DARPA Brussels Hackfest Problem Book
Understanding our Electromagnetic Environment

Existing and emerging software-defined tools provide unprecedented capabilities to manage and control the electromagnetic spectrum and in particular radio frequency signals. The DARPA Brussels Hackfest aims to challenge the user community to explore the limits of these new capabilities and push the technologies' ability to capture, identify, and characterize incidental RF emissions. These efforts will enable the Free and Open Source Software (FOSS) and defense communities to jointly build a better understanding of interference in the electromagnetic environments of present and future radio communications systems

Tom Rondeau
Thomas.rondeau@darpa.mil
Feb. 1 – 3, 2017
The Hotel, Brussels, Belgium

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 software radio hackfest just before the annual Free and Open Source Developers' European Meeting (FOSDEM) event in Brussels, Belgium. A hackfest, otherwise known as a hackathon or code sprint, is a common way for FOSS projects to engage and enable communities.

DARPA SDR Hackfests

As science and technology continue to advance 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. While the DARPA Brussels Hackfest is aiming to address complex issues of software radio (SR) and the electromagnetic spectrum (EMS), these questions can only be answered by addressing a set of problems that span several fields and disciplines. Traditionally, software radio 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 software radio. Already, software radio is being used successfully in research, prototyping, and development of new wireless communications and radar systems. Beyond those domains, SR 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 software radios, and much of the work going into massive multiple input multiple output (MIMO) systems is performed with software radio. The Brussels Hackfest and subsequent planned events 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 Brussels Hackfest

As the IoT and 5G—the next generation standard for mobile communications—become more foundational for our technological infrastructure, the wireless industry is becoming increasingly aware of issues of interference, noise, interoperability, and cooperation between all of our electronic devices. The ability to address these issues is no longer reserved for wireless and radio engineers because the problems now span a wide set of disciplines. In addition to spectrum allocation and usage, the management of wireless devices include issues such as security, authentication, access control, network routing, power and battery needs, and antenna placement and design. Furthermore, the design, deployment, and maintenance of wireless systems and networks require the development of a huge number of tools, including software

management for code development and debugging, diagnostic tools for addressing problems when devices are fielded, and user interfaces to lower the barriers to using these devices. These problems require a wide range of specialists to work alongside the traditional software radio developers. The industry will need to enlist interface designers, software engineers, data scientists, infrastructure experts, web developers, and many others in order to create a complete solution.

While the focus of the DARPA Brussels Hackfest is on radio frequency (RF) interference issues for commercial communications, DARPA and the U.S. Department of Defense (DoD) also have an interest in acquiring a better understanding of interference issues. Just as in the commercial sector, the DoD's increasing reliance on wireless connectivity entails an equally increasing risk from interference. In forward deployments and military bases, these issues are problematic due to the risk they pose for disrupting communications and, therefore, operations. A shared interest of the military and civilian worlds is RF interference in hospitals; reliance on wireless connectivity for many new diagnostic procedures and instrumentation leads to risks and problems arising from interference.

Recognizing the diversity of skills necessary to address this issue, DARPA is inviting anyone interested in this problem space to attend the DARPA Brussels Hackfest and contribute their talents to the task of better understanding the dynamic RF interference environment. As we have seen in the past, even non-experts in the software radio field can contribute significantly to solving problems while also being able to learn more about software radio and the electromagnetic spectrum. This is a highly consequential technical space that requires both a lot of work in many different fields and a lot of great ideas and innovative thinking.

The rest of this problem book will set up the areas DARPA has identified as important to tackle. DARPA Brussels Hackfest participants will likely organize smaller groups around these problem areas.

The Problem

The Incidental Emitter Interference Problem

The U.S. Federal Communications Commission (FCC) defines incidental emitters/radiators as devices that generate RF energy during the course of their operation but are not intentionally designed to generate or emit that energy [1]. The DARPA Brussels Hackfest aims to address the concept of incidental emissions. The incidental emitters problem has some significant challenges, but is generally not well considered or known even by industry experts.

