A REVIEW ON RFID, WSN AND IOT

Ashok Kumar Yadav, Associate Professor, Department of Computer Applications,

Galgotias University

ABSTRACT

RFID and wireless sensor networks (WSNs) are two critical foundations of the Internet of Things (IoT). RFID systems are capable of identifying and tracking devices, but WSNs work together to collect and transmit data from networked sensors. This entails overcoming obstacles such as changing RFID systems with identifying capabilities into sensing and computational platforms and treating them as architectures of wirelessly linked sensing tags. This, together with recent advancements in WSNs and the integration of both technologies, has enabled the development of unique IoT applications. This article discusses these two technologies in detail, as well as the barriers and problems that must be solved. Several of these problems include energy harvesting efficiency, communication interference, fault tolerance, increased data processing capacity, economic feasibility, and an effective integration of various aspects. Additionally, two major themes in IoT are discussed: the coupling of RFID and WSNs to maximise their benefits and mitigate their shortcomings, and wearable sensors, which allow new and exciting IoT applications.

KEYWORDS: IOT, RFID, WSN, Communication

INTRODUCTION

The Internet of things (IoT) concept is primarily focused on offering thousands of tiny networked devices that may collaborate to accomplish a shared goal. The proliferation of these little networked devices enables the Internet of Things to become a reality. These are intelligent yet straightforward items equipped with sensing and wireless communication capabilities. Two technologies are primarily employed in this framework, and have developed into the IoT's two core pillars: radio frequency identification (RFID) and wireless sensor networks (WSNs). Both technologies are centred on wireless sensing and communication, two of the IoT's primary requirements.

RFID is a kind of auto identification that utilises two distinct sorts of devices: a reader, which acts as the communication's master, and tags, which contain a corresponding electrical code that enables them to be individually recognised. The reader uses radio frequency (RF) impulses to interrogate these tags, and the tags answer with their unique identifying code (ID). Additionally, tags may integrate a sensor, in which case they may backscatter the data collected by the sensor. Tags may be active (battery-powered) or passive (harvesting energy from the reader's radio frequency signal). RFID is a consolidated technology for asset identification, security, and track-and-trace applications that utilises a dense array of tags inside the interrogation zone, most notably passive tags. WSNs are networks of sensor-equipped nodes that gather data in a dispersed fashion and wirelessly communicate it to a central node. A wireless sensor network (WSN) is primarily consisting of sensing nodes, gateways (base station or router), a coordinator, and a personal computer server. The sensing nodes gather data from their associated sensors and transmit it to a PC server through gateways. WSNs are extensively employed in a variety of applications, including medical, environmental, military, and security.

Unlike RFID, which is intended to identify and monitor devices, WSNs collect and transmit data from their sensors cooperatively. These two technologies may be used in conjunction to maximise their respective benefits and mitigate their respective drawbacks. The challenges in this area include converting RFID devices with identifying capabilities into sensing and computational platforms, as well as finding the right architectures for wirelessly linked sensor networks. This implies that RFID may be used independently as a WSN, consisting of a network of sensing nodes linked to a PC through a coordinator/reader, or it may be incorporated into another WSN, enhancing the capabilities of both systems. Thus, the combination of RFID and WSN technology provides an extremely promising strategy for addressing existing IoT difficulties and has opened a potential for developing unique IoT applications. Additionally, wearable sensors are an exceptional sort of wireless sensor. Additionally, they may be passive or active, and they may be RFID tags or WSN-connected sensors. All of this points to a burgeoning study area, which is discussed in detail in this study(Yu et al., 2011).

RFID

RFID technology has grown exponentially in popularity over the previous several decades for identifying and tracking applications. RFID's capacity to identify, monitor, and track data through readily deployed tags now enables applications outside supply chain management: it is being used in new fields of sensing, actuation, and even user engagement. RFID tags may be used independently of other sensors or as RF front-ends for other commercially available sensors. By incorporating sensing capabilities with RFID technology, the system can collect data from real-world items and effortlessly incorporate them into the IoT.

