Improving Security of Unmanned Aircraft Systems Using Physical-Layer Techniques

Dr. Adrian Kotelba, Senior Scientist, VTT Technical Research Centre of Finland
Need:

• Unmanned Aircraft Systems (UAS) rely on communications for command and control, telemetry, and dissemination of information captured from sensors.

• The communication link between ground station and unmanned aircraft is susceptible to electronic attacks, with data link spoofing, hijacking, and jamming being the most typical ones.

• These security issues must be carefully addressed when selecting the appropriate data link standard for future UAS communications, as data links are vital to the safety and seamless functioning of UAS.
Need:

- In military applications, efforts to standardize data links have resulted in the use of Common Data Link (CDL) for communications with UAS.
- Unfortunately, no similar standard for comparably secure communications exists in civilian applications.
- This problem needs to be tackled when aerospace and defense industry gradually turns to commercial-off-the-shelf technologies (COTS) and architectures, for example, standards-based LTE architecture.
Approach:

• The main challenges to UAS security, especially in civilian applications, are small size, weight constraints, and weak computational power of onboard data processing equipment.

• To overcome these challenges and significantly improve the security of wireless data links, we need new security technologies to complement conventional cryptography.

• One of the most promising approaches for improving security of wireless links is to exploit the physical-layer characteristics of the wireless channel.
Physical-layer security solutions:

- Channel-based approaches,
- Information-theoretic approaches,
- Code-based approaches,
- Power-based approaches,
- Signal-design approaches
Channel-based approaches:

- In channel-based physical layer security, the local measurements of a radio channel are used to construct secret keys which can be then used as cryptographic keys in other communication layers.
- This process is typically referred to as the key extraction.
Information-theoretic approaches:

- Information-theoretic security can be achieved by using special secrecy coding or intelligent jamming.
- In information-theoretic approaches one attempts to arrange communication channels in such a manner that the signal-to-noise ratio (SNR) observed by legitimate user is much greater than the corresponding SNR observed by eavesdropper.
Other approaches:

- In code-based approaches, spread-spectrum modulation techniques are typically used to obscure information transmission.

- Power-based approaches include various schemes with smart antennas and artificial noise injection schemes. In those schemes, the basic objective is to make the adversary’s channel noisier than the legitimate user channel.

- Signal-design approaches include various transmission schemes where, for example, special wave modes are used to carry information messages or an artificial noise is injected into transmitter signal to impair the adversary’s ability to correctly estimate the channel.
Phase-mode-excitation beamformer:
Benefits:

• Physical-layer security solutions are complementary to already existing security solutions.

• In physical-layer security solutions only the signals at the physical layer are processed and thus the security of wireless links is enhanced in a simple and energy-efficient way.

• Physical-layer security solutions require very limited interaction with upper layers of the transmission protocol and with network management.

• Physical-layer security solutions are able to seamlessly address a wide class of wireless applications in the coming future.