# *MATTEK9 Project: Advanced Wireless Network Activity Inference*

*Thomas Arildsen, Petar Popovski*
*E-mail: tha@es.aau.dk*

*September 2, 2019*

Figure 1: Detecting movement through walls.

Wireless networks are ubiquitous, constantly exchanging a huge volume of wireless radio signals. The availability of radio signals has motivated a number of research groups to use them for purposes that are different from their primary purpose, which is wireless data communication.

For example, a research group from UCL has shown how WiFi signals can be used to detect movements of users behind walls.[1] In a similar spirit, there are companies that offer home alarm solutions based on the detection of changes in WiFi signals.

The objective of this project is to investigate the possibility of extracting information about the user population at a given location based on the exchanged WiFi signals. For example, estimating the number of users in an office, detecting movements of users, recognizing a location based on the WiFi patterns, etc.[2] This does not rely on the payload data itself, as this is typically encrypted, but on header data such as receiver and transmitter IP addresses as well as meta-data such as packet lengths, frequency of transmission events, and signal power which can be gleaned without access to the payload data itself.

The students will collect data based on the selected WiFi access points at the university campus and apply methods of machine learning to explore what kind of information can be extracted from them. A wide range of methods from classical machine learning (e.g. dimensionality reduction, unsupervised learning via clustering etc.) and/or artificial neural networks could be employed to explore the solution space. Special attention needs to be given to the fact that the data will be a mix of categorical and intensity data that we expect must be combined in the solution.

It can be argued that methods like these could be used with malicious intent ("spying"). While this is true, in addition to benign purposes such as delivering services to detected users, terrorism counter-measures etc., one can also argue that it is better to get potentially risky techniques out into the open for timely examination and development of counter-measures, white-hat hacker-style, rather than to wait for malicious actors to develop them.

[1] Tan, Woodbridge, and Chetty 2016.

[2] Junges, François, and Festor 2019; Song et al. 2018.

## *References*

Junges, P., J. François, and O. Festor (Apr. 2019). "Passive Inference of User Actions through IoT Gateway Encrypted Traffic Analysis". In: *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pp. 7–12.

Song, B. et al. (Nov. 2018). "Robust Commuter Movement Inference from Connected Mobile Devices". In: *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, pp. 640–647. DOI: 10.1109/ICDMW.2018.00099.

Tan, B., K. Woodbridge, and K. Chetty (Oct. 2016). "A wireless passive radar system for real-time through-wall movement detection". In: *IEEE Transactions on Aerospace and Electronic Systems* 52.5, pp. 2596–2603. ISSN: 0018-9251. DOI: 10.1109/TAES.2016.140207.