RFID (Analog): Without the need for separate sensing circuits, these systems conduct analogue processing on the physical signals associated with communication between the reader and the tag. Without the need of extra electronics, the reader is able to collect far more information about the target than just identification. Analog RFID sensing is based on the understanding that the performance of an RFID tag is impacted by the item it is attached to, and therefore that sensing data may be retrieved simply by assessing the variation of the signals backscattered from the tags. Additionally, sensitive coating materials or lumped components moved across the antenna are employed to optimise the device's responsiveness.

RFID (Digital): To create an integrated sensor module, tags are combined with electrical components such as sensing material, analog-to-digital converters, and a microcontroller. These are referred to as Computational RFID systems (CRFID). CRFID systems enable embedded computers to execute programmes using solely scavenged Radio Frequency (RF) energy. The ability to create genuinely pervasive computing applications for the IoT requires battery-free, "invisible" sensing and processing. The CRFID tag serves as a data transmission interface. Passive RFID sensors gather radio frequency energy from radio frequency radiation to power the circuit, conduct sensing tasks, and store data in the RFID chip for access by RFID readers.

LIMITATION

These are two of the most significant constraints, since both sensor nodes and RFID tags are composed of finite materials. Existing RFID platforms used in the Internet of Things are mostly passive, in that they cannot work or detect data until they are positioned inside the reader's reading zone. The integrated circuit (IC), microcontroller unit, and sensor module on a passive tag are powered and communicate through backscattering the incident signal. This solution minimises manufacturing costs by minimising the cost of the integrated circuit. The long-range communication and power-hungry sensing capabilities, on the other hand, will be limited by the amount of power available at the tag.

Additionally, the Federal Communications Commission (FCC) (or comparable regional agency) limits the maximum power transmitted by the reader to 1 W (30 dBm), assuming a maximum gain of 6 dBi on the antenna. After route losses and polarisation mismatches, only a portion of this transmitted RF power reaches the integrated circuit. While all components are normally engineered to be energy efficient, the logic of the sensors is more complicated and time demanding to operate. As a result, it remains a difficulty to power all components and logic functions using solely captured RF energy. This difficulty is exacerbated when the sensors are embedded in the materials being tested, since the RF signal is attenuated by the surrounding materials and the received RF energy is insufficient to power all activities, severely limiting the RFID sensor's read/write range.

CONCLUSION

While the Internet of Things is becoming a reality, there are still some obstacles that must be overcome before it can be used successfully. RFID and WSN are two of the primary technologies that allow the IoT. These technologies, their primary uses, and some unresolved issues have been discussed in this study to pique researchers' interest in order for these two technologies to progress from research concepts and prototypes to strong and powerful solutions that benefit everyone. Several obstacles have been identified, including RFID scanners' restricted reach, their inefficiency while reading passive tags, and the low precision of low power sensors used in RFID technology. In the case of WSNs, routing protocols and energy usage are also critical areas for improvement.

REFERENCES

1. Çiftler, B. S., Kadri, A., & Güvenç, I. (2017). IoT Localization for Bistatic Passive UHF RFID Systems with 3-D Radiation Pattern. *IEEE Internet of Things Journal*, *4*(4), 905–916. https://doi.org/10.1109/JIOT.2017.2699976

2. Hester, J. G. D., & Tentzeris, M. M. (2016). Inkjet-printed flexible mm-wave van-atta reflectarrays: A solution for ultralong-range dense multitag and multisensing chipless RFID implementations for IoT smart skins. *IEEE Transactions on Microwave Theory and Techniques*, *64*(12), 4763–4773. https://doi.org/10.1109/TMTT.2016.2623790

3. Hester, J. G. D., & Tentzeris, M. M. (2017). A Mm-wave ultra-long-range energy-autonomous printed RFID-enabled van-atta wireless sensor: At the crossroads of 5G and IoT. *IEEE MTT-S International Microwave Symposium Digest*, 1557–1560. https://doi.org/10.1109/MWSYM.2017.8058927

4. Kang, Y.-S., Park, I.-H., Rhee, J., & Lee, Y.-H. (2016). MongoDB-Based Repository Design for IoT-Generated RFID/Sensor Big Data. *IEEE Sensors Journal*, *16*(2), 485–497. https://doi.org/10.1109/JSEN.2015.2483499

