REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK
31. évfolyam (2019) 2. szám 67–76. • DOI: 10.32560/rk.2019.2.5

Marek Košuda, Stanislav Szabo jr.

Signals of Opportunity: Using Signal Defined Radios to Identify Potential Candidate

This paper deals with the prospect of using cellular network signals as one of the candidates from the signals of opportunity as a supplementary or alternative source for navigation and positioning via on-board software defined radio. A low cost system for modelling GSM coverage over particular area is proposed.

Keywords: *signals of opportunity, software defined radio, opportunistic navigation*

Introduction

The rapidly growing world market of unmanned aerial systems is only one example of the modern era in which various industries undergo rapid changes due to the advancement of technology. From a historical perspective, the initial period of success of unmanned systems is undoubtedly linked with the defence industry. Today, however, the public sector represents the driving force of innovation due to the precipitously increasing number of privately owned unmanned systems in the sky. In 2017, around 174,000 unmanned systems were sold worldwide for commercial and non-commercial applications representing a 58% increase over the previous year [1]. There are a number of studies and surveys forecasting a market of unmanned systems eventually being worth over $100 billion with more than 3 million active units around the globe [2], [3]. On the other hand, the increment of unmanned systems in the airspace brings a new challenge in the form of unmanned traffic management and unmanned systems' navigation in GPS challenged environments such as deep urban canyons [4], [7]. Additionally, GPS spoofing incidents occur more frequently worldwide questioning the reliability of the GPS as the source for the ever increasing demand for autonomy in the emerging unmanned systems applications [8]. In the recent decade, signals of opportunity (SoPs), which are signals not purposefully designed for navigation or position determination, gathered considerable attention because of a plenitude of sources available in the GPS challenged environment. The exploitation of SoPs demands new methods for signals processing to be developed and implementation of unusual navigational hardware on board of unmanned systems. One of the possible readily accessible hardware solutions is Software Defined Radio (SDR). Analogously to unmanned systems, the beginnings of SDR go back to large-budget military projects a few decades ago and it slowly made its way to its present form of widely accessible device for signal processing [9]. The hardware of the SDR is similar to the traditional radio, except when we get the signal down to the baseband, and it is being sampled by an ADC converter and the components found further down the data stream are replaced by a programmable Digital Signal Processor (DSP).

The paper's objective is to discuss various methods used for non-GPS navigation and positioning, briefly introduces various signals of opportunity and their advantages and disadvantages, and introduces an elementary solution for searching potential SoP candidates in the radio signal environment.

SIGNALS OF OPPORTUNITY

Available signals and opportunistic navigation

Opportunistic navigation (OpNav) is the concept of using signals from an established transmitter infrastructure intended for other purposes, to be used for the localisation platform. The environment of our modern cities is especially abundant with a variety of these signals that can be used for OpNav including GSM, 3G, Digital Audio Broadcast (DAB), Digital Video Broadcast (DVB) and many others. Moreover, many emerging and potential utilisation of unmanned applications are to be deployed in cities at low altitudes, which requires a novel approach in accurate localisation as it represents a critical component for unmanned platforms. Figure 1 portrays the navigational gap occurring at ground level and within city canyons.

There are multiple possible sources of signals, which can be exploited for navigational purposes. Table 1 contains an output from a spectrum analyser depicting a number of opportunistic signal candidates on the airwaves in most of the modern cities ranging in frequency spectrum from 10 MHz to 3 GHz.

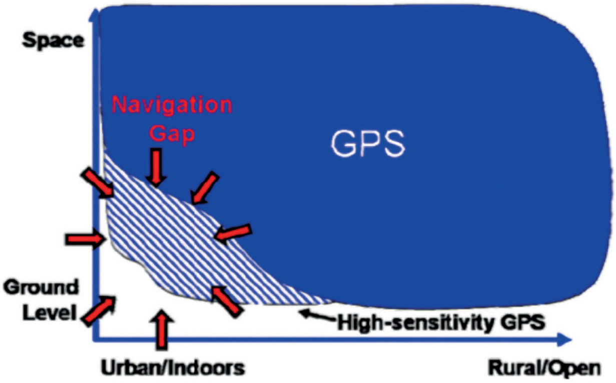

Figure 1.
Navigational gap [10]