Radio and wireless systems are intentional emitters. These systems are designed to create electromagnetic signals at specified frequencies. Generally, a regulator licenses the use of some frequency bands for use by a radio or system of radios. Take, for example, mobile communications, where there are channels allocated at various frequencies in the spectrum (see Figure *1*) for different service providers. Those service providers need to make sure that their radios stay within those channel limits. If they emit outside of those channels, they can interfere with radios using the adjacent channels.
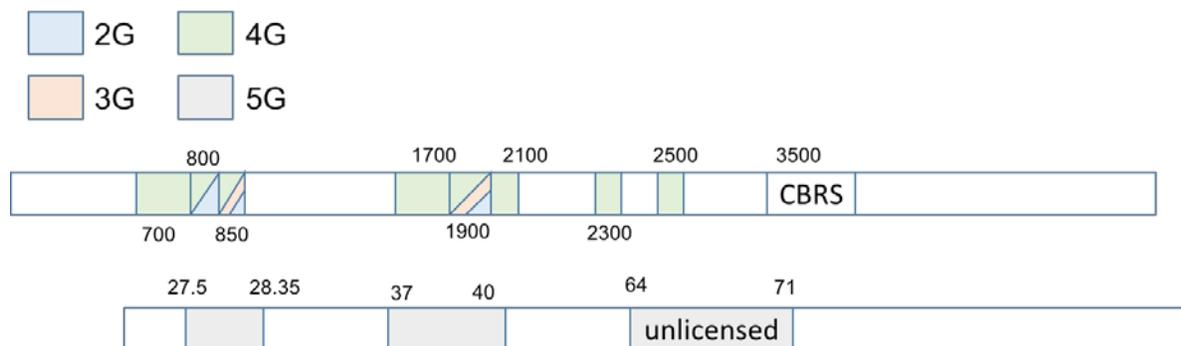

Figure 1: Spectrum allocations for 2G, 3G, 4G, and preliminary 5G (US from new FCC rules) *[2]*.

Another model for spectrum usage is unlicensed allocation. Unlike cellular communications, where operators own a license for use of spectrum and, therefore, can exclude others from using the same spectrum, unlicensed spectrum means that operators do not require a license, although the radio devices sold for unlicensed use are still regulated and must pass certain emission rules. A common use of unlicensed spectrum is WiFi, which is governed by the IEEE 802.11 set of standards. In the United States, these devices follow the Part 15 rules, which demand, among other things, that these devices must avoid interference with adjacent channels [3] [4]. Figure *2* shows the WiFi spectrum mask to which a device must conform so it does not emit too much energy out of band.
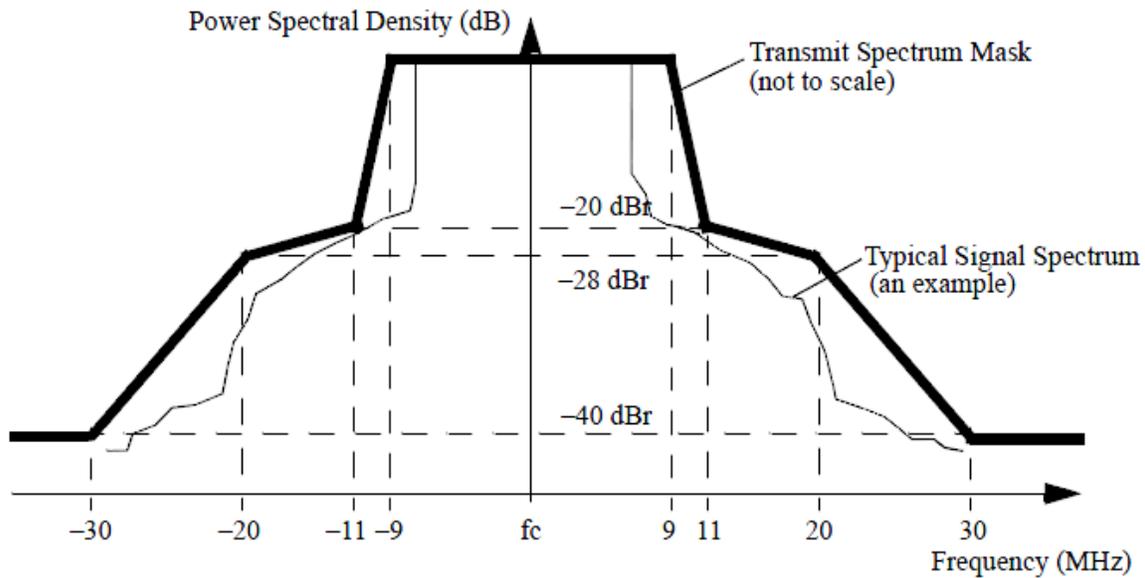
Figure 2: Spectrum mask for WiFi transmissions [5].

An interesting feature in the unlicensed spectrum where many WiFi devices operate is that there are many other radios that share the use of this band of spectrum. The 2.4 GHz band (spanning 2.40 to 2.483 GHz) is one of the Industrial, Scientific, and Medical (ISM) unlicensed bands (this is U.S.-based terminology, though it is not too different globally). Microwave ovens are strong sources of emissions in this band [6]. These devices contain powerful magnetrons that emit electromagnetic waves to excite the rotation of water molecules. The magnetrons are nominally centered around 2.45 GHz, but tend to have fairly wide emissions (10s of MHz). Yet, microwave ovens are not "radios" because their emissions are not designed to travel outside of the system; the emissions do not convey information to another system, nor are the emitted signals recaptured for radar purposes. Ideally, microwave ovens would never emit EMS outside of the oven itself, but they do. In practice, stopping electromagnetic propagation is difficult (e.g., a Faraday cage is really difficult to build in practice). Microwave ovens have also been the source of some interesting scientific problems by being mistaken for signals of interest by SETI [7].

