Secure Estimation for Unmanned Aerial Vehicles against Adversarial Attacks

Qie Hu*, Young Hwan Chang*, Claire J. Tomlin

On February 15, 2015, the Federal Aviation Administration proposed to allow routine use of certain small, non-recreational Unmanned Aerial Vehicles (UAVs) in today's aviation system [1]. Thus in the near future, we may see UAVs such as Amazon Prime Air [2] and Google Project Wing vehicles [3] sharing the airspace. In order to manage this UAV traffic, we may imagine a scenario in which each UAV periodically sends measurements such as its position and velocity wirelessly to a remote control center, which then estimates the vehicle's trajectory, for collision avoidance for example. The communications link between the UAV and the control center could be subject to Man-In-The-Middle (MITM) attacks in which a malicious agent spoofs the information being sent and/or received (Channel 1 in Figure 1) [4]. Similar attack scenarios could arise in UAV formation: for formation control, individual UAVs receive information from other UAVs wirelessly in order to estimate other vehicles' positions (Channel 2 in Figure 1). Maintaining security of UAVs under such cyber attacks is an important and challenging task, since these attacks can be erratic and thus difficult to model.

Secure estimation problems study how to estimate the true system states when measurements are corrupted and/or control inputs are compromised by attackers. We focus on secure estimation and control of systems under sensor attack, because this type of attack is relatively easy to perform and thus particularly interesting. Take UAVs for example: actuators are installed onboard with hardwired local feedback loops, which are unlikely to be corrupted by adversarial attacks. Communications with external sources, on the other hand, are much more vulnerable. This includes GPS position measurements and communications between a UAV and a remote control center for UAV traffic management.

We do not assume the attack signal to follow any model, in addition, the set of attacked measurements/nodes is allowed to change from time to time. We propose a computationally efficient secure estimator for this problem, and prove the maximum number of attacked nodes that can be corrected by the estimator. Our results show that sensor fusion can be used to increase the number of correctable attacked nodes as well as improving estimation accuracy. Focusing on linear state and measurement feedback, we show that the feedback controller can be designed to achieve a desired trade-off between control and secure estimation performance. Finally, we propose to combine the secure estimator with a Kalman Filter (KF) to improve its practical performance, and demonstrate its effectiveness using two examples of UAVs under adversarial attack: MITM attack and GPS spoofing (Figure 2).

Q. Hu, Y. H. Chang, C.J Tomlin are with the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA 94720 USA (e-mail:{qiehu@eecs., yhchang@, tomlin@eecs.}berkeley.edu). Phone: 1-510-643-6610 / Fax: 1-510-643-2356
*These authors contributed equally

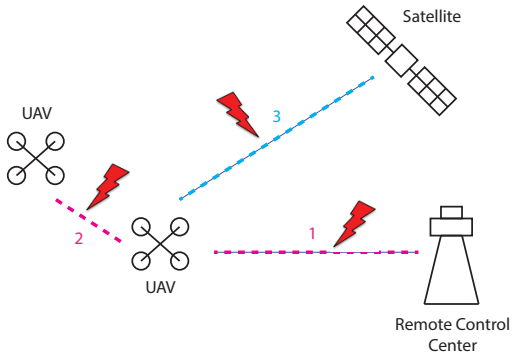

Fig. 1. Different communication channels that could be subject to adversarial attacks.

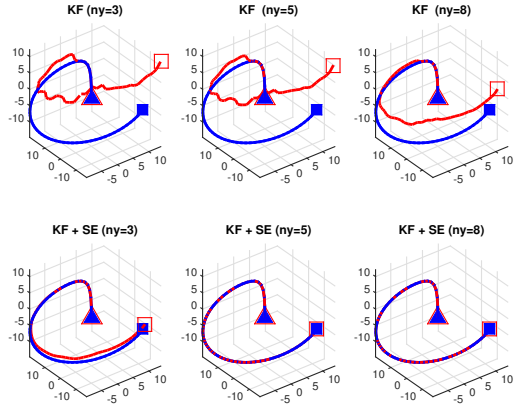

Fig. 2. Desired and actual UAV trajectories under GPS spoofing for: KF using 3, 5 and 8 measurements, and KF with secure estimation (KF+SE) using 3, 5 and 8 measurements. Blue solid line represents the desired trajectory from the triangle to the square. Red dash line represents actual UAV trajectory under GPS spoofing.

References

[1] "Press release – DOT and FAA propose new rules for small unmanned aircraft systems," http://www.faa.gov/news/press_releases/news_story.cfm/?newsId=18295, accessed: 2015-02-15.
[2] "Amazon Prime Air," http://www.amazon.com/b?node=8037720011.
[3] "Google project wing," http://www.theatlantic.com/technology/archive/2014/08/inside-googles-secret-drone-delivery-program/379306/?single_page=true, accessed: 2014-08-28.
[4] D. Welch and S. Lathrop, "Wireless security threat taxonomy," *IEEE Systems, man and cybernetics society information assurance workshop*, pp. 76 – 83, June 2003.