DARPA Bay Area SDR Hackfest Problem Book

UAV+SDR Control Links

Existing and emerging software tools provide unprecedented capabilities to manage and control the electromagnetic spectrum and, in particular, radio frequency signals. The DARPA Bay Area SDR Hackfest aims to challenge the user community to explore how to control drones through software defined radio links. These efforts will enable the free and open source software (FOSS) and defense communities to jointly build better ways of managing the significant challenges inherent in radio control of objects moving in three dimensions with the potential for intentional jamming and unintentional radio interference.

Tom Rondeau
Thomas.rondeau@darpa.mil
Nov. 13 – 17, 2017
NASA Ames, Moffett Field, CA, USA

Table of Contents

Introduction

Hackfests

In the tradition of many of the free and open source software (FOSS) events, the U.S. Defense Advanced Research Projects Agency (DARPA) will hold a hackfest in conjunction with the NASA Ames Research Center. Called the DARPA Bay Area SDR Hackfest, this hackfest will focus on opportunities to use software defined radio (SDR) to control unmanned aerial vehicles (UAV). A hackfest, often known as a hackathon or code sprint, is a common way for FOSS projects to engage and enable communities, and DARPA is using this hackfest as an opportunity to rethink how we can use the electromagnetic (EM) spectrum as a programmable element in our control over unmanned vehicles.

DARPA SDR Hackfests

As science and technology continue to advance and the speed of innovation increases, DARPA's interest in building common platforms, toolsets, and fundamental skills has grown. These have been long-standing tenets of FOSS, and DARPA believes that building an engagement between the FOSS and DARPA communities will allow both communities to benefit from and promote the use of advanced technology. DARPA's Software Defined Radio (SDR) Hackfests are set up to engage a community that includes more than just the core developers of a project. The use of the electromagnetic spectrum (EMS) is increasingly becoming more important as communications, radar, and EMS sensing are more tightly integrated and create unique challenges as a core part of technology. Addressing the intersections of computing, communications, and control requires asking questions that address problems which span several fields and disciplines.

Traditionally, SDR programming has been limited to a niche set of engineers and computer scientists specifically interested in this problem space. Yet a growing number of communities are identifying the utility of SDR. Already, SDR is being used successfully in research, prototyping, and development of new wireless communications and radar systems. Beyond those domains, SDR is finding its way into fields such as information security and cellular technology development. Security concerns in wireless are increasing due to the amount of data collected and transmitted through wireless internet connections as well as the growth of the Internet of Things (IoT). While future cellular standards evolve ever more quickly, so too must the communications infrastructure. In addition, most cellular base stations are SDRs, and much of the work going into massive multiple input multiple output (MIMO) systems is performed with SDR. The DARPA SDR Hackfests are designed as a way for DARPA to collaborate with a larger community of interested engineers and scientists working towards the future confluence of radio and information technology.

DARPA Hackfests need to meet a number of difficult and often competing goals to be of interest to the agency:

1. Hard and interesting enough of a problem for DARPA to ask.
2. The work is doable in a week's timeframe.

3. The work has military/DoD relevance.
4. The problems and any solutions generated are open to the public.

DARPA Bay Area SDR Hackfest

The success of drones is heralding a new era of innovation and freedom of movement in all three spatial dimensions. The commercial success of affordable drones and the already large market penetration for hobbyist use is proof of this. As the technology progresses, more commercial, industrial, and military uses of these low-cost and small to medium sized drones grows. The issue with this growth is that drones rely on radio frequency (RF) links for control. Even drones that use pre-programmed way-points have an RF control channel for backup and emergency control. Often, the role of the drone is to provide video or other data back to the operator or some other data center. These data links can require significant amounts of bandwidth, and to support this, the drones either have to mix together the control and data links or use different radios to support these different types of connections.