5. Khan, S. F. (2017). Health care monitoring system in Internet of Things (IoT) by using RFID. *2017 6th International Conference on Industrial Technology and Management, ICITM 2017*, 198–204. https://doi.org/10.1109/ICITM.2017.7917920

6. Mohideen, Z. A., Kiran, K., & Muhamad, S. (2017). IoT: QoS in the digital library RFID based LIS. *ACM International Conference Proceeding Series*, 101–105. https://doi.org/10.1145/3029387.3029398

7. Tewari, A., & Gupta, B. B. (2017). Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *Journal of Supercomputing*, *73*(3), 1085–1102. https://doi.org/10.1007/s11227-016-1849-x

8. Xiang, S., & Gao, Y. (2011). Discussion on IoT structure and analysis on property of RFID system. *2011 International Conference on Internet Technology and Applications, ITAP 2011 - Proceedings*. https://doi.org/10.1109/ITAP.2011.6006377

9. Yu, M., Zhang, D., Cheng, Y., & Wang, M. (2011). An RFID electronic tag based automatic vehicle identification system for traffic iot applications. *Proceedings of the 2011 Chinese Control and Decision Conference, CCDC 2011*, 4192–4197. https://doi.org/10.1109/CCDC.2011.5968962

10. Zhai, C., Zou, Z., Chen, Q., Xu, L., Zheng, L.-R., & Tenhunen, H. (2016). Delay-aware and reliability-aware contention-free MF–TDMA protocol for automated RFID monitoring in industrial IoT. *Journal of Industrial Information Integration*, *3*, 8–19. https://doi.org/10.1016/j.jii.2016.06.002

11. Zhao, G., Yu, H., Wang, G., Sui, Y., & Zhang, L. (2015). Applied research of IOT and RFID technology in agricultural product traceability system. *IFIP Advances in Information and Communication Technology*, *452*, 506–514. https://doi.org/10.1007/978-3-319-19620-6_57.

12. Geller, J., Grudzinskas Jr., A. J., McDermeit, M., Fisher, W. H., & Lawlor, T. (1998). The efficacy of involuntary outpatient treatment in Massachusetts. *Administration and Policy in Mental Health*, *25*(3), 271–285. https://doi.org/10.1023/A:1022239322212

13. Gia, T. N., Jiang, M., Rahmani, A.-M., Westerlund, T., Liljeberg, P., & Tenhunen, H. (2015). Fog computing in healthcare Internet of Things: A case study on ECG feature extraction. In J. S. L. L. C. R. A. H. J. M. G. G. N. W. Y. Atzori L. Jin X. (Ed.), *Proceedings - 15th IEEE International Conference on Computer and Information Technology, CIT 2015, 14th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2015, 13th IEEE International Conference on Dependable, Autonomic and Secure Computing, DASC 2015 and 13th IEEE International Conference on Pervasive Intelligence and Computing, PICom 2015* (pp. 356–363). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.51

14. He, D., & Zeadally, S. (2015). An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography. *IEEE Internet of Things Journal*, *2*(1), 72–83. https://doi.org/10.1109/JIOT.2014.2360121

15. Hiremath, S., Yang, G., & Mankodiya, K. (2015). Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare. *Proceedings of the 2014 4th International Conference on Wireless Mobile Communication and Healthcare - "Transforming Healthcare Through Innovations in Mobile and Wireless Technologies", MOBIHEALTH 2014*, 304–307. https://doi.org/10.1109/MOBIHEALTH.2014.7015971

16. Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In Z. L.-J. Bahsoon R. (Ed.), *Proceedings - 2015 IEEE World Congress on Services, SERVICES 2015* (pp. 21–28). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/SERVICES.2015.12

17. Hussain, A., Wenbi, R., Da Silva, A. L., Nadher, M., & Mudhish, M. (2015). Health and emergency-care platform for the elderly and disabled people in the Smart City. *Journal of Systems and Software*, *110*, 253–263. https://doi.org/10.1016/j.jss.2015.08.041

18. Jara, A. J., Alcolea, A. F., Zamora, M. A., Gómez Skarmeta, A. F., & Alsaedy, M. (2010). Drugs interaction checker based on IoT. *2010 Internet of Things, IoT 2010*.

