Network Traffic Characteristics of the IoT Application Use Cases

Jozef Mocnej
Technical University
of Kosice, Slovakia
Email: jozef.mocnej@tuke.sk

Adrian Pekar Winston K.G. Seah
Victoria University of Wellington
New Zealand
Email: {adrian.pelar,winston.seah}@ecs.vuw.ac.nz

Iveta Zolotova
Technical University
of Kosice, Slovakia
Email: iveta.zolotova@tuke.sk

***Abstract*—The Internet of Things (IoT) is a highly discussed paradigm aimed at the connection of everyday objects to the Internet. The idea of enabling objects to communicate with each other brings significant benefits, yet there are several challenges that have to be also addressed. In recent years, researchers have developed many solutions to resolve IoT issues and enhance the overall evolution. New technologies have been proposed and existing approaches redefined to meet the specific requirements of IoT. However, the complexity and diversity of the area make the process quite difficult. This paper describes the IoT paradigm and provides an overview of efforts expended to date. It discusses topics such as IoT definitions, categorisation of IoT application areas and the greatest IoT challenges. One contribution of this paper is the detailed description of IoT network technologies and their illustration in a single protocol stack. Another contribution is the definition of network traffic characteristics of IoT application use cases, which aims to help in better comprehension of IoT demands on network technologies. This knowledge is crucial not only to propose more efficient solutions but also improve the network technologies specifically designed for IoT needs.**

I. Introduction

The Internet of Things (IoT) is a novel paradigm based on interconnecting a tremendous number of heterogeneous end devices and providing the acquired data for all kinds of different digital services. The term 'Internet of Things' was first coined by Kevin Ashton in 1999 while referring to a global network of objects connected to Radio Frequency Identification (RFID) in a supply chain [1]. Since then, many new technologies have emerged and IoT has spread to other application areas as well. Nevertheless, the main goal has always remained the same – to empower computers with their own capabilities of gathering information without a human interference.

The idea behind IoT is to extend everyday things with a computing power and connection to the Internet and enable them to sense, compute, communicate and control the surrounding environment. These capabilities are desired in many application use cases due to their potential impact, from making our lives easier [2], [3] and safer [4], [5], through improving and simplifying the current processes [6], [7], up to creating completely new possibilities and opportunities [8], [9]. IoT offers a new point of view on what kind of data should be gathered, how often and from which place, so that it would be possible to get information that was not available before. In many cases, however, this benefit means the communication of low power devices over lossy networks, which creates high demands on the used technologies. Consequently, we need to understand the requirements of IoT application use cases in order to create more efficient IoT solutions.

The aim of this paper is to contribute to the highly discussed topic of IoT by looking at IoT application use cases and describe them from a traffic characteristics perspective. Our objective is to identify as accurately as possible the demands on networks defined by IoT application scenarios, which would help to clarify the requirements that IoT technologies need to target. The gained knowledge would not only be beneficial for researchers and developers to create more appropriate IoT network technologies but also for industry to better understand business opportunities and to facilitate their decision process about the most suitable network technologies for the particular IoT application. Furthermore, this paper provides an overview of the IoT paradigm and the most current efforts in network technologies specifically designed for IoT.

The rest of the paper is structured as follows: Section II describes the related work and highlights the main contributions of this paper. Section III introduces the IoT paradigm, its definitions, application areas and challenges. Section IV classifies IoT network communication technologies and summarises them in one detailed protocol stack. Section V defines the traffic characteristics of IoT application domains and Section VI evaluates the gained knowledge in the aggregated scatter charts. Lastly, Section VII presents the conclusion and required future work.

II. Related Studies

The IoT is a greatly debated topic in academia as well as industry. In recent years, researchers have put a lot of effort into IoT and proposed numerous solutions. Due to the novelty and complexity of this paradigm, there has been a continuous demand for summarising state-of-the-art work and keeping researchers up-to-date. This section provides a chronological overview of the notable survey papers in IoT.

Kortuem *et al.* [10] explored how emerging technologies transform everyday objects into *smart* objects. The authors' perceived smart objects to be more than just sensor nodes. Rather, they defined them as the interactive tools with input and output capabilities and declared them as the main building

blocks of IoT. The survey published in 2010 identified three canonical smart object types: activity-aware, policy-aware, and process-aware objects.

In the same year, Atzori *et al*. [11] surveyed the fundamental aspects of IoT and provided an overview of this complex discipline. To reduce the ambiguity, they defined the IoT paradigm as a result of the convergence of three main visions: things-oriented, Internet-oriented, and semantic-oriented vision. Moreover, they emphasised the potential applications and open issues requiring further research. As they claimed in the conclusion, the technologies back in 2010 could have made the IoT concept feasible but the lack of scalability and efficiency were the major drawbacks.

Bandyopadhyay *et al*. [12] studied the state-of-the-art of IoT in 2011 and presented the key technological drivers, potential applications, challenges and future research areas. They observed the growing interest in IoT solutions from the governance but raised the concern that without standardisation, the proliferation of applications would lead to a fragmentation of IoT, which could hamper its popularity and slow down the overall progress.

In 2012, the fragmentation of IoT communities had become a real obstacle. Miorandi *et al*. [13] targeted this issue noting that the researchers were too focused on the specific application domains, which the authors perceived to be potentially harmful to the development and successful adoption of IoT technologies. Therefore, they provided a holistic perspective on the IoT concept together with the relevant application fields, enabling technologies, and research challenges. Their objective was to help in bridging the existing communities and encourage cross-collaboration.

In 2013, Gubbi *et al*. [14] looked at the Internet of Things from the perspective of cloud computing and presented a cloud-centric vision for worldwide implementation of IoT, proposing a cloud-centric IoT architecture with the platform-as-service called 'Aneka' that connects private and public clouds to one solution.

The growing volume of data generated by IoT devices motivated Perera *et al*. [15] to survey IoT from the context-aware perspective. As they claimed in their paper published in 2014, the only way to process the raw data from IoT devices is to include the context-awareness into the IoT solutions. To validate their statement, the authors analysed 50 projects that had been proposed in the field of context-aware computing over the last decade and highlighted the lessons to be learnt from the past.

In the same year, Xu *et al*. [16] presented an IoT survey with a focus on industry. Their paper reviewed the state-of-the-art research in IoT, key enabling technologies, major industrial applications, and highlighted the challenges and possible research opportunities within the industry.

In 2015, numerous surveys were published. Sicari *et al*. [17] targeted IoT security, privacy and trust issues, and presented the main research challenges and existing solutions, together with the needed directions for the future research. Whitmore *et al*. [18] and Li *et al*. [19] approached from the general perspective in order to provide an up-to-date overview of IoT activities with the emphasis on current trends, applications, used technologies, and major challenges. Finally, Al-Fuqaha *et al*. [20] proposed another general IoT survey, but this time the major part was devoted to the communication protocols.

Understanding network traffic characteristics is essential for all aspects of network design and operation, including protocol design, resource provisioning, network management, and modeling and simulation [21]. The Poisson arrival process has been used to model call arrivals in telecommunication networks due to its analytical simplicity [22]. However, it has been found to be unsuitable for new network traffic types that have emerged from fundamental Internet protocols like TCP and applications like TELNET and FTP [23]. New applications like video streaming bring with them new traffic models that are necessary for traffic engineering [24]. While understanding the demands on the traffic characteristics is crucial for proposing efficient solutions, a detailed study of various IoT network traffic characteristics is still not available. This is the key motivation of this survey that distinguishes us from other published surveys. Nonetheless, we also aimed to target the typical survey topics and publish the updated state-of-the-art in IoT, as well as recap the already presented knowledge in the more compact format; this is our first contribution. Second, we analysed IoT application use cases in order to define their network traffic characteristics.

III. IoT PARADIGM

This section provides a general overview of the Internet of Things paradigm, including its definition, domain coverage and challenges to date.

A. IoT definitions

The diversity of IoT and the rapid progress resulting from the vast research being done has inevitably led to the lack of a standardised definition of IoT. Consequently, various definitions have been put forth by researchers and standardisation organisations, including:

- Definition by ITU [25]: "*The Internet of Things is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.*"
- Definition by IERC [26]: "*A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.*"
- Definition by ISOC [27]: "*The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume*

data with minimal human intervention. There is, however, no single, universal definition."

Despite the many similarities, one commonly accepted definition remains elusive. The IEEE IoT Initiative [28] collected and analysed dozens of different IoT definitions with the aim to identify core features of IoT that would help to clarify the entire concept and establish one baseline definition. As a result, they realised the scope of IoT is too broad to be effectively described only by one definition, and therefore they decided to provide two separate definitions of IoT, one for small environment scenario and one for large environment scenario:

- Definition for small environment scenario: "*An IoT is a network that connects uniquely identifiable 'Things' to the Internet. The 'Things' have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the 'Thing' can be collected and the state of the 'Thing' can be changed from anywhere, anytime, by anything.*"
- Definition for large environment scenario: "*Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'Things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/action capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration.*"

The main distinguishing element between the small environment scenario and the large environment scenario is complexity, considering the fact that small specific systems have fewer features than large global systems composed of many services and processes.

We perceive the definitions provided by the IEEE IoT Initiative to be sufficiently descriptive while general enough to cover the diversity of the IoT application domains. Therefore, we adopt them for our research work and this paper further references to both scenarios. IoT challenges are based on the issues of the large environment scenario, whereas the traffic characteristics of IoT application domains describe small specific systems individually.

Nevertheless, taking into consideration how difficult it is to agree on one general definition of IoT, it can clearly be seen the enormous amount of different IoT use cases. The next subsection categorises application domains into the groups in order to gain a better overview.

B. IoT Application Areas

The IoT paradigm is very diverse and understanding its application potential is crucial for further improvements. As the IoT definition says, connecting things to the Internet and giving them an ability to sense/actuate is a feature demanded everywhere. There is no application domain that would not benefit from having a better control over the environment. Yet trying to categorise the application use cases into more general groups can reduce the overall fuzziness of IoT and offer us the greater comprehension.

Since IoT covers many application scenarios, different researchers have offered different categorisations based on their experience and point of view:

- Perera *et al*. [15] defined three general categories based on the focus of application domains: industry, environment and society.
- libelium [29] listed 54 application use-cases under 12 categories: smart cities, smart environment, smart water, smart metering, security and emergencies, retail, logistics, industrial control, smart agriculture, smart animal farming, domestic and home automation, and eHealth.
- Atzori *et al*. [11] grouped applications into 4 categories: transport and logistics, healthcare, smart environment (home, office, plan), personal and social.
- IERC updated their classification list several times and in [30] defined 10 categories: smart food/water monitoring, smart health, smart living, smart environment monitoring, smart manufacturing, smart energy, smart buildings, smart transport and mobility, smart industry, and smart city.

From the aforementioned categories it is clear that although some researchers propose a more general classification, while others prefer a more detailed one, in any case, they all try to point out similar domains. Nonetheless, we consider the target audience to be more important than specifying the exact number of categories as, in general, the users define the requirements that IoT applications have to meet. Considering this perspective, we can recognise three groups of users:

- **individuals** – individual persons looking to improve their overall level of lifestyle.
- **society** – a community of people looking to find solutions for common issues.
- **industry** – any economic sector looking to satisfy customer's needs with their product.

Even though every user category has the specific driving needs, in general, they want to achieve three goals:

1) maximise health and safety
    - individuals – health and safety of their own and their families.
    - society – health and safety of its members (e.g. citizens).
    - industry – health and safety of the employees in the workplace.
2) minimise the amount of work while maximising the convenience of its execution

- individuals – minimise everyday routines.
- society – minimise the redundant public services.
- industry – minimise inefficient work.

3) minimise the costs
- individuals – minimise personal expenses.
- society – minimise costs of public services.
- industry – minimise production costs.

When it becomes apparent what expectations IoT has to fulfil, we can identify and categorise use cases suitable for their achievement. Obviously, the defined user groups have very diverse areas of interest and as we could see from the categorisations of other researchers, the number of domains may vary greatly according to the level of abstraction.

Our aim is to limit the number of domains while still making them self-explanatory so that it would always be clear what applications every domain covers, aiming for an optimal balance between generality and concreteness. Therefore, we have decided not to use the categorisations mentioned above and instead classify IoT use cases into the following eight application domains: *smart buildings and living*, *smart healthcare*, *smart environment*, *smart city*, *smart energy*, *smart transport and mobility*, *smart manufacturing and retail*, and *smart agriculture*.