Commercial drones use similar types of radio control waveforms and share the same spectrum. The existence of the unlicensed bands in the 400, 900, 2400, and 5800 MHz ranges allows commercial systems to operate there without burdening the individual operators with the need to obtain a license. While this is useful from an operator and regulatory perspective, it is not great technologically because of the presence of interference, sometimes extreme interference. When operating in the 2.4 GHz band, the radio-controlled drone will be competing with both other drones in the area as well as Wifi, Bluetooth, Zigbee, Z-Wave, and other devices that utilize that industrial, scientific, and medical (ISM) band. Drone control links are built with interference in mind and use techniques like frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS), often both together.

Software defined radio is an opportunity to address the interference problem posed by the increasing number of drones and their reliance on RF for control. By having flexibility in frequency selection as well as the design of the waveform, protocols, and transmission scheme, the control links can now be defined more appropriately and made adaptable to the conditions posed by the radio environment. **The overall mission of this Hackfest is to challenge the whole communications stack**.

SDR makes the spectrum programmable. SDR applications, then, can program the entire communications protocol stack from the physical layer up through to the application layer. Traditionally, applications like drones take an existing piece of radio hardware and integrate it into their system where they focus on fixing problems solely in the applications. This often means sacrificing efficiency in the lower layers and brute-forcing solutions higher up. A great example of this is using user datagram protocol (UDP) packets instead of transmission control protocol (TCP) packets. The latter requires acknowledgements and can stall transmission of information until the packet is acknowledge after retransmissions. The delays this causes is both inefficient use of the wireless medium (the spectrum) and causes poor control over the drones as time lag causes the pilots to lose sync with the motion of the drone. To fix this, the applications use UDP and blast many of them in a row to ensure that the packet is received. This is an even worse use of spectrum and a poor response to using the lower layers of the communications system. Similar stories exist in the utilization of all parts of the stack, and radio standards are defined and hardened for certain scenarios and expectations like non- or low congested spectrum. Changes in the spectrum are difficult to respond to with the way radios are delivered as black boxes.

Changing waveforms, bandwidth, and frequency use is problematic, however, because of radio and spectrum regulation. The Hackfest is focusing on the technology and so will ignore these kinds of issues. However, the policy and regulatory side of things is important and will be a topic of discussion throughout the week, though it will not impact the work being done by the Mission teams.

DARPA Bay Area SDR Hackfest Structure

The Bay Area SDR Hackfest is composed of three tracks:

- Hacker Space: A place to explore and interact with the experts and enthusiasts
- Speaker Series: Get inspired by new ideas
- Missions: Focus on solving specific, interesting problems

Hacker Space

The Hacker Space is an open, collaborative work environment, similar to traditional FOSS hackfests. This is a space to come together in throughout the week to engage with the community of developers and experts in the technology. Hackfests are all about solving problems and are often self-directed to either figure out a problem to work on or find others who have problems to help solve. Hackfests are meant to be friendly and collaborative, and all of the areas of technology such as SDR and UAVs have huge spaces of problems to be addressed. These problems span a wide range of technical skills and interests from significant mathematical and core programming issues to application and user interface design to webpage information, documentation, and outreach. Contributions in all areas are welcome.

Experts in the areas of SDR, UAVs, and cybersecurity will be present throughout the week at the hackfest, and they represent some of the biggest projects in those spaces. The Hacker Space is a great way to engage those projects and developers.

Another feature of the Hacker Space is a series of Brainstorming (BS) Session and Lightning Talks. The BS Sessions are meant to help people brainstorm onsite and provide information on the projects they are working on, successes they have had that week, and problems they are experiencing. This is a daily means to communicate and update the crowd of hackers on what is going on. The Lightning Talks are more formal presentations for people to explain themselves, their companies, and their interest in the hackfest such as recruitment opportunities or technology offerings.

