Implementation of cryptographic protocols for civil UAV communications

R. Aissaoui

ENAC, ReSCo, Toulouse, France.

Research Team

- Ridwane Aissaoui, Ph.D. Student
- Jean-Christophe Deneuville, Thesis director, Associate Professor
- Alain Pirovano, Thesis director, Associate Professor

Context

- The UAV industry is currently experiencing a massive growth of approximately 13% yearly [1]. It is therefore important to develop new systems in order to prevent incidents caused by UAVs. One of the most urgent problem faced is the protection against cyber attacks perpetrated by illegitimate users.
- The communications between a drone, its pilot, other drones and an eventual Traffic control need to be defended against several types of attacks. Protecting the control and data links is a task done through the use of cryptography, which grants authentication, confidentiality and integrity to the signals exchanged with a drone.
- Micro and nano drones (<2kg) have very limited onboard computational power available, and a limit in the bandwidth they can transmit. The usual cryptographic methods used over the internet cannot be used here, due to these restrictions.
- With future European regulation allowing more unmanned flights, a secure communication link will be required for drones to be integrated into the public airspace and allowed to fly beyond the visual line of sight.

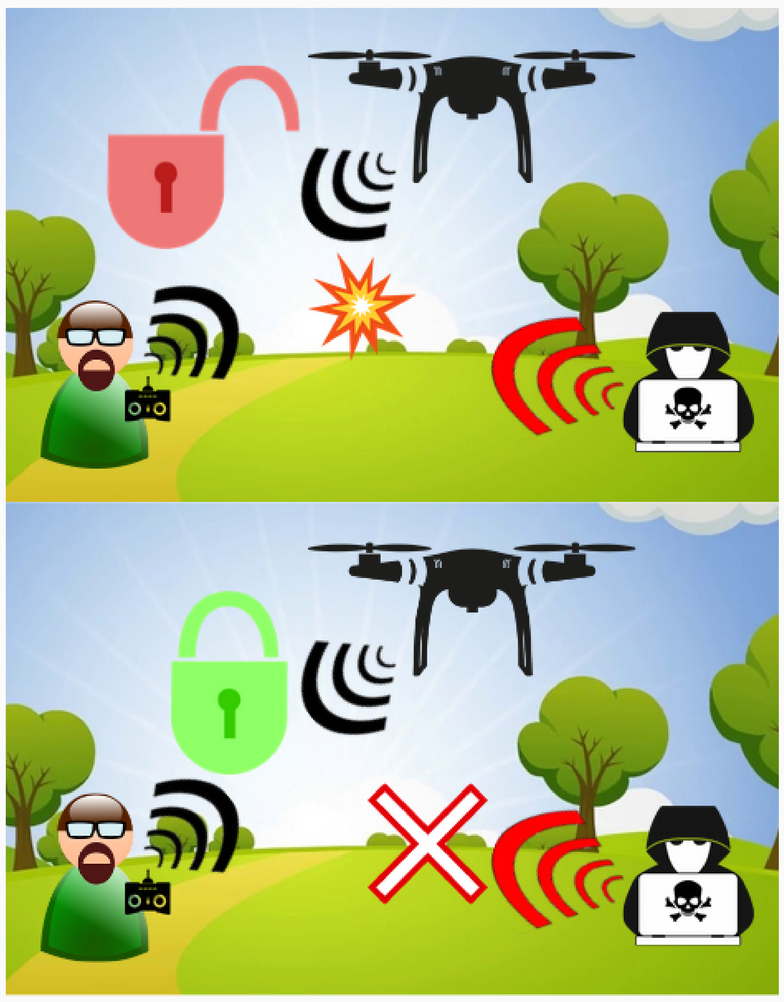

Figure 1: Unsecure Communication and secure link against an attacker

Objectives of the PhD thesis

- Implementing robust and efficient protocols able to garantee authentication, confidentiality and integrity to the data exchanged between the drone and the control station, other UAVs as well as the UTM (Unmanned Traffic Management).
- Within the contraints of small systems with limited communication ability and processing power, the use of lightweight cryptographic solutions will be necessary[3].
- Testing this solution on a network simulation tool in order to evaluate and validate the protocol by emulating real-time systems. Roughly estimating the performance loss due to the addition of a cryptographic protection. Then testing the solution in real life conditions on different UAV systems.

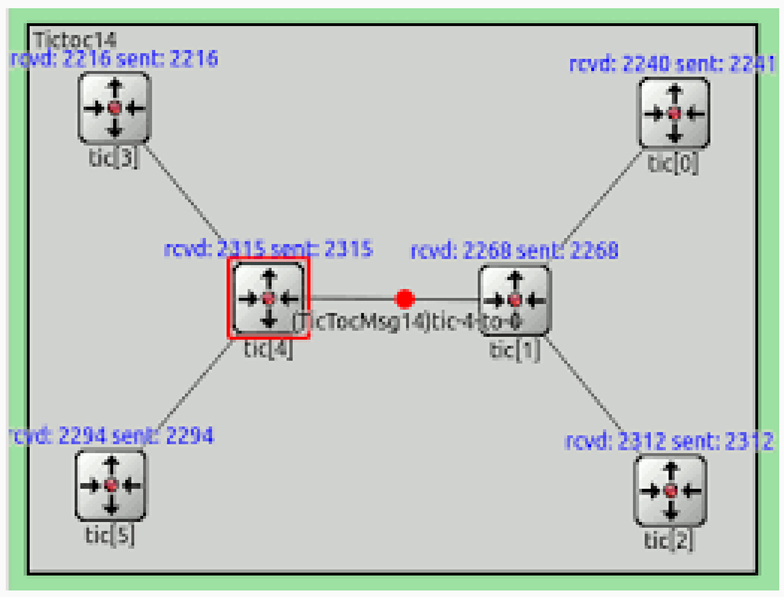

Figure 2: Network Simulation with OMNeT++ [2]

References

[1] Federal Aviation Administration. FAA Aerospace Forecast – Fiscal Years 2019-2039. FAA reports, 2019

[2] OMNet ++ Technical Articles https://docs.omnetpp.org/

[3] M Emin et J Morvan, Rapport de PIR : Étude de protocoles sécurisés pour les communications drones.