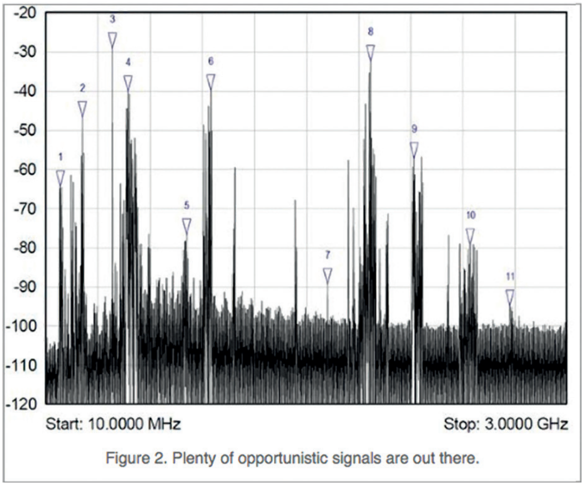

Figure 2.
Output from spectrum analyser showing SoPs [11]

Table 1.
The number of available opportunistic signals [11]

Signal marker	Frequency	Level	Identity
1.	93.72 MHz	–64.36 dBm	FM radio broadcast
2.	219.3 MHz	–46.67 dBm	DAB radio
3.	392.72 MHz	–29.10 dBm	TETRA – long distance navigational system
4.	482.42 MHz	–40.24 dBm	Digital TV
5.	817.3 MHz	–76.67 dBm	LTE band (EUDD band)
6.	954.84 MHz	–39.91 dBm	GSM signal (E-GSM band)
7.	1.6246 GHz	–89.28 dBm	Iridium
8.	1.8698 GHz	–32.37 dBm	GSM (DCS1800 band)
9.	2.1209 GHz	–57.23 dBm	WCDMA (IMT IMT)
10.	2.4439 GHz	–79.22 dBm	Wi-Fi (2.4 GHz band)
11.	2.6711 GHz	–94.81 dBm	LTE (IMT-E band)

Advantages and disadvantages of SoPs

There are multiple advantages in using SoPs for navigation in clutter and challenged environments such as modern cities where a multitude of signals is freely available at any location. The biggest one has an abundance of potential candidates, as depicted in Figure 1. The frequency spectrum of potential signals allows for prospective navigational applications not only in outdoor environment but also within buildings themselves. Another advantage is the transmitting power, for example, GPS satellite transmits 282 Watts of EIRP (Effective Isotropic Radiated Power) from an altitude of 22,000 km, if its directly above the receiver. In comparison to FM transmitters, which transmit 50,000 Watts on average at a distance of 20 km, we have more than 82 dbW/m^2 received power density [10]. This much power at disposal allows for walls and building penetration with further exploitation of signal indoors. In case of SoPs or OpNav, the financial perspective is also attractive because of already existing infrastructure of transmitters broadly spread out around cities.

However, there are several challenges before a successful OpNav can be widely implemented as a viable form of localisation either as a supplementary or sole source of navigational method.

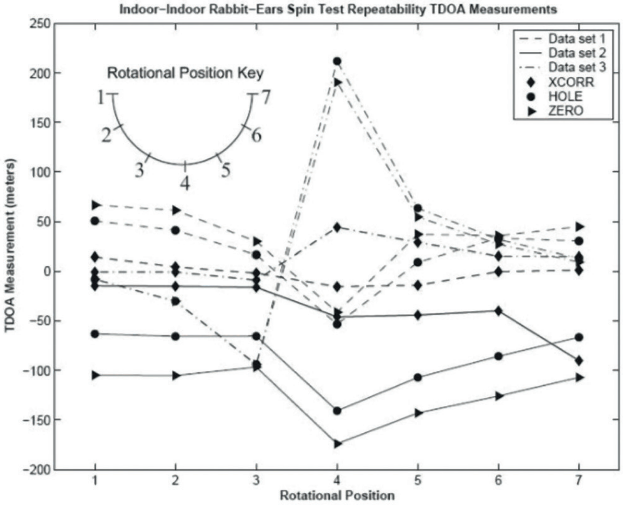

Figure 3.
Variation in analogue television time difference of arrival (TDOA) measurements [13]