Speaker Series

DARPA has invited experts and luminaries in technical areas at the core of this hackfest to come and speak. There are speakers lined up for all five days of the event to provide insight, motivation, and generally kick off new ideas and thoughts for how to think about and approach technology. Monday will feature two keynote talks during the afternoon to help us kick off the week. Similarly, Friday will feature two other keynotes to help us close down the hackfest. During the rest of the week, the hackfest will feature two speakers in the evening focused on certain areas of interest at the hackfest:

- Tuesday: SDR
- Wednesday: UAV
- Thursday: Cyber

Mon	Keynotes	Cory Doctorow *A Computer You Put Your Body Into*	Amie Stepanovich *What Future Are We Building?*
Tues	SDR	Ben Hilburn *Welcome to Software Defined Radio*	Heather Kirksey *Open Source Software and the Network of Tomorrow*
Wed	UAV	Parimal "PK" Kopardekar *Unmanned Aircraft System Traffic Management (UTM)*	Chris Anderson *Dronecode and the Regulatory Embrace of Open Source*
Thurs	Cyber	Joe Grand *Turning Science into Startups: Lessons from Television and the Real World*	Samy Kamkar *TBD*
Fri	Keynotes	Linda Doyle *Why the World Has Not Changed More!*	Pierre de Vries *Drones in a 3D Wireless World*

Missions

The Missions are a new feature to the typical SDR hackfests, and they are designed to provide significant challenges and a focus on the event. While the Hacker Space is open for all attendees and has open goals and expectations on any specific outcome, the Missions required teams to apply earlier in the year for selection.

During the hackfest, the teams will work on a Mission selected from a set of Missions developed by DARPA. The Missions, as described in the next section, are designed to challenge the communications link between the ground stations and the UAV. The teams will focus on the Missions throughout the week and will have 24-hour access to the facilities, although the UAV range will be shut down daily between 8pm and 8am.

The Missions

General Mission Challenge: Control Link Interference

As described in the introduction, interference is a concern for all radio operations. The control RF link between the ground station and the UAV is always susceptible to breaking due to co-channel and adjacent channel interference. DARPA is providing *gr-uaslink* that consists of a simple physical (PHY) layer to enable controlling the UAV through the SDR-based ground station. The PHY and medium access control (MAC) layer are simple and very susceptible to interference. The problem exists both in interference at the ground station as well as at the drone itself. In all of the Missions, teams must expect some level of interference generated by the DARPA organizers that will challenge the communications links.

Background

Drone swarms are of significant interest to DARPA, which has multiple programs dedicated to new swarm technologies. As the DARPA Service Academy Swarm Challenge showed, having dozens of drones operating in a swarm is possible using off-the-shelf Wifi wireless technology, but the spectrum congestion and interference-prone communications system starts to become a serious issue when trying to control more than 50-60 drones. Going beyond this limit will require more advanced communications systems with either more robust, interference-tolerant links or better use and management of the spectrum, or both. In either case, a new concern becomes relevant to the interference challenge in the three-dimensions of space. In normal circumstances, spectrum and interference is managed by thinking of the surface of the Earth, and so two-dimensionally. The situation of satellite and air traffic is both tightly regulated and a small percentage of overall traffic. When thinking about many dozens to hundreds of radio systems operating in motion in all three dimensions, radio propagation and management is an even more difficult discussion. This mission is scoped around thinking more broadly about interference resilience and the impact of approaches to using spectrum under these conditions.

For the Hackfest, DARPA will provide one or more *Interferer* drones or other radios, as shown in ***Figure 1***. *Interferer* exists in the same airspace using the same spectrum that will cause interference. The DARPA team will control *Interferer* as either a stationary SDR system or potentially as an SDR on another drone. This will be the only other source of RF interference in the team's channel during the experiments. DARPA may change the interference profile to increase the level of difficulty throughout the week to continually challenge the solutions.

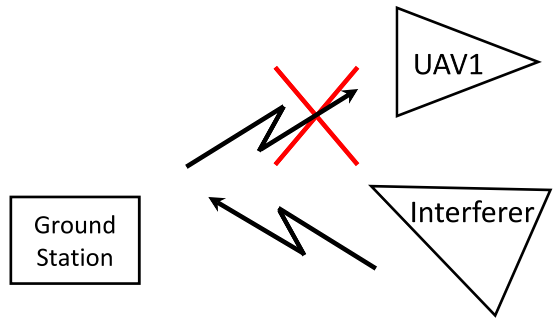

Figure 1. Drone Interference Mission Setup

Teams should develop techniques to defend against sources of interference during all of the other Missions. The limited processor capabilities on the UAV will provide challenges to the design. The DARPA-provided PHY and MAC layers from gr-uaslink are severely susceptible to interference of any kind, and the *Interferer* may provide a significant challenge to providing any control packets to *UAV1*. The interference link from *Interferer* will evolve to continuously challenge the Mission Team's solutions.

