Application Domain-based Overview of IoT Network Traffic Characteristics

ADRIAN PEKAR, Budapest University of Technology and Economics, Hungary
JOZEF MOCNEJ, Technical University of Košice, Slovakia
WINSTON K.G. SEAH, Victoria University of Wellington, New Zealand
IVETA ZOLOTOVA, Technical University of Košice, Slovakia

Over the past decade, the Internet of Things (IoT) advanced rapidly. New technologies have been proposed and existing approaches optimised to meet user, society and industry requirements. However, as the complexity and heterogeneity of the traffic that flows through the networks are continuously growing, the innovation becomes difficult to achieve in both, IoT and legacy networks. This paper provides an overview of IoT application domains from a traffic characteristics perspective. Specifically, it identifies several groups of major IoT application use cases and discusses the exhibited traffic characteristics, used network technologies for implementation, and their feasibility as well as challenges. We stress that a key factor in future IoT development are network technologies and the way they handle and forward network traffic. The traffic characteristics emerging from this work can serve as a basis for future design proposals to develop more efficient solutions as well as improving the network technologies.

CCS Concepts: • **General and reference → Surveys and overviews**; • **Networks → Network properties**; • **Hardware → Sensor devices and platforms**.

Additional Key Words and Phrases: IoT, IoT network properties, IoT traffic characteristics

ACM Reference Format:
Adrian Pekar, Jozef Mocnej, Winston K.G. Seah, and Iveta Zolotova. 2020. Application Domain-based Overview of IoT Network Traffic Characteristics. *ACM Comput. Surv.* 1, 1 (May 2020), 35 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The idea behind IoT is to extend everyday things with computing power and a 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 streamlining and securing everyday life [27, 97, 100], through improving and simplifying the current processes [39, 78], to proposing new approaches [56, 69]. IoT

Authors' addresses: Adrian Pekar, Budapest University of Technology and Economics, Department of Networked Systems and Services, Budapest, Hungary, apekar@hit.bme.hu; Jozef Mocnej, jozef.mocnej@tuke.sk, Technical University of Košice, Department of Cybernetics and Artificial Intelligence, Košice, Slovakia; Winston K.G. Seah, Victoria University of Wellington, School of Engineering and Computer Science, Wellington, New Zealand; Iveta Zolotova, Technical University of Košice, Department of Cybernetics and Artificial Intelligence, Košice, Slovakia.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2020 Association for Computing Machinery.
0360-0300/2020/5-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

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.

IoT networks have unique traffic characteristics that are different from traditional (legacy) computer networks. IoT networks are deployed for heterogeneous purposes and thus, they generate highly diverse traffic. The traffic generated in IoT networks heavily depends on the application. In most IoT application scenarios, the generation of traffic is event-driven. Event-driven traffic load generation is usually triggered by events such as target detection or object sensing, and exhibit characteristics often leading to bursty traffic [37]. Event-driven traffic generation can be relatively well handled inside IoT networks themselves. However, as IoT network traffic (with often bursty character) starts to be transferred through legacy computer networks (according to the IoT paradigm [104]), the overall heterogeneity of the internet significantly increases that consequently leads to complications in terms of network performance, scalability and manageability.

Many survey papers on IoT have been written in recent years [12, 13, 21, 48, 74, 75, 81, 111, 115, 136]. To the best of our knowledge, none of the existing surveys have covered the IoT traffic characteristics in a wide spectrum of application domains. While these works focus on the enabling technologies, architectures, protocols, applications, challenges, and future visions, they do not undertake a characterisation of the IoT traffic. IoT traffic characterisation has been a challenge for several years now. Only a handful of attempts exists in the IoT domain such as [96, 117–119]. However, these works are aimed at specific applications, scenarios or enabling technologies (e.g. Machine-to-Machine (M2M) communication, which can be seen as a subset of IoT) rather than at a comprehensive, multi-application overview. Ahmed et al. [3] surveyed the state-of-the-art research efforts in selected IoT-based smart environments and presented a high-level overview without any in-depth analysis. In conclusion, a detailed study of various IoT network traffic characteristics in smart environments is still not available.

We stress that the measurement and characterisation of IoT traffic can be of high significance for future innovation. This is the key motivation of this survey that distinguishes us from other published surveys. Our aim is to define the IoT traffic characteristics that can be regarded as the reference guide for proposing more efficient solutions and understanding the demands on network technologies from the IoT perspective. The summary of contributions of this manuscript relative to recent literature in the field is as follows:

- Compared to other papers, this survey is the first of its kind that provides a deeper summary of the most relevant enabling network technologies and their characteristics relative to different application domains.
- We compare the surveyed application domains among one another based on their traffic characteristics. The comparisons are presented from three different perspectives: network size and coverage area, traffic rate and quality of service (QoS) demands, and sustainable energy and demands on the longevity of devices. Moreover, we also summarise the key characteristics of individual IoT applications.
- We present the current trends, challenges, and future research perspectives in IoT, with regard especially to network traffic measurement and characterisation.

This paper is intended for readers who wish to become familiar with the field of IoT network traffic without having to go through the details provided in related works, standards, and specifications. The intended audience is researchers as well as professionals including solution decision makers, evaluators and architects. This paper can be beneficial to network providers for planning new network deployments or the expansion of existing infrastructures. IoT traffic characterisation with a list of traffic requirements is also important for designing solutions for supporting QoS. 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.

The rest of the paper is structured as follows: Section 2 introduces the application areas of interest and key characteristics we survey, followed by the IoT Network Technology Stack in Section 3. Section 4 then summarises their most typical traffic characteristics while Section 5 summarises the gained knowledge and takeaways. In Section 6 we discuss the key traffic characteristics of the application domains. This is followed by a discussion of challenges surrounding IoT traffic measurement which is provided in Section 7. In Section 8, we present some thoughts regarding future IoT traffic-specific research prospects while Section 9 list the general challenges in IoT. Lastly, Section 10 presents the conclusion.

2 METHODOLOGY

IoT applications play an important role in IoT traffic characterisation. As each application has a different target audience, they are used in different ways. In consequence, different kinds of IoT applications experience different types of traffic behaviour. As such, the IoT application domains in this work have been identified based on the target audience. IoT user/consumers can be categorised into three groups:

- *Individuals* – persons looking to improve their overall level of lifestyle.
- *Society* – a group of people (community) looking to find solutions for common tasks and issues.
- *Industry* – an economic or industry sector looking to satisfy customer needs and requirements.

Obviously, the defined user groups have very diverse areas of interest and the number of domains may vary greatly according to the level of abstraction. Even though every user category has specific driving needs, in general, individuals want to maximise well-being (health and safety), the society wants to maximise the efficiency of every day routines (minimise the amount of work while maximising the convenience of its execution), and the industry wants to maximise the profit (minimise the costs).

When it becomes clear what expectations IoT has to fulfil, we can identify and categorise use cases suitable for their achievement. 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. As such, we 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. Therefore, we identify them as building blocks for a better comprehension of IoT application coverage.

IoT application domains consist of many services, which can have very diverse traffic characteristics. *This creates a trade-off between generality and specificity.* The characterisation of IoT traffic is further complicated by the fact that the number of publicly available datasets for researchers to use and build upon is *very limited.* A traffic trace perhaps worth mentioning was published by Sivanathan et al. [117]. While the traces are very useful and provide valuable insight into traffic characteristics, they do so only in the smart home application domain. As such, they are not sufficient to cover the whole spectrum of IoT application domains we discuss in this paper.

In conclusion, due to the lack of comprehensive traffic traces, it is challenging to compare the individual characteristics across different applications domains. During our process, we aimed to define the optimal traffic characteristics that would capture the core demands on network technologies at the expense of creating an in-depth analysis.

To give a better understanding of the key characteristics of the IoT applications and the traffic they typically carry, we first briefly discuss some widely used IoT network technologies and protocols.

3 IOT NETWORK TECHNOLOGY STACK

IoT protocols are a fundamental part of the IoT technology stack. The interaction between various IoT components such as sensors, devices, and user applications, rely on these protocols. The overview of these protocols is, however, a challenging task. The heterogeneity and multiplicity of the IoT devices have driven the IoT network technology stack to a state when there are a plethora of various protocols working at different layers to enable IoT communication at any level. This variety is perhaps given by the very nature of IoT itself: a diverse world of Things that IoT aims to connect.

In this section we focus on two types IoT network technologies and protocols. Specifically, the (i) IoT Enabling Standards and Protocols and (ii) IoT Messaging Protocols. A comprehensive discussion of these standards and protocols is however out of the scope of this paper; detailed information can be found in [76, 99, 133].

The best way to understand the role of protocols and standards in the IoT environment is perhaps to first investigate the relation between the traditional TCP/IP model and the IoT network stack. Figure 1 depicts this relation. From the figure it is obvious that some technologies use their own solutions at the network layer, however, this may change in the future, especially with the widespread adaptation of IPv6 over constrained networks.

3.1 IoT Enabling Standards and Technologies

Several technologies exist for establishing the communication of IoT components. On small scale, IoT networks use Wireless Personal Area Network (WPAN) while on a larger scale, Wireless Local Area Network (WLAN). The former relies on technologies such as 6LowPAN and Bluetooth. The latter is based on technologies such as Wi-Fi. In this section, we briefly summarise the most popular enabling technologies for IoT networking. Table 1 summarises the similarities and differences of the discussed standards.

6LoWPAN [85, 102, 109] is a standard based on IEEE 802.15.4 providing encapsulation and header compression to allow low-power devices to communicate via IPv6. Features of 6LoWPAN include 16 and 64 bit addressing, header compression, low power consumption using Bluetooth Low Energy, and fragmentation.

Bluetooth Low Energy [29, 34, 88] is destined for ultra-low-power applications. Due to its low power consumption (can be ten times less than the classic Bluetooth), this

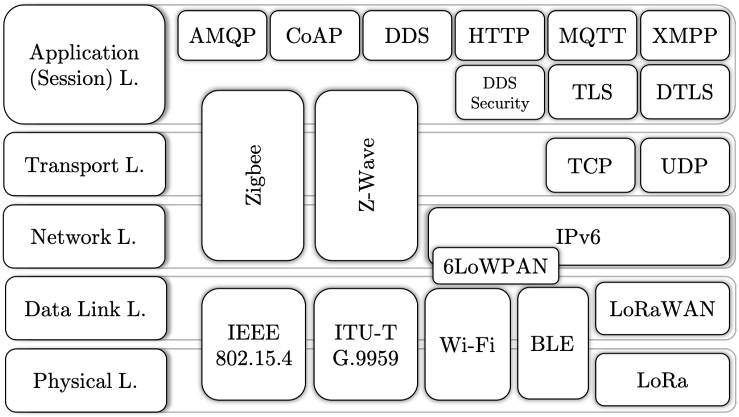

Fig. 1. IoT Network Technology Stack.

Table 1. IoT Enabling Standards and Technologies

	6LowPAN	**BLE**	**LoRaWAN**	**Wi-Fi**	**ZigBee**	**Z-Wave**
Frequency	Regional sub-Ghz bands, Global 2.4 Ghz band	Global band: 2.4 Ghz	Regional sub-Ghz bands	Global bands: 2.4 Ghz, 5.8 Ghz	Regional sub-Ghz bands, Global 2.4 Ghz band	Regional sub-Ghz bands
Coverage	100 m	100+ m	10 km	100 m to several km	10–100 m	15–150 m
Data Rate	0 – 250 kbps	125 kbps – 2 Mbps	0.3 kbps – 50 kbps	10 – 100+ Mbps	20 – 250 kbps	9.6 – 100 kbps
DL/UL Bandwidth	600 kHz, 2 MHz, 5 MHz	2 MHz	125 kHz, 500 kHz	20, 21, 22, 23, 24, 40, 80, 160 MHz	600 kHz, 1.2 MHz, 2 MHz	200 kHz
Power	Low	Lower	Low	Medium	Low	Low
Battery Life	months to years	days to weeks	10+ years	hours to days	months to years	months to years
Topology	Star, Mesh, Tree	P2P, Star	Star of Star	Star	Star, Mesh, Tree	Mesh, Proprietary

technology is ideal for connecting devices within a small range, to establish, for example, in-vehicular networking.

LoRaWAN [7, 80, 130], Long Range WAN, is a specification designed for wireless communications between a large number of constrained devices. The main features of this technology are low data rate, long energy consumption, and wide communication radius. LoRaWAN is also popular for its protected bi-directional communication.