We consider these eight domains to be diverse enough to cover all IoT applications that can satisfy the needs of our user groups. However, rather than looking at these categories as being completely distinct from each other, it might be more appropriate to perceive them as being mutually complementary. For example, the smart city can include smart buildings and living, smart healthcare, smart transport and mobility, as well as smart energy. Similarly, smart manufacturing and retail domain can involve smart transport and mobility domain, and smart buildings and living domain. Therefore, we identify these categories as the building blocks for a better comprehension of IoT application coverage and for easier classification of IoT research areas.

To understand the connection between user groups and application domains, we group them under the three user groups as shown in Fig. 1.

It should be clear from the figure that some application domains are influenced by only one user group, while others have to fulfil the needs of two or even all three groups. Meeting the requirements of three groups may appear to be more difficult than only one, but, as we have pointed out earlier, all these groups have similar demands for different application domains. Therefore, the overall feasibility of IoT application use cases is influenced more by other aspects, such as technical issues described in the next subsection.

C. IoT Challenges

The pace at which the IoT is progressing brings with it many challenges in various aspects, including security [31], [32], communication and networking [33], [34], middleware [35], among others [36]–[38].

To sum it up, IoT challenges can basically be divided into four categories: *hardware*, *software*, *connectivity,* and *security* (see Fig. 2). Each of these groups defines its specific issues that eventually influence the overall quality of IoT solutions. Since "a chain is only as strong as its weakest link" every group deserves the same amount of attention in further research.

1) Hardware: The number of Internet-connected devices grows exponentially leading to the following issues:
- **Cost of devices** – IoT devices have to be extremely low cost in some specific use cases, otherwise, the added value will not be able to justify the cost.
- **Battery life** – most of the IoT devices will be battery-powered and, in some cases, powered by unpredictable renewable energy sources. Therefore, the devices should be working as long as possible.
- **Physical specifications** – there is certainly a big pressure on the overall size of devices while maintaining or even increasing their computing power.

2) Software: No IoT solution would work without a sufficient software. The software used to date does not meet the emerging IoT requirements, motivating new developments. To meet the continuously increasing demands, new software solutions need to be targeted at:
- **Interoperability** – the IoT not only connects things to the Internet, but it also interconnects things in a meaningful way to enable a mutual machine-to-machine (M2M) communication. This approach requires a globally accepted standardisation, which has been a motivation for many organisations to take the initiative.
- **Data processing** – the IoT continues to generate increasingly more data as more devices are connected. Decentralised data processing is inevitable with much of it done as close to the data sources as possible.
- **Context awareness** – to fulfil the idea of controlling an environment without human interaction, the artificial intelligence has to be implemented to provide context-aware computing.

3) Connectivity: Connectivity is a glue for the IoT. The Internet has been around for decades but new applications have emerged, generating new data traffic characteristics that the original Internet protocols were not designed for. The latest phenomenon is the IoT which brings with it new requirements, and a totally new wave of data traffic types. New network technologies are expected to support the IoT and have to address the following challenges:
- **Coverage** – extended coverage is needed both in indoor spaces and wide outdoor areas [39]. A combination of both multihop short-range as well as one-hop long-range technologies would be essential.
- **Scalability and diversity** – networks have to scale efficiently and rapidly to meet the increasing demands of up to millions of connected devices. Furthermore, the diversity of connection scenarios requires the network to be able to adapt to different traffic requirements.
- **Reliability** – IoT is the foundation of cyber-physical systems (CPS) that we have become more and more reliant on. Consequently, network reliability is a criti-

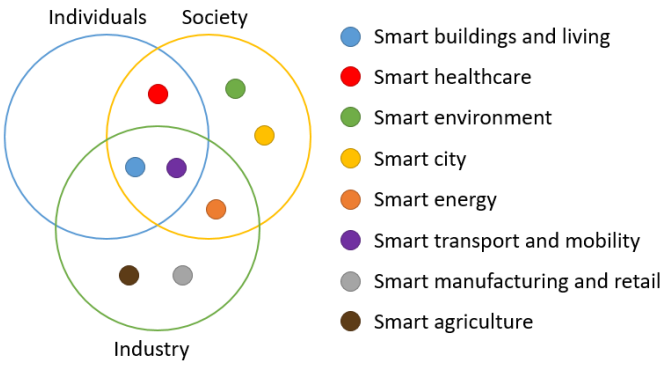

Fig. 1. Impact of user groups on the applications domains.

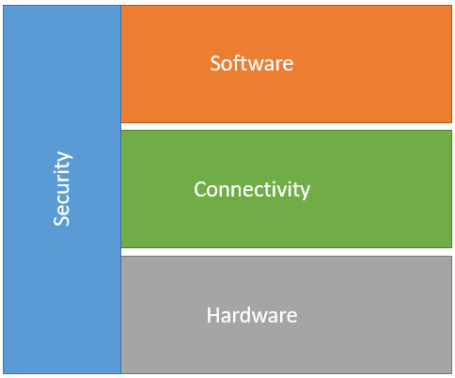

Fig. 2. Categories of IoT challenges.

cal requirement, much more than the best-effort service model that original Internet was designed for.

4) Security: Security is emerging to be the IoT's greatest challenge. Being a cyber-physical system, it has been acknowledged that its vulnerability to attacks can lead to costly or even life-threatening consequences. However, another side of the IoT security problem has emerged where a massive number of IoT devices is easily exploited to execute malicious activities, namely, distributed denial-of-service (DDoS) attacks [40]. This implies that IoT solutions need to offer:

- **Attack resistance** – since resource-constrained IoT devices need to be resistant to attacks as well as from being used as attack vectors, security measures must be an integral component of every IoT device's protocol stack.
- **Confidentiality, integrity, and availability** – since both information and device require different measures that impose different requirements on the resource-constrained IoT devices, the appropriate choice of measure(s) is crucial to balance the needs against the available resources.

IV. IoT Network Technologies

When we look at the IoT application domains, it is clear that the only way how to connect such an amount of devices to the Internet is to connect them wirelessly. Consequently, one of the main IoT building blocks is a Wireless Sensor Network (WSN) or a Wireless Sensor and Actuator Network (WSAN) comprising sensors and/or actuators called *nodes* which sense and possibly perform some control task/action by cooperating within their communication infrastructure. A lot of research has been done in WSN/WSAN [41]–[43], nevertheless, it is still important to see the role and its significance these network technologies play in IoT.

The Internet as we know it today is based on the Internet Protocol [44], which is maintained by the Internet Engineering Task Force (IETF). Using IP addresses to identify connected devices and route traffic has become completely natural. Therefore, one might think the similar analogy would be applied in the IoT as well in order to preserve compatibility, but it is not so obvious.

One attempt to resolve the issue of insufficient IP addresses due to the limited IPv4 address space was simply replacing IPv4 with IPv6. However, this created a new problem. The IPv6 packet header presents an unacceptable overhead in constrained environments with battery-powered nodes where every bit counts. This led to the formation of an IETF working group (WG) called 6LoWPAN (acronym of IPv6 over Low power Wireless Personal Area Networks) [45] to define header compression mechanisms so that IPv6 could be used even on devices with highly limited resources. As a result, they managed to define the transport of IPv6 on IEEE 802.15.4 networks. The 6LoWPAN WG evolved into the 6Lo (IPv6 over Networks of Resource-constrained Nodes) WG [46], formed in 2013 to continue in adapting IPv6 for other constrained networks, e.g. IPv6 over Bluetooth Low Energy [47], IPv6 over NFC [48], etc. Another successor is the 6tisch (IPv6 over the TSCH mode of IEEE 802.15.4e) working group [49] that defines IPv6 over the time slotted channel hopping (TSCH) mode of IEEE 802.15.4e.

Concurrently, many other wireless communication and networking technologies have been developed by the industry to meet the needs of IoT applications, leading to numerous interoperability issues. Many began without any support for IPv6 but are slowly integrating IPv6 support. In Fig. 3, we present a detailed protocol stack that aims to consolidate the diverse technologies into a single view, using the five traditional layers: physical, data link, network, transport, and application. In proprietary solutions, where the exact protocols of the technology are not publicly known, we made a decision based on the functionalities they provide. One conclusion that can be derived from the stack in Fig. 3 is that many technologies use their own solutions at the network layer, however, this may change by future improvements in the adaptation of IPv6 over constrained networks.

From the coverage area perspective, we can conclude that the network technologies can be categorised into short and long range groups. The long range group can be further divided into unlicensed and licensed networks. While a number of technologies might look high at first glance, IoT application scenarios are so diverse that every network technology has

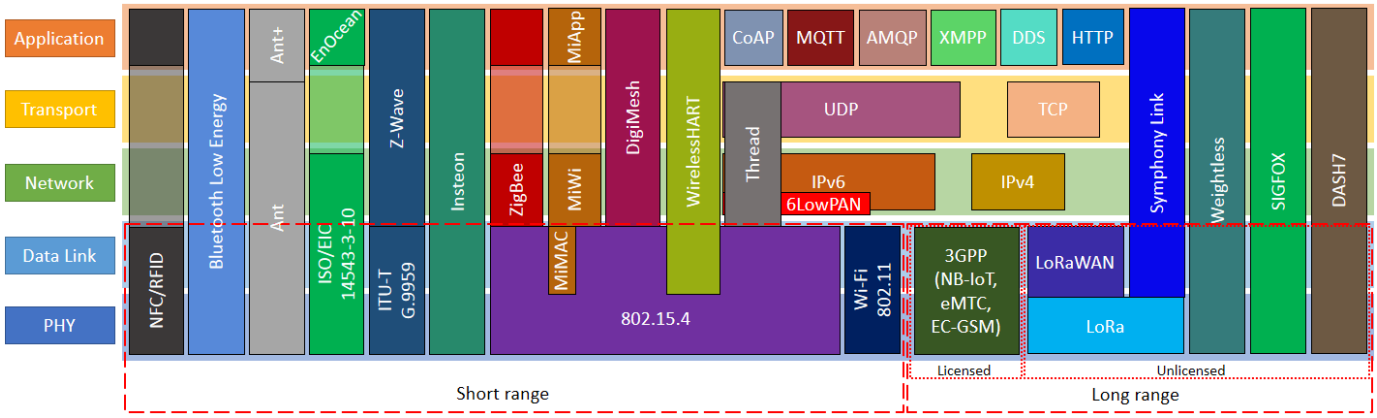

Fig. 3. Protocol stack of IoT network technologies.

found its utilisation. Their similarities and differences are highlighted in Table I. As the communication network technologies have been described by many researchers in great detail, we shall not repeat the published work. Rather, we present the following subsections with the aim to provide a very general overview of the IoT technologies and include the references to other papers where more information can be found.

A. Short range networks

Short range networks use wireless technology that communicate over ranges of a few centimetres up to hundreds of metres. These include close range contactless data transfer technologies, wireless personal area networks (WPANs) as well as, wireless local area networks (WLANs).

