ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 4, April 2014

EPCglobal Gen-2 RFID Tag to Reader Communication Simulation Using GNU Radio

S Chaithanya Sai Srinivas[1], A Salivahana Reddy[2], G V Sai Yeswanth[3], Braj Bhushan Jha[4], Dhaneshs G Kurup[5]

Student, Electronics& Communication Department, Amrita School of Engineering, Bangalore, India[1,2,3]

Professor, Electronics& Communication Department, Amrita School of Engineering, Bangalore, India[4,5]

Abstract: RFID is a revolutionary step in wireless technology, which can be deployed for identification and tracking of objects. This technology is complex and expensive, but decrease in cost of VLSI components gives a pathway to this technology into developing countries. In RFID, the communication takes place between the tags to the reader and vice versa. In this paper, we simulated the tag to reader communication of an EPCglobal Gen-2 RFID system with the aid of GNU Radio, a free software development toolkit that provides the signal processing runtime and processing blocks to implement software radios using readily-available, low-cost external RF hardware.

Keywords: RFID, GNU Radio, EPCglobal standard, Readers, Tags

I. INTRODUCTION

Radio-Frequency Identification (RFID) is a technology used to identify and track objects based on radio signals. In RFID technology, a small electronic device that consists of a chip and an antenna together called as a tag stores identification information of the object. RFID devices can work within a few feet from the scanner or reader, so multiple devices can be scanned at a time without the necessity of the line of sight [1] [2]. GNU Radio is a free & open-source software development toolkit that provides the signal processing runtime and processing blocks to implement software radios using readily-available, low-cost external RF hardware. It replaces most of the hardware with software and can efficiently process the real time signals and virtually produces real time output. So, we can use the same equipment for a variety of applications. In this paper, we simulated tag to reader communication of RFID system using GNU Radio. We created new signal processing blocks in C++ for encoding and modulation techniques in addition to performance parameter estimations. We analysed the signal at every stage of the communication process and presented it in this paper.

II. RADIO FREQUENCY IDENTIFICATION (RFID)

RFID system consists of mainly three segments tags, readers and middleware.

A. *Tags*

The purpose of an RFID tag is to physically attach data about an object (item) to that item. Each tag has some internal mechanism for storing data and a way of communicating that data. Based on the power source, tags are classified into passive tags - obtain operating power from the reader's electromagnetic waves, semi passive tags - uses a battery to maintain memory in the tag, but for communication works same as passive, active tags – uses a battery for both memory and communications. They generally ensure a longer read range than passive tags.

B. *Readers*

Readers are also called as the interrogators. The purpose of a reader is to communicate between various tags simultaneously and interrogate them for their unique identity. The communication between reader and tag is wireless and no line of sight is required. The RF module in the reader acts as a transceiver. The readers can be classified into two type's namely active readers and passive readers. An active reader is designed to communicate with active tags and a passive reader for passive tags.

C. *Middleware*

The middleware is a software program that supports or mediates two separate entities. Middleware provides a single platform for two different applications so that they can communicate edifyingly. It lies below the application level. Middleware frameworks, process the entire data and are basically designed to eliminate or hide some kinds of heterogeneity of hardware and networks.

D. *EPCglobal Class 1 Generation 2*

Electronic Product Code (EPC) tag capabilities are broken down into classes and each class has specific capabilities and is backward compatible with the preceding class. Each higher class maintains the previous capabilities and characteristics and adds new capabilities. Gen 2 or EPCglobal Class 1 Generation 2 defines the physical and logical requirements for a passive-backscatter, Reader (RFID Gen 2 Reader), RFID system operating in the 860 MHz - 960 MHz frequency range with a data rate of 40/640 Kbps.

III. GNU RADIO

The main objective of the GNU Radio is to allow easy combination of signal and data processing blocks into modulation, demodulation or complex signal processing systems. The GNU Radio has *a python* based interface, but the signal processing blocks are written in C/C++. Signal processing blocks that can be identified in GNU Radio are as follows,

1. *Source*: It is used for signal generation and consists only output ports.
2. *Sink*: It is a graphical interface to observe the signals in any part of the circuit. It consists only input ports.

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 4, April 2014

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

3. *Interleave*: It acts as a parallel to serial converter which takes N inputs and gives a single output.
4. *De-interleave*: It acts as a serial to parallel converter which takes a single input and gives N outputs.
5. *Threshold*: The output has two levels i.e., 0, 1. If the data is greater than the threshold, then the output is '1' else it is '0'.

