The Role of Ad Hoc Networks in the Internet of Things: A Case Scenario for Smart Environments

Daniel G. Reina, Sergio L. Toral, Federico Barrero,
Nik Bessis, and Eleana Asimakopoulou

Abstract. Internet of Things is an emerging area and it visions an inter-connected world full of physical as well as virtual objects, devices, processes and services capable of providing a different lens on how to link them via the Internet. While Internet of Things as part of the Future Internet has been described as a paradigm that mainly integrates and enables several technologies and communication solutions a notable interest is to define how current standard communication protocols could support the realization of the vision. Within this context, we offer a state-of-the-art review on ad hoc and wireless sensor networks, near field communications, radio frequency identification and routing protocols as a mean to describe their applicability towards an Internet of Things realization. We conclude by presenting a brief case scenario to describe a future smart environment and illustrate its possible model architecture.

1 Introduction

For many years, wired networks used to be the only way to connect computers to the Internet. During the last decades, wireless communications have changed inter-connectivity by enabling computers to communicate and also exchange information stored on them on a wireless fashion. While the Internet is formed primarily by inter-connecting homogeneous devices (i.e. computers) there have been recently several paradigms in networking such as mobile, grid and cloud computing which enabled a purposeful inter-connectivity between various semi-homogeneous devices such as computers, cameras, smart-phones, sensors and other instrumentation (i.e. satellites).

The latest vision is to enlarge the inter-connectivity between devices making possible the formation of pure heterogeneous networks and contexts by inter-connecting hardware devices ranging from computers to simple sensors. This is by

Daniel G. Reina · Sergio L. Toral · Federico Barrero
Electronic Engineering Department, University of Seville, Spain
e-mail: dgutierrezreina@us.es, {toral,fbarrero}@esi.us.es

Nik Bessis · Eleana Asimakopoulou
School of Computing and Maths, University of Derby, UK
e-mail: n.bessis@derby.ac.uk, eleana.asimakopoulou@gmail.com

N. Bessis et al. (Eds.): *Internet of Things & Inter-cooperative Comput. Technol.*, SCI 460, pp. 89–113.
DOI: 10.1007/978-3-642-34952-2_4

visioning an Internet of Things (IoT), an inter-connected world full of physical as well as virtual devices capable of providing services over the Internet. Within the IoT context, a thing refers to a physical or virtual object such as spaces and rooms, chairs, fruits, bottles, clothes, suitcases and bags, animals or even a process and a service like a cloud virtual machine.

During the last years, IoT has emerged as one of the most important paradigmatic strings of thought with regards of the future state of Internet. Its importance is described in terms of providing a different lens on how to link the Internet with real world's objects. In contrast to currently dominant paradigm within Internet which is based on human-to-human interaction, the IoT paradigm proposes a novel emerging paradigm of thought which postulates that any object, identified with a unique identifier will be considered as inter-connected [1]. As such, IoT has been proposed as a combination of the Internet and emerging technologies such as near-field communications, real-time localization, and embedded sensors as a way to transform everyday objects into smart objects [2]. Those objects can be transformed in ways that they can be understood better by reacting to and with their environment in a more advanced and meaningful manner. IoT has also been described as a paradigm that mainly integrates and enables several technologies and communication solutions including but not limited to tracking technologies, wired, wireless sensors, their networks, exchanged networked communication which in turn, lead to a shared next generation Internet, what is also known as Future Internet. IoT has also been defined as ''a world-wide network of inter-connected objects uniquely addressable, based on standard communication protocols.'' In a more comprehensive way, it has been perceived as a paradigm that connects real world with digital world [3].

Within this context, one of the fundamental challenges for the IoT realization is that like when integrating heterogeneous data that have been originally produced for a purpose other than their integration [4], objects also differ significantly in terms of their functionality, technology and application and in other words, they have been originally produced for a purpose other than their inter-connection over the Internet communication environment.

The development in digital hardware made possible portable computers, increasing the mobility, processing capability and reducing size and cost. While static powerful computers are already capable of participating in Internet and thus, in web-based communication services, small simple hardware devices will also be able to inter-connect in an IoT setting by using Radio Frequency Identification (RFID) techniques.

On the other hand, ad hoc networks have attracted a lot of attention in the last decades. They represent a new paradigm of communications where decentralized wireless nodes communicate with each other in a collaborative way to achieve a common goal. Nodes collaborate to establish unicast or multicast communications between a source node and a one or several destination node(s). When mobility of nodes is considered, communications refer to Mobile Ad Hoc Networks (MANETs). With the increment of mobile devices which are equipped with wireless transceivers such as smart phones, tablets, sensors and so on, the number of deployed devices with wireless communications capabilities is continuously

increasing. Commercial wireless technologies such as Bluetooth, UWB, WiMAX, Wi-Fi or Zigbee make possible the connections among devices that are made by different manufactures, enabling ad hoc communications to be established on either regular or ad hoc basis. When vehicles are capable of exchanging information among them Vehicular Ad Hoc Networks (VANETs) are formed. Mobility is an intrinsic characteristic in VANETs, but unlike MANETs fixed mobility patterns are followed in vehicular scenarios. VANETs enable the formation of Intelligent Transport Systems (ITS). Normally, two types of communications can be found in ITS, (a) Vehicle-to-Vehicle communications (V2V) that is two or more vehicles forming a VANET, and (b) Vehicle-to-Infrastructure communications (V2I) that is a hybrid VANET with both static and mobile nodes. In general, the aforementioned communications can be extended to include nodes to infrastructure communications (N2I), where the nodes may be either vehicles or people. The fixed infrastructure can be easily connected to Internet acting as an access point for the VANETs or MANETs. Furthermore, the deployment of Wireless Sensor Networks (WSNs) is a reality in urban scenarios by sensing data parameters such as temperature, humidity, CO2 emissions, etc. The integration of MANETs, VANETs, WSNs and the fixed infrastructure is an interesting challenge which will enable the IoT manifestation, see Figure 1.

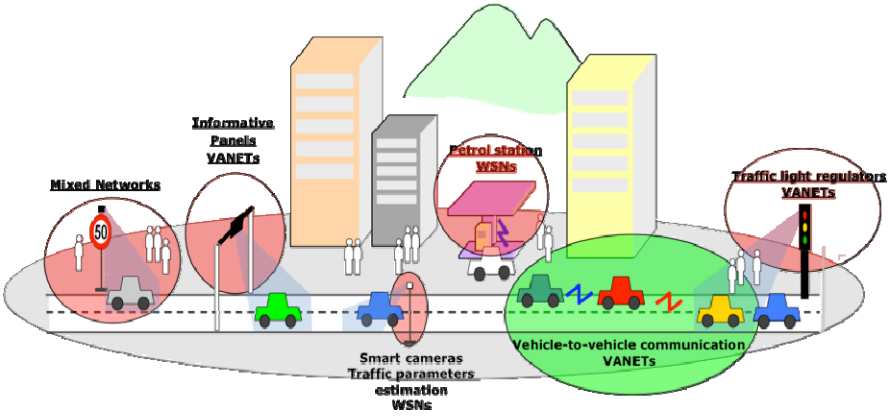

Fig. 1 Example of different network's deployments in the Internet of Things (IoT)

With these intelligent ambiences the provided services in wireless networks will increase notably as well as the complexity of them. The interactions with an urban smart environment will permit the collection of information from the environment and improve the decision-making of human beings. For that to happen, a high connectivity level between objects, processes, services and people must be guaranteed. While there will be a significant increase of the number of deployed wireless devices within the environment there should be a scalable infrastructure capable in enabling sufficient and full utilization of available resources as to take advantage of the IoT concept potential capabilities. Apart from that, the concept of

green wireless networks has been lately appeared with the aim of reducing the use of resources in wireless communications as to reduce energy consumption. Having said that, it has been proved that the majority of energy is consumed during the access point stage in wireless communications since the terminal devices like mobile phones are optimized to be fed by batteries having low power consumption. The ad hoc networks have been proposed and implemented in numerous applications areas such as disaster management [5] [6] [7], health care [8], intelligent transportation systems [9], traffic management, and military applications among others [10], due to their self-organized and decentralized features.

