Integrated CMOS Active Low-Pass Filter for IoT RFID Transceiver

Mahfuzur Rahman[1], Md. Faishal Rahaman[1], Md. Moazzem Hossan Munna[1], Kelvin Jian Aun Ooi[2], Khairun Nisa' Minhad[2], Mohammad Arif Sobhan Bhuiyan[2(✉)], and Mahdi H. Miraz[2(✉)]

[1] Southern University Bangladesh, Chittagong, Bangladesh
[2] Xiamen University Malaysia, Sepang, Malaysia
arifsobhan.bhuiyan@xmu.edu.my, m.miraz@ieee.org

Abstract. While providing unique identity to the objects, analogous to wireless sensor network (WSN) technologies, radio frequency identification (RFID) technology can be used to automate data collection and thus can significantly limit human involvements as well as errors. Therefore, utilisation and implementation of RFID technology in multifaceted applications has recently been widely observed. In the modern internet of things (IoT) radio frequency identification (RFID) transceivers, the low pass filter (LPF) circuits play an important role to suppress the unwanted high frequency signals and noises. The LPF circuit performance greatly influences the overall performance of the transceivers. However, the passive types of LPFs in modern devices highly suffer from several drawbacks such as low-quality factors, less tuning ability, unwanted harmonic interruptions and the large die size. On the contrary, active types of low pass filters can resolve these limitations to some extent. Therefore, this research presents an active LPF design for 90 nm complementary metal oxide semiconductor (CMOS) technology in Cadence environment. The simulation results reveal that the proposed active low pass filter can achieve 6.5 dB gain with 35.48 MHz bandwidth while having 20.87 dB noise figure. The designed circuit consumes 1.56 mW power from a 1.3 V DC supply, for its smooth operation. The core die size of the proposed LPF is only 85.29 μm^2 and therefore, suitable for compact modern transceiver applications.

Keywords: CMOS · Inductorless · IoT · LNA

1 Introduction

The advancement of technology has opened new horizons for mankind by conceiving and materialising the concept of IoT which is considered as the next step in the internet revolution. The incorporation of the Internet with next generation radio communication technologies as well as embedded wireless sensor networks is notably playing a vital role in the paradigm shift of connecting our everyday devices through the Internet and transforming them into the 'smart' ones - intelligent and context-aware. As we keep on

M. H. Miraz et al. (Eds.): iCETiC 2021, LNICST 395, pp. 73–84, 2021.
https://doi.org/10.1007/978-3-030-90016-8_5

forwarding, IoT is expected to find its place in almost all facets of human life where everything will be connected through a wireless network for exchanging information amongst different nodes in real-time, to facilitate fast and accurate decision making, as shown in Fig. 1. Today's smart world, comprising various smart aspects such as smart health-care, homes, offices, traffics, cities, industries, etc., makes the best use of this technology for a better present and future.

In fact, the twenty-first century is perceived as the IoT-enabled era, leveraged with a network of networks comprising multifaceted smart devices powered by both hardware and software. All IoT devices, ranging from household to industry, should be distinctively identifiable through an embedded system and be connected from everywhere, to provide with better services and greater values [1–3]. Therefore, it has become a dire necessity to ensure a completely seamless, highly secure and exceedingly efficient IoT network facilitating multidimensional information technology (IT) services [1, 4], such as data integration and analysis from diverse sources, comprehensive security, scalability and flexibility, device diversity, management and power efficiency, etc. Apart from these, as the volume of the IoT network is rapidly growing, to uniquely identify each device from billions of devices has becoming a big concern. As a consequence, the current radio frequency identification (RFID) standard, protocol, hardware, and security are required to be modified and/or adapted to satisfy the requirements of IoT devices [5].

Fig. 1. The IoT is everywhere [6].

To simply put, Radio frequency identification (RFID) is a very broad term representing a system which transmits wireless signals, particularly electromagnetic radio waves, containing the unique identity of any object. RFID enables identification from a certain distance and unlike barcode technology, it does not require line of sight. The technology comprises mainly transponders (or tags) and readers, as shown in Fig. 2. The transponder, which is fundamentally an integrated circuit (IC) with an antenna, stores information about its identification along with some additional information which is, generally, transferred to the reader on request. In RFID communication, a reader receives data from the transponders wirelessly using different frequency bands which are decided by the respective nature of the applications. Currently, RFID operating frequencies, ranging from 30 to 300 kHz (commonly known as low frequency (LF)) and 3 MHz to 30 MHz (commonly known as high frequency (HF)), are widely used in industrial applications. 300 MHz

to 3 GHz band, referred to as Ultra-high-frequency (UHF), RFID mainly operates at 900 MHz and using smaller antenna it delivers comparatively a higher data rate than HF. Other frequencies, such as 2.45 GHz and 5.8 GHz, which have smaller antennae and are suitable for less populated frequency ranges, are also suggested for RFID operation [7].

