Acta Universitatis Sapientiae
Electrical and Mechanical Engineering, 8 (2016) 5-18

DOI: 10.1515/auseme-2017-0001

GNU Radio Based Testbed (GRaTe-BED) for Evaluating the Communication Link of Unmanned Aerial Systems

András SZABÓ

Department of IT, Faculty of Military Sciences and Officer Training,
National University of Public Service, Budapest,
e-mail: szabo.andras@uni-nke.hu

Manuscript received October 15, 2016; revised December 15, 2016

Abstract: UAS (Unmanned Aerial Systems) are commonly used in 3D (dull, dirty and dangerous) missions, because these are not endangering the operators life, while reduce maintenance costs and increase maneuvering capabilities. Despite of these advantages we should consider the possible vulnerabilities of this technology as well. Unmanned vehicles can be controlled via direct communication link, or they can work in a preprogrammed mode. Usually the preprogrammed mode is based on radio navigation systems, so we can draw a conclusion that both depend on the RF environment. In this paper I analyze a possibility to effectively evaluate the communication link of an UAS. Developers have to consider several key factors (type of operation, endurance, payload type and size, propulsion, communication link, etc.) during the development process. They are also responsible that the final product meets the predefined requirements. On the other side commercial UAS owners should have a possibility to compare and evaluate the UAS before the acquisition. Finally, operators and frequency management entities need tools to diagnose the possible sources of interference regarding the unmanned vehicles. To understand the consequences of interference in the RF spectrum we have to be able to measure the quality of the communication link in different usage scenarios. In my research I evaluate the usage of SDRs (Software Defined Radios) in RF Test and Evaluation processes. After analyzing the possibilities for a flexible testbed, I demonstrate the usability with some measurements in the GNU Radio signal processing framework.

Keywords: UAS, SDR, RF, Test & Evaluation, USRP, GNU Radio.

1. Introduction

There are multiple names for Unmanned Aircraft Systems (UAS) like drone, remotely operated aircraft (ROA), remotely piloted aircraft (RPA), remotely piloted vehicle (RPV), and autonomous aerial vehicle. The innovations of the last few years let this technology become so popular today. For hobbies through commercial and governmental entities all the way up to the military.

The driving force behind this technology was originally the military, similarly to other inventions in the field of telecommunication and computer science. This technology is getting into our everyday life so suddenly and drastically, like the Internet and the mobile communication several years ago. Those caused major changes in the economy, scientific world, culture, education and most importantly transformed our social life. The question is what these unmanned devices will cause in the history of mankind. The global term for these devices is Cyber-Physical Systems, which describe the fact that they exist and act in both dimensions. The technical and legal backgrounds haven't been established yet, as it is still an emerging technology.

From the security perspective the drones are rising threats and unused opportunities in the same time. We have heard notable cases (drone crashes[1] [2], jamming incident[3], counter operations in conflicts[4] [5], football hooliganism[6], drug smuggling[7]) in the news which prove that unaware hobbyist, criminals, malicious users and even state-actors recognized the possibilities of this technology.

2. Background and motivation

The before mentioned threats have to be addressed with proper countermeasures. We have to consider the possible counter UAS techniques, and also the usable defense mechanisms. While putting together the elements of the threat model, we have to consider the basic requirements of the UAS as well as the possible exploitation methods.

The duality of this technology is represented by the fact that we have to encounter jamming [1] or dazzling attack[8] against the UAS sensors [2], [3] or attackers can disturb public event using drones (fly over with a political interest[1, 6] or endangering the public (several drones crashed in crowded public space like stadiums[9]). So we have to be prepared for the offensive and defensive operations

[1] Source: http://www.independent.co.uk/news/world/asia/man-arrested-for-landing-radioactive-drone-on-japanese-prime-ministers-roof-10203517.html

[2] Source: http://www.washingtonpost.com/wp-srv/special/national/drone-crashes/database/

[3] Source: http://www.osce.org/ukraine-smm/140586

[4] Source: https://medium.com/war-is-boring/ukraine-scrambles-for-uavs-but-russian-drones-own-the-skies-74f5007183a2

[5] Source: http://www.abc.net.au/news/2015-04-22/ukraines-diy-drone-war/6401688

[6] Source: http://www.bbc.co.uk/sport/0/football/29624259

[7] Source: http://www.bbc.co.uk/news/technology-30932395

[8] like pilots have blinded by lasers or other light source

[9] Source: http://edition.cnn.com/2015/09/06/us/drones-sports-events/
http://www.droneinjurieslawyer.com/read-me/ http://www.bbc.com/news/technology-26921504

too. It is quite contradictory, that micro UAS are publicly available for a low price, but security of the used communication standards, and the possible counter-UAS techniques are not well known. Law enforcement and security agencies need counter-UAS techniques [4], which are still available on the market (solutions for detecting[10, 11, 12, 13, 14] and for detecting and countering[15, 16]. These governmental entities are in a difficult position because these countermeasures usually haven't been inspected by independent test facilities and the results aren't available publicly (which is understandable regarding the sensitive nature of these countermeasures). Both the effectiveness and the limits have to be analyzed to ensure proper counter-UAS capability and to minimize unneeded interference with legitimate spectrum users (to decrease the footprint of the equipment only to that location which has to be secured). Test procedures have to be defined and made publicly available to standardize the requirements. It is also a challenge to navigate in the field of UAS technology, where there are multiple companies on the drone market with wide portfolio, several frequency ranges (usually 72 MHz, 433 MHz, 915 MHz, 2,4 GHz for control 900 MHz, 1,2 GHz, 2,4 GHz or 5,8 GHz for payload communication), and different protocols (Wifi, 3DR, MAVlink, etc.) for the control channel. In [5] researchers highlighted the lack of standardized protocols for civil UAS control communication. So we have to evaluate devices with different kind of RF parameters, and various proprietary, or open source upper layer protocols.

