Internet-of-Things-Based Smart Cities: Recent Advances and Challenges

Yasir Mehmood, Farhan Ahmad, Ibrar Yaqoob, Asma Adnane, Muhammad Imran, and Sghaier Guizani

The authors devise a taxonomy to best bring forth a generic overview of the IoT paradigm for smart cities, integrated ICT, network types, possible opportunities, and major requirements. Moreover, an overview of the up-to-date efforts from standard bodies is presented.

ABSTRACT

The Internet of Things is a novel cutting edge technology that proffers to connect a plethora of digital devices endowed with several sensing, actuation, and computing capabilities with the Internet, thus offering manifold new services in the context of a smart city. The appealing IoT services and big data analytics are enabling smart city initiatives all over the world. These services are transforming cities by improving infrastructure and transportation systems, reducing traffic congestion, providing waste management, and improving the quality of human life. In this article, we devise a taxonomy to best bring forth a generic overview of the IoT paradigm for smart cities, integrated ICT, network types, possible opportunities and major requirements. Moreover, an overview of the up-to-date efforts from standard bodies is presented. Later, we give an overview of existing open source IoT platforms for realizing smart city applications followed by several exemplary case studies. In addition, we summarize the latest synergies and initiatives worldwide taken to promote IoT in the context of smart cities. Finally, we highlight several challenges in order to give future research directions.

INTRODUCTION

The Internet of Things (IoT) is a revolutionary communication paradigm that aims to bring forth an invisible and innovative framework to connect a plethora of digital devices with the Internet. Thus, it intends to make the Internet more immersive and pervasive [1]. The emerging IoT market is continously gaining momentum as operators, vendors, manufacturers, and enterprises begin to recognize the opportunities it offers. According to the latest IDC forecast,[1] the worldwide IoT market will reach US$1.7 trillion in 2020 up from US$655.8 billion in 2014 with a compound annual growth rate of 16.9 percent. The devices alone are expected to represent 31.8 percent of the total worldwide IoT market in 2020. This greater percentage of the revenue in 2020 is expected through building IoT platforms, application softwares, and service-related offerings.

A smart city is a complex ecosystem characterized by the intensive use of information and communications technologies (ICT), aiming to make cities more attractive and more sustainable, and unique places for innovation and entrepreneurship [2]. The major stakeholders include application developers, service providers, citizens, government and public service providers, the research community, and platform developers. Furthermore, the smart city cycle consists of numerous ICT technologies, development platforms, maintenance, and sustainability, apps for evolving citizens, and technical, social, as well as economic key performance indicators (KPIs). Consequently, IoT systems will play a fundamental role in the deployment of large-scale heterogeneous infrastructures. A high-level illustration of an IoT-based smart city is given in Fig. 1.

IoT-based smart city applications can be categorized on the basis of network type, scalability, coverage, flexibility, heterogeneity, repeatability, and end-user involvements [3]. In general, these applications can be grouped into personal and home, utilities, mobile, and enterprises. For instance, *personal and home* applications include ubiquitous e-healthcare services to live independently via body area networks (BANs), which help doctors monitor patients remotely. *Utilities* applications include smart grid, smart metering/monitoring, water network monitoring, and video-based surveillance. Similarly, *mobile* applications include intelligent transportation system (ITS) and logistics, traffic management, congestion control, and waste management. Additionally, IoT-based enterprise applications usually consist of a network of things within a work environment.

Several research efforts have been made to integrate IoT with smart city environments. For instance, Zanella *et al.* [1] presented a comprehensive survey of the architectures, protocols, and enabling technologies for a web-service-based IoT framework in the Padova smart city project. The proof of concept implementation with numerous technical solutions aims to monitor street lighting, the quality of air, and identification of the most critical issues. A survey on the fundamental IoT elements in realizing smart cities was conducted in [4], which also described a case study on noise monitoring. Nathalie *et al.* [5] proposed a different perspective of smart cities in which IoT devices were considered service providers mimicking cloud-based services. The proposal offered a higher level of abstraction to deploy innovative ubiquitous applications by eliminating the barriers between physical IoT devices and the logical (cloud service providers) world. A generic top-down smart city architecture was proposed in [6]

[1] https://www.telecompaper.com/news/global-iot-market-to-reach-usd-17-tln-in-2020-idc–1085269, accessed October 20, 2016.