Semi-passive of semi-active transponders may optionally be equipped with embedded battery. However, in such cases the battery is primarily utilised in order to administer the chip. Analogous to the functionalities of an active tag, the energy harvested from the electromagnetic field is used for waking up the chip as well as transmitting the data to the reader. The semi-passive or semi-active tags are occasionally called battery-assisted passive tags [8].

A passive tag is batteryless and uses the energy induced by the electromagnetic wave propagated by the antenna of the reader, in order to powering up the chip as well as for transmitting the data to the reader. A passive tag reflects the energy obtained from the reader or receives and momentarily stores the energy in order to process the response [9].

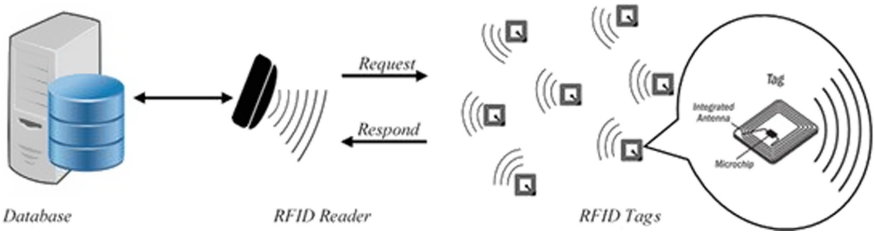

Fig. 2. The RFID communication [10].

The RFID systems use varying frequencies for different purposes that require various types of receivers. As per the findings of a survey conducted by NECTEC, the delay in the deployment of RFID occurred due to four (4) determinants: RFID standard, cost, technology aptness as well as lack of knowledge [11]. For efficient data transmission, the level of security of an RFID network is reduced considering the resource scarcity of the technology. Therefore, user privacy remains as a major concern. The reader, of an RFID eco-system, is the most expensive component. For instance, the cost of a small automated materials handling (AMH) can be US $50,000 [12]. Moreover, a limitation is placed on RFID tag implementation when the reader is used. However, such shortcomings can easily be subdued by deploying wireless network interface card (WNIC). With the use of Wi-Fi networks and an internet protocol version 6 (IPv6) address as tag ID, a novel RFID tagging system has been introduced [13]. The electronic product code (EPC) of a transponder is mapped with the interface ID (64 bit) of an IPv6 address as a unique identifier of an object. However, the implementation of a readerless RFID system should ensure several factors, such as privacy, standards, data management, mobility and scalability [14].

In RFID ecosystems, an identification number is required to track any product or object. This number should be unique to ensure security and proper communication. Therefore, a new global address structure is necessary for RFID systems. In fact, IPv6

addressing scheme, which establishes object-to-object communication, can be utilised to serve this purpose. EPC, extended unique identifier (EUI)-64, uniform resource identifier/locator (URI/URL), medium access control (MAC) addresses, etc. are examples of identification codes. In fact, for energy efficient communications amongst the nodes of WSN/IoT networks, MAC protocol has been the principal target for finding the most optimised and appropriate adaptive approach [15]. Moreover, most identification codes utilise large numbers and thus, require voluminous addressing schemes. IPv6 (128 bits) addressing scheme is becoming an essential future network infrastructure because of its large address space. IPv6 uses a unique local address with an anycast communication scheme, which exhibits service discovery and self-organisation via auto-configuration. Furthermore, making use of IPv6 header information, improved service capabilities were achieved. Moreover, IPv6 addressing scheme facilitates multi-homing. A fusion of IPv6 with wireless systems, such as the IEEE 802.11 protocol (Wi-Fi), will reduce the current problems of dual scarcity in the internet protocol version 4 (IPv4) addressing scheme, i.e. security and quality of service (QoS) from the IP side as well as spectrum and bandwidth limitations from the wireless side. IPv6 is set to gradually supersede IPv4 while providing end-to-end connections utilising 128-bit addressing scheme. It also possesses the potentials to eliminate IPv4's scalability problem due to address depletion. Moreover, IPv6 exhibits scalability, mobility, security and multicast/anycast features, thereby making it an in-demand addressing scheme at present.

