dtec.bw

JAHRESTAGUNG 2024

Adaptive C-UAS Swarm with Ad-hoc 5G-SA Network

K. Tebbe , R. Pommeranz, G. Scholl
Chair for Electrical Measurement Engineering
Helmut-Schmidt-University, University of the Federal Armed Forces Hamburg

AI-Based Location Analysis and Autonomous Mission Execution in Jammed Environments

Abstract

Threat scenarios with hostile Unmanned Aerial Vehicles (UAVs) are becoming increasingly difficult to handle. Additional to the variety of UAV types with their different capabilities, the situation will become even more difficult when Global Navigation Satellite Systems (GNSS) are occasionally jammed or unavailable [1]. Therefore, C-UAS (Counter-Unmanned Aerial Systems) need to have a robust communication for a reliable operation. Our C-UAS solution, where multiple UAVs interact to prevent a potential threat, operates agile and autonomously to cover a broad range of scenarios also in hostile environments. By using an ad-hoc 5G airborne network with AI-based carrier frequency selection, swarm communication in jammed environments will be feasible. Communication traffic will be exchanged between Public 5G Mobile Networks and the Private HSU 5G Campus Network, established under the dtec.bw-DS2CCP project [2].

Concept

This work presents an AI-based approach to protect, e.g. critical infrastructure or military areas against UAV threats. The upper part of Fig.1 shows the system idea consisting of the C-UAS swarm to be developed and hostile UAVs, eventually controlled by an operator close to the scene. This C-UAS solution will be able to be operated also in GNSS-denied areas employing as relevant operational and navigation data are derived from on-board sensors communicated by the Swarm Coordinator. The Swarm Coordinator is hosting the 5G-SA core parts and RAN (Radio Access Network) [4] of an airborne 5G network. Information is exchanged with all swarm members using a frequency-agile 5G connection. In a classical urban environment all requirements imposed by the national network agency can be met. In a hostile environment the operational frequency is adapted according to the threat scenario. Initially, if a potential threat is detected, e.g. using a ground-based sensor system, positions and velocities of the hostile UAV swarm are transmitted to the Swarm Coordinator by the ground station. A second UAV in the vicinity of the Swarm coordinator localizes and classifies the hostile UAVs with its own on-board cameras and antennas, including model and current flight mode. With this information the Operator (Command & Control) can choose the most suitable effector-UAV combination (manual intervention or AI-based, soft- or hard-kill), which in our scenario could be a jammer, net launcher or kamikaze drone. A part of this solution is the net launcher previously developed in the C-UAS FALKE project [5]. The lower part of Fig.1 visualizes the backbone of the C-UAS system. C-UAS data is transmitted into the cloud platform [2] through a VPN tunnel across a public 5G network, where data can be processed by a high-performance computing cluster (HSUper) [6] with very low latency times. All data acquired are used to train an AI program suite.

Scope

This project explores advancements in UAV swarm technology across different technology domains. Software solutions for reliable UAV swarm navigation in GNSS-denied areas are developed. Additionally, AI models are used to classify hostile UAVs, enhancing situational awareness. And a robust AI-enhanced frequency-agile 5G communication solution will be implemented, which can be adapted to various jamming techniques. The integration of existing and new effector UAVs increases the versatility of the C-UAS system. In the first step the Counter-UAS UAS developed in the FALKE [5] project will be integrated. A second effector UAV with extensive jamming capabilities will be designed and integrated into the Counter-UAV-swarm.