- Signals of opportunity are not indented for navigational application and therefore they lack certain characteristics. In comparison to GPS, SoPs do not carry a time information marking the beginning of broadcast, which is important for determining the location. Moreover, transmitter clocks are quite unstable with large drifts in oscillators causing large frequency offsets [12]. In general, most of the communication systems are not time-synchronised to an accuracy of several nanoseconds, which is required in order to navigate without a reference receiver.
- The availability of signals is determined by user location. While there are numerous candidates within cities, very few can be found in more remote areas. But given the possibilities of this paper, we focus on urban environments.
- The most important challenges necessary to overcome are multipath effects and the non-line of sight operations. When considering indoor or clutter urban environment, it is certain that many received radio frequency signals will be reflected or scattered signals rather than direct signals. This presents a crucial problem in the form of corrupted timing data, which are crucial for navigation. A good example of the multipath can be seen in Figure 3, which shows TDOA measurements generated from analogue television in an indoor environment using rabbit ears antennas. Three different data sets were collected at different times but in the same location, and three different TDOA measurement techniques were applied (denoted as XCORR, HOLE and ZERO in the figure). The large variation in TDOA measurements observed

when the antenna was simply rotated is strongly suggestive of a multipath effect, as the gain pattern of antenna changes relative to the environment [13]. However, a multipath effect does not influence only OpNav methods but also other navigation systems in urban environment.

Alternative methods used for Non-GNSS navigation

There are at least three categories encompassing basic alternative methods for Non-GNSS navigation:

- ✈ Image/lidar/Doppler/DR aiding of inertia. These methods are based on inertial system technology, but constrain the drift by incorporating one or more sources of aiding. Examples include image-aided inertial navigation [14] and lidar-aided inertial navigation [15]. These systems are mostly self-contained systems.
- ✈ Beacon-based navigation. Some challenged environments might degrade GNS signals and render them unreliable for navigation. There is a possible solution in the form of transmitting an additional signal or signals that are specifically designed for navigational purposes. However, this solution found its application in an indoor environment for the moment [16], [17].
- ✈ Navigation using signals of opportunity. Signals of opportunity are, as defined in this paper, radio frequency signals that are not intended for navigation. Examples from previous research include AM radio [18] and analogue television [19].

Furthermore, OpNav is a navigation approach heavily depending on sensors and methods used for radio signals processing. In order to determine the user's location, we measure the distance of the transmitter from the sensor receiving signal, the signal's time of travel and the energy of the received signal or the combination of them.

There are two basic methods used for OpNav:

- ✈ Signal propagation modelling. This method is based on computing parameters such as Received Signal Strength Indicator (RSSI), the Angle of Attack (AOA), the Time of Arrival (TOA) and the Time Difference of Arrival (TDOA). In general, this approach implements methods like lateration and angulation. These methods have some drawbacks. In deep urban canyons it is difficult to use a direct line-of-sight channel between the transmitter and the receiver. Moreover, the multipath effect would noticeably degrade accuracy.
- ✈ Signal fingerprinting. It is a popular approach not to use signal propagation geometry, but a signal data based collection which provides high accuracy. This approach demands building a database of Received Signal Strength (RSS) and subsequent coordinates of measurement. Fingerprinting consists of two phases: 'recording' and 'positioning'. During the recording phase, the fingerprint database is created. The database contains real coordinates of reference and related to these signal are the strength values of accessible transmitters. The positioning phase measures accessible radio signals and searches matches in the database of the nearest point to the receiver using an appropriate search/match algorithm. However, there are drawbacks in the training

because it requires a vast number of RSS measurements and some signals might be unstable causing changes in the primary radio map.

Potential candidate – GSM

Over the last 15 years several wireless standards have been introduced into the cellular market and each geographical region has developed a set of radio access technologies based on Global System Mobile (GSM) and Code Division Multiple Access (CDMA) because of specific regional frequency allocation and policies.

