“IoT”

Collecting Data in a noisy world

The Coexistence Conundrum

White Paper WP-004
Issue 1 (24-08-2018)

Abstract

With over 25 billion wireless devices expected to connect by 2025, interference between these devices is inevitable. What I see missing in those who are currently designing Wireless Sensor Networks (WSN) is awareness of this problem.
It will be good if we try to prevent the "Conundrum" from becoming a "Nigthmare".

Coexistence on the "Unlicensed" frequencies

The problem of the coexistence of multiple services on the same frequency bands goes back to the beginning of the Radio. On the "Unlicensed" frequency bands (ISM, SRD, etc.) the proliferation of wireless applications in the absence of universally recognized "Standards", but also due to the same intrinsic diversity of applications has already led (2018) to situations of reduction of reliability in many "IoT" wireless network. And the situation tends to get worse.
Problems of coexistence that users can already notice are in the 2.4 GHz ISM band, saturated by WiFi, Bluetooth, etc.
Protocols, such as those of the Wi-Fi Alliance, ensure that networks of similar devices that use the same standard can communicate and share the channel, following the rules of that standard. However, it remains a problem: different standards are not able to share channels cooperatively. A Bluetooth device that uses the Frequency Hopping Spread Spectrum (FHSS), for example, is unable to detect and understand an IEEE 802.11 transmission that uses orthogonal frequency division modulations (OFDM) and direct sequence spread spectrum (DSSS) on same radio frequencies.
Efforts have been made to improve coexistence in these standards, but to date, no active cooperation has been defined. Bluetooth, for example, can sense which of its frequency hopping channels are experiencing a high error rate, and drop those channels from its hopping sequence. However, this indirect method of channel sharing is only marginally effective in crowded environments where many different devices operate.

"IoT" Low Power Wireless Sensor Network

Those described above (WiFi, Bluetooth, etc.) are international protocols and standards with specific algorithms for managing coexistence. They are above all "ICT", devices of Information Technology, and they already have problems between them. The NB-IoT system works on mobile cellular radio bands and is therefore to be treated differently.
In the case instead - as in the case of most of the "billions" of our interest - of small sensors and devices, at low cost and above all with "low energy" requirements, things get complicated. It is unthinkable that a "IoT" wireless sensor that costs only a few dollars, powered by a Lithium button battery and designed for years of maintenance-free service, can apply sophisticated algorithms to manage messages on shared radio channels. The thing is then obviously impossible with unidirectional systems.

EMI and EMC

Interference is not only emissions on the radio channel, but also broadband disturbances and noise generated by other RF devices and other electronic circuits. This problem concerns only the receiver and, in unidirectional networks, the "Access Point" or "Gateway". It is normal to suffer from insufficient operating range problems and then discover that a switch mode regulator is mounted on the same PCB as the receiver. In this case, the poor range is not due to the low ERP (Effective Radiated Power) of the Tx or to the obstacles, but rather to the broadband noise generated by the regulator. With the effect of worsening the S / N ratio of the receiver. Another case of interference from broadband noise, which cannot be traced back to co-channel emission from other "IoT" or "ICT" devices, occurs when a transmitter of any type is present nearby. Here "nearby" can be a few tens of centimeters in the case of another wireless device, for example a WiFi (100mW), but also hundreds of meters if it is an FM Broadcast station (10kW). Or more likely, cellular network stations (which are now everywhere). In this case the disturbance is the "Noise" present on the sidebands generated by the RF carriers digitally modulated and by the relative RF transients.

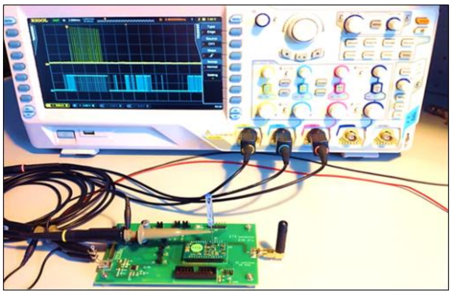

Fig.1 – Monitoring the radio channel .

