The Effect of Radio Waves on the Quality and Safety of Wearable Sensors in Healthcare

Hooman Kashanian[a], Negar Chitgar[b*]

[a] *Department of Computer Engineering, Islamic Azad University, Ferdows Branch, Iran*
[b] *Department of Computer Engineering, Mazandaran University of Science and Technology, Babol, Iran*

Abstract

The industrial Internet of Things (IoT) is aiming to interconnect humans, machines, materials, processes and services in a network. Wireless Sensor Network (WSN) comprises the less power consuming, light weight and effective Sensor Nodes (SNs) for higher network performance. Radio Frequency Identification (RFID) and sensor networks are both wireless technologies that provide limitless future potentials. ZigBee is a sensor based special network which pulls the trigger to establish it in wireless network standard. ZigBee is the real time application for the WSN used for low-cost data and energy consumption characteristics. Radio Frequency Identification (RFID) system is a contactless automatic identification system using small, low-cost RFID tag to an animate or inanimate object. Because of the advantage of simultaneous recognition of massive amounts of information, it is expected to replace the traditional bar-code system. We evaluated based on the work done on the features which is best for wearable sensors.
Keywords: ZigBee, RFID, BSN, HealthCare, Radio Frequency.

1. Introduction

Advances in information and communication technologies have led to the emergence of Internet of Things (IoT). In the modern health care environment, the usage of IoT technologies brings convenience of physicians and patients since they are applied to various medical areas (such as real-time monitoring, patient information management, and healthcare management). The body sensor network (BSN) technology is one of the core technologies of IoT developments in healthcare system, where a patient can be monitored using a collection of tiny-powered and lightweight wireless sensor nodes. It is basically a collection of low-power and lightweight wireless sensor nodes that are used to monitor the human body functions and surrounding environment [1]. Most BSNs use ZigBee or other IEEE 802.15.4 based transmission technologies [2]. ZigBee Network or accurately known as IEEE 802.15.4/ZigBee, on the other hand, is known to be a low power consumption device with good and stable data transmission range, higher network flexibility and large number of nodes [3].

Wireless sensors and sensor networks have become a great interest to research, scientific and technological community. Though sensor networks have been in place for more than a few decades now, the wireless domain has opened up a whole new application space of sensors. Wireless sensors and sensor networks are different from traditional wireless networks as well computer networks and, therefore, pose more challenges to solve such as limited energy,

* Corresponding author, n.chitgar@gmail.com

restricted life time, etc. Wireless sensing units integrate wireless communications and mobile computing with transducers to deliver a sensor platform which is inexpensive to install in numerous applications. Indeed, co-locating computational power and radio frequency (RF) communication within the sensor unit itself is a distinct feature of wireless sensing. Today, the progress in science and technology offers miniaturization, speed, intelligence, sophistication, and new materials at lower cost, resulting in the development of various high-performance smart sensing system [4], diagram of wireless body area networks shown in the Figure 1.

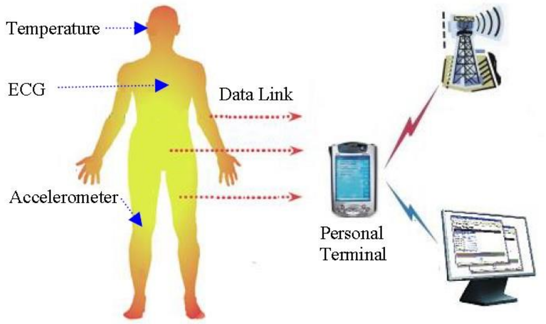

Figure 1. Conceptual diagram of wireless body area networks

Radio Frequency Identification (RFID) system is a wireless technology, which is used to automatically identify remote objects embedded with RFID tags. Introduced in 1940s, RFID technology has been used in various applications such as supply chain management, transportation, livestock management, e-payment system, e-passport system, and patient medical care. An RFID tag is small and low cost, massive amounts of RFID tags can be simultaneously recognized with radio frequency communication. RFID system is a contactless automatic identification system using small, low-cost RFID tag to an animate or inanimate object. Because of the advantage of simultaneous recognition of massive amounts of information, it is expected to replace the traditional bar-code system [5].

ZigBee is just one of several ways to get signals wirelessly from device to device within a smart home. Some Control4 products use Wi-Fi or wired Ethernet connections (802.3); others leverage the power of Bluetooth, AirPlay and DLNA. Our systems also inter-operate with partner products to enable Z-Wave compatibility. But for our lighting systems, ZigBee home automation was a very appropriate choice [6].

