TECHNICAL UNIVERSITY OF LIBEREC
Faculty of Mechatronics, Informatics
and Interdisciplinary Studies

# Methods of Improving Wireless Communication in Home Automation and Security

## Dissertation thesis summary

| | |
|---|---|
| *Study programme:* | P2612 – Electrical Engineering and Informatics |
| *Study branch:* | 2612V045 – Technical Cybernetics |
| *Author:* | **Ing. Tomáš Jakubík, M.Eng.** |
| *Supervisor:* | Ing. Jiří Jeníček, Ph.D. |

Liberec 2022

# Methods of Improving Wireless Communication in Home Automation and Security

## Abstrakt

Tato práce představuje možnosti vylepšení bezdrátové komunikace pro systémy domácí automatizace a zabezpečení. Většina dnešních systémů používá jednofrekvenční komunikaci. Přidání frekvenčního skákání zvyšuje odolnost proti rušení, ale přináší problémy s výdrží baterie nebo s rychlostí odezvy, které nejsou v této třídě elektroniky jednoduše řešitelné.

První metoda představená v této práci je vícekanálový přijímač pro centrální jednotku. To umožňuje senzorům spát a po probuzení neřešit synchronizaci se sítí.

Druhá metoda je kombinace vícekanálového přijímače s komunikací bezdrátových kamer. Komunikace senzorů se skryje do přenosu obrazu bez přidání dalšího rádia.

## Abstract

This thesis presents methods of improving wireless communication in home automation and security. Most current systems use single-frequency communication. Frequency hopping improves resistivity to interference but brings problems with battery lifespan or communication delay, which cannot be simply solved in this class of electronics.

The first method proposed in this work is an all-channel receiver for the central unit. It allows the sensors to sleep and avoid lengthy network synchronization after wakeup.

The second method is a combination of the all-channel receiver with a communication of wireless cameras. The sensor communication is hidden in video transfer without additional hardware.

## Keywords

frequency hopping, frequency agility, OFDM,
home automation, security system, sensor network

# Contents

# 1 Introduction

Home automation and security is a specific area of consumer electronics. A security system usually consists of a Central Unit (CU) and many independent devices which need to be small and cheap. There are Passive Infrared (PIR) sensors, magnetic door contacts, smoke detectors, key fobs, smart light switches and many more. All can be connected to the CU via a wired bus or wireless network. This thesis is focused only on wireless communication.

Wireless communication in the area of home automation and security is advancing much slower than in other areas of consumer electronics. There are several difficulties [1] that don't allow quickly reusing foreign ideas. Requirements of very low energy consumption, short communication delay and relatively long range stand against each other. Current wireless networks are not usable in home automation and security for various reasons:

- Modern industrial technologies are several orders of magnitude faster than what is needed, but cannot be powered by batteries [2].
- Modern consumer technologies have high bandwidth and a nearly acceptable delay, but still consume too much current [3].
- Modern IoT technologies can live a long time on a small battery [4], but the delay before the information gets processed is neither usable for automation nor for security systems.

The hardware used in this area has improved over the past decade, but it barely matched the increasing requirements of security. CR2032 battery remains to be a very limited reservoir of energy. Security, on the other hand, has seen constant development in attacks and countermeasures. Older garage door remotes used static codes and can be easily opened by the de Bruijn sequence in 8 seconds [36]. Some manufacturers sell these even today, but it should be avoided if possible. The only viable solution today is AES, possibly improved by an asymmetric key exchange. The cheap and small devices need enough power for computing and more complicated exchange of packets. There is very little space for improvements in modulation and communication techniques.

A common solution nowadays is still a single-frequency network that is susceptible to interference and doesn't efficiently use the available spectrum. The purpose of this work is to design and verify new methods which would allow new communication techniques, with emphasis on frequency agility, while satisfying the requirements for this area of electronics.

# 2 Goals

The main goal of the thesis is to present ways to improve wireless communication in home automation and security. The improvements need to satisfy both technical needs such as latency, power, datarate, range, or size of the devices as well as financial limits. There might be a more elegant solution, but if it would increase the price of a sensor by an order of magnitude, it is not viable. If Moore's law should hold, we can discuss at least those solutions which will probably drop into the available budget in a foreseeable future.

## 2.1 Example Situation

The example situation is a small house with one larger CU and many small low-power sensors. Sensors can be magnetic contacts guarding closed doors, PIR detectors for person movement, acoustic glass-break detectors, flooding detectors, smoke detectors, light switches and many more. The CU is powered by mains at all times and has a large backup battery in case there is a power outage or in case the power connection is intentionally cut. The size of the CU's battery is designed to keep the system running only for a few days, sometimes even only hours. On the other side of communication are sensors that need to survive many years on a small battery. The delay between triggering any sensor and information being available in the CU needs to be at most a fraction of a second.

At least one device in the network is usually the keypad. This device does not communicate directly with the sensors but allows the user a normal day-to-day operation of the system. The user interface can be composed of several kB of texts. That puts more constraints on the available network datarate. The latency of the user interface should be a fraction of a second, similar to the sensors. A keypad can usually hide a somewhat larger battery in exchange for output functionality.

Another output device is a siren. An outdoor siren needs a considerably larger battery to be able to drive the $100\,\mathrm{dB}$ piezo element even when the outside temperature is $-20\,^{\circ}\mathrm{C}$. The output devices are usually time synchronized with the CU to periodically open receiving windows. When the device is synchronized, it requires only a time-frequency chart to add pseudorandom frequency switching. It makes most of this thesis not applicable to this class of devices, but even synchronous devices can use the ability to randomly switch frequencies at will. Either way, it adds more constraints on compatibility with the rest of the wireless devices.

The network needs to reach over a small family house. Having routing between sensors is not practical for various reasons. On one side, the network is set up in advance and most of the devices do not move. That would allow storing paths and time synchronization of an optimal tree network permanently in all devices. On the other side, all devices would have to open their receiving windows at a precise time. Using only devices with a larger battery for routing would not bring many benefits as most devices have small batteries. The need to synchronize all devices will increase power consumption and latency. On top of that, there would be retransmissions discharging unevenly the devices near CU.

Routing or a mesh network would be a viable option in home automation, where there are a lot of output devices connected to the mains supply and the user can quickly replace the batteries of the rest. The preferred way for a security system is to cover the entire house with one or at most a few radio hubs. These radio hubs can be connected to the CU by a high speed wired bus or they can be directly embedded inside of the CU. In the scope of this text, the CU is synonymous with the radio hub and the connection between them is neglected.

Modern systems can also optionally provide visual verification. When an intrusion is detected, the system makes one or more pictures of the situation. A homeowner or the security agency gets a picture and can decide whether the situation is a real threat (eg. burglar) or a false alarm (eg. misbehaving pet). Even though there are such products available, transmitting pictures over the sensor network is not a viable solution. It takes a minute to carry a $640 \times 480$ pixel low resolution picture [37]. In a model situation, a person entering the building will be gradually triggering low-power sensors while the cameras start transmitting video. The low-power sensor network has to work together with the high-bandwidth link of the cameras and not interfere. The needs of the sensor network are almost the opposite of the needs of the camera.