Instead of using an RFID reader, the modified system presented in [13] can simply use WNIC to receive information from the mapped EPC–IPv6 transponder. The proposed system eliminates the need for an expensive vendor-specific RFID reader and provides a global ID number to every object. An IPv6 address format is subdivided into two portions. The initial 64 bits represent the subnet, whereas the remaining 64 bits represents the interface/device ID. The subnet or network prefix is used to signify the 'physical' location predefined by the router. An interface/device ID is required in order to uniquely identify or tracking any object. A simple algorithm is used to generate a modified EUI-64 by converting a MAC address. In this algorithm, the seventh bit of the MAC address, which is also known as the global flag, is reversed. Then extra bits are placed in between the third and the fourth bytes of the address. This modified version of the address, i.e. the EUI-64 address, is then utilised as the interface ID, the second part of an IPv6 addressing scheme.

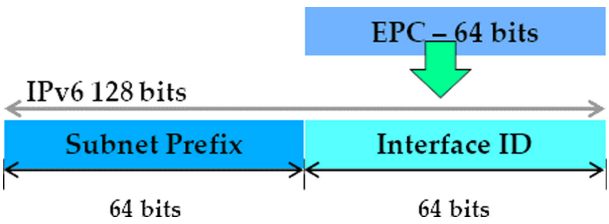

Fig. 3. The IoT RFID mapping with EPC [16].

Similarly, EPC-64 bits can be inserted into the IPv6 addressing scheme to be utilised as an interface ID in a readerless RFID system. Thus, the product information inside

EPC-64 bits will be held by the IPv6 address structure to track any product destination information. Figure 3 shows the modified address structure after the later 64 bits being replaced by the EPC-64 bits. In this manner, all the product information previously held by the EPC will be mapped directly onto the interface ID part of the IPv6 addressing scheme [16]. Thereafter, this modified and mapped address should be stowed in the RFID transponder memory, which can be a non-volatile memory, such as electrically erasable programmable read-only memory (EEPROM). In this way, each of the RFID tags become addressable in any IPv6 networks, providing provisions for physical location identification too.

Figure 4 shows the communication procedure through IEEE 802.11b between an RFID tag with the mapped EPC–IPv6 address structure and a computer with WNIC. The RFID tag will store the entire EPC–IPv6 address by using the mapping mechanism of this address. The RFID tag can be consigned to a range of 1–100 m in the industrial, scientific and medical (ISM) frequency band of 2.4 GHz. When an IPv6 RFID tag enters a Wi-Fi network, the system that contains WNIC will recognize it. First, WNIC will broadcast a message and all the RFID tags in that Wi-Fi network will receive this message. After receiving the message, the RFID transponder will send the acknowledgment packet. WNIC will then obtain the RFID transponder IP address from the acknowledgment packet [17].

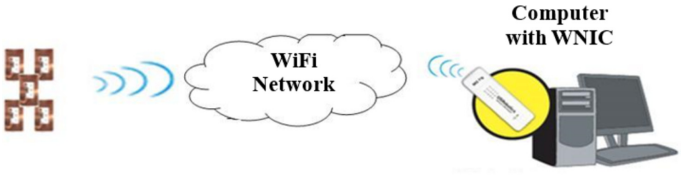

Fig. 4. The communication procedure through IEEE 802.11b between an RFID tag with the mapped EPC–IPv6 address structure and a computer with WNIC.

Figure 5 exhibits the fragment of an IoT RFID front-end. In such arrangement, along with other circuits., a low pass filter (LPF) is considered as a very substantial block which suppresses every type of undesirable signals or noises [18]. An LPF design requires a tank circuit to customise the cut-off window. However, on-chip inductors are not advisable to be utilised, due to immoderate loss and comparatively bigger die size [19–22]. As the inductors are an inherent part of amplifier and filter design, CMOS based active inductors are being introduced in order to overcome the shortcomings of the on-chip inductors [23].

