

LARGE SCALE COLLABORATIVE DETECTION AND LOCATION OF THREATS IN THE ELECTROMAGNETIC SPACE

Domenico Giustiniano (domenico.giustiniano@imdea.org)

IMDEA Networks Institute, Madrid, Spain

Vincent Lenders (vincent.lenders@electrosense.org)

Electrosense, Switzerland

Sofie Pollin (sofie.pollin@esat.kuleuven.be)

KU Leuven, Belgium

Abstract. In the 21st century, the security of the electromagnetic spectrum has tremendous strategic importance to society. In particular, the wireless infrastructure that carries vital services such as 5G cellular networks, communication to aircraft and Global Navigation Satellite System is especially critical. This rapid change is even more impressive considering that in the 80s the only concern for spectrum management was mostly about radio/television broadcasting and military communications. The allocation of spectrum has become over the years more and more complex with different players and stakeholders that depend on largely of their correct operation. However, today, the cost of commodity radio technology prices is so low that access to it is no longer restricted to governments and network operators. It is now affordable to individuals, giving them the potential to become malicious intruders. More frequent and more sophisticated threats from such infiltrators could wreak havoc and are among the most serious challenges faced by society. Unauthorized transmissions could threaten the operation of networks used by air traffic control systems, police, security and emergency services in populated areas. The SOCRATES (Large Scale Collaborative Detection and Location of Threats in the Electromagnetic Space, Grant G5461) project started in June 2018 and aims to deliver a security system to protect our electromagnetic environment and the services and users that depend upon it. SOCRATES will provide an accurate, autonomous, fast and secure system based on a novel and disruptive IoT (Internet of Things) architecture. By detecting and locating unusual RF signal and source activity it will identify intruders in the electromagnetic space, before a threat can become serious, learning about its physical layer features and its geographic location. By providing the capability to detect, identify and locate potential threats to electromagnetic infrastructure security, SOCRATES represents an important step in ensuring society's readiness to respond effectively to them. SOCRATES will shield economic and social structures from those who would harm them. In this contribution we present a summary of published results achieved in the first year of the project, how funds from SOCRATES have foster the collaboration between NATO countries Spain and Belgium and partner country Switzerland, including the activities led by Electrosense as partner country.



1. Introduction

Protecting the wireless infrastructure and detecting malicious intruders in the spectrum are deemed essential for the society in the 21st century. In light of this problem, new technologies for detecting threats in the electromagnetic space must be devised to counteract possible catastrophic threats and take fast decisions. In the SOCRATES project we aim to deliver a security system to protect our electromagnetic environment and the services and users that depend upon it (SOC, 2019). SOCRATES started in June 2018 and will be delivered in May 2021. Our system will blend new emerging and diverse disruptive technologies in order to provide accurate and fast detection, classification and location of intruders in the spectrum in the time, frequency and space domains. Using the innovative solutions developed in the project, stakeholders will be able to significantly reduce the danger of threats and have access to advanced methodologies for swiftly taking the correct actions. Our system builds on top of the emerging Electrosense (<https://electrosense.org>) initiative led by the partner country of the consortium. Electrosense is a non-profit association for distributed crowdsourcing, monitoring and storage of the wireless spectrum, which uses low-cost spectrum sensors, with its beta version already operative both for research and for providing a first set of applications to end users and stakeholders (Rajendran et al., 2018). We will build on top of this network to address the most dangerous threats in the wireless electromagnetic space, with the objective of spotting and locate the spectrum saboteurs.

The paper is organized as follows. In Section 2 we present the overall goal of the project, followed by Section 3, that shows the results in this first year of the project, with particular emphasis on published material. Finally, in Section 4, we briefly present the deployment status of Electrosense through the funding received in SOCRATES, the key factor for collecting large scale data set as needed to execute the project.