3. Objectives and Scope of the Research

In this paper I will investigate the possibilities to evaluate the communication systems of Unmanned Aerial Systems (UAS). As highlighted by several researches, the communication link [6], [7] is vital for the future UAS development and deployments of unmanned systems. Engineers meet a challenge when trying to analyze the different open source (like MAVlink[17, 18]])

[10] SHARPEYETM SxV RADAR TECHNOLOGY https://www.kelvinhughes.com/security/uav-drone-detection

[11] ARRIER DSR-200 Drone Surveillance Radar http://www.detect-inc.com/DeTect%20-%20Security/TDS%20-%20HARRIER%20DSR%20200d%20150406US.pdf

[12] Army Tests New Acoustic Threat Detection System http://defensetech.org/2015/05/20/army-tests-new-acoustic-threat-detection-system/

[13] DroneTracker http://www.dedrone.com/en/dronetracker/drone-detection-hardware

[14] Domestic Drone Countermeasures http://www.ddcountermeasures.com/

[15] Anti-UAV Defence System (AUDS) http://www.securitynewsdesk.com/?post_type=post&p=50833

[16] Falcon Shield http://www.janes.com/article/54319/dsei-2015-selex-es-unveils-falcon-shield-counter-uav-system

[17] MAVLink micro air vehicle marshalling / communication library https://github.com/mavlink/mavlink

[18] MAVLINK Common Message Set https://pixhawk.ethz.ch/mavlink/

and closed-source UAS communication protocols. Nowadays the possibility offered by SDR is adequate choice for RF test and evaluation (T&E) facilities. SDR can speed up the measurement and validation process, and also migrate the bulk of the physical measurements to simulation, emulation (only essential field tests are done in the real world) [8]. SDRs already facilitate the integrating simulations to the real-word RF measurements. Subsystems or essential components can be simulated in frameworks like the open-source GNU Radio (or commercial tools like Labview and Matlab) and access the RF world with tools such as ETTUS research's USRP SDR family.

New opportunities, like measurement devices organized and controlled in a distributed network will increase the reliability of the measurement results. Device-to-device communication enabled us to automatize, synchronize and fusion different measurements (like measuring wind, temperature, humidity and other weather condition while sensing the RF spectrum and validating the position of the Device Under Test - DUT).

In my research I highlight these possibilities and proof them with a GNU radio based concept. My research was aiming to achieve the following goals: Design an integrated testbed for RF interference and jamming measurements, Implement a network centric measurement capability, Create a flexible, scenario drive testbed (*Fig. 1*), Create the SWOT analysis (Strengths and Weaknesses, Opportunities and Threats) of this approach.

4. Previous Work

UAS technology is a hot research topic nowadays, there are several publications related to my field of interest. In [9], [10] authors highlighted the importance of robust communication between the UAV and the ground control station, which means that we have to test these UA in a possible not-cooperative/hostile EM environment (to be prepared to the unintentionally hazardous or hostile situations) and also develop suitable response to aerial terrorist attacks (especially which conducted with commercial UAS [10]. In spite of the high proliferation of mini UAV systems, there are only a few recommendations about testing the DUT as a hardware in the loop [11], evaluate its communication [7], [12] or analyze the performance of the sensor/payload systems [13]. Engineers are focusing on the vulnerability of the communication link against unintentional interference [14] or adversaries with RF jamming capabilities [15], the cyber exploitation of these devices are also a hot topic [16]. However, very few of the before-mentioned papers try to understand the threat against UAS, or attempt to manage this problem in holistic point of view. In fact the security of these cyber-physical devices has to be analyzed in a comprehensive approach [17], from the physical level[19] to the application layer. In the military this classification is mentioned as CEMA (Cyber Electromagnetic Activities) [18]. There are several researches about the usage of SDR as communication link testbed [19]. They are focusing on the communication protocol under development and using SDRs only as a point-to-point link test equipment, not taking the advantage of the previously mentioned opportunities.

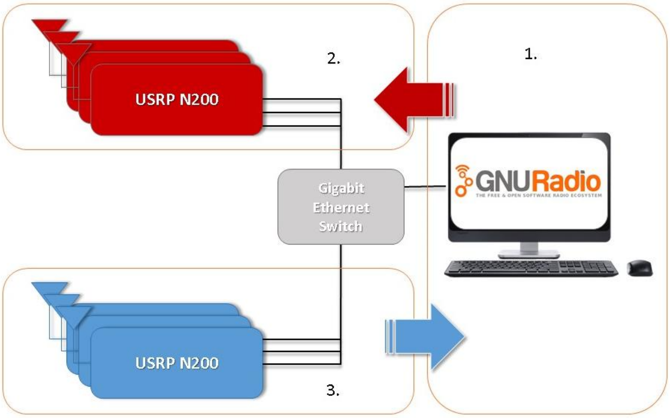


Figure 1: Networked measurement instrument (1. is the network segment of the management node(s), 2. is the team-jammer network and 3. is the RF sensor network)

Different jamming scenarios against advanced wireless standards are analyzed, and organized in a methodical manner in [15]. Researchers in [20] collected the possible threats against UAS, but they focused on the computer based simulation.