In fact, all electronics create some form of radio emissions. Anything that has a time-changing current will produce electromagnetic emissions. With respect to interference concerns, the questions to ask are how much power is emitted and at what frequencies? Answers to these questions are found in the basic principle of electromagnetics captured in the two Maxwell's equations known as Faraday's Law and Ampere's Law:

$$1) \qquad \nabla \times E = -\mu_0 \frac{\partial H}{\partial t}$$

$$2) \qquad \nabla \times H = J + \varepsilon_0 \frac{\partial E}{\partial t}$$

6

Faraday's Law states that a time-changing electric field induces a magnetic field, and Ampere's Law states that a time-changing magnetic field induces an electric field. These equations describe the basic operation of antennas, in that when a time-varying current (e.g., a sine wave) is applied to a wire (the antenna), this current is converted into an electromagnetic field. Likewise, when a time-varying electromagnetic field passes a wire, the field is converted into a current that flows through the wire.

Throughout the environment, there are devices producing incidental electromagnetic emissions. The challenge of the DARPA Brussel Hackfest is to capture, identify, and characterize as many of these incidental electromagnetic emissions as possible. Understanding what the room, the hotel, the city block, or the host city looks like electromagnetically is an interesting challenge unto itself, but it can lead to potential benefits such as:
- providing a better understanding of urban electromagnetic environments
- improving the scientific understanding of how these signals are generated helping to overcome the interference and other challenges posed by the low-power, localized effects and unspecified frequencies of incidental emissions
- providing useful data to inform the future of wireless communications, specifically by describing the likely environment in which IoT and 5G devices will need to operate
- creating input for regulators and raising new questions that emerge from the data

The DARPA Brussels Hackfest is set up as a "bring your own equipment" event. DARPA aims to provide some tools and equipment to aid and augment the work, but everyone is encouraged to bring their own hardware, such as laptops, software radio front ends, and antennas.

Historical Information
Today's challenges involving software radios and RF interference have interesting historical roots in the early work of Edwin Armstrong, who capitalized on EM emissions to invent the modern radio receiver early in the last century. While asked by the Army to make more sensitive receivers for higher-frequency signals, Armstrong was motivated by the following conjecture: if the spark plugs of (World War I era) airplanes fired at a certain rate, there should be an electromagnetic emission centered around that property, which turns out to be about 10 MHz. Armstrong imagined that if he could build a receiver to detect these emissions from far away, it could provide long-distance warning for approaching bombers. The receiver he created for this purpose, well-known now as the superheterodyne receiver, became the basis for nearly all radios designed for the last hundred years. Today, concerns about RF noise from unmanned aerial vehicles (UAVs) and car motors have been discussed in a similar context [8].

On another historic front, the advent of semiconductor devices posed additional interference challenges. While a crystal will oscillate and emit signals at fairly well-defined frequencies, semiconductors have different behaviors. When a signal is applied to a semiconductor, it has a linear and nonlinear response region. A diode is a semiconductor device, and diodes are used in rectifiers—converting alternating current (AC) to direct current (DC). Although our power grids today are based on an AC system, many of our electronics are based on DC power, which is

created via conversion of AC power by means of power supply/converter devices, which use diodes and other semiconductors. The nonlinear responses of an electronic circuit are defined such that frequencies at circuit outputs are different than frequencies at the inputs. That means all of these circuits are emitting electromagnetic signals in various frequencies across the spectrum. Among the relevant devices that the FCC identifies as exhibiting this emission behavior are light-emitting diode (LED) light bulbs, chargers for cell phones and other consumer devices ("wall warts"), and lithium-ion power supplies such as those found on many commercial UAVs.

Extending the ideas developed above to how different devices emit signals leads to the primary question DARPA is asking in this hackfest: what does this space of incidental emissions look like? More detailed questions are outlined later in the problem book.

Reading Material

The potential of incidental RF emissions to affect the performance of communication systems has been known and studied for more than four decades [9] [10] [11]. More recently, with the anticipation of the IoT, 5G, machine-to-machine communications, and autonomous vehicles [12], spectrum regulators are becoming increasingly concerned that background noise and interference has (or will) become the performance-limiting factors in the envisioned proliferation of wireless communications [13] [14]. Preliminary research and findings [15] indicate the need for follow-on, high-quality studies including data collection/measurement of incidental RF emissions, storage, dissemination, and analysis.