The downscaling of integrated circuits (IC) technology allow the designers to design low-power, low-cost but compact wireless communication systems [24–27]. A low pass filter is an inherent block for all the modern transceivers. The LPF performance determines the overall transceiver functionality. Therefore, this research proposes a completely integrated active inductor based low pass filter design in Generic Process Design Kit (GPDK) 90 nm CMOS process for IoT RFID transceiver applications.

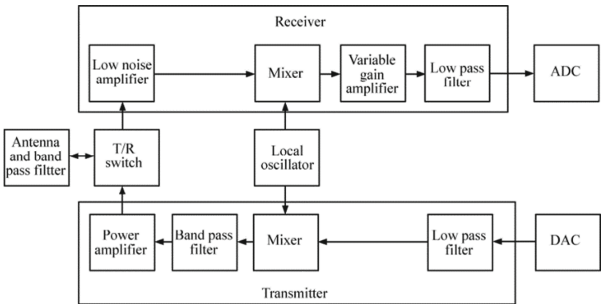

Fig. 5. The front-end block diagram for the design of IoT-RFID [24].

2 Proposed LPF

In conventional low pass filter design, inductors and resistors are generally used. The structure of the low pass filter usually adopts conventional resistive feedback method since it experiences high power consumption as well as parasitic capacitance at high frequencies. The proposed LPF is designed in three successive steps: common gate input buffer, active inductor based tank circuit and common drain output buffer as illustrated in Fig. 6.

Fig. 6. The realisation of the LPF.

The common gate input buffer, as demonstrated in the schematic in Fig. 7, has a good impedance match characteristic. In this structure, the bottom NMOS (M11) functions as a simple MOS resistor whereas the top transistor M8 adjusts the input impedance through its transconductance. The biasing voltages (Vb and V2) keep both the transistors in 'on state' for smooth operation of the LPF.

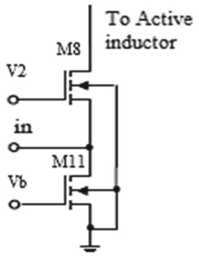

Fig. 7. Common gate input buffer.

The input buffer is followed by the frequency decisive tank circuit which consists of a double feedback active inductor as shown in Fig. 8 [28]. To satisfy the gyrator-capacitor model, in this active inductor, M3 and M4 act as non-inverting transconductors (gM1) whereas M2 act as an inverting transconductor (–gM2). Therefore, -gM2 and gM1 constitute the gyrator. This gyrator builds up the inductor at node 1 because of the parasitic capacitances at node 3. The equivalent RLC circuit is presented in Fig. 8.

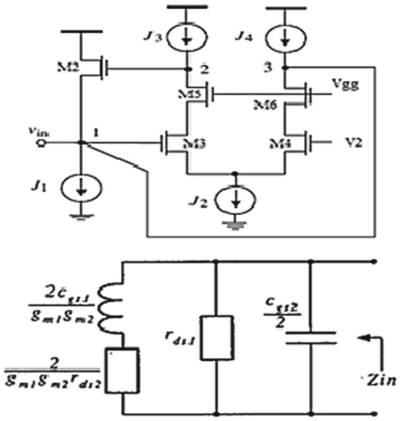

Fig. 8. Double feedback active inductor and its equivalent [27].

The final stage of this LPF is the common drain output buffer which offers a very small impedance, suitable for accomplishing a better output impedance matching. In the output buffer, as shown in the schematic diagram in Fig. 9, the transistor M10 functions as an active resistor. Figure 10 exhibits the final schematic diagram of the proposed LPF. In this LPF, adjusting the aspect ratio of the transistors M2, M3, M4, M8 and M10 results in the adjustment of the LPF gain and NF. However, a compromise has been made to these transistor aspect ratios to reach the best trade-off between the gain and the minimum NF. The W/L ratios of the transistors are presented in Table 1, the biases are set as V1 = 0.60 V, V2 = 0.40 V and Vgg = 0.80 V.

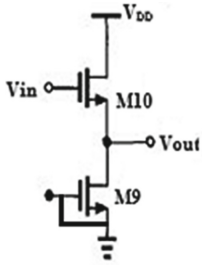

Fig. 9. Common drain output buffer.