- **RFID** – Radio Frequency IDentification forms a critical component of the IoT concept when it was first introduced in 1999 by Kevin Ashton [1]. The falling price of passive RFID tags has enabled the rapid proliferation of this technology into all kinds of tracking and monitoring applications, securing its place in IoT again [50]–[52].
- **NFC** – based on the technology used for RFID, Near Field Communication [53]–[55] has found its usage in the IoT paradigm as well. NFC operates in three modes – card emulation, reader/writer, and P2P, offering the information about the objects "by touch".
- **BLE** – Bluetooth Low Energy [56]–[58], also called Bluetooth Smart, has been designed for ultra-low-power applications, which makes it ideal for connecting devices within a small range. In addition, due to the popularity of BLE, the most salient challenges (for instance, communication over IPv6 [47]) are being addressed constantly in order to improve the technology even more.
- **Ant** – Ant is a proprietary protocol designed for long-term monitoring applications [59]. It specifies the physical, data link, and network layers. The application layer is provided by Ant+ [60], the extension that standardises communication between different devices.
- **EnOcean** – EnOcean is an energy harvesting technology for home and building automation, but also adapted to other domains. EnOcean devices can be battery-free and therefore the protocol must be simple and lightweight [61], [62].
- **Z-Wave** – intended primarily for the smart home application domain, Z-Wave is a protocol used for home monitoring and control [63]–[65]. Many manufacturers have decided to implement Z-Wave into their products because of its features and wide support.
- **Insteon** – Insteon is a home automation technology based on dual-mesh topology, which is a combination of wireless radio frequency and existing electrical wiring [66], [67]. Although the protocol is completely proprietary, it has found its use in many homes.
- **ZigBee** – ZigBee [68]–[70] is a standard-based network protocol built on IEEE 802.15.14 physical and data link layer, and is often incorrectly used as a generic reference to IEEE 802.15.4 radios. Based on the different networking system requirements, Zigbee Alliance offers three specifications – ZigBee PRO, ZigBee RF4CE, and ZigBee IP, all designed for low-power and low-cost devices. While supposedly an open-standard, Zigbee's concept of application profiles is also a source of incompatibility among Zigbee products.
- **MiWi** – MiWi is a simple networking protocol designed by Microchip Technology Inc. The MiWi stack aims to be an alternative to ZigBee for microcontrollers with constrained memory as its footprint is even smaller. MiWi uses MiMAC at the data link layer to communicate with Microchip RF transceivers and MiApp at the application layer to provide an interface for applications [71]–[73].
- **DigiMesh** – DigiMesh is another proprietary technology based on the IEEE 802.15.4 standard. Digimesh networks are represented by a simple topology where all devices are homogeneous and therefore function as end-nodes, routers, coordinators, etc., at the same time. This is a big difference compared to ZigBee and further distinctions are detailed in [74].
- **WirelessHART** – WirelessHART [75], [76] is an open standard based on the popular Highway Addressable Remote Transducer (HART) protocol and a popular solution

TABLE I
CHARACTERISTICS OF IOT NETWORK TECHNOLOGIES

Technology	Frequency band	Range	Data rate	Battery life	Topology	Standardisation	Governing body
RFID	varies (Low / High / Ultra-high frequencies)	1 cm – 100 m	1 – 100 kbps	N/A (passive) / 3–5 years (active)	P2P	open standard	no single body
NFC	13.56 MHz	0.2 m	424 kbps	N/A (passive) / 3–5 years (active)	P2P	open standard	ISO/IEC
BLE	2.4 GHz	10 – 100 m	1 Mbps	months to years	P2P / Star	open standard	Bluetooth SIG
Ant	2.4 GHz	30 m	1Mbps	years	P2P / Star / Tree / Mesh	proprietary	Garmin
EnOcean	sub-1 GHz	30 – 300 m	125 kbps	N/A (self-powered – harvesting energy)	Mesh	proprietary (standard at 1-3 layers)	EnOcean Alliance
Z-Wave	sub-1 GHz	40 – 200 m	100 kbps	months to years	Mesh	proprietary	Z-Wave Alliance
Insteon	sub-1 GHz	30 – 50 m	37.5 kbps	months to years	Mesh	proprietary	Smartlabs
ZigBee	sub-1 GHz, 2.4 GHz	10 – 100 m	250 kbps	months to years	Star / Mesh / Tree	open standard	ZigBee Alliance
MiWi	sub-1 GHz, 2.4 GHz	10 – 100 m	250 kbps	months to years	Star / Mesh / Tree	proprietary	Microchip Technology
DigiMesh	sub-1 GHz, 2.4 GHz	10 – 100 m	250 kbps	years	P2P mesh	proprietary	Digi International
WirelessHART	sub-1 GHz, 2.4 GHz	10 – 100 m	250 kbps	years	Mesh	open standard	HART Communication Foundation
Thread	sub-1 GHz, 2.4 GHz	10 – 100 m	250 kbps	months to years	Star / Mesh / Tree	open standard	Thread Group Alliance
6LowPAN	sub-1 GHz, 2.4 GHz	10 – 100 m	250 kbps	months to years	Star / Mesh / Tree	open standard	IETF
Wi-Fi	2.4 GHz, 5 GHz; sub-1 GHz (Wi-Fi HaLow)	100 m; 1 km (Wi-Fi HaLow)	varies (Mbps to Gbps)	days to months	Star	open standard	Wi-Fi Alliance
NB-IoT	450 MHz – 3.5 GHz (2G/3G/4G spectrum)	10 – 15 km	250 kbps	10+ years	Star	open standard	3GPP
eMTC	450 MHz – 3.5 GHz (same as legacy LTE)	10 – 15 km	1 Mbps	10+ years	Star	open standard	3GPP
EC-GSM-IoT	850 – 900 MHz, 1800 – 1900 MHz (same as GSM)	10 – 15 km	70 – 240 kbps	10+ years	Star	open standard	3GPP
LoRaWAN	sub-1 GHz	10 – 15 km	50 kbps	10+ years	Star of stars	open standard	LoRa Alliance
Symphony Link	sub-1 GHz	10 – 15 km	50 kbps	10+ years	Star	proprietary	Link labs
Weightless	sub-1 GHz (-N and -P), TV white space spectrum (-W)	2 – 5 km	100 kbps (-N and -P), 10 Mbps (-W)	3 – 10 years	Star	open standard	Weightless SIG
SIGFOX	sub-1 GHz	10 – 50 km	100 bps	10+ years	Star	proprietary	Sigfox
DASH7	sub-1 GHz	2 – 5 km	167 kbps	10+ years	Star / Tree	open standard	Dash7 Alliance

for real-time industrial process control [77].

- **Thread** – Thread is an IPv6-based networking protocol for home automation [78], [79]. The technology enables creating mesh networks using IP-addressable devices while keeping power consumption low. Although the full protocol specification is accessible only to the members of Thread Group Alliance, there is an open-source implementation called OpenThread.
- **6LowPAN** – 6LowPAN is a standard providing encapsulation and header compression to allow even low-power devices to send and receive IPv6 packets [80]–[82]. The 6LowPAN working group has defined 6LowPAN for the communication over IEEE 802.15.4, albeit the group's successors (6lo and 6TiSCH) work on IPv6 connectivity over other constrained networks as well.
- **Wi-Fi** – Although Wi-Fi was certainly not designed for IoT, it has been utilised in many IoT solutions due to its widespread usage [83]–[85]. Several lightweight application protocols, such as CoAP, MQTT, AMQP, etc., have been developed to reduce the unnecessary overhead

and to make Wi-Fi suitable even for constrained environments. Moreover, Wi-Fi Alliance has recently introduced Wi-Fi HaLow as a low-power Wi-Fi solution for different IoT use cases [86].

B. Long range networks

Long range networks use wireless technology capable of transferring messages up to tens of kilometres to cover large areas. Low-Power Wide Area Networks (LPWAN) represent the specialised type of network technologies designed for interconnecting devices in constrained environments, focusing on the energy efficiency and long-range coverage. We differentiate between unlicensed and licensed LPWAN according to the assigned frequency bands.

Unlicensed networks:

- **LoRaWAN** – Long Range WAN (LoRaWAN) is a specification designed for wireless communication between constrained devices [87]–[89]. The main features of this technology are low data rate and wide communication radius. LoRaWAN, which is the MAC layer defined by the LoRa Alliance, is based on a proprietary spread spectrum modulation technique called LoRa.
- **Symphony Link** – Symphony Link [90] is another wireless specification using LoRa at the physical layer. Unlike LoRaWAN, Symphony Link offers a full protocol stack to ease the process of setting up a network, making the technology interesting especially for enterprise and industrial customers.
- **Weightless** – Weightless [91] is a technology from the global standards organisation called Weightless SIG that defined three open standards: Weightless-N, Weightless-P, and Weightless-W. The standards differ according to their capabilities and requirements. Weightless-N can handle only one-way communication but is also the most lightweight, Weightless-P is the flagship offering the full feature set and two-way communication, whereas Weightless-W has the extensive feature set but also the highest requirements.
- **SIGFOX** – SIGFOX is a technology created by the identically named company that aims at building wireless networks in an unlicensed frequency band. The technology employs the proprietary ultra narrow band (UNB) modulation with a heavily limited uplink connection. The low bit rate enables communication over large distance while using very low transmission power [92]–[94].
- **DASH7** – DASH7 Alliance protocol (D7AP) is an open source technology for low power communication [95]–[97]. Historically, it was based on the ISO/IEC 18000-7 standard for active RFID but has been significantly extended over the years. D7AP currently defines a full protocol stack from the physical layer up to the application layer.

Licensed networks:

- **eMTC** – enhanced Machine Type Communication (eMTC) [98]–[100] is an evolution of LTE that has been optimised for IoT. Developed with energy efficiency in the mind, LTE-M is much less demanding than LTE, while still able to work within the normal construct of LTE networks. LTE is a part of the Release 12 and Release 13 specifications published by 3GPP.
- **NB-IoT** – NarrowBand Internet of Things (NB-IoT) has been standardised recently in 3GPP's Release 13 and it is aimed to address even more energy constrained devices than eMTC. NB-IoT does not require developing any additional networks as it is built from existing LTE functionalities and can be deployed in three different operation modes – stand-alone, in-band, or guard band [39], [101].
- **EC-GSM-IoT** – Extended Coverage GSM IoT (EC-GSM-IoT) [102] is a standard based on eGPRS that enables low power communication over GSM frequency bands. Since the GSM networks require only software updates to connect EC-GSM devices, the existing cellular infrastructures of the network operators can be re-used to offer low power connectivity.

V. Traffic Characteristics of IoT Application Domains

M2M communication is the fundamental part of the IoT paradigm. The number of devices connected to the Internet grows exponentially and so does the network traffic. In most situations, we are dealing with low-power, battery-operated devices that send and receive messages over constrained networks, unlike traditional human-centric communications. Understanding the characteristics of the traffic generated by users of the network is the crucial first step in network design. The more accurately a technology meets the application requirements, the better it utilises the constrained resources. Moreover, the knowledge of traffic characteristics facilitates the formation of new business opportunities. End users can estimate the approximate costs arising from the network communication and compare them to the value of acquired information, while network operators can find new markets for providing their services. Last but not least, the traffic characteristics reveal the feasibility of IoT use cases and major barriers to spread IoT globally. A proper comprehension of these issues can not only improve the current solutions but can also speed up the entire deployment process.

IoT application domains consist of many services, which, as we show in this section, can have very diverse traffic characteristics. Therefore, we need to look at every service individually; to this end, we reviewed the state-of-the-art solutions to identify suitable representative application domains for our study. It is necessary to note that different solutions targeting the same service could use slightly different configurations, which is completely acceptable. During our process, we aimed to define the optimal traffic characteristics that would capture the core demands on network technologies. Specific situations might need specific adjustments, but the fundamental principles have always remained the same.

TABLE II
TRAFFIC CHARACTERISTICS OF SMART BUILDINGS AND LIVING

Service	Network size	Traffic rate	Demands on QoS	Energy source
Building condition monitoring (excluding anomaly detection)	small to medium, 10s to 100s of devices	regular, 1 message every hour per device;	low, tolerable delay 1 min	mains/battery powered (non-rechargeable)
Anomaly detection		irregular, infrequent	high, tolerable delay 3 sec	mains/battery powered (non-rechargeable)
Lighting control		irregular, infrequent	high, tolerable delay 3 sec	mains powered
Indoor climate control		regular, 1 message every 15 min per device	high, tolerable delay 5 sec	mains powered
Smart appliances		irregular, infrequent	high, tolerable delay 3 sec	mains/battery powered (rechargeable)
Energy and water use	small, <10 devices	irregular, infrequent	high, tolerable delay 3 sec	mains powered/ self-powered

To facilitate discussion and comparison, all the eight application domains follow the same structure, viz. short introduction, typical applications, traffic characteristics, preferred network technologies, and feasibility and major challenges. Moreover, the traffic characteristics of IoT services are always summarised in the referenced tables. This hierarchy reduces the distraction and focuses on the main objective – defining the traffic characteristics of IoT application domains.

A. Smart buildings and living

The smart buildings and living domain aims to increase the energy efficiency of buildings and improve our quality of life. There has certainly been a significant demand for automation in this field during the last few years and as a result, many solutions have been proposed. Nevertheless, the benefits of IoT push the possibilities even further and from simple systems, with statically-defined behaviour, we can now develop highly dynamic architectures that collect user activity patterns and adapt to them accordingly.