Sources of incidental RF emissions are numerous. Among them are microwave ovens [7] [6], car engines [9] [16], power lines [10] [11], digital electronics [17] [18], railway systems [19], USB keyboards [20], and RF LED lighting products [21].

Many techniques and approaches have been proposed for measurement, detection ([17] [18] [22] [23] [24]), acquisition, identification [25], characterization ([18] [26]), localization ([24] [25]), and recognition ([16] [25]) of incidental RF emissions. An automated measurement system for an incidental emitter is reported in [27].

DARPA provides this limited list for reference only. It is not meant to be exhaustive or imply disinterest in other incidental emitters or approaches that participants may consider important to investigate.

DARPA Brussels Hackfest Structure

Attendees may work on any or all aspects of the problem set below. Collaboration and teaming are recommended in order to support communication and information sharing between groups. There are a number of potential dependences that may exist between each problem space below.

To frame how to work at the hackfest and address the problems defined in the bullets below and in further detail later, think of a scenario for collection. In many respects, this follows the scientific method.

- Set up the hardware system and antenna(s) near the device/location of interest
- Capture the data and store metadata information about the capture
- Analyze the data to isolate and identify emissions
- Characterize the emissions that have been isolated and identified
- Share the results with the community and/or prepare them for publication

Data Collection

Capture

The ability to observe and record incidental emissions is a key challenge of this hackfest. The difficulty in capturing emissions results from a lack of knowledge about the environment as the number and variation in emitting electronic devices continues to increase. All electronic devices emit incidental radiation. The references at the end of this document provide some insight into the techniques available to capture such emissions.

The Capture Challenge presented to the DARPA Brussels Hackfest is to develop new or improved capture techniques to enable capture of sufficient spectrum for subsequent identification and characterization of incidental emitters in our environment.

- Can we develop methods and experimental practices to control the capture of emitters in the field?
- To best capture the signals, are there procedures for localizing and running control-based experiments?
- Which type of instrumentation is required? (antennas, receiver chain, detection range and sensitivity, spatial and temporal resolution, frequency-scale resolution, directionality, data statistics, environmental impacts, etc.)
- Where are incidental emissions signals located (nearfield, far-field)?
- How does the physical environment impact capture?
- Which characteristics of incidental emissions can be captured?
- Which emission characteristics are required to inform the signal capture and support subsequent identification and characterization?
- How can captured data be formatted for subsequent processing? (Please see guidance on GNU Radio formatting below)

The most basic, easy way to get started capturing signals is to use GNU Radio and a compatible SDR device (see Equipment Study section). GNU Radio supports all UHD-based (USRP Hardware Driver) devices as part of the main code, and any other compatible device will either work with the gr-osmosdr [28] or a similar out-of-tree module to support it. If UHD compatible, then we can use the UHD capture script that comes with GNU Radio:

$ uhd_rx_cfile <args> filename

The "args" are arguments we pass to this script to set up variables such as the frequency, bandwidth, gain, and other adjustable parameters of the SDR device. The "filename" is the name of the file where data is stored during the capture time. The data is stored in a simple binary file format [29], though we are encouraging the use of the metadata file format [30], which requires using the '-m' argument in the script. As discussed later in the Characterize section, the metadata format will allow better management of the information about the data to help later data analysis.

The gr-osmosdr module has a useful script called "osmocom_rx_cfile" with similar inputs. Part of the Capture problem will be to understand what the correct settings are for the different signals we are looking to study.

Some additional problems to consider addressing during the hackfest include methods to increase the capabilities of the file capture scripts to better handle the metadata processing. For instance, one could:

- Add an argument to use the detached header mode of the metadata file capture
- Add the ability to insert custom metadata information to store in the metadata headers to identify the experiment
- Add metadata file support to osmocom_rx_cfile

Equipment Study

There is a large and growing number of types of software defined radio hardware available on the market today. The links below provide a sense of some of the types of equipment available, which may support the problem book for this hackfest.

- Roundup of Software Defined Radios [31]
  Compiled list of available SDRs (as of 08/2014) comparing the cost, frequency range, ADC resolution, maximum instantaneous bandwidth, and whether or not it can TX and if it has any pre selectors built in.

- Software Radio Front Ends (RFEs), GRCon15 [32]
  Overview, comparison, and evolution of the many radio front ends that have support in one way or another from GNU Radio.

- Software Radio Front Ends (RFEs), GRCon14 [33]
  2014 GNU Radio presentation overviewing the history and use of software defined radios.

An interest of the DARPA Brussels Hackfest is if the community is able to bring new/innovative equipment capable of capturing emissions from incidental emitters. We can then ask how each of these devices performed to answer the questions posed here.

