapses provide an opportunity to study rich neural dynamics in close relation to biological data, and specifically, recordings from the brain tissue. This way both dynamical and functional aspects of fascinating cortical phenomena can be studied. Such spiking neural network models are usually developed using dedicated simulation software, e.g. Nest, Neuron, Genesis etc.

More abstract networks relying on rate-based units (i.e. with non-spiking real-valued input/output) on the other hand allow for constructing larger systems with the aim of exploring functional aspects of the simulated attractor memory system. In this context, both generic theoretical investigations into computational capabilities of memory (learning, memory capacity etc.) as well as specific applications in pattern recognition, whether in a biological or non-biological data mining context, can be pursued. Within this theme other computational theories of the brain, e.g. liquid state machines, can also be studied. In this regard, computational or dynamical aspects as well as application-oriented questions may be explored. Students can make use of existing software simulators or developed their own implementations of network models.

Project ideas

1. Studying the effect of different connectivity patterns, network architectures and their dimensionality on the dynamics and function of the attractor model.
2. Investigating the sensitivity of the model to the level of biological detail being accounted for (discussion on the required level of complexity and the relevance of biological constraints).

Exploring population-level (e.g. simple mean-field approximation) approaches to describing the neural dynamics exhibited by a modular attractor network.

Project O2: Brain-like computing algorithms – theoretical developments and applications

Supervisor: Pawel Herman (paherman@kth.se), Department of Computational Science and Technology (CST)

General theme

Development of brain models to study neural phenomena, as broadly discussed in topic 1.1 above, often leads to better understanding of the nature and purpose of neural computations. From a broader perspective, these computations can be seen as an inspiring model for novel approaches to generic information processing. Good reputation of neural network architectures in this regard is largely due to the impressive capabilities of information processing in the brain, which robustly handles large volumes of noisy multi-modal data received in continuous streams. Consequently, brain-like computing has long been considered as a particularly appealing concept in a broad field of information science. With the increasing availability of powerful computing platforms and intensive development of brain models as well as a growing body of knowledge about computational mechanisms underlying brain function, there is a surge of interest in adapting these functional aspects to devise algorithms for more generic applications in the field of data mining, pattern recognition etc. These efforts are urgently needed and particularly relevant to real-world problems involving so-called big data, for example in exploratory analysis of large volumes of high-dimensional neuroimaging data for research or clinical purposes.

Project ideas

1. Adapting selected brain-like computing paradigms for large-scale data mining, e.g. to perform exploratory search for patterns in brain imaging data (medical diagnostics, see also Theme 3).
2. Devising new brain network inspired approaches to generically process temporal or sequential data and/or comparing to the existing state-of-the art attempts.
3. General evaluation and validation of brain-like computing algorithms on speech recognition, computer vision or other challenging real-world problems.
4. Testing robustness (sensitivity analysis, noise handling capabilities, computational speed) and benchmarking brain-like computing methods against more conventional machine (/statistical) learning techniques on a selected set of benchmark problems.
5. Devising network hierarchical architectures to model behavioural phenomena like prediction, expectation and filtering (at a reasonable level of abstraction).