IV. TAG TO READER COMMUNICATION

There are many phases in this block of communication between the tag and reader such as encoding and modulation techniques. Here we follow the EPC class1 gen2 protocol, which implements the modulation techniques like Phase Reversal - Amplitude Shift Keying (PR-ASK) and encoding techniques like miller (FM-0) encoding.

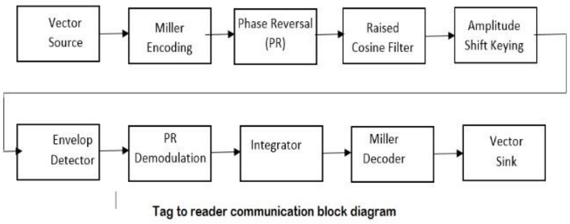

Figure 1, Tag to reader communication block diagram.

A. Phase Reversal Amplitude Shift Keying (PR-ASK)

In PR-ASK, PR the phase reversal refers to binary phase shift keying (BPSK). In PR-ASK, the input data stream is first binary phase shifted and the output is given to an ASK (amplitude shift keying) modulator. The advantage of BPSK is that, it requires a low signal to noise ratio (SNR) and the advantage of ASK is that it requires less bandwidth to transmit the signal. One of the limitations of the ASK is that, it is sensitive to atmospheric noise which can be overcome by using BPSK modulation scheme. Therefore, by implementing PR-ASK good bandwidth efficiency with a decent BER performance.

The mathematical equation for ASK is,

$$Y(t) = (1+G*M(t))\,C(t) = C(t) + G*M(t)\,C(t) \qquad (1)$$

Where,
Y (t) = Output of the ASK
M (t) = Input message signal
C (t) = Carrier signal
G = Modulation index

B. Miller Encoding

Tag communicates with reader using either FM0 or Miller sub-carrier encoding. The basis functions of these two encoding methods are the same, so, the BER performance is equal. On the other, Miller code can be spread to reduce the rate by multiplying the encoded symbols by a sequence. These sequences can include 2, 4, or 8 cycles per encoded symbol.

In the Miller encoding the n bit data is converted into 2n bit data. The Miller encoding follows the following logic,

If i/p is 0 - O/P will have no transition
If i/p is 1 - O/P will have a transition in the middle
If i/p have two zero's sides by side, then O/P will have a transition at the start of the second symbol

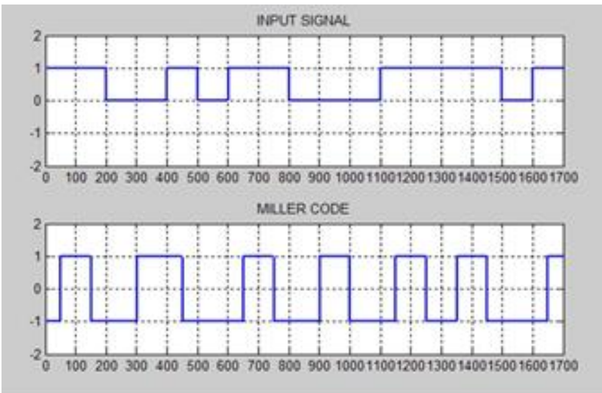

Figure 2, Miller logic code for given input signal.

Previous state	Previous i/p	Present i/p	o/p 1	o/p 2
0	0	0	1	1
0	0	1	0	1
0	1	0	0	0
0	1	1	0	1
1	0	0	0	0
1	0	1	1	0
1	1	0	1	1
1	1	1	1	0

Table 1, Truth table of Miller logic.

The Boolean expression for Miller logic is

$(M_0, M_1) = (0, 1)$, if IN = 1
$= (0, 0)$, if IN = 0

$M_{2N+1} = IN'.M'_{2N-1} + IN.\,M_{2N}$

$M_{2N+2} = IN'.M'_{2N-1} + IN.\,M'_{2N}$, N= 1, 2, 3..,

V. IMPLEMENTATION

A. Step-1

Let the input be an 8-bit data stream. (Ex. 00001011). Here a 'vector source' block is used with a 'vector to stream' block in the series.

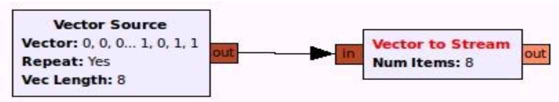

Figure 3a, Flow graph of input data stream.

