

Implementation Of Ultrawide Band Radiation Securing Rfid

SRIDHAR RAJA D¹, B.KALAISELVI², ABINETHRI R³ T.VIJAYAN⁴

^{1, 2, 3, 4} Assistant Professor, Dept. of Electronics & Instrumentation

BIST, BIHER, BHARATH UNIVERSITY, Chennai – 73.

sridharraja.eie@bharathauniv.ac.in

Abstract: Current implementations of secure RFID rely on digital cryptographic primitives in the form of hashes and block ciphers. The presence of these blocks is motivated by privacy requirements, but they increase the overall processing latency, the power consumption, and the silicon area budget of the RFID tag. In addition, existing passive RFID systems rely on simple coding and modulation schemes using narrowband radio frequencies, which can be easily eavesdropped or jammed. We propose to implement the link from RFID to reader using ultra-wideband (UWB) communications. We show that the use of an advanced modulation scheme offers a new approach to the secure RFID problem. By using the modulation spreading code as a secret parameter of the communications link, we can make eavesdropping extremely difficult and increase the communication reliability. We also show that it decreases the latency and the risk for side-channel attacks. We present the digital base band architecture of a passive UWB-RFID that uses time-hopped pulse-position modulation (TH-PPM) and present area- and power estimates that are competitive to solutions using digital cryptography.

Keywords: RFID, UWB, PPM, Time-Hopped Pulse Position Modulation.

1 INTRODUCTION

Passive RFID capture and reuse incoming radio-frequencies to power internal circuitry and to respond back to the RFID reader. The available RF power of the reader-transponder system is constrained at both sides of the link, either by regulations or else by technological limits. A typical example of an UHF (900 MHz) tag enables a power budget of 150 μ W for a tag located at 2 meters from a reader that uses a 500mW transmitter [1-5]. Current systems implement a half-duplex link between reader

and tag. The reader sends a power-carrying RF carrier to the tag, adding additional data by means of amplitude modulation. The reverse link, from tag to reader, is based on adaptive reflection (backscatter) of the phase of the incoming RF carrier, or on adaptive loading [2]. In both directions a narrowband signal is used, with a bandwidth much smaller than the carrier frequency. These communication schemes have been developed with simplicity in mind. They are susceptible to passive attacks such as eavesdropping [3][4][8] and active attacks [5]. In recent years, many proposals have been made to address the privacy issues related to such tags, as well to extend their application domain to include authentication besides detection [6, 10, 12, 13]. All of these proposals are enhancements at either the protocol-level. They make the implicit assumption that the communications link between tag and reader can be eavesdropped and thus that privacy must be guaranteed by the data link layer. Many of these proposals rely on digital block ciphers or hashes. Indeed it has been shown that traditional digital cryptography can be implemented within typical implementation constraints of passive tags. A Feldhofer present an implementation of AES of 3595 equivalent NAND gates that consumes 8.5 μ W [611]. This shows that symmetric-key implementations can meet area and power constraints of tags. A similar conclusion, made for the case of low-frequency tags (13.56MHz), can be found.

In recent years, many schemes have been proposed to address the privacy issues related to such tags, as well to extend their application domain to include authentication besides detection [6, 10, 12, 13]. All of these proposals are enhancements at either the protocol-level or the algorithm-level of the communications link. They assume implicitly that the communications link between a tag and a reader can be eavesdropped and thus that privacy must be

