ON MULTIPLE SENSOR UAS SECURITY

RESEARCH ASPECTS AND FIRST EXPERIMENTAL RESULTS

Wolfgang Koch

wolfgang.koch@fkie.fraunhofer.de
Fraunhofer FKIE, Dept Sensor Data and Information Fusion
Fraunhoferstrße 20, D-53343 Wachtberg (Germany)

Abstract

Unmanned Aerial Systems UAS, also called *drones*, revolutionize the market for mobility based services and enable more efficient defence and police operations. A new generation of SME founders opens up innovative products and business models with barely foreseeable consequences for the everyday life of people. Also this rapidly developing technology, however, proves to be Janus-faced. Despite their unquestionable benefits, UAS increasingly pose serious safety and security threats. In this paper, we wish to identity relevant research questions to be answered before any effective drone threat recognition and countering system can be developed. First experimental results illustrate the key role of multiple sensor data fusion algorithms for detecting, tracking and classifying UAS.

Keywords: unmanned aerial system UAS, UAS detection / tracking / classification, multiple sensor data fusion, heterogeneous sensors, electronic counter measures.

1 SAFETY AND SECURITY ISSUES OF DRONES

Protection against any undesired use of drones is not only demanded in the interest of public safety and security, but is also an increasingly important requirement for protecting military and police forces in their challenging missions, which in turn leads to innovative product ideas. Evidently, systems for protecting against threats and risks related to drones play a crucial role for enabling socially accepted, legally regulated and commercially viable drone applications and to develop the huge market potential for new mobility services made technologically possible by drones [1].

The photo showing a popular toy drone hovering before the amused Chancellor Angela Merkel and her frightened minister of interior affairs, also responsible for Merkel's security, was distributed around the world. Its payload could easily have been an explosive device. Security specialists have for a long time been concerned about "Airborne Improvised Explosive Devices" that can be easily deployed by "everyday drones". A simple Google search reveals the global dimension of this new threat: "Drone Causes Power Cut in San Francisco", "Flight delayed at Heathrow When Drone Flies Over One of its Runways", "Drone Used to Smuggle Drugs into Prison", "A Drone Rattles the White House". Drones have also been used spying on industrial plants, product prototypes under development and critical infrastructures, such as nuclear power plants. Another abuse has been for covert recording of sensitive conversations by flying directional microphone drones.

Protection against drones, however, must not hinder their intended use. In the public domain, the safety and security issues should be harmonized with the social and economic opportunities presented by this new dimension of mobility. In dealing with the risks related to automobile mobility, a triple strategy is likely to be successfully utilized here: Any mobility related safety and security concept is expected to be based on a legal framework, on appropriate insurance products and on safety and security technologies, which need to be investigated and developed by research institutions and industry.

Fig. 1 shows a schematic view of a modular and scalable sensor data fusion architecture with standardized interfaces for drone reconnaissance. It is the very basis of any technical counter UAS system. The multiple sensor data fusion algorithms needed for this new application are available and need only to be appropriately adapted. See [2], for example, as a reference.

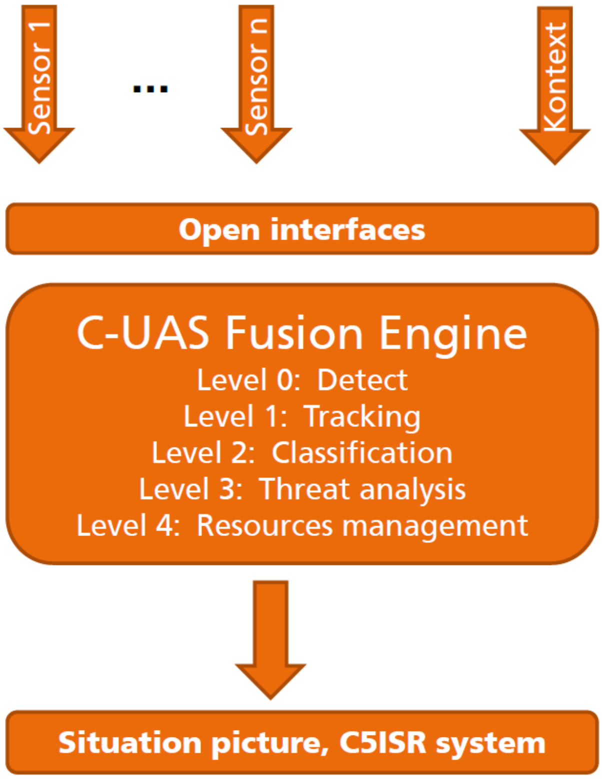

Fig. 1: Schematic view of a modular and scalable fusion architecture for Counter UAS with standardized interfaces.