This article is organized as follows: section 2 describes the ZigBee technology, section 3 overview of radio frequency identification systems (RFID), section 4 present different of ZigBee and RFID, and section 5 contains the conclusions.

2. ZigBee

ZigBee is a standard for personal-area networks developed by the ZigBee Alliance (including companies like Samsung, Philips, Motorola, Texas Instruments and many others) with the aim of providing a low-cost, low-power consumption, two-way, reliable, wireless communication standard for short range applications. The standard is completely open and gained ratification by the Institute of Electrical and Electronics Engineer (IEEE) in 2003. Advantages of choosing ZigBee are the provision of long battery lifetime, the support of a large number of nodes (up-to 65000) in a network, the easy deployment, the low costs and global usage. ZigBee is used for example in Remote Control, Input Devices, Home Automation, Building Automation, Health Care, etc. [7].

The ZigBee stack consists of four layers:

1. Physical Layer (PHY)
2. Medium Access Control Layer (MAC)
3. Network Layer (NWK)
4. Application Layer (APL)

The IEEE 802.15.4-2003 standard is used for the two lowest layers, the physical layer (PHY) and the medium access control layer (MAC). The other two layers are defined by the ZigBee Protocol Stack [7].

The MAC layer responsibilities of IEEE 802.15.4 include: generating network beacons (coordinator), synchronizing to network beacons, supporting MAC association and disassociation, supporting MAC encryption, employing unslotted/slotted CSMA/CA mechanism for channel access, and handling guaranteed time slot (GTS) allocation and management. IEEE 802.15.4 defines four frame structures: beacon frame, data frame, acknowledgement frame, and MAC command frame. For data transfer, three types of transactions exist: from a coordinator to a device, from a device to a coordinator, and between two peer devices. Data transfers are completely controlled by the devices rather than by the coordinator. A device either transfers data to the coordinator, or polls the coordinator to receive data, both according to the application-defined rate. This provides the energy conservation feature of the ZigBee/IEEE 802.15.4 network, since the device can sleep whenever possible, rather than keeping its receiver continuously active [8].

Two modes are provided for IEEE 802.15.4 multiple access scheme: beacon enabled and non-beacon enabled modes. In a beacon enabled mode, a superframe structure is used. A superframe (SF) is divided into two portions: active and inactive. During the inactive portion, devices may enter a low-power mode according to the requirement of its application. The active portion consists of contention access period (CAP) and contention free period (CFP). Any device wishing to communicate during the CAP shall compete with other devices using a slotted CSMA/CA mechanism, while the CFP contains guaranteed time slots where no contention exists. However, if a coordinator does not prefer to use the beacon-enabled mode, it may turn off the beacon transmissions, and the unslotted CSMA/CA algorithm is used. Both downlink and uplink compete for the same resources. No duplex scheme is specified [8].

Figure 2 shows the structure of the ZigBee network. Check out the features of this technology in Table 1.

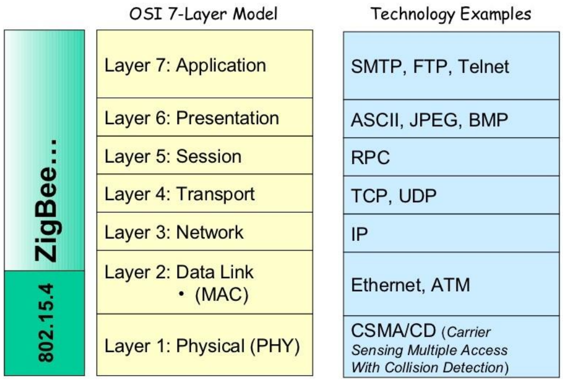

Figure 2. ZigBee and OSI Model

At present, the international attention to the remote medical monitoring system is increasing. The ZigBee technology provides a good solution for wireless transmission through sensor signals. The ZigBee nodes have the coverage of tens of meters. It can also increase the routing nodes, and expands the coverage. Moreover, the data traffic of physical custody signal is not large, so the transfer rate of 250KB of ZigBee can meet the physiological signal transmission requirements. And its power consumption is very small, which can monitor and transmit distance physiological data. This system adopts a variety of body sensors to collect physiological indicators of patients, then sent them to the coordinator node in the ward node. So, it can determine the physical condition of patient through the received physiological data [9].

