Implementation of an Anti-Collision Differential-Offset Spread Spectrum RFID System

*Anil Rohatgi, Gregory D. Durgin

Georgia Institute of Technology
School of Electrical and Computer Engineering
777 Atlantic Dr. NW, Atlanta, GA 30332-0250

1. INTRODUCTION

Radio Frequency Identification (RFID) describes a system by which any product can be labeled with any information that can be accessed at any time without having direct contact with the item. This information can be stored on the item itself, making automation and control incredibly simple, fast, and noninvasive. The possibilities are endless [1, 2].

A typical RFID system includes two parts: the interrogator and the tags. The interrogator consists of the transmitting and receiving antennas used to query a tag. The tags are the components that store the information and are physically placed upon each item. Typically, these tags consist of an antenna and a backscatter modulating circuit [1, 2].Since many applications of RFID require only one interrogator and multiple tags, the problem of signal collision arises. When the interrogator transmits a wave to query an item, what it receives is backscatter from every tag within its read range. A single tag's information is buried within interference from every other tag transmitting simultaneously [2, 3].

Currently in industry, one solution to multi-tag interference is found by establishing a two-way communication link between the tag and the interrogator. This standard of operation is known as Interrogator-Talks First (ITF) protocol, and is currently the Electronic Product Code (EPC) standard for handling anti-collision for RFID systems operating in the 860MHz-960MHz range [4]. Using this configuration, the interrogator must query each tag individually to discover if the tag has the correct ID. If it does not, the tag is commanded to shut down. Through sequential power up and shut down commands, the RFID system searches through all the tags within the environment until all audible tags are identified [2].

Although this solution works, there are many disadvantages to its implementation. First and foremost is cost. To create a two way communication link between the interrogator and tags, complex and specialized hardware must be on board each tag to demodulate and interoperate signal commands, and transmit responses to these queries. Not only is this hardware expensive and power-hungry, but given a large number of tags within a sensing environment the anti-collision algorithm is slow. Furthermore, since there is no encryption or interference once a data link has been established, the typical RFID system is prone to privacy loss.

This paper offers a novel anti-collision solution by using the spread spectrum algorithm to solve the anti-collision problem and eliminates the need for a two-

way communication link. The solution requires minimal hardware to accommodate multiple tags and is consequently low cost, low power and fast.

2. SPREAD SPECTRUM

The spread spectrum technique is used in a variety of wireless communication applications ranging from military encryption to cellular phones [3]. For our solution, a modification of this technique was used for anti-collision in RFID.

Spread spectrum works by multiplying the low frequency data stored on each tag with a high frequency pseudo-random chipping sequence that is unique to each tag. Knowledge of the chipping sequence on each tag allows software in the interrogator to separate the desired data from the incoming signal [3]. Figure 1 below shows the mixing procedure performed in the tag hardware. The resultant output is the overall signal that is transmitted by each tag and sent to the interrogator via backscatter. The overall waveform the interrogator receives is the superposition of every tag's data modulated by their chipping sequence, which is a broadband signal. Assuming that the data and the chipping sequences in the tag were set to a voltage ranging from negative to positive one, multiplying the incoming waveform by the desired tag's chipping sequence will leave behind a low frequency component corresponding to the desired tag's data. Figure 2 below shows how the demodulation and data recovery stage works. This data can then be isolated from the signal using a low pass filter.

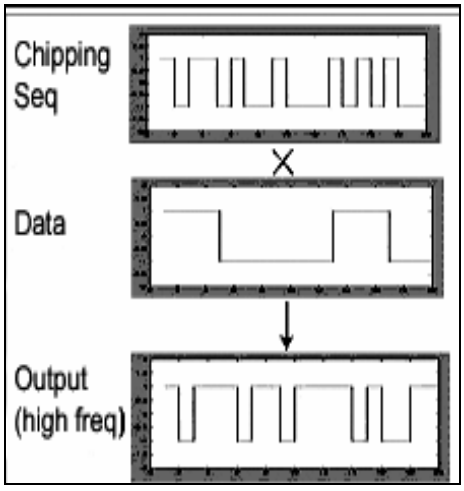

Figure 1. Single tag modulation

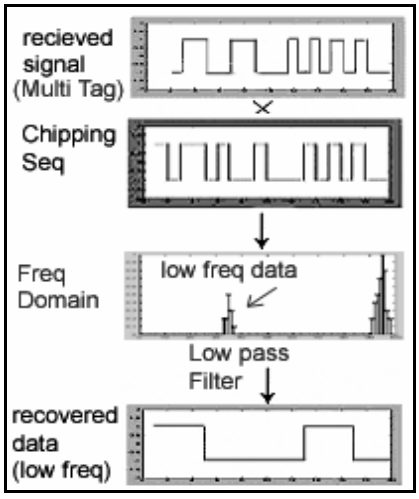

Figure 2. Data demodulation

3. HIGH LEVEL SYSTEM DESCRIPTION

A system designed to accommodate the spread spectrum anti-collision technique was constructed for use in experiments, measurement, and application testing. To query the tags, a carrier wave of frequency 915 MHz was sent from an RF signal generator and transmitted through a horn antenna. The transmission setup can be shown in Figure 3, below. The illuminated tags then modulate the carrier wave with data, and reflect it back to the reader. The receiving antenna is an open rectangular waveguide attached to a custom IQ-demodulator and a baseband data acquisition board that performs analog-to-digital conversion of both in-phase and quadrature channels. Figure 4 shows a photograph of the hardware configuration

for waveform acquisition. The transmitter and receiver together are able to interrogate backscatter RFID tags in the 915 MHz band.