Security cameras require a lot more power, so it is common to use Power Over Ethernet (POE) or a wireless connection with a power adapter and a small battery for backup. It is a part of the security system, so it needs tampering detection and connection to the secure network, even if there already is Wi-Fi for video. Having two radios is more complicated, expensive and adds interference. In particular, interference between Orthogonal Frequency Division Multiplex (OFDM) and frequency hopping is known for Bluetooth and Wi-Fi [5].

## 2.2 Parameters

Depending on the context, simpler contemporary home security sensors can live for over two years on a single CR2032 coin cell battery [38]. The context, in this case, is to comply with grade 2 of EN 50131 [39]. To arm the system, the latest message from the sensor needs to be 20 minutes old or newer. The sensor needs to periodically transmit and receive. The CR2032 battery has a capacity of around 220 mAh which over 2 years gives continuous current of 13 µA or average power of 31 µW. Part of this current is consumed all the time by the sleeping MCU and radio, part of the current is needed to keep the actual sensor running and very little current is remaining for wireless communication. Common Gaussian Frequency Shift Keying (GFSK) transceivers consume more than 10 mA when active [40]–[42], which translates to only a small amount of short packets in either direction.

Another important constraint is the delay between triggering the sensor and a reaction in the CU. A light switch needs to turn the lights on in a fraction of a second. A smoke detector cannot have any unnecessary delay when a fire is detected. Some wireless technologies take time to get from a sleeping state to a ready state in which information can be passed over. This is especially true for frequency hopping networks which need to synchronize before sending any information. Other wireless technologies are intentionally designed for applications that are not time critical. The device can transmit at any time, but it gets an acknowledgment after a second or not at all. In our case, the wireless hub should be able to immediately verify and acknowledge the message. If any message gets lost, the device needs to quickly repeat the important information. There cannot be any exchange of packets negotiating parameters of the communication.

Communication from sensors to the CU needs to work over an area of a one-family home. Datasheet values can be a few hundred meters in an open area [38] and in reality even more. The range is one of the significant reasons for using the sub-GHz frequencies in these systems. The range is much shorter when considering multipath propagation and other effects present in buildings. That is the main reason for trying to bring principles of frequency agility and hopping into this area [6]. Another reason is the cohabitation of multiple systems from the same manufacturer. In especially bad conditions, two systems will be far enough that they will not detect each other by their Clear Channel Assessment (CCA) tools, but they will add too much interference to each other's messages. The problem can be worse if both systems use the same timing principles. Using many frequency channels for hopping will significantly reduce the risk of collision in these situations.

The security system is composed of one larger CU and many small sensors. The price of these sensors can add up quickly to an amount comparable to other household reconstruction works. The price of sensors is an important aspect, so the system is affordable to many potential customers. Sensors should also be hidden or have a fashionable design that forbids adding any large hardware or antennas. The cost of the CU is important as well, but the increase is not multiplied by the number of sensors, so a larger increase can be tolerated. The CU has also much faster MCU, sometimes even running Linux, which could handle some computation of the radio.

# 3 Results

## 3.1 Affordable All-channel Receiver

The first idea of improving communication in a security system is similar to the LoRaWAN Long Range FHSS (LR-FHSS) setup. A specialized receiver could be added to the system CU, where there is enough room for a slight price increase. This solution doesn't take into consideration the high bandwidth cameras which are requested for some security systems.

The main problem of the frequency agile or hopping network is sleeping sensors which need to quickly connect to the hopping communication. The sensor is sleeping long enough to lose synchronization. It doesn't have information about time and channel mapping and cannot easily Tx to CU. Basic frequency agility could be solved by scanning multiple channels or by having more physical receivers, but it is limited to a few and not tens of channels.

A Software Defined Radio (SDR) receiver was created which is able to listen on all channels of the sensor network. The core of the receiver is a $64$-sample FFT which produces two samples per a Gaussian Minimal Shift Keying (GMSK) symbol for every channel. A change of phase in the FFT output is used to decide on each GMSK symbol. First, the receiver was prototyped and simulated in Matlab Simulink. This model was also tested on RTL-SDR. Then the receiver was ported to LPC4370 and R820T2, a three-core Cortex-M MCU with a demodulator chip from DVB-T.

Figure 3.1 shows Packet Error Rate (PER) of both receivers depending on the used channel. The receiver in Matlab Simulink was tested at a distance where a hardware GMSK transceiver stopped receiving. It showed that the SDR receiver has at least the same performance if it is not better. The drop at low channels may have been caused by demodulator filter settings, but it was not explained as Matlab sources are closed. In each test, over $20 \cdot 10^3$ packets were sent. The resulting PER without the first $3$ channels is $3 \cdot 10^{-2}$. Test at a shorter distance didn't show the issue and had PER of $2 \cdot 10^{-4}$.

For the MCU receiver, both receiver and transmitter were in the same room, about $1\,\mathrm{m}$ apart and about $30\,\mathrm{cm}$ from any obstacle. An unusually small distance was selected because the receiver can successfully work only in a range of one room. The drop around channel $51$ was expected. The downconversion process in the demodulator flips the frequency spectrum and its high pass image filter cuts approximately $500\,\mathrm{kHz}$ [54] which approximates $13$ channels. It

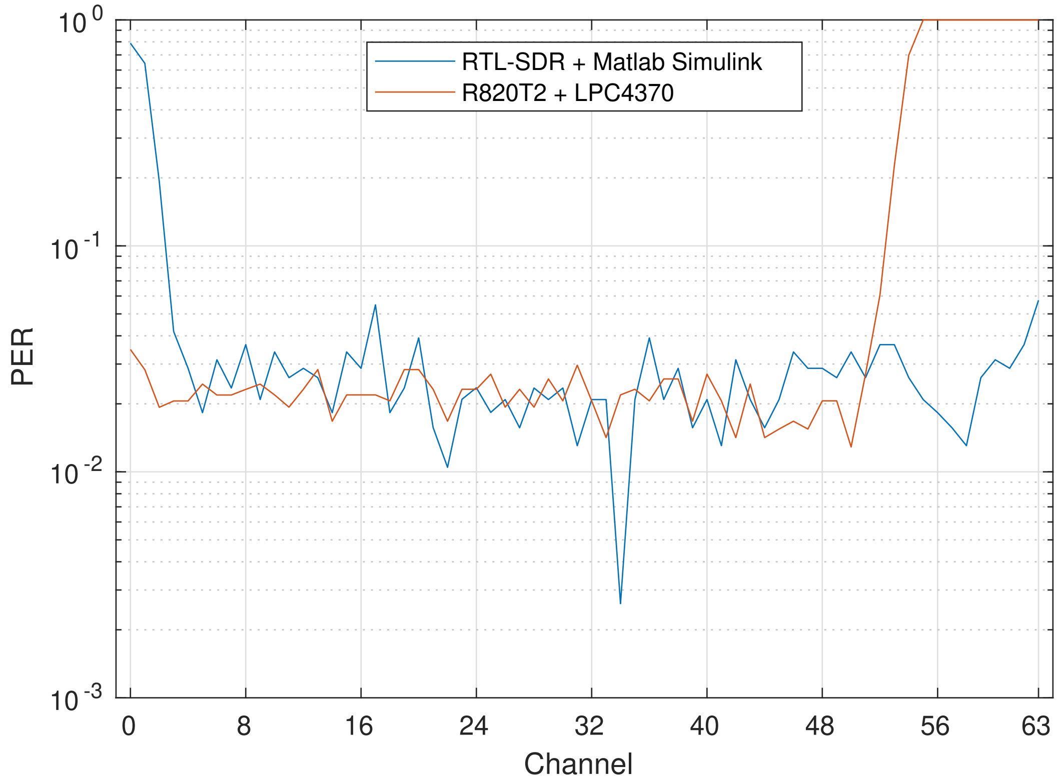

Figure 3.1: Channel Statistics

is the downside of the FFT simplifications necessary to fit the receiver inside an MCU. When only channels $0$ to $51$ are considered, PER was $2 \cdot 10^{-2}$.