1) Typical applications: The typical applications for smart buildings and living include automated lighting and heating control [103], energy and water usage monitoring for saving expenses [104], remote control of smart appliances and personal adjustments based on user's preference [105], but also anomaly detection for increased security of the property [106].

2) Traffic characteristics: From data traffic perspective, smart buildings and living is relatively undemanding but requires a scalable infrastructure because every property is different. The network size is small to medium, usually consisting of tens up to hundreds of connected devices. The traffic rate is infrequent and many times also irregular, considering the fact that people move within the building during the day. Nevertheless, the requirements on QoS can be high as a user wants fast response times and is not willing to wait half a minute till the lights are turned on or the appliance executes the desired command. As far as the energy source is concerned, depending on the service, the devices can be mains or battery powered, with or without the possibility to easily recharge, but they can also be self-powered, for example by water flow in the case of water monitoring devices. Table II summarises the traffic characteristics of the most common services in smart buildings and living.

3) Preferred network technologies: Based on the defined data traffic of smart buildings and living applications, the short-range network technologies might be preferable. For example, Wi-Fi is very widespread and as it has been shown, many times the energy resources are not the biggest issue. For more constrained devices, some of WPANs specifically designed for IoT (such as Bluetooth, ZigBee, Z-Wave, Thread, etc.) could be a good choice.

4) Feasibility and major challenges: The smart buildings and living domain already has lots of application solutions and since the traffic is not so demanding, the technology itself is not a major challenge. The bigger issue seems to be the poor interoperability between devices from different manufacturers and thus the lack of one common platform, from which the devices could be managed. Currently, there are two approaches to solve this problem. The first approach aims to propose a globally accepted network technology (like ZigBee, Z-Wave, Thread, etc.), whereas the second is based on hiding the underlying network technology by offering an integration framework.

B. Smart healthcare

Smart healthcare is another highly discussed domain with impact on two user groups – individuals and society. Individuals mainly focus on the ability to track their physical activities, whereas the goal of the society is to increase the quality of medical treatment while reducing healthcare costs. These benefits can be achieved by utilising wearable devices able to monitor a person's health and provide on-the-go diagnostics capabilities, which create new possibilities for disease treatments or even making early predictions to intervene illnesses. IoT can help with having the right information at the right time.

1) Typical applications: Applications for individuals aim at monitoring personal condition, which includes measuring physiological changes and analysing motion for activity classification [107]. The outcome can be utilised anywhere from fitness tracking [108] through child and elder care [109] up to the assisted living [110]. Similarly, doctors and hospitals seek solutions that gather desired information about patients' health condition and simplify the evidence as well as report

TABLE III
TRAFFIC CHARACTERISTICS OF SMART HEALTHCARE

Service	Network size	Traffic rate	Demands on QoS	Energy source
Chronic disease management	small, <10 devices	regular, frequency based on the type of disease	high, tolerable delay based on the type of disease	battery powered (rechargeable)
Personal condition monitoring	small, <10 devices	regular, 1 msg every 10 sec per device	high, tolerable delay 5 sec	
Personal assistance	small, 10s of devices		high, tolerable delay 3 sec	mains/battery powered (rechargeable)
Patients surveillance	medium, 100s of devices		high, tolerable delay 3 sec	

TABLE IV
TRAFFIC CHARACTERISTICS OF SMART ENVIRONMENT

Service	Network size	Traffic rate	Demands on QoS	Energy source
Forest fire detection	medium to large, 100s to 1000s of devices	irregular, infrequent	medium, tolerable delay 15 sec	battery powered (non-rechargeable, but possible to harvest energy)
Earthquake detection	medium to large, 100s to 1000s of devices	irregular, infrequent	high, tolerable delay 5 sec	
Tsunami detection	medium to large, 100s to 1000s of devices	irregular, infrequent	high, tolerable delay 5 sec	
Landslide and avalanche detection	medium to large, 100s to 1000s of devices	irregular, infrequent	high, tolerable delay 5 sec	
Volcano activity monitoring	small, 10s of devices	irregular, infrequent	high, tolerable delay 5 sec	
Air pollution monitoring	medium to large, 100s to 1000s of devices	regular, 1 msg every 15 min per device	medium, tolerable delay 15 sec	
Wildlife tracking	medium, 100s of devices	regular, 1 msg every 30 min per device	low, tolerable delay a few hours	

distribution process so that it would be easier to access the patients' data [4].

2) Traffic characteristics: The traffic characteristics reflect the capabilities of wearable devices and requirements of healthcare applications. The network size depends on the application scenario – self-tracking can be effectively realised using a few devices, in which case the network size is small, whereas tracking patients in the hospital may require medium network size with hundreds of nodes to cover the entire building. The traffic rate can be defined as regular with fast frequency as the health condition may change rapidly. Demands on QoS are undoubtedly high, the message loss or long delay is unacceptable in the case of emergency. Wearable devices are battery powered, and their longevity is an issue due to the high traffic rate. Nevertheless, they can be easily recharged. Besides dynamic nodes, services such as patients surveillance can also use static nodes with mains power source. Table III describes the traffic characteristics of different healthcare and safety services.

3) Preferred network technologies: Since the network size is small to medium, the short-range network technologies will do their job well. In particular, RFID, Bluetooth, and ZigBee are very popular among healthcare applications with a smartphone as a gateway.

4) Feasibility and major challenges: Many of the defined services are definitely feasible using today's technologies, but they have to be error-free and it can be expensive. Nonetheless, the gained benefits may save even more, so the initial investment would be worth it. The main challenge of developing solutions for healthcare is how to guarantee the quality and availability of the services while keeping the devices simple, portable and non-intrusive. Ideally, the persons or patients being monitored do not have to carry/wear the devices and can be remotely monitored by sensing devices around them.

C. Smart environment

The smart environment is an endeavour to monitor the space around us for a better comprehension. Although we cannot control a force of nature, by careful observation we can detect different natural phenomena and react to them accordingly. Especially in the case of rare events such as natural disasters, a quick reaction is crucial. IoT can offer wide sensing capabilities at relatively low costs, which can be extremely beneficial in many scenarios.

1) Typical applications: When monitoring natural environments, there is the primary focus on detecting disasters like forest fire [111], earthquake [112], tsunami [113], landslide [114], avalanche [115], etc. Nevertheless, some of the solutions aim to observe less time-critical phenomena, such as air pollution [116] or wild animals tracking [117].

2) Traffic characteristics: Meeting the requirements for traffic characteristics of smart environment applications might be challenging. The network size can be defined as medium up to large, usually with hundreds of devices connected over a wide area. Since many applications are based on detecting rare events, the traffic rate is irregular and relatively infrequent, although with high demands on QoS. Applications for regular environmental monitoring come with medium to low demands on QoS, such as air pollution monitoring or wildlife tracking. Smart environment applications are typically deployed in large

rural areas so devices need to be battery-powered. However, recharging them would be economically infeasible, and therefore there are attempts to minimise energy consumption or alternatively utilise renewable energy technology like photovoltaic and wind energy harvesting. The summary of smart environment applications can be found in Table IV.

3) Preferred network technologies: Looking at the required coverage of smart environment applications, this should be an ideal domain for low-power wide area networks. Many solutions, however, have been proposed using short-range networks with multi-hop routing. This can be attributed to the infancy of LPWANs, but in fact, there is also one advantage of using short-range networks. A mesh topology can offer decentralised communication between sensor nodes themselves, which may be quite useful in some scenarios.

4) Feasibility and major challenges: Smart environment applications, especially for rare event detection, are highly demanding because they can warn us of the potential natural disasters. Therefore, researchers are dealing with this topic for some time and countries with a high occurrence of natural phenomena like earthquakes or volcano activity are already using various detection systems for protection and mitigation. However, in order to proliferate these systems globally and to monitor less critical events, further research is inevitable. The major issue involves the battery life of cheap devices, which makes them difficult to remain powered on for years without any human interference.

D. Smart city

With the rapid increase of the urban population worldwide, making public services sustainable requires finding new ways to improve the utilisation of public resources, decrease the running costs and optimise the core infrastructure components of a city. The topic of making a city more intelligent is certainly not novel, yet IoT can offer computing and sensing capabilities that could boost the speed of overall progress.

1) Typical applications: The applications for smart city target wide spectrum of objectives, from the reduction of expenses on everyday services such as lightning [118] or waste management [119], through to the monitoring of city conditions like noise [120] or air pollution [121], up to the enhancement of available information about current traffic congestion [7] or parking situation [122].

2) Traffic characteristics: Due to the number and variety of services, the traffic characteristics of the smart city domain is quite diverse. The network size is usually medium up to large, connecting hundreds to thousands of devices. Moreover, the urban area is typical with its high density and amount of obstacles, which must be taken into consideration. On the other hand, the traffic rate and QoS are less demanding as IoT urban services are usually not that critical. In most cases, the frequency of data transfer is lower, or even irregular, with an acceptable delay of up to 1 minute. As far as the energy source is concerned, the majority of services rely on battery-powered sensors, which should have a very good longevity and, therefore, some energy harvesting solutions would be useful. Table V describes the traffic characteristics of different services individually.

3) Preferred network technologies: An urban area has usually a good coverage of all kinds of networks, so both short and long range network technologies would be suitable. However, looking at the traffic characteristics, LPWANs can meet all the requirements while offering an easier implementation.

4) Feasibility and major challenges: From the technical point of view, creating a smart city is not an issue. All of the described services could be easily developed and deployed using current technologies. But the question is at what cost. Moreover, it is important to mention that a city is not a green field and many systems are already implemented. The majority of these systems are proprietary and mutually incompatible, yet must be integrated into one complex smart city platform. The cost efficiency and closeness of current solutions present complex challenges that are slowly being overcome, but there is still a need for further research.

E. Smart energy

The smart energy domain refers to the improvements in distribution and consumption of utilities such as electricity, gas, and water. The production of electricity is the focal point as there is a global effort towards renewable energy sources, which produce environment-friendly but fluctuating power. Due to its volatile nature, the electrical grid has to be much more flexible and dynamic. IoT can monitor the changing conditions and generate the patterns for more accurate grid reconfiguration.

1) Typical applications: Smart energy applications precisely monitor energy consumption and create patterns that can be used for a greater comprehension of power utilisation. Then, the predictions can be made from the gained information, which ultimately leads to the better optimisation of resources. Moreover, a smart grid system not only improve a balance between energy production and consumption but also raises a public understanding how to use energy more efficient [123]–[125].

2) Traffic characteristics: The smart energy domain is specific for its great coverage area requirement and large-scale emerging industrial applications. The network size is medium to large, especially big cities with many households create a big demand on the efficient network utilisation. The traffic rate is typically regular as periodic data are very valuable for consumption analyses of industrial applications. There are, however, some services, for instance an outage detection, which do not need to send data regularly. These services are designed for monitoring rare events and require near real-time responses. Besides alarms, some delay is tolerable in other applications. The devices for smart energy are mostly mains powered or less commonly battery powered in specific non-invasive solutions. The summary can be found in Table VI.

3) Preferable network technologies: The smart energy domain requires good wide area coverage and this is where LPWANs excel at. While premises networks can be based short range technologies (e.g. smart meters can be connected

TABLE V
TRAFFIC CHARACTERISTICS OF SMART CITY

Service	Network size	Traffic rate	Demands on QoS	Energy source
City energy and water consumption monitoring	medium to large, 100s to 1000s of devices	regular, 1 msg every 10 min per device	low, tolerable delay 1 min	mains powered/ self-powered
Lightning control	large, 1000s of devices	irregular, infrequent	medium, tolerable delay 15 sec	mains powered
Parking tracking	large, 1000s of devices	irregular, infrequent	medium, tolerable delay 10 sec	battery powered (non-rechargeable, but possible to harvest energy)
Traffic management	large, 1000s of devices	regular, 1 msg every 10 min per device; irregular for alarms	medium, tolerable delay 15 sec; high for alarms	
Waste management	large, 1000s of devices	irregular, infrequent	medium, tolerable delay 30 sec	
Urban conditions monitoring	medium to large, 100s to 1000s of devices	regular, 1 msg every 15 min per device; irregular for alarms	medium, tolerable delay 30 sec; high for alarms	
Structural health monitoring				

TABLE VI
TRAFFIC CHARACTERISTICS OF SMART ENERGY

Service	Network size	Traffic rate	Demands on QoS	Energy source
Smart metering	medium to large, 1 device per household	regular, 1 msg every 15 min per device	medium, tolerable delay 15 sec	mains/battery powered (non-rechargeable)
Asset management	medium to large, 100s to 1000s of devices			
Outage detection	medium to large, 1 device per household	irregular, infrequent	high, tolerable delay near real-time	

to home Wi-Fi), power transmission and distribution require communication over long distances. Yet even smart meters can benefit from long range technologies, such as LoRa, to avoid unnecessary complications with various home network configurations.