In this chapter, we aim to offer a state-of-the-art review of the role of ad hoc networks in IoT. To achieve this, we start off with a review on the classification of ad hoc networks including mobile and vehicular ad hoc networks, wireless sensor networks and radio frequency identification. While we provide a discussion of their functionality we also highlight and brief their application and how these could be realized in an IoT setting (section 2). We also provide a discussion of routing protocols for IoT in an effort to present existing routing protocols applicability and suitability for an IoT realization (section 3). In section 4, we do present a visionary business scenario to illustrate a possible IoT model architecture. We finally conclude in section 5.

2 Classification of Ad Hoc Networks

2.1 Mobile Ad Hoc Networks (MANETs)

Mobile Ad Hoc Networks are self-organized networks which are deployed without the need for any fixed infrastructure. Having seen them as a new paradigm of mobile wireless communication, MANETs have attracted a lot of attention during the recent years. In MANETs every entity is called a node and works independently as a router. In the context of IoT, MANETs could represent scenarios such as people using mobile phones, a rescue team in an evacuation operation or soldiers in military applications, among others. MANETs are self-configuring, self-maintaining, self-healing, and self-repairing networks and such features are very suitable for mobile computing. The mobility of nodes is an intrinsic characteristic of nodes in MANETs which make even more challenging the deployment of these networks in real environments. The design of MANETs is much focused on routing protocols. They are one of the key components of MANETs. Figure 2 shows the importance of routing protocols in MANETs. The source node requires certain service A so it generates a discovery process to find such a service. The black arrows represent the discovery process flow. The intermediate nodes retransmit the incoming request until any request reaches the destination node. The destination node is the element of the network that can supply the required service.

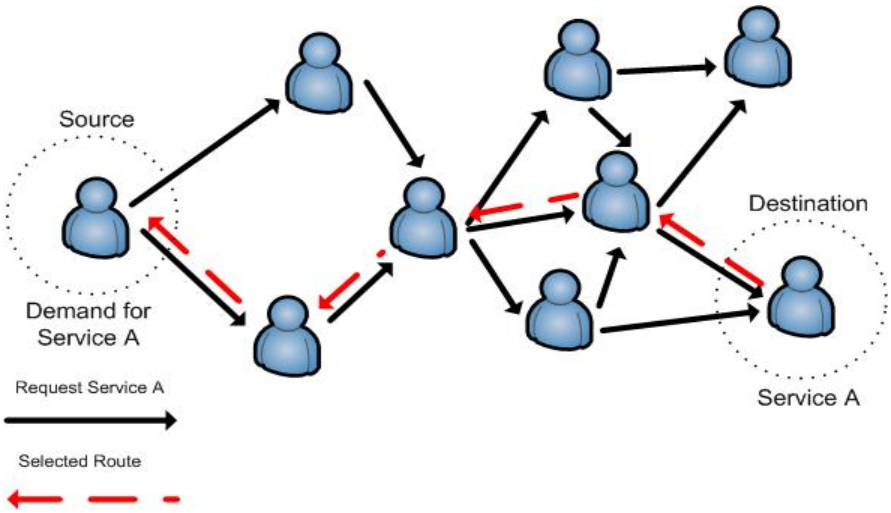

Fig. 2 Routing protocols in MANETs

Whenever several routes are found, the routing protocols are responsible for selecting the most appropriate route among those found. Several metrics are normally used to determine the quality of routes, such as hop count distance, end-to-end delay, and throughput. Since the mobility of nodes causes very changeable topologies, routing protocols should deal with such mobility conditions by acting against possible changes and implementing mechanisms to re-establish broken communication routes. Another important issue related to the discovery process of routing protocols in MANETs is the broadcast storm problem caused by the redundancy of request packets. As can be seen in Figure 2 many packets are redundant. This causes packet collisions and packet contentions which deteriorate the performance of ad hoc communications. In order to cope with this issue, several solutions have been proposed including GOSSIP, Multipoint Relay, Connected Dominant Sets and counter-based schemes. The main idea behind these algorithms is to reduce the number of redundant packets in the discovery process of routing protocols.

Mesh networks have appeared in recent years as an extension of typical ad hoc networks. Bruno et al [11], defined mesh networks as a flexible and low cost extension of wired infrastructure networks in which nodes collaborate with fixed infrastructure. Unlike MANETs, mesh networks are hierarchical networks, see Figure 3. Mobile nodes communicate with wireless routers which connect to access point in order to establish Internet connections. The wireless routers are forming a backbone which connects the “wired world” to the “wireless world”. Note that there is a high redundancy of connections in mesh networks so routing protocols must be focused on selecting the best path towards the wired world. Another important issue is to guarantee fairness in the network. MAC and routing protocols must guarantee that each user receives the same fair share of resources independent of how far is from the access point.

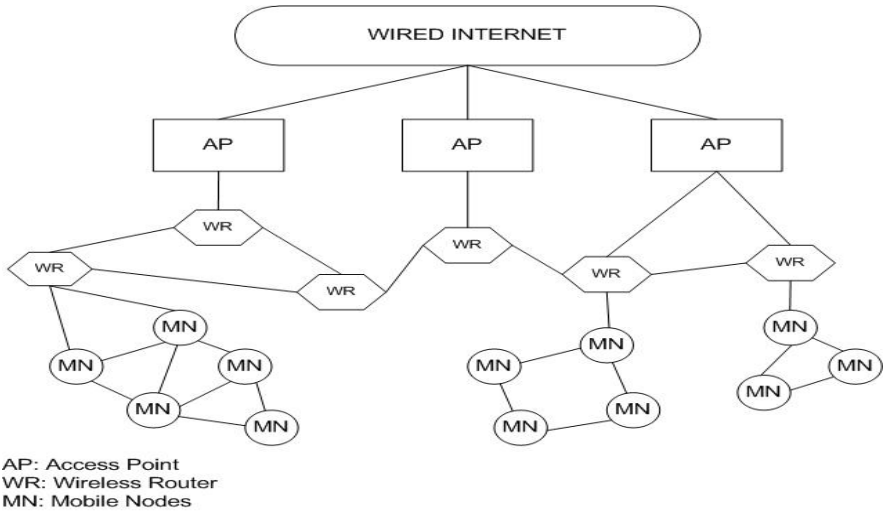

Fig. 3 Architecture of mesh networks

2.1.1 Service and Resource Discovery in Ad Hoc Networks

Service and resource discovery are also crucial for an efficient performance in ad hoc networks. Nodes must be aware of the available services and resources in their vicinity. Service and resource discovery mechanisms should work in collaboration with routing protocols. Two types of architectures have been proposed to develop service discovery [12]: 1) directory based architecture and 2) directory-less based architecture. The directory based architecture can also be divided into two categories: a) centralized directory and b) distributed directory. In the directory-less based architectures, nodes reactively request services and proactively advertise services. On the contrary, directory based schemes encompass a directory agent which is in charge of registering and handling services. Depending on the number of nodes which implement the directory agent we can distinguish between centralized directory and distributed directory. These nodes are responsible for keeping up-to-date the existing directory of services available in the network. The services discovery mechanisms are also very important for connecting ad hoc networks to the IoT.

2.1.2 Applications of MANETs

Since mobile ad hoc networks are self-organizing networks, they are suitable for those applications in which the deployment of a new fixed infrastructure is unfeasible and/or costly. In addition, the capability of dealing with mobility conditions makes MANETs appropriate for mobility applications. In addition, MANETs can also be used as a backup network whenever the main wired network fails, e.g. in disaster scenarios. The main applications of MANETs are [12]:

- Tactical networks: Military operations in battlefields
- Emergency services: Evacuating and rescue operations, disaster recovery, and health care applications
- Commercial and civilian environments: E-commerce, sport stadiums, and vehicular services among others
- Home and enterprise networking: Home networking, conferences, etc
- Education: Universities and virtual campuses
- Personal Area Networks: Clothing, etc
- Entertainment: Multi-user games, robotic pets
- Context aware services: Location specific services and time dependent services
- Coverage extension: Extending cellular network access.