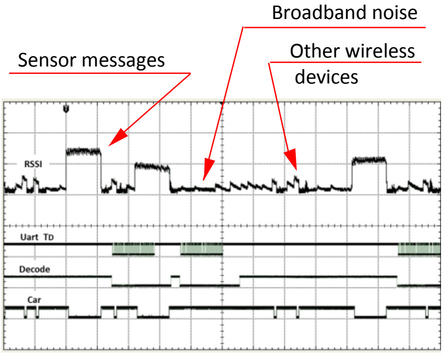

Fig.2 – Noise and interference.

Improve coexistence before the system is on the field

It is important that during the design of the wireless network and related devices, appropriate coexistence tests are performed: before, not after the system becomes operational.

- EMI/EMC compliance tests ensure that network and devices meet the requirements of a given standard.
- Coexistence tests evaluate the performance of a wireless network in a mixed signal environment and in the "Noisy" world.

Once the problems have been identified, countermeasures can be taken. Screens and filters can be applied to the receiver and you can try to neutralize external noise sources. It is also possible to intervene on the antennas and their position in the network.

Coexistence criteria

Three coexistence techniques can be adopted in Wireless Network design :

(1) A first technique involves frequency separation, but this implies a radio channel allocation strategy that can hardly be predicted on the "Free" bands.
(2) A second technique is the separation of time and code. This technique can be applied especially in bidirectional sensor networks, less in unidirectional networks, but presents problems. International standards and regulations to allow the general use of these bands have introduced the "Duty-cycle" and other frequency sharing techniques. But the multiplicity of applications and the proliferation of devices in highly urbanized areas very often make this technique not very useful.
(3) The third technique is physical separation, in practice small areas where it is possible to guarantee a level of RF signal sufficient to cover interference. It is employed the scarcely known “Co-channel rejection” characteristic of the receiver, the receiver's ability to correctly demodulate a signal, even in the presence of interference if they are 10-15 dB weaker than the useful signal.

In practice, if we think of the "billions", billions of sensors and alarms that are small and cheap and last for many years, the third technique must be used. It is difficult to imagine that these devices could be designed to handle the complex sharing of the service with other more sophisticated devices.
This leads us to consider the solution of using small areas, where "small" is naturally always a relative term: a few tens of meters in urban areas, about 100 meters in rural areas. In other words, the purpose of the International Rules which limits the power of the Tx to a few milliwatts is to limit the area by allowing the use of "Free" frequencies to other users.
Just to allow the "Coexistence"…..
Therefore, if necessary, the area can be enlarged by connecting with other gateways, possibly "wired" connected to the local LAN network.
It's complicated? Yes, it's complicated, but it's better not to increase frequency abuse with a proliferation of wireless connections.

The myth of the “Long Range"
A great concern in "IoT" to guarantee the "Long Range" (10-20 km). Of course, there are cases where a long haul is needed: consider, for example, the application in agriculture. But consider, as another example, the cellular service: here the trend is towards ever smaller cells. It is a problem of coexistence….
Most "IoT" applications will be in high-density urban areas and there is a cohabitation problem here. But in an area of high density, it will be good not to think of kilometers, but of cells of a few tens of meters.
On the other hand, the "billions" reside here….

Coexistence by design

In addition to intervening and fighting against interference and noise, it is also of fundamental importance to limit as much as possible the source of the non-sustainable occupation of the "Free" frequencies. That is, even thinking of the future, do not passively suffer the situation, but design the "Wireless Devices" in a conscious way. In all the International Rules there is already the obvious Tx output power limit. And there is also a limit on the transmission time and a "Duty-cycle".
Especially in "IoT" applications, a coexistence strategy must be applied to the design of the "Wireless Sensor Network" to avoid the proliferation of unnecessary transmissions. In any case, the strategy starts at the "Wireless Device" level.
A simple example: it must be clear that a hundred wireless sensors all together in a "local" area and that transmit a message every three or six seconds collide with each other and with an obvious problem of coexistence. It seems superfluous to refer to such an obvious case, but unfortunately they are things that have happened .....
Coexistence must begin with a correct timing of transmission messages and with a plan for distributing message control to the "Access Point" network and then to the local area data management center.
Now, without any idea of being exhaustive, we will propose two simple examples of correct wireless sensor design. Just to give an idea of how to intervene to limit the RF band occupation.