4) Feasibility and major challenges: The transformation to sustainable and renewable energy sources has already started. Many good solutions have been developed during the last decade, yet volatility of power generation remains as the biggest technological challenge that requires significant changes in the energy grid. It takes some time to design fully renewable energy systems, mainly due to the economic barriers, but many countries understand the gained benefits for the environment and therefore are actively making progress.

F. Smart transport and mobility

The rapid urbanisation connected with growing traffic congestion and globalisation of markets have created a demand for managing transport and mobility in a smarter way. The aim is to make transportation quicker, cheaper, and safer, which can be achieved by collecting all kinds of data and analysing them in order to find optimal solutions.

1) Typical applications: Among the most discussed applications of smart network and mobility domain are undoubtedly automated and autonomous vehicles [126] because it is related to every user group – individuals, society, as well as industry. Nevertheless, other typical applications include vehicle localisation and tracking [127], quality of shipment monitoring [128], dynamic traffic lights control based on the current traffic situation [129], and road condition monitoring [130].

2) Traffic characteristics: The smart transport and mobility domain can be demanding in terms of traffic characteristics. The number of sensors in vehicles is increasing rapidly, such that a network capable of handling thousands of mobile connected devices with good coverage is not inconceivable. The traffic rate varies based on the service. There might be a need to send a message every few seconds, for example in the case of public transport arrivals prediction, but the frequency could be extended to as far as 1 message every 24 hours, in scenarios such as data acquisition for analytical purposes. The demands on QoS are usually high, with the tolerable delay being near real-time in vehicle-to-vehicle communication, although the majority of services do not require immediate delivery times and a few seconds delay is tolerable. The devices for smart transport and mobility are mostly powered by batteries of the vehicles or mains powered for roadside devices/sensors, so the precision and accuracy are preferred over energy savings. However, even in this domain, it is possible to find devices for which the energy efficiency is critical, such as non-invasive road sensors, or sensors for monitoring the quality of shipment conditions. More information about traffic characteristics of the smart transport and mobility domain is shown in Table VII.

3) Preferred network technologies: It cannot be said which types of network technologies are preferred in smart transport and mobility as the requirements on traffic characteristics are very diverse. Vehicle-to-vehicle communications definitely must be built upon short-range technologies, whereas vehicle localisation and monitoring require a long-range network

TABLE VII
TRAFFIC CHARACTERISTICS OF SMART TRANSPORT AND MOBILITY

Service	Network size	Traffic rate	Demands on QoS	Energy source
Vehicle automation	large, 1000s of vehicles	regular, 1 msg every 24 hours per vehicle, irregular and frequent in vehicle-to-vehicle (V2V) communication	low, tolerable delay 1 min; high for V2V, tolerable delay near real-time	vehicle's battery powered
Vehicle localisation and monitoring	large, 1000s of vehicles	regular, 1 msg every 30 sec per vehicle	medium, tolerable delay 10 sec	vehicle's battery powered
Quality of shipment conditions monitoring	medium, 100s of devices	regular, 1 msg every 15 min per device	medium, tolerable delay 15 sec	battery powered (rechargeable)
Dynamic traffic lights control	large, 1000s of devices	regular, 1 msg every 1 min per device	high, tolerable delay 5 sec	mains powered
Road condition monitoring	large, 1000s of devices	irregular, infrequent	medium, tolerable delay 30 sec	battery powered (may be rechargeable)

TABLE VIII
SMART MANUFACTURING AND RETAIL

Service	Network size	Traffic rate	Demands on QoS	Energy source
Production line	medium, 100s of devices	regular, frequency varies; irregular for alarms	usually high, tolerable delay a few sec; high for alarms	mains/battery powered (non-rechargeable)
Inventory tracking	medium to large, 100s to 1000s of devices	irregular, infrequent	medium, tolerable delay 10 sec	passive/battery powered (non-rechargeable)
Indoor localisation	large, 1000s of devices	irregular, infrequent	high, tolerable delay 5 sec	passive/battery powered (non-rechargeable)
Environment monitoring	medium, 100s of devices	regular, 1 msg every 10 min per device; irregular for alarms	medium, tolerable delay 15 sec; high for alarms	mains/battery powered (non-rechargeable)
Maintenance and repair optimisation	medium, 100s of devices	regular for condition reports, 1 msg every 10 min per device; irregular for alarms	medium, tolerable delay 10 sec; high for alarms	mains/battery powered (non-rechargeable)

technology. Therefore, it is necessary to look at every service individually.

4) Feasibility and major challenges: Smart transport and mobility applications, such as vehicle automation, presents the start-of-the-art of the current possibilities. While there is active ongoing research on autonomous vehicles globally, the realisation of fully automated transportation is still some distance away due to the major challenges like the complexity of the domain, extremely dynamic conditions, and the required reliability. Nevertheless, the current research is taking giant leaps.

G. Smart manufacturing and retail

The globalisation and raising expectations of fully customisable products create high demands on manufacturing and retail. In order to keep up with this trend, the production has to offer shorter development periods, a great amount of flexibility, resource efficiency, and new innovative business models. The IoT can provide real-time information due to the massive deployment of cyber-physical systems, which is also the cause of the next industrial revolution, called Industry 4.0.

1) Typical applications: In this domain, the aim is to improve the production line by implementing quality assurance and flexible customisation [131], tracking the inventory for more efficient supply chain management [132], utilising localisation of both items and workers [133], monitoring the environment to ensure the safe conditions [134], as well as monitoring the machines in order to optimise their maintenance and repair schedules [135].

2) Traffic characteristics: The network size of smart manufacturing and retail is usually medium to large, considering the amount of items, machines and workers to be monitored. The traffic rate is both regular and irregular as many applications need to collect data reports of production conditions, but also must be able to detect different events and alarms. QoS depends on the type of message. While sending basic reports can be delayed up to fifteen seconds, the alarms must always be detected immediately. The devices for smart manufacturing and retail domain cover a great variety of tasks and based on the utilisation they can be passive, mains powered, or battery powered. Table VIII provides a summary of traffic characteristics for different services.

3) Preferred network technologies: Since the majority of manufacturing and retail processes are indoor, short-range network technologies play an important role. In particular, RFID is a very popular short-range technology due to availability of passive and cheap RFID tags. Nonetheless, long-range network technologies find their utilisation in manufacturing as well.

TABLE IX
TRAFFIC CHARACTERISTICS OF SMART AGRICULTURE

Service	Network size	Traffic rate	Demands on QoS	Energy source
Irrigation	small to medium, 10s to 100s of devices	regular, 1 msg every 6 hours per device	low, tolerable delay 1 min	battery powered (non-rechargeable, possible to harvest energy)
Fertilization	small to medium, 10s to 100s of devices	regular, 1 msg every 6 hours per device	low, tolerable delay 1 min	battery powered (non-rechargeable, possible to harvest energy)
Pest control	small to medium, 10s to 100s of devices	regular, 1 msg every 6 hours per device	low, tolerable delay 1 min	battery powered (non-rechargeable, possible to harvest energy)
Animal monitoring	small to medium, 10s to 100s of devices, possibly 1000s	regular, 1 msg every 6 hours per device; can be irregular	low, tolerable delay 1 min; high for alarms	battery powered (non-rechargeable)

4) Feasibility and major challenges: The manufacturing and retail domain is an industry that has been experiencing continuous changes due to high consumer expectations and demands. Currently, the applications based on IoT are non-critical and mostly supportive, but there has been a significant progress in the reliability of wireless network technologies during the last years. Sometimes companies prefer well-tested and time-proven solutions, but if they want to keep up with today's leaders like Amazon and Alibaba, the constant change is the only option.

H. Smart agriculture

Agriculture is an important sector for everyone, yet it faces challenges that cannot be ignored. The growth of global population has prompted a demand to increase food production by continually improving agriculture techniques. Moreover, due to the changes in the climate, these techniques need to increase food security by facilitating the climate adaptation and mitigation. The concept of climate-smart agriculture was created in order to target the mentioned challenges and IoT plays a significant role in it.

1) Typical applications: IoT enables comprehensive in-field monitoring, which can offer a lot of valuable information. Therefore, applications for agriculture aim to improve typical services such as irrigation [136], fertilisation [137], pest control [138], and animal monitoring [139].

2) Traffic characteristics: The traffic characteristics of smart agriculture domain reflect its requirements – sending a small amount of data about the environment conditions over a long period of time. The network size is medium to small, depending on the area the application should cover. The traffic rate is usually regular, although not very frequent as the conditions are changing rather slowly. In the case of animal monitoring, the traffic rate can be both regular and irregular, depending on the specific implementation. Demands on QoS are low with the tolerable delay of one minute. However, the alarms should be sent in real-time, for example when cattle goes beyond the pastures' borders. The biggest requirements are on energy source because the devices have to be battery-powered. Recharging them would be difficult, but plant sensors can harvest the energy and thus extend their battery life. Table IX summarises the traffic characteristics of smart agriculture.

3) Preferred network technologies: Agriculture is very demanding on battery consumption and, therefore, requires very lightweight communication. LPWANs, such as NB-IoT from licensed networks, or LoRaWAN from unlicensed networks, could fulfil the needs and thus be a good choice. On contrary, short-range technologies may be preferable in areas with a poor network coverage.

4) Feasibility and major challenges: Smart agriculture is an inevitable trend if we want to mitigate climate changes and produce food in a sustainable way. The major challenge is the cost of innovation as the agriculture sector has very tight margins. In order to proliferate solutions for smart agriculture globally, the devices must be extremely low-cost, durable and with long battery life. Although it is not an easy task, new network technologies aimed specifically for IoT are trying to target these needs and make smart agriculture applications feasible to be deployed into the production.

VI. EVALUATION

In the previous section, we defined traffic characteristics of IoT application domains. To achieve our objective, i.e. to determine with high accuracy the demands on networks defined by various IoT application scenarios, we identified and discussed the most typical services for every domain, examined the network configurations proposed by other researchers, and combined the information with our research interests to derive the outcomes.

Together, we described 42 services from eight application domains as shown in Table II to Table IX. During the process, we encountered solutions that were addressing the same issue with slightly different configurations, depending on the specific implementation and authors' perception. We find these differences completely acceptable as there is no universal answer to all possible situations. The important fact is that the fundamental aspects remained the same in all cases. Therefore, our defined traffic characteristics can be regarded as the reference guide for proposing more efficient solutions and understanding the demands on network technologies from the IoT perspective.

We present three charts to compare the IoT application domains among one another based on their traffic characteristics. As shown in the previous section, the services within

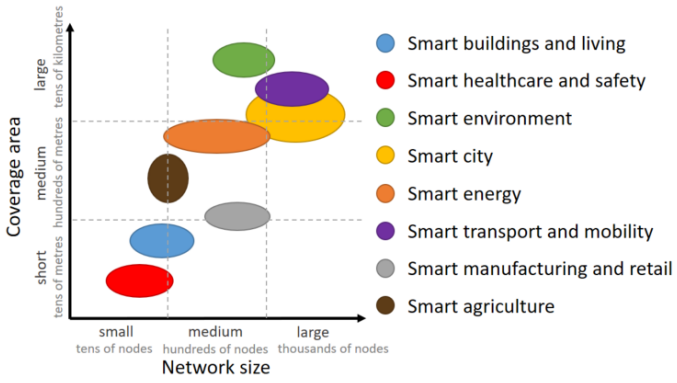

Fig. 4. Relationship between network size and coverage area of application domains.