DARPA will collect the RF spectrum data continuously to observe how teams created solutions, the evolution of the interference challenges, and how fast the teams can respond to these challenges.

Mission 1: Range Extender

Or 1-Hop Denied RF

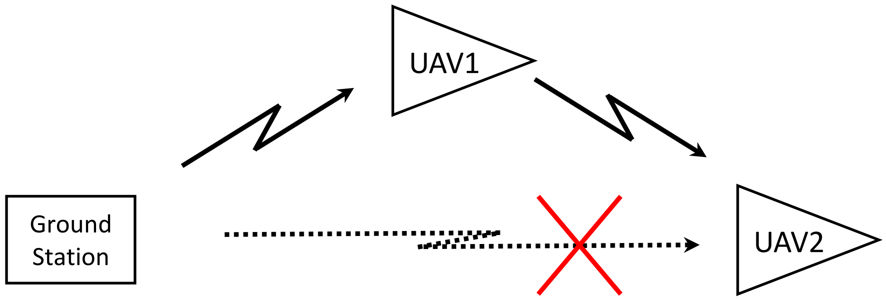

Figure 2. Ground Station link denied to UAV2 and so relays through UAV1

In the scenario diagramed in **Figure 2**, the *Ground Station* needs to communicate with *UAV2*. Some obstruction of the control link either through radio interference, bad propagation, or transmission range issues are preventing the ground station from closing the link. A second UAV that the teams will control, *UAV1*, is in the same airspace and has a better path to both the *Ground Station* and *UAV2*. This mission is to use *UAV1* to hop the messages meant for *UAV2* through it as a router. Both *UAV1* and *UAV2* need to know which packets are destined for itself and which packets are destined for other UAVs. Because the RF environments can change rapidly, the link between the *Ground Station* and *UAV2* may be intermittent, but *UAV1* might still forward on the information. *UAV2* needs to track the received commands for duplications as well as be tolerant of delays in messages and if messages are received out of order.

UAV2 will be a stationary system run by DARPA. It will consist of a computer running the Ardupilot simulator. The laptop will have a USRP to receive the flight control packets that will then be passed into the simulator to control the drone. Teams will have to ensure that all three nodes in this network can speak to each other, so the teams will have access to load their SDR software onto the *UAV2* laptop.

UAV2 will start in a flight stabilized, altitude hold mode and will just loiter and wait for commands. Teams will have to establish and maintain a connection with *UAV2*.

Solutions to this problem should include judicious use of resources. Modifications of the physical, MAC, network, and other layers should all be considered as part of this solution to minimize power and frequency use. Even if both *Ground Station* and *UAV1* are in communications range of *UAV2*, there may be different solutions to maintain communications that optimize for different resources.

Security and authentication are farther challenges to this mission. Show solutions to protecting the connections and data between the drones. *UAV2* should only respond to authorized connections and *UAV1* should not be able to read the packet information to *UAV1*.

Background

A core concept being explored here is how to think about the use of standard wireless solutions that already exist in UAVs. Many of them use the same types of control links, often using standard wireless protocols like Wifi, Zigbee, or cellular standards. Many of these standards are not designed to be robust enough to address key issues in managing fast moving platforms with many propagation issues far different than the intended operation of the standard. Some of these issues are interference related, the ability to support many connected nodes and manage data between them, or are rooted in concepts of a centralized management system like a cellular base station. Each of these ideas quickly finds its limits in complex scenarios that drones present, and this Mission is a way to explore those limitations.

Use of relays in comms links is not a new idea and is central to mobile ad hoc networks (MANET). This isn't even a new idea for UAVs. However, this challenge is to enhance the space by building new tools and a more open developer space for exploring the challenges presented in this scenario. Because of the overall programmability of the communications stack, this Mission is looking to develop innovative ideas for managing the resources and handling the dynamic environments posed here.