These researches encouraged me to create the GNU Radio Test BED (GRaTe-BED) for testing UAS communication link, with the capability to analyze unintentional interference or malicious jamming activity, anomalies from Layer 1 to Layer 7.

[19] Layer 1 35.100: Open systems interconnection (OSI) Source: http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_ics_browse.htm?ICS1=35&ICS2=100

5. Methodology

Design considerations

In the following I will present the main features which I had to consider during my research.

SDR platform

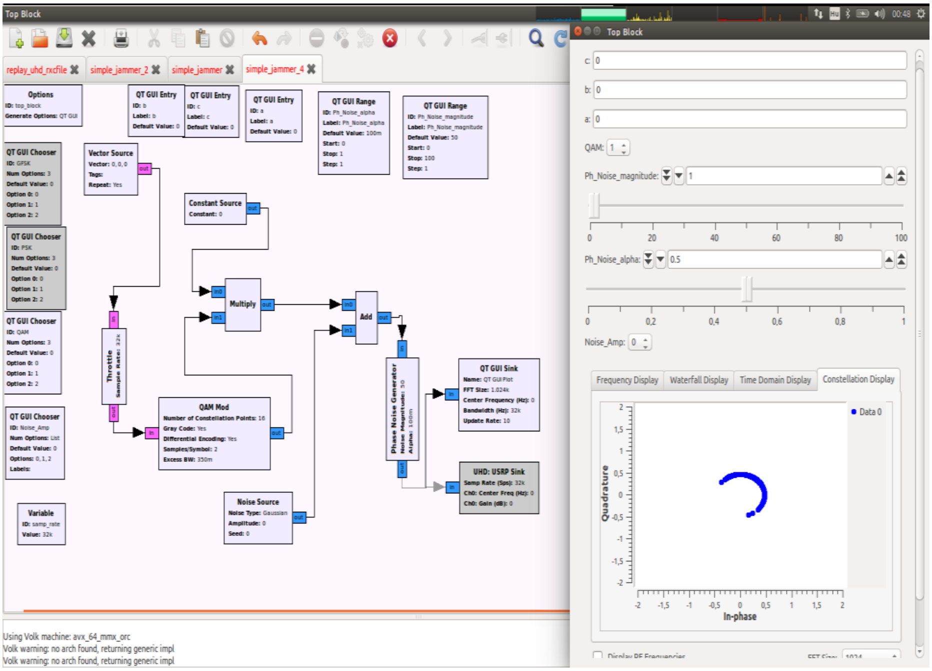
SDR solves the flexibility needs by converting most of the PHY layer signal processing blocks into a software layer. This method not only simplifies design and implementation of advanced radio system, but it also made new approaches possible. SDR receivers, transceivers can be deployed in different locations, multiple radios can be organized into a network (see *Fig. 1*), to mention a few novel features. This technology simplifies RF testing, by transforming measurement into scriptable steps. Multiple scenarios can be tested and validated, minimizing the human error (measurement errors). The repeatable steps can be automatized but the design of the scenario and the analysis of the final results should done by engineers. It’s important to mention that the testbed can’t operate without human interaction.

For the hardware part of the testbed I used USRP N200 with UHD_003.005.005 driver, usrp_n200 firmware and usrp_n200_r4 FPGA image (openly available from ettus.com), the software component was GNU radio (Version 3.7.2.1). There are several simulation platforms which would have been utilized for this project (for example Labview, Matlab and Simulink). My choice was Gnu Radio. The reasons behind this decision were my previous experience with this tool, and also to make the results publicly, and freely available for other researchers. The hardware parameters are well documented (for us it’s important that maximum output power is between 17-20 dBm, usable between 400 to 4400 MHz with SBXv3, and 68.75 to 2200 MHz with WBXv3 frontend boards [21]).

USRP hardware can work both with command line tools like (UHD_FFT, UHD_SIGGEN) or graphical interface of the GNU Radio Companion. Both have advantages and some drawbacks as well.

To automate different scenarios cli tools are useful, because they can be organized and executed in a script, without user interaction (besides that usually users triggers the start and check the integrity of the output).

On the other hand if the analysis needs human interaction, the results are not predictable, then it is recommended to conduct the evaluation under supervision of a human operator.



