Journal of Theoretical and Applied Information Technology
15th August 2016. Vol.90. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ACQUISITION DEVICES IN INTERNET OF THINGS: RFID AND SENSORS

[1]Anouar DALLI, [2]Seddik BRI

[1]Groupe Signaux Aléatoires, Réseaux et Systèmes (S.A.R.S.), Ecole Nationale des Sciences Appliquées de Safi (ENSAS), Université Cadi Ayyad, Marrakesh, Morocco

[2]Groupe Matériaux et Instrumentations, Département Génie Electrique, Ecole Supérieure de Technologie (ESTM), Université Moulay Ismail, Meknes, Morocco.

E-mail: [1]anouar_dalli@yahoo.fr, [2]briseddik@gmail.com

ABSTRACT

Internet of things (IoT) will gradually change our life. IoT is finding a wide range of applications in various domains, including healthcare, industrial and production monitoring, control networks and many other fields. Evolution of IoT is based the constant development of sensors and RFID, this paper presents some considerations for using of these technologies. The IoT architecture consists of three main layers, perception layer, network layer and application layer. RFID and sensor are most important technologies in acquition layer. This paper present considerations to use RFID and sensors in an IoT system and define a set of requirement for deployment of this technologies in IoT environment. Finally, the paper outlines many challenges for IoT which we target to address in the near future.

Keywords: *Internet Of Things, RFID, Sensors, Acquisition Layer,Tags.*

1. INTRODUCTION

The Internet of Things (IoT) is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. IoT concept consists to connecting objects together over the Internet. It means everyday objects are identifiable, readable, recognizable, addressable, and controllable via the Internet [1].

IoT is widely used in many environments such as military applications, transportation, business, healthcare, industrial automation and environmental monitoring. The significant development of IoT is opening new opportunities that many objects that surround us will be on the network. Radio Frequency IDentification (RFID) and sensor network technologies will rise to meet this new challenge. Service providers can use IoT to link sensor devices to the internet for different purposes such as monitoring medical staff, collecting information, storing, combining, and aggregating data, environment lighting control, water systems, fire sensors and to contribute to smart buildings such as using green technology in building control [2].

According to the authors of [3-4], RFID and Sensor still stands at the forefront of the technologies driving this vision. They state that a wide portfolio of device, network, and service technologies will eventually build up the IoT. However, Sensors together with RFID are recognized as ‘‘the atomic components that will link the real world with the digital world”.

This paper outlines some considerations to using sensor technology and RFID in IoT, their applications and challenges. The paper is organized as follows: Section 2 present architecture of IoT, section 3 discusses about RFID and sensor technology, section 4 discusses various challenges of IoT applications.

2. IOT ARCHITECTURE

The IoT architecture consists of three main layers [5]:

2.1 Perception layer

This layer is sensor-based technology responsible for collecting real time data from different sources. The data will be captured from physical world devices which have the ability to receive and transmit data wirelessly.

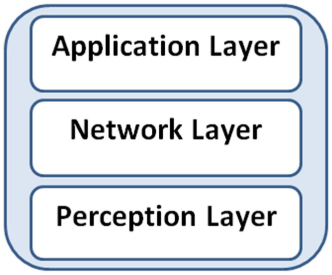

Figure 1: Proposed IoT Architecture

In this layer there are three feature blocks: the Identification, Location and Data Acquisition. In this paper we are interested in sensors and RFID, these technologies are used in object/item identification and location; the object is required to have ‘tag(s)’ and a ‘receiver’ as the two main components to track and identify the location of objects. The real-time system requires an inexpensive node or tag attached to/or embedded in the object that enables it to be tracked or monitored by the system. The receiver which reads these tags is to be deployed at a designated location, where it can easily receive the wireless signals from these tags and the system.

2.2 Network layer

The Network Layer provides the functional and procedural means of transferring multiple length data structures from different sources on one or multiple networks to a destination hub. The Network layer contains several technologies which provide the functionality of a structured data exchange using a computer network [4].