The setup for the drone, *UAV1*, is likely a two antenna solution to support the receive-only (RX2) and transmit/receive (TX/RX) antenna ports on the USRP B200mini. While this setup allows full duplex operation in a single band, the use of it as a relay of two-way traffic is difficult to time share the resources. Teams will have to work around this, potentially providing delayed information to *UAV2* and work to minimize that delay. Teams may also want to think of other, more creative solutions to this problem that may minimize the hardware requirements.

Using the same control channels between the *Ground Station* and *UAV1* and between *UAV1* and *UAV2* provides potential for interference. Solutions may require different channels to prevent interference, but now channel management becomes an issue as do frequency tuning times on a single radio. This Mission seeks to explore new solutions to these problems.

Part of this Mission is to push the solutions through the entire communications stack from the application layer to the physical layer. Mostly, today, solutions are explored by assuming that the radio is a black box that works or doesn't. Solutions are then built only into the application layer as the only programmable part of the drone. The DARPA Missions are making the entire stack programmable, and so solutions can be solved anywhere in the stack or by sharing responsibilities throughout the entire stack. An example of this might even be within the transport layer. We default to using TCP and UDP connections because of the significant amount of work as well as the ease of use built into operating systems. TCP has proven challenging for drones because the repeat and acknowledgement requirements can often create unsustainable latency issues, and so UDP is preferred. But with UDP connections, delivery is unreliable, and so applications transmit multiple copies of the same data to ensure delivery. This is a significant waste of resources, and so the Mission should look into methods to optimize.

Another challenge that this Mission presents is privacy and security issues. Controlling a drone by communicating messages through another hop point means that the signal meant for *UAV2* can be changed or corrupted by *UAV1*. How can we manage security and privacy in these solutions? How might this work impact future standards in the drone space, like new MAVLink protocols?

Mission 2: Dynamic Handoff

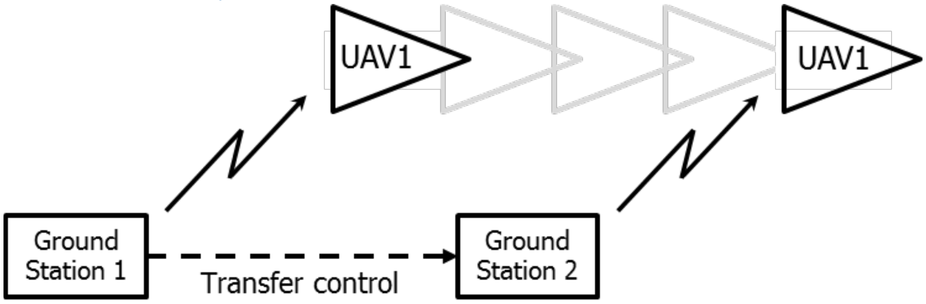

Figure 3. Dynamic handoff of control of *UAV1* as it moves out of range of *Ground Station 1* to *Ground Station 2*.

In the scenario diagramed in ***Figure 3***, *UAV1* is moving away from the controlling ground station, *Ground Station 1*. *Ground Station 1* (GS1) may either be concerned with losing the connection to the drone or has need to transfer control for another reason. *Ground Station 2* (GS2) is asked to take over control of the drone, and so must coordinate with *GS1* to assume control, establish the connection with *UAV1*, and take over flying responsibilities. The connection between *GS1* and *GS2* can be assumed to be robust via direct cable connection or Wifi through the local network.

The goal of this Mission is to show that control can be easily and repeatedly transferred between two ground stations. When one ground station has control, the other ground station should no longer be able to send commands to control the drone until or unless control is transferred back.

An extension of this Mission is to break the connection between the Ground Stations and perform the handoff through the UAV. Making the UAV the center of its communications management would extend to more contested scenarios where the ground stations are not as well coordinated or presence and location are not guaranteed.