Options
ID: top_block
Generate Options: QT GUI

QT GUI Entry
ID: b
Label: b
Default Value: 0

QT GUI Entry
ID: c
Label: c
Default Value: 0

QT GUI Entry
ID: a
Label: a
Default Value: 0

QT GUI Range
ID: Ph_Noise_alpha
Label: Ph_Noise_alpha
Default Value: 100m
Start: 0
Stop: 1
Step: 1

QT GUI Range
ID: Ph_Noise_magnitude
Label: Ph_Noise_magnitude
Default Value: 50
Start: 0
Stop: 100
Step: 1

QT GUI Chooser
ID: GFSK
Num Options: 3
Default Value: 0
Option 0: 0
Option 1: 1
Option 2: 2

Vector Source
Vector: 0, 0, 0
Tags:
Repeat: Yes

Constant Source
Constant: 0

QT GUI Chooser
ID: PSK
Num Options: 3
Default Value: 0
Option 0: 0
Option 1: 1
Option 2: 2

QT GUI Chooser
ID: QAM
Num Options: 3
Default Value: 0
Option 0: 0
Option 1: 1
Option 2: 2

Throttle
Sample Rate: 32k

Phase Noise Generator
Noise Magnitude: 50
Alpha: 100m

QT GUI Sink
Name: QT GUI Plot
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 32k
Update Rate: 10

QT GUI Chooser
ID: Noise_Amp
Num Options: List
Default Value: 0
Options: 0, 1, 2
Labels:

QAM Mod
Number of Constellation Points: 16
Gray Code: Yes
Differential Encoding: Yes
Samples/Symbol: 2
Excess BW: 350m

UHD: USRP Sink
Samp Rate (Sps): 32k
Ch0: Center Freq (Hz): 0
Ch0: Gain (dB): 0

Variable
ID: samp_rate
Value: 32k

Noise Source
Noise Type: Gaussian
Amplitude: 0
Seed: 0

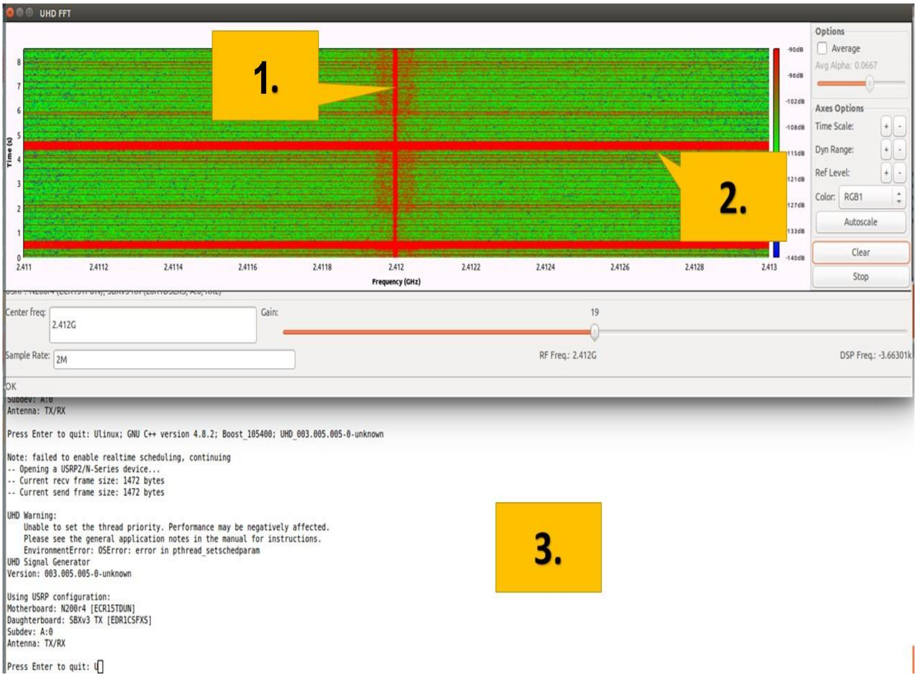
```
Using Volk machine: avx_64_mmx_orc
Volk warning: no arch found, returning generic impl
Volk warning: no arch found, returning generic impl
```

Top Block
c: 0
b: 0
a: 0
QAM: 1
Ph_Noise_magnitude: 1
0 20 40 60 80 100
Ph_Noise_alpha: 0.5
0 0,2 0,4 0,6 0,8 1
Noise_Amp: 0

Figure 2: Flowgraph of the jammer in GNU Radio (left), with the constellation diagram of the output (right)

To organize the graphical interface we can choose from a notebook view (different graphical elements are on different "pages") or we can create only one "common View", and we can orient different elements with a Grid Position parameter. I find it much handier to organize into a notebook view then to a complex diagram.

At the jammer node similarly pre-programed steps like scripts using uhd_siggen (*Fig. 3*) or interactive user control with uhd_siggen_gui can be utilized (as a signal generator it can create basic signals sine, sweep, square, noise). If we are using GNU Radio Companion then we can use virtual measurement devices (spectrum analyzer, waterfall display, oscilloscope, histogram view, constellation diagram, etc.) to monitor the state of the flow graph. On the other hand the output should be inspected with external device (to check that the SDR generating the predefined signals with the allowed power).