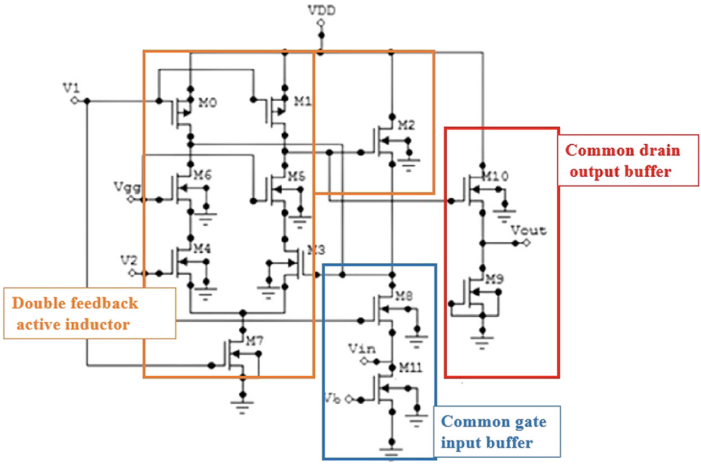

Fig. 10. LPF schematic circuit.

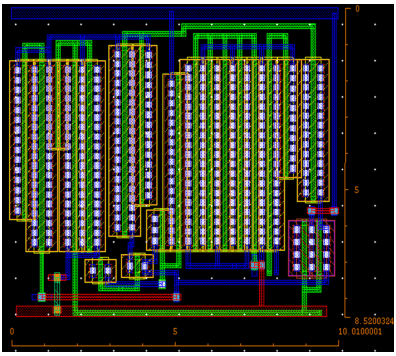

Fig. 11. LPF core layout.

Table 1. Transistors' W/L Aspect Ratio for the LPF.

Transistors	W/L ratio (μm/μm)
M0, M1	1.27/0.13
M2	0.84/0.13
M3, M4	9.11/0.13
M5, M6	0.36/0.13
M7	12.15/0.13
M8	3.66/0.13
M9	25/0.13
M10	4.58/0.13
M11	8/0.13

The LPF's core layout has been designed utilising the EDA tools of cadence ADE (Analog Design Environment), as shown in Fig. 11. The LPF successfully bring about a small core die area of 85.28 μm^2 only.

3 Results

The schematic and layout design of the proposed LPF have been considered utilising GPDK-90 nm CMOS process technology with cadence ADE tool. The simulation uses a 1.3 V DC supply as VDD and the temperature has been set to 300 K. For this LPF performance study various aspects such as gain, noise figure and bandwidth have been considered.

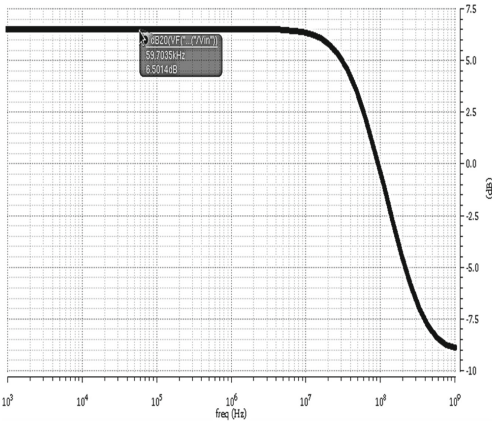

Fig. 12. LPF gain analysis.

Figure 12 shows the AC analysis of the LPF where a moderate peak gain of 6.5 dB is reported. The gain is flat and the cut off frequency is 35.48 MHz. Figure 13 shows the noise analysis of the LPF which shows a 20.78 dB noise figure at 35 MHz offset. The noise figure seems to be quite high which is mainly because of the flicker noise contribution at the low frequencies.

The power consumption of the proposed low pass filter for its operation is only 1.56 mW, as shown in Fig. 14. This reasonably low consumption could have been achieved due to the application of smaller but optimised transistors in the design.

Table 2 summaries the performance of the proposed LPF design, with regards to various parameters. This LPF achieved a moderate gain, a very small core die area and an extremely low power dissipation.

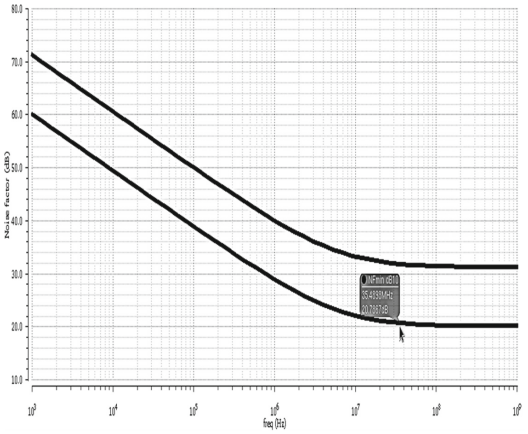

Fig. 13. LPF noise analysis.