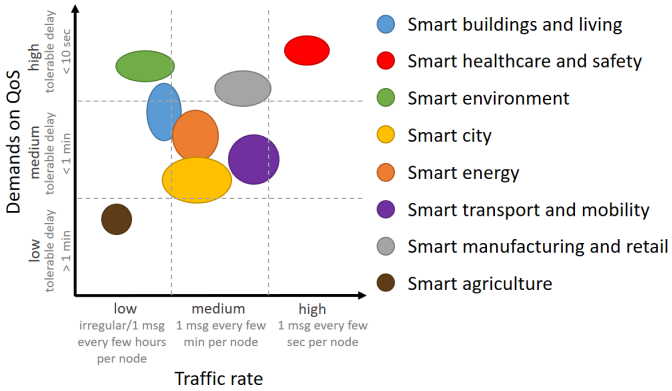

Fig. 5. Relationship between traffic rate and demands on QoS of application domains.

one application domain may quite differ in some cases, so in order to make a comparison at the domain level, some generalisation is inevitable. We did so by aggregating values into more general definitions, which are now represented by the oval shapes in the charts. To make the charts more consistent and readable, the biggest outliers (services that are too distinct from the majority) might not be depicted, although they still had been taken into consideration in the aggregation process. We admit this generalisation might have involved the subjective opinions of the authors and therefore could be the topic of further discussion, nevertheless, we made our decisions purely based on the presented traffic characteristics to reduce the potential ambiguity and to be as objective as possible. Furthermore, we provide the arguments with every chart to make our point of view clearer.

Firstly, Fig. 4 depicts the relationship between network size and coverage area that IoT application domains require. By network size, we mean the number of connected devices, while coverage area represents a physical space in which the devices are distributed. This correlation aims to highlight the differences in demands among application domains. So, for example, the smart healthcare domain is depicted in the bottom-left corner, symbolising low requirements on both network size and coverage area. The reason is that the most typical applications monitor activities of a single person, which means only a few devices connected in body area network (BAN), or personal area network (PAN).

In contrast, smart city is the other end of the spectrum, connecting thousands of devices over several square kilometres. Another interesting item worth pointing out is the comparison of domains like the smart manufacturing and retail to the smart environment. As we can see from the network size perspective, these domains are almost equivalent. However, applications in the smart environment usually have to cover much larger area, which makes the overall requirements on network technologies significantly different. Looking at Fig. 4, we could reasonably state that the domains on the right side are more demanding than the domains on the left side. But this, as shown in Fig. 5, would only be partially true.

A relationship between traffic rate and demands on QoS is illustrated in Fig. 5. These aspects of traffic characteristics have been discussed for every service in IoT application domains, but no direct comparison has been made between them. However, as shown in Fig. 5, the correlation is significant. In most cases, the higher traffic rate also means the higher demands on QoS, especially with regard to tolerable delay. The typical example is the smart healthcare, in which even minor changes in conditions can result in a critical situation and thus services need to update data regularly and reliably.

On the contrary, the traffic rate and demands on QoS are not equal every time, such as in the case of the smart environment. This domain does not send data on a regular basis, but once a rare event is detected, the system should immediately trigger the alert. Furthermore, we would like to highlight the differences between Fig. 4 and Fig. 5. While the smart healthcare domain could be considered to be the least demanding in Fig. 4, this relationship shifts it to the opposite corner in Fig. 5. Therefore, we cannot ascertain the demand levels of the domains solely according to the individual graphs. These analyses are essential for understanding the specific requirements of the IoT domains so that we are able to design more cost-effective solutions.

Next, the correlation depicted in Fig. 6 represents a relationship between sustainable energy and demands on the longevity of devices. By sustainable energy, we mean the way of powering devices. In the high sustainable energy category, we think of passive RFID tags or mains-powered devices. The medium group consists of battery-powered devices with an option to be more or less often recharged. The last group represents situations with the most scarce energy, where recharging batteries would be very difficult and thus inefficient. Therefore, it is necessary to find other options how to prolong the battery life, such as harvesting energy from the environment. The vertical axis represents demands on longevity, from a few days up to years of devices' lifespan.

From Fig. 6, we can see a few interesting patterns. The distribution of the domains is mainly in the upper part of the graph, which means high demands on the longevity of devices. This comes from the IoT paradigm itself, which aims to realise IoT services that are accessible anytime and from

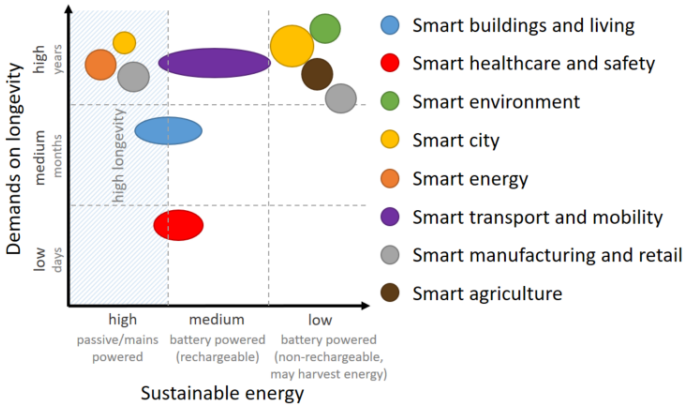

Fig. 6. Relationship between sustainable energy and demands on longevity of application domains.

anywhere. Although we can accept the lower longevity when the devices can be recharged, such as in the case of smart healthcare, the expectations are very high in general. In fact, the longevity of devices is one of the major deal-breakers when thinking of spreading IoT applications globally. To depict the domains accurately in terms of sustainable energy, we had to differentiate between smart city and smart manufacturing and retail. As mentioned in the previous section, the devices of these domains are usually mains powered or battery powered, but in the latter case, recharging them would be complicated and thus inefficient. The applications should harvest the energy whenever possible to meet the demands on longevity. Otherwise, efficient power management and strict restrictions in communication must be applied to ensure the sufficient battery lifespan. In any case, the expectations on energy-efficiency are significant.

As all three charts have shown, every IoT domain is demanding from the different perspective. By comparing application domains among one another, it is possible to see the divergence of their requirements, which substantiate the difficulty of developing suitable network technologies for the efficient solutions. We cannot target all needs with just one technology, but by having the right set of technologies, we can make the development progress much faster and easier. The aim of this section was to provide an overview of the traffic characteristics at the application domain level so that it could contribute to a better comprehension of IoT challenges and required future work.

VII. Conclusion and Future Work

The Internet of Things is a highly debated topic due to the potential it can offer, thus attracting immense interest from the industry and academia. Although it is still far from mainstream deployment, researchers are proposing state-of-the-art solutions to raise the maturity of technologies. Our objective is to review these activities and present the IoT applications from the traffic characteristics perspective.

We first differentiated our survey from existing IoT surveys and highlighted its relevance. Next, we succinctly introduced the IoT paradigm and pointed out the issues with one globally accepted definition. Then, we looked at the IoT application areas and three broad user groups that fulfil their needs with applications from eight different domains, and used Venn diagrams to illustrate the impact of user groups on application domains (cf: Fig. 1). When describing the current IoT challenges, we divided them into four categories (cf: Fig. 2) to provide a more readable overview. We then classified the most popular IoT network technologies based on their features and put them into one protocol stack, highlighting their similarities and differences.

The main part of our work is dedicated to the traffic characteristics of IoT application domains, where we examined eight application domains, specifically: smart buildings and living, smart healthcare, smart environment, smart city, smart energy, smart transport and mobility, smart manufacturing and retail, and smart agriculture. For each domain we defined the typical applications, traffic characteristics, preferred network technologies, and feasibility and major challenges. In order to provide as accurate as possible definition of the traffic characteristics, we reviewed the definitions from published works and combined them with our study. In the evaluation section, we aggregated the defined traffic characteristics from service to domain level and compared the application domains, as shown in Fig. 4 to Fig. 6. As we pointed out, each domain is demanding from different perspectives.

The main contributions of this paper come from the defined traffic characteristics of IoT application domains, which provide an overview of demands on network technologies. In addition, we depicted the detailed protocol stack for the most popular network technologies to make the comparison between them even simpler and clearer. Last but not least, we also referenced the state-of-the-art works of other researchers that have been done in recent years to highlight the current progress in IoT.

As we have shown in this paper, despite the efforts in recent years, there is still a lot to be done to proliferate the IoT. Our analysis emphasised the importance of adapting network technologies to the application needs to optimise the utilisation of constrained resources. If we want to support real deployments, both short range and long range network technologies will be needed to fulfil the demands of varying network traffic types of IoT services. In addition, new technologies, such as nanosensor networks, should be also considered and further explored as they could offer many promising innovations [140], [141]. Technologies that have been defined to meet specific application requirements brings diversity but, as we also explained, this diversity creates compatibility issues, which is another critical challenge in IoT. It is not possible to have one network technology suitable for all IoT use cases, yet we still need to ensure the cross-domain interoperability between devices.

Therefore, our objective regarding future work is to propose an integration platform that would ‘hide’ the underlying network technologies by defining an abstract layer for standardised communication. Ultimately, IoT applications would

be based on multi-network environments without the reduction or loss of intercompatibility Nonetheless, research is required in all four categories of IoT challenges: hardware, connectivity, software, and security. Only by their simultaneous improvement could be the core idea of the Internet of Things accomplished – to create the world of fully interconnected objects.

ACKNOWLEDGMENT

Jozef Mocnej would like to thank the European Commission under the Thelxinoe project for the funding that supported his visit to Victoria University of Wellington, New Zealand, where this research was conducted.

REFERENCES

[1] K. Ashton, "That 'internet of things' thing," *RFiD Journal*, vol. 22, no. 7, pp. 97–114, 2009.

[2] S. Mennicken, J. Vermeulen, and E. M. Huang, "From today's augmented houses to tomorrow's smart homes: new directions for home automation research," in *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 2014, pp. 105–115.

[3] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Sensing as a service model for smart cities supported by internet of things," *Transactions on Emerging Telecommunications Technologies*, vol. 25, no. 1, pp. 81–93, 2014.

[4] L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi, and L. Tarricone, "An IoT-aware architecture for smart healthcare systems," *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 515–526, 2015.

[5] S. Poslad, S. E. Middleton, F. Chaves, R. Tao, O. Necmioglu, and U. Bügel, "A Semantic IoT Early Warning System for Natural Environment Crisis Management," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 2, pp. 246–257, 2015.

[6] A. Medvedev, P. Fedchenkov, A. Zaslavsky, T. Anagnostopoulos, and S. Khoruzhnikov, "Waste management as an IoT-enabled service in smart cities," in *Proceedings of the Conference on Smart Spaces*. St. Petersburg, Russia: Springer, 26-28 Aug 2015, pp. 104–115.

[7] S. Djahel, R. Doolan, G.-M. Muntean, and J. Murphy, "A communications-oriented perspective on traffic management systems for smart cities: challenges and innovative approaches," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 125–151, 2015.

[8] J. Lee, H.-A. Kao, and S. Yang, "Service innovation and smart analytics for industry 4.0 and big data environment," *Procedia Cirp*, vol. 16, pp. 3–8, 2014.

[9] S. Hiremath, G. Yang, and K. Mankodiya, "Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare," in *Proceedings of the EAI 4th International Conference on Wireless Mobile Communication and Healthcare (Mobihealth)*, 2014, pp. 304–307.

[10] G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, "Smart objects as building blocks for the internet of things," *IEEE Internet Computing*, vol. 14, no. 1, pp. 44–51, 2010.

[11] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[12] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wireless Personal Communications*, vol. 58, no. 1, pp. 49–69, 2011.

[13] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[14] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[15] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414–454, 2014.

[16] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[17] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[18] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends," *Information Systems Frontiers*, vol. 17, no. 2, pp. 261–274, 2015.

[19] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.

[20] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[21] M. E. Crovella and A. Bestavros, "Self-similarity in World Wide Web traffic: evidence and possible causes," *IEEE/ACM Transactions on Networking*, vol. 5, no. 6, pp. 835–846, Dec 1997.

[22] V. S. Frost and B. Melamed, "Traffic modeling for telecommunications networks," *IEEE Communications Magazine*, vol. 32, no. 3, pp. 70–81, March 1994.

[23] V. Paxson and S. Floyd, "Wide area traffic: the failure of Poisson modeling," *IEEE/ACM Transactions on Networking*, vol. 3, no. 3, pp. 226–244, Jun 1995.