Avg Alpha: 0.0667

Color: RGB1

Center freq: 2.412G

Gain: 19

Sample Rate: 2M

RF Freq.: 2.412G

DSP Freq.: -3.66301k

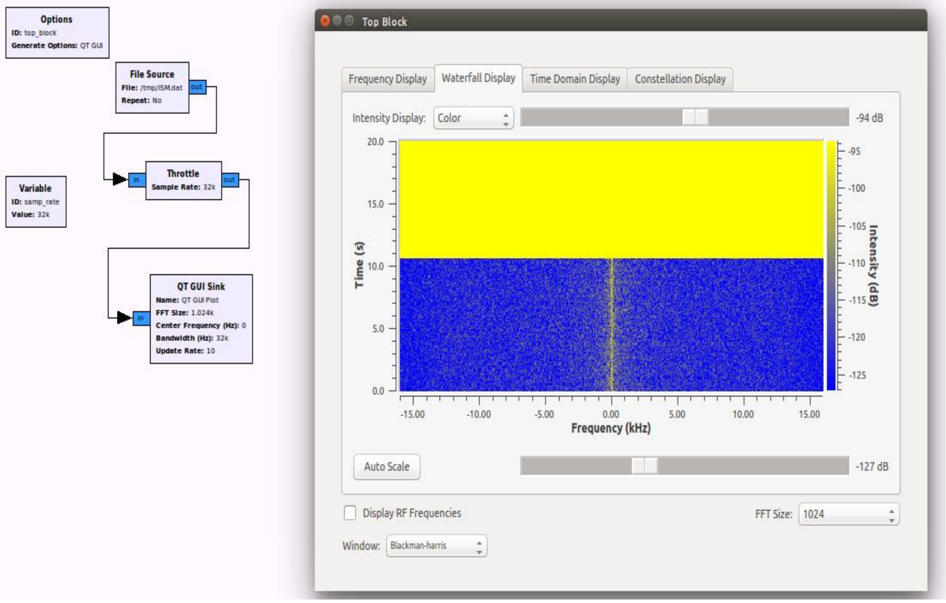
```
Subdev: A:0
Antenna: TX/RX

Press Enter to quit: Ulinux; GNU C++ version 4.8.2; Boost_105400; UHD_003.005.005-0-unknown

Note: failed to enable realtime scheduling, continuing
-- Opening a USRP2/N-Series device...
-- Current recv frame size: 1472 bytes
-- Current send frame size: 1472 bytes

UHD Warning:
    Unable to set the thread priority. Performance may be negatively affected.
    Please see the general application notes in the manual for instructions.
    EnvironmentError: OSError: error in pthread_setschedparam
UHD Signal Generator
Version: 003.005.005-0-unknown

Using USRP configuration:
Motherboard: N200r4 [ECR15TDUN]
Daughterboard: SBXv3 TX [EDR1CSFXS]
Subdev: A:0
Antenna: TX/RX

Press Enter to quit: U
```

Figure 3: DJI Phantom 2 vision control channel (1) with a pulsed jammer signal (2) generated with uhd_siggen script

Threat library

The effectiveness of the testbed is highly dependent on the interference/jam library, and the topology represented by the scenario. The utilized error detection/correction algorithms, media access schema, the channel coding made sophisticated RF standards cause that the effectiveness of the jammer signal is difficult to represent with mathematical models. Likewise in [22] the author mentioned the difficulties of simulating complex Electronic Warfare systems to measure the effectiveness. In this case SDRs can solve the problem by interconnecting the simulation and the real world RF measurements.

Unknown RF standards can be observed in a black box approach, with replaying signals we can spoof pre-recorded control signals and analyze the system responses [23]. For the "replay attack" (*Fig. 4*) we can save multiple different samples, and replay them in different orders, but it can increase the complexity of the software if we do not merge these samples.



Options
ID: top_block
Generate Options: QT GUI

File Source
File: /tmp/ISM.dat
Repeat: No

Variable
ID: samp_rate
Value: 32k

Throttle
Sample Rate: 32k

QT GUI Sink
Name: QT GUI Plot
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 32k
Update Rate: 10

Intensity Display: Color
-94 dB
-127 dB
☐ Display RF Frequencies
FFT Size: 1024
Window: Blackman-harris

Figure 4: Replay attack demonstrated in GNU Radio Companion

Channel modeling

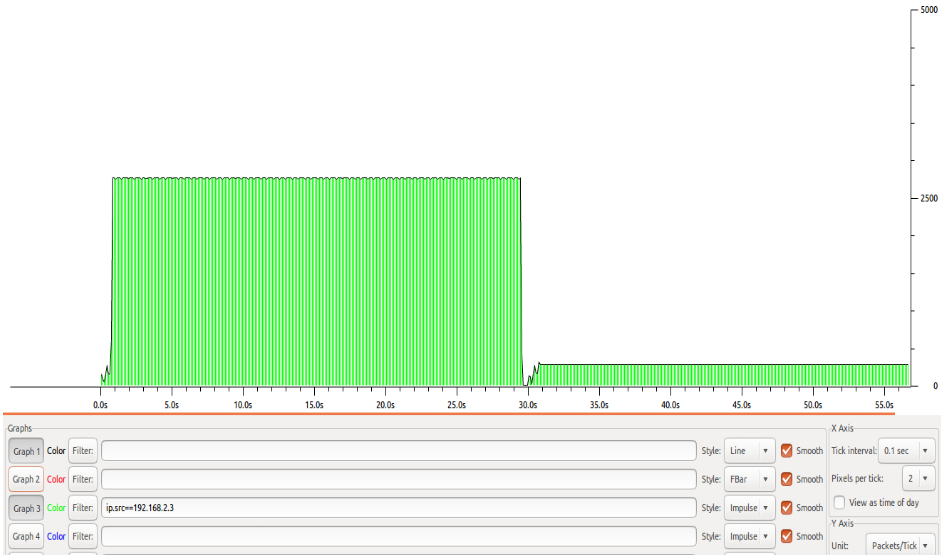
Author in [24] compared the possibilities for channel simulation in GNU Radio. With these models we can introduce different channel degradation effects (multipath, frequency selective fading, etc.) to observe the DUT response to the possible RF anomalies (not only the Transmitter but also the jammer performance can be degraded by environmental conditions).