Digital Object Identifier: 10.1109/MCOM.2017.1600514

Yasir Mehmood (corresponding author) is with the University of Bremen; Farhan Ahmad and Asma Adnane are with the University of Derby; Ibrar Yaqoob is with the University of Malaya; Muhammad Imran is with King Saud University; Sghaier Guizani is with Alfaisal University.

in which service providers play a role of central information unit that is connected to a set of IoT-based services. It also offers IoT convergence and acceptance of numerous ICT technologies for realizing smart cities.

Although several studies exist on IoT and smart cities, convergence of these two areas grants further academic efforts for the flourishing of IoT-based smart cities. Thus, unlike other studies, this article best bring forths an IoT-based smart cities taxonomy, prime open source platforms, and case studies of recent deployments, as well as unearthing several open research challenges. The contributions of this study are as follows:

- First, we devise a taxonomy of the IoT-based smart city environment.
- We present an overview of major open platforms for smart cities.
- Further, we present recent synergies and a number of case studies on various smart city deployments reported by various enterprises.
- Finally, we unearth several IoT-related open research challenges to give future directions.

IoT-Based Smart City Taxonomy

This section presents a taxonomy of IoT-based smart cities that categorizes the literature on the basis of existing communication protocols, major service providers, network types, standardization efforts, offered services, and crucial requirements. An overview of the devised smart city taxonomy is depicted in Fig. 2.

Communication Protocols

IoT-based smart city realization significantly relies on numerous short- and wide-range communication protocols to transport data between devices and back-end servers. The most prominent short-range wireless technologies include ZigBee, Bluetooth, Wi-Fi, WiMAX, and IEEE 802.11p, which are primarily used in smart metering, e-healthcare, and vehicular communication. Wide-range technologies such as Global System for Mobile Communication (GSM) and general packet radio service (GPRS), Long Term Evolution (LTE), and LTE-Advanced are commonly utilized in ITS such as vehicle-to-infrastructure (V2I), mobile e-healthcare, smart grid, and infotainment services. Additionally, LTE-M is considered as an evolution for cellular IoT (C-IoT). In Release 13, the Third Generation Partnership Project (3GPP) plans to further improve coverage, battery lifetime, and device complexity [7]. Besides well-known existing protocols, the LoRa Alliance is standardizing the LoRaWAN protocol to support smart city applications, primarily ensuring interoperability between several operators. Moreover, SIGFOX is an ultra narrowband radio technology with full star-based infrastructure that offers a highly scalable global network for realizing smart city applications with extremely low power consumption. A comparative summary[2] of the major communication protocols is presented in Table 1.

Service Providers

Pike Research estimated that the smart cities market will grow to hundreds of billions of dollars by 2020, with an annual growth of nearly US$16 billion. IoT is recognized as a potential source to increase the revenue of service providers. Thus, well-known worldwide service providers have already started exploring this novel cutting-edge communication paradigm. Major service providers include Telefonica, SK Telecom, Nokia, Ericsson, Vodafone, NTT DOCOMO, Orange, Telenor, and AT&T, which offer a variety of services and platforms for smart city applications such as ITS and logistics, smart metering, home automation, and e-healthcare.

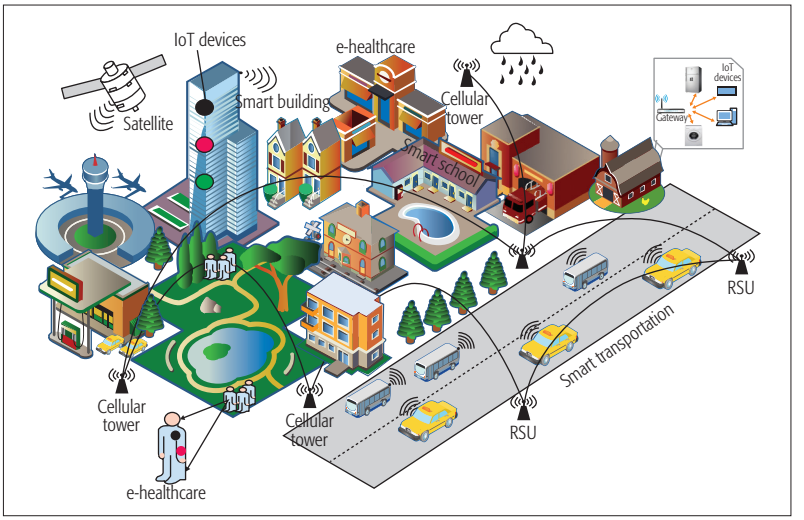

Figure 1. An illustration of an IoT-based smart city.