[24] A. Rao, A. Legout, Y.-s. Lim, D. Towsley, C. Barakat, and W. Dabbous, "Network Characteristics of Video Streaming Traffic," in *Proceedings of the 7th COnference on Emerging Networking EXperiments and Technologies*, ser. CoNEXT '11. New York, NY, USA: ACM, 2011, pp. 25:1–25:12.

[25] "ITU-T Y.4050/Y.2069 - Terms and definitions for the Internet of things," accessed: 12/10/2016. [Online]. Available: http://handle.itu.int/11.1002/1000/11700

[26] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, "Vision and challenges for realising the Internet of Things," *Cluster of European Research Projects on the Internet of Things, European Commision*, 2010.

[27] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview," *The Internet Society (ISOC)*, pp. 1–50, 2015.

[28] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the Internet of Things (IoT)," *IEEE Internet Initiative, Torino, Italy*, 2015.

[29] libelium, "50 Sensor Applications for a Smarter World," accessed: 12/10/2016. [Online]. Available: http://www.libelium.com/resources/top_50_iot_sensor_applications_ranking/

[30] O. Vermesan and P. Friess, *Internet of things-from research and innovation to market deployment*. River Publishers Aalborg, 2014.

[31] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[32] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security Challenges in the IP-based Internet of Things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.

[33] Z. Sheng, S. Yang, Y. Yu, A. V. Vasilakos, J. A. Mccann, and K. K. Leung, "A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities," *IEEE Wireless Communications*, vol. 20, no. 6, pp. 91–98, December 2013.

[34] "NB-IoT - Enabling New Business Opportunities," accessed: 13/10/2016. [Online]. Available: http://www.huawei.com/minisite/4-5g/img/NB-IOT.pdf/

[35] M. A. Chaqfeh and N. Mohamed, "Challenges in middleware solutions for the internet of things," in *Proceedings of the International Conference on Collaboration Technologies and Systems (CTS)*, May 2012, pp. 21–26.

[36] Y. K. Chen, "Challenges and opportunities of internet of things," in *Proceedings of the 17th Asia and South Pacific Design Automation Conference*, Jan 2012, pp. 383–388.

[37] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with china perspective," *IEEE Internet of Things journal*, vol. 1, no. 4, pp. 349–359, 2014.

[38] H.-D. Ma, "Internet of Things: Objectives and Scientific Challenges," *Journal of Computer Science and Technology*, vol. 26, no. 6, pp. 919–924, 2011.

[39] "NB-IoT: A sustainable technology for connecting billions of devices," accessed: 31/10/2016. [Online]. Available:

https://www.ericsson.com/res/thecompany/docs/publications/ericsson_review/2016/etrnarrowbandiot.pdf
[40] C. Rodriguez, "IoT Risk Becomes Real: DDoS Emerges as Primary Threat Vector for IoT," *Stratecast Perspectives & Insight for Executives (SPIE), Frost & Sullivan*, vol. 16, no. 41, 11 November 2016.
[41] I. F. Akyildiz and M. C. Vuran, *Wireless sensor networks*. John Wiley & Sons, 2010, vol. 4.
[42] K. Yang, "Wireless sensor networks," *Principles, Design and Applications*, 2014.
[43] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, "Wireless sensor networks: a survey on recent developments and potential synergies," *The Journal of supercomputing*, vol. 68, no. 1, pp. 1–48, 2014.
[44] J. Postel, "Internet Protocol," Internet Requests for Comments, RFC Editor, STD 5, September 1981, http://www.rfc-editor.org/rfc/rfc791.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc791.txt
[45] "IPv6 over Low power WPAN (6lowpan)," accessed: 9/12/2016. [Online]. Available: https://datatracker.ietf.org/wg/6lowpan/charter/
[46] "IPv6 over Networks of Resource-constrained Nodes (6lo)," accessed: 9/12/2016. [Online]. Available: https://datatracker.ietf.org/wg/6lo/charter/
[47] C. Gomez, S. M. Darroudi, and T. Savolainen, "IPv6 Mesh over BLUETOOTH(R) Low Energy using IPSP," Internet Engineering Task Force, Internet-Draft draft-ietf-6lo-blemesh-02, Sep. 2017, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-6lo-blemesh-02
[48] Y. Choi, J.-S. Youn, Y.-G. Hong, D. Kim, and J. Choi, "Transmission of IPv6 Packets over Near Field Communication," Internet Engineering Task Force, Internet-Draft draft-ietf-6lo-nfc-06, Mar. 2017, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-6lo-nfc-06
[49] "IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch)," accessed: 9/12/2016. [Online]. Available: https://datatracker.ietf.org/wg/6tisch/charter/
[50] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in *Proceedings of the 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Yichang, China, 21-23 April 2012, pp. 1282–1285.
[51] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, and G. Borriello, "Building the Internet of Things Using RFID: The RFID Ecosystem Experience," *IEEE Internet Computing*, vol. 13, no. 3, pp. 48–55, May 2009.
[52] 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*, vol. 1, no. 2, pp. 144–152, April 2014.
[53] K. Finkenzeller, *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. John Wiley & Sons, 2010.
[54] P. C. Garrido, G. M. Miraz, I. L. Ruiz, and M. Á. Gómez-Nieto, "A model for the development of NFC context-awareness applications on Internet of Things," in *Proceedings of the 2nd International Workshop on Near Field Communication (NFC)*, 2010, pp. 9–14.
[55] V. Coskun, B. Ozdenizci, and K. Ok, "A survey on near field communication (NFC) technology," *Wireless personal communications*, vol. 71, no. 3, pp. 2259–2294, 2013.
[56] K. H. Chang, "Bluetooth: a viable solution for IoT? [Industry Perspectives]," *IEEE Wireless Communications*, vol. 21, no. 6, pp. 6–7, December 2014.
[57] J. Nieminen, C. Gomez, M. Isomaki, T. Savolainen, B. Patil, Z. Shelby, M. Xi, and J. Oller, "Networking solutions for connecting bluetooth low energy enabled machines to the internet of things," *IEEE Network*, vol. 28, no. 6, pp. 83–90, Nov 2014.
[58] M. Collotta and G. Pau, "Bluetooth for internet of things: A fuzzy approach to improve power management in smart homes," *Computers & Electrical Engineering*, vol. 44, pp. 137–152, 2015.
[59] "ANT Message Protocol and Usage," accessed: 15/12/2016. [Online]. Available: https://www.thisisant.com/resources/antmessage-protocolandusage
[60] N. Q. Mehmood and R. Culmone, "An ANT+ protocol based health care system," in *Proceedings of the IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 2015, pp. 193–198.
[61] J. Ploennigs, U. Ryssel, and K. Kabitzsch, "Performance analysis of the EnOcean wireless sensor network protocol," in *Proceedings of the IEEE Conference on Emerging Technologies and Factory Automation (ETFA)*, Bilbao, Spain, 13-16 Sep 2010, pp. 1–9.
[62] "EnOcean Technology – Energy Harvesting Wireless," accessed: 15/12/2016. [Online]. Available: https://www.enocean.com/fileadmin/redaktion/pdf/white_paper/WP_EnOcean_Technology_en_Jul11.pdf
[63] J. Hall, B. Ramsey, M. Rice, and T. Lacey, "Z-Wave Network Reconnaissance and Transceiver Fingerprinting Using Software-Defined Radios," in *Proceedings of the International Conference on Cyber Warfare and Security*, Boston, MA, USA, 17-18 Mar 2016.
[64] B. Fouladi and S. Ghanoun, "Security evaluation of the Z-Wave wireless protocol," *Black hat USA*, vol. 24, 2013.
[65] P. Amaro, R. Cortesão, J. Landeck, and P. Santos, "Implementing an advanced meter reading infrastructure using a z-wave compliant wireless sensor network," in *Proceedings of the 2011 3rd International Youth Conference on Energetics (IYCE)*. IEEE, 2011, pp. 1–6.
[66] P. Darbee, "The details," INSTEON, Whitepaper, 2013.
[67] P. Darbee, "Compared," INSTEON, Whitepaper, 2013.
[68] "ZigBee Overview - Website," accessed: 28/10/2016. [Online]. Available: http://www.zigbee.org/zigbee-for-developers/zigbee/
[69] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards," *Computer communications*, vol. 30, no. 7, pp. 1655–1695, 2007.
[70] S. Farahani, *ZigBee wireless networks and transceivers*. newnes, 2011.
[71] D. Flowers and Y. Yang, "Microchip MiWi™ Wireless Networking Protocol Stack," 2010.
[72] M. A. N. AN1283, "Microchip Wireless Media Access Controller–MiMAC," 2009.
[73] M. A. N. AN1284, "Microchip Wireless Application Programming Interface–MiApp," 2009.
[74] "Wireless Mesh Networking ZigBee® vs. DigiMesh™," accessed: 16/12/2016. [Online]. Available: https://www.digi.com/pdf/wp_zigbeevsdigimesh.pdf
[75] D. Chen, M. Nixon, and A. Mok, "Why WirelessHART," in *WirelessHART™*. Springer, 2010, pp. 195–199.
[76] D. Chen, M. Nixon, S. Han, A. K. Mok, and X. Zhu, "WirelessHART and IEEE 802.15.4e," in *2014 IEEE International Conference on Industrial Technology (ICIT)*. IEEE, 2014, pp. 760–765.
[77] J. Song, S. Han, A. Mok, D. Chen, M. Lucas, M. Nixon, and W. Pratt, "WirelessHART: Applying wireless technology in real-time industrial process control," in *Proceedings of the Real-Time and Embedded Technology and Applications Symposium (RTAS)*, St. Louis, MO, USA, 22-24 April 2008, pp. 377–386.
[78] Thread Group, "Thread Stack Fundamentals," July 2015, accessed: 16/12/2017. [Online]. Available: https://www.silabs.com/documents/public/white-papers/Thread-Stack-Fundamentals.pdf
[79] "OpenThread," accessed: 16/12/2016. [Online]. Available: https://github.com/openthread/openthread
[80] Z. Shelby and C. Bormann, *6LoWPAN: The wireless embedded Internet*. John Wiley & Sons, 2011, vol. 43.
[81] G. Mulligan, "The 6LoWPAN architecture," in *Proceedings of the 4th workshop on Embedded Networked Sensors (EmNets)*. Cork, Ireland: ACM, 25-26 June 2007, pp. 78–82.
[82] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, and U. Roedig, "Securing communication in 6LoWPAN with compressed IPsec," in *Proceedings of the International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, Barcelona, Spain, 27-29 June 2011, pp. 1–8.
[83] L. Li, H. Xiaoguang, C. Ke, and H. Ketai, "The applications of WiFi-based Wireless Sensor Network in Internet of Things and Smart Grid," in *Proceedings of the 6th IEEE Conference on Industrial Electronics and Applications*, Beijing, China, 21-23 June 2011, pp. 789–793.
[84] G. R. Mendez, M. A. M. Yunus, and S. C. Mukhopadhyay, "A WiFi based smart wireless sensor network for monitoring an agricultural environment," in *Proceedings of the IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, Graz, Austria, 13-16 May 2012, pp. 2640–2645.
[85] S. Tozlu, M. Senel, W. Mao, and A. Keshavarzian, "Wi-Fi enabled sensors for internet of things: A practical approach," *IEEE Communications Magazine*, vol. 50, no. 6, 2012.

[86] W.-F. Alliance, "Wi-Fi HaLow," 2016, accessed: 16/12/2016. [Online]. Available: http://www.wifi.org/discoverwifi/wifihalow

[87] L. Vangelista, A. Zanella, and M. Zorzi, "Long-Range IoT Technologies: The Dawn of LoRa™," in *Proceedings of the 1st International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures*, Ohrid, Macedonia, 23-25 Sept 2015, pp. 51–58.

[88] K. Mikhaylov, J. Petäjäjärvi, and T. Haenninen, "Analysis of Capacity and Scalability of the LoRa Low Power Wide Area Network Technology," in *Proceedings of the 22th European Wireless Conference*, Oulu, Finland, 18-20 May 2016, pp. 1–6.

[89] L. Alliance, "A technical overview of LoRa and LoRaWAN," *White Paper, November*, 2015.