For this reason, an electronic labeling requirement similar to car license plate is foreseeable for drones as well, which is based on transponder technologies used in air traffic control. Under discussion are “drone pilot’s licenses” and “electronic ignition keys". By automated drone identification systems, registered drone traffic can be observed and identified, as such, at any time. This would also indicate whether there is any non-cooperative and potentially threatening use of drones. In addition, geo-fencing is a viable option in establishing "no-fly zones" using geographic information systems. Since financial risks related to drone-based mobility services may easily exceed the resources of private individuals or companies, a new line of drone-related insurance products is likely to be developed. See reference [3] for a comparable discussion of socially, legally and ethically relevant issues in security assistance systems.

Which technology is to be chosen? What is to be protected against drone threats and by whom? Under consideration are especially low-signature Unmanned Aerial Systems, which are popular and their distribution is difficult to control. Because they can operate in a highly agile manner and achieve high speeds, the response times for any countermeasures are short.

2 MULTIPLE SENSOR DRONE THREAT ASSESSMENT

In order to detect drone threats quickly and reliably, we first need high performance sensors capable of detecting complementary characteristics of approaching drones. By utilizing efficient algorithms of multiple sensor data fusion, a suit of heterogeneous sensors can be integrated into a drone detection system. Fig. 2 illustrates the experimental setup of a measurement campaign for counter UAS at Fraunhofer FKIE in September 2015, where E/O, IR, acoustic and passive radar sensors have been used, their data fused and the results evaluated. Further research and experimentation is in progress with industrial partners. Fig. 3 shows two readily available drones from different weight classes and with different sensor signatures.

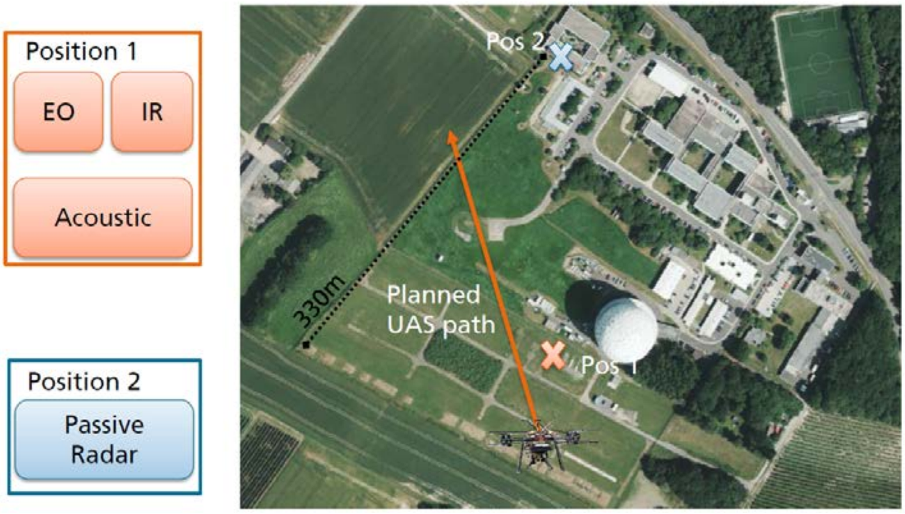

Fig. 2: Experimental Setup of a measurement and data fusion campaign counter UAS at Fraunhofer FKIE (September 2015) exploiting E/O, IR, acoustic and passive radar.