guaranteed by the data link layer. Many of these proposals rely on digital block ciphers or hashes. It was shown that traditional digital cryptography can be implemented within typical implementation constraints of passive tags. Feldhofer presents an implementation of AES of 3,595 equivalent NAND gates that consumes 8.5 μ A [14-16]. This shows that symmetric-key implementations can meet area and power constraints of tags. A similar conclusion, made for the case of low-frequency tags (13.56MHz), can be found in [17-21]. However, the use of digital cryptography in a power- and silicon-area constrained RFID tags comes with cost. The presence of digital ciphers in RFID tags increases their response-time. A high cycle count combined with a low operating frequency results in substantial computation times for these ciphers. For example, the AES implementation discussed in [22-25] requires 995 cycles. At a tag clock frequency of 1 MHz, one round of encryption takes close to 1 ms. The new Gen-2 tags take 1.6 ms to transmit a 128-bit tag [9]. Consequently, the tag encryption time is of the same order of the transmission time of the encrypted result. This latency reduces overall system throughput and may violate the constraints of the standard [26-30]. In addition, a tag's computation and communication periods are clearly separated in time, making it easier to mount a power analysis side-channel attack that focuses on the cipher [31-36]. Recent work in so-called 'light-weight' protocols tries to alleviate the requirements of encryption or even to eliminate them altogether. The HB+ protocol, for example, uses a protocol modelled after human authentication [10]. It uses repeated challenges directly derived from the shared key K. Unfortunately; the HB+ protocol was not resistant against active attacks [37-40]. Using a man-in-the-middle attack, an attacker is able to reveal a single chosen key-bit per challenge response iteration. Besides HB+, several other proposals have been presented recently, all of which use a cryptographic primitive (hash function or cipher). The hash-lock scheme from Sarma and Weis [12] uses the concept of a lock based on hash-functions. The YA-TRAP protocol from Tsudik [41-45] relies on time stamping RFIDs and a hash function to prevent unauthorized tracking. Most existing secure RFID tags therefore still rely on cryptographic primitives, either in the reader or else in the tag. This is unavoidable as current systems implicitly

assume that communications can be eavesdropped at will.

2. ULTRA WIDEBAND MODULATION SCHEME

In this paper, we propose to use physical communications as a new dimension in the reader-tag system design to implement those secure protocols. We propose to secure physical communications based on ultra-wideband (UWB) modulation and time-hopping. Rather than encrypting the tags' identifier, we use a private modulation code, specifically time hopping sequence. Only a receiver who knows the hopping sequence is able to receive the overall message. Our approach offers the following benefits over existing secure RFID tags.

- UWB transmissions are very difficult to eavesdrop because of their low power-level.
- Secure-UWB modulations do not require data encryption. As will be seen later, eavesdropping on a 15-bit secret modulation code requires prohibitively powerful communications equipment, which is impractical.
- Secure-UWB tags have low latency, and are able to respond much faster to a reader.
- UWB transmissions are more robust to interference than narrowband transmissions. They are difficult to jam and allow multiple transmissions in the same band.

In this paper, we present a protocol for secure RFID tags based on a UWB modulation scheme and its implementation in the baseband signal processing. In Section 2, we briefly review the properties of ultra wideband modulation, and discuss our proposed time hopped pulse-position modulation.

2.1 ULTRA-WIDEBAND RFID

2.1.1 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 to 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 $B \log_2(1+\text{SNR})$, 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. UWB signaling can be carrier-based or impulse based, and impulse-based UWB is more suitable for the RFID due to its simple hardware. Impulse-based UWB is based on a train of narrow pulses (which are typically a few tens to hundreds picoseconds wide). Various modulation schemes such as on-off keying, pulse amplitude modulation, pulse position modulation (PPM), and binary phase shift keying are available for UWB. A binary PPM scheme has 2 distinctive time positions in a time slot, and one pulse carries 1 bit of information. We adopt PPM due to its low hardware complexity [18]. A k -bit time hopping PPM (TH-PPM) allocates $2k$ time slots for each bit and hops time slots between pulses. Figure 1(a) shows an example THPPM scheme with four time slots in each frame. The first pulse occupies the second time slot, the second pulse the first slot, and the third pulse the fourth slot in the figure. Like any other PPM, the position of a pulse within a time slot carries the information bit for THPPM. For example, a pulse aligned to the start of a slot represents logic 0 (Figure 1(b)). A pulse delayed by Δ with respect to the start of a time slot carries logic 1