Wi-Fi [73, 79, 128] has been also frequently used in IoT application, despite is has been designed with different requirements in mind. It ranges around 50 m. However, the original Wi-Fi standards are not suitable for IoT applications due to their frame overhead and high power consumption. Several lightweight application (messaging) protocols, such as CoAP, MQTT, AMQP, etc., have been developed to reduce the unnecessary overhead of Wi-Fi, to make it suitable also for constrained environments. The Wi-Fi Alliance has recently introduced Wi-Fi HaLow as a low-power Wi-Fi solution for different IoT use cases [8].

Zigbee [1, 14, 42] is a standard-based network protocol based on IEEE 802.15.4. Zigbee is dedicated for medium-range communication in smart homes, remote controls, and healthcare systems. It is popular for its low power and low bit rate, however, power consumption still requires improvements. The enhanced version of this standard (Zigbee Pro) offers additional features such as data encryption, authentication, data routing and forwarding.

Z-Wave [10, 43, 49] is a protocol used for home monitoring and control. As such, it is intended primarily for the smart home application domain. It provides reach features and wide support. Therefore it became soon popular amongst manufacturers. It communicates in a 30-meter range, provides point-to-point communication and small message sizes.

The technologies described above are standardised by development groups and standardisation initiatives such as IEEE, IETF, and W3C. In general, the most widely used standards are ZigBee and Bluetooth while Wi-Fi is also often utilised, mainly because of its high compatibility. However, due to the diversity of IoT application domains, every technology has found its utilisation in niche domains. The proliferation of IoT network standards also has a major drawback: a massive number of standards. In consequence, it is often not obvious which technology is the most suitable for a given application. In addition, interoperability also faces challenges that can impact the selection of one technology over the other.

3.2 IoT Messaging Protocols

In computer networks, several protocols exist for messaging. These protocols are developed at the application layer of the OSI TCP/IP model, however, some works associate them with the session layer. In general, not all the existing computer network messaging protocols are suitable for lightweight, low-energy consumption communication. In this section, we discuss only those protocols that have been widely used in IoT. The major properties of these protocols are message management, lightweight message overhead and small messaging. We provide complementary information in Table 2.

AMQP [120] – Advanced Message Queuing Protocol is an application layer messaging protocol originally designed for industrial and business management. The main goal of AMQP is ensuring interoperability, and the reliable and secure delivery of messages. The processing chain of AMQP consists of 3 necessary components: Exchange, Message Queue and Binding. The Exchange component gets the messages and puts them in the queues. The Message Queue (MQ) is responsible for storing the messages until they are obtained by the client app safely. Binding maintains the connection between the Exchange and MQ. AMQP is preferred whenever the communication requirements go beyond simple publish-subscribe messaging between the components. AMQP is reliable, proven and feature-rich. However, it is not particularly fast or lightweight.

CoAP [110] – Constrained Application Protocol was mainly developed for the restricted smart gadgets. By design, CoAP is for devices that have an identical restricted community. CoAP is based on the Representational State Transfer (REST) architecture and it runs over UDP. As such, reliability is ensured using flags: "confirmable" messages require acknowledgements while "non-confirmable" do not. Security is provided using Datagram Transport Layer Security (DTLS). CoAP provides reliability, security, low overhead, and simplicity for constrained environments.

DDS [47] – Data Distribution Services is a standard designed for high-performance and secure data-centric publish/subscribe message delivery. DDS is based on a decentralised architecture. It uses multicasting to achieve high reliability and 23 QoS services. These services are diverse enough to cover a wide variety of application and communication use cases. QoS control includes data availability, security aspects, data availability and traffic prioritisation. DDS is typically used by complex real-time applications that require high-performance, reliability, security, and speed.

HTTP [87] – Hyper Text Transfer Protocol is one of the oldest protocols used for IoT. As it runs over TCP, it requires more resources. Therefore, it is not suitable to run over embedded processes with low power. HTTP follows the client-server model: the communication takes place using request/response messages. HTTP is associated with REST. For updating, creating, reading and deleting the GET, POST, PUT and DELETE methods are used. The limitations of HTTP in IoT comes from its scalability challenges, high power consumption, unidirectional communication (client-server), and one-to-one communication.

MQTT [121] – Message Queue Telemetry Transport, is predominantly used to facilitate communication between servers and low-powered IoT devices. It sits on top of TCP and provides publish/subscribe functionality as well as some additional functionalities such as delivery guarantees. MQTT is a lightweight protocol and explicitly designed to work in unstable and unpredictable network environments. It is made of three core components: Subscriber, Publisher, and Broker. The Publisher generates the data and transmits it to the Subscriber via the Broker. Secure MQTT (SMQTT) is the secure extension of the MQTT protocol. SMQTT uses lightweight encryption attributes to enhance the security feature of MQTT.

XMPP [106] – Extensible Messaging and Presence Protocol, allows for real-time exchange of structured (XML) but extensible data between two or more network clients. It was originally designed for instant message exchange between applications to achieve security including end-to-end encryption and authentication. XMPP can implement publish-subscribe as well as client-server interaction. The advantage of XMPP is scalability which improves the performance of IoT applications.

The deployment of the above-discussed protocols is application dependent. For example, MQTT is the most widely used messaging protocol in IoT. It provides low overhead and power consumption. However, MQTT might not be suitable for a given application. For example, if the application requires communication via REST, then HTTP or CoAP would be a better choice. As all these protocols are application layer protocols, security is usually ensured via lower layers protocols such as TLS/SSL at the session layer. However, this does not mean that all the protocols provide high security. In fact, not all the messaging protocols have been designed with security as high priority. This is mainly because security features often bring burden to the protocol that is not desired in constrained environments. Nonetheless, there still some protocols that offer integrated security such as DDS and XMPP. In terms of delivery guarantees (i.e., QoS), most messaging protocols provide only limited functionality. For MQTT, AMQP and CoAP, QoS can be ensured via controlling and maintaining message exchange in an application. XMPP and REST/HTTP have no explicit QoS control. Message reliability depends on the underlying transport layer. If QoS is important, DDS would be the best option if not the only one as it provides over 20 QoS guarantees. Options for QoS include reliable or best effort delivery, data availability, ordering, and traffic prioritisation.

Table 2. Comparison of Messaging Protocols used in IoT Environments

	AMQP	**CoAP**	**DDS**	**HTTP**	**MQTT**	**XMPP**
Interraction Model	Req/Resp Pub/Sub	Req/Resp Pub/Sub	Req/Resp Pub/Sub	Req/Resp	Pub/Sub	Req/Resp Pub/Sub
Msg Header Size [bytes]	8	4	unspecified	unspecified	2	unspecified
Msg Payload Size	variale	lower than a single IP datagram	variable	variable	up to 256 MB	variable
Transport Protocol	TCP	UDP	TCP, UDP	TCP	TCP, UDP via MQTT-SN	TCP
Security	SASL, TLS/SSL	DTLS	DTLS, TLS/SSL, DDS Security	HTTPS	TLS/SSL	SASL, TLS/TLS
Delivery Guarantees (QoS)	At most once (settle), at least once (unsettle)	At most once (confirmable), At least once (non-confirmable)	Extensive (20+)	TCP congestion and flow control	At most once, At least once, Exactly once	n/a

4 IOT APPLICATIONS TRAFFIC CHARACTERISTICS

To facilitate discussion and comparison, all the eight application domains discussed in this paper follow the same structure, viz. brief description, network size and coverage, traffic characteristics, demands on QoS and, energy source and longevity. The descriptions of these characteristics are as follows:

Network size and coverage define the number of connected devices and their geographic area. This paper distinguishes three sizes: (a) small network with less than 100 devices, (b) medium networks with the number of devices between 100 and 1000, and (c) large networks with more than 1000 devices. The coverage can also be divided into small (tens of metres), medium (hundreds of metres), and large (tens of kilometres) groups.

Traffic characteristics describe the traffic rate, directionality of communication as well as an indication for possible traffic bursts (although the latter is based on logical reasoning). By traffic rate, we aim to define the regularity and frequency of message exchange. The communication between devices can be either regular or irregular, and the frequency is expressed by the sending interval. The communication direction represents the direction of the communication flow, which can be unidirectional (one-way) or bidirectional (two-way).

Demands on QoS specify the requirements for network communication. We characterise every area by a QoS label with respect to the delay it can tolerate. These labels specifically are: low-QoS (tolerable delay $>$ 1 min), medium-QoS (tolerable delay $<$ 1 min), and high-QoS (tolerable delay $<$ 10 s). It is important to emphasise that assigning QoS labels to the individual areas is not trivial. Characterising a diverse range of application domains that have various QoS requirements, network and traffic dynamics, without a standardised end-to-end protocol for QoS, is complex. For instance, in the case of some services, the primary concern is bandwidth (e.g., environment monitoring)

Table 3. Characteristics of Smart Buildings and Living

Service Name	Network Size	Network Coverage	Traffic Rate	Traffic Direction	Demands on QoS	Energy Source	Battery Longevity
Building condition monitoring [127]	small (10s) to medium (100s)	small (10s of m)	regular, 1 message every 1 min per device	bidirect.	low, tolerable delay 1 min	mains / battery (non-rechargeable)	NA / years
Lighting control [123]			irregular, infrequent		high, tolerable delay 3 sec	mains	NA
Indoor climate control [86]			regular, 1 message every 15 min per device		high, tolerable delay 5 sec		
Smart appliances [52]			irregular, infrequent		high, tolerable delay 3 sec	mains / battery (rechargeable)	NA / months
Monitoring for security and safety [16, 83]			regular, frequent		medium, tolerable delay 3s; high, for alarms		
Entertainment [17, 45]			irregular, frequent		high, tolerable delay in hundreds of ms		

while in the case of others, the delay and packet loss (e.g., health monitoring). As such, our QoS label assignment is purely based on generalising the network and service requirements of the surveyed areas.

Energy source and longevity explains the power options of devices. Devices are most commonly mains powered, battery powered (with or without a possibility to recharge and harvest energy), or passive. In case of battery power, the longevity parameter outlines the demands on devices' lifespan for a better comprehension of energy-efficiency expectation.

The characteristics of various IoT services are summarised into the eight application domains. The main objective is to define the network and traffic characteristics of these application domains. To increase the readability, within each application domain, we summarise the key characteristics in a table where we also list the most typical services.

4.1 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. An area that continuously grows in popularity is monitoring for security and safety in the smart building and living domain (although this area is also related to the smart city IoT application domain). This area is aimed at services such as smart alarm systems, cameras, and door locks. In recent years, the demand has also increased for devices that promote user entertainment. These devices aim to increase the comfort and facility of the users via personalised amusement content and social communication services. The entertainment area typically involve smart TVs and speakers, streaming devices, and game consoles. Considering the purpose of these devices, the security and entertainment areas generate a considerable volume of traffic. The traffic characteristics of the most common services in the smart buildings and living domain are summarised in Table 3.

4.1.1 Network Size and Coverage. The typical network size for this domain is small to medium, vary from tiny homes consisting of tens of connected devices and go up to hundreds

Table 4. Characteristics of Smart Healthcare

Service Name	Network Size	Network Coverage	Traffic Rate	Traffic Direction	Demands on QoS	Energy Source	Battery Longevity
Chronic disease management [60]	small (<10s)	small (10s of cm to 10s of m)	regular, frequency is based on the type of disease	bidirect.	high, tolerable delay based on the type of disease	battery (rechargeable)	days to months
Personal condition monitoring [77]			regular, 1 message every 5 sec per device		high, tolerable delay 3 sec	mains / battery (rechargeable)	NA / days
Personal assistance [61]	small (10s)	small (10s of m)					
Patients surveillance [27]	medium (100s)						

of devices in commercial buildings. The required coverage area is generally small but includes many obstacles like walls, furniture, etc.

4.1.2 Traffic Characteristics. Traffic rate can be characterised as infrequent, which is caused by the low dynamics of the sensed environment. Devices exchange messages both on irregular and regular basis, but sending rates are usually set from a few seconds up to minutes. The direction of communication is bidirectional which enables interaction with the user. Services need to support remote-control and on-demand information queries. Traffic bursts can occur at some services, particularly when an anomaly is detected or an appliance is controlled by a user.

4.1.3 Demands on QoS. The demands on QoS are typically high, as fast response times are desirable for the interaction with the user.