2.1.3 Connecting MANETs to IoT

Several approaches have been proposed to connect mobile ad hoc networks to Internet. Since nodes in mobile ad hoc networks have IP addresses for routing purposes, it could be logical that such IPs may be used to route a packet through Internet. However, the main problem of this approach is that a node needs an efficient way to work out whether a certain address in the MANET is present or not and whether it is necessary to use a gateway or an access point. In principle, nodes are not aware of their contexts so it is difficult to collect neighboring nodes IPs. Discovery procedures must be carried out in order to collect neighboring information. However, these processes are normally time and message consuming since they require nodes to exchange a high number of packets. Normally, an access point should be placed so as to enable mobiles nodes connect to Internet. The effective placement of a gateway could be a challenging design factor due to the mobility of nodes and the optimum placement for a gateway could strongly depend on mobility conditions. As a consequence, the access point could be also mobile. Another approach is to use two different IPs, one to communicate through Internet and another one to identify nodes in the MANET. However, nodes can move freely so the target gateway could be changeable. If a node switches to another gateway, a new IP address should be used and the outgoing connections will probably break. Another possible approach is to use dynamic addresses by using the dynamic host configuration protocol (DCHP). This approach solves the problem of IP address when nodes are moving. On the other hand, the increasing use of smart mobile phones enable nodes to connect to Internet through cellular technologies such as 3G and 4G technologies, for instance the emerging Long Term Evolution (LTE) technology. However, these technologies are not unlicensed so users (or object owners within the IoT context) have to subscribe to these services. In addition, satellite communication can also be used in safety-related applications like military applications. To sum-up, the connection of ad hoc network to Internet is still a challenge requiring further research.

2.2 *Vehicular Ad Hoc Networks (VANETs)*

Vehicular Ad Hoc Networks could be seen as a specific type of MANETs. However, it has become a different research field in the last few years. Although this fact is noticeable, it is also clear that both VANETs and MANETs share similar features such as multi-hop communications, changeable topologies, mobility and power transmission constrains. VANETs have arisen from the increased wireless communications in vehicles. Nowadays, most vehicles are equipped with Bluetooth transceivers so it can be seen as the standard for intra-vehicle communications. To establish V2V other technologies such as WiFi and Zigbee are preferred since their performances are more suitable for longer distances. In recent years, the IEEE 1609 family for Wireless Access in Vehicular Networks (WAVE) [13] – which relies on the standard IEEE 802.11p – has become a promising technology for both V2V and V2I communications.

Figure 4 illustrates V2V communications in a VANET. This situation emulates a significant situation where one vehicle is aware of certain warning. This warning may be information about traffic or environment related conditions. In such situation, the node must inform others about the warning so as for other vehicles to adapt their behaviors appropriately. This dissemination should be done as quickly and as effective as possible. Since the density of nodes could be high, there is a trade off between reducing redundancy and increasing reliability of packets. Furthermore, mobility of nodes is a crucial parameter is VANETs since it is normally higher than in MANET scenarios. Mobility should be taken into account by routing and MAC protocols to adapt their performances to such high mobility conditions. The last vehicle on the queue, see Figure 4, may require adapting its speed to match the collected information from other vehicles and infrastructure. The establishment of connections should be done rapidly to permit the information to be exchanged by vehicles in a short time (directly via V2V or indirectly via V2I). For instance, Bluetooth connections take a long time to be established, and therefore Bluetooth could not be suitable for this short of V2V communications.

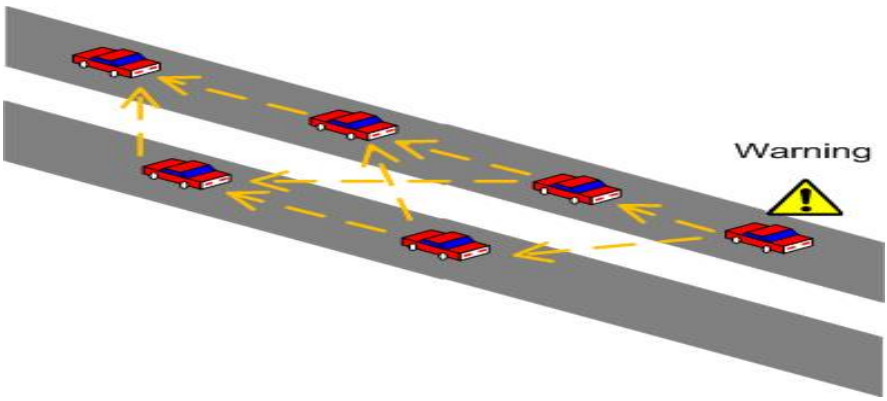

Fig. 4 Vehicle-to-Vehicle (V2V) communications

Several examples of V2I communications are illustrated in Figure 5. In these situations nodes are informed on certain conditions such as the state of traffic lights, traffic signals, or the state of traffic barriers. Clearly VANETs help to improve driver's decision making. Unlike pure MANETs, a VANET can collaborate with fixed infrastructure. The features of vehicular ad hoc networks can be improved by using wired network as backbone for providing data services. However, the deployment of Access Points (APs) is a challenging task since it depends on parameters like density and traffic conditions. The ideal placements for APs in vehicular networks are the typical vehicular public infrastructure such as traffic lights, light poles, and so on. Such hybrid behavior means that vehicles can communicate to APs within little number of hops leading vehicles forming self-organized wireless networks. A stand-alone sight of VANETs is only possible in dense networks. However, vehicular networks are very changeable and only under congested traffic flow such assumption could be ensured.

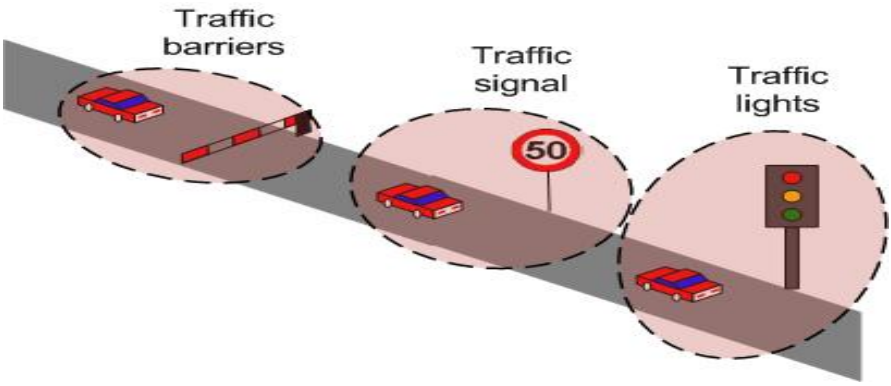

Fig. 5 Vehicle-to-Infrastructure (V2I) communications

Unlike mesh networks, VANETs are not hierarchical networks. In V2I communications, vehicles communicate directly with APs.

2.2.1 Applications of VANETs

Vehicular communications are aimed to form intelligent transportation systems using mobile devices and fixed infrastructure. Many applications are focused on improving the safety conditions in vehicles. The main applications of VANETs are [14]:

- Navigation safety applications: Prevention of traffic accidents, dissemination of warning messages, improvement of driver decision-making, post accident information, etc
- Navigation efficiency: Intelligent transportation systems, road congestion avoidance, and pollution mitigation among others

- Entertainment: Download multimedia, video streaming, etc
- Vehicle monitoring: Mobile sensor networks through vehicle communications
- Urban sensing: Congestion, traffic flows, pollution, etc
- Social networking: Friendship, proximity and correlation analysis
- Emergency: Evacuation emergency, disaster scenarios, etc.

2.2.2 Connecting VANETs to IoT

Similar mechanisms of that used in MANETs are also used in VANETs to connect vehicles to the IoT. Consequently, the vehicular networks are normally connected to Internet by means of APs using a Wireless Local Area Networks (WLAN) technology such as WiFi, WiMAx or Bluetooth.