https://doi.org/10.1109/IOT.2010.5678458

19. Karafiloski, E., & Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review. In K. L. Latkoski P. Cvetkovski G. (Ed.), *17th IEEE International Conference on Smart Technologies, EUROCON 2017 - Conference Proceedings* (pp. 763–768). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/EUROCON.2017.8011213

20. Laplante, P. A., & Laplante, N. (2016). The Internet of Things in Healthcare: Potential Applications and Challenges. *IT Professional*, *18*(3), 2–4. https://doi.org/10.1109/MITP.2016.42

21. Lee, Y. H., Jang, M., Lee, M. Y., Kweon, O. Y., & Oh, J. H. (2017). Flexible Field-Effect Transistor-Type Sensors Based on Conjugated Molecules. *Chem*, *3*(5), 724–763. https://doi.org/10.1016/j.chempr.2017.10.005

22. Mandula, K., Parupalli, R., Murty, C. H. A. S., Magesh, E., & Lunagariya, R. (2016). Mobile based home automation using Internet of Things(IoT). *2015 International Conference on Control Instrumentation Communication and Computational Technologies, ICCICCT 2015*, 340–343. https://doi.org/10.1109/ICCICCT.2015.7475301

23. Mano, L. Y., Faiçal, B. S., Nakamura, L. H. V, Gomes, P. H., Libralon, G. L., Meneguete, R. I., Filho, G. P. R., Giancristofaro, G. T., Pessin, G., Krishnamachari, B., & Ueyama, J. (2016). Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition. *Computer Communications*, *89–90*, 178–190. https://doi.org/10.1016/j.comcom.2016.03.010

24. Moosavi, S. R., Gia, T. N., Rahmani, A.-M., Nigussie, E., Virtanen, S., Isoaho, J., & Tenhunen, H. (2015). SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. In S. E. (Ed.), *Procedia Computer Science* (Vol. 52, Issue 1, pp. 452–459). Elsevier B.V. https://doi.org/10.1016/j.procs.2015.05.013

25. Muhammad, G., Rahman, S. M. M., Alelaiwi, A., & Alamri, A. (2017). Smart Health Solution Integrating IoT and Cloud: A Case Study of Voice Pathology Monitoring. *IEEE Communications Magazine*, *55*(1), 69–73. https://doi.org/10.1109/MCOM.2017.1600425CM

26. Nawir, M., Amir, A., Yaakob, N., & Lynn, O. B. (2017). Internet of Things (IoT): Taxonomy of security attacks. *2016 3rd International Conference on Electronic Design, ICED 2016*, 321–326. https://doi.org/10.1109/ICED.2016.7804660

27. Ndiaye, M., Hancke, G. P., & Abu-Mahfouz, A. M. (2017). Software defined networking for improved wireless sensor network management: A survey. *Sensors (Switzerland)*, *17*(5). https://doi.org/10.3390/s17051031

28. Pang, Z., Zheng, L., Tian, J., Kao-Walter, S., Dubrova, E., & Chen, Q. (2015). Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things.

Enterprise Information Systems, *9*(1), 86–116. https://doi.org/10.1080/17517575.2013.776118

29. Rahmani, A.-M., Thanigaivelan, N. K., Gia, T. N., Granados, J., Negash, B., Liljeberg, P., & Tenhunen, H. (2015). Smart e-Health Gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems. *2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, 826–834. https://doi.org/10.1109/CCNC.2015.7158084

30. Rajandekar, A., & Sikdar, B. (2015). A survey of MAC layer issues and protocols for machine-to-machine communications. *IEEE Internet of Things Journal*, *2*(2), 175–186. https://doi.org/10.1109/JIOT.2015.2394438

31. Roehrs, A., Da Costa, C. A., Da Rosa Righi, R., & De Oliveira, K. S. F. (2017). Personal health records: A systematic literature review. *Journal of Medical Internet Research*, *19*(1). https://doi.org/10.2196/jmir.5876

32. Singh, R., Singh, E., & Nalwa, H. S. (2017). Inkjet printed nanomaterial based flexible radio frequency identification (RFID) tag sensors for the internet of nano things. *RSC Advances*, *7*(77), 48597–48630. https://doi.org/10.1039/c7ra07191d