Networking

While creating a high density SDR network array we have to consider the difficulties caused by multiple measurement device sets to high sampling rate (like 100 Msamp/sec with 20 MHz RF bandwidth) [25].

USRP N200 has Gigabit Ethernet network interface, supporting IPv4, and only the IP address can be changed (not even the netmask). So theoretically the maximum number of sensors in the network is 254 (because USRP doesn't support routing, so we can’t create a routed topology).

Sampling rate is a critical parameter to the network load (*Fig. 5*), and the proper configuration of the TCP/IP stack is also vital [26].



Graph 3 Filter: ip.src==192.168.2.3

Graph 1 Style: Line ☑ Smooth

Graph 2 Style: FBar ☑ Smooth

Graph 3 Style: Impulse ☑ Smooth

Graph 4 Style: Impulse ☑ Smooth

Tick interval: 0.1 sec

Pixels per tick: 2

□ View as time of day

Unit: Packets/Tick

Figure 5: Network load in Wireshark IO Graph (the network traffic of uhd_fft was monitored)

The script used for measurement:

```
/usr/sbin/tcpdump -i eth1 -s 65535 -w /tmp/USRP_10M+1M_uhd_FFT.pcap & timeout -sHUP 30
/usr/bin/uhd_fft --args="addr=192.168.10.2" --fft-size=2048 --fft-rate=40 -f 2G -s
10000000;timeout -sHUP 30 /usr/bin/uhd_fft --args="addr=192.168.10.2" --fft-size=2048 --fft-rate=40 -f 2G -s 1000000;pkill -HUP -f /usr/sbin/tcpdump
```

The first 30 sec. uhd_fft was configured to sample 10 Msps, than 30 sec. with only 1 Msps.

RF Navigation

Global (like GPS, GNSS, etc.) or autonomous [9] radio navigation systems are commonly used in UAS for the autopilot system, and also have important role in remotely operated device in “link lost” situations. Likewise, these technologies can be tested on SDR platform [27]

Test scenario building

It’s a mandatory requirement for T&E equipment to perform in a repeatable, flexible way and to be able to adapt to new technologies (like new protocols). In GNU radio basic signal processing blocks are available (modulators, demodulators, filters, etc.), if a new / special purposed processing function is required, it is straightforward to integrate into GNU Radio (as block is develop in C++).

Evaluation of the results

We have to define metrics before performing the test, for example a 4 state metric look like this: I. "*No effect*" II. "*No operator control over the vehicle*" III. "*Position change caused by jam signal*" "*Full control achieved by the attack*". The RF measurement results and these metrics should be logged to the final report.

Fuzzing

If we are analyzing a standardized protocol with a reason to create a protocol aware jamming scenario, then we need information about the communication protocol. CGRAN (Comprehensive GNU Radio Archive Network)[20] hosts a lot of "out-of the tree modules"[21] (like GSM, LTE, Bluetooth, IEEE 802.11 protocols). These modules can be utilized in a high protocol level fuzzing. To check the availability of the DUT, we have to create an entity which analyzes its responses. In IT security this called as *oracle* [28]. If the DUT can cooperate (it can measure and log the signal quality), then we only have to synchronize the jamming scenario with this logging mechanism, and after the tests we get information about the jamming efficiency. It is difficult to analyze the onboard navigation, guidance and control loop, if the DUT is in flight. Most commercial UAS have proprietary control channel and debugging procedures (there are reverse engineering attempts like [29])

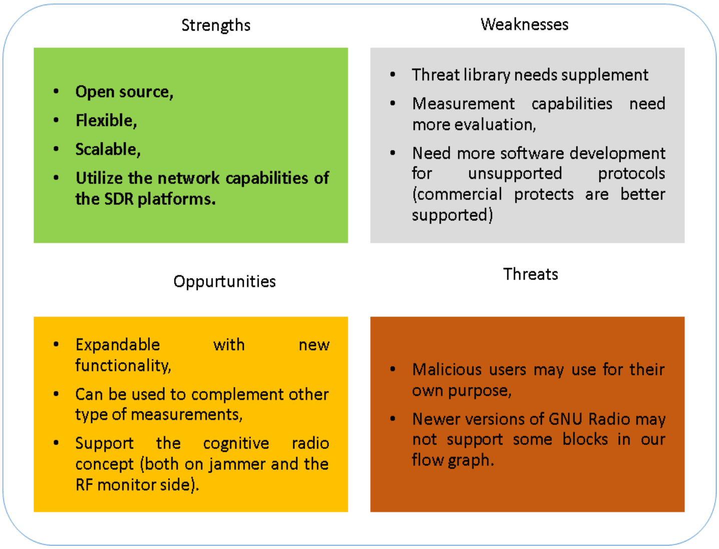
If the DUT isn't capable to log, than we should create some external sensor to evaluate the jammer performance in an indirect mode. The testbed for cyber-physical systems can utilize multiple sensors to analyze the DUT response to environmental changes. Visual recording of the responses is the easiest, but difficult to organize and analyze after the measurements. Atmospheric conditions can be useful, with low cost devices like Raspberry Pi or Arduino we can create a sensor network, and logs can be collected to the management node which schedule the RF tests.

