Software Graphical Interface as a part of a Spoofing System to Take Over Criminal Drones

Felipe C. Frazatto*, Mauricio M. Donatti, Leandro T. Manera

Abstract
Drones have been used by criminals to smuggle cell phones and drugs into prisons. They also may cause accidents in airports and other heavy flight traffic zones, so it is clear that is interesting to take control of drones in some specific situations. This work is part of a project intended to develop a system (hardware and software) to take control of the law-breaking drones.

Key words: RF Spoofing Attack; Drones; Homeland Security.

Introduction
Nowadays we are experiencing a rapid growth in the drone market and, as consequence, in drone related utilities, ranging from simple flight to military recognition missions. However, some users are taking advantage of this new technology to break the law and smuggle items and drugs into prisons. Criminals used Drones to smuggle drugs and contraband into prisons in New York on Sept. 2015 [1]. São Paulo’s police captures Drone taking 18 cell phones to a prison on Aug. 2014 [2] and CCTV shows drone delivering stash of drugs to prison cell window. London, UK on May 2016 [3]

Results and Discussion
We have used a beaglebone board, running our spoofing program and a USB connection with an UART (CP2102) to communicate with the graphic user interface. The GUI, as shown in image 2, developed using de programming language C#, enables the user to easily take control of the drone and the system itself automatically sending standardized messages to the hardware that in turn sends the simulated signal to the drone.

Conclusions
We were able to develop a user friendly interface that enables any user to take control over the drone, enabling the control of all drone flight parameters: Yaw, pitch, throttle and roll. Further hardware improvements are under development to increase drone models that can be spoofed.

Acknowledgement
This work was supported by a partnership between Neger Telecom (CNPq RHAE project) and School of Electrical and Computer Engineering (FEEC) at the University of Campinas (UNICAMP).

DOI: 10.19146/pibic-2016-51897