Table 1
characteristics of ZigBee

Attribute	ZigBee
Number of Channels	27
Radio Frequency Band[s]	•2.4 GHz with 16 channels for global use •915 MHz with 10 channels for N. America, Australia and a few additional countries •868 MHz with 1 channel for EU countries
Network Capabilities	Self-organizing and self-healing dynamic mesh network based on ZigBee public standard
Network Size	Thousands of devices per Network

3. RFID

Radio Frequency Identification technology is a wireless technology that allows for automated data collection and a unique identification of objects. RFID systems are composed of RFID tags attached to the objects, readers that can read the tags from a distance, and application software. Every RFID enabled object has its own unique identification number (ID). Tags can be classified into three main groups based on power supply namely, passive, semi-passive and active. Passive tags operate without battery and are powered by the readers when they are in the proximity of the readers. Passive RFID tags use backscattering to reflect back the reader radio waves to the reader, usually at the same carrier frequency. The reflected signal is modulated to transmit data. The frequency ranges, characteristics and typical applications of RFID systems are provided in Table 2 [10].

Table 2
Frequency band, characteristics and typical applications of RFID systems

Frequency band	Characteristics	Typical applications
125 kHz -134 kHz (Low frequency)	Penetration through materials, can be read in proximity of metals and liquids, low data transmission rates and low reading range	Manufacturing support, large vehicle and container identification, access control, animal identification, explosive detection
13.56 MHz (High frequency)	Penetration through materials except metal, higher data rate, reading of large number of tags simultaneously, potentially inexpensive	Parcel tracking and services, airline baggage management and reconciliation, library systems and rental services, smart cards, access control, explosive detection
900 MHz (Ultra-high frequency)	Higher reading range, smaller antenna, Line of sight required for higher range communication	Supply chain management applications
2.45 GHz or 5.8 GHz (Microwave)	High data rates (100 Kbits/s), high reading range, absorbed by water and water based solutions and reflected by metal and quasi conductive surfaces, line of sight required	Factory automation, access control, road tolling, supply chain and military logistics, mining industry applications

Semi-passive (battery assisted) tags use battery for their internal operations but they use backscattering for communication with the reader. The energy needed to power up the chip is obtained from the battery but backscattered mechanism is still used for communication between the reader and tags. The antenna of passive tags is optimized for collecting energy and not for achieving the maximum signal level. On the other hand, battery-assisted tags are designed to reflect maximum signal achieving in this way longer reading range. Therefore, this technology has a great potential in mining industry too for example tracking of miners, equipment and mobile assets. Active tags use battery power for both communication and internal operations. RFID readers are used to excite passive and semi-passive tags and read data encoded on tags. The frequency of RFID ranges from low frequency (LF) to microwave [10].

Assemblages of tags, attached to objects and readers can be used to form Real-Time Locating Systems (RTLS), which enable the locating of required objects within a space in Real Time [10]. Flexible, reliable and compact wearable RFID-enabled sensor nodes are required in order to establish and maintain a fast and secured body-area network. To realize optimized designs, it is necessary to determine the influence of substrate on the electromagnetic performance of the sensor node, especially the antenna part. Material characterization with resonator methods will be a must to include the consideration of effects of the textiles in the design procedure. In the next step, a UHF RFID tag will be optimized, deploying inkjet-printing as a fast direct-write solution to fabricate the RFID antenna directly on flexible eco-friendly organic materials. The direct-write technology also provides the feasibility to have all-printed wearable RFID tag integrated with sensors and power sources. A suggested outline of RFID/sensor integration will be illustrated [11].

The wearable RFID-enabled sensor node can potentially find broad usage in real-time monitoring and medical monitoring applications. In this integrated module, the sensor part will detect the condition of the patient, such as body temperature, and transmit the signal out through the use of the RFID section. The readers implemented over the hospital will gather the information transmitted by the RFID, and trigger the alarm to notify the doctors if some severe condition information is detected. Therefore, real-time biomedical monitoring can be realized with the aid from RFID without adding more labor force. In addition, extra information, such as the recommended patient's drug dosage could be included also in the RFID module of the RFID-enabled sensor node to minimize the risk of overdose or wrong treatment [11].

3.1 HOW RFID WORKS

The underlying technology architecture of RFID is based on these components:

- tag and its associated data structure
- reader with antenna and the reader's associated software
- communications protocol suite
- communications network
- database - data synchronization

A reader can be either stationary in a fixed state (e.g., mounted above a conveyor belt) or mobile as in a handheld device or attached to a forklift. The tag is a miniature chip with an affixed radio antenna. The tag is attached to an item or its packaging. A radio wave signal is transmitted between a reader and tag to communicate an Electronic Product Code (EPC). The EPC is used to uniquely identify the pallet, case, or item [12].

3.2 HOW TAG WORKS

There are currently two types of tags: passive and active. Passive tags have no directly associated power source, while active tags do. Passive and active tags can be either class 0 (read only) or class 1 (read/write) tags. The approved radio frequency range for RFID applications is 900MHz for Class 0, and either 13.56 MHz ISM Band or 860-930 MHz for Class 1, depending on the strength of signal required [12].