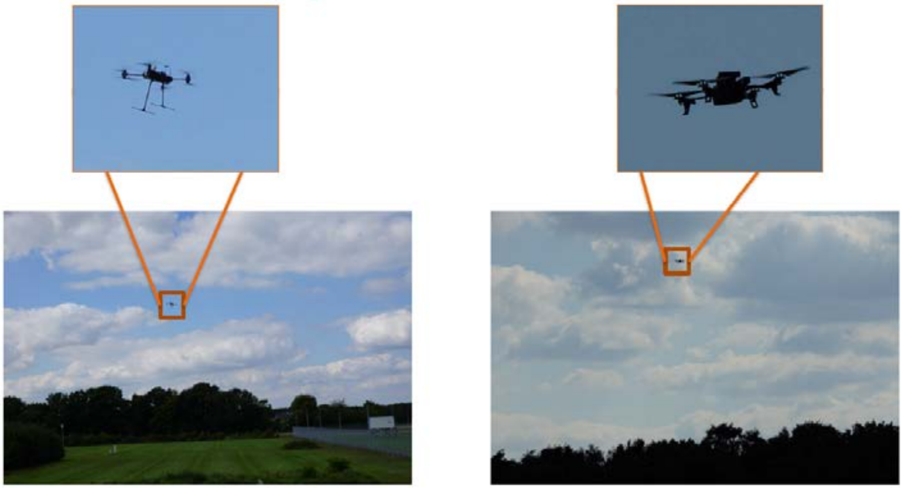

Fig. 3: UAS used for multiple sensor experimentation – weight > 8 kg and < 0.4 kg

Because of its range and all-weather capability, radar optimized for drone detection is the backbone sensor. Radar systems send signals either themselves or use existing "electro smog" as a source of illumination. Echoes reflected from drones are analyzed to estimate position and velocity, as well as to provide clues for classification. Passive radar uses radiation from mobile phone base stations for illumination, e.g. Since transmission permits for active radar operation are rarely granted, passive radar enables surveillance wherever mobile phones are working, and illuminate the airspace predominantly used by drones without any emission load. Fig. 4 shows an experimental passive radar system developed by Fraunhofer FKIE which exploits electromagnetic illumination provided by the broadcast signals of GSM mobile phone base stations. In the experiment, six illuminating GSM base stations have been used.

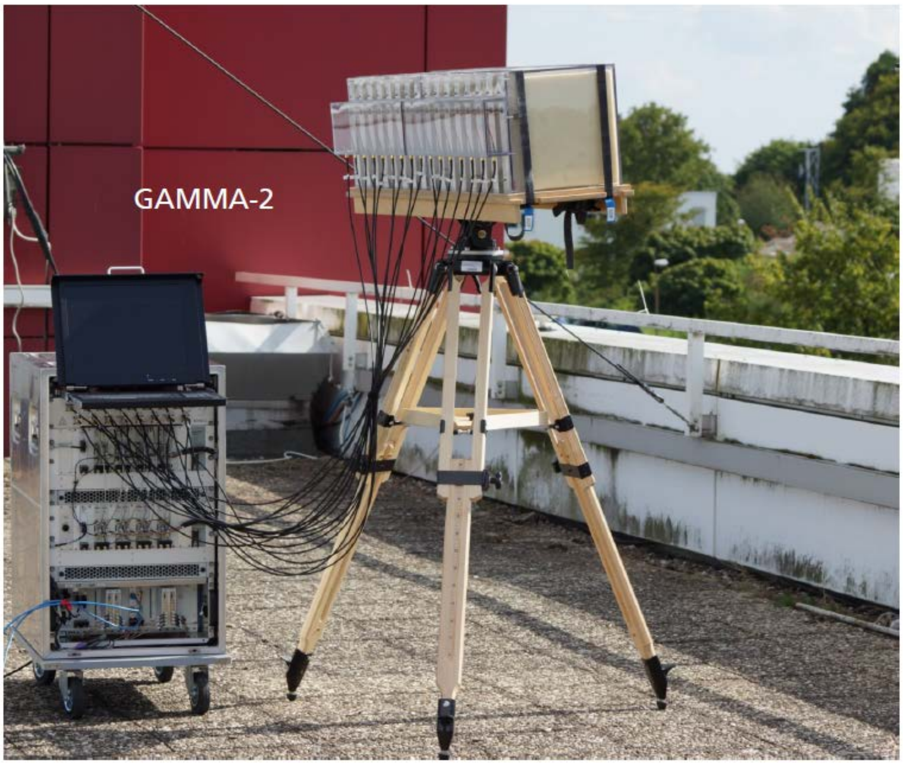

Fig. 4: Experimental passive radar exploiting six illuminating GSM base stations. In the measurement campaign, GPS-loggers provided the ground truth.