These technologies can work independently or be integrated with each other, and include Cloud Computing, ZigBee, WLAN, Cellular Mobile Network and PANs (Personal Area Networks).

Cloud computing provides remote access, and WLANs (Wireless Local Area Network) or mobile phone networks will be used to connect data-collection devices and the data hub. Internet services and Cellular Mobile Networks provide mobile access features that can be accessed anywhere, used over large-scale areas, and can link sites over a large geographic distance of national size. ZigBee is a wireless communications standard, used between large numbers of consumer devices in commercial applications, and has a low power output with larger coverage.

Ad-hoc Network and ZigBee technology needs to be connected and for nodes to be installed consequently, the cost is relatively higher and it is unsuitable for national-scale applications, being more appropriate for a manufacturing plant. Because of their limited coverage, PANs and WLAN are typically for personal use, and they are usually affected or interfered by metal objects.WSN (Wireless Sensor Network) is a communication standard using radio frequency (RF) to communicate between computers and other devices [5-6].

2.3 Application layer

The application layer is responsible for processing the huge amount of data and information using knowledge to achieve the objectives of companies. This layer provides logistical support, guidance for operational staff support and collection arrangements, and incident solutions. It is based on information and data gathered from the lower layer, and adopts a knowledge-based technology with rule-based reasoning. The collected information is processed and the reasoned result sent to the higher layer. In this layer two components are used: a knowledge base which stores the domain knowledge used in making a rule, and the fact base, which stores the current situation and equates to the main database in the lower layer. A reasoning engine is responsible for providing the best results by applying the domain knowledge to the current situation.

In this layer, user has the visual representation and organization of data, for example through creation of text, tables, pictures and diagrams to provide a Management Information System. This layer presents automatic identification and collection of healthcare information systems and user best-solutions for real-time remote sensor data access, processing, visualization, or for a different application for the same purpose. This explanation is one of the features of this layer, and uses the explanation mechanism of the Knowledge-Based System (KBS) to explain the results and the reasoning procedure used in a user-friendly and easily understandable format. The result will be translated and displayed on a terminal device, which enables communication with a computer. Depending on the user device, for example computer screen, phone or smart device, a short message or web pages may be displayed. Additionally, this layer uses a Human-Machine interface function to communicate between users and the system. This function receives a command from the user community, sends it to the system, and presents the feedback to users.

2.4 Applications of Iot

The presented architecture of IoT could be adapted for many applications in many domains. In this architecture, the application layer can be changed or modified for use with different application and domain areas, but the perception layer have to be redesigned based on the application requirements, as shown in the following examples[1-2,13-15]:

- Healthcare: Sensors and RFID tags are attached to identify, detect and locate patients, staff and equipment to provide continuous monitoring inside and outside of the hospital.
- Air shipping companies: Sensors and RFID tags are attached to identify, detected and locate customer consignments and to provide continuous monitoring in real-time.
- Hotels: Sensors and RFID tags are attached to identify, detect and locate equipment and staff to provide continuous monitoring inside and outside of hotels.
- Shops: Sensors and RFID tags are attached to identify and detect product, locate shopping carts and provide continuous monitoring within shops.
- Police: Sensors and RFID tags are attached to detainees and visitors to provide continuous monitoring in police stations.

In these examples, we can see the importance of using suitable RFID and sensor in each application. In section 3, we present a review of sensor and RFID.

2.2.2 Identification of subsections

Subsub section has to be in sentense case with no spacing above or blow the srat of it.

3. RFID IN IOT

3.1. Principe of RFID

RFID is a mean of storing and retrieving data through electromagnetic transmission to an RF compatible integrated circuit [4]. It is usually used to label and track items in supermarkets and manufactories. For example, Wal-Mart or Procter and Gamble have deployed RFID systems with their supply chains [9]. However, potential of RFID is much more than that.