2.3 Wireless Sensor Networks (WSNs)

Sensor networks are normally centralized networks where there is a central node in charge of gathering sensed data from sensor nodes [15]. The central node is called the sink of communications. The collected information is usually environment-related. Parameters such as temperature, humidity and proximity are normally measured. However, there have been important advances in electronic, micromechanical and chemistry manufacturing processes that make possible to find more sophisticated sensor nodes. The main characteristic of WSNs is the limited resources available in terms of memory and power energy. WSN nodes are fed by batteries so power consumption is an important design factor in WSNs. To tackle such constraints, nodes should transmit efficiently their sensed data to the sink node. Consequently, the majority of routing and MAC protocols for WSNs are focused on reducing the node's power consumption in order to extend the lifetime of the network and to avoid frequent battery replacements. The topologies of WSNs are less changeable than that of MANETs or VANETs. In general, nodes are static in WSNs, so topological changes are due to bad performances of nodes mostly, i.e. low battery problems or medium access problems. Peer-to-peer (P2P, also known as mesh), Star and Tree topologies are common topologies found in deployed WSNs, see Figure 6.

In star topology the nodes are normally located at only one hop distance from the sink so redundant data can be collected from different sensors. The sink is in charge of post-processing such information. In both mesh and tree topologies multi-hops communications take place. Several algorithms based on graph theory have been proposed to reduce power consumption such as minimum Connected Dominant Set (CDS) or minimum Spanning Tree. As the data is post-processed by sinks, they are normally connected to a higher-level network like Internet in order to monitor the network. With regard to IoT, WSNs can be seen in two different ways: 1) Every node is a different entity or 2) the whole network is an entity accessible through the sink node which has full information about the network. This point of view is very interesting since a WSN can be integrated into more complex networks. A further step in WSNs is the Wireless Body Area Networks (WBAN)

[16]. These networks rely on the feasibility of attaching or implanting very small bio-sensors inside the human body that are comfortable and that do not impair normal activities. The main application area of WBANs is health care applications. For example, nodes are attached on or inside human body in order to sense body parameters and then to communicate wirelessly to a central node which is connected to Internet. WBAN will effectively make possible, doctors to monitor patient's health in real time, anywhere and at any time.

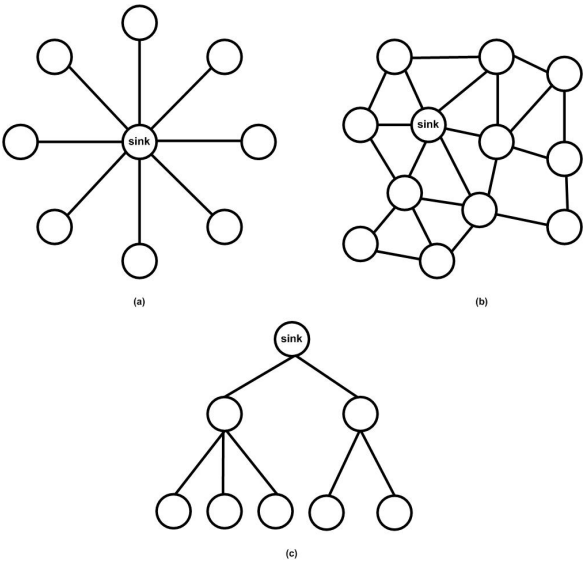

Fig. 6 WSN Topologies: (a) Star topology; (b) P2P or mesh topology; (c) Tree topology

The manufacturing process is the main challenge in WBANs since it is a multidisciplinary process involving electronic, chemistry and wireless communications, among others. There has also appeared a new tendency for including actuator nodes in WSNs forming a new type of network called Wireless Sensor and Actuator Networks (WSANs) [17]. In WSANs three types of nodes can be distinguished sink, sensor and actuator. While sensors are capable of sensing the environment, actuators are capable of acting on it. As in WSNs, sink nodes gather information from sensor nodes. WSANs should not be seen as a mere extension of WSNs since they have their own features. Actuator nodes are more complex and powerful nodes as compared to sensor nodes so a WSAN should not be considered as a homogeneous network. With regard to communication flows, there is a significant difference from WSNs. In WSANs multiple sensors may send data to a sink node, and multiple sinks may send data to an actuator node. As a consequence, communications can be divided into two types: one-to-many and many-to-one communications. To sum up, the interaction of WSNs with the IoT will enable to provide more useful services related to real-time data monitoring.

2.3.1 Applications of WSNs

The main applications of wireless sensor networks are related to monitoring ambient conditions. With the development of micro-electromechanical systems (MEMS) and digital electronic manufacturing, the variety of available sensors is increasing. In addition, the cost of sensor is decreasing as well. Such scenario makes possible to extend the scope of WSNs applications. The following list includes some important WSNs application areas [15] [18]:

- Military applications: Monitoring friendly forces, equipment and ammunition, battlefield surveillance, reconnaissance of opposing forces and terrain, and battle damage assessment among others
- Environmental applications: Forest fire detection, bio-complexity mapping of the environment, agriculture, flood detection, etc
- Healthcare applications: Tele-monitoring of human physiological data, tracking and monitoring doctors and patients and drug administration in hospitals
- Home applications: Home automation and smart environments.

2.3.2 Connecting WSNs to IoT

Since sensor nodes are simple devices with limited resources, the major issue is how to connect such simple devices to an inter-connected world of things. Several architectures have been proposed to connect WSNs to Internet. These architectures can be classified into three categories [19]: 1) the IP overlay over WSN, 2) the sensor overlay over IP, and 3) the higher-level gateway overlays.

When IP overlay over WSN, sensor nodes should be addressed with IPs as the same nodes connected to Internet. This scheme is complicated due to the limited networks resources of sensor nodes. In directed diffusion routing, which is typically used in WSNs, sensor nodes are not addressable with IPs. However, this model is drawing a lot attention in last few years thanks to the integration of IPv6 in sensor networks. In the second model data is encapsulated in IP packets. When the sensed data arrive at the sink, it encapsulates the data in IP packets. In the third level, WSNs and Internet are seen as two separate networks. A linking entity, the gateway, is responsible for adapting the incoming traffic from both networks. The gateway translates routing information of Internet into WSN routing mechanisms. Clearly, the first model represents the pure paradigm of the IoT in which each entity can be addressable. The protocol 6LoWPAN is an example of an implementation of the first model [20]. This is a version of the new IPv6 networking protocol for WSNs developed by the Internet Engineering Task Force (IETF) in the working group 6LoWPAN. The protocol 6LoWPAN is developed over the IEEE 802.15.4 standard. In this protocol, the features of IPv6 are adapted to the WSN constraints. The project Blip 2.0 [21], which is developed at the University of Berkeley, implements Ipv6 for TinyOS an operating system for WSNs [22]. In the second model, the sink node is connected to Internet and the sensor nodes are virtualized. The third model is the classical architecture for connecting WSNs to Internet. The sink node has an adapter in order to translate IP packets from Internet nodes.

On the other hand, the developments of middleware for WSNs are playing an important role in the introduction of WSNs in the IoT. Middleware provides users an abstraction of low communication layers of sensor nodes. MIRES is an example of middleware architecture for WSNs [23]. It is built on top of TinyOS and provides routing and service interfaces based on the publish/subscribe paradigm. WSN-SOA is an implementation of service-oriented architecture (SOA) for WSNs [24]. WSN-SOA is also implemented over TinyOS. The available attributes and the operations are described as web services. However, important modifications have to be done over the classical SOA in order to deal with the limited resources of wireless sensor nodes.

Constraint Application protocol (CoAP) [25], which is being developed by the IETF in the working group CoRE, is intended for designing a generic web protocol for the special requirements of this constrained environment, especially considering energy, building automation and other Machine-to-Machine (M2M) applications. CoAP is based on 6LoWPAN so it implements the first model. The interaction model of CoAP is similar to the client/server model of Hypertext Transfer Protocol (HTTP). Another similar approach was proposed in [26], the TinyREST that is a protocol aimed to connect WSNs to the Internet using Client/Server architecture. Sensor nodes in REST are addressed via Uniform Resource Locators (URL) using the Hypertext Transfer Protocol (HTTP) and its methods for accessing them. In TinyREST the client is a sensor and the server is a computer connected to the Internet. Consequently, TinyREST is based on the third connection model since there is a gateway to connect the WSN to the Internet. The HTTP methods such as GET, POST, PUT and DELETE, are also used in TinyREST. Moreover, TinyDB allows users to see WSNs as a database [27]. The data sensed by nodes is the information available in a database and it is accessible by sending SQL-like queries. Figure 7 illustrates several architectures for connecting WSNs to IoT.

