Microwave Backscatter for RFID Application

Péter Kovács¹, Levente Dudás¹, Rudolf Seller², Péter Renner³

¹ PhD Student, Budapest University of Technology and Economics, Goldmann Gy. tér 1-3., H-1111 Budapest, Hungary
² Assistant Professor, Budapest University of Technology and Economics, Goldmann Gy. tér 1-3., H-1111 Budapest, Hungary

Abstract. The traditional meaning of RFID is to identify an object without contact. There is usually a requirement in these cases that the object must not use battery or power supply. This article deals with a new feature, which is the hiding of the object. It means there would be a requirement to identify an object without risk uncovering by unauthorized.

Keywords: RFID, hiding, identification, backscatter

1 Introduction

A system which is used for identification is called RFID when perform a simple condition, it must not be galvanic coupling between two main sections called RFID tag and reader. Generally, the tag is passive and it is placed outside of an object to identify it, readers can read the data out which are consisted by the tags. This amount of data is not a lot, but it can identify an object e.g. in a factory. The read data can be more, when the tag is active, which means, it has an own battery or power supply.

There is another opportunity of the RFIDs’ classification. One case, we are interested in identification of the object and the stored data are public. In the other case, we are interested in hiding the object, which means that, it is unacceptable to detect the being of the object.

This article deals with this ‘hiding’ kind of identification. We are introducing simulations, block diagrams, measurements and plans in the future.

2 Theoretical background

The problem is: the object has to be invisible to everybody, who are unauthorized or it is forbidden to know about the existence of the object. However, have to be someone who is entitled to get information about the object and its location.
It could be a solution when we place an antenna on the object, reflectivity can be controlled electronically. It means that, we are able to produce BPSK modulated backscattered signal. This solution ensures that it will not radiate power, so it will be passive, but through the phenomena of reflection we can transmit information about the object. When using a binary noise series in the modulation with an appropriate bandwidth, the object stays hidden.

When the antenna is radiated by an unmodulated RF signal, the response will be a noise-like signal for the unauthorized user, who does not know the right bit series. If the user knows the bit series, it is possible to make a correlator (FIR filter), which suits for the right bit series; in this way, the object becomes visible.

3 RFID reader

The block scheme of the realized reader is shown in Fig. 1. A little part of the transmitted RF signal is backscattered from the object, this RF signal is gained and converted down to base-band, and digitalized in I-Q field (amplitude and phase is known). The controller contains a correlator, which can ‘recognize’ the modulated backscattered RF signal. Thanks to the spectral extension, the signals under the noise level can be detectable.

![Fig. 1. Block diagram of the RFID reader. It radiates a sinusoidal signal, which is modulated by tags. It uses incoherent receiver and matched filter for a searched code.](image)

4 RFID tag

In generally the tag on the object can contain the following RFID hardware – Fig. 2. It receives the unmodulated sinusoidal RF signal. The necessary supplying power is coupled out from the antenna, which can be very small, because the task is to change the load of the microwave signal route.
We realized the tag with a QAM modulator (Fig. 3.) which can be functionally passive. This means that the transfer function of the modulator is less than 0 dB. When we use BPSK modulation, we do not have to control the amplitude of the transmitted power. This hardware allows other modulations e.g. QPSK and QAM, but in practice the operation of theory is demonstrable by analyzing only the BPSK modulation.

In the experimental phase, miniaturizing is not an aim, only the function and a QAM modulator offers us a wider range of experiments.
5 Simulations

To authorize the object, it is necessary to use pseudo-random codes. A possible code generator using shift registers, feedback by mod 2 adders is in Fig. 5.

![Fig. 5. A possible pseudo-random code generator](image)

The code is unambiguously determined by a 2N long bit series, which contains the initialize vector and the feedback vector. Where the feedback vector component is 1, the output of the flip-flop is connected to a mod 2 adder. According to the previous figure, it is the following:

\[ [00100001;11100111] \] (1)

The length of the code will be \( 2^N - 1 \) where \( N \) is the number of the D-flip-flops. The maximal output signal-to-noise ratio could be achieved by using matched filter, which transfer function is the complex conjugate of the transmitter filter. In this case, it is a FIR filter. Its weighting vector (impulse response) is the complex conjugate of the inverse transmitted bit series (2). If using BPSK code, it is enough to know the inverse bit series.

\[ H_\text{R}(f) = H_\text{R}^*(f) \Leftrightarrow h_\text{R}[T \cdot (2^N - 1) - t] = h_\text{R}^*(t) \] (2)

This binary code and its autocorrelation function – which are generated by the Code Generator to the RFID tags – are in Fig. 6.
If the transmitted code is known for the correlator, the output signal will be similar to the autocorrelation function. If the correlator output signal is higher than e.g. 250, the object is authorized. If we do not know the code, the correlator output will be less than the e.g. 250.

The (PSL) peak-side-level is more than 18 (25 dB), so, the gain will be the same, when the code is known.

The task is to find such codes, which PSL is high enough to make easy setting up the threshold level in noisy environment and the cross-correlation function between codes have to be the lowest.
Here is introduced a simulation when the amplitude of the transmitted signal is 1 and the noise level is ten times more than the transmitted signal. The received signal is in Fig. 7 up, the correlator output signal is in Fig. 7 down. The communication under noise level is realizable but naturally a capacity decrease.

6 Measurement results

The used code is downloaded to the Controller and the reader radiates the sinusoidal RF signal, the tag (QAM) receives this signal, modulates it according to the code, and radiates it back to the reader. The reader receives this reflected modulated RF signal, and demodulates it.
The black box is the controller, middle up – the tag, left down – the reader, middle – two RF preamplifiers, and left up – a ventilator for perturbation RF signals.

We made some measurements with different code length. The result of a 63 bits binary code is shown in Fig. 10. We can make an easy decision according to the correlation function, but it will be more indifferent for noise when the code longer.

Fig. 10. Received signals in time measured in a noisy environment and its correlation function with the transmitted code

Fig. 11 shows another measurement result using the mentioned 255 bits long code. The different is clearly shown between Fig. 10 and Fig. 11, the code is longer, gain is higher than the previous.
If we place a rotating ventilator between the reader and the tag, it can cause Doppler-effect. This effect is shown in Fig. 12 with low rev.

With higher rev, the measured received signal is in Fig. 13.
Conclusion

A civil right friendly RFID system had been developed, which are able to authorize only the in-demand object. The RFID detection is simultaneously impossible, because all objects have quasi-orthogonal code (to authorize it, the code should be known).

According to the simulation and the measurement results, the RFID hardware using CRCS is practicable. In the near future, we are going to deal with the examination of different spectrum extension modulation, and the RFID hardware miniaturization and its technological aspects.

References

1. EDMUND W. SCHUSTER, STUART J. ALLEN, DAVID L. BROCK: Global RFID. The Value of the EPCglobal Network for Supply Chain Management (2007)
3. KNOTT, E. F; SHAEFFER J. F; TULEY M. T. Radar Cross Section, 2nd ed. SciTech, 2004