Today, RFID has been widely applied in supply chain tracking, retail stock management, tracking library books, parking access control, marathon races, airline luggage tracking, electronic security keys, toll collection, theft prevention, and healthcare. Current trends and forecasts indicate that the market will grow fast in the next 10 years. Total value of the market, including hardware, systems and services, is expected to grow from €500 million to €7 billion by 2016 [8].

Briefly, RFID systems consist of two main components: tags and readers. A tag has an identification (ID) number and a memory that stores additional data such as manufacturer, product type, and environmental factors such as temperature, humidity, etc.. The reader is able to read and/or write data to tags via wireless transmissions.

In a typical RFID application, tags are attached or embedded into objects that are in need of identification or tracking. By reading tag IDs in the neighborhood and then consulting a background database that provides a mapping between IDs and objects, the reader is able to monitor the existence of the corresponding objects [9].

Figure 1 below shows the basic building blocks of RFID system.

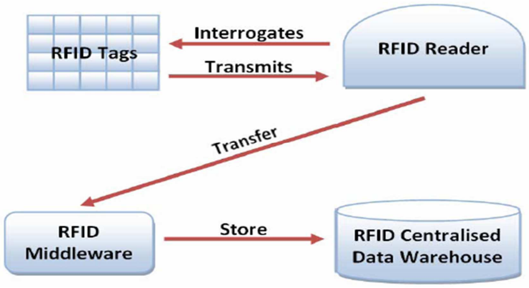

Figure 2 The basic building blocks of RFID system

3.2. Tags and Frequency Ranges

RFID tags can be classified into three major categories by their power source:

- Active tags:

Contains both a radio transceiver and a battery that is used to power the transceiver.

- Passive tags:

Operates without any battery. It reflects the RF signal transmitted to it from a reader or a transceiver and adds information by modulating the reflected signal. The passive tag does not use any battery to boost the energy of the reflected signal.

- Semi-passive (semi-active) tags:

Use the radio waves of senders as an energy source for their transmissions. However, a semi-passive tag may be equipped with batteries to maintain memory in the tags or power some additional functions.

Active tags are more powerful than passive tags/semi-passive tags, such as larger range and memory, more functions. Meanwhile, the active tags are more expensive than passive/semi-passive tags. RFID tags operate in three frequency ranges:

Table.1 frequency ranges for RFID

RFID Tags	Frequency ranges
Low Frequency (LF)	30~500kHz
High Frequency (HF)	10~15MHz
Ultra High Frequency (UHF)	850~950MHz, 2.4~2.5GHz

LF tags are less affected by the presence of fluids or metals compared to the higher frequency tags. They are fast enough for most applications, and are also cheaper than any of the higher frequency tags. However, low frequency tags have shorter reading ranges. The most common frequencies used for LF tags are 125~134.2kHz and 140~148.5kHz.

HF tags have higher transmission rates and ranges but are also more expensive than LF tags. RFID smart cards, working at 13.56MHz, are the most common member of this group.

UHF tags have the highest transmission rate and range among all tags. They range from 3~6 meters for passive tags and more than 30 meters for active tags. High transmission rate of UHF allows reading a single tag in a very short time. This feature is important in the application where tagged objects move very fast and remain within a reader's range only for a short time.

UHF tags are more expensive than any other tag and are severely affected by fluids and metals. These properties make the UHF tags most appropriate in automated toll collection systems. Typical frequencies of UHF tags are 868MHz (Europe), 915MHz (USA), 950MHz (Japan), and 2.45GHz. Frequencies of LF and HF tags are license exempt and can be used worldwide while frequencies of UHF tags require a permit and are different from country to country.

4. SENSORS IN IOT

4.1. Sensor classification

The wireless sensor network application field can be divided into three main categories [11-12]:

- Monitoring space:

For example: environmental monitoring. Sensors are deployed in particular environments including forests, and mountains in order to gather environmental parameters during long periods. Temperature, moisture or light sensor readings allow analyzing environmental phenomena.