Ideas on antennas

Based on the review of the above academic literature, broadband biconical antennas [34] or broadband log-periodic antennas [35] are typically used in setups for measurement of incidental emissions. In addition, use of loop antennas [36] and near field probes [37] has been reported. An interest of this hackfest is if the community is aware of other antenna technologies/architectures capable of receiving emissions from incidental radiators.

As the DARPA Brussels Hackfest is a "bring-your-own equipment" event, anyone with interesting antennas is encouraged to bring them along to help in the work and study.

Isolate/Identify

The ability to identify signals within the successfully captured spectrum is a second key challenge of this hackfest. For the purposes of the DARPA Brussels Hackfest, isolation refers to the pulling out of incidental emissions from the captured spectrum. A variety of signal processing algorithms and extraction techniques have been used to isolate small signals from large noise floors and/or decouple overlapping signals.

The Isolation/identification Challenge presented to DARPA Brussels Hackfest attendees is to expand upon existing techniques or develop new approaches to isolate/identify signals of incidental emitters within the captured spectrum.

Hackfest Isolate/Identify Questions
- Which features and attributes of incidental radiation can be used for identification?
- Which signal processing algorithms can be used?
- How can techniques like machine learning, such as neural networks, be applied to facilitate signal identification?
- How can environmental and situational awareness facilitate identification?
- What insights can be pulled from other fields where small signal identification is required?

Visualization tools are important for this step as it will be necessary to perform various transforms and look through large amounts of data in different ways to develop new understandings of the signals. GNU Radio provides some very basic scripts for displaying data but also has a large collection of blocks and visualization aids to construct new ways of manipulating and viewing signals. Other tools to do offline data processing include Octave and Matlab. Inspectrum [38] also offers a set of tools, based on GNU Radio, for doing offline signal analysis.

The stand-alone tools are often sufficient for reading the binary data format from GNU Radio, but most are not capable of reading the metadata header file. GNU Radio supports a block that can read both the data and metadata header files together and source that information into the flowgraph. Can we extend the offline analysis tools to make better use of the metadata file information?

Characterize

After successful isolation of incidental signals from the captured spectrum, the ability to characterize or otherwise attribute signals to a particular electronic system is another key challenge being addressed by the DARPA Brussels Hackfest. A number of signal processing algorithms and pattern-recognition methods, which have achieved varying degrees of success, can be found in the referenced literature.

The Characterization Challenge presented to DARPA Brussels Hackfest attendees is to expand upon existing techniques or develop new approaches to characterize the source of incidental signals and uniquely attribute the signal to a particular source.

Hackfest Characterization Questions
- How can metadata be used to support characterization? What data formats and taxonomies are most useful?
- Are large signal processing approaches applicable to small signal incidental emitters?
- Does the complexity of the incidental emitter environment require or enable new/alternative approaches to characterization?
- How do capture and identification methods impact characterization? Would capture of larger frequency ranges or smaller time steps enable better characterization?
- What features/characteristics of isolated signals enable attribution to specific electronics?
- What training is necessary to enable unique characterization?
- What level of signal fidelity is required for unique characterization?
- How can techniques like machine learning and neural networks enable characterization?
- How much data do we need? How should it be labeled?
- How do estimators support characterization?
- What atypical spectral properties enable characterization?

Challenge Problem: RF-Based Localization

Most of the problems as specified so far are fundamental technology challenges for handling the data collection and signal identification. Knowing more about these signals and how to collect them can lead to some specific, interesting questions. One problem in this hackfest for any participants who are looking for a bigger challenge is to use the ability to collect incidental emissions from the current environment to provide a form of RF-based mapping. If all of the emitters in a room are characterized and located, can we reverse that process through a single collection location, and then, based on the received results can we determine where in the room we are positioned? Would this be possible with a single antenna? How much of a problem is multipath transmission/reception in these scenarios with the power levels emitted? Would directional antennas help?

Managing the Data

Metadata Tagging

As illustrated during the discussion on characterization above, metadata tagging is a critical step to efficient and coordinated processing of signals within an SDR environment, particularly when a variety of equipment types is being used within the community. To help limit the difficulty for attendees to share information during the DARPA Brussels Hackfest, everyone will be required

to standardize file formats to the GNU Radio's metadata file format [30]. Attendees should use the detached header mode format for the metadata files so each collection ends up with two files: the data file itself (filename.dat) and the metadata file (filename.meta). Inside the metadata, we should add a header field for the filename of the associated data file. In the Dissemination of Data section, we will talk about changing this to a URL from where the data file can be downloaded.

The Metadata Challenge presented to DARPA Brussels Hackfest attendees is to develop improved methods of reading, writing, passing, and otherwise handling metadata file information during the capture/identify/characterize/disseminate process chain.