2. Overall goal

To counteract the threats in the electromagnetic space, there is the pressing need to design novel, flexible and autonomous methods to protect the wireless infrastructures from cyber-attackers and develop novel architectures and technologies to support cyber defence capabilities. In order to address this problem, the vision of SOCRATES is to create the foundations for an accurate, autonomous, fast and secure system that identifies intruders in the electromagnetic space, before the threat can become serious, learning about its physical layer features and its geographic location. SOCRATES is led by

IMDEA Networks, Spain (NATO country), which works in this project with non-profit association Electrosense, Switzerland (partner country), and KU Leuven, Belgium.

In the project we will exploit novel techniques and new disruptive technologies emerging in diverse research sectors and their largely unexplored mutually interactions to find ground-breaking solutions to the grand challenges in security above described. We will start from the current Electrosense spectrum monitoring system, currently in its beta version, designed and deployed by project members for civilian applications, and investigate novel system concepts, methods, and algorithms to introduce the second generation of the Electrosense system that will target security applications. Electrosense uses off-the shelf software-defined low-cost spectrum sensors (but it can also operate with more expensive boards, such as Ettus), currently mainly located around Europe. It has a backend component to control the sensors, support low-latency stream processing and large-scale batch analyses at the same time. Spectrum data computation and storage in Electrosense is implemented using state-of-the-art big data lambda architecture (Rajendran et al., 2018).

The new system that will be developed in SOCRATES will process raw observables in the sensor, that is, in-phase and quadrature phase (I/Q) samples of spectrum received from the RF front-end, which we consider a key enabler for the security applications studied in the project. The availability of I/Q samples will unleash new opportunities to innovate on the methods to extract information in the data received by each spectrum sensor. In fact, while derived observables such as averaged power spectral density (PSD) measurement data suffices for coarse understanding of the usage of the spectrum, accessing and processing raw I/Q measurements is fundamental in security contexts.

The raw observables (I/Q data) can have a tremendous potential to provide greater performance in cooperatively detecting and locating RF intruders beyond state-of-the-art solutions. Yet, it first implies a deluge of data to be transmitted to the backend, which is not feasible to sustain for every users at their home with current Internet deployments. Therefore, it is not possible to collect continuously I/Q data. Second it requires more powerful machines to process data in the backend and novel algorithmic solutions that can scale well with the number of sensors. These algorithms must find the best solutions to process (at least partially) raw observables in the spectrum sensors while taking advantage of derived and lower-complexity observables such as PSD for a first level of detection of the intruder. SOCRATES will dynamically select what observables to fetch and their structure in time, frequency and space dimensions. In turn, careful decision about what observables (raw, derived, type of derived, etc.) to fetch at any point in time from the spectrum

sensors is needed.

Proper and flexible integration of new disruptive technologies will be used to investigate methods for geo-locating radio transmitters that can work with low-cost software-defined spectrum sensors distributed over the public Internet. In the envisioned system, we expect to concurrently localize and detect the anomaly, and we will look for novel approaches to perform these tasks jointly. At the end of the project, real experiments will showcase the systems ability to detect the waveforms and wireless technologies of adversaries who are misusing wireless resources. We will also demonstrate how the physical location of an intruder can be swiftly identified. Adopting an agile approach, SOCRATES will build, demonstrate and showcase early prototypes throughout the project.

3. Results in the first year of the project

In this section, we present the scientific contribution and other dissemination activities of the project. The three partners of the project are largely collaborating in the project, as the Electrosense infrastructure from the partner country Switzerland is used for experimentation. This is also demonstrated by several joint top publications among project partners, as well as two hackathons that have been organized in Spain and Germany as training activities. Members from all three organizations have participated in the hackathons (the results of these hackathons have resulted in papers that are currently under submission).

3.1. SCIENTIFIC CONTRIBUTION

In terms of scientific output, the project has resulted in the first year in one ACM/IEEE IPSN 2019, a top conference in networked embedded systems, one ACM Mobicom 2019, the premier conference in mobile computing, and one IEEE Dyspan 2019, a very well recognized international conference that mixes technology and policy issues, becoming the reference meeting point for sharing and exploring advanced spectrum technologies. Furthermore, one paper has been published in IEEE Transactions on Cognitive Communications and Networking (TCCN) (extension of the IEEE Dyspan 2019 paper).

In what follow, we describe in details the scientific output in the first year, mainly focusing of published material and open source code.