- Monitoring objects:

This category centers on observing particular objects. Structural monitoring is one of the possible illustrations. By sensing modes of vibration, acoustic emissions and responses to stimuli, mechanical modifications of bridges or buildings indicating potential breakages of the structure may be detected.

- Monitoring interactions between objects and space:

Monitoring interaction between objects and space is the combination of both previous categories and includes monitoring environmental threats like floods and volcanic activities.

The proposed classification can be extended by an additional category monitoring human beings. The deployed sensors can gather acceleration information and physiological parameters like heart beat rate. Especially in applications in the medical area, such deployments may help diagnosing bipolar patients and monitoring elderly people in a home [10].

The proposed classification illustrates the high diversity of sensors applications in term of monitored subjects and environments. Beneficial for the Internet of Things, this important scenario diversity must however be taken into account by considering suitable approaches for the sensor integration into IoT.

Under the context of diversity of sensors, we consider the two main driving factors that take place in an industry environment: business and technology considerations as presented below [11].

4.2. Business Considerations

- Cost:

The overall amount that needs to be allocated so as to make the sensor operational. This includes not only the cost of the hardware but possibly any software which must be purchased. The cost is calculated per unit of coverage e.g. a switch can cover a shelf but a camera can cover a room of shelves.

- Installation procedure:

How straight forward or complex is the deployment of the sensor in the correct place and whether or not a redevelopment of several physical parts of the system is required.

- Proven in industry:

Whether the sensor has already been deployed in industrial applications and has satisfactory proven to operate under the rough conditions of a real environment.

4.3. Technical Considerations

- Dimensions:

The size of the sensor, a critical parameter in particular applications.

- Power Consumption:

Influences simplicity of installation and use, an important factor when power supply is not available.

- Reliability:

Detecting false positives/negatives e.g. the human hand is not a product moving in or out.

- Software and hardware requirements:

that is needed in order to support the operation of the sensor.

- Redundancy:

If the sensor or the software can be duplicated in order to take part in a mission-critical system.

- Network requirements:

The communication requirements of the system (wired or wireless), protocol that can support the operation and bandwidth requirements.

.

5. CHALLENGES FOR IOT

The IoT promises to reshape the society. Although the devices technologies discussed in the previous section make the realization of the IoT feasible, more research efforts are still required to overcome challenges at all layers as well as across layers, in order to make the IoT vision a reality. In the following, we present the major challenges to a realization of the IoT [13-16].

6.1. Small Physical Size

The IoT vision predicts a future where we will be surrounded by smart environments that constantly take care of and assist us in every aspect of our life. In order to realize this future, it is desired that the augmenting devices, i.e., devices that are to be attached to real-world objects to form Things, are as small in physical size as possible. For example, in healthcare applications, body-worn sensors should be as small in physical size as possible in order to not interfere with patients' daily activities. Current technologies already help to reduce the size of a sensor node to fit in a cubic centimeter via micro-integration techniques and system-on-chip solutions, or even in a few cubic millimeters via laser-based communication.

6.2. Limited Resources

A direct consequence of physical size reduction are limited resources, namely energy, computation, memory, and communication, that can be provided by a single IoT device such as a sensor node or an RFID tag. A passive RFID tag, which is the most popular type of RFID tag, has from 64 bits to 1 KB of non-volatile memory, and an antenna for transceiving RF signals within the typical range of several meters. An RFID active tag has, in addition, an on-board battery, longer transmission-range antenna (could be up to 100 meters), more memory (rarely but could be up to 128 KB), and possibly interfaces to external sensors (for gathering information about the surrounding environment), and an external processing unit (e.g., microcontroller). Such limited resources require a high level of optimization and simplification of programs that run on IoT devices. Furthermore, energy saving is of paramount important for IoT devices, since they are usually cheaply manufactured and deployed in large quantities into the environment, and are expected to operate over long periods of time without manual intervention, making replacement of energy supply (i.e., battery) for each IoT device extremely difficult. Thus, processing tasks must be optimized as well. Last but not least, the IoT implies that every IoT devices should be connected to the IoT network infrastructure and wirelessly communicable. Since wireless communication usually dominates the energy consumption of an IoT device, it should be kept to the absolute minimum.