Questions about Handling Metadata
- What methods/approaches can be adopted to enable better reading from/writing to metadata headers?
- Does the current GNU Radio metadata capture the necessary fields? Should it be modified and, if so, how?
- How can metadata files be effectively updated at any point during the flow chain?
- How can metadata integrity be maintained throughout processing and dissemination?
- Which verification tools are required?
- Where and how should metadata files be hosted to support these new approaches?
- Is remote hosting and parsing possible? If so, how?

Dissemination of Data

Dissemination of collected data after the DARPA Brussels Hackfest is over is another key challenge. Sampling spectrum over multiple MHz or GHz of bandwidth can create significantly large file sizes that are difficult to store and transfer. We also require metadata attached to the data files to explain what is in the data files as well as information on how the data was collected.

The data Dissemination Challenge presented to DARPA Brussels Hackfest attendees is intended to develop efficient and effective methods for storing, accessing, and otherwise interacting with data collected during the event.

> **Questions about data dissemination**
> - Can/should metadata files be stored separately from data files for optimized storage and retrieval?
> - Can existing hosting services like Github be effectively used for this purpose?
> - What impact does hosting and file separation have on required metadata fields?
> - How can data files be effectively verified and validated to ensure trust within the community? What level of verification is required?
> - How do downstream updates to a data file impact version control and attribution?
> - How do local, potentially limited, or varying upload/download rates impact dissemination?

Dissemination of Code

Another issue, which is similar to the challenge of data dissemination, is how to manage and disseminate code that is generated during the DARPA Brussels Hackfest. In keeping with the FOSS spirit, it is essential to the Hackfest that all code generated during the event is shared and available to the community. The intent of the event is build a foundation for a community of technologists who want to continue to work on these problems.

The Code Dissemination Challenge presented to DARPA Brussels Hackfest attendees is intended to develop the capability to effectively and efficiently share code with the community.

> **Questions about code dissemination**
> - How can multiple coding languages and platforms be effectively shared between attendees?
> - How can code be efficiently verified and validated to ensure trust amongst users?
> - How can code be effectively uploaded/downloaded between attendees?
> - How can updates/modifications be properly shared? What "header" information should be required to properly communicate the purpose and utility of a particular piece of code?
> - Do sharing service sites like Github make sense as a central repository of developed code?
> - What group development media are available to quickly and efficiently develop code?
> - Can previously developed code be effectively integrated into this hackfest?

Hackfest Organization

Teaming

A hackfest is a place to both bring your special skills to interesting problems and learn more about areas outside your field of expertise. DARPA Brussels Hackfest attendees are not expected to have an expert grasp on all issues addressed in this problem book. What's more, in the mere three days of the event, it would be difficult for everyone to address all of the problems. Therefore, teaming is encouraged and expected.

The DARPA Brussels Hackfest will begin with a description of the problems, subproblems, and expectations for how they can be addressed over the course of the three days. Next will be a general discussion session to answer questions and clarify the problems, subproblems, expectations. Teaming will follow to allow attendees to find the right approach.

A common theme in open source software development is that you make of it what you want, which translates into stepping up and engaging with the problems you find interesting. At a hackfest, this means actively engaging with fellow participants and finding out how to use your collective backgrounds and skills to help solve problems of interest to you.

Schedule

Wednesday, Feb. 1
- 8:00: Registration
- 9:00: Introductory remarks and problem description (Tom Rondeau, DARPA)
- 9:30: Open discussion to problem formulation and approaches
- 10:00: Teaming
- 10:30: Open work
- 17:00: Daily wrap-up; reporting on progress
- 20:00: Room closed

Thursday, Feb. 2
- 8:30: Registration
- 9:00: Hackfest day 2, begins
- 17:00: Daily wrap-up; reporting on progress
- 20:00: Room closed

Friday, Feb. 3
- 8:30: Registration
- 9:00: Hackfest day 3 begins
- 16:00: Teams report on work
- 18:00: Hackfest concludes

Anticipated Outcomes

The outcome of a hackfest is only really discernible through the perspective of time, based on how much the participants grew the technology and community. In the short term, however, we would like to have some measurements for a successful hackfest based on the problems provided here.

Some simple metrics of activity can include:
- Lines of code written/changed
- Number of new applications
- Number of commits to existing programs
- Number of working novel demonstrations

We can use these metrics to acquire some data that we can reference for activity, but no single line of code or commit is by itself meaningful. For the purposes of this hackfest, which is dedicated to incidental emissions, we can identify a few more specific metrics:
- Number of signals collected/found/identified/characterized
- Feedback for the FCC and other regulatory bodies
- Answers to the questions posed in the problem book
- Continued investment and involvement in building tools and techniques to carry this work forward after the Hackfest is over

Over time, DARPA would like to see increasing activity in the software radio space, to include application development and data analysis. Is there a general increasing trend in the number of contributors and commits to specific projects? Does the work generate better and improved applications, documentation, and motivations to lower the barrier to entry to working on communications and electromagnetic problems using software radio?