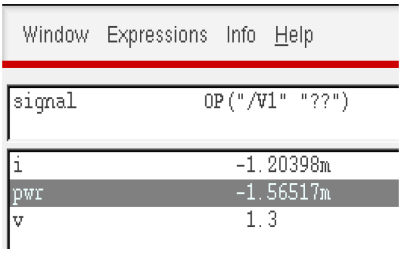

Fig. 14. LPF power dissipation.

Table 2. Performance summery of the LPF

Parameters	Value
Technology	90 nm CMOS
Gain (dB)	6.5
Supply Voltage (V)	1.3
Bandwidth (MHz)	35.48
NF min (dB)	20.78
Power Consumption (mW)	1.56
Chip Area (μm^2)	85.28

4 Conclusions

IoT RFID is considered as one of the most advantageous devices for the present as well as the future of the smart connected world. In this research, a low power compact LPF has been designed and simulated in GPDK 90-nm CMOS technology for IoT RFID

transceiver. It exhibits a high gain of 6.50 dB, a competitive noise figure of 20.56 dB with a wide bandwidth of 35.48 MHz. The LPF operates with a single 1.3 V supply voltage and consumes only 1.56 mW power. In this design, avoiding passive spiral inductors helped to keep the die area very small which is only 85.28 μm^2. Overall, such LPF increases the performance of the IoT RFID transceiver.

Acknowledgements. The authors acknowledge the support of the grant FRGS/1/2020/TK0/XMU/02/5 from the Ministry of Higher Education (MoHE), Malaysia.

References

1. Miraz, M.H., Ali, M., Excell, P.S., Picking, R.: Internet of nano-things, things and everything: future growth trends. Future Internet **10**(8), 68 (2018)
2. Bhuiyan, M.A.S., et al.: CMOS series-shunt single-pole double-throw transmit/receive switch and low noise amplifier design for Internet of Things based radio frequency identification devices. Informacije MIDEM **50**(2), 105–113 (2020)
3. Farooq, H., Rehman, H.U., Javed, A., Shoukat, M., Dudley, S.: A review on smart IoT based farming. Ann. Emerg. Technol. Comput. (AETiC) **4**(3), 17–28 (2020). https://doi.org/10.33166/AETiC.2020.03.003, http://aetic.theiaer.org/archive/v4/v4n3/p3.html.
4. Badal, M.T.I., Reaz, M.B.I., Bhuiyan, M.A.S., Dhawale, C.A.: Nano CMOS charge pump for readerless RFID PLL. Informacije MIDEM **49**(2), 53–60 (2019)
5. Bhuiyan, M.B.I., Reaz, M.B.I., Jalil, J., Rahman, L.F., Chang, T.G.: A compact transmit/receive switch for 2.4 GHz reader-less active RFID tag transceiver. J. Central South Univ. **22**(2), 546–551 (2015)
6. https://www.electronicproducts.com/wp-content/uploads/sensors-and-transducers-sensors-vppo-iot-aug2014-lores.gif. Accessed 9 May 2021
7. Badal, M.T.I., Reaz, M.B.I., Jalil, Z., Bhuiyan, M.A.S.: Low power high-efficiency shift register using implicit pulse-triggered flip-flop in 130 nm CMOS process for a cryptographic RFID tag. Electronics **5**(4), 92 (2016)
8. Kantareddy, S.N.R., Mathews, I., Bhattacharyya, R., Peters, I.M., Buonassisi, T., Sarma, S.E.: Long range battery-less PV-powered RFID tag sensors. IEEE Internet Things J. **6**, 6989–6996 (2019)
9. Philipose, M., Smith, J.R., Jiang, B., Mamishev, A., Sumit, R., Sundara-Rajan, K.: Battery-free wireless identification and sensing. IEEE Perv. Comput. **4**, 37–45 (2005). https://doi.org/10.1109/MPRV.2005.7
10. https://www.mdpi.com/sensors/sensors-18-03584/article_deploy/html/images/sensors-18-03584-g001-550.jpg. Accessed 9 May 2021
11. SRII: Report on Development plan for RFID in Industry and Service (RFID). NECTEC (2006)
12. Ayre, L.B.: RFID Costs, Benefits, and ROI: Number 5, July 2012. https://www.journals.ala.org/index.php/ltr/article/view/4513. Accessed 12 Nov 2020
13. Dinesh, V., Gupta, R.: IPv6 vs EPC (2004). http://www.worldinternetcenter.com/Pubs/Pubs2004/feb05/IPv6vEPC.pdf. Accessed 12 Nov 2020
14. Bi, H.H., Lin, D.K.J.: RFID-enabled discovery of supply networks. IEEE Trans. Eng. Manag. **56**, 129–141 (2009). https://doi.org/10.1109/TEM.2008.922636
15. Ubrurhe, O.N.H., Excell, P.S.: A review of energy efficiency in wireless body area/sensor networks, with emphasis on MAC protocol. Ann. Emerg. Technol. Comput. (AETiC) **4**(1), 1–7 (2020). https://doi.org/10.33166/AETiC.2020.01.001, http://aetic.theiaer.org/archive/v4/v4n1/p1.html.