Network Types

IoT-based smart city applications rely on numerous network topologies to accomplish a fully autonomous environment. The capillary IoT networks offer services over a short range. Examples include wireless local area networks (WLANs), BANs, and wireless personal area networks (WPANs). The application areas include indoor e-healthcare services, home automation, and street lighting. On the other hand, applications such as ITS, mobile e-healthcare, and waste management use wide area networks (WANs), metropolitan area networks (MANs), and mobile communication networks. The above networks pose distinct features in terms of data, size, coverage, latency requirements, and capacity.

Activities of Standard Bodies

The vast smart city applications not only demand large scale deployment of numerous kinds of IoT devices, but also require device interoperability. Therefore, most prominent governing bodies such as the Internet Engineering Task Force (IETF), Third Generation Partnership Project (3GPP) European Telecommunications Standards Institute (ETSI), oneM2M, IEEE, and Open Mobile Alliance (OMA) are actively involved in developing standards to support smart city applications on a large scale. This section discusses the major contributions and ongoing activities of the prime standard bodies for enabling smart city applications.

IETF: The first IETF working group (WG), 6LoWPAN, standardized techniques for handling IoT small packets using header compression and neighbor discovery optimization. Moreover, the Routing Over Low-power and Lossy networks (ROLL) WG standardized Routing Protocol for Low Power and Lossy Networks (RPL) for smart

[2] https://www.global-logic.com/wp-content/uploads/2015/12/The-role-of-telecommunications-in-smart-cities.pdf, accessed December 10, 2016.

IoT offers diverse applications in a smart city, thus demands numerous requirements. For instance, IoT-based solutions are expected to be low cost, low energy consumption, high quality-of-service (QoS), wider coverage, increased flexibility, high security and privacy, ultra-dense deployments, and multivendor interoperability.

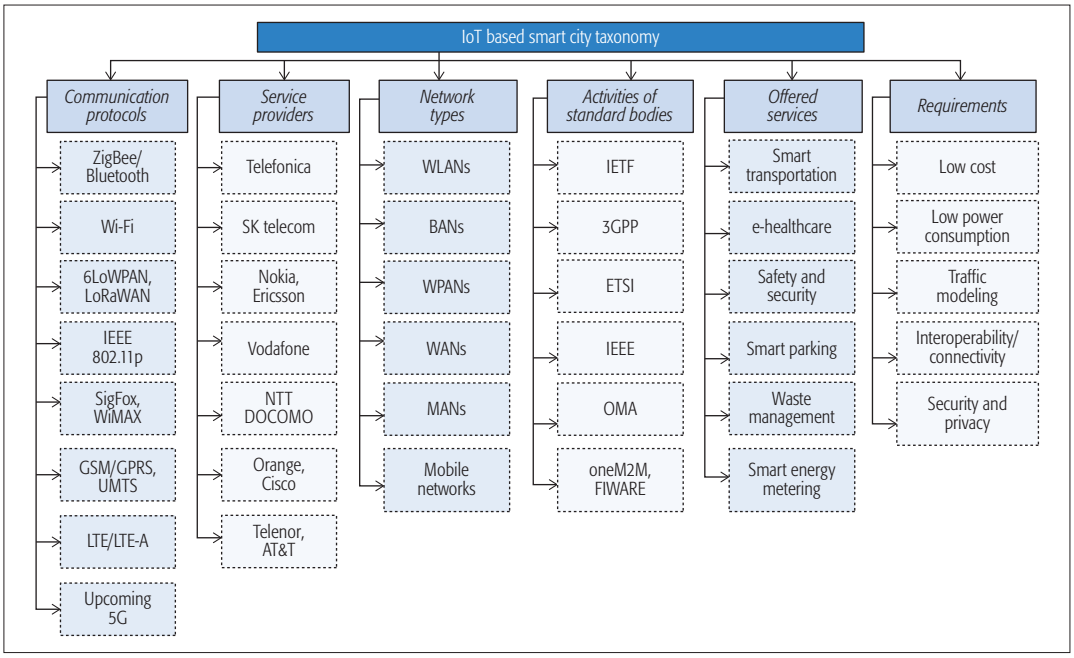

Figure 2. A representation of IoT-based smart city taxonomy.

city applications. In addition, several IETF WGs such as DICE are active in standardizing security profiles, such as Transport Layer Security (TLS) and Datagram-TLS (DTLS) for constrained IoT devices.