- A simple wireless "Reed-contact" sensor to be used to control and alarm a remote door entry.
- A more complex temperature sensor whose task is to draw a diagram of a daily temperature.

(1) In fig.3 a simple “Reed Switch” wireless sensor whose function is to control if a remote door is open or closed. Coexistence strategy to be applied is a correct timing of the “Reed” status and of the transmission time. First to be decided is the “Heartbeat” time. Heartbeat transmission is necessary for every wireless device, especially in alarm networks with unidirectional devices, to maintain control of the sensor health status and in general of all the network. Heartbeat message transmits also information, as an example the battery voltage, plus obviously the open/closed situation of the door. The second timing is controlled by the sensor microcontroller and is the open/closed sampling of the reed contact. "Reed" sampling can be done by the sensor MCU in 50 µs and be repeated every 3 seconds.

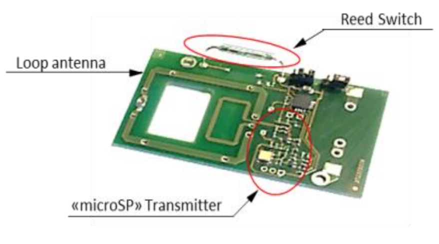

Fig.3 - “Reed-switch” wireless sensor

Finally the MCU is programmed to immediately send a message as soon as the "Reed" status has changed.
With this operating strategy, a "Heartbeat" message every 20 minutes and the "Reed" sampling every 3 seconds with a transmission at each door opening or closing, the band occupation is really very low.
And also the current from the battery ....

(2) The second example is a sensor that measures the temperature every three seconds and transmits it to the "Local network" to which it is given the task of processing the measurements in a graph. In this network there will be many other wireless devices and it is not possible to transmit every three seconds, for message collision and obviously also to limit the consumption of battery current.
A possible solution (Fig.4) involves a transmission every minute with a message containing the value of the twenty previous temperature measurements. The MCU sensor performs the twenty measurements in a few microseconds, stores them with an eight-bit resolution and transmits them together with a twenty-bit "ID", four battery status bits and the checksum.
It is possible to transmit all this data, using "microSP" technology, in a 192 bit message and in 20 ms. Even supposing to transmit two random distance messages, to reduce the probability of collisions, the occupation of the band will be 40 ms/minute and the Tx “Duty-cycle” a very low 0.066%.

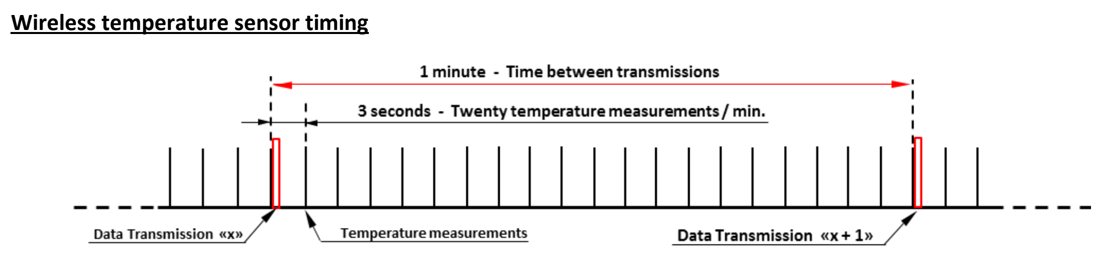

Fig.4 – Coexistence design