Overall design principles of GSM passive radar and experimental results related to security applications are discussed in reference [4]. For a comprehensive introduction into multistatic tracking see reference [5]. Fig. 5 shows a range-Doppler diagram where the expected Doppler frequency of the reflections caused by a drone according to ground truth is indicated over time. The comparison clearly indicates the suitability of GSM passive radar for drone detection applications in general.

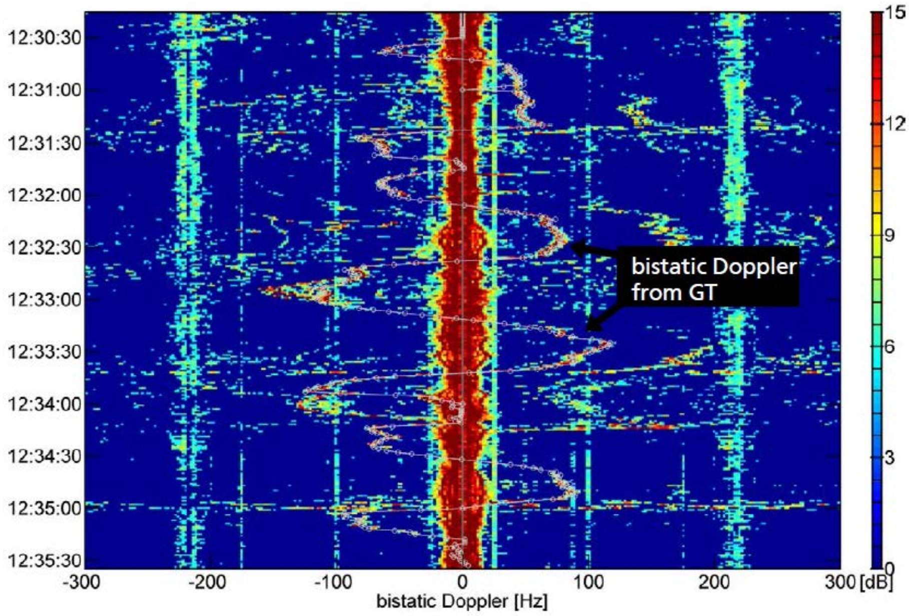

Fig. 5: Range-Doppler diagram with expected Doppler frequency according to ground truth over time. This provides a first confirmation of successful UAV detection.

In figures Fig. 6 and 7, preliminary results on solving illuminator-to-drone association problems are illustrated. These results are basic for ongoing work on developing and evaluating appropriate track-before-detect and drone tracking algorithms. Fig. 6 shows the number of correctly associated signal processing results to the ground truth whenever the estimation error of kinematic parameters (bistatic range, bistatic Doppler, azimuth) are below a certain threshold. The number of correct associations over the actual flight path of the UAS is illustrated in Fig. 7.

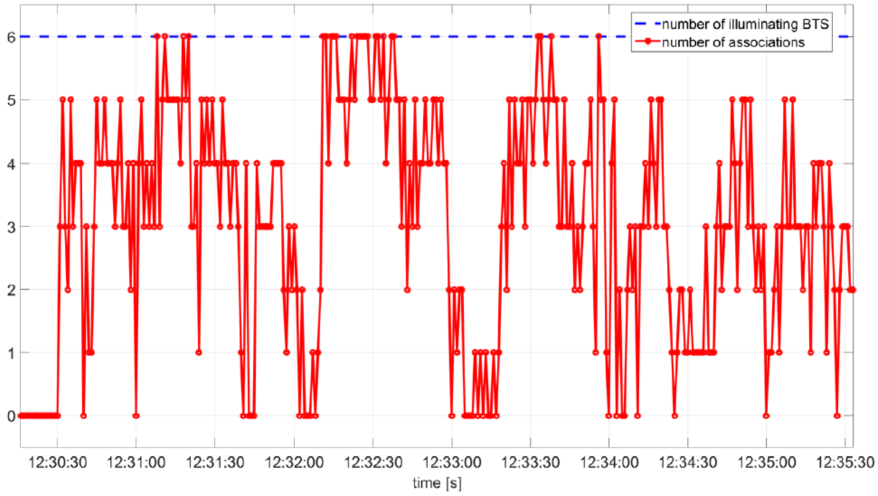

Fig. 6: Association of signal processing results to the ground truth wherever the estimation error of kinematic parameters are below a certain threshold.