4.1.4 Energy Source and Longevity. Static devices are mains powered, whereas mobile or hard-to-access devices run on batteries. In either case, the energy source has a small impact on the traffic characteristics in this domain as replacing batteries/devices is feasible. Therefore, the expected longevity of battery-powered devices is measured in months up to a few years.

4.2 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 societal goal is to increase the quality of medical treatment while reducing healthcare costs. These benefits can be achieved by utilising wearable devices that are able to monitor a person's health and provide on-the-go diagnostics capabilities, which create new possibilities for disease treatment or even making early predictions to prevent illnesses. IoT can help with having the right information at the right time. Table 4 summarises the traffic characteristics of common services in the smart healthcare domain.

4.2.1 Network Size and Coverage. The size of the network is from small up to medium. Services, monitoring a single person in the personal area network (PAN), typically utilise only a few devices to gather all the necessary data, whereas solutions for organisations such as hospitals are built on multiple PANs to obtain information about all patients.

4.2.2 Traffic Characteristics. The traffic rate is typically regular with the sending intervals usually measured in seconds. The conditions can change rapidly and all these changes need to be captured and processed in time. The communication direction is bidirectional to ensure the delivery of sent messages. An acknowledgement (ACK) is highly desirable in this domain

Table 5. Characteristics of Smart Environment

Service Name	Network Size	Network Coverage	Traffic Rate	Traffic Direction	Demands on QoS	Energy Source	Battery Longevity
Forest fire detection [11]	medium (100s) to large (1000s)	large (10s of km)	irregular, infrequent	unidirect.	medium, tolerable delay 15 sec	battery (non-rechargeable); possible energy harvesting	years
Earthquake detection [122]					high, tolerable delay 5 sec		
Tsunami detection [134]							
Landslide detection [101]							
Avalanche detection [129]							
Air pollution monitoring [59]			regular, 1 message every 15 min per device		medium, tolerable delay 15 sec		
Wildlife tracking [40]	medium (100s)				low, tolerable delay a few hours		

as communication can contain critical information about the patient's condition. Bursty traffic is likely to occur when an alarm is activated.

4.2.3 Demands on QoS. The demands on QoS are high, with immediate responses when an anomaly is detected.

4.2.4 Energy Source and Longevity. The devices are typically mains or battery powered with the possibility to recharge. Due to their easy accessibility, the communication and compact dimensions are superior to the battery longevity, making the short recharging cycles, e.g. every few days, acceptable. Nevertheless, extending the lifespan of battery-powered devices reduces the required maintenance and greatly improves convenience for a user.

4.3 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. The traffic characteristics of the most common services in the smart environment domain are summarised in Table 5.

4.3.1 Network Size and Coverage. The size of the network is typically from medium to large, which is caused by a large coverage area and an intentional redundancy that reduces measurement errors and increases the reliability of a detection system.

4.3.2 Traffic Characteristics. The traffic rate is usually irregular and infrequent to extend the battery life of the devices. Transceivers are known to be one of the biggest power-consumers [53], as such, unless a service is running in a multi-hop network, this component is usually kept in the OFF mode. Services informing about periodic changes have a regular traffic rate, but their sending interval is still very low for energy efficiency. The direction of the communication is typically unidirectional, devices gather the environmental data and send them to the sink node when some information is obtained. The one-way communication is preferred to maximise the lifespan of constrained devices with limited power sources. Traffic bursts are likely to occur for services with an irregular traffic rate that are configured to detect anomalies.

Table 6. Characteristics of Smart City

Service Name	Network Size	Network Coverage	Traffic Rate	Traffic Direction	Demands on QoS	Energy Source	Battery Longevity
Lightning control [25]	large (1000s)	large (10s of km)	irregular, infrequent	bidirect.	medium, tolerable delay 15 sec	mains	NA
Traffic management [39]			regular, 1 message every 30 sec per device; irregular for alarms		medium, tolerable delay 15 sec; high, for certain conditions; high, for alarms	mains / battery (non-rechargeable); possible energy harvesting	NA / years
Parking tracking [103]			irregular, frequent	unidirect.	medium, tolerable delay 10 sec		
Waste management [26]			irregular, infrequent		low, tolerable delay 1 min	battery (non-rechargeable)	NA
Urban conditions monitoring [95, 105]	medium (100s) to large (1000s)		regular, 1 message every 5 min per device; irregular for alarms		medium, tolerable delay 30 sec; high, for alarms	mains / battery (non-rechargeable); possible energy harvesting	NA / years
Public safety and surveillance [9, 143]	medium (100s) to large (1000s)		regular, frequent, irregular for alarms		medium, tolerable delay 3 sec; high, for alarms	mains / battery (non-rechargeable); possible energy harvesting	NA / years

4.3.3 Demands on QoS. The demands on QoS are high for alarm-based services, where systems need to be notified about anomalies immediately. Medium for less dynamic use cases, but can also be low, such as in the case of wildlife tracking, where the loss of connectivity can delay messages even for a few hours.

4.3.4 Energy Source and Longevity. The devices are usually battery-powered and non-rechargeable but can harvest energy to prolong their lifespan. The demands on longevity are high because of the difficult accessibility, thus devices are expected to operate for years.

4.4 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. A considerable proportion of the Smart City traffic is generated by devices in the public safety and surveillance area [9, 143]. This area is aimed at the safety of citizens, organisations, public spaces and facilities. The monitoring is usually achieved using static cameras (e.g., CCTV cameras) as well as mobile cameras (e.g., drones), however, other data sources such as social media feeds have also been included to improve the quality and information value of the data. The traffic characteristics of different services in the smart city domain are described in Table 6.

4.4.1 Network Size and Coverage. The network size is most commonly large, consisting of thousands of devices to cover an entire urban area characterised by its high density and plethora of obstacles.

4.4.2 Traffic Characteristics. The traffic rate varies in both, regularity and frequency. Services of the smart city domain are highly diverse and produce different traffic rates depending on how much an environment is changing and what data timeliness is required. The communication direction is unidirectional as well as bidirectional, some devices merely gather data, whereas others need to interact with users and other devices. Traffic bursts are likely to occur in services that expect user interaction, can detect anomalies and activate alarms, or the communication is automatically set to a specific time.

Table 7. Characteristics of Smart Energy

Service Name	Network Size	Network Coverage	Traffic Rate	Traffic Direction	Demands on QoS	Energy Source	Battery Longevity
Home energy management (HEMs) [142]	small (10s)	small (10s of m)	regular, 1 message every 1 min per device	bidirect.	high, tolerable delay 5 sec	mains	NA
Advanced metering infrastructure (AMI) [84]	medium (100s) to large (1000s)	medium (100s of m)	regular, 1 message every 1 hour per smart meter		medium, tolerable delay 15 sec		
Demand response management (DRM) [113]	large (1000s)	large (10s of km)	irregular, infrequent; 1 message per device per broadcast event		low, tolerable delay 1 min		
Wide area protection and control systems [125]			regular, 1 message every 10s to 100s of ms per device		high, tolerable delay 10s to 100s of ms		

4.4.3 Demands on QoS. The demands on QoS are usually medium; the smart city domain is not QoS-critical in general and some delay is acceptable. However, this mostly depends on the application. For example, traffic management could be logically considered as high-QoS. However, traffic management is composed of a variety of components including data gathering from multihop high mobility nodes that already involves certain delay [39]. In the case of congestion control (that we consider to be part of traffic management), a certain delay is tolerable before remediation (e.g., traffic light change) that is a result of the measurement – evaluation – alerting pipeline/workflow. Therefore, we assign traffic management a generalised medium-QoS label. Nevertheless, the alarms have to be received and detected near real-time, hence requiring high-QoS.

4.4.4 Energy Source and Longevity. The devices are either mains powered or battery-powered according to their location. For battery powered devices that are non-rechargeable, it is possible to harvest energy for the majority of services. The expected battery longevity is high, and devices are required to run for years to make the maintenance process sustainable.

4.5 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 yet 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. Table 7 summarises the traffic characteristics of typical services in the smart energy domain.

4.5.1 Network Size and Coverage. From a coverage area perspective, the domain can be divided into three groups:

- Small – commonly known as the home area network (HAN), usually consisting of tens of devices.
- Medium – also called the neighbourhood area network (NAN), typically a medium to large network.
- Large – referred to as the wide area network (WAN), covering thousands of devices.

4.5.2 Traffic Characteristics. The traffic rate is usually regular to ensure the timeliness of acquired data while the sending frequency is very diverse. For instance, smart meters sends aggregated data once per an hour, whereas wide area protection and control systems require data sampling intervals in tens to hundreds of milliseconds. This usage of 'sampling' is

Table 8. Characteristics of Smart Transport and Mobility

Service Name	Network Size	Network Coverage	Traffic Rate	Traffic Direction	Demands on QoS	Energy Source	Battery Longevity
Vehicle automation [44]	small (10s) to medium (100s)	medium (100s of m)	irregular, frequent	bidirect.	high, tolerable delay 100 ms	vehicle's battery	years
Vehicle localisation and monitoring [71]	large (1000s)	large (10s of km)	regular, 1 msg every 10 sec per vehicle	unidirect.	medium, tolerable delay 10 sec		
Quality of shipment conditions monitoring [19]	medium (100s)	small (10s of m)	regular, 1 msg every 5 min per device		medium, tolerable delay 15 sec	battery (rechargeable)	months to years
Dynamic traffic lights control [22]	large (1000s)	large (10s of km)	regular, 1 msg every 30 sec per device; irregular for alarms	bidirect.	high, tolerable delay 5 sec	mains	NA
Road condition monitoring [15]			irregular, infrequent		medium, tolerable delay 15 sec	battery (may be rechargeable)	days when rechargeable, years otherwise

distinct from 'sampling' meaning 1-in-every-n in the context of traditional computer network measurement. Monitoring methods in wide-area monitoring and grid monitoring rely on the high-sampling rate, for example dozens of samples in a second or millisecond [38]. In general, the number of samples per time unit affects the data quality, as the quality of the sample is likely to increase with the sampling frequency, with respect to reflecting temporal variation and fluctuations in the smart grid behaviour [2]. The communication is bidirectional for all services, as two-way communication is required to optimise the energy consumption and delivery. Traffic bursts are unlikely to occur when message exchange is configured to regular basis but is likely in services in which the communication is triggered by specific events such as DRM.

4.5.3 Demands on QoS. The demands on QoS differ based on the importance of sent information. While the services of HAN and NAN typically accept the delay in seconds up to minutes, WAN is QoS-critical, and therefore, latency is optimally kept at minimum.

4.5.4 Energy Source and Longevity. The devices are typically mains powered, which has a positive impact on the maintenance intervals. Nevertheless, energy-efficiency is still an important topic of this domain.

4.6 Smart Transport and Mobility

The rapid urbanisation in combination with the growing traffic congestion and globalisation of markets have created a high demand for managing transport and mobility in a smart way. The aim is to make transportation quicker, cheaper, and safer, which can be achieved by collecting all kinds of data for analysing and finding optimal solutions. The traffic characteristics of the individual services in the smart transport and mobility domain are shown in Table 8.

4.6.1 Network Size and Coverage. The network is typically large, which is achieved by the number of vehicles spread over a large area. Nonetheless, some services are based on short-range communication, e.g. vehicle automation or quality of shipment conditions monitoring, which require short/medium network coverage and consist of tens to hundreds of nodes.

4.6.2 Traffic Characteristics. The traffic rate is mainly characterised by the combination of regular and irregular communication while the frequency can be very high, especially in the case of vehicle automation service and decreases with less dynamic services that monitor the slowly changing environments, e.g. conditions in a truck trailer. The communication is

Table 9. Characteristics of Smart Manufacturing and Retail

Service Name	Network Size	Network Coverage	Traffic Rate	Traffic Direction	Demands on QoS	Energy Source	Battery Longevity
Mass customisation in production line [135]	medium (100s) to large (1000s)	small (10s of m) to medium (100s of m)	regular, frequency varies; irregular for alarms	bidirect.	high, tolerable delay in hundreds of ms	passive / mains / battery (non-rechargeable)	NA / months to years
Inventory and supply chain tracking [92]			regular, 1 message every 10 min per device		medium, tolerable delay 5 sec	passive / battery (non-rechargeable)	
Indoor localisation [30]			high; advertising interval in hundreds of ms per device	unidirect.	high, tolerable delay 500 ms		
Environment monitoring [137]	medium (100s)		regular, 1 message every 10 min per device; irregular for alarms		medium, tolerable delay 10 sec; high, for alarms	mains / battery (non-rechargeable)	
Maintenance and repair optimisation [70]							

bidirectional for services that require some kind of vehicle communication, while unidirectional for simple conditions monitoring of transported goods. Traffic bursts are likely to occur in services with the irregular traffic rate, for example in the inter-vehicular information exchange. On the other hand, it is unlikely in services with regular sending intervals and low probability of sudden anomaly occurrences.