The GSM, also known as second-generation (2G) networks, represents a crucial step in the introduction of mobile voice services. This led to a worldwide spread of devices that can be used seamlessly across different geographical regions. One of the key characteristics why the GSM represents a potential candidate is its narrow bandwidth relative to other widely used wireless standards. The GSM occupies a frequency channel of only 200 kHz. We must mention that emerging new technologies bring larger bandwidths and that presents a problem for Software Defined Radios as the required hardware becomes more complex in order to capture them. Moreover, another limitation is due to the constrained interface connecting the SDR to the computer. More bandwidth directly translates into more cost in terms of transfer rates, processing power and money. By and large, aiming for mobility puts a limit on size, weight and power consumption [21].

Basic GSM specifications

The full GSM specifications would be too excessive for this paper and therefore, we briefly discuss the relevant parts.

GSM is a multiple access technology allowing users to cram multiple phone calls or Internet connections into one radio channel. The frequency bands are divided into multiple channels so that more than one user can place a call through the tower at the same time. The GSM utilises a combination of Time, Space and Frequency Division Multiple Access techniques (TDMA, SDMA and FDMA).

The 900 or 1800 MHz band is separated to 200 kHz channels (FDMA). The Base Transceiver Stations (BTS) are given these frequencies in a way that adjacent cells do not use the same frequency in order to avoid interference. This ensures SDMA. Lastly, each 200 kHz carrier is split in time into 8 slots. This is illustrated in Figure 1.

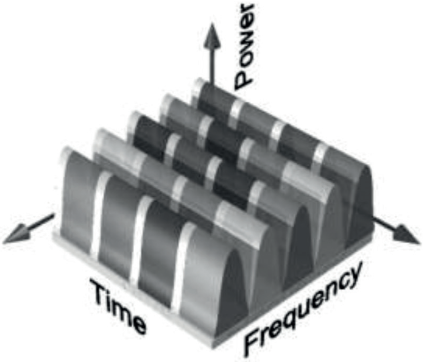

Figure 4.
The combination of TDMA and FDMA [20]

Proposed system

There are multiple projects with greater and more advanced capabilities, however, the aim of this proposed system is to showcase low-cost solution based on open-source and open-hardware.

We further propose the implementation of the proposed system, which is light weight and power efficient, on board of unmanned vehicle supporting MAV link protocol.

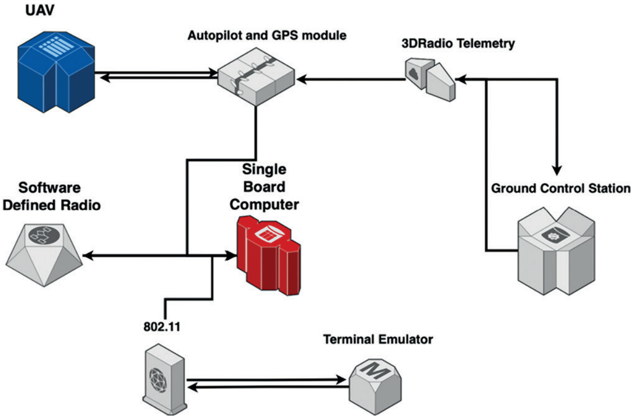

Figure 5.
Proposed system structure [compiled by the authors]

Hardware

The hardware encompasses three major components. At the core of the system is a single board computer acting as a data sink for the other components. It also performs signal processing of the captured samples and logs the results that we are interested in. The other parts include SDR and flight management unit (FMU). SDR tunes in to the desired frequencies of the RF spectrum and outputs a sampled signal ready to be processed by the single board computer. FMU controls UAV and it also feeds the position data to the SDR. The terminal emulator talks with the single board computer and the ground station supervises FMU.

Further discussion on the system

We propose to use GNURadio as the main software tool for radio data processing. However, most of the low cost single board computers do not come with enough space for its installation. It could be bypassed by GNURadio installation on an external SD card.