3.1.1. *Sensor Architecture*

In the first year of the project, we have designed an expansion dongle for Electrosense, to extend the sensing capabilities of the first generation dongle

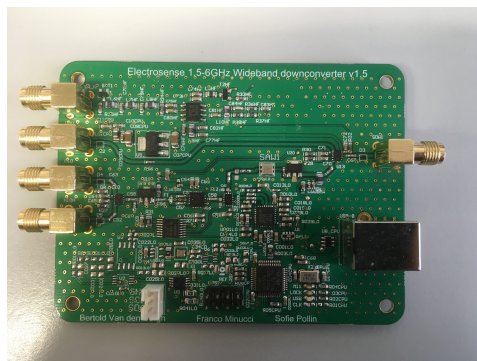


Figure 1. Electrosense expansion board to operate from DC to 6 GHz

from almost DC up to 6 GHz, compared to 24 MHz to 1.7 GHz for the first generation dongles. The expansion board is illustrated in Fig. 1 and it is required for collecting spectrum data in the most significant frequency bands. The up and downconverter board has three possible RF modes, operating at different bands:

- Up-conversion input: 0-30 MHz
- Direct input: 30 MHz-1.6 GHz
- Down-conversion input: 1.6 GHz - 6 GHz

The output of the convertor board has a bandwidth of 20 MHz, even though the RTL-SDR device (used in the typical Electrosense spectrum sensor) only has 2.4 MHz bandwidth. Higher quality SDRs can be used to take advantage of the higher bandwidth. The convertor is controlled by an STM32 ARM based microcontroller, which exchanges data with the Raspberry PI through a USB port. The firmware running on the microcontroller exposes a text based interface. Both the convertor board and the firmware have been tested and calibrated. We have distributed the boards to project members and have started to distribute them to the Electrosense community for deployments. We have released the schematic (<https://github.com/electrosense/hardware>) as open source.

In addition, we have worked on a new version of the software code running in the software-defined spectrum sensor. This new version allows to fetch I/Q data (I/Q pipeline) on demand from the GUI interface at Electrosense. This is the first step for collecting I/Q data for detection and localization using the Electrosense system. The code has been also optimized for efficiently scanning the spectrum, reducing the time to scan the full spectrum by 25%. The code has been also publicly released as open source at <https://github.com/electrosense/es-sensor>. We have also introduced a *decod-*

ing pipeline to allow to decode specific I/Q data directly in the spectrum sensor and provide this data directly to users in order to guarantee low latency, bypassing the backend processing. Currently, this decoded data can be requested by a user in near real time (see also work in Section 3.1.5). In the sensor architecture, we are now able to integrate different pipelines (PSD data, I/Q data, decoding pipeline), and that can be controlled seamlessly to deliver data requested by the backend and by the users.

3.1.2. *Data Quality, Trustworthiness and Obfuscation Techniques*

The work has focused on the investigation of techniques to transform spectrum data (PSD, I/Q) to a less complex space that preserves signal features, and send data in this domain to the backend. The motivation for this study is to limit the amount of network bandwidth needed to operate each spectrum sensor and perform computation extensively in this space. The majority of the work has been conducted to design a framework for analyzing the spectrum characteristics in large spatio-temporal scales. The framework operates in the SVD domains, where it extracts long-lived signal, short-lived signal, signal shape change, energy difference, etc. and it is characterized by high compression ratio, almost no information loss, and high run time efficiency (Zeng et al., 2019). However, the proposed framework still requires a high computational cost and it can work only on powerful embedded devices, we are also investigating different methodologies that can work on embedded boards.

3.1.3. *Detection of Intruders*

Related to intruder or anomaly detection, we have worked on a deep learning framework called SAIFE, an unsupervised wireless spectrum anomaly detection framework with interpretable features (Rajendran et al., 2019). Demanding anomalous behaviour or intruders in wireless spectrum is a demanding task due to the sheer complexity of the electromagnetic spectrum use. Anomalies can take a wide range of forms from the presence of an unwanted signal in a licensed band, to the absence of an expected signal, which makes manual labelling of anomalies difficult and suboptimal. SAIFE is based on an adversarial autoencoder based anomaly detector using PSD data which achieves good anomaly detection and localisation (in the spectrum) in an unsupervised setting. It is able to learn interpretable features such as signal bandwidth, class and center frequency in a semi-supervised fashion. It has been tested on data from one of the distributed Electrosense sensors over a long term of 500 hours showing its anomaly detection capabilities.