6.3. Interoperability

The wide range of heterogeneity issues introduced by the among of different IoT devices. Standardization therefore is a must, but is not enough as no single standard can cover everything, as well as some organizations (manufacturers, software companies) would like to follow different standards or even proprietary protocols. A solution is to extend IoT devices with multiple adapters, each of which conforms to a specific standard. However, the complexity of this extension would grow quadratically with the number of standards involved, which is inefficient at the level of low-end IoT devices. To mitigate this problem, bridges between standards are introduced.

Implementation of bridges is usually in the form of a border gateway or proxy that understands the \languages" of a number of different sets of IoT devices, thus acting as a translator among them. Standard bridges, unfortunately, still do not scale with the number of standards, and especially, the number of the IoT devices. Therefore, middleware solutions will play an important role of wrapping the functionalities of the underlying heterogenous technological layers into well-defined and well-organized services that can be used for communication among IoT devices, or used by upper layers (ex. application layer).

6.4. Imperfect and Heterogeneous Data

IoT devices are typically low-cost, low-power, and small in size, so that they can be deployed in large quantity (ex. large-scale RFID systems or sensors), operate on their battery for long time and be unobtrusive to human users. Due to these factors, the data collected by IoT devices will be subject to redundancy (ex. due to RFID tags are read by multiple RFID readers at multiple times), heterogeneity (ex. data come from different kinds of sensors of different organizations, with different sampling rates), and noise, jitter, outages, and outliers (ex. due to environmental influences or hardware malfunction). As IoT-enabled applications and services are built based on the data generated by the IoT, appropriate mechanisms will be needed to compensate for possible impacts of these imperfections on IoT applications.

6.5. Security and Privacy

The attraction of the IoT comes from the pervasiveness of vast numbers of IoT devices that are embedded into and constantly report information about the real world, so that we could interact with the real world much like we can now with the \virtual" world of the Internet and the Web. Unfortunately, this pervasiveness also poses serious security and privacy problems that need to be addressed in order for the IoT to be widely accepted by the public.

The reasons for this are due to the nature of how the IoT works. Firstly, IoT devices spend most of their time unattended, thus can be easily physically attacked. Secondly, the wireless communication between Things and between Things and the Internet is vulnerable to eavesdropping.

Thirdly, complex and resource-demanding security mechanisms are not suitable to be implemented on resource-constrained IoT devices (ex. passive RFID tags or low-end sensor nodes). Fourthly, information about the environment is autonomously and constantly collected by IoT devices without human awareness (ex. smart home applications recording inhabitants' living habits). Finally, how the extremely massive amount of heterogeneous data generated by the IoT is exploited, i.e., who has the right to access what kind of data and when, is not clear. For more information, readers can find detailed discussions about these and other problems as well as potential solutions in [1].

6. CONCLUSION

This paper discussed basics concepts of the IoT. In particular, the architecture of IoT is introduced. The proposed architecture is based on three layers: perception layer which is a sensor-based technology responsible for collecting real time data from different sources. Network layer comprises the tools, which are used in communication of IoT hardware to software applications. Then the application layer which is responsible for processing the huge amount of data and information using knowledge to achieve the objectives of companies.

For perception layer, where RFID and sensors can be placed. We reviewed the technologies of RFID and sensors that enable the existence of the IoT as well as drive its evolution. The principe of RFID is presented, RFID systems consist of two main components: tags and readers. Then we present categories of sensors, there are available in three categories: monitoring space, objects or monitoring interactions between objects and space. As IoT grows in importance, choosing the right technology of sensor to link to the communication module of an IoT device is very important, for this reason many technical and business requirement for implementation were detailed.

