Develop and analyse Physical Layer Security for Massive Unmanned Aerial Vehicle (UAV) Communication Networks

Highlights

- Designing the physical layer security enhancement schemes for UAV communications
- Analysing the secrecy and connectivity performance of massive UAV communication networks
- Utilising Non-Orthogonal Multiple Access (NOMA) assisted UAV networks to enhance the transmission efficiency and reliability of the system

Overview

With their high mobility and low cost, unmanned aerial vehicles (UAVs) have found a wide range of applications during the past few decades. Due to their autonomy, flexibility and broad range of application domains, once UAVs can be properly deployed and operated, they are able to provide reliable and low-cost wireless communication solutions in many practical scenarios.

The main advantages of UAV based wireless communications can be summarized as 1) Compared to conventional BS-based wireless networks, when UAVs are used as aerial BSs, they can establish a line-of-sight communication link to ground users. 2) Due to the mobility and flexibility of UAVs, they are capable of providing additional capacity to support massive connectivity and deliver coverage to some areas that are hard to reach. 3) UAVs can serve as wireless relays to communicate over a long range in practical scenarios such as the IoT. 4) Compared to conventional BS-based wireless networks, a UAV-based network is adjustable, which indicates that it has the opportunity to enhance communication performance through operating the UAVs. These evident benefits make UAV-aided wireless communication a promising component in future wireless systems. However, it also causes potential concerns to legitimate users and network administrators regarding information privacy and confidentiality since UAVs and ground users are exposed to free space. Furthermore, traditional security has been focused on higher layers using cryptographic methods. However, retaining security at high layers is becoming more challenging due to the increased potential for attack, therefore, physical layer security (PLS) has been widely utilized for secure data transmission by considering the physical properties of the radio channel based on Shannon theory.

Therefore, the goals of this project are:
• Designing the PLS enhancement schemes for UAV communications to overcome eavesdroppers (EDs), which are randomly located in the UAVs covered area. The enhanced schemes will mainly focus on power allocation, jamming and trajectory optimization.

• Analysing the secrecy and connectivity performance based on different scenarios, such as the communication within UAV swarms and communication between UAVs and ground users will be investigated.

• Utilizing the NOMA scheme to enhance the reliability and transmission efficiency of the system.

Methodology
The PhD student will develop their understanding of theoretical methods to analyse and optimize the security and connectivity performance in UAV communications. They will learn the power allocation, jamming, and trajectory optimization because these methods can be used to enhance the secrecy and connectivity performance with uncertainty EDs. The worst case for the security of the system will be considered, which means all the EDs are passive. Therefore, EDs are randomly dispersed in a region in the neighbourhood of the transmitter and the receiver will be assumed. To analyse the random location distribution of nodes in the project, stochastic geometry should be studied by the PGR. Moreover, because the practical scenarios in large-scale UAV network are different, i.e., the heights and location of the UAV, the effects of blockage and distribution of ground users should be studied. Finally, the PhD student is able to use the MATLAB and MAPLE software.

Further Reading

Funding
This research project is one of a number of projects in the Department. It is in competition for funding with one or more of these projects. Usually the project which receives the best applicant will be awarded the funding.

Home/EU Applicants
This project is eligible for a fully funded College of Science and Engineering studentship which includes:

• A full UK/EU fee waiver for 3.5 years
• An annual tax free stipend of £14,777 (2018/19)
International Applicants
This project is eligible for a fully funded College of Science and Engineering studentship which includes:

- A full international fee waiver for 3.5 years
- Research Training Support Grant (RTSG)

Application Instructions
The online application and supporting documents are due by Monday 21st January 2019.

Any applications submitted after the deadline will not be accepted for the studentship scheme.

References should arrive no later than Monday 28th January 2019.

Applicants are advised to apply well in advance of the deadline, so that we can let you know if anything is missing from your application.

Required Materials
1. Online application form
2. Two academic references
3. Transcripts
4. Degree certificate/s (if awarded)
5. Curriculum Vitae
6. CSE Studentship Form
7. English language qualification

Applications which are not complete by the deadline will not be considered for the studentship scheme. It is the responsibility of the applicant to ensure the application form and documents are received by the relevant deadlines.

All applications must be submitted online, along with the supporting documents as per the instructions on the website.

Please ensure that all email addresses, for yourself and your referees, are correct on the application form.

For more information, please visit our website at:
https://www2.le.ac.uk/colleges/scieng/research/postgraduate-opportunities/cse-2019/instructions