Background

Maintaining line-of-sight from a pilot to a drone is a current requirement of civilian operation of commercial drones. Similarly, there are many scenarios when doing detailed flight work for inspections and surveillance of sites may need the drone within sight of the operator. For first responders to disaster sites, this capability could become a crucial enabler when drones are being asked to move through harsh environments where visibility has been degraded such as through smoke or fire and other RF propagation issues may result through changes in geography or nearby structures. The ability to extend the range of operations can come from performing a handoff between operators that would enable a large amount of flexibility in how tasks are completed.

The concept of this Mission lends itself to other techniques in the future. Inverting the mission statement means that one ground station could take over for another to aggregate drones into a swarm. ***Figure 4*** shows this concept of merging drone operations from different ground stations into a swarm controlled by *Ground Station 1*. The Hackfest is not focusing on this particular issue due to the complexity of managing multiple drones, but the handoff of the Mission should translate to this scenario.

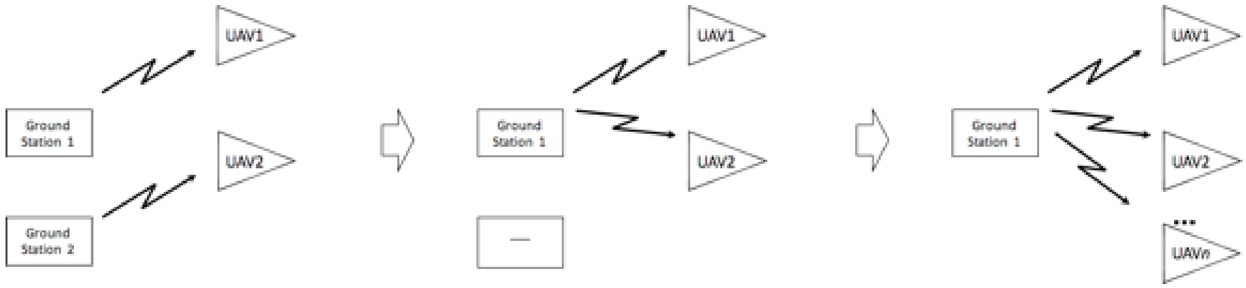

Figure 4. Transferring control over drones from different ground stations to a single swarm.

Mission 3: Sensor Comms and Integration

One of the driving principles of this Hackfest is that the use of SDR makes a drone a programmable extension of the ground station computer. That means programming from the physical link between the two platforms all the way up through the application layer. Given this programmable surface, this Mission seeks to explore how that changes the ability to use, design, and extend the upper-layer protocols. Are there ways to modify the physical link and data link (or medium access control (MAC)) layer to solve certain control issues?

MAVLink allows extensions for custom data sources to be easily integrated into the stream path (e.g., the mavlink_msg_named_value_float_send function). The protocol allows the system to manage the logical transfer of data. This Mission is interested in how we can quickly integrate new sensors into the UAV system and then establish and control the physical transfer of data over a physical channel. Resource management is important here to establish the appropriate bandwidth channel and manage processor resources on the drone to cut down or compress the data as much as possible. New ideas for integrated sensors can require small amounts or intermittent use of bandwidth such as for inertial measurement unit and sensors that sample the environment. Medium sized bandwidth uses might come from things like audio sensors. And large bandwidth sensors for video support. The task will involve appropriate selection of channel width along with modulation and channel coding to go beyond the limitations normally placed on the datalinks by just adding this to the MAVLink connection.

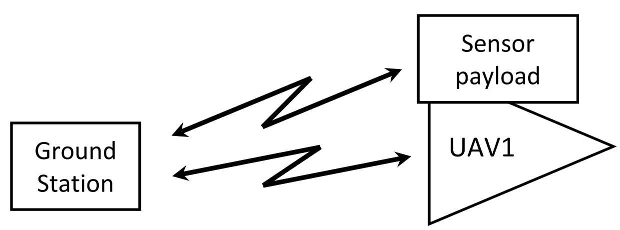

Figure 5. Adding sensors and incorporating sensor information into the link. The sensor's link to the Ground Station can be either a separate physical channel or an inband logical channel with the UAV control link.