On the other hand, Pachube is an open source platform that enables developers to connect sensor data to the IoT [28]. Pachube lets user tag and share data from physical and virtual devices through the Internet. The goal of Pachube is connecting to the environment rather than connecting to things. Pachube platform allows users to visualize world-wide data sensor through the Internet.

Furthermore, the idea of including sensor networks in the IoT is attracting the attention of several large companies. For example, the Hewlett-Packard with the Central Nervous System for the Earth (CeNSE) project is aimed to build a worldwide sensor network. The main goal of CenSE project is to deploy a massive amount of nano-scale sensors and actuators embedded in the environment and connect them via an array of networks with computing systems, software and services to exchange their information among analysis engines, storage systems and end-users. The main feature of CeNSE project is that HP is developing its own technology based on accelerometer to measure environmental parameters.

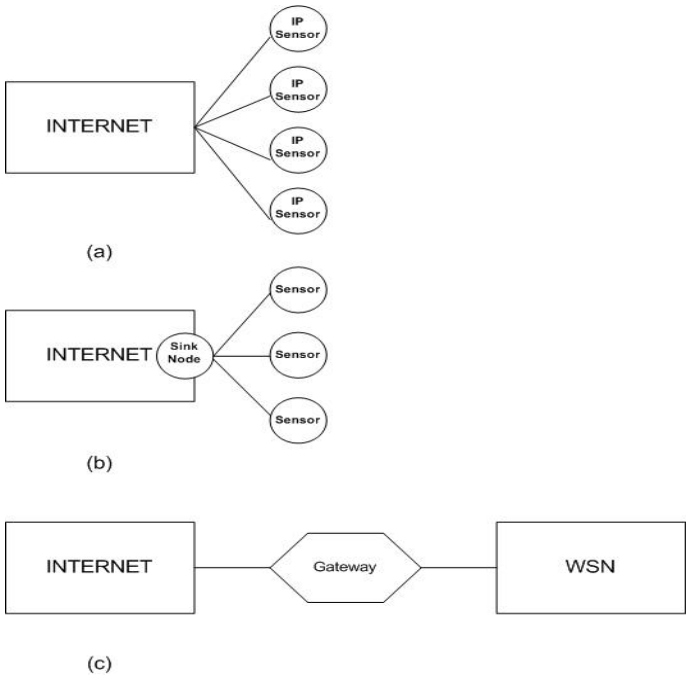

Fig. 7 Architectures for connecting WSNs to IoT

2.4 Radio Frequency Identification (RFID)

Another promising technology for supporting the IoT manifestation is RFID technology. It enables low-data communications between a simple device so called a tag, and a tag reader which is normally connected to a computer system. RFID communications have been used to identify and track objects wirelessly. Unlike bar codes, the RFID tags do not need to be within line of sight to communicate each other.

Two types of tags can be found, 1) passive tags which do not rely on any energy source and 2) active tags which contain an energy source like a battery. The main advantage of passive tags is that they do not require any power supply so they are simpler and cheaper than active tags. Passive tags use the radio energy transmitted by the reader as its energy source. The low cost of passive tags will enable a massive deployment of RFID tags attached to ordinary things like clothes, suitcases, bags, and so on. The information stored in the tags depends on the target application and the storage capability of a tag is limited by a few kilobytes of data.

RFID systems currently operate in the Low Frequency (LF), High Frequency (HF) and Ultrahigh Frequency (UHF) bands. Each frequency has its advantages and disadvantages. There is not any ideal frequency for all applications. In general, lower frequency means lower read ranges and slower data read rates.

LF-RFID systems are typically 125 kHz with a shorter read range (<0.5 m or 1.5 ft). LF-RFID systems tend to be less sensitive to interference than higher RFID systems. HF-RFID systems operate at 13.56 Mhz with read range which less than 1 m or 3ft. UHF-RFID systems utilizes the 860 to 930 MHz band, typically 860 MHz in Europe and 930 MHz in North America. The read range of ultrahigh RFID systems is up to 3 m or 9.5 ft.

RFID technology has been envisioned as the key wireless technology to accomplish the IoT. For instance, Electronic Product Code (EPC), which was created at MIT Auto-ID Center, was conceived as the starting point to develop the IoT. The EPC was designed as a universal identifier of every physical object in the world. Currently EPC is managed by EPCGlobal and it is aimed to identify a specific item in a supply chain context. In addition to the EPC code, EPCGlobal also provides the necessary infrastructure for a global IoT. However, EPCGlobal objectives are focused on industrial applications and in particular, for serving tracking and logistics management. The EPC network architecture enables partners of a business chain to share information. The main functionality of EPC network can be summarized as follows [29]:

- Provide linkage between physical objects and EPC tags.
- Manage huge amount of data from RFID sources.
- Provide a universally data format for transferring information.

The EPC network architecture is composed of tags, readers, middleware layer, information service layer, Object Name Service (ONS), Discovery Service (DS) and the Enterprise Applications [30]. Tags and readers are the sources of information. The middleware layer so-called Savant is in charge of capturing information from readers and managing that in order to provide meaningful data. The information service layer acts as a repository about any items identified. The ONS allows tracking objects and the DS is a set of service that enables user to find the data related to specific objects. Further detail about EPC network can be found in [29]. On the other hand, eCloudRFID [30] is framework architecture for mobile devices with the goal of facilitating the development process of embedded RFID applications and the integration of business applications and EPC networks instances. As in EPC network architecture, a middleware layer is necessary to connect the physical world with the IoT.

The RFID ecosystem [31] created at the University of Washington is oriented to investigate patterns of adoption and utilization of RFID applications in a realistic day-to-day setting. They pointed out that creating RFID applications for IoT is challenging since the data associated with tags, antennas, and events must be personalized and carefully controlled to create a safe, meaningful and user experience. They developed several RFID-based web applications such as a search engine for things, social applications, a digital diary, and an event-based search. Such applications can be personalized by using a tag manager. This application enables to transform RFID data into high-level events. The results in [31] show that most users were interested in using RFID applications especially the digital diary.

2.4.1 Applications of RFID

The main applications of RFID communications are identification-related and tracking. However, during the last years new applications are emerging [32] such as:

- Access management
- Retailing industry
- Food and restaurant industry
- Health care industry
- Library applications
- Travel and tourism industry
- Toll collection and contactless payment
- Smart-dusts
- Mechanism to speed up the pairing phase of Bluetooth and WiFi communications (NFC)
- Social networking.

2.4.2 Connecting RFID to IoT

The RFID tags are so far the simplest objects that can be connected to the IoT. RFID readers can collect information from tags and make such information accessible to the Internet. The RFID readers act as translators. As a consequence, those mechanisms applied to WSNs can also be applied to RFID communications. The RFID readers act as sensor nodes and the RFID technology is the wireless interface used to collect information from the tags. The information stored in the tags represents the data sensed from the environment. However, unlike sensor networks, the measurements are triggered whenever a tag gets closer to a reader.

A centralized architecture is presented in Figure 8, in which each reader is connected to a server. This server connects the RFID reader to the Internet. This architecture was adopted in the RFID ecosystem [31].

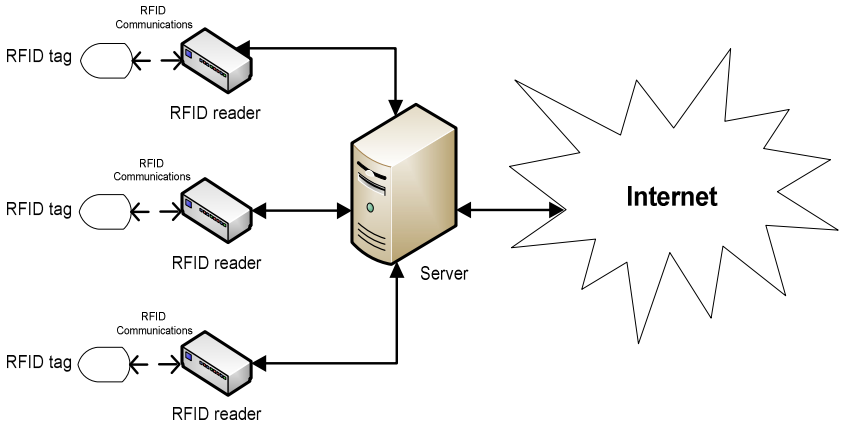

Fig. 8 Connecting RFID technology to IoT

In general, a middleware layer is needed in order to pass a request from the application to the readers. The main tasks of the middleware layer are data filtering and aggregation. Note that the amount of data from readers may be very large and redundant. Savant and eCloudRFID middleware are some example of middleware for connecting RFID data to the IoT. In [33] the authors proposed integrating IPv6 in RFID tags so whenever a RFID reader pass closer it can obtain an IPv6 address for connecting to the Internet.

