Application of Ultra Wideband (UWB) Modulation

Ms.Smita K.Shripad
V.L.S.I,P.C.E.
Nagpur,India.
smitashripad@gmail.com

Ms.Hema Lanje
Electronics Engg.,KITS.
Nagpur,India.
hemalanje@gmail.com

***Abstract*-- Ultra wide band (UWB) leads promising technology for next generation communication especially for high data rate & short range application. Existing secure RFID tags rely on digital cryptographic primitives in the form of hashes & blocks ciphers which leads to large system latencies. Existing RFID systems can easily be eavesdropped or jammed. To overcome the above problem we propose a new approach for secure passive RFIDs based on UWB communication. In architecture of UWB the time hopped pulse position modulation (TH-PPM), in which the hopping sequence is known only to the reader & the tag. Eavesdropping of the communication is extremely difficult by adopting the hopping sequence as a secret parameter, thus by using UWB modulation technique we can avoid digital cryptography.**

***Keywords*—** UWB, LFSR, PPM, PLL

I. INTRODUCTION

The growing demand for wireless data capability in portable devices at higher BW but lower in cost & power consumption than currently available. Crowding in the spectrum that is segmented & licensed by regulatory authorities in traditional ways. Shrinking semiconductor cost and power consumption for signal processing. Ultra wide band (UWB) transmission has recently been proposed for short-range wireless communication systems. This is due to characteristics such as high data rates, immunity to multipath fading and coexistence with narrowband wireless systems. In order to understand where UWB in with the current trends in wireless communication we need to consider the general problem that communication system try to solve specifically if wireless were an ideal medium, we could use it to send a lot of data very fast ,for many users and all at once. Unfortunately it is impossible to achieve all attributes simultaneously for systems supporting unique, private two way communication streams; one or more have to be given up if the others are to do well. Four trends are driving short range wireless in general and ultra wide band in particular.

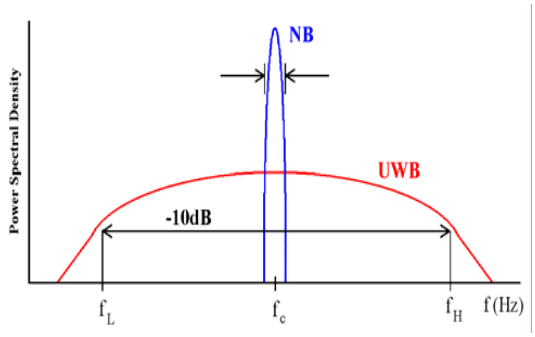
1. Availability of wireless data capability in portable devices at higher band width with lower cost.2. Crowding in spectrum.3. Growth of high speed wired access to the internet.4. Reduction in the semiconductor cost & reduction in the power consumption for signal processing.

Passive RFID capture and reuse incoming radio frequencies to power internal circuitry and to respond back to the RFID reader. The available RF power, equivalently the maximum distance, of the reader-transponder system is constrained at both sides of the link, either by regulation or else by technological limits. A typical example of an UHF tag can reach 2 m with the power budget of 150 micro watts for a tag and 500 mW for a transmitter. Current system implements the half-duplex link between a reader & a tag. A reader sends power carrying RF carrier to a tag, adding additional data by means of

Amplitude modulation. The reverse link, from a tag to a reader, is based on adaptive reflection (backscatter) of the phase of the incoming RF carrier, or on adaptive loading. current systems use a narrowband signal in both the directions, with a bandwidth much smaller than the carrier frequency (900 MHz).these existing communication schemes have been developed with simplicity in mind .they are susceptible to passive attacks such as eavesdropping as well as active attacks such as illegal readout. In recent years, many schemes have been proposed to address the privacy issues related to such tags, as well to extend their application to include authentication besides detection. All of

these proposals are highlighted at either the protocol level or algorithm level of the communication link .it assume that ,the communication link between the tag & reader can be eavesdropped & privacy must be guaranteed by the data link layer.

In recent years, many schemes have



been proposed to address the privacy issues related to such tags, as well to extend their application to include authentication besides detection. All of these proposals are highlighted at either the protocol level or algorithm level of the communication link .it assume that ,the communication link between the tag & reader can be eavesdropped & privacy must be guaranteed by the data link layer.