4.6.3 Demands on QoS. The demands on QoS can be very high in vehicle automation applications and services, which requires less than 100 milliseconds response time. Other services can usually accept communication delay in seconds.

4.6.4 Energy Source and Longevity. The energy source can be vehicle's battery, mains power, but also a separate battery. The longevity of battery-powered devices is typically high, albeit some specific devices such as smartphones used for the road condition monitoring, can be recharged on a daily basis.

4.7 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. IoT can provide up-to-date information due to the massive deployment of cyber-physical systems (CPS).

CPS integrate computing elements with physical components and processes [68]. They can be seen as systems that consist of a 'physical entity' and its 'cyber-copy' connected. The 'cyber-copy' can replicate the behaviour of the physical machine, giving thus valuable insight on how the device would act in various situations. The connection between these two 'worlds' is usually established using sensors and actuators [112]. CPS can gain profound knowledge of the environment by connecting all distributed intelligence. This enables more accurate actions and tasks. CPS can be found in a wide variety of application domains, such as aerospace, process control, manufacturing, telecommunication, and power grid [68]. The proliferation of CPS gives rise to the next industrial revolution, often referred to as Industry 4.0. We refer the reader interested in this topic to [46, 68, 112].

Table 9 summarises the traffic characteristics of the smart manufacturing and retail domain.

4.7.1 Network Size and Coverage. The network size is typically medium to large, based on the type and size of a company. The network area is small to medium but can be very

Table 10. Characteristics of Smart Agriculture

Service Name	Network Size	Network Coverage	Traffic Rate	Traffic Direction	Demands on QoS	Energy Source	Battery Longevity
Irrigation [41]	small (10s) to medium (100s)	medium (100s of m) to large (10s of km)	regular, 1 message every 1 hour per device	bidirect.	low, tolerable delay 1 min	battery (non-rechargeable); possible energy harvesting	years
Fertilization [55]				unidirect.			
Pest control [98]							
Cattle monitoring [64]	medium (100s) to large (1000s)		regular, 1 message every 5 min per device			battery (non-rechargeable)	

challenging due to the harsh conditions arising from the presence of metallic objects that affect signal propagation, dangerous materials / substances, high temperature, etc.

4.7.2 Traffic Characteristics. The traffic rate is regular, information is gathered periodically to enable services being deterministic. The frequency varies from a near real-time communication up to the interval of one message every ten minutes, which is specified by the environment dynamics. The direction is typically bidirectional when devices need to be configurable and can be controlled by operators. Otherwise, the communication is unidirectional. Traffic bursts are likely to occur in services that expect anomaly detection.

4.7.3 Demands on QoS. The demands on QoS are medium to high while there is a correlation between the traffic rate and demands on QoS. The near real-time communication have very strict requirements on QoS, whereas services with high sending intervals are usually not demanding.

4.7.4 Energy Source and Longevity. The devices can be passive, mains or battery powered. The reliability is superior to the battery lifetime, albeit energy-efficient technologies can contribute to the longevity of devices, and therefore improve the overall performance. The battery-powered devices are expected to operate for months to years.

4.8 Smart Agriculture

Agriculture is an important sector, yet it faces challenges that cannot be ignored. The growth of the 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 through climate adaptation and mitigation. The concept of climate-smart agriculture was created in order to address the mentioned challenges and IoT plays a significant role in it. The traffic characteristics of the smart agriculture domain are summarised in Table 10.

4.8.1 Network Size and Coverage. The network size is usually medium to cover the entire field. The network coverage is medium to large but does not contain significant obstacles.

4.8.2 Traffic Characteristics. The traffic rate is typically regular, yet infrequent due to the slowly changing environmental conditions and high demands on devices' battery life. Unidirectional communication is suitable for most services as they utilise IoT devices for data collection. Services that are also responsible for actuators control, such as irrigation systems, require bidirectional communication. Traffic bursts are unlikely to occur, which is due to the regularity in the sending rates and no requirement for alarms.

4.8.3 Demands on QoS. The demands on QoS are low with a tolerable delay of up to a minute. Devices do not have to respond immediately if that leads to energy conservation.

4.8.4 Energy Source and Longevity. The devices are battery-powered and non-rechargeable, although static sensors can harvest energy when used outdoors. The energy-efficiency is critical in the smart agriculture domain and all aspects are modified according to it in order to make devices running for years.

5 SUMMARY OF OBSERVATIONS

In the previous section, we described 38 services from eight application domains as shown in Table 3 to Table 10. During the process, we encountered solutions that were addressing the same issue with slightly different configurations, depending on the specific implementation and authors' perception. Nevertheless, it is important to note that the fundamental aspects remained the same in all cases. In this Section, we discuss the current position and research directions of the surveyed application domains.

5.1 Smart Buildings and Living

The smart buildings and living domain is already well-established and lots of working applications can be found in residential as well as commercial buildings. The possibility to lower operating costs and improve the overall living comfort of a property, together with the omnipresent Wi-Fi, have motivated the widespread adoption of IoT solutions. Nevertheless, poor interoperability between devices from different manufacturers persists, which, as a result, reduces the positive effect of the gained benefits and slows down the implementation progress. To overcome this problem, vendors need to shift from proprietary solutions to more open standards-based approaches that will enable devices to mutually interact regardless of the technology used and will ensure the compatibility with standardised integration platforms.

5.2 Smart Healthcare

The current position of IoT in the healthcare is represented mainly by the variety of wearables and accessories that provide additional information for a user. These wearables are popular among young and active people, as well as tech fans. Nevertheless, the IoT solutions are slowly being developed also for more serious use cases such as disease monitoring and assisted living. The main challenge of developing applications for healthcare is the way to guarantee the quality and availability of the services while keeping devices simple, portable, and non-intrusive. Ideally, the monitored persons or patients would not have to carry/wear the devices, but the surrounding sensors will monitor them remotely.

5.3 Smart Environment

Smart environment applications, especially for rare event detection, are highly demanding because they can warn of the potential natural disasters. Therefore, both scientists and the industry actively research this area for several years now while countries, with a high probability of natural phenomena occurrence (e.g. earthquakes, volcano eruptions, etc.), already use various detection systems for protection. However, in order to proliferate these systems globally and to monitor less critical events, further research is required. A major issue is, for example, the battery life of low-cost devices that leads to a frequent replacement of these devices.

5.4 Smart City

The smart city is an emerging concept for the society that can not only improve the quality of life in a city but also reduce the operating costs of public services. Consequently, many countries have already started transforming their capitals and other big cities into smart cities by implementing various solutions like traffic management, urban conditions monitoring, lighting control, etc. The problem with the wider adoption of this concept is in its implementation price. The large-scale deployment of applications comes with a high price. Moreover, a city is not a green field and many systems are already developed. 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.

5.5 Smart Energy

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 will certainly take 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 a progress.

5.6 Smart Transport and Mobility

Transport and mobility represent an important part of today's interconnected world. As such, a significant effort is put into this domain and several of the more traditional services, such as vehicle localisation, and quality of shipment conditions monitoring, are already widely adapted. Yet other services, like vehicle automation, are absolutely revolutionary and present the state-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 such as the complexity of the domain, extremely dynamic conditions, and reliability requirements. Nevertheless, the current research is taking promising leaps.

5.7 Smart Manufacturing and Retail

Industry 4.0 is a concept that comprises the state-of-the-art in both hardware and software in order to create new possibilities and shift the automation in manufacturing to the next level. Innovative companies have already started implementing new services to enable flexible customisation, to reduce the production costs and to improve the output quality, although it is still far from the mass adoption. The major barriers are the high initial expenses and low interest of companies making fundamental changes. To keep up with today's leaders, constant change is inevitable.

5.8 Smart Agriculture

The adoption of the mentioned services is heavily influenced by the level of development of a particular country. The smart agriculture concept is an inevitable trend if we want to mitigate climate changes and produce food in a sustainable way. However, 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, the current progress in hardware availability and energy-efficiency of LPWANs improves the speed of agriculture digitalisation.

6 KEY CHARACTERISTICS OF IOT APPLICATIONS

We compare the IoT application domains among one another based on their traffic characteristics and in doing so, we introduce three charts. As shown in Section 4, the services within one application domain may differ in some cases, so in order to make a comparison at the domain level, some generalisation is inevitable. As such, we aggregated the values into more general definitions, which are now represented by the circles in the charts. To make the charts more consistent and transparent, the largest outliers (services that are too distinct from the majority) are depicted using lines of the same colour. This generalisation was purely based on the presented traffic characteristics while the main aim was to reduce the potential ambiguity.

6.1 Network Size and Coverage Area

Figure 2 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 geographical 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 phenomenon 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 Figure 2, 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 Figure 3, would only be partially true.

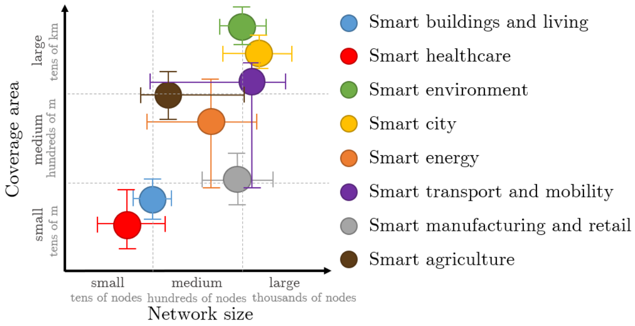

Fig. 2. Relationship between network size and coverage area.

6.2 Traffic Rate and Demands on QoS

A relationship between traffic rate and demands on QoS is illustrated in Figure 3. 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 Figure 3, the correlation is significant. In most cases, higher traffic rate means 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, a system should immediately trigger an alert. Furthermore, we would like to highlight the differences between Figure 2 and Figure 3. While the smart healthcare domain could be considered to be the least demanding in Figure 2, this relationship shifts it to the opposite corner in Figure 3. 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.

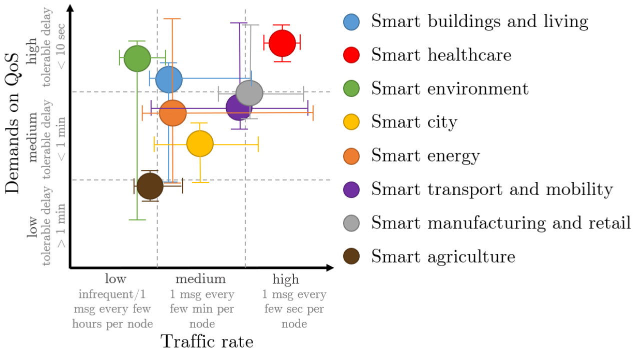

Fig. 3. Relationship between traffic rate and demands on QoS.

6.3 Sustainable Energy and Demands on the Longevity of Devices

The correlation depicted in Figure 4 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 envisage passive RFID tags or mains-powered devices where the power source is reliable. 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 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 Figure 4, 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 develop IoT services that are accessible anytime and from anywhere. Although we can accept the lower longevity when the devices can be recharged, such as in the case of smart healthcare, the majority of use cases utilise devices that are complicated to access physically, thus making the recharging process inefficient. Consequently, IoT solutions need to deal with energy wisely, e.g., they should harvest energy whenever possible or implement energy-efficient methods to achieve the desired battery life. The expectations are very high as the longevity of devices is one of the significant deal-breakers when thinking of proliferating IoT applications globally.

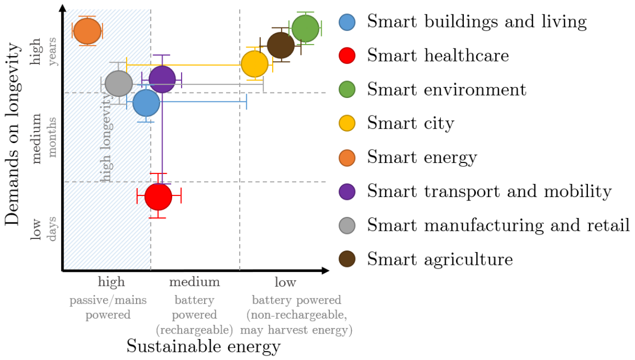

Fig. 4. Relationship between sustainable energy and demands on longevity.