The range of the MCU receiver is very limited. There may be several reasons for this insufficient range. It may be caused by the antenna which was not impedance fitted to the demodulator input. RF optimization would be a long and expensive process but have little to no effect on the goals of this prototype. It may also be caused by improper matching of the differential IF pair between the demodulator and the ADC. It would need proper documentation from the manufacturers of both chips. The last reason could be any of the many simplifications necessary for the low computational power of the MCU.

There was a very large number of packets received additionally on a different than the original channel. From previous experiments, we know that the receiver architecture is often able to receive a deformed signal that leaks to a neighboring FFT frequency. It would point to a possible problem in clipping with a signal that is too strong. Yet, a distance of several meters is enough for the receiver to stop working. Both problems may be linked together.

## 3.2 Proof of Concept Sensor

A proof of concept sensor was made to verify what consumption is possible for a network built from the all-channel receiver. Sensor hardware and firmware

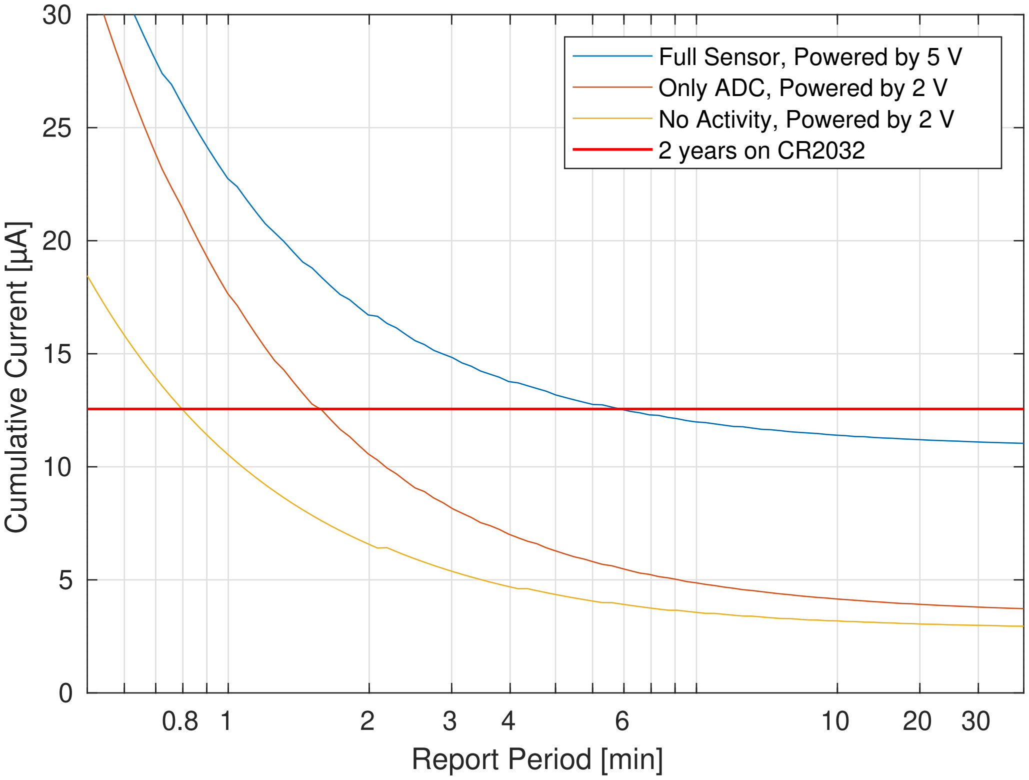

Figure 3.2: Sensor Cumulative Current Consumption

were made to measure a concentration of dangerous gases in intervals of either one minute or one second and to report to CU when it gathers 26 values. Additionally to that, there is an analog trigger and the sensor reports immediately if the concentration reaches a given threshold. It could be used as an additional layer of protection for a factory. The CU was based on a C++ GMSK all-channel receiver running on a PC with LimeSDR Mini which was prepared for the Section 3.3. This shows that it is possible to construct a sensor powered by CR2032 which uses a random transmit frequency. Figure 3.2 shows expected sensor consumption depending on the reporting period.

The full $NO_2$ gas sensor was powered by 5 V necessary for the gas concentration measurement. It corresponds to two CR2032 batteries in the middle of their life. The sensor was reporting to CU once every 26 minutes and was consuming a cumulative current of 11.2 μA.

The same sensor was reporting to CU once every 26 seconds and was consuming 48.7 μA. This is too much for coin cell batteries but could work as a more powerful sensor powered by four AAA batteries.

A generic sensor without a switching power supply and a frontend for gas concentration measurement was powered by 2 V. The ADC measurement timing was the same, but it represents a generic analog sensor running from a single CR2032. The sensor was consuming 4.1 μA.

The last version is a generic sensor without any periodic measurement. It represents a sensor that is only guarding a digital input or the analog trigger. It only needs to report to CU that it still exists. Its consumption was 3.1 µA.

## 3.3 Mixed Network with GMSK and OFDM

A more advanced solution for the problems of frequency agile sensors might be to use the high bandwidth radio of the camera link as the all-channel receiver. The cameras have complex OFDM receivers which have a similar construction as the SDRs used above. This solution will require a larger investment into development and hardware than the previous option.

The solution is to make holes into the regular Phase Shift Keying (PSK) OFDM signal by zeroing several neighboring tones. The sensor will start transmitting as soon as one OFDM packet ends and the OFDM radio needs to detect that and create a hole in the next packet to not disrupt the sensor. It can be received directly in the CU or one of the cameras and routed via the OFDM link. This allows the sensor communication with minimal loss of the OFDM datarate. It could be beneficial in the model situation when cameras and sensors need to transmit at the same time.

Getting the information to the CU is the important part, but the sensor needs to receive an acknowledgment, so it can go back to sleep to save power. The CU or a designated router will immediately respond on the same frequency with acknowledgment and allow the sleep mode. This can also be used to give the sensor updated information about the network and perhaps to synchronize the sensor into a frequency hopping plan.

Matlab simulation was created to learn how hole size, signal power and FFT size influence Bit Error Rate (BER). It showed that the concept is possible, but allows only a small variation of power between the two modulations. A real network would require dynamically setting the Tx power.