[90] "Symphony Link," accessed: 16/12/2016. [Online]. Available: http://www.linklabs.com/symphony/

[91] "Weightless," accessed: 16/12/2016. [Online]. Available: http://www.weightless.org/about/whichweightlessstandard

[92] "Sigfox Technology Overview," accessed: 28/10/2016. [Online]. Available: http://www.sigfox.com/en/sigfox-iot-technology-overview

[93] "SIGFOX - M2M and IoT Redefined through cost effective and energy optimized connectivity," accessed: 28/10/2016. [Online]. Available: https://lafibre.info/images/3g/201302_sigfox_whitepaper.pdf

[94] G. Margelis, R. Piechocki, D. Kaleshi, and P. Thomas, "Low Throughput Networks for the IoT: Lessons learned from industrial implementations," in *Proceedings of the IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, Italy, 14-16 Dec 2015, pp. 181–186.

[95] M. Weyn, G. Ergeerts, R. Berkvens, B. Wojciechowski, and Y. Tabakov, "DASH7 alliance protocol 1.0: Low-power, mid-range sensor and actuator communication," in *Proceedings of the IEEE Conference on Standards for Communications and Networking (CSCN)*, Tokyo, Japan, 28-30 Oct 2015, pp. 54–59.

[96] G. Ergeerts, M. Nikodem, D. Subotic, T. Surmacz, B. Wojciechowski, P. De Meulenaere, and M. Weyn, "DASH7 Alliance Protocol in Monitoring Applications," in *Proceedings of the 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, Krakow, Poland, 4-6 Nov 2015, pp. 623–628.

[97] "DASH7 Alliance," accessed: 16/12/2016. [Online]. Available: http://www.dash7alliance.org/

[98] A. Rico-Alvarino, M. Vajapeyam, H. Xu, X. Wang, Y. Blankenship, J. Bergman, T. Tirronen, and E. Yavuz, "An overview of 3GPP enhancements on machine to machine communications," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 14–21, June 2016.

[99] "LTE evolution for IoT connectivity," accessed: 31/10/2016. [Online]. Available: http://resources.alcatel-lucent.com/asset/200178

[100] "3GPP standards for IoT," accessed: 31/10/2016. [Online]. Available: http://www.3gpp.org/ftp/information/presentations/presentations_2016/-3GPP_Standards_for_IoT.pdf

[101] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for M2M communication," in *Proceedings of the Workshop on Device to Device communications for 5G NETWORKS (WD5G 2016) colocated with IEEE WCNC*, Doha, Qatar, 3-6 April 2016, pp. 1–5.

[102] "Cellular system support for ultra-low complexity and low throughput Internet of Things (CIoT)," accessed: 16/12/2016. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/45_series/45.820/45820d10.zip

[103] T. A. Nguyen and M. Aiello, "Energy intelligent buildings based on user activity: A survey," *Energy and buildings*, vol. 56, pp. 244–257, 2013.

[104] M. Pipattanasomporn, M. Kuzlu, and S. Rahman, "An Algorithm for Intelligent Home Energy Management and Demand Response Analysis," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 2166–2173, Dec 2012.

[105] S. N. Han, G. M. Lee, and N. Crespi, "Semantic Context-Aware Service Composition for Building Automation System," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 752–761, Feb 2014.

[106] A. M. Zeki, E. E. Elnour, A. A. Ibrahim, C. Haruna, and S. Abdulkareem, "Automatic interactive security monitoring system," in *Proceedings of the International Conference on Research and Innovation in Information Systems (ICRIIS)*, KL, Malaysia, 27-28 Nov 2013, pp. 215–220.

[107] S. C. Mukhopadhyay, "Wearable Sensors for Human Activity Monitoring: A Review," *IEEE Sensors Journal*, vol. 15, no. 3, pp. 1321–1330, March 2015.

[108] M. Mauriello, M. Gubbels, and J. E. Froehlich, "Social fabric fitness: the design and evaluation of wearable E-textile displays to support group running," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Toronto, ON, Canada: ACM, 26 Apr - 1 May 2014, pp. 2833–2842.

[109] J. Klonovs, M. A. Haque, V. Krueger, K. Nasrollahi, K. Andersen-Ranberg, T. B. Moeslund, and E. G. Spaich, *Distributed computing and monitoring technologies for older patients*. Springer, 2016.

[110] E. I. Konstantinidis, P. E. Antoniou, G. Bamparopoulos, and P. D. Bamidis, "A lightweight framework for transparent cross platform communication of controller data in ambient assisted living environments," *Information Sciences*, vol. 300, pp. 124–139, 2015.

[111] Y. E. Aslan, I. Korpeoglu, and Ö. Ulusoy, "A framework for use of wireless sensor networks in forest fire detection and monitoring," *Computers, Environment and Urban Systems*, vol. 36, no. 6, pp. 614–625, 2012.

[112] R. Tan, G. Xing, J. Chen, W.-Z. Song, and R. Huang, "Fusion-based volcanic earthquake detection and timing in wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 9, no. 2, p. 17, 2013.

[113] D. Virmani and N. Jain, "Intelligent information retrieval for Tsunami detection using wireless sensor nodes," in *Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Jaipur, India, 21-24 Sept 2016, pp. 1103–1109.

[114] M. V. Ramesh, "Design, development, and deployment of a wireless sensor network for detection of landslides," *Ad Hoc Networks*, vol. 13, pp. 2–18, 2014.

[115] A. Van Herwijnen and J. Schweizer, "Monitoring avalanche activity using a seismic sensor," *Cold Regions Science and Technology*, vol. 69, no. 2, pp. 165–176, 2011.

[116] A. Kadri, E. Yaacoub, M. Mushtaha, and A. Abu-Dayya, "Wireless sensor network for real-time air pollution monitoring," in *Proceedings of the 1st International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, Sharjah, UAE, 12-14 Feb 2013, pp. 1–5.

[117] V. Dyo, S. A. Ellwood, D. W. Macdonald, A. Markham, N. Trigoni, R. Wohlers, C. Mascolo, B. Pásztor, S. Scellato, and K. Yousef, "WILDSENSING: design and deployment of a sustainable sensor network for wildlife monitoring," *ACM Transactions on Sensor Networks (TOSN)*, vol. 8, no. 4, p. 29, 2012.

[118] M. Castro, A. J. Jara, and A. F. Skarmeta, "Smart lighting solutions for smart cities," in *Proceedings of the 27th International Conference on Advanced Information Networking and Applications workshops (WAINA)*, Barcelona, Spain, 25-28 Mar 2013, pp. 1374–1379.

[119] V. Catania and D. Ventura, "An approch for monitoring and smart planning of urban solid waste management using smart-M3 platform," in *Proceedings of 15th Conference of Open Innovations Association FRUCT*, St. Petersburg, Russia, 21-25 April 2014, pp. 24–31.

[120] L. Ruge, B. Altakrouri, and A. Schrader, "Soundofthecity-continuous noise monitoring for a healthy city," in *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, San Diego, CA, USA, 18-22 Mar 2013, pp. 670–675.

[121] M. Penza, D. Suriano, M. G. Villani, L. Spinelle, and M. Gerboles, "Towards air quality indices in smart cities by calibrated low-cost sensors applied to networks," in *Proceedings of IEEE SENSORS*, Valencia, Spain, 2-5 Nov 2014, pp. 2012–2017.

[122] J. Rico, J. Sancho, B. Cendon, and M. Camus, "Parking easier by using context information of a smart city: Enabling fast search and management of parking resources," in *Proceedings of the 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, Barcelona, Spain, 25-28 Mar 2013, pp. 1380–1385.

[123] H. Lund, *Renewable energy systems: a smart energy systems approach to the choice and modeling of 100% renewable solutions*. Academic Press, 2014.

[124] J. Byun, I. Hong, B. Kang, and S. Park, "A smart energy distribution and management system for renewable energy distribution and context-aware services based on user patterns and load forecasting," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 2, pp. 436–444, May 2011.

[125] B. V. Mathiesen, H. Lund, D. Connolly, H. Wenzel, P. A. Østergaard, B. Möller, S. Nielsen, I. Ridjan, P. Karnøe, K. Sperling *et al.*, "Smart Energy Systems for coherent 100% renewable energy and transport solutions," *Applied Energy*, vol. 145, pp. 139–154, 2015.

[126] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in

Proceedings of the IEEE World Forum on Internet of Things (WF-IoT), Seoul, South Korea, 6-8 March 2014, pp. 241–246.

[127] S. Lee, G. Tewolde, and J. Kwon, "Design and implementation of vehicle tracking system using GPS/GSM/GPRS technology and smartphone application," in *Proceedings of the IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, South Korea, 6-8 March 2014, pp. 353–358.

[128] D. J. Bijwaard, W. A. van Kleunen, P. J. Havinga, L. Kleiboer, and M. J. Bijl, "Industry: Using dynamic WSNs in smart logistics for fruits and pharmacy," in *Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems*. Seattle, WA, USA: ACM, 1-4 Nov 2011, pp. 218–231.

[129] Y. Bravo, J. Ferrer, G. Luque, and E. Alba, "Smart Mobility by Optimizing the Traffic Lights: A New Tool for Traffic Control Centers," in *Proceedings of the International Conference on Smart Cities*, Malaga, Spain, 15-17 June 2016, pp. 147–156.

[130] A. Ghose, P. Biswas, C. Bhaumik, M. Sharma, A. Pal, and A. Jha, "Road condition monitoring and alert application: Using in-vehicle Smartphone as Internet-connected sensor," in *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, Lugano, Switzerland, 19-23 March 2012, pp. 489–491.

[131] S. Wang, J. Wan, D. Li, and C. Zhang, "Implementing smart factory of industrie 4.0: an outlook," *International Journal of Distributed Sensor Networks*, vol. 2016, p. 7, 2016.

[132] Z. Pang, Q. Chen, W. Han, and L. Zheng, "Value-centric design of the internet-of-things solution for food supply chain: value creation, sensor portfolio and information fusion," *Information Systems Frontiers*, vol. 17, no. 2, pp. 289–319, 2015.

[133] Z. Chen, F. Xia, T. Huang, F. Bu, and H. Wang, "A localization method for the Internet of Things," *The Journal of Supercomputing*, vol. 63, no. 3, pp. 657–674, 2013.

[134] X. Xu, M. Zhong, J. Wan, M. Yi, and T. Gao, "Health Monitoring and Management for Manufacturing Workers in Adverse Working Conditions," *Journal of medical systems*, vol. 40, no. 10, p. 222, 2016.

[135] J. Lee, E. Lapira, B. Bagheri, and H.-a. Kao, "Recent advances and trends in predictive manufacturing systems in big data environment," *Manufacturing Letters*, vol. 1, no. 1, pp. 38–41, 2013.

[136] J. Elliott, D. Deryng, C. Müller, K. Frieler, M. Konzmann, D. Gerten, M. Glotter, M. Flörke, Y. Wada, N. Best *et al.*, "Constraints and potentials of future irrigation water availability on agricultural production under climate change," *Proceedings of the National Academy of Sciences*, vol. 111, no. 9, pp. 3239–3244, 2014.

[137] J. He, J. Wang, D. He, J. Dong, and Y. Wang, "The design and implementation of an integrated optimal fertilization decision support system," *Mathematical and Computer Modelling*, vol. 54, no. 3, pp. 1167–1174, 2011.

[138] D. Pimentel and R. Peshin, *Integrated pest management: pesticide problems*. Springer Science & Business Media, 2014, vol. 3.

[139] K. H. Kwong, T.-T. Wu, H. G. Goh, K. Sasloglou, B. Stephen, I. Glover, C. Shen, W. Du, C. Michie, and I. Andonovic, "Practical considerations for wireless sensor networks in cattle monitoring applications," *Computers and Electronics in Agriculture*, vol. 81, pp. 33–44, 2012.

[140] N. Chopra, K. Yang, J. Upton, Q. H. Abbasi, K. Qaraqe, M. Philpott, and A. Alomainy, "Fibroblasts cell number density based human skin characterization at THz for in-body nanonetworks," *Nano Communication Networks*, 2016.

[141] E. Zarepour, M. Hassan, C. T. Chou, and M. E. Warkiani, "Characterizing terahertz channels for monitoring human lungs with wireless nanosensor networks," *Nano Communication Networks*, vol. 9, pp. 43–57, 2016.