7 IOT TRAFFIC MEASUREMENT CHALLENGES

In legacy or packet-switched networks, the traffic usually refers to all kinds of transmitted information (e.g data, audio, video, control messages, etc.) during a given time period, but in some cases, it may be limited to certain transfers, messages, records or a selected group of communicating devices. IoT network traffic is highly heterogeneous while simpler in composition (it typically does not carry video and audio). The diversity of IoT traffic is given by the fact that IoT networks are deployed using different enabling technologies and for diverse purposes [6, 75].

Challenges arise when this heterogenous IoT traffic enters legacy networks (given the IoT paradigm) and combines with the legacy traffic. The primary function of network components (e.g. switches, routers, firewalls, etc.) is the fast and smooth delivery of information. In current networks, this means a massive data volume [32]. While these devices are designed to handle large data volumes, a factor that often leads to challenges is traffic measurement which is required for network monitoring related tasks such as traffic engineering, classification, and anomaly detection [72]. Traffic measurement is often performed in the network devices while the generated measurement data are usually carried over the same network where the legacy traffic is forwarded [57].

On one hand, when IoT data are carried over legacy networks, the overall traffic complexity significantly increases that can have an adverse effect on the network operation, performance and management. For example, the generation of measurement data alone can already negatively impact the CPU performance of the networking devices [31]. Forwarding the measurement data from the measurement point(s) to the monitoring system(s) can further adversely affect the performance of the network components that can subsequently lead to latency or even packet loss [31, 93, 94]. Moreover, given the increased traffic heterogeneity, making an operational sense out of the data for traffic classification is becoming a challenge as the processing required for online and offline analysis often lacks the resources to handle the complex traffic in a timely, reliable, and efficient manner [36, 138].

On the other hand, given the small size of IoT traffic (the data are usually transferred in a single data unit) yet bursty nature (result of the event-driven paradigm), from a legacy network perspective, it can exhibit similar characteristics as the traffic related to anomalous activities (e.g. DDoS attack, worm spreading, etc.). This has already been shown to have an adverse impact on the network performance [90, 107].

To ensure the reliability, quality, and sustainability of the networks, it is essential to observe and manage IoT traffic. However, its composition and behaviour (i.e. the characteristics it exhibits) have not been investigated, mainly due to two key reasons:

IoT traffic lacks proper characterisation schemes: Over the years, various schemes have been proposed for legacy network traffic characterisation. The most commonly used schemes are based on flow duration, size, rate, and burstiness [23, 28, 65]. It has been shown that the identification of flow types using these classification schemes is highly efficient in network performance managerial tasks including load-balancing, congestion control and QoS provisioning [18, 24, 35, 62]. However, the application of these schemes to IoT is not obvious. As the transferred information is small, it is often carried in a single information unit and thus, no data segmentation is required. In consequence, the flows consist of one (or few) packet(s) and thus, duration and size cannot be estimated in a classical manner. As such, IoT flows are typically short-lived (exist for a short duration) and small-sized. The most significant difference in IoT traffic is caused by the transmission rates (due to the various capabilities of enabling network technologies) and the likelihood of burstiness including its duration.

IoT measurement instrumentation is not mature enough: The instrumentation for measurement is not matured enough which consequently gives rise to concerns regarding resource consumption. Various standards compliant protocols exist for network monitoring. The most commonly used protocols are *flow-level information* (Netflow/IPFIX [4, 33]) and *sampled flow* (sFlow [91]). As flow export became widely recognised and accepted, these protocols were being deployed in the mainstream network product lines and used for network telemetry and traffic reporting. These protocols, however, have a major drawback when applied in IoT, namely, they have not been designed with resource utilisation efficacy mind. IoT components are often deployed in remote areas or away from fixed infrastructures and depend on mobile energy sources like batteries. As such, the energy efficient operation of IoT devices is crucial. In general, the communication has a higher cost than computation cycles on an average sensor node. For example, according to Zúniga et al. [144] the energy cost for transmitting one bit is higher than processing 100 instructions on a Berkeley sensor node. That being said, traditional computer network measurement approaches are not suitable for the use in IoT environments. In November 2017, the IETF published its specification of TinyIPFIX [108], a protocol that is adapted to the needs of constrained networks. TinyIPFIX does not require a steady network connection. Instead, it utilises a push-based mechanism where data are transmitted autonomically from the meters to one or more collectors [108]. The specification claims that as metering probes are only part of the IoT network as needed when there is data to be exported, they are suitable for reporting metering data in constrained networks.

There is also an ongoing debate regarding the incorporation of software-defined networking (SDN) in IoT and the benefits it could bring, including network measurement and management [124]. In the SDN paradigm, the control plane is decoupled from the forwarding plane via moving the control logic to a centralised device – the controller [89]. This way, the network devices become simple forwarders that are programmable through a standardised protocol such as OpenFlow [126]. However, there are several challenges with incorporating this paradigm in IoT. Firstly, control traffic consumes bandwidth that degrades the spectral efficiency of the IoT devices [124]. Control traffic can also have a significant impact on the battery. Moreover, the collection of per-flow statistics may also potentially overload the controller [54]. The main OpenFlow flow statistics elements are counters, precisely duration, packet count, and byte count [126]. The representative character of these flow statistics is also a challenge. The diversity of information obtained using OpenFlow-based flow statistics is significantly lower than when using IPFIX. It has been suggested that OpenFlow should be considered a flow-based configuration technology for packet forwarding devices, instead of a flow measurement technology [57]. Although the integration of IoT with SDN, programmability, and centralised control are highly anticipated, there is still a road ahead, and future work is required for achieving a new area in IoT network management based on SDN.

8 FUTURE RESEARCH PROSPECTS IN IOT TRAFFIC CHARACTERISATION

Interoperability and compatibility between various enabling technologies is a common issue. There is a number of different enabling network technologies that make up the IoT ecosystem [6, 75]. In order to interoperate, an efficient communication must be established between them. Efficient communication requires an underlying connectivity infrastructure that facilitates the exchange of information between the participants. Existing network models (the Internet Model and the OSI Model) do not satisfy all IoT connectivity requirements. IoT systems require a model that addresses a variety of aspects including the sensors, devices, and controllers.

To address this challenge, the Industrial Internet Consortium (IIC) has recently proposed an Industrial IoT (IIoT) connectivity stack model [58] that is based on the Internet and OSI models. At each layer, it defines the core functions and a number of considerations. One of the key architectural qualities of this connectivity stack model is network monitoring and analysis. This is a promising step-forward as the instrumentation for network monitoring and its adaptation have been a constant challenge for many years. As the significance of network monitoring has been recognised in network management, its deployment started to attract more attention. Today, it is an integral part of networks. However, previously it was only an afterthought. In consequence, it often required changes in the network infrastructure and adaptations in its instrumentation.

IoT network and traffic management systems (IoTNTMS) do not provide sufficient and accurate information (both, traffic and telemetry) to enable granular and timely monitoring and management of the network. A modern IoTNTMS in a smart environment should go through different phases, from information gathering (e.g., traffic parameters such as traffic volume, bandwidth, etc.), through data processing, and exploitation (i.e., extract useful information from the massive measurement data) to service delivery (deliver knowledge to the operators and users). All these phases increase the service delivery time (e.g., congestion alert, short-term traffic prediction, link and device failure) by a few seconds. Moreover, the gathered traffic data usually needs to also undergo filtering to improve its quality and eliminate the noise. Providing QoS guarantees is challenging in such conditions. The lack of an end-to-end protocol for establishing QoS, the complexity of network dynamics and traffic heterogeneity, and the difference of QoS requirements to be achieved (application-dependent QoS requirement) all contribute to this situation. The development of new IoT connectivity stack models with monitoring in mind is expected to lead to improvements in IoT network and traffic measurement and characterisation.

Traffic measurement results in the generation and transfer of data that inevitably brings an increase in energy consumption. This increase is highly undesired and avoided in resource-constrained environments like IoT. While the effects of measurements in IoT remain poorly analysed, concerns regarding energy consumption persist. Furthermore, the large number of IoT network technologies makes the deployment of metering approaches challenging. As mentioned above, from a practical viewpoint, IoT components are built in different ways. It is often unclear what combination best suits the social and economic needs. As a result, the network is becoming more complex, where an additional function such as metering has little to no space left.

Despite the benefits and well-described specification, the widespread deployment of TinyIPFIX and similar techniques in IoT is slow, and likewise, publications reporting on the experience with this protocol are lacking. Therefore, the investigation of the effects of measurement in IoT still requires considerable work. We expect research will continue to focus on the investigation of IoT network traffic including measurement techniques and standardisation. Furthermore, we also expect the proliferation of high-level standards that can ensure interoperability across hardware and software vendors.

9 GENERAL TRENDS, ISSUES, AND DIRECTIONS

IoT has gone through a rapid proliferation. Despite the attention this sector receives in recent years, the way IoT evolves opens several concerns. The primary challenge of IoT is complexity. Today, there is a diverse number of competing components, trends, and technologies that make IoT solutions challenging to implement and manage. Manufacturers often deliver their product with profit as key motivation while they tend to overlook the complexity caused by the introduction of new, proprietary products and technologies. Moreover, the design and delivery of new technologies are performed in an unregulated fashion. In consequence, the shipped products often contain severe security vulnerabilities at various layers and lack proper interoperability while the complexity of the entire IoT ecosystem is further increased.

9.1 Security

Security has also been a severe concern of IoT for a long time [50, 114, 140]. Traditional security is hard to implement in the IoT ecosystem. This is mainly because of two reasons. Firstly, the mechanisms that are associated with security incur a significant overhead to the network and its components. Many IoT devices work in constrained environments with limited battery-power, computing resources, and storage capacity. These devices are not suited for the increased overhead that is associated with encryption, authorisation, and authentication. Secondly, the interoperability between various devices, components, and network technologies at different layers of the network protocol stack is limited. This is mainly due to the absence of a unified, globally accepted 'language' that could be used for negotiating communication and security requirements by the IoT components.

Recognising this limitation, IETF have developed the Manufacturer Usage Description (MUD) Specification [67]. Via MUD, manufacturers can disclose the type and purpose of their devices, and what network policies they need for the devices to operate properly, including the necessary security [51]. The policies can be understood as whitelist statements built upon the standard YANG [20] model that can be used by the customers to deploy access policies in their networks without any ambiguity. While MUD is an important step forward in streamlining the behaviour of IoT devices, it still has its limitations [116]. For example, the YANG model is not evolved enough to provide an appropriate means for control. Also, creating a MUD policy might be a challenge if the behaviour depends on the operational environment.

IoT security still requires considerable work. Security breaches can happen at any level including the IoT devices, gateways, software, communication protocols, firmware, and the cloud. Remedial measures aimed at addressing the breaches are often taken only after security vulnerabilities are discovered. However, reactive approaches to security has been known to be an insufficient measure for a long time. The future IoT calls for smarter, proactive measures.

9.2 Privacy

Besides security, privacy has also become a critical concern of IoT [50, 114, 140]. There is a significant number of IoT applications which cary user-specific, sensitive information. Such data require careful handling and appropriate privacy measures. The data that are collected from the user and their devices/applications must therefore resist profiling, localisation, and tracking. This, however, often goes opposite business interests. Collecting information related to certain individuals via profiling is, for instance, a common technique in e-commerce to gain profit via targeted advertising. Therefore, there is a constant need for services that are aimed at delivering user-sensitive information. On the other hand, certain measurement and data analysis is required to maintain and improve the quality of various services. Balancing between these two interest is challenging.

Like security, IoT privacy also requires a framework that ensures the secure, confidential exchange of data between the individual IoT components while providing anonymity for both sides of the communication. It logically follows that the development of such frameworks comes hand-in-hand. Privacy concerns cannot be addressed without proper network/device security functions, and vice versa. As such, building a comprehensive IoT Security and Privacy framework must have high priority.