A. *UWB communications*

Since the FCC's allocation of a UWB spectrum in the range of 3.1 GHz to 10.6 GHz in 2002, UWB has gained phenomenal interest in academia and industry [14].Compared traditional narrowband communication systems, UWB has several advantages including high data-rate, low average radiated power, and simple RF circuitry. Many of these potential advantages are a direct consequence of UWB's large instantaneous bandwidth. Shannon's theorem states that the channel capacity C is given as B $\log_2$ (1+SNR), where B is the bandwidth and SNR is the signal-to- noise ratio [15]. As the bandwidth B is much larger (on the order of several GHz) for UWB than for a narrowband signal, the SNR can be much smaller for UWB to achieve the same data rate. Therefore, UWB is often able to recover data, even if the signal power is close to the noise level. In other words, the presence of UWB signals is harder to detect than narrowband signals.

The IEEE 802.15 WPAN task group has recognized the potential of UWB for low data rate applications, and is in the process of standardizing the physical layer [16]. Hancke and Kuhn presented a paper on securing RFIDs using UWB, to the best of our knowledge, the only one so far on this topic [17].

They suggested measuring the signal propagation delay between an RFID and the reader using UWB. If the delay exceeds a certain bound, the system signals a possible attack.

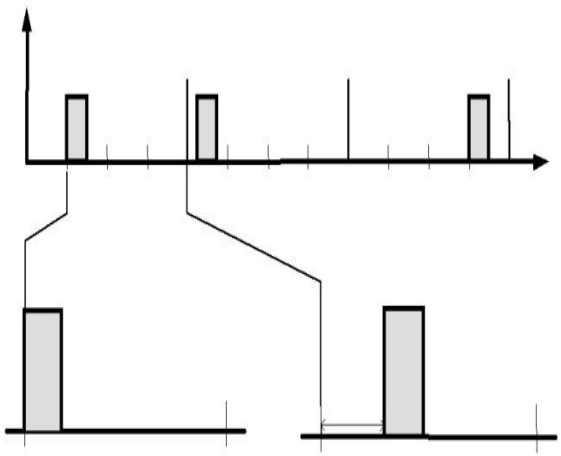


figure 1:time hopped pulse position modulation

ARCHITECTURE FOR AN ULTRA-WIDEBAND RFID

In this section we present an overview of the UWB - RFID tag architecture, including design of the digital baseband parts.

UWB-RFID tag architecture Figure 3 illustrates the architecture of our UWB-RFID tag. There are two front-ends in the tag: a narrowband receiver and a UWB transmitter. The narrowband receiver is responsible for energy harvesting and tag initialization. The energy harvesting part is the same as that of existing narrowband tags and is not discussed further. The position of a pulse within a slot is decided by "Preamble / Tag Memory" block. Upon a signal from the PPM, UWB pulse generator generates a single narrow pulse with the width of 100 ps. Due to the low duty cycle of the UWB pulses; we believe that the average

radiated power of the transmitter is very small. For example, [19] presents a transmitter design that delivers a 40 MHz UWB pulse rate with 2 mW of power consumption. glitches of digital logic are used as UWB pulses [20].

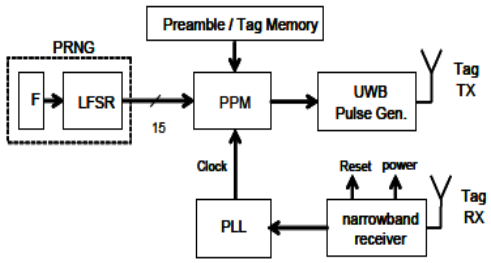


Figure 3: System architecture of the proposed UWB RFID tag

The pulse positions are decided by a programmable pseudo-random number generator (PRNG), which is based on a linear feedback shift register (LFSR). For the framing format shown in Figure 2, the PRNG generates a random number of 15 bits for a data bit. The PRNG operates in two modes: a preamble mode and a tag identifier mode. The PRNG generates a fixed known number, say 0, under the preamble mode. This enables the reader to synchronize with the tag clock. In tag identifier mode, the PRNG generates *a priori* known pseudorandom numbers to transmit from the data stored in the tag's memory.

The system clock for the tag is derived from the narrowband carrier, which eliminates the need for a clock generator for the tag. It also makes the tag clock in synchronous with the reader clock, which simplifies the clock synchronization for the reader. The frame format in Figure 2 requires a carrier frequency of 1,048 MHz, in which the period of a time slot is 954 ps. If we employ standard 900MHz UHF tags operating at 900 MHz, the period of the time slot should be increased slightly.