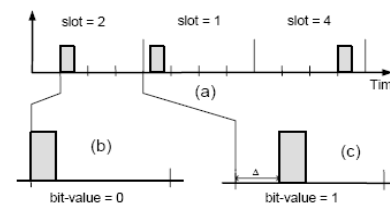


Figure 1: Time-Hopped Pulse-Position Modulation

Time-hopping has been used in communications for two purposes; multiple access and/or spreading of the spectrum. We introduce a new application of time-hopping, which is to secure physical layer communications. This is possible as explained following. To demodulate extremely narrow UWB pulses, a receiver should correlate incoming pulse signals with a template signal. The time slot of an incoming pulse is known *a priori* for a conventional TH-PPM scheme. The receiver performs two correlations starting at two different instances, one at $t=0$ as for the case in Figure 1(b) expecting a logic value 0 for the incoming signal and the other at $t=\Delta$ as in Figure 1(c) expecting logic 1. One of the two correlation operations will capture the received signal energy, while the other one will only correlate noise. If the time slots of pulses are assigned in a pseudo random manner, the eavesdropper should perform correlations for all possible time slots. If the total number of time slots is sufficiently large, eavesdropping of TH-PPM communications is practically impossible.

2.1.2 Frame format for our RFID system

We now discuss the data framing for our secure RFID system. Figure 2 illustrates a super frame for the transmission of a single ID. The transmission completes within 10 ms, similar to present-day no secure RFIDs. The super frame contains a 2 ms preamble and an 8 ms data-field. The preamble contains 32 known bits, which occupy the same time slot within each frame. The purpose of the preamble is to synchronize the reader. Next, a pulse train of 16 bits for the initial state of the random number generator (which is omitted in the figure for simplicity) and 128 bits for the identifier of a tag follows. Each bit uses a different pseudorandom time slot within a frame. The period of a frame, i.e., time window of a single bit, is $62.5 \mu\text{s}$, and a frame contains 216 ($=65,536$) time slots, each slot being 954 ps long. Among the available 65,536 time slots, a UWB pulse actually positions at the

second half of the frame, and the first half of the frame, 32,768 time slots or 31.3 μs , serves as guard time. This slot length is long enough for a UWB pulse not to interfere with the pulse from the following time slot.

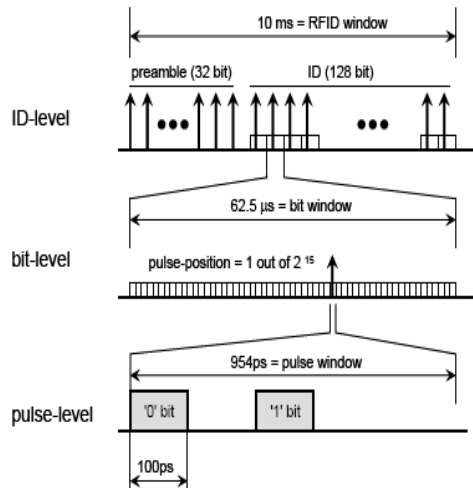


Figure 2: UWB frame format

3. ARCHITECTURE FOR AN ULTRA-WIDEBAND RFID

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

3.1 UWB-RFID tag architecture

Figure 3 illustrates the architecture of our UWBRFID 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. The pulse rate of 16 KHz adopted for our system is more than three orders of magnitude lower

than that, which would push average power consumption in the μW range. Lee and et al. proposed a UWB pulse generator constructed of a simple logic circuit, in which glitches of digital logic are used as UWB pulses [20]. Such a low-power pulse generator would be suitable for the proposed system.