As mentioned above, low cost SDR are not equipped with accurate clocks. Furthermore, the frequency error is not constant and it is highly dependable on environmental factors. There is a possible solution in a synchronisation with GPS in a more expensive SDR hardware. Additionally, the mobile stations in a cellular network face the same problem. The GSM built in a solution for this problem in the form of very tight requirements for frequency synchronisation. To overcome potential frequency mismatch for reliable timing acquisition, GSM has a logical channel dedicated to solving the problem. It is called the Frequency Correction Channel or FCCH [21]. While the GSM clearly outlines the FCCH, the detection method of frequency bursts is up to the SDR manufacturer. We propose to implement an algorithm developed in [22], which might require a few adaptations. The detection method uses an adaptive line enhancer (ALE) to identify frequency bursts. Timeslots are left unused when there are no users to utilise them. However, when a transmission occurs, the slot is filled with a burst. There are many types of bursts as a result of the long history of these technologies and amendments to keep it up to date. It is up to the user, which burst is to be detected.

Conclusion

In this paper we briefly discussed the emerging form of opportunistic navigation and signals, that could be exploited for localisation purposes. Despite the benefits of non-GNSS based navigation in a clutter urban environment, there are certain drawbacks to overcome. With the mentioned approaches used in OpNav ranging from a self-contained system such as Lidar, we see a greater benefit and wider applications in focusing on systems that interact with abundant signals in radio frequency environment. The paper proposed a system that could create a map of GSM network coverage for a particular area with a prospect for more detailed analysis of the RF environment, which could be used for the fingerprinting method used in OpNav.

References

[1] The Economist, “Commercial drones are the fastest-growing part of the market,” *The Economist,* June 8, 2017. [Online]. Available: www.economist.com/technology-quarterly/2017/06/08/commercial-drones-are-the-fastest-growing-part-of-the-market

[2] Goldman Sachs, "Drones: Reporting for work," *Goldman Sachs,* [Online]. Available: www.goldmansachs.com/insights/technology-driving-innovation/drones/

[3] Intelligence, Business Insider, "How Drones Will Change the World in the next 5 Years," *Business Insider,* 25 September 2017. [Online]. Available: http: //globalproductreview.com/how-drones-will-change-the-world-in-the-next-5-years-business-insider/

[4] A. Soloviev, J. Dickman, "Extending GPS phase availability indoors with a deeply integrated receiver architecture," *IEEE Wireless Communication,* vol. 18, no. 2, pp. 36–44, 2011. DOI: https: //doi.org/10.1109/mwc.2011.5751294

[5] E. Costa, "Simulation of the effects of different urban environments on GPS performance using digital elevation models and building databases," *IEEE Transactions on Intelligent Transportation Systems,* vol. 12, no. 3, pp. 819–829, 2011. DOI: https: //doi.org/10.1109/tits.2011.2122258

[6] J. C. Grabowski, "Personal Privacy Jammers: Locating Jersey PPDs Jamming GBAS Safety-of-Life Signals," *GPS World,* 1 April 2012, [Online]. Available: www.gpsworld.com/personal-privacy-jammers-12837/

[7] Ch. Günther, "A survey of spoofing and counter-measures," *Navigation,* vol. 61, no. 3, pp. 159–177, 2014. DOI: https: //doi.org/10.1002/navi.65

[8] J. Spicer, A. Perkins, L. Dressel, M. James, Y.-H. Chen, Sh. Lo, D. S. De Lorenzo, and P. Enge, "Jammer Hunting with a UAV," *GPS World,* 4 May 2015. [Online]. Available: www.gpsworld.com/jammer-hunting-with-a-uav/

[9] "Defining Next Generation Radio with SDR," Army-technology.com, 12. August, 2010. [Online]. Available: www.army-technology.com/features/feature92744/

[10] M. M. Miller, A. Soloviev, M. U. de Haag, and M. Veth, "Navigation in GPS Denied Environments: Feature-Aided Inertial Systems," *RTO-EN-SET-116(2011)* [Online]. Available: https: //pdfs.semanticscholar.org/f031/46a66a5d60b60da517d5dd28da934a65a22e.pdf

[11] M. Jones, "Signals of Opportunity: Holy Grail or a Waste of Time?" *GPS World,* 22 February 2018. [Online]. Available: www.gpsworld.com/signals-of-opportunity-holy-grail-or-a-waste-of-time/

[12] C. Yan, H. H. Fan, "Asynchronous Differential TDOA for Non-GPS Navigation Using Signals of Opportunity," In Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, 2008, pp. 5312–5315. DOI: https: //doi.org/10.1109/icassp.2008.4518859

[13] R. J. Eggert, J. F. Raquet, "Evaluating the Navigation Potential of the NTSC Analog Television Broadcast Signal," In Proceedings of the 17th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2004), Long Beach, CA, 2004, pp. 2436–2446.