In the case of a passive tag, the reader initiates communication via a radio signal strong enough to enable the tag to "answer" the reader with a return radio signal carrying information regarding the item to which it is attached. In the case of an active tag, either the tag or the reader can initiate communication. Further, active tags allow for a greater distance between the reader and the tag. It should be noted that with the recent improvements in passive tag technology the distance limitation is decreasing in other words some passive tags are crossing over into read distance ranges previously only supported by active tags (for more information check out Intel's R1000 chip [12].

3.3 HOW READER WORKS

A reader has a field (a distance range) within which it can query via radio waves for whatever tags may be present. The reader follows a protocol that is intended to enable it to avoid duplicate reads but capture all tags present within its range [12].

There is a large variation in reader capabilities, ranging from how many tags a reader can capture within a specific time period to more complicated tasks like filtering and communicating with a product database. Readers have to be matched to tag type: active or passive class: 0 (read only) or class 1 (read/write), gen 1 or gen 2 tags. Some readers can capture multiple tag types. Readers communicate with tags over radio waves and by following a specific RFID communications protocol [12].

3.4 RFID COMMUNICATION PROTOCOL SUITE

Current: The EPC and ISO have standardized the first two layers of the communication protocol stack between the readers and the tags. These two layers include the local wireless communication that occurs between a reader and the tags within its read field. The first layer standard is the physical, which describes the specific radio frequencies and whether tags and readers are communicating in half or full duplex mode. The second layer, referred to as the data link layer, has been standardized based on a slotted Aloha scheme [12].

Middleware standards have been defined to support temporary collection of event data for filtering and consolidating the EPC data coming from the readers. This standard is called Application Level Events or ALE. Another communication standard has been defined for the readers in terms of how they capture and communicate event data from tags and sensors, called the Reader Protocol (RP). Communications between readers and in-house databases are up to individual implementations. This is also true for inter-company communications [12].

3.5 RFID COMMUNICATION NETWORK

Current: Today there is no such thing as an "RFID network" except in the local/private sense, the extremely local communications between tags and readers, and subsequently between the reader and the in-house database system. Although it should be noted that the ALE middleware standard operates at that first edge between the reader and the in-house database. RFID network links include the local wireless (RF) network between tags and readers, between readers and the internal company database systems (e.g., ERP or WMS in the retail industry) and in the inter-company network links which today are individually negotiated between business partners [12].

Future: The planned-design intent behind RFID architecture is to ultimately standardize communications between entities based on an Internet architecture-based construct. There is considerable work that needs to be done to make this vision a reality [12].

3.6 RFID DATABASES

Current: Today, retail companies and their suppliers are using RFID very much like they have been using UPCs. Suppliers/manufacturers provide the retail companies with a listing of EPCs and what pallets/cases of product they represent. The retail companies typically then feed that information into their existing in-house database systems (e.g., WMS, ERP). In other words, today there aren't any real-world databases built on the RFID Internet based architecture proposed by EPC global [12].

A very real and major challenge facing the manufactures/suppliers and the retail distribution companies is keeping data synchronized. In fact, maintaining data synchronization within an individual company is challenging enough between companies is orders of magnitude more difficult [12].

4. Comparing ZigBee and RFID

Really, the only similarity between ZigBee and RFID is that the both use radio waves to transmit information; aside from that they're COMPLETELY different.in Table 3, investigate different between ZigBee and RFID.

Table 3
comparison between ZigBee and RFID

ZigBee	RFID
low-rate data	maximum range
cost less	prices vary with quantity
the nodes all have batteries	no battery
Detect any where	Need scan

We investigated QoS and Security for both Radio Frequency that choose better technology to use in healthcare in Table 4 (Based on research).

Table 4
QoS and Security for RFID and ZigBee

	QoS	Security
ZigBee	1. improved QoS in ZigBee network using Stochastic and Widest Path model of probability. The simulation study shows, there is about	1. The ghost attack can further trigger severe DoS and post-depletion attacks. the lifetime of nodes is significantly impacted