16. Bhuiyan, M.A.S., Minhad, K.N.B., Uddin, M.J., Reaz, M.B.I., Badal, M.T.I., Ullah, H.: CMOS LNA for IoT RFID. In: 2nd IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET 2020), pp. 1–4 (2020)
17. Bhuiyan, M.A.S., Taib, M.T.B.M., Reaz, M.B.I., Hasim, F.H., Ali, S.H.M.: Design of a band-pass filter in 0, 18 μm CMOS for 2, 4 GHz reader-less RFID transponder. Tech. Gaz. **24**(1), 31–34 (2017)
18. Pérez-Bailón, J., Calvo, B., Medrano, N.: A CMOS low pass filter for SoC lock-in-based measurement devices. Sensors **19**(23), 5173 (2019)
19. Zhang, C., Shang, L., Wang, Y., Tang, L.: A CMOS programmable fourth-order Butterworth active-RC low-pass filter. Electronics **9**(2), 204 (2020)
20. Deeb, A., Abugharbieh, K.: A CMOS gm-C low-pass filter for direct conversion receivers with tuning capability. In: 2019 Southeast Con, pp. 1–4 (2019)
21. Bhuiyan, M.A.S., Reaz, M.B.I., Omar, M.B., Badal, M.T.I., Jahan, N.A.: Advances in active inductor based CMOS band-pass filter. Micro Nanosyst. **10**(3), 3–10 (2018)
22. Sreenivasulu, P., Rao, G.H., Rekha, S., Bhat, M.S.: A 0.3 V, 56 dB DR, 100 Hz fourth order low-pass filter for ECG acquisition system. Microelectron. J. **94**, 104652 (2019)
23. Badal, T.I., Reaz, M.B.I., Bhuiyan, M.A.S., Kamal, N.: CMOS transmitters for 2.4-GHz RF Devices: design architectures of the 2.4-GHz CMOS transmitter for RF devices. IEEE Microwave Mag. **20**(1), 38–61 (2019)
24. Folla, J.K., et al.: A low-offset low-power and high-speed dynamic latch comparator with a preamplifier-enhanced stage. IET Circ. Dev. Syst. **15**(1), 65–77 (2021)
25. Bhuiyan, M.A.S., Badal, M.T.I., Reaz, M.B.I., Crespo, M.L., Cicuttin, A.: Design architectures of the CMOS power amplifier for 2.4 GHz ISM band applications: an overview. Electronics **8**(5), 477 (2019)
26. Alam, M.J., Bhuiyan, M.A.S., Badal, M.T.I., Reaz, M.B.I., Kamal, N.: Design of a low-power compact CMOS variable gain amplifier for modern RF receivers. Bull. Electr. Eng. Inform. **9**(1), 87–93 (2020)
27. Folla, J.K., et al.: An 8.72 μW low-noise and wide bandwidth FEE design for high-throughput pixel-strip (PS) sensors. Sensors **21**(5), 1760 (2021)
28. Yodprasit, U., Ngarmnil, J.: Q-enhancing technique for RF CMOS active inductor. In: 2000 IEEE International Symposium on Circuits and Systems (ISCAS 2000), pp. V-589–V-592 (2000)