The SONNET project is about security in future wireless communication networks, specifically, secure methods for generating machine learning models that will not expose users' private information to attacks.

In future wireless transmission systems, such as the currently implemented 5G and the already planned 6G, the dissemination of artificial intelligence is expected on many levels. Applications, user support, system applications, telecommunications traffic handling, etc. are to be intelligently managed by machine learning algorithms. The main requirement that must be met for the machine learning algorithm to work properly is to collect the appropriate (large) amount of data that will be used to generate (train) the machine learning algorithm (model). Such data must be collected under different conditions, for different types of information, etc., to collect as much information as possible, thanks to which the machine learning algorithm will be prepared to recognize and correctly identify new data and make the right decision. Due to the need to collect a variety of data, the problem of how to collect this data arises. The simplest and most intuitive way is to delegate this task to the network users themselves, who inevitably use the network in different ways and under different conditions. Unfortunately, this approach poses a threat to the private information of these users. Their collected data is exposed to attacks and the interception of sensitive information, because of the need to send that data to the central server that will be responsible for training the machine learning algorithm.

A solution that appears in the literature and is expected to be widely used in future telecommunications networks is the so-called distributed learning, specifically federated learning. This type of learning does not require all user data to be collected in a central location to generate there a common algorithm model but requires users to generate their local models based on locally collected data. Such models are then sent to a central place, which on their basis creates one, common, global model, e.g. by averaging the algorithms received from users. This approach ensures much greater security of users' private data.

However, the federated learning algorithm is not completely secure. Attacks on this type of machine learning model generation are expected to become more widespread. Honest users involved in generating the global model can be impersonated by malicious users who want to disrupt the way the global model works for some purpose. The SONNET project will consider poisoning attacks. Malicious users can attack by generating false data (so-called data poisoning) and on this basis generate an algorithm that does not work properly and will harm the averaged global algorithm. Another method of attack is the so-called poisoning of the model. It is a method that consists in modifying the local algorithm itself after it has been generated on real, unmodified data in any way. Such a model will also have a negative impact on the global model.

In the available literature, the topic of attacks on federated learning is gaining a lot of popularity. What is missing, however, is the consideration of what such attacks will look like on federated learning applied to a specific target. Most of the available work considers federated learning on abstract, widely available data. The SONNET project hypothesized that the use of federated learning is critical to the target of the attacks. Attacking users carry out attacks with the purpose to gain something. Research on abstract data cannot account for the attacker's motives. As part of the SONNET project, we consider attacks on federated learning applied to wireless communication systems to recognize spectrum occupancy taking into account the physical conditions prevailing in the radio channel. The purpose of attacks on the federated learning system used in this way may be e.g. generating a global model that often makes the wrong decision that radio resources are busy. Thanks to this, malicious users could carry out their own transmission without any obstacles.

As part of the SONNET project, firstly, effective and difficult-to-detect attacks using traditional methods will be designed on the federated learning system used in wireless communication systems to recognize the spectrum occupancy taking into account the physical conditions prevailing in the radio channel. The attacks will be intentional and maximizing the benefits for the attackers from carrying out them will be the main goal. The project will design effective defense methods against such attacks. As part of the defense algorithms, potential attack motives will also be taken into account to maximize the probability of detecting attacks. In both cases (alg. attack and defense) the use of artificial intelligence algorithms is expected.