3GPP: in its latest Release 13, 3GPP standardized narrowband IoT (NB-IoT) to provide better network coverage for smart city applications by further reducing the bandwidth to 200 kHz (uplink/downlink), reducing throughput on a physical resource block (PRB) level, supporting massive IoT devices and low power consumption, and enhancing coverage extension by 20 dB [10]. As a result, NB-IoT meets the application requirements in the industrial, public, personal, and home domains. Additionally, 3GPP is introducing extended discontinuous transmission/reception (eDTX/eDRX) techniques in Release 13 to further reduce power consumption, and thus increase the device operating time.

ETSI: ETSI aims to deliver interoperable and cost-effective solutions to support smart city applications. Particularly, oneM2M is the global initiative by ETSI in cooperation with the member research institutes such as the Broadband Forum, OMA, and Continua to support IoT connectivity on a large scale. oneM2M aims to develop a single horizontal platform for enabling interoperability among all applications through a distributed software layer.[3] Additionally, it delivers architecture, requirements, application programming interface (API) specifications, and privacy and security solutions, as well as an interoperability framework for smart city applications. Consequently, the standardized APIs and open interfaces can be used within several systems for enabling a plethora of IoT devices to connect worldwide with the backend servers.

IEEE: In the context of smart cities, IEEE mainly focuses on optimization of the air interface for ultra-IoT deployments. Furthermore, IEEE focuses on the use of sub-6 GHz spectrum for IoT connectivity to support numerous smart city applications.

OMA: *OMA* standardized the OMA Lightweight M2M (OMALWM2M) protocol for resource constrained IoT device management for both sensor and cellular networks. OMALWM2M is located at the device end, and offers a communication path between an LWM2M client and an LWM2M server. Therefore, OMALWM2M is a light and compact protocol that is frequently used with the Constrained Application Protocol (CoAP), and offers an efficient resource data model for the resource constrained IoT devices. Additionally, it provides a choice for service providers to deploy IoT systems for supporting corresponding smart city applications.

Offered Services

IoT offers numerous services that are of great interest in the context of smart cities to not only improve the quality of human lives, but also leverage the city administration by reducing the operational costs [1]. Major offerings include smart lighting, waste and water management. For instance, smart IoT modules can be deployed within grid stations, homes, and workplaces for distributing and consuming energy efficiently. In *e-healthcare*, IoT devices can be positioned on the bodies of patients for monitoring health parameters such as temperature, pulse rate, and sugar level, and provide opportunities for doctors to regularly monitor their patients. Besides, *urban IoTs* can provide solutions to control traffic congestion through monitoring of traffic intensity using either GPS services in modern vehicles or WANs. In *waste management*, the truck route can be optimized based on the load level indication by smart waste containers. Consequently, it enhances the quality of recycling by reducing the cost of waste collection.

Requirements

IoT offers diverse applications in a smart city, and thus demands numerous requirements. For instance, IoT-based solutions are expected to have

[3] oneM2M-TS-0001-V-2014-08, accessed June 5, 2016.

Technology	Operating frequency	Data rate	Coverage	Latency	Power usage	Use cases
ZigBee	2.4 GHz 868 MHz, 915 MHz	250 kb/s	50–100 m	16 ms	Low	Smart metering, indoor e-healthcare
Bluetooth	2.4 GHz	25 Mb/s	10 m	100 ms	Low	Indoor e-healthcare
Wi-Fi	2.4 GHz5 GHz, 802.11n	54 Mb/s, 6.75 Gb/s	140 m 100 m	46 ms	Medium	Metering, waste management automation, energy management, infotainment, automation
IEEE 802.11p	5.85–5.925 GHz	6 Mb/s	1000 m		Low	Vehicular communication, V2V/V2I, infotainment
DSRC/WAVE	5.8, 5.9 GHz	6 Mb/s	1000 m	200 μs	Low	ITS (V2V/V2I)
DASH7	433, 868, 915 MHz	55.5 kb/s, 200 kb/s	1000 m	15 ms	Low	ITS, automation
6LoWPAN	2.4 GHz, 868, 915 MHz	250 kb/s	100 m		Low	ITS, smart metering, logistics
LoRaWAN	433, 868, 780, 915 MHz	50 kb/s	2–5 km		Low	ITS, smart metering, waste management
GSM/GPRS	850, 900, 1800, 1900 MHz	80–384 kb/s	5–30 km	1.5–3 s	High	ITS, smart metering, m-health, energy management, logistics, infotainment
3G	850 MHz	3 Mb/s	5–30 km	100 ms	High	ITS, smart metering, energy management, m-health, logistics, infotainment
LTE/LTE-Advanced	700, 750, 800, 1900, 2500 MHz	1 Gb/s, 500 Mb/s	5–30 km	5 ms	High	ITS, smart metering, mobile health, logistics, infotainment