	28% less end-to-end delay in the application layer, 41% less delay, two-times lower data drop threshold in the global MAC layer, 3% smaller queue size in terms of the Stochastic modeling rather than the Widest Path modeling. However, in terms of the Widest Path model, around 80% increase in overall throughput; wherein for the network layer [13]. 2. the priority-based network has almost 14% and 44% less MAC delay and load, respectively. Moreover, there was 36% higher throughput compared to the without-priority based network, the proposed priority-based ZigBee network's performance is identified to be more effective than without-priority based ZigBee network [14].	with this attack. leading to battery depletion [15].
RFID	1.with Bayesian Coalition Game (BCG) as a service for RFID-based secure QoS management: **communication cost**: is high but cheap compared to **the rest Overhead generated**: increased with increase in number of tags. **successful delivery of data packets:** As overhead and communication cost are increased, delivery of the data packets is decreased. But the decrease in it is less. **Utility, cost**: rise with increase in number of coalitions [16].	1.Since the tags are also used for personal identification and access control, new challenges for identity management arise. Privacy enhancing identity management systems could provide a higher level of transparency and control for the user. Communication (NFC) protocol which allows a simplified exchange between electronic devices based on the RFID technique in the 13,56 MHz band.. Falling prices will make the RFID–technique especially relevant for pervasive or ubiquitous computing [17].

5. Conclusion

In this article, we have described ZigBee and RFID in BSN. We compared QoS and security of them in healthcare, based on the work done so far. To select one of these two radio frequencies in healthcare, criteria such as time and distance and the amount of security and cost to be paid must be taken into account, but, today, Scientists have investigated that ZigBee is a dangerous for human health.

6. References

[1] P. Gope and T. Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network," IEEE Sens. J., vol. 16, no. 5, pp. 1368–1376, (2016).

[2] S. Kim et al., "Evaluation of a 433 MHz band body sensor network for biomedical applications," Sensors (Switzerland), vol. 13, no. 1, pp. 898–917, (2013).

[3] H. Daud et al., "Monitoring Heart Rate and Body Temperature using Wireless Technology (Zigbee)," vol. 491, pp. 1565–1574, (2014).

[4] K. Malhi, S. C. Mukhopadhyay, J. Schnepper, and M. Haefke, "A Zigbee-Based Wearable Physiological Parameters Monitoring System," vol. 12, no. 3, pp. 423–430, (2012).

[5] P. Gope and T. Hwang, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system," Comput. Secur., vol. 55, pp. 271–280, (2015).

[6] Nojavan, T., Kashanian, H. Detection of children's activities in smart home based on deep learning approach. International Journal of Information, Security and Systems Management, 5(2): 605-609; (2016)

[7] T. Zillner, "ZigBee Exploited The good, the bad and the ugly 1 Introduction 3 ZigBee Security 2 The ZigBee Standard," pp. 699–704, (2016).

[8] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. M. Leung, "Body area networks: A survey," Mob. Networks Appl., vol. 16, no. 2, pp. 171–193, (2011).

[9] C. Ding and X. Wu, "Design and Implementation of the Zigbee-based body sensor network system," (2009).

"Very short overview of RFID," no. Id.

[10] L. Yang, R. Vyas, A +---++. Rida, J. Pan, and M. M. Tentzeris, "Wearable RFID-Enabled Sensor Nodes for Biomedical Applications," pp. 2156–2159, (2008).

"http://www.dataflows.com/RFID_Overview.shtml"

[11] N. Islam, J. H. Biddut, A. I. Swapna, and S. Asaduzzaman, "Improved Quality of Service in ZigBee Network with Statistical Modeling," pp. 17–20, (2015).

[12] M. J. H. Biddut, N. Islam, M. M. Karim, and M. B. A. Miah, "An Analysis of QoS in ZigBee Network Based on Deviated Node Priority," J. Electr. Comput. Eng., vol. 2016, (2016).

[13] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, "Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks," IEEE Internet Things J., vol. 3, no. 5, pp. 816–829, (2016).

[14] N. Kumar, R. Iqbal, S. Misra, J. J. P. C. Rodrigues, and M. S. Obaidat, "Bayesian Cooperative Coalition Game as-a-Service for RFID-Based Secure QoS Management in Mobile Cloud," IEEE Trans. Emerg. Top. Comput., vol. 6750, no. c, pp. 1–1, (2016).

[15] D. Trcek and P. Jäppinen, "RFID Security," pp. 147–167, (2009).

[16] J. Zhang, G. Tian, A. Marindra, A. Sunny, and A. Zhao, A Review of Passive RFID Tag Antenna-Based Sensors and Systems for Structural Health Monitoring Applications, vol. 17, no. 2. (2017).

[17] C. Zhai et al., "QoS based RFID system for smart assembly workshop," 2016 IEEE Int. Conf. RFID Technol. Appl. RFID-TA 2016, pp. 138–143, (2016).

[18] N. V. V. Kumar, "A Secure IoT-Based Modern Healthcare," vol. 6, no. 3, pp. 156–160, (2017).