The next step was to implement a prototype network and test the concept on real hardware. A GMSK all-channel receiver uses the same concept as the receiver on RTL-SDR but runs at a higher sample rate. Response to the sensor is created with the liquid DSP library and modulated to the correct frequency channel. The OFDM transmitter and receiver were modified from liquid `ofdmframegen` and `ofdmframesync`. The original receiver had problems with holes in the signal as it expected correct tones and was estimating the channel on random noise. An additional symbol was added to the packet header to detect up to two holes, correctly synchronize and estimate the channel. The modified transmitter and receiver was compared to the original in a C++ simulation. The modifications shouldn't have any impact on OFDM receiving.

All these receivers and transmitters were used to create C++ software for the camera and the CU. The camera is based on Raspberry Pi and CU on PC, both with LimeSDR Mini as the SDR hardware. The video data are put raw as quadrature PSK to the OFDM packet to completely fill the available

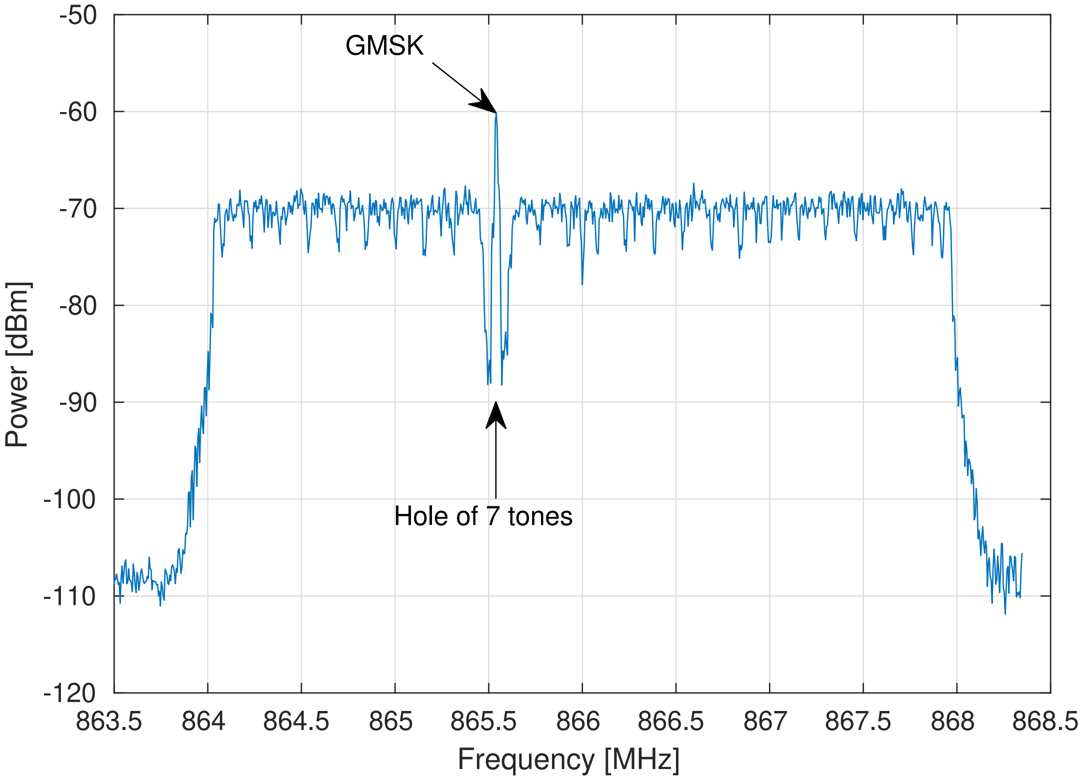

Figure 3.3: The Spectrum of OFDM with Hole and GMSK

datarate. Output data are shown on the PC screen together with statistics and utilities for testing. The GMSK sensor uses the same hardware as the gas sensor, but its firmware and communication were very simplified to ease development and testing. All devices were connected by 50-$\Omega$ cables and their Tx power was manually configured.

One OFDM packet with the delay between two packets totals approximately $18\,\mathrm{ms}$. One packet adds $7$ lines of a picture which results in one frame of raw video in $1.1\,\mathrm{s}$. It can also be converted to a datarate of $618\,\mathrm{KiB/s}$ or $5.1\,\mathrm{Mbit/s}$. The same numbers were also observed by counting the received data in CU. This datarate is without holes which will remove $6$ or $7 \times 64$ B from each packet, depending on pilot positions.

Some GMSK packets were also sent on channels that are in the OFDM guard bands. The real network doesn't have to use these GMSK channels or use them only for key fobs and other mobile devices. That would circumvent the problem with configuring the Tx power of mobile devices.

Figure 3.3 was measured with Resolution Bandwidth (RBW) of $5\,\mathrm{kHz}$. It shows the sensor GMSK signal inside a hole in the OFDM. Pilot tones modulated by binary PSK and the DC spike make small dimples in the spectrum.

Error rates were measured with the power of both signals as set manually during the development. It is the case of GMSK power set to $-23\,\mathrm{dBm}$.

The sensor transmitted one GMSK packet approximately once on every third OFDM packet, so only $1/3$ of the OFDM was affected by the GMSK.

- When only the OFDM was running, no packet out of $32962$ was lost. Out of more than $358$ MiB, only $2583$ bits were received wrong ($0.9 \cdot 10^{-6}$).
- When only the GMSK was running, no packet was lost out of $12549$ sent. Out of almost $221$ KiB, not a single bit was received wrong.
- OFDM with holes filled with GMSK has worse parameters.
  - None out of $32976$ OFDM packets was lost (few usually do), and $6893$ bits were wrong out of $355$ MiB ($2 \cdot 10^{-6}$).
  - $2268$ out of $11523$ GMSK packets were lost ($0.2$) and $14\,778$ bits were wrong out of $163$ KiB ($10^{-2}$).
- Without holes in the OFDM, the communication is unreliable.
  - $749$ out of $32976$ OFDM packets were lost ($2 \cdot 10^{-2}$) and $0.1$ out of $350$ MiB were wrong ($4 \cdot 10^{-4}$).
  - The GMSK communication wasn't usable at all and the CU software wasn't able to track the Tx packet counter to count lost packets.

These numbers show that the situation does favor the OFDM. The GMSK connection would be usable, but with drawbacks. In a low-power device, the frequent packet repetitions would increase its current consumption. The last test shows that if the OFDM link does not provide holes for the GMSK, the communication suffers a lot. Both PER and BER of the OFDM drop at least two more orders of magnitude. It also shows that it should be beneficial to be polite even if the GMSK communication is not a part of the same network. European norms do not require the use of CCA if the duty cycle is limited, but waiting or making holes should be preferred.

Figures 3.4 and 3.5 show how PER and BER change when the power of the GMSK signal is varied. The drop of OFDM BER at the right edge of the figure is probably a quirk of the test as the inaccuracy of BER rises with high PER and less data received. The optimum of BER would be for GMSK power above $-16$ dBm, a little higher than the value manually selected during development. PER of the GMSK signal stays unreasonable high even with increasing power.

It seems that the hole should be larger than the selected $7$ tones. A hole of $11$ tones would carry approximately $4/178 \approx 2\%$ less data but would improve the interference. More tests showed that although BER is improved with a larger hole, PER stayed almost constant for both OFDM and GMSK. Perhaps the bad PER of GMSK (over $4 \cdot 10^{-2}$) is not caused by interference of the signals but by saturation of the SDR receiver.