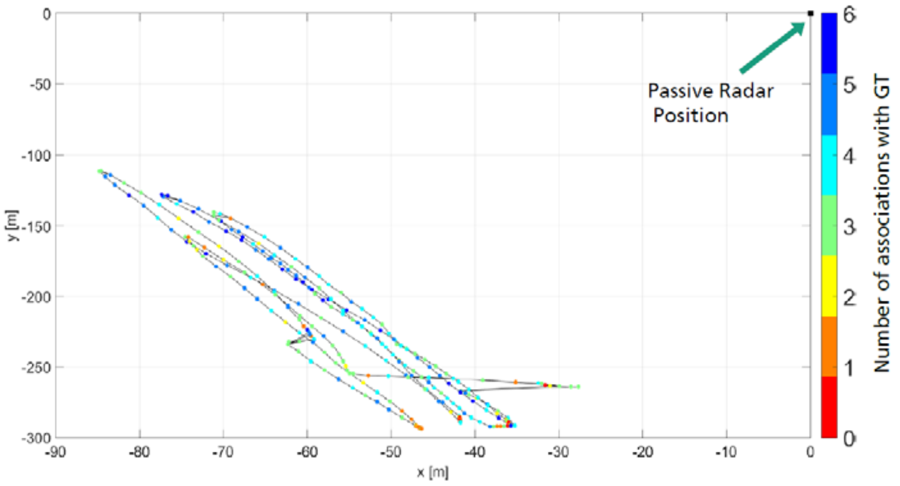

Fig. 7: The number of associations over the flight path illustrates the suitability of GSM passive radar for detecting and tracking UAS.

Radar data are to be fused with data streams provided by imaging sensors, typically covering several spectral regions [6]. Although they usually achieve lower ranges than radar sensors and are relying on weather conditions and the time of day, their resolution capabilities may well facilitate the target classification task and further reduce false alarm rates by using multiple sensor data fusion. Track-before-detect algorithms based on inhomogeneous Poisson point processes have been proven to provide a powerful methodology [7, 8]. Fig. 8 illustrates the chosen sensor data fusion approach.

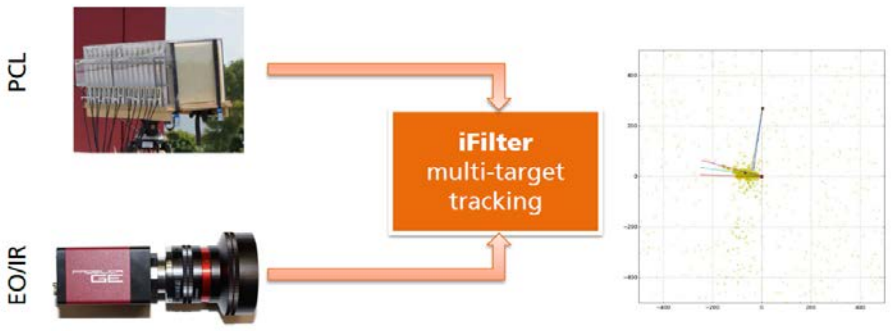

Fig. 8: Fusing GSM passive radar results with E/O-IR using intensity filtering.

Furthermore, emissions produced by the drones themselves enable drone detection, for example, emissions due to remote control. For details see reference [9]. Using appropriate data exploitations algorithms, a drone and its pilot can be localized. Also autonomously operating drones build up intermittent data links. Encouraging results have been obtained from acoustic emissions, which are detected by microphone networks. Therefore, array signal processing techniques are important [10].

The relevance of multiple sensor data fusion is thus evident. For sensor and resources management, however, game theoretical methods are required that enable robust system solutions.

