## Case Study 1: Securing Drone Communications Against New Electromagnetic Meta-Surfaces and Inferring their Trustworthiness in Wider Air Spaces

*Weisi Guo & Zhuangkun Wei*

This case study contains 4 bodies of work – see Figure S1.1. As drones fly close to terrestrial communication networks, their signals will interact with one of the most significant recent innovations – electromagnetic (EM) meta-surfaces / reflecting intelligent surface (RIS).

(1) These have the power to modify the EM channel, potentially expanding the channel capacity but also (we show for the first time), compromise certain security attributes such as channel-dependent key generation [S1.1].

(2) We go on to develop a world first in developing digital security attributes from physical swarm drone flight characteristics by exploiting mutual control states [S1.2]. We achieve triple verification through information theory, simulation, and experimentation.

(3) Our work in TAS-S attracted early-career-researchers (ECRs) to my wider team and two of them both won RAEng IC fellowships (Adolfo Perrusquia 2021-23; Deepak Panda 2023-25). Their work collaborated with the core TAS-S team to answer: (3a) would a third party find the drones trustworthy if they had no backdoor access to the algorithms, and (3b) how would adversarial AI attacks affect their safe navigation in future air spaces. In 3a, we developed control-physics informed machine learning to infer the intention of such drones [S1.3], with the wider body of work factoring in multiple sensory and communication aspects. In 3b, we develop robust reinforcement learning against conflict-induced spoofing in air traffic coordination [S1.4].

(4) We ask how can contextualise the RL work by using human prompts to change how RL elements (e.g., policy change or cost functions) can be affected [S1.5]. Our initial demo can turn different ethical ideas into different RL navigation outcomes.

The impact of the work has been felt across a wide range of UK government and commercial bodies, many of whom were part of the original TAS-S setup, and others joined later:

- [Academic] We have since then used the outcomes to successfully develop research as part of the new £11m EPSRC 6G Future Communications Hub (led by Imperial) and won 2 RAEng IC fellowships.
- [Government] We have developed strong collaborations with drone risk at Department for Transport, given evidence to JSARC at Home Office, and have a data sharing agreement to develop trustworthy monitoring of drones across UK with NPCC.
- [Commercial] We are developing and enhancing our strategic relationships on airborne autonomy with Leonardo UK who has co-funded 2 research fellows. Other partners such as Thales UK and Saab UK have together funded 3 EPSRC PhD studentships in the above areas.

- [Public Engagement] Our work in [S1.5] is on a website (https://ntutangyun.github.io/tas-demo/), which allows us to diverse expert and public users to play with LLM-driven RL guided navigation.

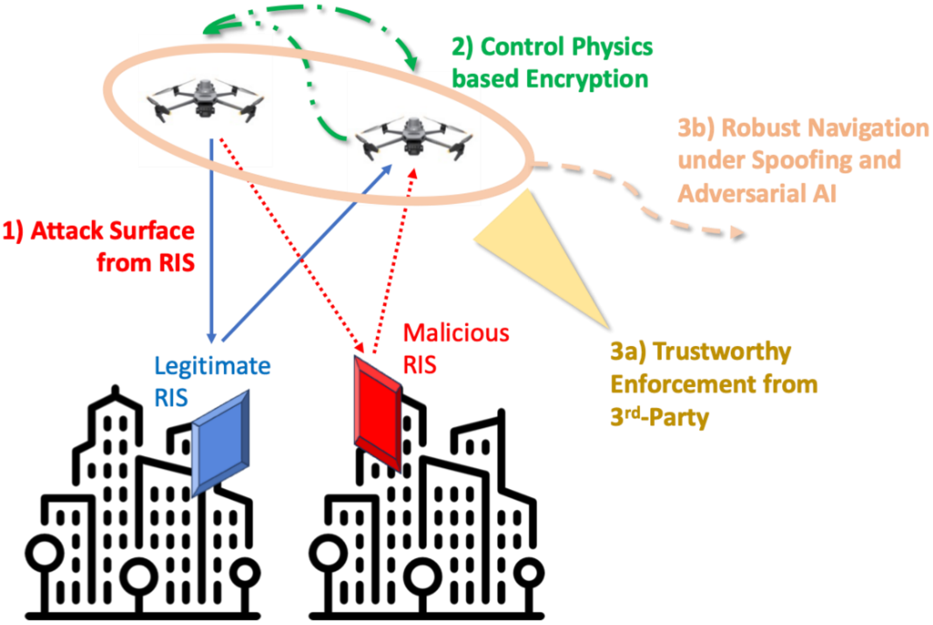
2) Control Physics based Encryption
3b) Robust Navigation under Spoofing and Adversarial AI
1) Attack Surface from RIS
Malicious RIS
Legitimate RIS
3a) Trustworthy Enforcement from 3rd-Party

*Figure 1: Swarm Drone Security and Trustworthiness: 1) communication security compromise from RIS attacks, 2) de-coupling digital communication security by exploiting swarm control physics, 3a) achieving trustworthiness from 3rd party perspective, and 3b) achieving navigation ecosystem security against adversarial AI.*

### References

[S1.1] ‘Adversarial Reconfigurable Intelligent Surface Against Physical Layer Key Generation,’ Z. Wei, B. Li, W. Guo, IEEE Transactions on Information Forensics & Security, 2023

[S1.2] ‘Control Layer Security: Exploiting Unobservable Cooperative States of Autonomous Systems for Secret Key Generation,’ Z. Wei, W. Guo, IEEE Transactions on Mobile Computing, 2024

[S1.3] ‘Uncovering Drone Intentions using Control Physics Informed Machine Learning,’ A. Perrusquia, W. Guo, B. Fraser, Z. Wei, Nature Communications Engineering, 2024

[S1.4] ‘Action Robust Reinforcement Learning for Air Mobility Deconfliction against Conflict Induced Spoofing,’ W. Guo, D. Panda, IEEE Transactions on Intelligent Transportation Systems, 2024

[S1.5] ‘Encoding Social & Ethical Values in Autonomous Navigation: Philosophies Behind an Interactive Online Demonstration,’ Y. Tang, L. Moffat, W. Guo, C. May-Chahal, J. Deville, A. Tsourdos, ACM International Symposium on Trustworthy Autonomous Systems (TAS), Sep 2024

*This work is supported by the Engineering and Physical Sciences Research Council [grant number EP/V026763/1]*