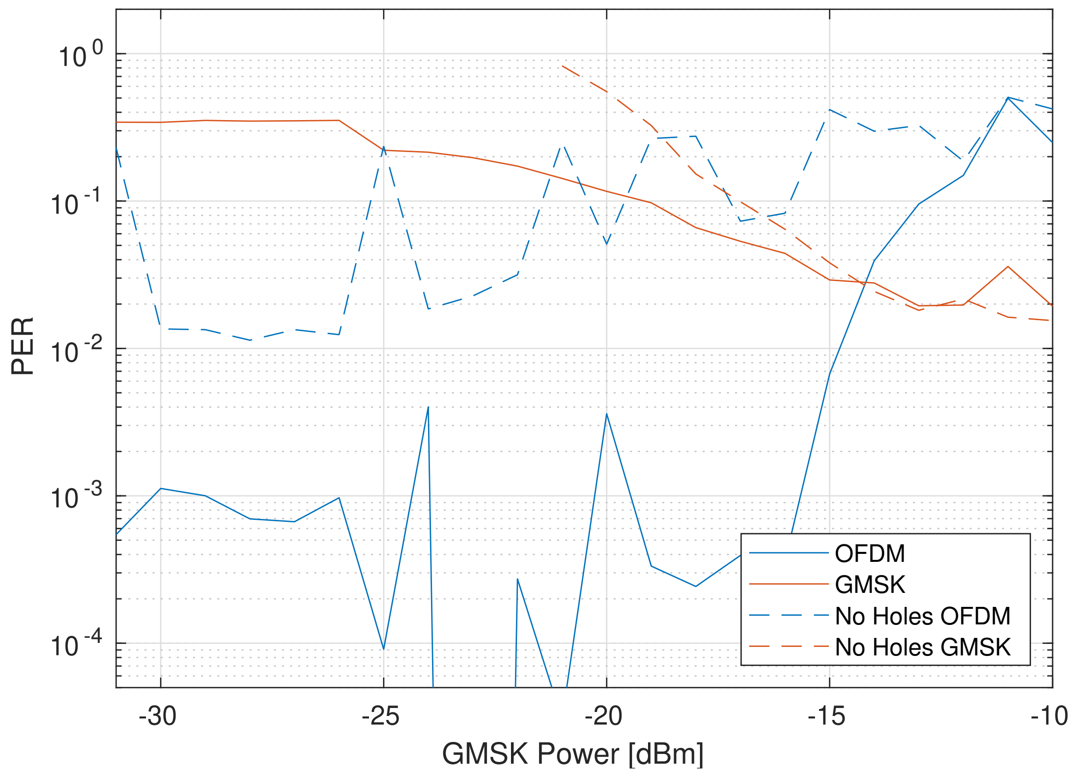

Figure 3.4: PER Test of the Prototype

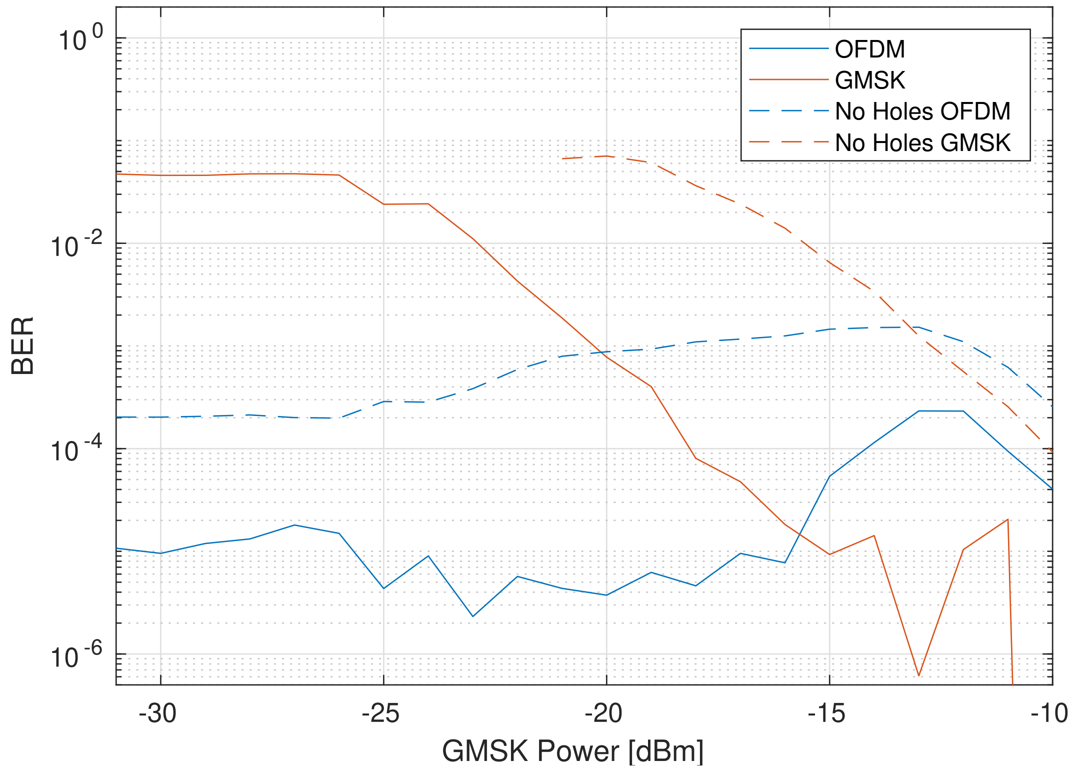

Figure 3.5: BER Test of the Prototype

# 4 Conclusion

Current security and automation systems are often stuck on single-frequency communication which is susceptible to jamming, no matter if intentional or caused by an external signal from poorly designed electronics. The main reason for a single-frequency system is the delay from a sensor waking up to information getting to a CU. This work proposes two methods on how to improve wireless communication in home automation and security systems.

One method improves sensor communication, is affordable and could be implemented with proper investment in development. The other method adds video cameras, but wouldn't currently fit into a budget of a CU of a security or home automation system. However, it might be available in near future.

Both methods allow sensors to wake up from sleep and immediately start transmitting on a random channel. A network can be designed based on these principles. The sensor hardware, power consumption, range and communication delay can stay the same as for the simple single-frequency solution that is currently available. The main improvement is increased robustness by frequency agility. If one channel is occupied, the sensor can randomly select another. With some invention, these principles could also be used to synchronize the sensor into a slow frequency hopping without the usual disadvantages.

The second method allows coexistence between the signals of a sensor and a video camera. It allows the security camera to have only one hardware radio for both the low-power sensor network and the high datarate video link.

## 4.1 Affordable All-channel Receiver in Cortex-M

This receiver allows receiving all GMSK channels at the same time. The construction uses a cheap demodulator from a DVB-T tuner connected to the MCU's ADC, so the additional complexity of the CU is acceptable for home automation or security.