Mobile phones can also be used as NFC readers so they can serve as translators, converting RFID data into Internet data, see Figure 9. Since the new generation of smart-phones incorporates the functionality for Internet connectivity, the approach can be a reality in the near future.

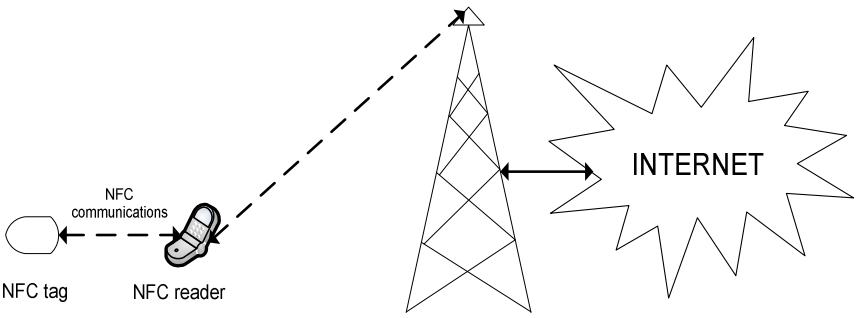

Fig. 9 Connecting NFC to IoT

2.5 Near Field Communications (NFC)

Near Field Communication (NFC) is a set of standards for short-range communications. NFC attracts much of attention [34] and it is estimated that by 2015 today's market value will be increased by eight times. [35] suggest that within the same time frame 785 million NFC enabled devices will be spread across the world, mainly incorporated within smart-phones.

Various companies already utilize NFC, based on the fact that users are more comfortable with using mobile devices as secure payment tools. McDonalds aims to expand the NFC potential by conducting trials that combine mobile-based coupon distribution with payments and collecting user data for marketing purposes [36]. Barclays Bank and Orange launched a service allowing their consumers to tap their phones in order to pay for purchases up to a specific amount by bringing the phone into a close proximity range. Starbucks allows customers to swipe their phones by using an internal service for making payments, instead of using cards or cash. Markets in France use NFC for improving the shopping experience for the visually impaired or elderly people [37].

In NFC communications there is an initiator and a target device that is normally a passive tag. The main advantage provided by NFC technology is that it has been incorporated in the new generations of mobile phones. The first mobile phone

which used NFC was the Nokia 6216 classic. New smart phones, like Nexus S of Google, are also incorporating NFC capabilities. As a consequence, the mobile phone can act as the NFC initiator. Since current mobile phones are connected to Internet, they can easily serve as bridges to transfer RFID information to the IoT. The use of NFC will enable an expansion of RFID applications.

NFC operates at 13.56MHz and its data rates are ranging from 106 kbit/s to 424 kbit/s. NFC protocols cover communication protocols and data exchange formats. It includes RFID protocols such as ISO/IEC 14443 and FeliCa and other protocols such as ISO/IEC 18092 and those defined by NFC forum. This forum was founded by Nokia, Philips and Sony in 2004 and currently more than 150 companies have been incorporated.

3 Routing Protocols for the IoT

The development of routing protocols is a very active research field in ad hoc networks. The design of routing protocols for ad hoc networks is challenging due to mobility conditions and the limited resources of nodes. Most routing protocols for ad hoc networks are focused on guaranteeing Quality of Service (QoS) metrics such as bandwidth and end-to-end delay [38] [39]. On the other hand, routing protocols for WSNs are focused on maximizing network's lifetime by reducing the energy consumption [40]. However, the introduction of ad hoc networks in IoT requires new routing protocols oriented to connecting such limited devices to the Internet. Routing protocols for the IoT must guarantee connectivity, fairness and QoS between the nodes both in ad doc networks and the APs. Note that it is clearly different from the classical concept of routing protocol for ad hoc networks where QoS must be guaranteed between any pair of nodes in the network. In an the IoT setting, routing protocols must ensure fairness so that each node can communicate with the APs. Hierarchical solutions are normally adopted in order to reduce redundancy and for ensuring data association and data aggregation. Moreover, cross-layer designs are attracting attention since they are suitable for variable channel conditions which are normally found in ad hoc scenarios. Cross layers designs make possible the collaboration between MAC and routing layers so as to optimize routing decisions. A routing protocol using Received Signal Strength Indicator (RSSI) is an example of a cross layer design in which the routing protocol can use RSSI values to estimate Euclidean distance between two nodes or the link quality.

One possible solution is to adapt existing routing protocols to the requirements of the IoT. For example classical routing protocols for ad hoc networks such as Ad Hoc On-Demand Distance Vector (AODV) routing protocol and Dynamic Source Routing (DSR) can be modified to fulfill IoT requirements. For instance, AOMDV-IOT [41] is an extension of Ad Hoc On-demand Multipath Distance Vector routing protocol. AOMDV allows a user to find several node-disjoint routes and link-disjoint routes between a source node and a destination node. However, in an IoT context the objective is to find a node connected to the Internet. This issue is solved by AOMDV-IOT and in particular, by implementing an Internet Connecting Table (ICT). In addition, an Internet Linking Address (ILA) is also defined so as to be used when the node is connected to the Internet.

Mesh networks are focused on the creation of hierarchical architectures that enable mobile nodes to connect to the fixed infrastructure creating a mixed network. Clustering algorithm can be a solution to accomplish such associability. Mesh Adaptive Routing Tree (MART) [42] is defined by the IEEE 802.15.5 working group and its objective is to develop a routing tree for Mesh networks. In tree architecture, a node can only communicate with its one-hop neighbors. A Hierarchy structure is built in order to forward packets from the root to the leaves. Three phases are defined in MART: 1) initialization (or configuration) phase, 2) normal phase, and 3) recovery phase. During the initialization the tree is formed. The number of branches of each node depends on its capacity. The MART tree formation is functionally divided into two stages: association and address assigning. In the normal phase, packets can be routed throughout the tree. Finally, the recovery phase is carried out whenever broken links are detected.

With regard to WSNs, routing strategies are being focused on integrating IPv6 so that each node is the network that can be identified by an IP address. In this way, RPL routing protocol [43], which was developed by the IETF in the working group namely Routing Over Low power and Lossy networks (ROLL), is a distance vector based IPv6 routing protocol which specifies how to build a Destination Oriented Directed Acyclic Graph (DODAG) using an objective function and a set of metrics/constraints. These metrics determine the quality of the paths found. Depending on the requirements of the deployed application different metrics can be defined and multiple DODAGs can be defined in order to satisfy such requirements. Note that RPL is a hierarchical routing protocol. The graph starts at the root called LowPan Border Router (LBR). ICMPv6 messages are then exchanged by nodes in order to share graph related information. In DODAG formation, each node of the graph has to select a parent node (or multiple parents depending on the objective function) in a hop-by-hop fashion and the leaf nodes can communicate with the root node by just forwarding the packet to its immediate parent. In addition, RPL also supports P2P communications so any node can communicate with any other node in the network. On the other hand, existing routing protocols for WSNs can also be adapted to support IPv6. For instance, 6LoWPAN SPEED [44] is an evolution of SPEEP protocol. SPEED is a routing protocol that supports soft real-time communications in large-scale sensor networks. The end-to-end soft real-time is achieved by maintaining a desired delivery speed across the network by means of feedback control and non-deterministic geographic forwarding. Three types of communications services are implemented in SPEED routing protocol, 1) real-time unicast, 2) real-time area-multicast, and 3) real-time area-anycast. In SPEED protocol, each packet is forwarded towards the direction of the destination node. In [44] speed protocol is adapted to support 6LoWPAN by encapsulating SPEED messages into ICMPv6 headers. This mechanism based on encapsulation may be used by other routing protocols in WSNs.