In the following, we discuss the operation and implementation of the PRNG and of the pulse-position modulator. Next, we discuss several aspects related to the system timing such as system reset and clock synchronization.

B. Linear Feedback Shift Register

A key characteristic of our system is that its security does not come from a cryptographic operation, but from the inability to detect TH-UWB signals for an eavesdropper. We propose the use of a programmable LFSR as a pseudo-random number generator. By itself, an LFSR is not very useful as a cryptographic algorithm: the linear properties of an LFSR make it relatively simple to predict the next-state from a given set of previous states. However, we do not rely on the cryptographic properties of an LFSR for our system, but rather on the pseudorandom properties of an LFSR sequence.

We require that each tag has its own pseudorandom time-hopped sequence to ensure that the reverse engineering of a single tag (e.g. reverse engineering a tag's integrated circuit) cannot be used on another tag. Therefore, we use a *programmable* LFSR as illustrated in Figure 4. Using a programmable feedback pattern, we can choose the LFSR polynomial, defined as

$g(x) = 1 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 + x^5$ where f_i is 0 or 1.

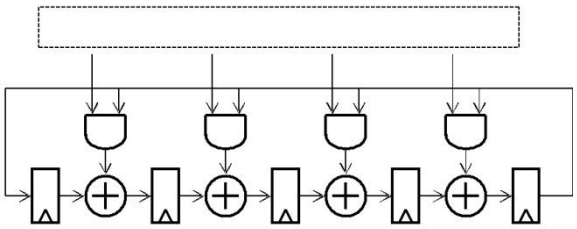


Figure 4: 5-bit programmable LFSR

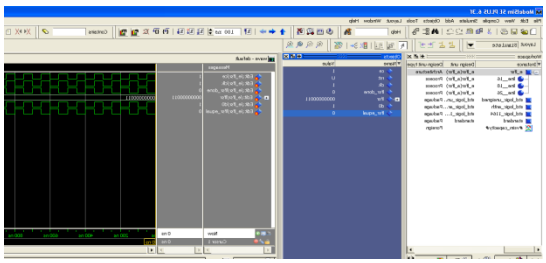


Figure 5– Simulation report for LFSR

An N-bit LFSR has 2^{N-1} possible feedback patterns, equivalently keys. The LFSR should generate a random number of 15 bits for each data bit at the clock rate of 16 KHz (whose period is 62.5 µs). So the LFSR should have at least 15 bits. As the number of bits increases, the size of the pool for possible keys also increases at the cost of higher silicon area. It is called a maximal-length sequence (m-sequence) if an N-bit LFSR goes through all

possible (2^N-1) states. Such an m-sequence is desirable for our RFID system, as it ensures that a pulse-position will not be reused within the next (2^N-1) transmitted bits. However, the number of keys for m-sequences is often a small set of all possible keys. For example, a 16-bit LFSR has 32,768 (=2^{15}) possible keys. Of those 32,768 patterns, 2,048 patterns result in m-sequences. Consequently, in an LFSR with sufficient bits, there will be plenty of choices that offer an m-sequence feedback-pattern. Our proposed architecture can support all possible sequences including m-sequences.

C. Pulse Position Modulator

The purpose of a pulse-position modulator (PPM) is to generate a required time delay to position a UWB pulse within a frame, i.e., a bit window. As mentioned earlier, a pulse appears only at the second half of a bit window, while the first half is used as a guard time. The guard time is necessary to ensure that two Consecutive pulses are apart by at least 31.3 µs. The guard time allows the power harvesting circuit to recharge in between pulses, and it also avoids inter-symbol interference between two consecutive UWB pulses. Within a 31.3 µs time window, the PPM has to implement a resolution of 2^{15} time steps, where a time step is 954 ps long, equivalently 1.048 GHz. A straightforward approach is to use a 15-bit counter running at 1.048 GHz, but this is a power-hungry solution. Figure 4 shows a distributed solution for the delay generation. The clock frequency of a stage *i* is running at two times the clock frequency of the stage (*i*+1). The rightmost stage 0 runs at the clock frequency of 1.048 GHz, while the leftmost stage 14 at 64 KHz. A stage *i* of the PPM chain delays the input signal E_i by one clock period, if p[*i*] = 0, and two clock periods if p[*i*] =1. So the total delay between E_{in} and E_{out} ranges from 2^{15}-1 time steps (when P[14..0] = 00…0) to 2^{16}-2 time steps (when P[14…0] = 11…1). The range ensures that a UWB pulse positions in the second half of a bit window. P[14..0] are the 15 bit UWB position information generated by the LFSR. The distributed solution minimizes the number of registers running at high clock speed, which saves power dissipation for the PPM. An open issue is the average power consumption of the pulse-position modulator.

