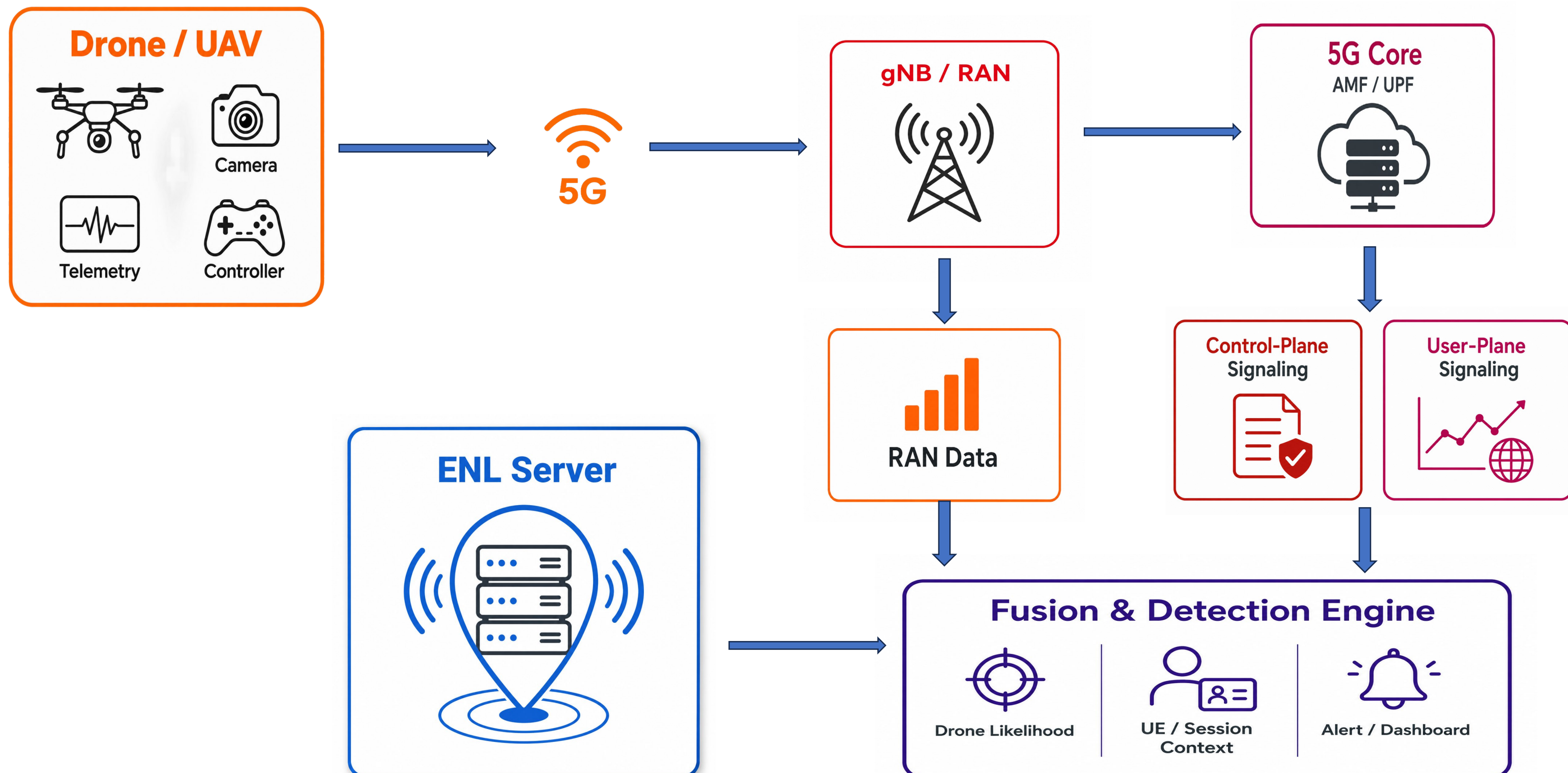


# Drone Detection over 5G Cellular Networks

Kunal Singh, Song Son Ha, Gerd Scholl



## Motivation

- Drones are increasingly used for surveillance, delivery, inspection, and autonomous operations, but unauthorized drones can also create serious safety and security threats, including intrusion into restricted areas, disruption of airports, illegal surveillance, smuggling, and potential attacks on critical infrastructure.
- Modern drones can use public or private 5G networks for command and control, telemetry, navigation data, and high-bandwidth video streaming, making cellular connectivity an important part of their operational footprint.
- Conventional RF-based drone detection mainly observes over-the-air emissions and may struggle with interference, encrypted communication, or drones using standard cellular links.
- Our goal is to detect and identify probable drone activity from 5G network observations by correlating RAN behaviour, control-plane signalling, UE/session information, and user-plane traffic patterns.

## Key Indicators

- 5G RAN: Radio-access and mobility behaviour of connected User Equipment's.
- Control Plane: Registration, signalling, and session-management information.
- User Plane: Application and traffic behaviour carried through the 5G network.
- UE & Session Context: Correlation of device identity and active network sessions.
- Drone Communication: Command-and-control, telemetry, and video-streaming activity.
- Cross-Layer Correlation: Combined evidence from RAN, control plane, and user plane to determine drone likelihood.

## Use Cases

- Critical infrastructure protection — detection of unauthorized drones near military sites, power plants, ports, industrial facilities, or communication infrastructure.
- Airport and restricted-airspace monitoring — identifying suspicious cellular-connected drones operating close to protected areas.
- Public-event security — monitoring drone activity around stadiums, concerts, demonstrations, and large gatherings.
- Private 5G campus security — detecting unexpected or unauthorized UAV activity within industrial or enterprise 5G networks.
- Drone identification and tracking — correlating a detected drone with its cellular UE and network session.
- Network-assisted threat assessment — distinguishing normal mobile devices from drone-like activity and providing a drone-likelihood score to a security system.
- Multi-sensor drone defence — using 5G-network observations together with RF, radar, camera, or acoustic sensors to improve detection confidence and reduce false alarms.

## Conclusion

A 5G network can provide a valuable additional sensing layer for drone detection. By combining information from the RAN, control plane, user plane, and UE/session context, suspicious drone-like communication behaviour can be identified without relying on a single indicator. The proposed approach enables network-assisted drone detection, identification, and situational awareness and can complement conventional RF, radar, acoustic, or visual sensing systems.



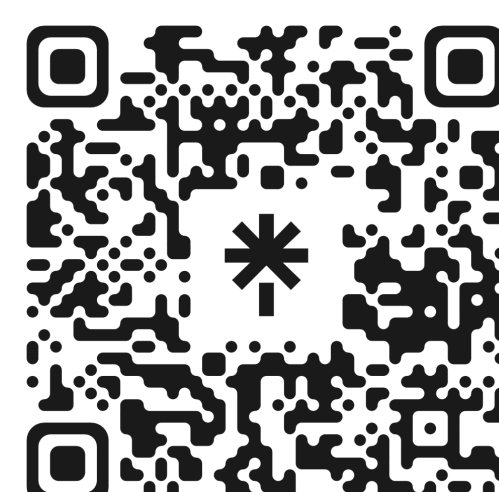
unibw.de



hsu-hh.de



dtec.bw.de



gefördert durch

dtec.bw

Zentrum für Digitalisierungs- und  
Technologieforschung der Bundeswehr

Finanziert von der  
Europäischen Union  
NextGenerationEU