3.1.4. *Geo-location of Intruders*

We have worked on the problem of collaborative decoding to decode data from a transmitter of larger bandwidth than the one of the single receiver. In order to circumvent the hardware limitations of single receivers, we envision a scenario where non-coherent receivers sample the signal collaboratively to cover a larger bandwidth than the one of the single receiver and then, enable the signal reconstruction and decoding in the backend. In the work we have proposed and verified with real experiments a methodology to synchronize I/Q samples of multiple non-coherent spectrum sensors. In order to cover a large bandwidth, we suppose there exists only a very limited band in the spectrum where the signals received by multiple sensors overlap in frequency (Calvo-Palomino et al., 2019). The work is an enabler for the investigation of localization techniques, as it allows to study to synchronize I/Q samples in a very challenging application (with very limited amount of information available).

3.1.5. *System Solutions, Integration and Demonstrations*

We have worked on a new architecture (Electrosense+ (Calvo-Palomino et al., 2020)) to give power to the users. We have found that this approach was necessary to provide incentives to users to install sensors, key for a crowdsourcing initiative. The idea has been to introduce the capability of decoding I/Q samples directly in the spectrum sensors, for broadcast and control data (and thus without privacy concerns), and provide this information to users in real time. The work has relied on open source implementations for the decoders, that has been optimized to work with low-cost embedded hardware. Large engineering effort has been done to integrate the proposed solution with the current Electrosense system in order to control the status of the sensor and to manage the signaling server needed by this new approach. In addition, we have integrated WebRTC as tool for direct streaming from the sensor. The system is already operative in test mode and it is currently able to decode FM and AM radio (with audio), Cell ID of LTE base stations, ADS-B, AIS and ACARS (with maps). It will be launched to the community in Fall 2019.

3.2. OTHER DISSEMINATION ACTIVITIES

Project members have also disseminated the results of the project in other activities. The NPD Dr. Giustiniano gave a keynote speech at EAI Crowncom 2018, the International Conference on Cognitive Radio Oriented Wireless Networks, in front of about 60 scientists. This has allowed to give high visibility to the research and the roadmap in Electrosense and SOCRATES. Dr. Giustiniano gave also an invited talk in April 2019, as part of the IEEE 5th

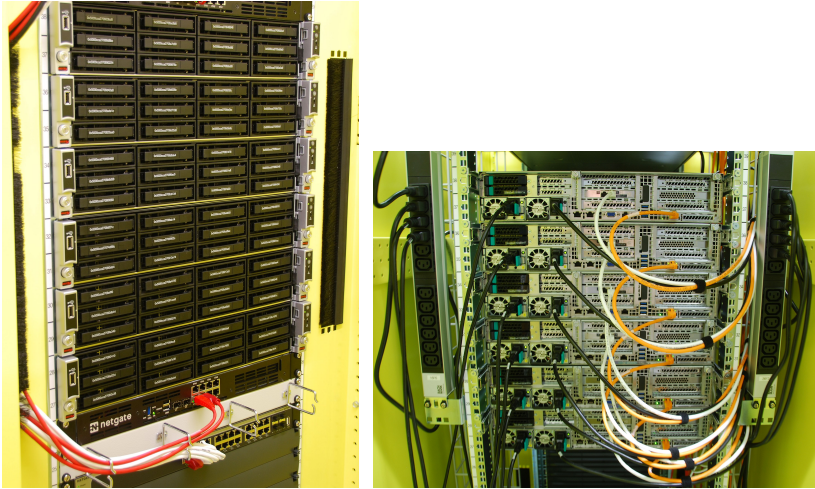


Figure 4. Electrosense servers

World Forum on Internet of Things. Sofie Pollin gave a keynote speech during the workshop on IoT, Big Data & Smart Cities (ITCities' 18, www.itcities.org) in June 2018 in Rabat, and explained how citizen science, and Artificial Intelligence all meet in Electrosense. Furthermore, following the agile approach in the project, we have shown early demonstrators of SOCRATES. In all events, the feedback has been very positive.