9.3 Decentralised IoT

The current IoT ecosystem is based on a centralised paradigm. In this paradigm, all devices are connected through the cloud, usually via a controller. The advantage of this design is the relatively simple setup and management of the network and its devices. However, this architecture also comes with a drawback. The centralised connection and management of devices come with increased resource utilisation and cost. The former is given by the fact that the traffic between the devices goes through the internet, even if they are located only a few meters apart. The latter comes from the infrastructure and maintenance costs associated with the cloud hosts (servers) and the network infrastructure. A recent study by Verma et al. [132] claims that centralised IoT approaches will eventually face performance challenges due to the rapid growth in the number of IoT devices, connected users, services as well as the generated traffic volume.

Edge Computing: An approach aimed at addressing this challenge is the decentralised architecture [82], also often referred to as *fog computing* [131]. In this architecture, the logic is moved from the cloud to the network edge where forwarding is performed by gateways and intermediate devices. Compared to the centralised approach, the advantage of decentralisation materialises in the low amount of transmitted data through the internet. This consequently leads to the reduction of transmission delay (smaller bandwidth) as well as resource utilisation (lower power consumption). Moreover, the edge devices (gateways) can also be involved in the collection of data for various network-related managerial activities. This can consequently open new opportunities in network measurement and security.

However, the decentralised IoT paradigm also comes with challenges. The data that are processed at an intermediate level are usually not forwarded to the central controller. As such, the controller 'losses' certain visibility over the network and its devices. What data should be processed at the edge and what should be forwarded to the controller is far from being clear, primarily due to the heterogeneity of the connected devices, their communication needs, and the QoS requirements of the applications. Therefore, the specification of configuration settings to make a system adequately adaptable requires further research.

Blockchain: Another approach to the decentralised IoT paradigm is via adopting a peer-to-peer (P2P) communication standard. While this architecture can also lead to the benefits mentioned above, P2P communication has many flaws, chief among which is security. Security limitations of P2P allow IoT devices to be compromised easily and expose applications/users to dangers. Blockchain is a popular solution to P2P communication security challenges [63, 141]. In the simplest terms, blockchain is a decentralised, distributed ledger (public or private) of different kinds of transactions. This ledger is shared among the nodes of a P2P network instead of being stored on a central server. Since the transactions are verified and confirmed by other nodes, there is no need for a central authority. Each transaction that is added to the ledger is secured with a digital signature (encryption) that proves its authenticity. Once data are stored, they cannot be altered without the consensus of the network (each node).

While the concept of blockchain can be applied to IoT with benefits that include security, transparency, and decentralisation, merging these two paradigms also faces some challenges [139]. The blockchain technology is, for example, well known for scalability issues that arise with the growth of the network and the number of transactions. Power consumption is also a point of concern. Encryption and verification of transactions are demanding processes and require considerable resources. The majority of IoT devices, unfortunately, lack suitable resources. Moreover, storage is also a challenge as redundantly storing the ledgers requires considerable capacity.

Nonetheless, decentralisation (either via edge computing or blockchain) is very promising and is expected to have a decisive role in the future of IoT. However, a road is still ahead. Future research is required in this area to address the complexities of IoT.

9.4 Future Directions

Finally, based on current tends and related challenges discussed above, we briefly outline several directions future IoT solutions are expected to be targeted at:

- *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.
- *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.

- *Coverage* – extended coverage is needed both in indoor spaces and wide outdoor areas [66]. A combination of both multi-hop 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 critical requirement, much more than the best-effort service model that original Internet was designed for.
- *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.

With no doubts, IoT involves massive volume of data. However, the continuous exchange of these data puts a significant strain on the network and the devices. Fortunately, with the implementation of 5G networks, things are expected to be improved. Compared to previous solutions, 5G has the following benefits: (i) more bandwidth, (ii) higher reliability, (iii) lower latency, and (iv) better capability to support a greater density of connected devices [5]. 5G will therefore also play a vital role in the future of IoT. It can open new opportunities in every of its aspects.

10 CONCLUSION

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.

In this paper, we reviewed the IoT applications from the traffic characteristics perspective. The main contributions of this work come from the defined traffic characteristics of IoT application domains, which provide an overview of demands on network technologies. Every IoT domain is demanding from a 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.

Despite the limitations and challenges, IoT network traffic is rapidly increasing in volume and heterogeneity [32]. As this traffic is usually carried through legacy networks where they are combined with other traffic types, the amplified effect can have a critical impact on the network operation. We stress that the measurement and characterisation of IoT traffic can be of high significance for future innovation.

ACKNOWLEDGMENTS

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 (VUW), New

Zealand. Adrian Pekar and Winston K.G. Seah are supported in part by VUW's Huawei NZ Research Programme, Software-Defined Green Internet of Things (project #E2881). The work of Jozef Mocnej and Iveta Zolotova is partly supported by the VEGA - 1/0663/17 2017-2020 grant, provided by the Scientific Grant Agency of The Ministry of Education, Science, Research and Sport of the Slovak Republic, and the Slovak Academy of Sciences.

REFERENCES

[1] [n.d.]. ZigBee Overview - Website. http://www.zigbee.org/zigbee-for-developers/zigbee/ Accessed: 28/10/2016.

[2] R. Abo and A. Even. 2017. Sampling density and frequency as data quality determinants in smart grids. In *2017 Smart City Symposium Prague (SCSP)*. 1–6. https://doi.org/10.1109/SCSP.2017.7973349

[3] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani. 2016. Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. *IEEE Wireless Communications* 23, 5 (October 2016), 10–16.

[4] Paul Aitken, Benoit Claise, and Brian Trammell. 2013. Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information. RFC 7011. https://doi.org/10.17487/RFC7011

[5] Ian F. Akyildiz, Shuai Nie, Shih-Chun Lin, and Manoj Chandrasekaran. 2016. 5G roadmap: 10 key enabling technologies. *Computer Networks* 106 (2016), 17 – 48. https://doi.org/10.1016/j.comnet.2016.06.010

[6] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials* 17, 4 (2015), 2347–2376.

[7] LoRa Alliance. 2015. A technical overview of LoRa and LoRaWAN. *White Paper, November* (2015).

[8] Wi-Fi Alliance. 2016. Wi-Fi HaLow. https://www.wi-fi.org/discover-wi-fi/wi-fi-halow Accessed: 16/12/2016.

[9] S. H. Alsamhi, O. Ma, M. S. Ansari, and F. A. Almalki. 2019. Survey on Collaborative Smart Drones and Internet of Things for Improving Smartness of Smart Cities. *IEEE Access* 7 (2019), 128125–128152. https://doi.org/10.1109/ACCESS.2019.2934998

[10] Pedro Amaro, Rui Cortesão, Jorge Landeck, and Paulo Santos. 2011. 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, 1–6.

[11] Yunus Emre Aslan, Ibrahim Korpeoglu, and Özgür Ulusoy. 2012. A framework for use of wireless sensor networks in forest fire detection and monitoring. *Computers, Environment and Urban Systems* 36, 6 (2012), 614–625.

[12] Luigi Atzori, Antonio Iera, and Giacomo Morabito. 2010. The internet of things: A survey. *Computer networks* 54, 15 (2010), 2787–2805.

[13] Debasis Bandyopadhyay and Jaydip Sen. 2011. Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications* 58, 1 (2011), 49–69.

[14] Paolo Baronti, Prashant Pillai, Vince WC Chook, Stefano Chessa, Alberto Gotta, and Y Fun Hu. 2007. Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards. *Computer communications* 30, 7 (2007), 1655–1695.

[15] Sultan Basudan, Xiaodong Lin, and Karthik Sankaranarayanan. 2017. A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing. *IEEE Internet of Things Journal* 4, 3 (2017), 772–782.

[16] Jordi Mongay Batalla, Athanasios Vasilakos, and Mariusz Gajewski. 2017. Secure Smart Homes: Opportunities and Challenges. *ACM Comput. Surv.* 50, 5, Article 75 (Sept. 2017), 32 pages. https://doi.org/10.1145/3122816

[17] Radoslaw Belka. 2019. An indoor tracking system and pattern recognition algorithms as key components of IoT-based entertainment industry. In *Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2019*, Ryszard S. Romaniuk and Maciej Linczuk (Eds.), Vol. 11176. International Society for Optics and Photonics, SPIE, 1694 – 1703. https://doi.org/10.1117/12.2536728

[18] C. Bi, X. Luo, T. Ye, and Y. Jin. 2013. On precision and scalability of elephant flow detection in data center with SDN. In *Proceedings of the IEEE Globecom Workshops (GC Wkshps)*. Atlanta, GA, USA, 1227–1232. https://doi.org/10.1109/GLOCOMW.2013.6825161

[19] Dennis JA Bijwaard, Wouter AP van Kleunen, Paul JM Havinga, Leon Kleiboer, and Mark JJ Bijl. 2011. Industry: Using dynamic WSNs in smart logistics for fruits and pharmacy. In *Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems*. ACM, Seattle, WA, USA, 218–231.

[20] Martin Bjorklund. 2016. The YANG 1.1 Data Modeling Language. RFC 7950. https://doi.org/10.17487/RFC7950

[21] Alessio Botta, Walter de Donato, Valerio Persico, and Antonio Pescapé. 2016. Integration of Cloud computing and Internet of Things: A survey. *Future Generation Computer Systems* 56 (2016), 684 – 700.

[22] Yesnier Bravo, Javier Ferrer, Gabriel Luque, and Enrique Alba. 2016. 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, 147–156.

[23] A. Callado, C. Kamienski, G. Szabo, B. P. Gero, J. Kelner, S. Fernandes, and D. Sadok. 2009. A Survey on Internet Traffic Identification. *IEEE Communications Surveys Tutorials* 11, 3 (rd 2009), 37–52. https://doi.org/10.1109/SURV.2009.090304

[24] F. Carpio, A. Engelmann, and A. Jukan. 2016. DiffFlow: Differentiating Short and Long Flows for Load Balancing in Data Center Networks. In *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*. Washington, DC, USA, 1–6. https://doi.org/10.1109/GLOCOM.2016.7841733

[25] Miguel Castro, Antonio J Jara, and Antonio FG Skarmeta. 2013. Smart lighting solutions for smart cities. In *Proceedings of the 27th International Conference on Advanced Information Networking and Applications workshops (WAINA)*. Barcelona, Spain, 1374–1379.

[26] Vincenzo Catania and Daniela Ventura. 2014. 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, 24–31.

[27] Luca Catarinucci, Danilo De Donno, Luca Mainetti, Luca Palano, Luigi Patrono, Maria Laura Stefanizzi, and Luciano Tarricone. 2015. An IoT-aware architecture for smart healthcare systems. *IEEE Internet of Things Journal* 2, 6 (2015), 515–526.

[28] Kun chan Lan and John Heidemann. 2006. A measurement study of correlations of Internet flow characteristics. *Computer Networks* 50, 1 (2006), 46 – 62. https://doi.org/10.1016/j.comnet.2005.02.008

[29] K. H. Chang. 2014. Bluetooth: a viable solution for IoT? [Industry Perspectives]. *IEEE Wireless Communications* 21, 6 (December 2014), 6–7.

[30] Zhikui Chen, Feng Xia, Tao Huang, Fanyu Bu, and Haozhe Wang. 2013. A localization method for the Internet of Things. *The Journal of Supercomputing* 63, 3 (2013), 657–674.

[31] Cisco and/or its affiliates. 2005. *White paper: NetFlow Performance Analysis*. Technical White Paper. Cisco Systems, Inc.

[32] Cisco and/or its affiliates. 2019. Complete Visual Networking Index (VNI) Forecast. https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html

[33] Benoit Claise. 2004. Cisco Systems NetFlow Services Export Version 9. RFC 3954. https://doi.org/10.17487/RFC3954

[34] M Collotta and G Pau. 2015. Bluetooth for internet of things: A fuzzy approach to improve power management in smart homes. *Computers & Electrical Engineering* 44 (2015), 137–152.

[35] A. R. Curtis, W. Kim, and P. Yalagandula. 2011. Mahout: Low-overhead datacenter traffic management using end-host-based elephant detection. In *Proceedings of the IEEE Infocom*. Shanghai, China, 1629–1637. https://doi.org/10.1109/INFCOM.2011.5934956

[36] Alberto Dainotti, Antonio Pescape, and Kimberly Claffy. 2012. Issues and Future Directions in Traffic Classification. *Netwrk. Mag. of Global Internetwkg.* 26, 1 (Jan. 2012), 35–40. https://doi.org/10.1109/MNET.2012.6135854

[37] I. Demirkol, F. Alagoz, H. Delic, and C. Ersoy. 2006. Wireless sensor networks for intrusion detection: packet traffic modeling. *IEEE Communications Letters* 10, 1 (Jan 2006), 22–24.