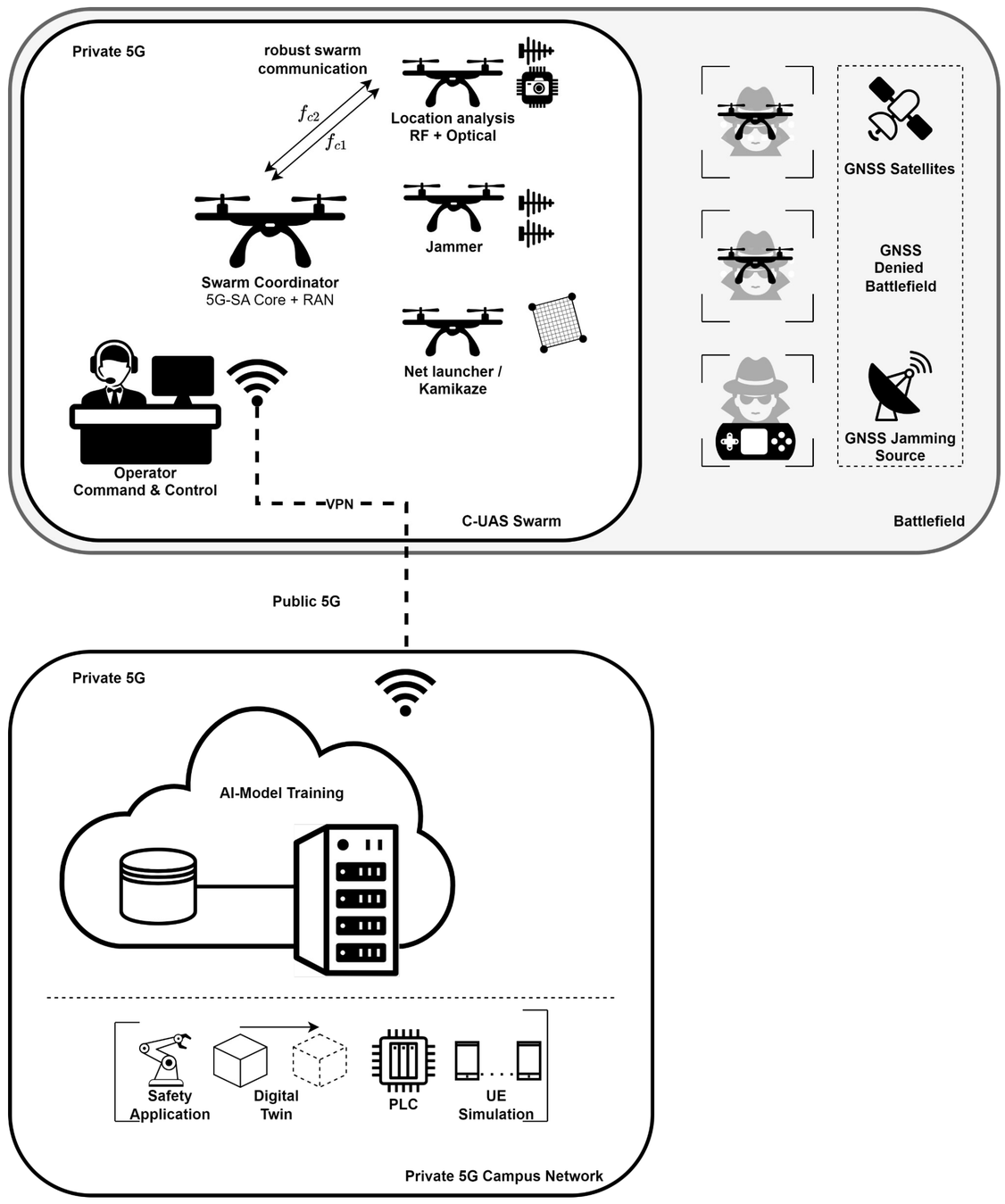

Fig. 1: Adaptive C-UAS Swarm in the Battlefield connected to a Private 5G Campus Network via VPN over public 5G

References

[1] 2019. [Online]. Available: https://www.timesofisrael.com/flights-at-ben-gurion-airport-suffer-weeks-of-interruption-to-gps-systems/
[2] Helmut-Schmidt-University, “DS2CCP – Entwicklung einer digitalen Sensor-2-Cloud Campus-Plattform,” dtec.bw Project website: http://dtecbw.de/home/forschung/hsu/project-ds2ccp.
[3] Rohde & Schwarz PACE , Advanced protocol and application classification with metadata extraction for application-aware networking, online available: https://www.ipoque.com/products/
[4] F. John, J. Schuljak, L. B. Vosteen, B. Sievers, A. Hanemann and H. Hellbrück, "A Reference Deployment of a Minimal Open-Source Private Industry and Campus 5G Standalone (SA) System," 2022 IEEE 10th International Conference on Information, Communication and Networks (ICICN), Zhangye, China, 2022, pp. 1-9, doi: 10.1109/ICICN56848.2022.10006563.
[5] Wentzel, Alexander, Jan Cornils, and Marco Valentin. “Compact Counter-UAS System for Defeating Small UAV in Complex Environments”, 9.-10. Okt. 2023, Copenhagen, Denmark.
[6] Neumann, P./Duffek, J./Kleinschmidt, J./Leinen, W./Breuer, M./Schmidt-Lauff, S./Fink, A./Mayr, M./Firmbach, M./Popp, A. & Auweter, A. (2022): hpc.bw: A Supercomputer with Competence Platform for the Universities of the FederaIn: Schulz, D./Fay, A./Matiaske, W. and Schulz, M. (eds.): dtec.bw-Beiträge der Helmut-Schmidt-Universität. Forschungsaktivitäten im Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr dtec.bw. Band 1. Hamburg: OpenHSU, pp. 305–310. https://openhsu.ub.hsu-hh.de › openHSU_14569l Armed Forces.

unibw.de hsu-hh.de dtecbw.de

Digital Sensor-2-Cloud Campus-Platform

gefördert durch
dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr
Finanziert von der Europäischen Union
NextGenerationEU