SWOT

The Strengths and Weaknesses of the testbed, the identified Opportunities open to us and the Threats we have to face are shown in *Fig 6*.

[20] http://cgran.org/

[21] more details can be found at https://gnuradio.org/redmine/projects/gnuradio/wiki/OutOfTreeModules



Strengths

- Open source,
- Flexible,
- Scalable,
- Utilize the network capabilities of the SDR platforms.

Weaknesses

- Threat library needs supplement
- Measurement capabilities need more evaluation,
- Need more software development for unsupported protocols (commercial protects are better supported)

Oppurtunities

- Expandable with new functionality,
- Can be used to complement other type of measurements,
- Support the cognitive radio concept (both on jammer and the RF monitor side).

Threats

- Malicious users may use for their own purpose,
- Newer versions of GNU Radio may not support some blocks in our flow graph.

Figure 6: SWOT analysis

6. Conclusion and recommendations

Several researchers analyzed possibilities to exploit the control subsystem of UASs. However, these analyses are mostly focusing on the cyber part of the security (in a network oriented view only the upper OSI layers are covered) or on just one type of communication link/protocol. To understand and evaluate the threat against this technology we have to manage this problem in a comprehensive manner. Security of the unmanned technology should not be based on “security through obscurity”. Communication protocols have to be publicly available to enable adequate security analysis.

I demonstrated a possible approach with a flexible, open source, easily implementable framework. I already highlighted the importance of the comprehensive threat modeling. Full disclosure [30] of UAS vulnerabilities was out of my scope. It would be unethical, because changing the hardware in embedded systems is in most of the cases impossible, modifying the software is difficult, and in most of the cases it is impossible for the end-user. I recommend to all my colleagues in this field of research to follow this procedure. In my paper I highlighted possible testing techniques and toolsets helping the reliable evaluation of this technology.

Future plans

- Creating a database back-end to manage the measurement and to store the results;
- Testing with different UAS;
- Expanding the RF spectrum (the current hardware can analyze up to 4,4 GHz, with down converters it is possible to analyze upper portion of the spectrum);
- Analyzing RF immunity and interference in UAS swarming operations.

References

[1] Kerns, A. J., "Unmanned aircraft capture and control via gps spoofing", *http://radionavlab.ae.utexas.edu/images/stories/files/papers/unmannedCapture.pdf.*

[2] United States Air Force Scientific Advisory Board, "Report on operating next-generation remotely piloted aircraft for irregular warfare", *Section 2.4.2 http://info.publicintelligence.net/USAF-RemoteIrregularWarfare.pdf*, 2011.

[3] Federal Aviation Administration, "Laser hazards in navigable airspace" *https://www.faa.gov/pilots/safety/pilotsafetybrochures/media/laser_hazards_web.pdf .*

[4] Makkay, I., "Fight of drones" ("Drónok harca"), 2015 *http://www.repulestudomany.hu/ folyoirat/2015_1/2015-1-05-0192-Makkay_Imre.pdf.*

[5] Bob Kerczewski, Jeff Wilson, Bill Bishop – "Frequency Spectrum for Integration of Unmanned Aircraft", *NASA http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6719706.*

[6] Yanmaz, E.; Kuschnig, R. ; Bettstetter, C.," Channel Measurements over 802.11a-based UAV-to Ground Links" *http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber= 6162389 &abstractAccess =no&userType=inst.*

[7] Steve Gardner, "A communication link reliability study for small unmanned aerial vehicles", *Enerdyne Technologies, Inc.- COMM OPS Trends in Communication Systems For ISR UAVs*, January 2009, *http://www.milsatmagazine.com/story.php?number=893938022.*

[8] Pywell, M., Midgley-Davies, M. "EW test and evaluation - assuring survivability and operational effectiveness", *Electromagnetic Engineering Department BAE SYSTEMS, Military Air & Information http://tangentlink.com/wp-content/uploads/2014/07/2.-Electronic- Warfare-Test-Evaluation-Mitch-Midgley-Davies.pdf .*

[9] Miko, G. , Nemeth, A., "Combined communication and radio navigation system for small UAVs", *Radioelektronika 2013 23rd International Conference*, pp. 284-288, ISBN: 978-1-4673-5516-2.

[10] Turan, M., Gunay, F., Aslan, A. , "An analytical approach to the concept of counter-UA ops (CUAOPS)", *Journal of Intelligent & Robotic Systems*, January 2012, Volume 65, Issue 1-4, pp 73-91, ISSN 1573-0409, *http://link.springer.com/article/10.1007%2Fs10846-011-9580-6.*

[11] Zheng, Y., Wang, Y., "Hardware in the Loop Simulation for Low-altitude UAV Link in the Complex Terrain", *Applied Mechanics and Materials* Vols. 336-338 (2013), pp. 1907-1912, ISBN:9783037857519.