[38] X. Deng, D. Bian, D. Shi, W. Yao, Z. Jiang, and Y. Liu. 2019. Line Outage Detection and Localization via Synchrophasor Measurement. In *2019 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia)*. 3373–3378. https://doi.org/10.1109/ISGT-Asia.2019.8881142

[39] Soufiene Djahel, Ronan Doolan, Gabriel-Miro Muntean, and John Murphy. 2015. A communications-oriented perspective on traffic management systems for smart cities: challenges and innovative approaches. *IEEE Communications Surveys & Tutorials* 17, 1 (2015), 125–151.

[40] Vladimir Dyo, Stephen A Ellwood, David W Macdonald, Andrew Markham, Niki Trigoni, Ricklef Wohlers, Cecilia Mascolo, Bence Pásztor, Salvatore Scellato, and Kharsim Yousef. 2012. WILDSENSING: design and deployment of a sustainable sensor network for wildlife monitoring. *ACM Transactions on Sensor Networks (TOSN)* 8, 4 (2012), 29.

[41] Joshua Elliott, Delphine Deryng, Christoph Müller, Katja Frieler, Markus Konzmann, Dieter Gerten, Michael Glotter, Martina Flörke, Yoshihide Wada, Neil Best, et al. 2014. Constraints and potentials of future irrigation water availability on agricultural production under climate change. *Proceedings of the National Academy of Sciences* 111, 9 (2014), 3239–3244.

[42] Shahin Farahani. 2011. *ZigBee wireless networks and transceivers.* newnes.

[43] Behrang Fouladi and Sahand Ghanoun. 2013. Security evaluation of the Z-Wave wireless protocol. *Black hat USA* 24 (2013).

[44] Mario Gerla, Eun-Kyu Lee, Giovanni Pau, and Uichin Lee. 2014. 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, 241–246.

[45] K Gram-Hanssen and SJ Darby. 2017. "Home is where the smart is" ? Evaluating smart home research and approaches against the concept of home. *Energy Research and Social Science* 37 (2017), 94–101.

[46] Christopher Greer, Martin Burns, David Wollman, and Edward Griffor. 2019. *Cyber-Physical Systems and Internet of Things.* Technical Report NIST.SP.1900-202.

[47] Object Management Group. 2015. Data Distribution Service (DDS) Version 1.4. https://www.omg.org/spec/DDS/1.4/PDF

[48] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems* 29, 7 (2013), 1645–1660.

[49] Joseph Hall, Benjamin Ramsey, Mason Rice, and Timothy Lacey. 2016. 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.

[50] Sufian Hameed, Faraz Idris Khan, and Bilal Hameed. 2019. Understanding security requirements and challenges in Internet of Things (IoT): A review. *Journal of Computer Networks and Communications* 2019 (2019). https://doi.org/10.1155/2019/9629381

[51] Ayyoob Hamza, Dinesha Ranathunga, Hassan Habibi Gharakheili, Matthew Roughan, and Vijay Sivaraman. 2018. Clear as MUD: Generating, Validating and Applying IoT Behavioral Profiles. In *Proceedings of the 2018 Workshop on IoT Security and Privacy* (Budapest, Hungary) *(IoT S&P '18)*. Association for Computing Machinery, New York, NY, USA, 8–14. https://doi.org/10.1145/3229565.3229566

[52] S. N. Han, G. M. Lee, and N. Crespi. 2014. Semantic Context-Aware Service Composition for Building Automation System. *IEEE Transactions on Industrial Informatics* 10, 1 (Feb 2014), 752–761.

[53] DC Harrison, D Burmester, Winston K. G. Seah, and R Rayudu. 2016. Busting myths of energy models for wireless sensor networks. *Electronics Letters* 52, 16 (2016), 1412–1414.

[54] M. Hayes, B. Ng, A. Pekar, and W. K. G. Seah. 2018. Scalable Architecture for SDN Traffic Classification. *IEEE Systems Journal* (2018), 1–12. https://doi.org/10.1109/JSYST.2017.2690259

[55] Jianlei He, Jianlun Wang, Dongxian He, Jinyong Dong, and Yongbin Wang. 2011. The design and implementation of an integrated optimal fertilization decision support system. *Mathematical and Computer Modelling* 54, 3 (2011), 1167–1174.

[56] Shivayogi Hiremath, Geng Yang, and Kunal Mankodiya. 2014. 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)*. 304–307.

[57] R. Hofstede, P. Čeleda, B. Trammell, I. Drago, R. Sadre, A. Sperotto, and A. Pras. 2014. Flow Monitoring Explained: From Packet Capture to Data Analysis With NetFlow and IPFIX. *IEEE Communications Surveys Tutorials* 16, 4 (Fourthquarter 2014), 2037–2064. https://doi.org/10.1109/COMST.2014.2321898

[58] Rajive Joshi, Paul Didier, Jaime Jimenez, and Timothy Carey. 2018. *The Industrial Internet of Things Volume G5: Connectivity Framework.* Technical Report IIC:PUB:G5:V1.01:PB:20180228. Industrial Internet Consortium. https://www.iiconsortium.org/IICF.htm

[59] Abdullah Kadri, Elias Yaacoub, Mohammed Mushtaha, and Adnan Abu-Dayya. 2013. 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, 1–5.

[60] Juris Klonovs, Mohammad A Haque, Volker Krueger, Kamal Nasrollahi, Karen Andersen-Ranberg, Thomas B Moeslund, and Erika G Spaich. 2016. *Distributed computing and monitoring technologies for older patients*. Springer.

[61] Evdokimos I Konstantinidis, Panagiotis E Antoniou, Giorgos Bamparopoulos, and Panagiotis D Bamidis. 2015. A lightweight framework for transparent cross platform communication of controller data in ambient assisted living environments. *Information Sciences* 300 (2015), 124–139.

[62] Martin Kriska, Jozef Janitor, and Peter Fecilak. 2014. Dynamic routing of IP traffic based on QoS parameters. *International Journal of Computer Networks & Communications* 6, 4 (2014), 11.

[63] N. Kshetri. 2017. Can Blockchain Strengthen the Internet of Things? *IT Professional* 19, 4 (2017), 68–72. https://doi.org/10.1109/MITP.2017.3051335

[64] Kae Hsiang Kwong, Tsung-Ta Wu, Hock Guan Goh, Konstantinos Sasloglou, Bruce Stephen, Ian Glover, Chong Shen, Wencai Du, Craig Michie, and Ivan Andonovic. 2012. Practical considerations for wireless sensor networks in cattle monitoring applications. *Computers and Electronics in Agriculture* 81 (2012), 33–44.

[65] Kun-Chan Lan and John Heidemann. 2003. *On the correlation of Internet flow characteristics*. Technical Report ISI-TR-574. USC/Information Sciences Institute. https://www.isi.edu/~johnh/PAPERS/Lan03c.pdf

[66] S. Landström, J. Bergstróm, E. Westerberg, and D. Hammarwall. 2016. NB-IoT: A sustainable technology for connecting billions of devices. *Ericsson Technology Review* 93 (2016). Issue 3.

[67] Eliot Lear, Ralph Droms, and Dan Romascanu. 2019. Manufacturer Usage Description Specification. RFC 8520. https://doi.org/10.17487/RFC8520

[68] Jay Lee, Behrad Bagheri, and Hung-An Kao. 2015. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters* 3 (2015), 18 – 23. https://doi.org/10.1016/j.mfglet.2014.12.001

[69] Jay Lee, Hung-An Kao, and Shanhu Yang. 2014. Service innovation and smart analytics for industry 4.0 and big data environment. *Procedia Cirp* 16 (2014), 3–8.

[70] Jay Lee, Edzel Lapira, Behrad Bagheri, and Hung-an Kao. 2013. Recent advances and trends in predictive manufacturing systems in big data environment. *Manufacturing Letters* 1, 1 (2013), 38–41.

[71] SeokJu Lee, Girma Tewolde, and Jaerock Kwon. 2014. 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, 353–358.

[72] Bingdong Li, Jeff Springer, George Bebis, and Mehmet Hadi Gunes. 2013. A survey of network flow applications. *Journal of Network and Computer Applications* 36, 2 (2013), 567 – 581. https://doi.org/10.1016/j.jnca.2012.12.020

[73] L. Li, H. Xiaoguang, C. Ke, and H. Ketai. 2011. 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, 789–793.

[74] Shancang Li, Li Da Xu, and Shanshan Zhao. 2015. The internet of things: a survey. *Information Systems Frontiers* 17, 2 (2015), 243–259.

[75] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao. 2017. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal* 4, 5 (Oct 2017), 1125–1142.

[76] Pavel Masek, Jiri Hosek, Krystof Zeman, Martin Stusek, Dominik Kovac, Petr Cika, Jan Masek, Sergey Andreev, and Franz Kropfl. 2016. Implementation of True IoT Vision: Survey on Enabling Protocols and Hands-On Experience. *International Journal of Distributed Sensor Networks* 12, 4 (2016), 8160282. https://doi.org/10.1155/2016/8160282

[77] Matthew Mauriello, Michael Gubbels, and Jon E Froehlich. 2014. 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*. ACM, Toronto, ON, Canada, 2833–2842.

[78] Alexey Medvedev, Petr Fedchenkov, Arkady Zaslavsky, Theodoros Anagnostopoulos, and Sergey Khoruzhnikov. 2015. Waste management as an IoT-enabled service in smart cities. In *Proceedings of the Conference on Smart Spaces*. Springer, St. Petersburg, Russia, 104–115.

[79] G. R. Mendez, M. A. Md Yunus, and S. C. Mukhopadhyay. 2012. 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, 2640–2645.

[80] Konstantin Mikhaylov, Juha Petäjäjärvi, and Tuomo Haenninen. 2016. Analysis of Capacity and Scalability of the LoRa Low Power Wide Area Network Technology. In *Proceedings of the 22th European*

Wireless Conference. Oulu, Finland, 1–6.

[81] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. 2012. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks* 10, 7 (2012), 1497–1516.

[82] Jozef Mocnej, Winston K.G. Seah, Adrian Pekar, and Iveta Zolotova. 2018. Decentralised IoT Architecture for Efficient Resources Utilisation. *IFAC-PapersOnLine* 51, 6 (2018), 168 – 173. https://doi.org/10.1016/j.ifacol.2018.07.148 15th IFAC Conference on Programmable Devices and Embedded Systems PDeS 2018.

[83] Dragos Mocrii, Yuxiang Chen, and Petr Musilek. 2018. IoT-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet of Things* 1-2 (2018), 81 – 98. https://doi.org/10.1016/j.iot.2018.08.009

[84] Ramyar Rashed Mohassel, Alan Fung, Farah Mohammadi, and Kaamran Raahemifar. 2014. A survey on advanced metering infrastructure. *International Journal of Electrical Power & Energy Systems* 63 (2014), 473–484.

[85] Geoff Mulligan. 2007. The 6LoWPAN architecture. In *Proceedings of the 4th workshop on Embedded Networked Sensors (EmNets)*. ACM, Cork, Ireland, 78–82.

[86] Tuan Anh Nguyen and Marco Aiello. 2013. Energy intelligent buildings based on user activity: A survey. *Energy and buildings* 56 (2013), 244–257.

[87] Henrik Frystyk Nielsen, Jeffrey Mogul, Larry M Masinter, Roy T. Fielding, Jim Gettys, Paul J. Leach, and Tim Berners-Lee. 1999. Hypertext Transfer Protocol – HTTP/1.1. RFC 2616. https://doi.org/10.17487/RFC2616

[88] J. Nieminen, C. Gomez, M. Isomaki, T. Savolainen, B. Patil, Z. Shelby, M. Xi, and J. Oller. 2014. Networking solutions for connecting bluetooth low energy enabled machines to the internet of things. *IEEE Network* 28, 6 (Nov 2014), 83–90.

[89] B. A. A. Nunes, M. Mendonca, X. Nguyen, K. Obraczka, and T. Turletti. 2014. A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. *IEEE Commun. Surveys Tuts.* 16, 3 (03 2014), 1617–1634. https://doi.org/10.1109/SURV.2014.012214.00180

[90] Naouel Ouroua, Wassila Bouzegza, and Malika Ioualalen. 2017. Formal Modeling and Performance Evaluation of Network's Server Under SYN/TCP Attack. In *Mobile, Secure, and Programmable Networking*, Samia Bouzefrane, Soumya Banerjee, Françoise Sailhan, Selma Boumerdassi, and Eric Renault (Eds.). Springer International Publishing, Cham, 74–87.