[14] M. Veth, J. Raquet, "Fusion of Low-Cost Imaging and Inertial Sensors for Navigation," In Proceedings of the 19th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2006), Fort Worth, TX, 2006, pp. 1093–1103.

[15] J. Campbell, M. Miller, M. Uijt de Haag, D. Venable, and M. Smearcheck, "Flash-LADAR Inertial Navigator Aiding," In Proceedings of IEEE/ION PLANS, San Diego, CA, 2006, pp. 677–683. DOI: https://doi.org/10.1109/PLANS.2006.1650661

[16] J. Barnes, Ch. Rizos, M. Kanli, D. Small, G. Voigt, N. Gambale, J. Lamance, T. Nunan, and Ch. Reid, "Indoor Industrial Machine Guidance Using *Locata:* A Pilot Study at BlueScope Steel," In Proceedings of ION Annual Meeting 2004, pp. 533–540.

[17] G. Opshaug, P. Enge, "GPS and UWB for Indoor Positioning," In Proceedings of ION GPS, Salt Lake City, UT, 2001, pp. 1427–1433. DOI: https://doi.org/10.1109/ICICS.2007.4449630

[18] T. Hall, C. Counselman III, and P. Misra, "Radiolocation Using AM Broadcast Signals: Positioning Performance," In Proceedings of ION GPS, Portland, OR, 2002.

[19] R. Eggert, J. Raquet, "Evaluating the Navigation Potential of the NTSC Analog Television Broadcast Signals," In Proceedings of ION GNSS, Long Beach, CA, 2004, pp. 2436–2446.

[20] "SkyDSP," skydsp.com, [Online]. Available: www.skydsp.com/publications/4thyrthesis/chapter1.htm

[21] T. Volčko, V. Moucha, P. Lipovsky, and K. Draganova, "Possibility of usage the latest GSM generations for the purpose of UAV communication," In Proc. New Trends in Signal Processing, 2016, pp. 102–105. DOI: https: //doi.org/10.1109/ntsp.2016.7747794

[22] G. N. Varma, U. Sahu, G. P. Charan, "Robust Frequency Burst Detection Algorithm for GSM/GPRS," In Proc. IEEE 60th Vehicular Technology Conference, 2004. DOI: https: //doi.org/10.1109/vetecf.2004.1404796

Further reading

P. Bahl, V. N. Padmanabhan, "RADAR: An In-Building RF-Based User Location and Tracking system," In Proceedings of IEEE Infocom, Tel Aviv, 2000. DOI: https://doi.org/10.1109/INFCOM.2000.832252

KISEGÍTŐ JELEK: SZOFTVERRÁDIÓ ALKALMAZÁSA A LEHETSÉGES JELFORRÁSOK MEGHATÁROZÁSÁRA

Ez a tanulmány bemutatja, hogy lehet a mobilhálózatot – mint alternatív, kiegészítő navigációs lehetőséget – szoftverrádiókkal ellenőrizni. A javasolt alacsony költségű rendszer a GSM-lefedettséget modellezi egy adott területen.

Kulcsszavak: *kisegítő jelek, szoftverrádió, kisegítő navigáció*

M. Eng. Ing. Marek Košuda
Educational Technician, Doctoral Student
Technical University in Košice, Slovakia
Faculty of Aeronautics
Department of Aviation Technical Studies
marek.kosuda@tuke.sk
https://orcid.org/0000-0002-4179-4738

Ing. Bc. Stanislav Szabo, jr. MBA
Research Worker, Doctoral Student
Technical University in Košice, Slovakia
Faculty of Aeronautics
Department of Air Transport Management
stano.szabo@tuke.sk
https://orcid.org/0000-0003-2403-2288

http://journals.uni-nke.hu/index.php/reptudkoz/article/view/270/167