The press release of the start of the project has received significant attention from Spanish and international media. We highlight an interview in Spanish from the newspaper *Vozpopuli* and the international outreach in website such as phys.org, a very well know portal for news in science and technology.

4. Deployment

The approach of Electrosense is to use its own backend infrastructure as alternative to cloud services. Doing the processing in the cloud can be very expensive because of the egress costs and data management via public cloud. Furthermore, it forces to trust cloud providers and results in data loss/not more accessible after the end of the project, as leasing of space ends. As processing data for the applications envisioned in the process is a fundamental challenge for a large scale distributed system, Electrosense has upgraded its backend through the funding received in SOCRATES. Fig. 4 shows a picture of the servers acquired by Electrosense within the project. Each server runs 2 x 12 Core Intel Xeon Silver 4116 2.1GHz Processor.

In addition, SOCRATES requires sensors deployed in any location to collect data and train the models. For this reason, budget of the project has been used for making Electrosense sensors available to the community. In particular, part of these sensors operate up to 6 GHz (cf. Section 3.1.1). At the time of writing, we have started the distribution of sensors to interested applicants. Finally, project budget has been used in part to support the deployment of controlled testbeds for experimentation with higher-end software defined radios.

5. Conclusion

In this contribution, we have presented SOCRATES, Large Scale Collaborative Detection and Location of Threats in the Electromagnetic Space, with particular focus on the overall goal of the project and the results achieved in the first year of the project. The three partners of the project largely collaborate in the project, as the Electrosense infrastructure from the partner country Switzerland is used for experimentation. This is also demonstrated by several joint top publications among project partners. In the follow up of the project, we plan to massively deploy our sensors with expansion boards and send them to interested users in populated regions of the world. We also plan to release Electrosense+ to allow users to connect to any sensors and listen to a variety of events. This will provide incentives to users to deploy sensors on their own, further allowing to demonstrate the finding of the project in real conditions. With these new sensors, SOCRATES will be able to test in real life conditions new approaches for detecting and localizing intruders as investigated in the project.

References

- (2019) SOCRATES project, Large Scale Collaborative Detection and Location of Threats in the Electromagnetic Space, Grant G5461, <https://socrates.networks.imdea.org/>.
- Calvo-Palomino, R., Cordobés, H., Ricciato, F., Giustiniano, D., and Lenders, V. (2019) Collaborative Wideband Signal Decoding Using Non-coherent Receivers, In *Proceedings of the 18th International Conference on Information Processing in Sensor Networks*, New York, NY, USA, ACM.
- Calvo-Palomino, R., Cordobés, H., Engel, M., Fuchs, M., Jain, P., Liechti, M., Rajendran, S., Schfer, M., den Bergh, B. V., Pollin, S., Giustiniano, D., and Lenders, V. (2020) Electrosense+: Crowdsourcing radio spectrum decoding using IoT receivers, *Computer Networks* **174**, 107231.
- Rajendran, S., Calvo-Palomino, R., Fuchs, M., den Bergh, B. V., Cordobés, H., Giustiniano, D., Pollin, S., and Lenders, V. (2018) Electrosense: Open and Big Spectrum Data, *IEEE Communications Magazine*.

- Rajendran, S., Meert, W., Lenders, V., and Pollin, S. (2019) Unsupervised Wireless Spectrum Anomaly Detection With Interpretable Features, *IEEE Transactions on Cognitive Communications and Networking* **5**, 637–647.
- Zeng, Y., Chandrasekaran, V., Banerjee, S., and Giustiniano, D. (2019) A Framework for Analyzing Spectrum Characteristics in Large Spatio-temporal Scales, In *Proceedings of the 25th Annual International Conference on Mobile Computing and Networking*, New York, NY, USA, ACM.