The prototype hardware is not optimized and its analog design could use a lot of attention from an RF engineer. The final prototype had only a range of several meters. A receiver of a similar structure running on PC with RTL-SDR with a proper antenna had a range comparable to or greater than a standard GMSK receiver. That might indicate that there is nothing fundamentally wrong with the concept, just an imperfect design of the Rx chain.

Despite the prototype parameters, it demonstrates the possibilities of software radio in small embedded microprocessors. Apart from the direct application, the design explores a new interesting area of embedded electronics. A simple SDR receiver doesn't need an expensive FPGA to work. This potentially opens a whole new market of consumer electronics to innovative and experimental designs in RF communication, radars or similar. A receiver without the need for FFT would fit into the MCU easily. For more complicated designs, even faster Cortex-M microprocessors are already available.

## 4.2 Mixed Network with GMSK and OFDM

This set of OFDM transmitter and receiver allows making holes several frequency tones wide. These holes can be used by the GMSK communication. The OFDM receiver will automatically detect the hole layout. It could be useful for a home security system with wireless cameras. In this case, the previous all-channel GMSK receiver can be run on the same hardware in parallel with the OFDM. The results for the GMSK receiver while the OFDM is running are not good even when power and hole size are varied. More research might be needed to get the PER reasonably low.

The implementation presented here is only one of many possibilities of the entire network design. For example, a much simpler solution for the cohabitation would be a time division multiplex between the two modulations. In this specific setup, it would reduce the OFDM datarate to $2/3$. It would be the preferred solution if the sensor packets would be sparse enough. However, if the expected situation is multiple sensors reporting at the same time as the video cameras start transmitting, then the holes can be a significant improvement.

Currently, common SDRs available on the market are too expensive for consumer electronics, but the price could be pushed way down with proprietary chips used in the mobile phone segment. Security cameras will need both a processor to encode the video stream and an SDR for communication. Both components are cheaply manufactured for every mobile phone but unfortunately kept secret to protect the design. The situation could change rapidly in the same way as embedded computing became easily available by Raspberry Pi and SDR became available by the leaked datasheet of RT820T2 and RTL-SDR.

## 4.3 Applications and More Research

Still, a lot of development would be needed between this work and a production device. The development of a real network should start with up-to-date hardware. There are new options instead of the LPC4370 as more powerful MCUs became available during the studies. For example, STM32H7 offers up to 480 MHz Cortex-M7 with M4 as a coprocessor. A complete CU could instead use something like an STM32MP1 with embedded Linux and radio running on an M4 coprocessor. Both of these M4 coprocessors are comparable to the main core of the LPC4370.

Instead of the RT820T2 demodulator, there are also other options. With the upcoming IEEE 802.15.4 OFDM, more SDR-capable modems are expected. They can be used as a cheaper alternative between LimeSDR Mini and RTL-SDR. Recently, the CaribouLite[1] was crowdfunded to connect the raw IQ stream directly to Raspberry Pi's memory interface. It will be a nice and affordable concept for more SDRs which could be transformed into a CU. The IEEE 802.15.4 chips can already work with OFDM on their own which would allow time-multiplexed systems with cameras and sensors with relatively little computing power required.

An experiment showed that making the hole is advantageous in sense of correctly received OFDM packets. Even if the hole mechanism shouldn't be used for an own sensor network, it might be useful to avoid interference such as a narrow bandwidth LPWAN device. The device (eg. Sigfox) can use more than a second long, very narrow packets for its communication. Instead of waiting for the IoT device to end, it would be beneficial to eliminate a few tones and communicate. This might become even more important if the sub-GHz frequencies fill up with both LPWAN and IEEE 802.15.4 OFDM devices.

The OFDM prototype was able to communicate with 5.1 Mbit/s. Theoretical datarate without spaces between packets would be closer to 6 Mbit/s which, given the bandwidth and quadrature PSK, is on par with the oldest IEEE 802.11a. Today, much higher speeds are expected. A lot of improvements could be obtained by dynamically assigning modulation to tones, simpler binary PSK for tones next to the GMSK signal and more complex Quadrature Amplitude Modulation (QAM) further away.

One path of future research would be the principles of OFDM based M-ary FSK (OFDM-MFSK). The communication in the direction from the CU to the sensor should not be hard. Some tones would use regular PSK or QAM and some intended for the sensor would use two or four-symbol FSK. It would allow reducing the hole as the FSK signal would be orthogonal to the rest of the OFDM. In the direction from the sensor to the CU, it would be more difficult to synchronize the two. Perhaps an OFDM-MFSK preamble could encode the hole position and the sensor could precisely fit in. The rest of the OFDM packet could continue with regular modulation. It might again work only for stationary devices and many issues common with Orthogonal Frequency Division Multiple Access (OFDMA) synchronization would probably arise.

An important aspect of these methods would be the design of the entire network. The CU radio would be much simpler if it didn't have to transmit and receive at the same time. Timing of the OSI transport layer could ensure that the CU has enough time to compose a response to multiple sensors and the camera into one OFDM-MFSK packet. It would have to be balanced with the maximal delay allowed before a repeated packet gets to CU.

[1] Funded at crowdsupply.com/cariboulabs/cariboulite-rpi-hat.

# Bibliography

[1] M. Starsinic, “System architecture challenges in the home M2M network,” in *2010 IEEE Long Island Systems, Applications and Technology Conference*, 2010. DOI: 10.1109/LISAT.2010.5478336.

[2] V. K. Huang, Z. Pang, C.-J. ( Chen, and K. F. Tsang, “New Trends in the Practical Deployment of Industrial Wireless,” *IEEE Industrial Electronics Magazine*, 2018. DOI: 10.1109/MIE.2018.2825480.

[3] C. A. Trasviña-Moreno, Á. Asensio, R. Casas, R. Blasco, and Á. Marco, “WiFi Sensor Networks: A study of energy consumption,” in *2014 IEEE 11th International Multi-Conference on Systems, Signals and Devices (SSD14)*, 2014. DOI: 10.1109/SSD.2014.6808887.

[4] P. S. Cheong, J. Bergs, C. Hawinkel, and J. Famaey, “Comparison of LoRaWAN classes and their power consumption,” in *2017 IEEE Symposium on Communications and Vehicular Technology (SCVT)*, 2017. DOI: 10.1109/SCVT.2017.8240313.

[5] J. So and Y. Kim, “Interference-aware frequency hopping for Bluetooth in crowded Wi-Fi networks,” *Electronics Letters*, 2016. DOI: 10.1049/el.2016.1773.

[6] N. H. Motlagh, “Frequency Hopping Spread Spectrum: An Effective Way to Improve Wireless Communication Performance,” *Advanced Trends in Wireless Communications*, 2011. DOI: 10.5772/15482.

[7] D. Newell and M. Duffy, “Review of power conversion and energy management for low-power, low-voltage energy harvesting powered wireless sensors,” *IEEE Transactions on Power Electronics*, 2019. DOI: 10.1109/TPEL.2019.2894465.

[8] R. Piyare, A. L. Murphy, C. Kiraly, P. Tosato, and D. Brunelli, “Ultra low power wake-up radios: A hardware and networking survey,” *IEEE Communications Surveys Tutorials*, 2017. DOI: 10.1109/COMST.2017.2728092.