Finally, we identified several technological challenges that need to be addressed for a realization of the IoT. We have selected some important challenges emerging IoT adoption: Dimensions, Energy, Security, QoS, and configuration management. Their analysis revealed that the solutions currently deployed in the Internet are not suitable for the limited sensor node resources and consequently, novel mechanisms have to be developed to adapt to this capabilities and constraints. We plan to investigate existing approaches and find suitable modifications for resource-constrained sensor platforms to tackle these challenges.

REFERENCES

[1] L.Atzori, A.Iera and G.Morabito "The Internet of Things: A survey" Computer Networks, 2010, No. 54, pp 2787–2805

[2] O.Vermesan and P.Friess "Internet of Thing from research and innovation to Market Deployement" River publishers 2014

[3] Y.Wang « The Development of Wireless Personnel Positioning in Internet of Things Based on ZigBee and Sensors » International Journal of Digital Content Technology and its Applications, 2012, Vol. 6, No.12, pp 47-54

[4] A.S. Atkins and N.Alharbe "Sensor Technologies using ZigBee and RFID within the Cloud of Internet of Things in Healthcare Applications" International Journal of Computing Science and Communication Technologies, 2014, Vol.6, No. 2, pp 923-929

[5] R. Sujitha, N.V. Raghavan, K. S. Suganya and A. Devipriya "A Novel Survey on Internet of Things Security and its Application » International Journal of Advanced Information and Communication Technology, 2014, Vol.1, No.8, pp 726-730

[6] K.Hong-yan « Design and Realization of Internet of Things Based on Embedded System Used in Intelligent Campus » International Journal of Advancements in Computing Technology, 2011, Vol.3, No.11, pp 291-298

[7] P.Darcy, S.Tucker, B.Stantic " Integrating RFID Technology with Intelligent Classifiers for Meaningful Prediction Knowledge" Advances in Internet of Things, 2013, Vol.1, No.3, pp 27-33

[8] S.Amendola, R.Lodato, S.Manzari, C.Occhiuzzi, and G.Marrocco "RFID Technology for IoT-Based Personal Healthcare in Smart Spaces " IEEE Internet Of Things Journal, 2014, Vol.1, No.2, pp 144-153

[9] S.Yu , Y.Peng , J.Yang "Research of routing protocol in RFID-based internet of things" International Journal of Computer and Information Technology, 2012, Vol.01, No.02, pp 94-96

[10] K. Anagnostopoulos, A. Vakaloudis, N. Chalikias, C. Leslie, J. Liang "Evaluating Sensor Technologies for Gate-Based Object Counting in an Internet of Things Set-up" Sensors & Transducers, 2015, Vol. 185, No.2, pp. 1-6

[11] V.Potdar, A.Sharif and E.Chang "Wireless Sensor Networks: A Survey" 2009 International Conference on Advanced Information Networking and Applications Workshops

[12] S. K. Gupta and P. Sinha "Overview of Wireless Sensor Network: A Survey" International Journal of Advanced Research in Computer and Communication Engineering, 2014, Vol. 3, Issue 1, pp 5201-5207

[13] K.Cai « Internet of Things Technology Applied in Field Information Monitoring" Advances in information Sciences and Service Sciences, 2012, Vol.4, No.12, pp 405-414

[14] K.Boulos and Al-Shorbaji "On the Internet of Things, smart cities and the WHO Healthy Cities" International Journal of Health Geographics 2014, Vol.13, No.10, pp 1-6

[15] C.Turcu, C.Turcu and V.Gaitan « Integrating robots into the Internet of Things" International Journal of Circuits, Systems and Signal Processing, 2012, Vol.6, No.6, pp430-438

[16] O.Said M.Masud "Towards Internet of Things: Survey and Future Vision" International Journal of Computer Networks (IJCN), 2013, Vol.5, No.1, pp 1-17