For this mission, the teams might look to see what kind of sensor and data is available on the Raspberry Pi or the USRP or look at other sensors to add to the drone. The task is to then look at the sensor payload like in ***Figure 5*** and make sure that the sensor can be tasked from *Ground Station* and passed back through the *UAV1* link. Adding new sensors should be seamless and easily integrated into the communications link to make accessing new information simpler, and the new data should not cause a dramatic burden on the communications link with more data than required.

This Mission can also support many other innovative ideas, like enabling predictive/corrective behaviors to flight patterns and reject/smooth out control inputs from bad communications links. The use of onboard sensors could inform *Ground Station* about the conditions of *UAV1's* environment to help *Ground Station* change its control signal information more adaptively to the flight pattern needs. This can also impact resource allocation such as power, spectrum access/control/optimization, adaptive/predictive comms based on environment, and other innovative ideas.

If moving data from onboard sensors or directing control of the sensors and actuators onboard is a part of a team's solution for this Mission, then the team would also need to think about the privacy, security, and authentication of the commands.

Background

UAVs are, among other things, platforms for experimentation. One of their biggest use cases has been as an enabler for new ways to take video and pictures, so a camera and gimbal have been the first obvious extensions of the drone platforms. Sensors expand well beyond just imagery. In fact, most cases in the past that have mixed SDR with UAVs have been to use the SDR as a very flexible sensor for measuring and monitoring the electromagnetic sensor. Meanwhile, most smart phones and tablets include tens to dozens of sensors of all kinds that lead to innovative uses in our computer apps. This Missions asks: what kinds of new apps can be built from better augmentation of a drone with sensors?

As described in the Mission's problem statement, the protocols are generally already set up with ways to augment the control link with user data, but that presents a significant constraint to the ability to engage the sensor outside just the standard protocol connection. Limitations should only come from the sensor itself, such as how much data it can provide, what latency is inherent in the sensor's activity, and how fast the sensor can be polled. Providing a simplified way to integrate new sensors onto the platform and providing a communications link that can better absorb the sensor's requirements would enable new opportunities to think about UAVs as sensor platforms. Providing the means to stitch into the drone these payloads extends the programmable surface beyond the spectrum and the drone to the inputs that the drone also carries.

Hackfest Organization

Teaming

DARPA selected teams to participate in the Missions during the summer prior to the Hackfest. The teams had three months to prepare for the Hackfest, including two months to work with the software DARPA released. The teams were selected based on the team's capabilities in all areas required to manage the Missions. However, teams are encouraged to work together and can grow or shrink their team as needed during the week of the hackfest. This can include having multiple teams work together or teams could work with the Hacker Space attendees if the talent present there can supplement or address problems.

The hackfest will not be judged as a challenge or competition, so teams are not competing against each other. Instead, teams are competing to put the best technology and ideas in front of DARPA. Because of this, DARPA encourages teams to work on the best solutions, which might involve working with others at the Hacker Space or other Mission teams

Judging

Judging of the teams' solutions will occur on Friday afternoon at the end of the hackfest. The judges are a collection of DARPA Program Managers and will observe the teams' short presentations that will describe the work they were pursuing for one of the Missions before conducting their final test flights. Each team will have 30 minutes to setup, present, and fly. The judges will watch the flights and engage with the teams as necessary to understand the work accomplished, what ideas and technologies were developed during the week, and how these technologies might impact DARPA and the DoD's future needs. Judges will provide unofficial feedback to teams, and any decisions to pursue the technology by DARPA farther will be done directly with the teams post event.

Brainstorming Sessions

A Brainstorming, or BS, Session at the DARPA SDR Hackfest is an opportunity for attendees to engage the larger audience about what they are working on or interested in working on, at the Hackfest. The point of these talks is to give people the chance to discuss immediate problems and successes associated with the work on they are pursuing. This session is not the time for self-promotion or company pitches, which is what the Lightning Talks are for. Instead, this will be a platform to share ongoing Hackfest experiences with kindred spirits and for everyone at the session to discover other ideas, solutions, or overlaps that could be valuable for everyone's respective goals.