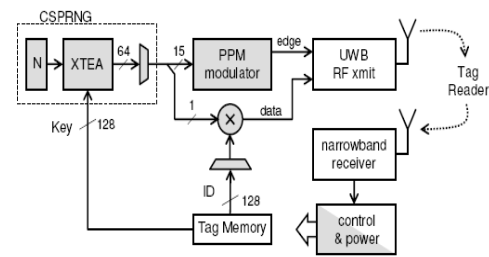


Figure 3: System architecture of a passive UWB RFID Tag

The digital baseband generates a pulse-position modulated signal for the UWB frontend. The pulse positions are selected by means of a cryptographically secure pseudo-random number generator (CSPRNG). Since the CSPRNG is used to select the modulation code rather than for strong encryption, we can opt for a simple block cipher operating in output feedback (OFB) mode, which provides less area and cycle count overhead when compared with strong cipher such as AES. For the framing format defined in Figure 2, a 16-bit block cipher would have been adequate. Since no standard ciphers are available with this block-length, we selected instead an existing 64-bit cipher (XTEA) and used the output of each encryption round for four subsequent UWB pulse-positions. The most significant bit of each number of the pseudo-random sequence is used to encrypt the data bit. This is done to circumvent an eavesdropping attack on a fixed timeslot. Note that we only used 15 bits to select the timeslot, i.e., in our current implementation we position UWB pulse over only half the range of a $62.5 \mu\text{s}$ timeslot. We will show that this considerably relaxes the timing constraints on the baseband implementation, and it limits the peak power consumption of the UWB front-end. In the following, we will discuss the operation and implementation of the CSPRNG and of the pulse-position modulator. Next, we will discuss several aspects related to the system timing, and propose a reader-tag communication protocol to synchronize the CSPRNG.

3.2 Pulse-position modulator

The purpose of the pulse-position modulator is to generate precise time delays and communicate the location of UWB pulses to the UWB front-end transmitter. Within a 62.5 μ s time window, the PPM has to implement a resolution of 216 time steps, which corresponds to 954ps per step. This resolution prohibits us to use a counter-based approach in generating the delays, since the counter would have to be run at 1.048GHz. Figure 4 shows a distributed solution to delay generation. Each stage of the PPM chain implements a single bit of delay, equal to either one or two clock periods of that stage. In addition, each stage generates a divided clock for the next (earlier) stage. The delay contribution of each stage will thus increase in powers of 2. This way, the design minimizes the number of registers that run at high clock speed. We opted to introduce at least one period of delay per stage since this enables us to pipeline the entire pulse-position modulator. The complete chain includes 15 stages, which have clocks from 1.048GHz to 64 KHz.

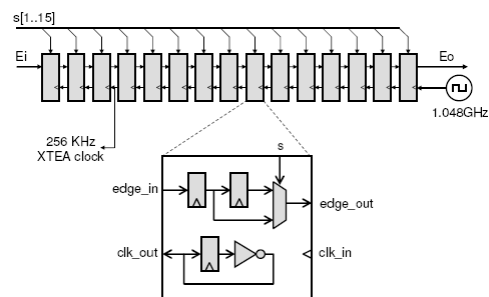


Figure 4: 15-bit Pulse Position Modulator with 1ns resolution

The delay generated by the PPM is defined in terms of a 15-bit input number S:

$$\Delta = C \left(1 + \frac{S}{2^{15}} \right)$$

$$C = 31.25\mu s - 954ps$$

Figure 5 shows the relationship between the input and output signals of the PPM. The input signal is a 15.625 μ s pulse created by the controller. The delay chain delays this signal between a half and a full bit window based on the delay parameter S. Therefore, two subsequent UWB pulses will always be

separated at least half a bit window apart, and the immediate UWB pulse rate cannot exceed 32 KHz. This limits the peak power consumption of the UWB front-end.

4. 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 first results show that the system is technically feasible and a valid alternative to solutions based on narrowband communications. We are presently refining our concept and the system parameters. We are also considering how UWB can be used to cover other RFID applications as well. In particular, the multi-access properties of UWB will be useful to define more efficient approaches to the time-consuming simulation process of present RFID systems. Second, UWB has better propagation properties than traditional narrowband communications. We thus envisage UWB RFID to be useful in environments that are unsuited for small-band tags.