[91] Sonia Panchen, Neil McKee, and Peter Phaal. 2001. InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks. RFC 3176. https://doi.org/10.17487/RFC3176

[92] Zhibo Pang, Qiang Chen, Weili Han, and Lirong Zheng. 2015. Value-centric design of the internet-of-things solution for food supply chain: value creation, sensor portfolio and information fusion. *Information Systems Frontiers* 17, 2 (2015), 289–319.

[93] A. Pekár, E. Chovancová, P. Fanfara, and J. Trelová. 2013. Issues in the passive approach of network traffic monitoring. In *Proceedings of the IEEE 17th International Conference on Intelligent Engineering Systems (INES)*. San Jose, Costa Rica, 327–332. https://doi.org/10.1109/INES.2013.6632836

[94] A. Pekár, M. Chovanec, L. Vokorokos, E. Chovancová, Peter Feciľak, and Miroslav Michalko. 2018. Adaptive Aggregation of Flow Records. *Computing and Informatics* 37, 1 (2018), 142–164. https://doi.org/10.4149/cai_2018_1_142

[95] Michele Penza, Domenico Suriano, Maria Gabriella Villani, Laurent Spinelle, and Michel Gerboles. 2014. Towards air quality indices in smart cities by calibrated low-cost sensors applied to networks. In *Proceedings of IEEE SENSORS*. Valencia, Spain, 2012–2017.

[96] Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. 2014. Context aware computing for the internet of things: A survey. *IEEE Communications Surveys & Tutorials* 16, 1 (2014), 414–454.

[97] Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. 2014. Sensing as a service model for smart cities supported by internet of things. *Transactions on Emerging Telecommunications Technologies* 25, 1 (2014), 81–93.

[98] David Pimentel and Rajinder Peshin. 2014. *Integrated pest management: pesticide problems*. Vol. 3. Springer Science & Business Media.

[99] Karthikeyan Ponnusamy and Narendran Rajagopalan. 2018. Internet of Things: A Survey on IoT Protocol Standards. In *Progress in Advanced Computing and Intelligent Engineering*, Khalid Saeed, Nabendu Chaki, Bibudhendu Pati, Sambit Bakshi, and Durga Prasad Mohapatra (Eds.). Springer Singapore, Singapore, 651–663.

[100] Stefan Poslad, Stuart E Middleton, Fernando Chaves, Ran Tao, Ocal Necmioglu, and Ulrich Bügel. 2015. A Semantic IoT Early Warning System for Natural Environment Crisis Management. *IEEE Transactions on Emerging Topics in Computing* 3, 2 (2015), 246–257.

[101] Maneesha Vinodini Ramesh. 2014. Design, development, and deployment of a wireless sensor network for detection of landslides. *Ad Hoc Networks* 13 (2014), 2–18.

[102] Shahid Raza, Simon Duquennoy, Tony Chung, Dogan Yazar, Thiemo Voigt, and Utz Roedig. 2011. Securing communication in 6LoWPAN with compressed IPsec. In *Proceedings of the International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*. Barcelona, Spain, 1–8.

[103] Juan Rico, Juan Sancho, Bruno Cendon, and Miguel Camus. 2013. 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, 1380–1385.

[104] Karen Rose, Scott Eldridge, and Lyman Chapin. 2015. The internet of things: An overview. *The Internet Society (ISOC)* (2015), 1–50.

[105] Lukas Ruge, Bashar Altakrouri, and Andreas Schrader. 2013. 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, 670–675.

[106] Peter Saint-Andre. 2011. Extensible Messaging and Presence Protocol (XMPP): Core. RFC 6120. https://doi.org/10.17487/RFC6120

[107] Mahmood Salehi, Azzedine Boukerche, and Amir Darehshoorzadeh. 2016. Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks. *Ad Hoc Networks* 50 (2016), 88 – 101. https://doi.org/10.1016/j.adhoc.2016.07.004

[108] Corinna Schmitt, Burkhard Stiller, and Brian Trammell. 2017. TinyIPFIX for Smart Meters in Constrained Networks. RFC 8272. https://doi.org/10.17487/RFC8272

[109] Zach Shelby and Carsten Bormann. 2011. *6LoWPAN: The wireless embedded Internet*. Vol. 43. John Wiley & Sons.

[110] Zach Shelby, Klaus Hartke, and Carsten Bormann. 2014. The Constrained Application Protocol (CoAP). RFC 7252. https://doi.org/10.17487/RFC7252

[111] Z. Sheng, S. Yang, Y. Yu, A. V. Vasilakos, J. A. Mccann, and K. K. Leung. 2013. A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities. *IEEE Wireless Communications* 20, 6 (December 2013), 91–98.

[112] J. Shi, J. Wan, H. Yan, and H. Suo. 2011. A survey of Cyber-Physical Systems. In *2011 International Conference on Wireless Communications and Signal Processing (WCSP)*. 1–6. https://doi.org/10.1109/WCSP.2011.6096958

[113] Pierluigi Siano. 2014. Demand response and smart grids—A survey. *Renewable and sustainable energy reviews* 30 (2014), 461–478.

[114] S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini. 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks* 76 (2015), 146 – 164. https://doi.org/10.1016/j.comnet.2014.11.008

[115] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks* 76 (2015), 146–164.

[116] Simran Singh, Ashlesha Atrey, Mihail L. Sichitiu, and Yannis Viniotis. 2019. Clearer than Mud: Extending Manufacturer Usage Description (MUD) for Securing IoT Systems. In *Internet of Things – ICIOT 2019*, Valerie Issarny, Balaji Palanisamy, and Liang-Jie Zhang (Eds.). Springer International Publishing, Cham, 43–57.

[117] A. Sivanathan, H. Habibi Gharakheili, F. Loi, A. Radford, C. Wijenayake, A. Vishwanath, and V. Sivaraman. 2018. Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics. *IEEE Transactions on Mobile Computing* (2018), 1–1. https://doi.org/10.1109/TMC.2018.2866249

[118] K. Smiljkovic, V. Atanasovski, and L. Gavrilovska. 2014. Machine-to-Machine traffic characterization: Models and case study on integration in LTE. In *2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE)*. 1–5. https://doi.org/10.1109/VITAE.2014.6934482

[119] E. Soltanmohammadi, K. Ghavami, and M. Naraghi-Pour. 2016. A Survey of Traffic Issues in Machine-to-Machine Communications Over LTE. *IEEE Internet of Things Journal* 3, 6 (Dec 2016), 865–884.

[120] OASIS Standard. 2012. Advanced Message Queuing Protocol (AMQP) Version 1.0. http://docs.oasis-open.org/amqp/core/v1.0/amqp-core-complete-v1.0.pdf

[121] OASIS Standard. 2019. MQTT Version 5.0. https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.pdf

[122] Rui Tan, Guoliang Xing, Jinzhu Chen, Wen-Zhan Song, and Renjie Huang. 2013. Fusion-based volcanic earthquake detection and timing in wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)* 9, 2 (2013), 17.

[123] Samuel Tang, Vineetha Kalavally, Kok Yew Ng, and Jussi Parkkinen. 2017. Development of a prototype smart home intelligent lighting control architecture using sensors onboard a mobile computing system. *Energy and buildings* 138 (2017), 368–376.

[124] Sahrish Khan Tayyaba, Munam Ali Shah, Omair Ahmad Khan, and Abdul Wahab Ahmed. 2017. Software Defined Network (SDN) Based Internet of Things (IoT): A Road Ahead. In *Proceedings of the International Conference on Future Networks and Distributed Systems* (Cambridge, United Kingdom) *(ICFNDS '17)*. Association for Computing Machinery, New York, NY, USA, Article 15, 8 pages. https://doi.org/10.1145/3102304.3102319

[125] Vladimir V Terzija, Gustavo Valverde, Deyu Cai, Pawel Regulski, Vahid Madani, John Fitch, Srdjan Skok, Miroslav Begovic, and Arun G Phadke. 2011. Wide-area monitoring, protection, and control of future electric power networks. *Proc. IEEE* 99, 1 (2011), 80–93.

[126] The Open Networking Foundation. 2015. OpenFlow Switch Specification Version 1.5.1 (Protocol version 0x06). ONF TS-025. http://opennetworking.wpengine.com/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf

[127] Tom Torfs, Tom Sterken, Steven Brebels, Juan Santana, Richard van den Hoven, Vincent Spiering, Nicolas Bertsch, Davide Trapani, and Daniele Zonta. 2013. Low power wireless sensor network for building monitoring. *IEEE Sensors Journal* 13, 3 (2013), 909–915.

[128] Serbulent Tozlu, Murat Senel, Wei Mao, and Abtin Keshavarzian. 2012. Wi-Fi enabled sensors for internet of things: A practical approach. *IEEE Communications Magazine* 50, 6 (2012).

[129] A Van Herwijnen and J Schweizer. 2011. Monitoring avalanche activity using a seismic sensor. *Cold Regions Science and Technology* 69, 2 (2011), 165–176.

[130] Lorenzo Vangelista, Andrea Zanella, and Michele Zorzi. 2015. 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, 51–58.

[131] D. R. Vasconcelos, R. M. C. Andrade, V. Severino, and J. N. De Souza. 2019. Cloud, Fog, or Mist in IoT? That Is the Question. *ACM Trans. Internet Technol.* 19, 2, Article 25 (March 2019), 20 pages. https://doi.org/10.1145/3309709

[132] S. Verma, Y. Kawamoto, Z. M. Fadlullah, H. Nishiyama, and N. Kato. 2017. A Survey on Network Methodologies for Real-Time Analytics of Massive IoT Data and Open Research Issues. *IEEE Communications Surveys Tutorials* 19, 3 (thirdquarter 2017), 1457–1477. https://doi.org/10.1109/COMST.2017.2694469

[133] Ovidiu Vermesan and Peter Friess. 2013. *Internet of things: converging technologies for smart environments and integrated ecosystems*. River publishers.

[134] Deepali Virmani and Nikita Jain. 2016. 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, 1103–1109.

[135] Shiyong Wang, Jiafu Wan, Di Li, and Chunhua Zhang. 2016. Implementing smart factory of industrie 4.0: an outlook. *International Journal of Distributed Sensor Networks* 2016 (2016), 7.

[136] Andrew Whitmore, Anurag Agarwal, and Li Da Xu. 2015. The Internet of Things—A survey of topics and trends. *Information Systems Frontiers* 17, 2 (2015), 261–274.

[137] Xiaoya Xu, Miao Zhong, Jiafu Wan, Minglun Yi, and Tiancheng Gao. 2016. Health Monitoring and Management for Manufacturing Workers in Adverse Working Conditions. *Journal of medical systems* 40, 10 (2016), 222.

[138] Y. Xue, D. Wang, and L. Zhang. 2013. Traffic classification: Issues and challenges. In *Proceedings of the International Conference on Computing, Networking and Communications (ICNC)*. San Diego, USA, 545–549. https://doi.org/10.1109/ICCNC.2013.6504144

[139] W. Yang, E. Aghasian, S. Garg, D. Herbert, L. Disiuta, and B. Kang. 2019. A Survey on Blockchain-Based Internet Service Architecture: Requirements, Challenges, Trends, and Future. *IEEE Access* 7 (2019), 75845–75872. https://doi.org/10.1109/ACCESS.2019.2917562

[140] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao. 2017. A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal* 4, 5 (Oct 2017), 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844

[141] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and Privacy on Blockchain. *ACM Comput. Surv.* 52, 3, Article 51 (July 2019), 34 pages. https://doi.org/10.1145/3316481

[142] Bin Zhou, Wentao Li, Ka Wing Chan, Yijia Cao, Yonghong Kuang, Xi Liu, and Xiong Wang. 2016. Smart home energy management systems: Concept, configurations, and scheduling strategies. *Renewable and Sustainable Energy Reviews* 61 (2016), 30–40.

[143] H. G. Ziegler. 2016. Privacy-preserving and IoT-capable crowd analysis and detection of flow disturbances for enhancing public safety. In *2016 5th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS)*. 1–8.

[144] Marco Zúniga, Bhaskar Krishnamachari, et al. 2003. Integrating future large-scale wireless sensor networks with the internet. *USC Computer Science, Tech. Rep* (2003).