The BS Sessions will run during 30-minute windows after lunch on Tuesday, Wednesday, and Thursday. A fourth wrap-up session will run on Friday morning. The first part of the BS Session is to figure out who wants to speak. Someone from DARPA's Hackfest team will organize each session by identifying attendees who want to speak and assigning up to ten minutes to talk, but making sure all speakers can have their say.

One possible use of the BS Sessions is as a way for the Mission Teams to expand their capabilities. If teams run into unexpected problems during the week, someone in the Hacker Space might be able to help solve that problem. Since teams are not competing against each other for a rank throughout the week, but instead are working to showcase their best technology and solutions, it will be up to each team to decide how it engages with other teams and the other Hackfest attendees.

Teams and attendees should use these sessions as a way to let others know about work, capabilities, and activities of interest throughout the Hackfest. This is a great time for demos or announce the intention of showing a demo to fellow attendees.

Lightning Talks

The Hacker Space will host a set of Lightning Talks on Monday through Thursday in the afternoon right before dinner. The Lightning Talks are 5-minute “pitches” to give attendees an opportunity to publicly engage the larger Hackfest community. These talks can feature explanations of a company’s interests, announcements of employment opportunities, descriptions of specific problem areas of interest, stories about past works and hacks, and other topics and information that expose your capabilities and interests.

Lightning Talks are pre-scheduled for the whole Hackfest, and attendees signed up for slots during registration or with the DARPA organizers beforehand.

References

There are no sources in the current document.

Glossary of Acronyms

DARPA	Defense Advanced Research Projects Agency
DoD	Department of Defense
DSSS	Direct Sequence Spread Spectrum
EM	Electromagnetic
EMS	Electromagnetic Spectrum
FHSS	Frequency Hopping Spread Spectrum
FOSS	Free and Open Source Software
IoT	Internet of Things
ISM	Industrial, Scientific, and Medical
MAC	Medium Access Control
MANET	Mobile ad hoc Network
MIMO	Multiple Input, Multiple Output
PHY	Physical layer
RF	Radio Frequency
SDR	Software Defined Radio
TCP	Transmission Control Protocol
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol

Appendix A: Team Spectrum Allocations

Team	Start Frequency (MHz)	Stop Frequency (MHz)
Adversarial Science Laboratory	3010	3020
DeepEdge	3030	3040
DROGON	3050	3060
Fat Cat Flyers	3070	3080
Hacker Dojo Fly-by-SDR Team	3090	3100
Team Platypus Aerospace	3110	3120
Texas Radio Terminator (TRT)	3130	3140
YeS DR	3150	3160
Hacker Space	3170	3190

Appendix B: Technical Information

DARPA has provided a basic SDR physical layer implementation that allows the ground control station to control the SDR-enabled 3DR Solo drone. The source code can be found here:

https://github.com/deptofdefense/gr-uaslink

The drone will host a USRP B200mini as the SDR and a Raspberry Pi 3 (RPi3) as the embedded computer to run GNU Radio and the other software packages. The operating system running on the RPi3 is a Linux distribution created using OpenEmbedded (OE). The recipes and image files for the OE distribution can be found here:

https://github.com/deptofdefense/meta-darpahackfest

The following table lists some of the main software packages and other important information teams should know for how to engage and program the SDR and drones.

Software	URL
GNU Radio	https://www.gnuradio.org/
GNU Radio Modules	http://www.cgran.org
OpenEmbedded	https://www.openembedded.org/wiki/Main_Page
USRP/UHD	https://github.com/EttusResearch/uhd
PyMavlink	https://github.com/ArduPilot/pymavlink
Pixhawk-2	https://pixhawk.org/modules/pixhawk2
Dronekit	http://dronekit.io/
PyBOMBS	https://github.com/gnuradio/pybombs
MAVLink	http://mavlink.org/messages/common
QGroundControl	http://qgroundcontrol.com/

Information on setting up the ArduPilot software-in-the-loop:

http://ardupilot.org/dev/docs/setting-up-sitl-on-linux.html#setting-up-sitl-on-linux