4 Towards an IoT Smart Environment

However, a concern [45] with current real-world implementations is that they cover narrow visions where technology core specification stands in-between organizations and end-users as an instrument for data gathering.

In this chapter, we describe a "thereuGO" case scenario incorporating an all-in-one inclusive approach. That is by suggesting the use of the MANETS, RFID, NFC and IoT to transform physical and virtual business processes, services and products into smart objects and inter-connect them into an Internet-like structure. This is by tagging them in a way that customers and businesses can perform intelligence by using personalized technology and other computational approaches like Cloud computing to manage their tailored interactions in a scalable manner.

While the "thereuGO" case scenario is driven by the specifics of a gaming operator, there is evidence of its scope and applicability in wider business and organizational contexts.

4.1 The "thereuGO" Case Scenario

Bob is an occasional player in Gaming Operator (GO), one of Europe's leading gaming operators. When visiting GO, Bob spends few hours playing, and socializing with others like Alice and Ted. Bob owns a smart-phone, which effectively enables him to access Internet services through WiFi. When entering GO premises, Bob does not need to show his loyalty card, "thereuGO" (the acronym for GO's smart IT environment) registers his entry automatically. In fact, "thereuGO" informs Carol who is the manager and bar attendant – a few rooms away from Bob's positioning – to pour a pint of Guinness ready for Bob to collect next to his favorite slot machine. As Bob enters from one room to another, his smart-phone guides him to his favorite slot machine that is available at the time. Most importantly, it tells him what services and products are available in a dynamic and timely fashion for each room as he enters them. He finds the room-based browse feature very exciting; he is now aware of things that he had never noticed them before like the odd slot machine with the most money to be won; last winner was three weeks ago; Bob took a picture of it and shared it with Carol. This Friday, Bob decided to play cards. Using his smart-phone, he browses the tables available and realizes that Alice and Ted are also playing cards specifically, on table 3, room 3. He claims the space and as Carol tracks his way, Bob confirms delivery of his drink in table 3. Later on, Bob used his smart-phone to order some drinks by taking a photo of the label from the printed menu. While they were chatting, Bob informed that the little odd slot machine is now available but he decided to stay with his friends. Few minutes later, Alice coveted a plate of cold snack that she had never seen before when a waiter delivered it to the table next to them. She took a picture of it, checked the ingredients (Alice knows that by reading Ted's social network profile tat he is allergic in nuts) and sent the order to Carol. Minutes after, Ted reserved more drinks for later (all like Blue-Monkey by the reading of their social network sites); he found the offer sent from Carol a timely opportunity not to miss. Carol and her team now feel much more comfortable in responding to customers' preferences and ad-hoc requests and most importantly, they can now manage their resources more efficiently; they know – at anytime – what are the most and least desirable services; which ones are available; who is drinking what at what frequency; when they would most likely need top-up; what are their stock levels and profits; how many people in each room; how many in the pre-hallway entry for more than 5 minutes, etc. Carol knows that undecided

newcomers will most likely accept a treat. All these, through a GUI which illustrates the relationship between the customers and her tagged smart environment resources. “thereuGO” seems to be a Win-Win and Show-me-the-money opportunity for customers and business; both ends can self-manage their desires and commodities. Later on, our actors waived each other and promised to play cards online. On the way out, Bob realizes that the odd slot machine still has the money; he is now thinking to play from home online.

4.2 A “thereuGO” IoT Model Architecture

Figure 10 extends low-level architectures discussed in [4] [5] [6] by illustrating more technical aspects related to the “thereugo” case scenario.

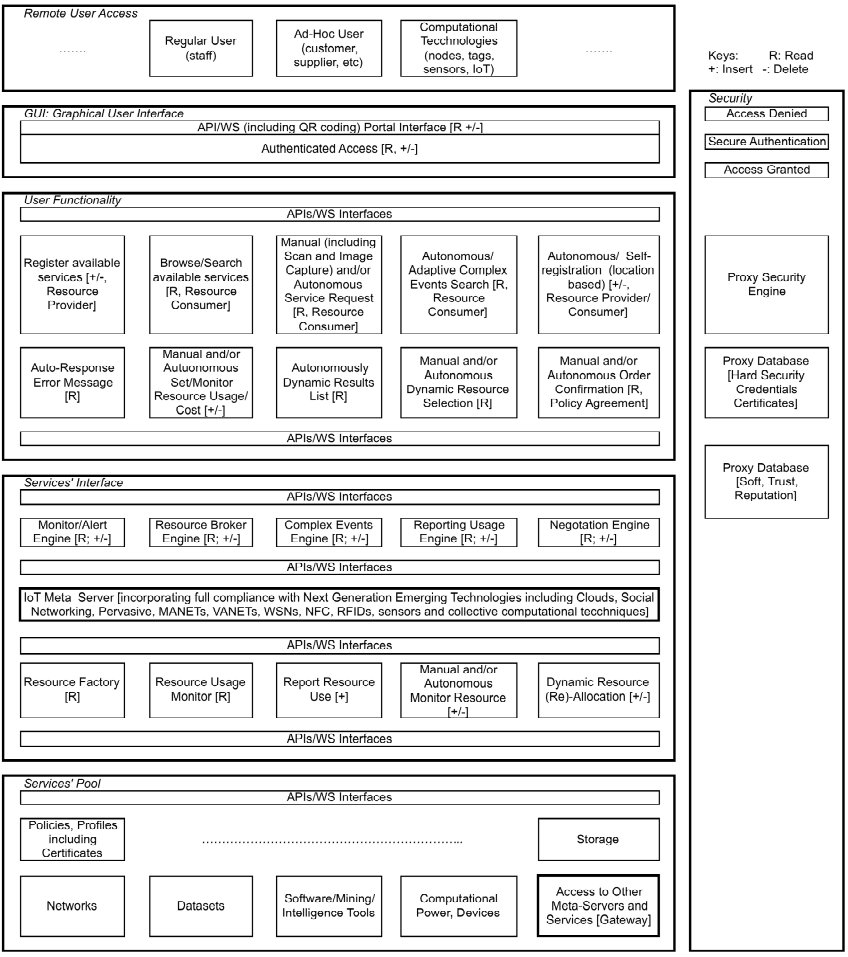

Fig. 10 A IoT Technical Model Architecture

Our past works explain the flow of interactions between computational devices capable of sensing the environment and establishing an ad-hoc mobile network. Herein, we use the "thereuGO" case scenario to demonstrate how the functionality available and the aforementioned technologies relate and impact in realizing, making sense of and ultimately enabling a more informed decision-making based on the actual situation rather than a speculative analysis. Specifically, the model appreciates that each user may have different needs, which requires personalization technologies like personalized URLs and personalized femtocell techniques. Due to the complexity involved we have not made links between functions and services.

In terms of the functionality available, the model appreciates that users will use their smart devices to access resources available from the smart environment remotely and on an ad hoc basis. Users get access to the portal after a successful authentication control. Authentication takes decisions on the basis of both security standards (PKI, X509, etc) and softer issues such as privacy, trust and reputation as there is a need to ensure the reputation of a service requestor and/or provider. Following the authentication procedure users can register their resources using some metadata descriptions, which can be stored in a factory for their future harvesting. Users may also request for resources in either manual or autonomous manner. Following the search procedure (manual or autonomic) a broker will negotiate between resource provider and requestor on the basis of user profile and policies prior to any resource confirmation and allocation. A monitoring function is used to dynamically re-allocate resources when these become unavailable for any reason. A complex events engine is suggested in order to monitor and ensure that combination of tailored parameters may lead to alerts. It is important to note that each function or service support multiple instances regardless if they are shown as single instances.

5 Conclusions

In this chapter, we provided a state-of-the-art review on how current standard communication protocols could support the realization of the IoT vision. In particular, we discussed ad hoc and wireless sensor networks, near field communications, radio frequency identification and routing protocols as a mean to describe their applicability towards the IoT realization.

Within this context, we highlighted that although most standard communications and protocols are supportive their connection to Internet and thus, to the IoT is still a challenge which requires further research. We also presented a brief case scenario describing a future smart environment; this was to illustrate its possible IoT model technical architecture.