Thank you for being part of this community effort to characterize and better understand the increasingly complex electromagnetic environment in which we all live, work, and play.

References

[1]   FCC, "Equipment Authorization – RF Device," [Online]. Available: https://www.fcc.gov/oet/ea/rfdevice.

[2]   "Cellular frequencies in the US," 22 October 2016. [Online]. Available: https://en.wikipedia.org/wiki/Cellular_frequencies_in_the_US.

[3]   FCC, "Radio Spectrum Allocation," [Online]. Available: https://www.fcc.gov/engineering-technology/policy-and-rules-division/general/radio-spectrum-allocation.

[4]   T. N. A. f. A. Radio, "Part 15 - Radio Frequency Devices," [Online]. Available: http://www.arrl.org/part-15-radio-frequency-devices.

[5]   P. d. Vries, "Is 2.4GHz Wi-Fi the next GPS/LightSquared?," [Online]. Available: http://www.policytracker.com/free-content/blogs/pierre-de-vries/is-2.4ghz-wi-fi-the-next-gps-lightsquared.

[6]   T. W. Rondeau, M. F. D'Souza and D. G. Sweeney, "Residential Microwave Oven Interference on Bluetooth Data Performance," *IEEE Transactions on Consumer Electronics,* vol. 50, no. 3, pp. 856-863, 2004.

[7]   N. Drake, "National Geographic," 10 04 2015. [Online]. Available: http://phenomena.nationalgeographic.com/2015/04/10/rogue-microwave-ovens-are-the-culprits-behind-mysterious-radio-signals/.

[8]   B. Seeber, "DEF CON 24 Wireless Village - Balint Seeber - SDR Tips and Tricks," 9 November 2016. [Online]. Available: https://www.youtube.com/watch?v=yZ5G0nYSM98.

[9]   R. B. Schulz and R. A. Southwick, "APD Measurements of V-8 Ignition Emanations," *IEEE Electromagnetic Compatibility Symposium Record,* pp. 1-8, 1974.

[10]   J. A. Malack, "Development of a Power Line Conducted Emanation Limit," in *1977 IEEE International Symposium on Electromagnetic Compatibility*, 1977.

[11]   J. R. Engstrom and J. M. Malack, "Simulation of Electronic Data Processing/Office Machines Equipment Emanations in AM Broadcast Receiver Studies," in *IEEE 1976 International Symposium on Electromagnetic Compatibility*, Washington, DC, 1976.

[12]   A. Palaios, "Contemporary Radio Noise Characteristics and Low-Cost Transceivers in the Era of New Deployments (IoT, M2M, 5G, Autonomous Vehicles)," 6 December 2016. [Online]. Available: https://www.linkedin.com/pulse/contemporary-radio-noise-characteristics-low-cost-era-palaios.

[13]   FCC, "Federal Communications Commission," 15 June 2016. [Online]. Available: https://apps.fcc.gov/edocs_public/attachmatch/DA-16-676A1.pdf.

[14]   D. R. R. J. M. MARK A. MCHENRY, "IEEE Spectrum," 18 August 2015. [Online]. Available: http://spectrum.ieee.org/telecom/wireless/electronic-noise-is-drowning-out-the-internet-of-things.

[15]   A. Palaios, "Federal Communications Commission," 26 October 2016. [Online]. Available: https://www.fcc.gov/ecfs/filing/10261021302342/document/102610213023421003.

[16] X. Dong, H. Weng, D. G. Beetner,, T. H. Hubing,, D. C. Wunsch II,, M. Noll,, H. Goksu and B. Moss, "Detection and Identification of Vehicles Based on Their Unintended Electromagnetic Emissions," *IEEE TRANSACTIONS ON ELECTROMAGNETIC COMPATIBILITY,* vol. 48, no. 4, pp. 752-759, 2006.

[17] C. Stagner, D. G. Beetner and S. L. Grant, "A Comparison of Algorithms for Detecting Synchronous Digital Devices Using Their Unintended Electromagnetic Emissions," *IEEE Transactions on Electromagnetic Compatibility,* vol. 56, no. 6, pp. 1304-1312, 2014.

[18] H. Garbe, "How to reproducibly measure the unintended EM-emission from handheld devices," in *2015 IEEE 5th International Conference on Consumer Electronics - Berlin*, Berlin, 2015.

[19] H. W. M. Smulders and H. A. Prins, "Fast and efficient determination of Eigenfrequencies of railway systems," in *2015 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings*, Pisa, 2015.