Table 1. A summary of major communication protocols for realizing IoT-based smart cities [8].

low cost, low energy consumption, high quality of service (QoS), wider coverage, increased flexibility, high security and privacy, ultra-dense deployments, and multivendor interoperability. To fulfill the above requirements, several new techniques must be adopted. For instance, traffic modeling can play an essential role in handling massive IoT traffic. Therefore, instead of using the traditional source traffic modeling approach, where each IoT device accesses the network individually for sending and receiving important messages, an aggregated traffic modeling approach must be commonly used, as illustrated in Fig. 3. In this way, several IoT devices can share scarce resources for sending and receiving small-sized data. To achieve this, a gateway can be deployed, which may operate using any of the existing communication technologies. For instance, the data from IoT devices can be transported to a gateway using short-range communication standards such as ZigBee, Bluetooth, Wi-Fi, and other dedicated short-range communications (DSRC) protocols. In addition, LTE and LTE-A relays and femtocells can be deployed to perform data aggregation.

Aggregated traffic modeling can improve the performance of IoT networks by supporting enormous numbers of devices. Since tiny IoT systems also demand low power consumption in order to increase device lifetime (up to 10 to 15 years), data aggregation can be used to ensure low energy consumption through improved coverage along with the network capacity. This is achieved by improving the channel conditions using intermediate gateways and relays. Furthermore, provisioning of QoS is also essential in critical IoT applications such as e-healthcare and emergency alert. Therefore, incorporating data differentiation schemes along with the aggregation approach can potentially fulfill QoS requirements and satisfy the delay requirements of critical smart city applications. High-priority traffic (e.g., e-healthcare data) should be served immediately followed by low-priority traffic (e.g., regular monitoring). Besides traffic modeling, ultra-dense IoT realization demands strong collaboration among modem manufacturers and vendors in order to increase interoperability. Consequently, this will further reduce the associated cost factors. Besides, data security and integrity is of significant importance to ensure safe and secure IoT communications.

Besides traffic modeling, ultra-dense IoT realization demands strong collaboration among modem manufacturers and vendors in order to increase interoperability. Consequently, this will further reduce the associated cost factors. Besides, data security and integrity is of significant importance to ensure safe and secure IoT communications.

IoT Open Source Platforms

Open source implementations always play a vital role in sharing information in order to achieve multi-vendor interoperability. Worldwide, the following prime open communities offer easy and fast development platforms for smart cities.

FIWARE[4]

FIWARE is a standard open platform for realizing smart city applications. It was launched by the European Commission, and aims to develop the core future technologies in the IoT paradigm. It is based on software components named generic enablers. These components provide common functionalities to the multiple vertical sectors with

[4] http://www.fiware.org/about-us/, accessed October 10, 2016..