3 REMARKS ON COUNTERMEASURES

Although their threat potential is high, “everyday drones" have the advantage of offering little electronic self-protection measures due to payload limitations. "Soft kill" measures may, therefore, limit their functionality. "Hard kill" measures, for example projectiles, laser, or high energy electromagnetic pulses, are excluded here because one wishes to avoid crashes with incalculable consequences in view of the chemical, biological, radioactive and explosive payloads that are possibly to be taken into account. The assessment and minimization of collateral damage must therefore accompany any discussion of done countermeasures.

To a certain extent, known methods of electronic warfare can be used to “hijack” the remote control of a drone. This is actually rather simple in the case of WLAN-based approaches. For more demanding, but increasingly common communication links the challenges are much larger. If a drone operates autonomously, the jamming or deception of satellite navigation can be appropriate (navigation warfare). The extent to which this is possible in a civil environment and the assurance that only potentially threatening drones are affected raise many research questions.

Whenever a drone is used for spying purposes, the data downlink or the sensors used can be disrupted by electromagnetic countermeasures. In a spying operation, where the sensor data is collected on board the drone and is not transmitted, the drone operator would be forced to bring the drone back into his possession. As a countermeasure, the drone would be tracked to lead directly to the perpetrators.

Whenever kamikaze drones are to be expected, intercept drones are an option that try to neutralize the undesirable drone by a network and transport it to a safe destination. It does not seem necessary to emphasize the great challenges in platform, sensor and control technologies that are implied by this approach.

Also, the problem of counter drone defense has to be considered: What can be done to ensure the use of drones in presence of counter drone technologies used by potential adversaries?

4 CONCLUSIONS

Advanced algorithms of multiple sensor data fusion and management of sensors play a key role in designing counter drone systems. In the context of C5ISR systems (Command, Control, Communications, Computer, Cyber, Intelligence, Surveillance and Reconnaissance), the technological challenges can be met, but require close cooperation between the military and police forces, research institutes and the relevant industries. In the protection of stationary equipment and mobile units in urban or open terrain, the integration of drone detection / tracking / classification in decision support systems is crucial.

REFERENCES

[1] W. Koch. *Multisensorielle UAS-Abwehr - Forschungsaspekte einer technologischen Herausforderung*. DWT Symposium „Angewandte Forschung für Verteidigung und Sicherheit in Deutschland“, Februar 2016, Bonn.

[2] W. Koch. *Tracking and Sensor Data Fusion – Methodological Framework and Selected Applications*. Springer Mathematical Engineering Series. 2014.

[3] W. Koch. *The Role of Context in Multiple Sensor Systems for Civil Security*. Chapter 5 in: L. Snidaro, J. Garcia, J. Llinas, E. Blasch (Eds.). *Context Enhanced Information Fusion – Improving Real World Performance with Domain Knowledge*. Springer Series on Advances in Computer Vision and Pattern Recognition (2016).

[4] M. Broetje, B. Knoedler, W. Koch. *Evaluation of GSM Passive Radar Data and Its Use in Multistatic Tracking*. 19th International Conference on Information Fusion (FUSION), Heidelberg, Germany, 2016.

[5] M. Daun, U. Nickel, W. Koch. *Tracking in multistatic passive radar systems using DAB/DVB-T illumination*. In: EURASIP Signal Processing, Vol. 92, Nr. 6, pp. 1365–1386 (2012).

[6] W. Koch. *Situationsanalyse durch multispektrale Sensordatenfusion – Architekturen und Experimente*. DWT Symposium „Angewandte Forschung für Verteidigung und Sicherheit in Deutschland“, Februar 2016, Bonn.

[7] M. Schikora, W. Koch, R.L. Streit, D. Cremers. *Sequential Monte Carlo method for the iFilter*. 14th International Conference on Information Fusion (FUSION), 2011.

[8] M. Schikora, D. Bender, W. Koch. *Airborne emitter tracking by fusing heterogeneous bearing data*. In: 17th International Conference on Information Fusion (FUSION), 2014.

[9] D. Musicki, R. Kaune, W. Koch. *Mobile emitter geolocation and tracking using TDOA and FDOA measurements*. In: IEEE Transactions on Signal Processing, vol. 58, nr. 3, pp. 1863-1874 (2010).

[10] M. Häge, W. Koch. *Threat Recognition with Various Distributed Sensors*. In: NATO IST-SET-126 Symposium on “Information Fusion (Hard and Soft) for ISR”, May 2015.