Preliminary experiments with 0.18 µm CMOS technology have shown that the circuit in Figure 5 consumes almost 600 µW, with the very first stage at the highest clock consuming about half of that (298 µW), and subsequent stages each consuming half the power of the previous stage. Further reducing this power consumption is one of the key research issues for this design.

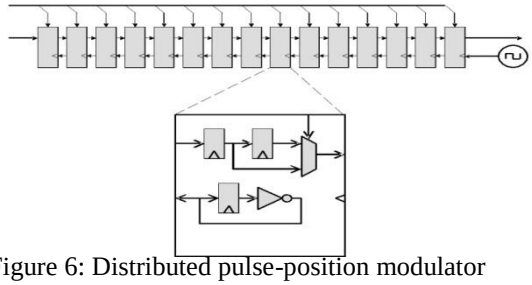


Figure 6: Distributed pulse-position modulator

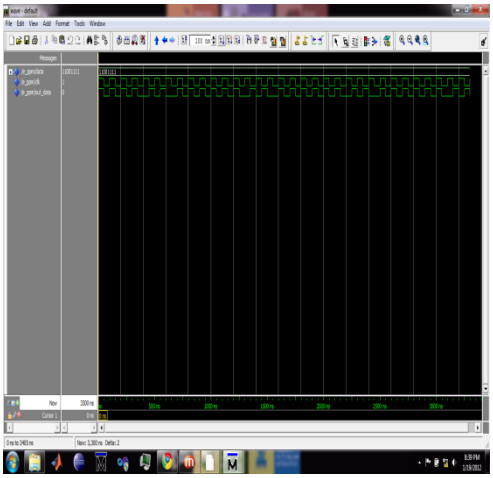


Figure 7: simumulation Report for PPM

CONCLUSIONS AND FUTURE WORK

We have proposed the use of UWB communications to implement secure RFID. Instead of encrypting data, we focus on making the communications difficult to eavesdrop. Our initial research findings show that the system is theoretically feasible and may be a valid alternative to solutions based on narrowband communications. While it is not possible to claim that secure UWB will perfectly resist attacks, we have shown that they are very difficult to mount. In addition, the eavesdropping protection offered by UWB is much cheaper in hardware and is complementary to traditional cryptography used in RFIDs.

The multiple access property of TH-PPM UWB can be explored for simultaneous reading of multiple tags, which can address the time-consuming process of reading one tag at a time for

present RFID systems. Also, UWB has better propagation properties than traditional narrowband communications. Further research is necessary to verify practicality of the proposed secure RFID system. First, the power budget should be analyzed to verify that the energy harvest from the narrowband receiver is sufficient to power necessary UWB circuits. Second, the strength of the security should be analyzed in conjunction with various methods of attacks. Third, as keys are hardwired for the proposed system, change and distribution of keys is more difficult than software based keys. An effective method for managing keys needs to be investigated as well.

REFERENCES

[1] U. Karthaus, M. Fischer, "Fully Integrated Passive UHF RFID Transponder IC With 16.7-μW Minimum RF Input Power," IEEE Transactions on Solid-State Circuits, 38(10):1602-1608, October 2003.

[2] K. Finkenzeller, "RFID Handbook: Radio Frequency Identification Fundamentals and Applications," Chapter 4 – Physical Principles of RFID Systems, John Wiley & Sons, 1999.

[3] I. Kirshenbaum, A. Wool, "How to build a low-cost, extended-range RFID skimmer," IACR eprint architecture 2006/054.

[4] K. Mahaffey, M. McGovern, P. Simmonds, J. Callas, "Long Range RFID and its Security Implications," presentation at BlackHat USA 2005, Las Vegas.

[5]L. Grunwald, "RFID and Smart Labels: Myths, Technology, and Hacks," BlackHat USA 2004, Las Vegas, July 2004.