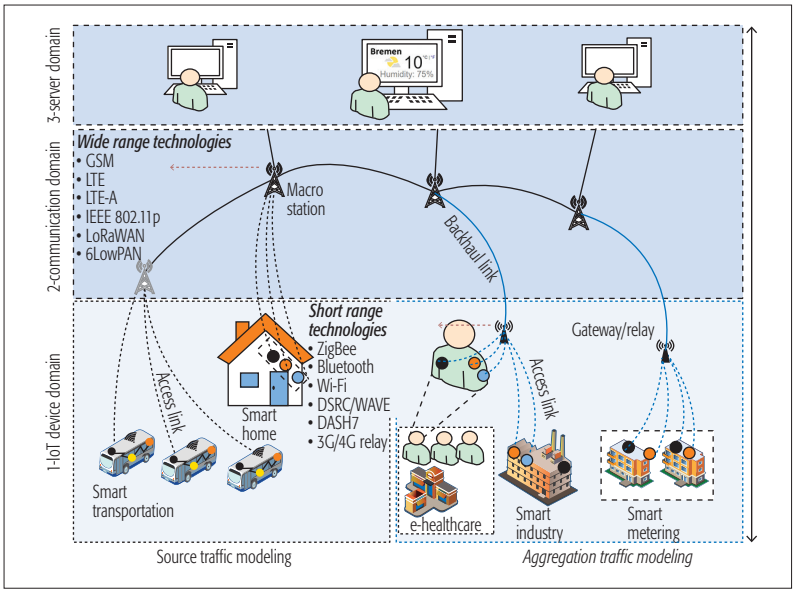

Figure 3. An illustration of traffic modeling for an IoT based smart city.

the objective of enabling interoperability among them. FIWARE enablers are classified into seven wide technical categories: cloud hosting, applications, services and data delivery, security, interface to networks and devices, advanced web, IoT services enablement, and data/context management. Moreover, FIWARE provides a simple and powerful set of APIs that ease the development of smart applications. Despite many advantages of FIWARE, the lack of a complete set of functionalities is one of the key issues that remains to be addressed.

OCEAN[5]

The Open Alliance for IoT Standard (OCEAN) was initiated in January 2015 by the Korea Electronics Technology Institute (KETI) and the Korean government. It is a global alliance that aims to bring forth open source implementations for smart cities based on IoT standards. Additionally, the initiative focuses on promoting the development and commercialization of platforms, products, and services by widespread adoption of IoT standards-compliant open source code. OCEAN is responsible for releasing the source code for IoT standards as open source, and helping vendors and developers collaborate with each other to create new innovative products and services under a global partnership, finally establishing a global IoT ecosystem for smart cities. Currently, OCEAN provides several oneM2M-based platforms for devices, gateways, and servers.

OM2M[6]

The OM2M project was initiated by the ECLIPSE Foundation to deliver an open source implementation of the oneM2M and SmartM2M standards. The primary goal of this initiative is to support the deployment of vertical applications and heterogeneous devices by providing a horizontal machine-to-machine (M2M) service platform for developing services independent of the underlying network. Thus, it provides a horizontal service common entity (SCE), which can be deployed in an M2M device, a gateway, or a server. The major SCE functionalities include application enablement, triggering, notification, security, persistence, interworking, and device management. Additionally, it provides RESTful interfaces for authentication, registration, resources discovery, containers management, synchronous/asynchronous communications, access rights authorization, groups organization, and re-targeting.

Open DayLight IoT Data Management[7]

The IoT Data Management (IoTDM) from the Open DayLight (ODL) project is about developing a data-centric middleware that will represent an IoT broker compliant with oneM2M. It will also authorize applications to recover data uploaded by any IoT device used in a smart city. The ODL platform is used to implement the oneM2M data store, which models a hierarchical containment tree, where each node in the tree represents a oneM2M resource. Typically, IoT devices and applications interact with the resource tree over standard protocols such as CoAP, Message Queue Telemetry Transport (MQTT), and HTTP.

Contiki[8]

Contiki is also an open platform that offers fast and easy development of numerous IoT-based smart city applications. It offers powerful Internet communication to tiny microcontrollers and operates at extremely reduced cost and low power. Additionally, it fully supports standard IPv4 and IPv6 protocols such as UDP, TCP, and HTTP. Besides, it offers support of the latest low-power wireless and mobile networks such as 6LowPAN, CoAP, and multihop RPL. Furthermore, it provides highly efficient memory allocation procedures for various smart city applications.

IoT Synergies and Case Studies

This section presents a number of case studies provided by different enterprises along with the modern IoT synergies for the realization of smart cities. The aim is to provide a summary of the current deployments and recent initiatives of IoT-based solutions to tackle various city-related issues. A detailed summary of the case studies and projects is given in Table 2.

Busan Green u-City[9]

Busan Green u-City (ubiquitous city) is the first IoT-enabled smart city in South Korea. It is one of the modern practical examples of IoT-based smart cities, using a cloud-based infrastructure to improve the efficacy of city management and local business opportunities, improving the quality of human lives. It is a public-private cooperation among the Busan city government, major technology suppliers, Cisco, and South Koreas largest telco, KT, with an approximate investment of US$452 million. The primary objective of this cooperation is to deliver an improved transportation system, e-healthcare services, increased jobs and business opportunities, and improved information accessibility through various devices and communication sources.