[9] R. Rondón, M. Gidlund, and K. Landernäs, “Evaluating Bluetooth Low Energy Suitability for Time-Critical Industrial IoT Applications,” *International Journal of Wireless Information Networks*, 2017. DOI: 10.1007/s10776-017-0357-0.

[10] P. H. Kindt, M. Saur, M. Balszun, and S. Chakraborty, "Neighbor Discovery Latency in BLE-Like Protocols," *IEEE Transactions on Mobile Computing*, 2018. DOI: 10.1109/TMC.2017.2737008.

[11] K. Mikhaylov, "Accelerated Connection Establishment (ACE) Mechanism for Bluetooth Low Energy," in *2014 IEEE 25th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2014. DOI: 10.1109/PIMRC.2014.7136362.

[12] R. Liu, A. Beevi K.T., R. Dorrance, *et al.*, "An 802.11ba-based wake-up radio receiver with wi-fi transceiver integration," *IEEE Journal of Solid-State Circuits*, 2020. DOI: 10.1109/JSSC.2019.2957651.

[13] A. Dementyev, S. Hodges, S. Taylor, and J. Smith, "Power Consumption Analysis of Bluetooth Low Energy, ZigBee and ANT Sensor Nodes in a Cyclic Sleep Scenario," in *2013 IEEE International Wireless Symposium (IWS)*, 2013. DOI: 10.1109/IEEE-IWS.2013.6616827.

[14] L. Flueratoru, S. Wehrli, M. Magno, E. S. Lohan, and D. Niculescu, "High-accuracy ranging and localization with ultrawideband communications for energy-constrained devices," *IEEE Internet of Things Journal*, 2022. DOI: 10.1109/JIOT.2021.3125256.

[15] C. Yao, Y. Liu, X. Wei, G. Wang, and F. Gao, "Backscatter technologies and the future of internet of things: Challenges and opportunities," *Intelligent and Converged Networks*, 2020. DOI: 10.23919/ICN.2020.0013.

[16] A. S. Arezoomand and M. Pourmina, "Prolonging network operation lifetime with new maximum battery capacity routing in wireless mesh network," in *2010 The 2nd International Conference on Computer and Automation Engineering (ICCAE)*, 2010. DOI: 10.1109/ICCAE.2010.5451679.

[17] J. Ding, M. Nemati, C. Ranaweera, and J. Choi, "Iot connectivity technologies and applications: A survey," *IEEE Access*, 2020. DOI: 10.1109/ACCESS.2020.2985932.

[18] G. Boquet, P. Tuset-Peiró, F. Adelantado, T. Watteyne, and X. Vilajosana, "Lr-fhss: Overview and performance analysis," *IEEE Communications Magazine*, 2021. DOI: 10.1109/MCOM.001.2000627.

[19] C. Gomez, J. Carlos Veras, R. Vidal, L. Casals, and J. Paradells, "A Sigfox Energy Consumption Model," *Sensors*, 2019. DOI: 10.3390/s19030681.

[20] R. Mozny, P. Masek, M. Stusek, K. Zeman, A. Ometov, and J. Hosek, "On the performance of narrow-band internet of things (nb-iot) for delay-tolerant services," in *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, 2019. DOI: 10.1109/TSP.2019.8768871.

[21] H. Chougrani, S. Kisseleff, W. A. Martins, and S. Chatzinotas, "Nb-iot random access for non-terrestrial networks: Preamble detection and uplink synchronization," *IEEE Internet of Things Journal*, 2021. DOI: 10.1109/JIOT.2021.3123376.

[22] T. Jakubík and J. Jeníček, "Asymmetric Low-power FHSS Algorithm," in *Proceedings of the IEEE 13th International Workshop On Electronics, Control, Measurement, Signals and their Application in Mechatronics*, 2017. DOI: 10.1109/ECMSM.2017.7945892.

[23] T. Jakubík and STMicroelectronics, "Cortex-M Simulator," in *2020 International Conference on Applied Electronics (AE)*, 2020. DOI: 10.23919/AE49394.2020.9232712.

[24] T. Jakubík and J. Jeníček, "SDR All-channels Receiver for FHSS Sensor Network," in *2018 International Conference on Applied Electronics (AE)*, 2018. DOI: 10.23919/AE.2018.8501460.

[25] T. Jakubík and J. Jeníček, "SDR All-channels Receiver for FHSS Sensor Network in Cortex-M," in *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, 2019. DOI: 10.1109/TSP.2019.8769064.

[26] M. A. Wickert and M. R. Lovejoy, "Hands-on Software Defined Radio Experiments with the Low-cost RTL-SDR Dongle," in *2015 IEEE Signal Processing and Signal Processing Education Workshop*, 2015. DOI: 10.1109/DSP-SPE.2015.7369529.

[27] M. Rice, *Digital Communications: A Discrete-Time Approach*. Pearson Education, Inc., 2009, ISBN: 9780130304971.

[28] M.-R. Awan and P. Koch, "Combined Matched Filter and Arbitrary Interpolator for Symbol Timing Synchronization in SDR Receivers," in *Design and Diagnostics of Electronic Circuits and Systems (DDECS), 2010 IEEE 13th International Symposium on*, 2010. DOI: 10.1109/DDECS.2010.5491797.

[29] S. Rajan, S. Wang, R. Inkol, and A. Joyal, "Efficient approximations for the arctangent function," *IEEE Signal Processing Magazine*, 2006. DOI: 10.1109/MSP.2006.1628884.

[30] P. P. Ann and R. Jose, "Comparison of papr reduction techniques in ofdm systems," in *2016 International Conference on Communication and Electronics Systems (ICCES)*, 2016. DOI: 10.1109/CESYS.2016.7889995.

[31] M. Wetz, I. Periša, W. G. Teich, and J. Lindner, "Robust Transmission Over Fast Fading Channels on the Basis of OFDM-MFSK," *Wireless Personal Communications*, 2008. DOI: 10.1007/s11277-007-9395-8.

[32] T. Jakubík and J. Jeníček, "Feasibility of OFDM and FHSS in a Single Home Automation and Security Network," in *2020 43rd International Conference on Telecommunications and Signal Processing (TSP)*, 2020. DOI: 10.1109/TSP49548.2020.9163493.

[33] M. Morelli, M.-O. Pun, and C.-C. J. Kuo, "Synchronization Techniques for Orthogonal Frequency Division Multiple Access (OFDMA): A Tutorial Review," in *Proceedings of the IEEE / Vol. 95, No. 7*, 2007. DOI: 10.1109/JPROC.2007.897979.

[34] G. Al-Juboori, A. Doufexi, and A. R. Nix, "Feasibility study of ofdm-mfsk modulation scheme for smart metering technology," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2017. DOI: 10.1109/ISGTEurope.2017.8260200.

[35] H. Zhou, A. V. Malipatil, and Y.-F. Huang, "Synchronization issues in ofdm systems," in *APCCAS 2006 - 2006 IEEE Asia Pacific Conference on Circuits and Systems*, 2006. DOI: 10.1109/APCCAS.2006.342228.

## Manuals, Datasheets and Online

[36] S. Kamkar. "OpenSesame." (2015), [Online]. Available: https://samy.pl/opensesame/.