5. REFERENCES

1. Nimal, R.J.G.R., Hussain, J.H., Effect of deep cryogenic treatment on EN24 steel, International Journal of Pure and Applied Mathematics, V-116, I-17 Special Issue, PP-113-116, 2017
2. Parameswari, D., Khanaa, V., Deploying lamport clocks and linked lists, International Journal of Pharmacy and Technology, V-8, I-3, PP-17039-17044, 2016
3. Parameswari, D., Khanaa, V., Case for massive multiplayer online role-playing games, International Journal of Pharmacy and Technology, V-8, I-3, PP-17404-17409, 2016
4. Parameswari, D., Khanaa, V., Deconstructing model checking with hueddot, International Journal of

- Pharmacy and Technology, V-8, I-3, PP-17370-17375, 2016
5. Parameswari, D., Khanaa, V., The effect of self-learning epistemologies on theory, International Journal of Pharmacy and Technology, V-8, I-3, PP-17314-17320, 2016
 6. Pavithra, J., Peter, M., Gowtham Aashirwad, K., A study on business process in IT and systems through extranet, International Journal of Pure and Applied Mathematics, V-116, I-19 Special Issue, PP-571-576, 2017
 7. Pavithra, J., Ramamoorthy, R., Satyapira Das, S., A report on evaluating the effectiveness of working capital management in googolsoft technologies, Chennai, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-129-132, 2017
 8. Pavithra, J., Thooyamani, K.P., A cram on consumer behaviour on Mahindra two wheelers in Chennai, International Journal of Pure and Applied Mathematics, V-116, I-18 Special Issue, PP-55-57, 2017
 9. Pavithra, J., Thooyamani, K.P., Dkhar, K., A study on the air freight customer satisfaction, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-179-184, 2017
 10. Pavithra, J., Thooyamani, K.P., Dkhar, K., A study on the working capital management of TVS credit services limited, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-185-187, 2017
 11. Pavithra, J., Thooyamani, K.P., Dkhar, K., A study on the analysis of financial performance with reference to Jeppiaar Cements Pvt Ltd, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-189-194, 2017
 12. Peter, M., Dayakar, P., Gupta, C., A study on employee motivation at Banalari World Cars Pvt Ltd Shillong, International Journal of Pure and Applied Mathematics, V-116, I-18 Special Issue, PP-291-294, 2017
 13. Peter, M., Kausalya, R., A study on capital budgeting with reference to signware technologies, International Journal of Pure and Applied Mathematics, V-116, I-18 Special Issue, PP-71-74, 2017
 14. Peter, M., Kausalya, R., Akash, R., A study on career development with reference to prem heera surgicals, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-415-420, 2017
 15. Peter, M., Kausalya, R., Mohanta, S., A study on awareness about the cost reduction and elimination of waste among employees in life line multispeciality hospital, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-287-293, 2017
 16. Peter, M., Srinivasan, V., Vigneshsa, A., A study on working capital management at deccan Finance Pvt Limited Chennai, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-255-260, 2017
 17. Peter, M., Thooyamani, K.P., Srinivasan, V., A study on performance of the commodity market based on technical analysis, International Journal of Pure and Applied Mathematics, V-116, I-18 Special Issue, PP-99-103, 2017
 18. Philomina, S., Karthik, B., Wi-Fi energy meter implementation using embedded linux in ARM 9, Middle -