Smart Santander[10]

Santander, the Spanish city, is widely recognized as an IoT-based smart city. This *Future Internet Award* winning project is a cooperation

[5] http://www.iotocean.org/main/, accessed June 5, 2016.

[6] http://www.eclipse.org/om2m/, accessed June 5, 2016.

[7] https://www.opendaylight.org/,accessed June 5, 2016.

[8] http://www.contiki-os.org/, accessed October 10, 2016.

[9] http://www.gsma.com/connectedliving/busan-green-u-city-a-successful-example-of-a-smart-city-in-south-korea/, accessed April 15, 2016.

[10] http://www.smartsantander.eu/, accessed April 1, 2016.

City	Country	Population	Solutions	Major partners
Busan	South Korea	3.4 million	Safety service for childrens/elderly, drone based smart marine, smart parking, crosswalk and energy usage	Busan government, Cisco, ETRI, KETI, SK telecom, KT
Santander	Spain	0.1 million	Smart metering of temperature, traffic intensity, humidity, transportation plans, water needs, etc..	Ericsson, Telefonica, Telefonica I+D
Chicago	United States	2.7 million	Smart grid, smart living, emergency alert, reduced crime	Cisco, IBM, Chicago government
Milton Keynes	United Kingdom	0.2 million	Smart transportation, reduced corbon emission, smart energy, water management	Milton Keynes Council, Samsung, Huawei, CATAPULT, Cambridge University

Table 2. A comparison of case studies.

of 15 big companies and institutions including Ericsson, Telefonica, and several universities and research groups in Spain, Greece, Germany, Denmark, the United Kingdom, and Australia. The city is equipped with approximately 20,000 smart IoT devices that perform several intelligent tasks such as measurement of temperature, humidity, speed and position of vehicles, traffic intensity, public transportation conditions and timetables, air quality, and water networks. The acquired sensor data is transmitted to Munoz's laboratory and compiled into a big picture by a central computer. Thus, everything is recorded in this digital city.

Chicago[11]

The project focuses on infrastructure management, economic development, and community engagement to tackle major issues of education, economic development, crime, and transport in Chicago, Illinois. In cooperation with IBM, Chicago deployed around 300,000 smart IoT devices to support smart grid operations. The primary objective of this project is to reduce energy waste to save customers US$170 million. The project developed an analytics platform on Cisco technology that has helped to minimize crime rates in the city. Also, a model was created that has more than 31 variables to predict and prevent rodent infestations. Analytics is also incorporated to identify buildings that are anticipated to become vacant. Numerous apps have been built using 600 datasets of an open city portal to notify citizens about several unwanted situations expected within a territory.

Milton Keynes[12]

The Milton Keynes Smart project is coordinated by the Open University and aims to develop a data hub within the city that collects and manages data received from several smart devices. The project emphasizes control of corbon emissions and support of sustainable growth without deploying additional infrastructure. The project is a collaboration between Samsung, Huawei, CATAPULT, and Cambridge University that aims to bring forth innovative solutions involving the aforementioned issues. Also, the project aims to deliver an efficient transportation system, water usage, and smart energy solutions as well as focusing on business, education, and community engagement activities.

Open Research Challenges

Besides the aforementioned advances, there are several open research issues and challenges in adopting IoT for smart cities. The purpose of discussing these challenges is to give research directions to new researchers in this domain. Table 3 summarizes the future research directions along with their advantages and requirements.

Security, Privacy, and Trust

Security in general is required for every IoT device. As smart cities provide Internet connectivity to an ample variety of devices, security becomes a very critical challenge. According to HP, about 70 percent of IoT devices in a smart city were at risk of attack due to sufficient vulnerabilities such as insufficient authorization, inadequate software protections, and weak encrypted communication protocols [11]. These vulnerabilities instigate various threats and attacks, leading to several issues in terms of security and privacy. In order to design a successful IoT-based smart city, the following issues must be addressed aforementioned:

- Privacy-aware communication for user data should be provided.
- Simple, lightweight, and efficient security solutions should be designed to ensure data authenticity and integrity, and to provide secure communication between IoT devices and a cloud-based application center [13].
- Detailed risk assessment must be performed to identify present and newly emerging attacks based on vulnerabilities and threats. One such risk assessment framework is proposed by ENISA, which identifies possible emerging attacks in ITS [13].
- An active and adequate decentralized trust management system must be designed.
- Users' trust and consent must be ensured by providing strong privacy measures.