Figure 3b, Graphical representation of input data stream.

B. Step-2

To the input bit stream Miller encoding is performed. Here in taking example input is '00001011' so Miller encoded data is '0011001110000110'.

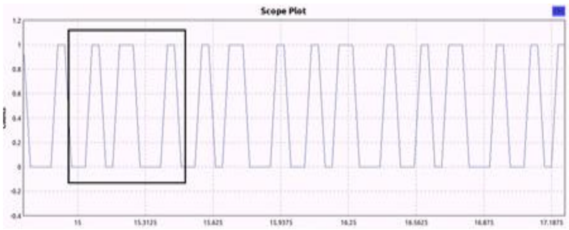

Figure 4, Graphical representation of Miller encoded data.

C. Step-3

After encoding, modulation is performed on the signal. Here PR-ASK modulation used which comprises of two stages BPSK and ASK. After performing BPSK, Raised Root Cosine filter block is used to smoothen the signal so that the bandwidth required to transmit the signal can be reduced. After Raised Root Cosine filtering, ASK is performed. For ASK carrier frequency is 896 MHz and sampling frequency is 4480MHz.

Figure 4a, Graphical representation of BPSK output.

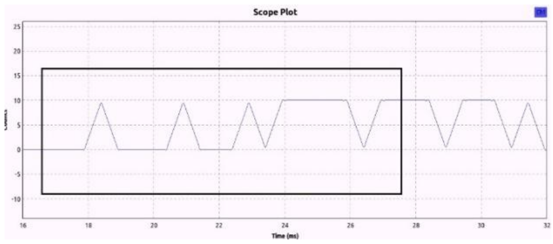

Figure 4b, Graphical representation of the Raised Root Cosine filter

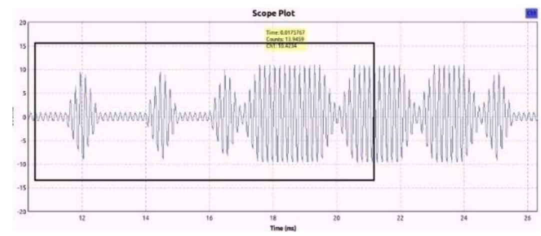

Figure 4c, Graphical representation of ASK output.

D. Step-4

After receiving the signal, demodulation is to be performed. In demodulation, there are two stages namely, the envelope detector for ASK and Phase reversal demodulator for BPSK.

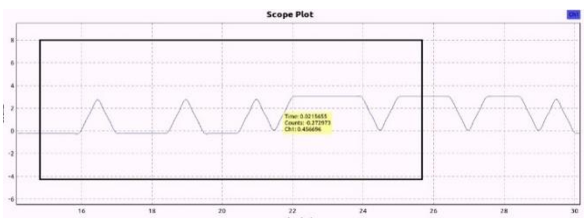

Figure 5a, Graphical representation of Envelope Detector output

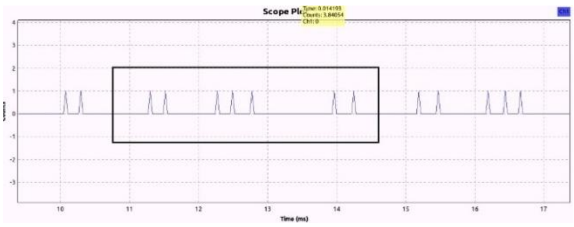

Figure 5b, Graphical representation of the BPSK demodulated output

E. Step-5

The output of the BPSK demodulator is in the form of spikes so in order to obtain the appropriate output an Integrator is employed.

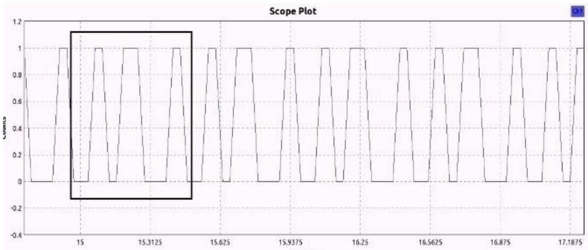

Figure 6, Graphical representation of Integrator output

F. Step-6

The integrated output is decoded using Miller decoder to obtain the transmitted input data. The Boolean expression for Miller decoder is:

If $M_{2N+1}= M_{2N+2}$ then IN (input bit) =0

Else

IN=1 where N=1, 2, 3,..