[37] "JA-160PC Wireless PIR motion detector combined with a camera," Jablotron Alarms a.s. (2018), [Online]. Available: https://www.jablotron.com/en/produkt/wireless-pir-motion-detector-combined-with-a-camera-296/.

[38] "JA-151M Mini wireless magnetic detector," Jablotron Alarms a.s. (2018), [Online]. Available: https://www.jablotron.com/en/produkt/mini-wireless-magnetic-detector-213/.

[39] *EN 50131-1*, CENELEC, 2006.

[40] *SX1232 868 and 915MHz Ultra Low Power High Link Budget Integrated UHF Transceiver*, Semtech Corporation, 2013.

[41] *CC1200 Low-Power, High-Performance RF Transceiver*, Texas Instruments Incorporated, 2014.

[42] *S2LP Ultra-low power, high performance, sub-1 GHz transceiver*, STMicroelectronics NV, 2019.

[43] *LoRaWAN 1.0.4 Specification*, LoRa Alliance, Inc., 2020.

[44] *IEEE Standard for Low-Rate Wireless Networks*, IEEE 802.15.4-2020, IEEE Computer Society, 2020.

[45] *CFR Title 47, §15.247*, FCC, 2003.

[46] *Atmel AT86RF215 Device Family*, Atmel Corporation, 2016.

[47] *ATA8352 Impulse-Radio Ultra-Wideband (IR-UWB) Transceiver*, Microchip Technology Inc, 2021.

[48] *DW3000 Ultra Wideband Transceiver*, Qorvo Inc, 2021.

[49] *SX1302 LoRa Gateway Baseband Transceiver*, Semtech Corporation, 2019.

[50] *TS 103 357*, ETSI, 2018.

[51] *nRF9160 Product Specification v2.1*, Nordic Semiconductor ASA, 2021.

[52] *EN 300 220-2*, ETSI, 2017.

[53] A. Collins, *All Programmable RF-Sampling Solutions*, Xilinx, 2017.

[54] T. Leconte. “Playing with the Airspy R820T IF bandwidth.” (2018), [Online]. Available: https://tleconte.github.io/R820T/r820IF.html.

[55] *LPC4370 Datasheet*, Rev. 2.3, NXP B.V., 2016.

[56] RTL-SDR Blog. “R820T2 Chip Discontinued: Low Cost R820T2 RTL-SDRs will Continue, Airspy Will Redesign.” (2018), [Online]. Available: https://www.rtl-sdr.com/r820t2-chip-discontinued-low-cost-r820t2-rtl-sdrs-will-continue-airspy-will-redesign/.

[57] RTL-SDR Blog. “The R860 Will Replace The R820T2 - Same Chip Different Name.” (2021), [Online]. Available: https://www.rtl-sdr.com/the-r860-will-replace-the-r820t2-same-chip-different-name/.

[58] *LPC4370 User Manual, UM10503*, Rev. 2.3, NXP B.V., 2017.

[59] *DT0087 Coordinate rotation digital computer algorithm (CORDIC) test and performance verification*, STMicroelectronics, 2017.

[60] *STM32L062K8 STM32L062T8 STM32L062C8 Ultra-low-power 32-bit MCU Arm-based Cortex-M0+*, STMicroelectronics NV, 2020.

[61] *LMP91000 Sensor AFE System*, Texas Instruments Incorporated, 2014.

[62] *IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE 802.11-2020, IEEE Computer Society, 2020.

[63] Joseph D. Gaeddert. “Ofdm flexible framing structure (ofdmflexframe).” [Online; accessed May 12, 2022]. (2022), [Online]. Available: https://liquidsdr.org/doc/ofdmflexframe/.

## List of Published Results

[22] T. Jakubík and J. Jeníček, “Asymmetric Low-power FHSS Algorithm,” in *Proceedings of the IEEE 13th International Workshop On Electronics, Control, Measurement, Signals and their Application in Mechatronics*, 2017. DOI: 10.1109/ECMSM.2017.7945892.

[23] T. Jakubík and STMicroelectronics, “Cortex-M Simulator,” in *2020 International Conference on Applied Electronics (AE)*, 2020. DOI: 10.23919/AE49394.2020.9232712.

[24] T. Jakubík and J. Jeníček, “SDR All-channels Receiver for FHSS Sensor Network,” in *2018 International Conference on Applied Electronics (AE)*, 2018. DOI: 10.23919/AE.2018.8501460.

[25] T. Jakubík and J. Jeníček, “SDR All-channels Receiver for FHSS Sensor Network in Cortex-M,” in *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, 2019. DOI: 10.1109/TSP.2019.8769064.

[32] T. Jakubík and J. Jeníček, “Feasibility of OFDM and FHSS in a Single Home Automation and Security Network,” in *2020 43rd International Conference on Telecommunications and Signal Processing (TSP)*, 2020. DOI: 10.1109/TSP49548.2020.9163493.

[64] T. Jakubík and J. Jeníček, “OFDM and FHSS Hybrid Network,” in *Počítačové architektúry & diagnostika PAD 2017*, 2017, ISBN: 978-80-972784-0-3.

[65] T. Jakubík and J. Jeníček, “Mnohokanálový softwarový FHSS přijímač na Cortex-M,” in *Počítačové architektury a diagnostika PAD 2018*, 2018, ISBN: 978-80-261-0814-6.

[66] T. Jakubík and J. Jeníček, “Asymmetric Low-power FHSS Algorithm,” in $5^{th}$ *Prague Embedded Systems Workshop*, 2017, ISBN: 978-80-01-06178-7.

## Software Created for this Work

Most of the software used in this work should be obtainable from GitLab, but its long-term availability cannot be guaranteed. Use any of the code only at your own risk and be sure to check local radio regulations first. Details can be found in the full thesis.

- gitlab.com/users/ratiafak/projects

# Tomáš Jakubík

## WORK EXPERIENCE

APR 2019 – OCT 2019
### INTERNSHIP, CORTEX-M FIRMWARE DEVELOPER – STMICROELECTRONICS ROUSSET SAS

Sophia Antipolis, France

JAN 2017 – CURRENT
### PART-TIME, CORTEX-M FIRMWARE DEVELOPER – JABLOTRON ALARMS A.S.

Jablonec nad Nisou, Czechia

## EDUCATION AND TRAINING

DEC 2016 – CURRENT – Liberec, Czechia
### DOCTORAL STUDIES OF TECHNICAL CYBERNETICS – Technical University of Liberec

ISCED 8

SEP 2014 – FEB 2017 – Liberec, Czechia
### MASTER'S DEGREE IN MECHATRONICS – Technical University of Liberec

ISCED 7

SEP 2015 – SEP 2016 – Zittau, Germany
### MASTER'S DEGREE IN MECHATRONICS – Zittau/Görlitz University of Applied Sciences

ISCED 7

## LANGUAGE SKILLS

Mother tongue(s): **CZECH**

Other language(s):

| | UNDERSTANDING | | SPEAKING | | WRITING |
|---|---|---|---|---|---|
| | Listening | Reading | Spoken production | Spoken interaction | |
| **ENGLISH** | C2 | C2 | C1 | B2 | C1 |
| **FRENCH** | A1 | A2 | A1 | A1 | A1 |

*Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user*