Our future work involves the identification of suitable network simulation environments; this will be of particular importance since the IoT will open several opportunities in the real-world. This study, will also aim to define the network performance and metrics for several IoT case scenarios.

References

1. Tan, L., Wang, N.: Future Internet: The Internet of Things. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), August 20-22, pp. V5-376–V5-380 (2010)
2. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: A survey. Computer Networks 54(15), 2787–2805 (2010)
3. Presser, M., Gluhak, A.: The Internet of Things: Connecting the Real World with the Digital World. In: EURESCOM mess@ge – The Magazine for Telecom Insiders, vol. 2 (2009)
4. Bessis, N., Asimakopoulou, E., French, T., Norrington, P., Xhafa, F.: The Big Picture, from Grids and Clouds to Crowds: A Data Collective Computational Intelligence Case Proposal for Managing Disasters. In: 5th IEEE International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC 2010), November 4-6, pp. 351–356 (2010)
5. Asimakopoulou, E., Bessis, N., Varaganti, R., Norrington, P.: A Personalised Forest Fire Evacuation Data Grid Push Service – The FFED-GPS Approach. In: Asimakopoulou, E., Bessis, N. (eds.) Advanced ICTs for Disaster Management and Threat Detection: Collaborative and Distributed Frameworks, pp. 279–295. IGI (2010) ISBN: 978-1615209873
6. Bessis, N., Asimakopoulou, E., Xhafa, F.: A Next Generation Emerging Technologies Roadmap for enabling Collective Computational Intelligence in Disaster Management. International Journal of Space-Based and Situated Computing (IJSSC) 1(1), 76–85 (2011)
7. Reina, D.G., Toral, S.L., Barrero, F., Bessis, N., Asimakopolou, E.: Modelling and assessing ad hoc networks in disaster scenarios. Journal Ambient Intelligence and Humanized Computing, JAIHC (2012), doi:10.1007/s12652-012-0113-3.
8. Hande, A., Ersoy, C.: Wireless sensor networks for health care: A survey. Computer Networks 54, 2688–2710 (2010)
9. Gutiérrez-Reina, D., Toral, S.L., Johnson, P., Barrero, F.: An evolutionary computation approach for designing mobile ad hoc networks. Expert Systems with Applications 39, 6838–6845 (2012)
10. Wolfgang, K., Martin, M.: A survey on real-world implementations of mobile ad hoc networks. Ad Hoc Networks 5, 324–339 (2007)
11. Bruno, R., Conti, M., Gregori, E.: Mesh Networks: Commodity multihop ad hoc networks. IEEE Communications Magazine 3, 123–131 (2005)
12. Hoebeke, J., Moerman, I., Dhoedt, B., Demeester, P.: An overview of mobile ad hoc networks: Applications and chanllenges. Journal of Communications Networks 3, 60–66 (2004)
13. Morgan, Y.L.: Notes on DSRC & WAVE standards suite: Its architecture, design, and characteristics. IEEE Communications Surveys & Tutorials 12(4) (2010)
14. Gerla, M., Kleinrock, L.: Vehicular networks and the future of internet mobile. Computer Networks 55, 457–469 (2010)
15. Yick, J., Mukherjee, B., Ghosal, D.: Wireless sensor networks survey. Computer Networks 52, 2292–2330 (2008)
16. Huasong, C., Leung, V., Chow, C., Chan, H.: Enabling technologies for wireless body area networks: A survey and outlook. IEEE Communications Magazine 47, 84–93 (2009)

17. Bur, K., Omiyi, P., Yang, Y.: Wireless sensor and actuator networks: Enabling the nervous system of active aircraft. IEEE Communications Magazine 48, 118–125 (2010)
18. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks. IEEE Communications Magazine 40, 104–112 (2002)
19. Cristin, D., Reinhardt, A., Parag, S., Mogre, P.S., Steinmetz, R.: Wireless sensor networks and the internet of things: Selected Challenges. Structural Health Monitoring 5970, 31–33 (2009)
20. Jeonggil, K., Terzis, A., Dwason-Haggerty, S., Culler, D.E., Hui, J.W., Levis, P.: Connecting low power and lossy networks to the internet, vol. 49, pp. 96–101 (2011)
21. http://smote.cs.berkeley.edu:8000/tracenv/wiki/blip
22. http://www.tinyos.net/
23. Souto, E., Guimaraes, G., Vasconcelos, G., Vieira, M., Rosa, N., Ferraz, C., Kelner, J.: J. Personal and Ubiquitous Computing 10, 37–44 (2006)
24. Avilés-López, E., García-Macías, A.: TinySOA: A service oriented architecture for wireless sensor networks. Service Oriented Computing and Applications 3, 99–108 (2009)
25. Shelby, Z., Hartke, K., Bormann, C., Frank, B.: Constrained Application Protocol (CoAP). draft-ietf-core-coap-09 (2012)
26. Luchkenbach, T., Gober, P., Arbanowski, S., Kotsopoulos, A., Kim, K.: TinyREST- a protocol for integrating sensor networks into the internet. In: Proceedings of REALWSN (2005)
27. http://telegraph.cs.berkeley.edu/tinydb/
28. https://pachube.com/
29. Leong, K.S., Ng, M.L., Engels, D.W.: EPC network architecture. Autoidlabs-wp-swnet-012, 1 edn. white paper series, pp. 1–14 (2005)
30. Amaral, L.A., Hessel, F.P., Bezerra, E.A., Corrêa, J.C., Longhi, O.B., Dias, T.F.O.: eCloudRFID-A mobile software framework architecture for pervasive RFID-based applications. Journal of Networks and Computer Applications 34, 972–979 (2011)
31. Welbourne, E., Battle, L., Garret, C., Gould, K., Rector, K., Raymer, S., Balanzinska, M., Borriello, G.: Building the internet of things using RFID: The RFID ecosystem experience. IEEE Internet Computing 19, 48–55 (2009)
32. Xiaowei, Z., Mukhopadhyay, S.K., Kurata, H.: A review of RFID technology and its managerial applications iin different industries. Journal of Engineering and Technology Management 29, 152–167 (2012)
33. Yi-Wei, M.: Mobile RFID with IPv6 for phone services. In: 13th IEEE International Symposium on Consumer Electronics (ISCE 2009), pp. 169–170 (2009)
34. http://www.abiresearch.com/research/1003525-Near+Field+Communications+NFC
35. http://www.nfcworld.com/2010/06/02/33802/ims-forecasts-785-million-nfc-chips-to-ship-in-2015/
36. http://www.device-solutions.com/downloads/NFC%20Enabling%20Technology%20Final.pdf
37. http://www.rfidjournal.com/article/view/8793
38. Boukerche, A., Turgut, B., Aydin, N., Ahmad, M.Z., Bölöni, L., Turgut, D.: Routing protocols in ad hoc networks: A survey. Computer Networks 55, 3032–3088
39. Hanzo II, L., Tafazolli, R.: A survey of QoS routing solutions for mobile ad hoc networks. IEEE Communications Tutorials & Surveys 9, 50–70 (2007)

40. Akkaya, K., Younis, M.: A survey on routing protocols for wireless sensor networks. Ad Hoc Networks 3, 325–349 (2005)
41. Tian, Y., Hou, R.: An improved AOMDV routing protocol for internet of things. In: International Conference on Computational Intelligence and Software Engineering (CiSE), pp. 1–4 (2010)
42. Zheng, J., Liu, Y., Zhu, C., Wong, M., Lee, M.: IEEE 802.15.5 WPAN Mesh Networks. IEEE P802.15-05-0260-00-0005 (2005)
43. Vasseur, J.P., Agarwal, N., Hui, J., Shelby, Z., Bertand, P., Chauvenet, C.: RPI: The IP routing protocol designed for low power and lossy networks. IPSO Alliance (2011)
44. Bocchino, S., Petracca, M., Pagano, P., Ghibaudi, M., Lertora, F.: SPEED routing protocol in 6LoWPAN networks. In: IEEE 16th Conference on Emerging Technologies & Factory Automation (ETFA), pp. 1–9 (2011)
45. http://www.freshbusinessthinking.com/business_advice.php?CID=30&AID=10320&PGID=2