[20] D.-j. Sim,, H. S. Lee, J.-G. Yook and K. Sim, "Measurement and Analysis of the Compromising Electromagnetic Emanations from USB Keyboard," in *2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, Shenzhen, 2016.

[21] "RADIO FREQUENCY LED LIGHTING PRODUCTS," 17 June 2016. [Online]. Available: https://apps.fcc.gov/kdb/GetAttachment.html?id=K0pZdRE7biF3aqgO4XZ8cw%3D%3D&desc=640677%20D01%20RF%20LED%20LIGHTING%20v01&tracking_number=20518.

[22] M. Vuagnoux and S. Pasini, "An improved technique to discover compromising electromagnetic emanations," in *2010 IEEE International Symposium on Electromagnetic Compatibility*, Fort Lauderdale, 2010.

[23] S. P. Acharya and I. G. Guardiola, "Detection of RF devices based on their unintended electromagnetic emissions using Principal Components Analysis," in *2013 Wireless Telecommunications Symposium (WTS)*, Phoenix, 2013.

[24] V. Thotla, M. T. A. Ghasr, M. Zawodniok, J. Jagannathan and S. Agarwal, "Detection and localization of multiple R/C electronic devices using array detectors," in *2012 IEEE International Instrumentation and Measurement Technology Conference Proceedings*, Graz, 2012.

[25] I. G. Guardiola and F. Mallor, "A Nonparametric Method for Detecting Unintended Electromagnetic Emissions," *IEEE Transactions on Electromagnetic Compatibility,* vol. 55, no. 1, pp. 58-65, 2013.

[26] M. Prvulovic, A. Zajić, R. L. Callan and C. J. Wang, "A Method for Finding Frequency-Modulated and Amplitude-Modulated Electromagnetic Emanations in Computer Systems," *IEEE Transactions on Electromagnetic Compatibility,* vol. 59, no. 1, pp. 34-42, 2017.

[27] F. Joseph, B. Arnold and N. Van, "Development of an automated unintended radiated emission (URE) radio frequency (RF) measurement system," in *84th ARFTG Microwave Measurement Conference*, Boulder, 2014.

[28] D. Stolnikov, "gr-osmosdr," 2015. [Online]. Available: http://cgran.org/pages/gr-osmosdr.html.

[29] G. Radop, "GNU Radio," [Online]. Available:
http://gnuradio.org/redmine/projects/gnuradio/wiki/FAQ#What-is-the-file-format-of-a-
file_sink-How-can-I-read-files-produced-by-a-file-sink. [Accessed December 2016].

[30] G. Radio, "GNU Radio," [Online]. Available:
http://gnuradio.org/doc/doxygen/page_metadata.html. [Accessed December 2016].

[31] RTL-SDR.COM, "ROUNDUP OF SOFTWARE DEFINED RADIOS," 20 August 2014. [Online].
Available: http://www.rtl-sdr.com/roundup-software-defined-radios/.

[32] T. Newman, "GRCon15 Presentations," [Online]. Available:
http://www.trondeau.com/grcon15-presentations#monday_Newman_RFEs. [Accessed
December 2016].

[33] T. Rondeau. [Online]. Available:
http://static1.1.sqspcdn.com/static/f/679473/25461569/1411158616463/Sep15_03_Ron
deau_RFEs.pdf. [Accessed Decemeber 2016].

[34] Schwarzbeck. [Online]. Available: http://www.schwarzbeck.de/en/antennas/biconical-
antennas.html. [Accessed December 2016].

[35] "Standard LPDA," [Online]. Available:
http://www.schwarzbeck.de/en/antennas/logarithmic-periodic-broadband-
antennas/standard-lpda.html. [Accessed December 2016].

[36] E. T. Systmes. [Online]. Available: http://www.schwarzbeck.de/en. [Accessed December
2016].

[37] Beehive Electronics, [Online]. Available: http://www.beehive-
electronics.com/datasheets/100SeriesDatasheetCurrent.pdf. [Accessed December 2016].

[38] GitHub, [Online]. Available: https://github.com/miek/inspectrum. [Accessed December
2016].

Glossary of Acronyms

Free And Open Source Software (FOSS)
Defense Advanced Research Projects Agency (DARPA)
Free and Open Source Developers' European Meeting (FOSDEM)
Software Defined Radio (SDR)
Electromagnetic Spectrum (EMS)
Internet of Things (IoT)
Multiple Input Multiple Output (MIMO)
The U.S. Federal Communications Commission (FCC)
Industrial, Scientific, and Medical (ISM)
Radio Frequency (RF)
Alternating Current (AC)
Direct Current (DC)
Light Emitting Diode (LED)