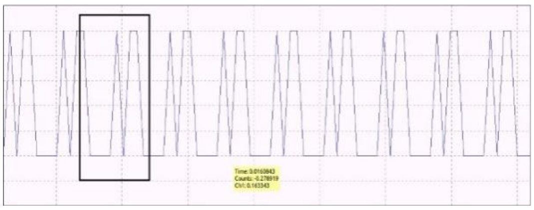

Figure 7, Graphical representation of Miller decoder output

VI. CONCLUSION

By using GNU Radio, the system level design can be implemented with minimal hardware. The fault detection can be verified at application level. With assistance of the USRP the entire real time communication can be simulated and verified in the computer. It enables the virtual implementation of the entire communication system in real time. Here the tag to reader communication is performed successfully in an ideal environment. In future, the entire RFID system can be designed and implemented using the GNU Radio. The real time BER performance can also be monitored and improved.

ACKNOWLEDGMENT

We express a deep sense of gratitude to the developers of GNU Radio for providing it as a free and open source, valuable information and guidance. We take this opportunity to express our profound gratitude and deep regards to our guides Dr. Dhanesh G Kurup and Prof Braj Bhushan Jha for their support and guidance. The blessing,

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

help and guidance given by them from time to time shall carry us a long way in the journey of professional life on which we are about to embark.

REFERENCES

[1] Mohaisen, M., Yoon, H., & Chang, K. (2008, February). Radio transmission performance of EPCglobal Gen-2 RFID system. In Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on (Vol. 2, pp. 1423-1428). IEEE.

[2] Roy Want,"An Introduction to RFID Technology", Published by The IEEE CS and IEEE ComSoc, March 2006.

[3] Elisabeth, Ilie-Zudo, ZsoltKemény, PéterEgri, LászlóMonostori, "The RFID Technology And Its Current Applications," MITIP 2006, ISBN 963 86586 5 7, pp.29-36

[4] Carla R. Medeiros, Jorge R. Costa, and Carlos A. Fernandes, "RFID Reader Antennas for Tag Detection in Self-Confined Volumes at UHF", IEEE Antennas and Propagation Magazine, Vol. 53, No.2, April 2011

[5] Chien, H. Y., & Chen, C. H. (2007). Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. Computer Standards & Interfaces, 29(2), 254-259.

[6] Nikitin, P. V., & Rao, K. V. S. (2009, April). Effect of gen2 protocol parameters on RFID tag performance. In RFID, 2009 IEEE International Conference on (pp. 117-122). IEEE.

[7] Schmid, T. (2006). Gnu radio 802.15. 4 en-and decoding. Networked & Embedded Systems Laboratory, UCLA, Technical Report TR-UCLANESL-200609-06.

[8] Catarinucci, L., De Donno, D., Guadalupi, M., Ricciato, F., &Tarricone, L. (2011, July). Performance analysis of passive UHF RFID tags with GNU-radio. In Antennas and Propagation (APSURSI), 2011 IEEE International Symposium on (pp. 541-544). IEEE.

BIOGRAPHIES

G V Sai Yeswanth is a student pursuing Electronics & Communication Engineeringatn Amrita Vishwa Vidyapeetham University, Amrita School of Engineering, Bangalore, India. His research work is concentrated on Robotics and Automation. His current research is on Photonics and designing microwave components in Meep and MPB.

S Chaithanya Sai Srinivas is a student pursuing Electronics & Communication Engineering at Amrita Vishwa Vidyapeetham University, Amrita School of Engineering, Bangalore. His research work is inclined towards Data communication and Networks. His current research is in Network applications.

A Salivahana Reddy, pursuing his B. Tech in electronics & communication. He is a technology enthusiast interested in the application of electronics to day to day life. His current interests are in the areas of RFID technology and Through Wall Imaging.

Professor Braj Bhushan Jha is a professor in Electronics & Communication Engineering Department at Amrita Vishwa Vidyapeetham University, Amrita School of Engineering, Bangalore. His research interests are Command Control and Communication Networks and Network Management Systems.

Dr. Dhanesh G Kurup is a professor in Electronics & Communication Engineering Department at Amrita Vishwa Vidyapeetham University, Amrita School of Engineering, Bangalore. His research interests are RF Engineering, Signal processing and Wireless systems.