[12] Yanmaz, E.; Bettstetter, C., " Channel measurements over 802.11a-based UAV-to-ground links", *GLOBECOM Workshops (GC Wkshps) IEEE*, 2011, ISBN:978-1-4673-0039-1.

[13] Wan, J., Suo, H., Yan, H., Liu, J., "A general test platform for cyber-physical systems:unmanned vehicle with wireless sensor network navigation", *2011 International Conference on Advances in Engineering, http://ac.els-cdn.com/S1877705811054658/1-s2.0-S1877705811054658-main.pdf?_tid=3c747952-6b8b-11e5-bae9-00000aab0f6b&acdnat=1444068326_18bdf0fe9b500d0fcc69e141753afc30.*

[14] Koepke, G., Young, W., Ladbury, J., Coder, J., “Complexities of testing interference and coexistence of wireless systems in critical infrastructure”, 2015, *http://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.1885.pdf* .

[15] Slater, D., Tague, P., Poovendran, R., Li, M., “A game-theoretic framework for jamming attacks and mitigation in commercial aircraft wireless networks” *http://www.ee.washington.edu/research/nsl/papers/aiaaInfotech09c.pdf*.

[16] Jamshidi, M., ‚Jaimes Betancourt, A. S., Gomez, J., “Cyber-physical control of unmanned aerial vehicles”, *http://ac.els-cdn.com/S1026309811000691/1-s2.0-S1026309811000691-main.pdf?_tid=71385718-66c6-11e5-9137-00000aab0f6b&acdnat=1443543999_0cc41af19de0b2765c48bdb1e55402c3*.

[17] Saeed, A., Neishaboori, A., Mohamed, A., Harras, K. A., “Up and away: a cheap UAV *cyber-physical testbed” http://arxiv.org/pdf/1405.1823v1.pdf*.

[18] Department of the Army, “Cyber electromagnetic activities, field manual no. 3-38”, Washington, DC, 12 February 2014 *http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf*.

[19] Zainudin, A., Sudarsono, A., Astaw, I. G. P., “Reliability analysis of digital communication for various data types transmission using GNU Radio and USRP” *http://www.researchgate.net/publication/259477837_Reliability_Analysis_of_Digital_Communication_for_Various_Data_Types_Transmission_Using_GNU_Radio_and_USRP*.

[20] Javaid, A., Sun, W., and Alam, M., “A Cost-Effective Simulation Testbed for Unmanned Aerial Vehicle Network Cyber Attack Analysis”, *Safe & Secure Systems & Software Symposium (S5)* June 9-11, 2015, *http://www.mys5.org/Proceedings/2015/Day_3/2015-S5-Day3_0805_Sun.pdf*.

[21] Ettus Research Application Note, “Selecting an RF Daughterboard”, *http://www.ettus.com/content/files/kb/Selecting_an_RF_Daughterboard.pdf*.

[22] Tucker, T.W. “Jammer testing and chaos”, *Tactical Technologies Inc.http://tti-ecm.com/uploads/resources_technical/jammer%20testing%20and%20chaos.pdf*.

[23] Chen, J., Zhang, S.†, Wang, H., Zhang, X., "Practicing a record-and-replay system on USRP", *Sigcomm Conference 2013, http://conferences.sigcomm.org/sigcomm/2013/papers/srif/p61.pdf* .

[24] O’Shea, T. “GNU Radio channel simulation: trolling sub-par modem algorithms and implementations for fun and profit”, *Research Faculty, Virginia Polytechnic Institute and University, Arlington, VA*, 1 Oct 2013 *http://static1.1.sqspcdn.com/static/f/679473/23654472/1381240802597/grcon13_oshea_chansim.pdf?token=iRbiWsmfTNpfPqITN708izU3fQU%3D*.

[25] Department of Electrical and Computer Engineering, Ben-Gurion University of the Negev, “Introduction to USRP”, *http://www.researchgate.net/file.PostFileLoader.html?id=545b5550d039b12d7c8b4567&key=80f8366d-3355-40ad-a657-7ffb6b904ff8&assetKey=AS:272121316478982@1441890186007*.

[26] Ettus Research, “Latency”, *https://github.com/EttusResearch/uhd/wiki/Latency*.

[27] Brown, A., Tredway, R., and Taylor, R., “GPS signal simulation using open source GPS receiver platform” *https://wireless.vt.edu/symposium/2011/posters/GPS%20Signal%20Simulation_Brown.pdf*.

[28] Knudsen, J., Varpiola, M., “What is fuzzing: the poet, the courier, and the oracle”, 2015, *http://www.codenomicon.com/resources/white-paper/pdf/WhatisFuzzing.pdf* .

[29] “Hijacking DJI Phantom 2 Vision and P2V+”, *https://github.com/noahwilliamsson/dji-phantom-vision*.

[30] Cencini, A., Yu, K., Chan, T., “Software vulnerabilities: full-, responsible-, and non-disclosure”, December 7, 2005, *http://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/software_vulnerabilities_by_cencini_yu_chan.pdf p. 10*.