Figure 3. Transmission hardware

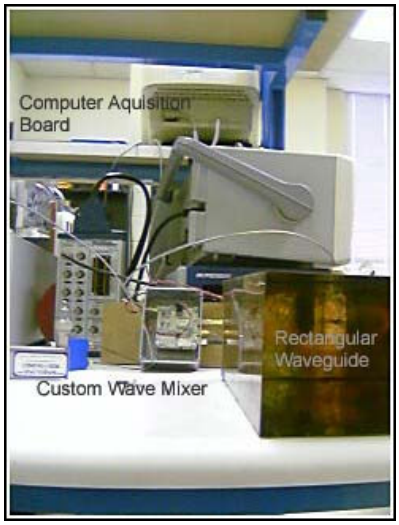

Figure 4. Receiver Hardware

The result is a signal corresponding to the bit pattern received from all the tags within the sensing environment. This waveform is captured and sampled in LabView, and the data stream is sent to Matlab to be processed.

4. TAG DESIGN AND HARDWARE

The ability to uniquely resolve the identity of a tag and decode its information from a sea of backscatter requires more than just software processing at the receiver. Hardware modifications must be made to the tags themselves in order to provide key elements needed to process a tag. The crucial part of each tag that allows the anti-collision to work is the unique chipping sequence assigned to each tag. The system fabricated in our lab was designed to handle simultaneous collisions from up to 255 different tags within a single sensing environment. This requires 255 unique chipping sequences to be created. We used the sum of two differentially-offset m-sequences to encode the ID of a chip. To create these unique sequences with minimal hardware, dual identical 8-bit m-sequence generators were placed on each tag, constructed from a feedback chain of 8-bit shift registers. These pseudo-random (PN) sequence generators were designed to have with maximum length output frequency of 255 bits. This number directly corresponds to the number of allowable tags in the sensing environment.

However, simply having a single m-sequence of code length of 255 chips is not enough to create a set of uniquely despreadable codes. Instead, the ID of each tag is encoded within the phase shift between the two sequences produced by the dual identical PN generators onboard each tag. By combining the two phase-shifted PN sequences, a unique sequence is created. Thus, with a code length of 255 bits there are 255 possible phase shifts, and therefore 255 possible output sequences. The configuration for this system is included below as Figure 5 along with a physical picture of the tag hardware as Figure 6.

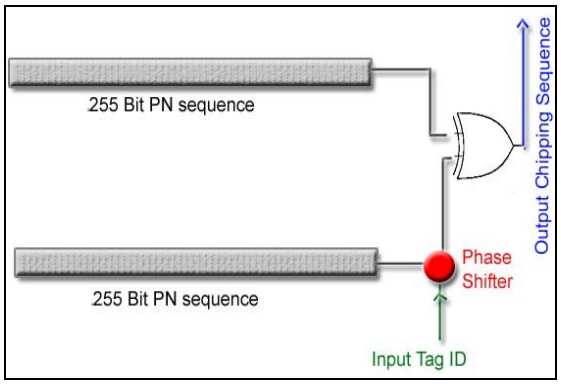

Figure 5. Chipping sequence diagram

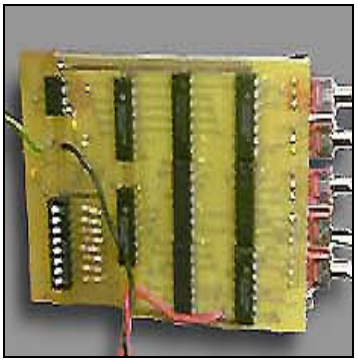

Figure 6. Physical tag photo

5. DATA PROCESSING

Once a signal has been obtained from the system, there are multiple operations that can be performed on the data depending on the application. Algorithms were written in Matlab to do two separate operations. Operation one is to isolate the data from a desired tag surrounded by backscatter interference. This is done by simulating the hardware state on the desired tag and generating a digital duplicate of the chipping sequence. The input signal is then multiplied by this sequence, and the low frequency data can be recovered. The second possible operation is to recover the ID of a single anonymous tag placed in front of the reader. This brute force approach simulates all the possible shift combinations for 255 tags, and checks these patterns against the incoming waveform. The corresponding phase shift that produces a sequence with the least mean-squared bit error is the ID of the tag. This technique and algorithm could be used on any number of RFID and sensor applications.

6. CONCLUSION

Using the differential-offset spread spectrum technique in conjunction with RFID has proved to be a simple and effective method to solve the problem of anti-collision. This low-cost, low-power solution avoids the need for excess signal processing chips on the tags, and can be extended to accommodate a large number of tags with minimal circuitry. It is a fast solution that also provides a unique encryption scheme inherent to the chipping sequence generation. Furthermore, the simplicity of its design allows this system to be deployed in a myriad of possible applications.

7. REFERENCES

[1] Christoph Seidler, "RFID Opportunities for Mobile Telecommunication Services", ITU-T Lighthouse Technology Watch, May 2005. <http://www.itu.int/ITU-T/techwatch/rfid.pdf>

[2] Mike Beigel, "Dynamic Performance of Inductive RFID Systems", European Conference on Circuit Theory and Design, Stresa, Italy, Aug. 1999.< http://www.beitec.com/articles/dynamic/dynamic1.htm>

[3] Randy Roberts, "Introduction to Spread Spectrum. "The ABCs of Spread Spectrum -- *A Tutorial*. 23 Sept. 2004. SSS online, Inc., 9 Jan. 2006. <http://www.sss-mag.com/ss.html>

[4] "Specification for RFID Air Interface", EPCglobal Inc., 31 January 2005, Version 1.0.9, 94pgs.