Achieving Full Cognitive Autonomy In Drone Navigation for Smart City Applications

DOI: https://doi.org/10.62658/COFAC/ILIND/COPELABS/4/2023

Project Reference: COFAC/ILIND/COPELABS/4/2023

Slavisa Tomic[1]

Principal Investigator

01/06/2024 – 30/11/2025

Project Date

Team members:

Marko Beko[1], Luís Manuel Camarinha-Matos[2], João Pedro Leal Abalada de Matos Carvalho[1], Ricardo Jorge Serras Santos[1]

1. COPELABS: Centro de Investigação em Computação Centrada nas Pessoas e Cognição
2. CTS-UNINOVA – Instituto Desenvolvimento de Novas Tecnologias, Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa

Abstract:

The main goal of this research is to motivate disruption of traditional design principles and revolutionize the development of localization systems so that they can accompany the growth and overcast vulnerabilities in the forthcoming technologies. Perhaps the biggest threat is related to security; thus, we believe that it is time to "de-virtualize" and "get physical" again in order to fully secure future intelligent wireless systems, such as 5G and beyond. Boosting security can be achieved by exploiting location information as an additional security parameter to prevent undesirable scenarios and potential casualties (e.g., drone collision, car hijacking, identity thefts, etc.).

Most existing localization systems are intended for non-adversarial settings, in which no malicious/damaged devices are assumed to exist. This makes them highly susceptible to spoofing attacks, where devices can counterfeit their own locations or can manipulate location estimations of other devices in the network (e.g., by reporting false distance measurements). In contrast to the existing systems, this research will be based on a cross-layer approach and will address the following paramount questions: 1) Physical layer. How to design secure location estimation techniques that provide resilience to physical-layer attacks, but preserve the performance (accuracy and execution time) of their non-secure counterparts? 2) Link layer. What are the right coding schemes to detect attacks at the link-layer? How can we use them to prevent attacks from occurring and what are their scalability limits? 3) Systems. How can developed solutions be integrated in mobile platforms, especially within untrusted environments? How can this integration strengthen the security of the solutions and support their use in a wide range of applications?

Therefore, we seek to widen our knowledge about attacker models and understand the fundamental limits on the localization security under realistic models, and ultimately develop a fully-secure localization solution in the form of a prototype application.