- East Journal of Scientific Research, V-20, I-12, PP-2434-2438, 2014
19. Philomina, S., Subbulakshmi, K., Efficient wireless message transfer system, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-289-293, 2017
 20. Philomina, S., Subbulakshmi, K., Ignition system for vehicles on the basis of GSM, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-283-286, 2017
 21. Philomina, S., Subbulakshmi, K., Avoidance of fire accident by wireless sensor network, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-295-299, 2017
 22. Pothumani, S., Anuradha, C., Monitoring android mobiles in an industry, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-537-540, 2017
 23. Pothumani, S., Anuradha, C., Decoy method on various environments - A survey, International Journal of Pure and Applied Mathematics, V-116, I-10 Special Issue, PP-197-199, 2017
 24. Pothumani, S., Anuradha, C., Priya, N., Study on apple iCloud, International Journal of Pure and Applied Mathematics, V-116, I-8 Special Issue, PP-389-391, 2017
 25. Pothumani, S., Hameed Hussain, J., A novel economic framework for cloud and grid computing, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-5-8, 2017
 26. Pothumani, S., Hameed Hussain, J., A novel method to manage network requirements, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-9-15, 2017
 27. Pradeep, R., Vikram, C.J., Naveenchandra, P., Experimental evaluation and finite element analysis of composite leaf spring for automotive vehicle, Middle - East Journal of Scientific Research, V-12, I-12, PP-1750-1753, 2012
 28. Pradeep, R., Vikram, C.J., Naveenchandra, P., Experimental evaluation and finite element analysis of composite leaf spring for automotive vehicle, Middle - East Journal of Scientific Research, V-17, I-12, PP-1760-1763, 2013
 29. Prakash, S., Jayalakshmi, V., Power quality improvement using matrix converter, International Journal of Pure and Applied Mathematics, V-116, I-19 Special Issue, PP-95-98, 2017
 30. Prakash, S., Jayalakshmi, V., Power quality analysis & power system study in high voltage systems, International Journal of Pure and Applied Mathematics, V-116, I-19 Special Issue, PP-47-52, 2017
 31. Prakash, S., Sherine, S., Control of BLDC motor powered electric vehicle using indirect vector control and sliding mode observer, International Journal of Pure and Applied Mathematics, V-116, I-19 Special Issue, PP-295-299, 2017
 32. Prakesh, S., Sherine, S., Forecasting methodologies of solar resource and PV power for smart grid energy management, International Journal of Pure and Applied Mathematics, V-116, I-18 Special Issue, PP-313-317, 2017
 33. Prasanna, D., Arulselvi, S., Decoupling smalltalk from rpcs in access points, International Journal of Pure and Applied Mathematics, V-116, I-16 Special Issue, PP-1-4, 2017

34. Prasanna, D., Arulselvi, S., Exploring gigabit switches and journaling file systems, International Journal of Pure and Applied Mathematics, V-116, I-16 Special Issue, PP-13-17, 2017
35. Prasanna, D., Arulselvi, S., Collaborative configurations for wireless sensor networks systems, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-577-581, 2017
36. Priya, N., Anuradha, C., Kavitha, R., Li-Fi science transmission of knowledge by way of light, International Journal of Pure and Applied Mathematics, V-116, I-9 Special Issue, PP-285-290, 2017
37. Priya, N., Pothumani, S., Kavitha, R., Merging of e-commerce and e-market-a novel approach, International Journal of Pure and Applied Mathematics, V-116, I-9 Special Issue, PP-313-316, 2017
38. Raj, R.M., Karthik, B., Effective demining based on statistical modeling for detecting thermal infrared, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-273-276, 2017
39. Raj, R.M., Karthik, B., Energy sag mitigation for chopper, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-267-270, 2017
40. Raj, R.M., Karthik, B., Efficient survey in CDMA system on the basis of error revealing, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-279-281, 2017
41. Rajasulochana, P., Krishnamoorthy, P., Ramesh Babu, P., Datta, R., Innovative business modeling towards sustainable E-Health applications, International Journal of Pharmacy and Technology, V-4, I-4, PP-4898-4904, 2012
42. Rama, A., Nalini, C., Shanthi, E., An iris based authentication system by eye localization, International Journal of Pharmacy and Technology, V-8, I-4, PP-23973-23980, 2016
43. Rama, A., Nalini, C., Shanthi, E., Effective collaborative target tracking in wireless sensor networks, International Journal of Pharmacy and Technology, V-8, I-4, PP-23981-23986, 2016
44. Ramamoorthy, R., Kanagasabai, V., Irshad Khan, S., Budget and budgetary control, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-189-191, 2017
45. Ramamoorthy, R., Kanagasabai, V., Jivandan, S., A study on training and development process at Vantec Logistics India Pvt Ltd, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-201-207, 2017