Interoperability

Interoperability is the capability of two different devices and networks to communicate with each other for the exchange of important information. Smart cities include IoT devices from a diverse range of domains (e.g., smart metering, e-healthcare, logistics, monitoring, and intelligent transport). In a smart city, interoperability plays a vital role in providing connectivity among devices operating with different communication technol-

According to HP, about 70 percent of IoT devices in a smart city were at risk of attack due to sufficient vulnerabilities such as insufficient authorization, inadequate software protections, and weak encrypted communication protocols. These vulnerabilities instigate various threats and attacks, leading to several issues in terms of security and privacy.

[11] http://www.smartchicagocollaborative.org/category/city-of-chicago/, accessed June 4, 2016.

[12] http://www.mksmart.org/, accessed: May 1, 2016.

ogies. For example, smart metering uses WLAN technologies as the underlaying communication protocols, while ITS mainly utilize DSRC and mobile technologies for communication. According to the World Economic Forum, interoperability between devices from different domains is a major barrier to IoT success due to lack of universal standards [14]. To overcome this barrier, interoperability issues should be identified at different levels (e.g., device, network, communication, application, and platform). To address these issues, an intelligent and holistic approach is required to provide connectivity to billions of IoT devices. For instance, standardization of oneM2M and FIWARE is a major step in overcoming the interoperability issues with the collaboration of world's largest standardization bodies such as ETSI, 3GPP, and OMA.

Low-Power and Low-Cost Communication

Usually, IoT devices are small in nature and equipped with a group of sensors. In order to operate these devices, a continuous source of energy is constantly required, which poses a significant challenge in terms of battery life and cost. To address these issues in IoT-based smart cities, the devices must feature low power consumption at very low cost. This can be achieved through advancements in the domain of wireless communication and micro-electronics.

Feature	Applications	Advantages	Research challenges	Major requirements
Security	ITS, e-healthcare, smart schools, logistics	Secure attack-free execution environment to deploy services	1) Lack of standardized security solutions without hindering data integrity 2) Secure deployment and integration of cloud-based services at the device and network levels 3) Efficient early identification of both insider and outsider threats	Identification of vulnerabilities in the network that serve as weak entry points for various attacks
Privacy	ITS, e-healthcare	Provides data protection and user privacy in the network	Ensuring users' anonymity in the IoT network for using particular services	Pervasive network model with strong encryption and cryptographic tools
Trust	ITS, e-healthcare	Ensures users' belief and trust that the desired services are free from vulnerabilities	1) Efficient decentralized trust management system 2) Intelligent trust evaluation during service unavailability and compromised IoT network	Decentralized trust model avoiding a single point of failure in the network
Risk management	ITS, indoor e-healthcare	Ensures security by identifying uncertain events and threats in the IoT network	1) Low-cost and efficient risk management systems to identify newly emerged attacks effectively 2) Fast and ultra-efficient risk decision mechanisms to counter identified threats	1) Detailed threat modeling to identify various threats in the network 2) Identify various risks areas through threat actors and asset-based threat modeling
Interoperability	ITS, smart home, personal e-health ecosystem	Provides a platform for two IoT devices from different domains to communicate	Integrating devices for vendor locked-in services	Generic, centralized, flexible, and open reference models for devices to integrate and communicate (e.g., IP, CoAP)
Low-power and low-cost communication	ITS, smart meters, e-healthcare	Provides a wide range of applications in IoT-based smart cities if communication is low-cost	How to prolong the battery life of the IoT devices?	Advancements in micro-electronics and wireless communication to provide low-cost communication and increased battery life
Big data	Smart meters, ITS, e-healthcare	Increases IoT network performance by processing useful information identified by authenticated sources (e.g, analyzing traffic data can reduce traffic congestion processing)	1) Lack of appropriate tools to handle the massively generated information 2) Protection of users' privacy and security 3) Efficient centralized data acquisition and information	1) Centralized big data processing centers 2) Public awareness to utilize resources in the IoT network safely
Connectivity	ITS, waste management, e-healthcare, smart industry	Ensures that IoT devices can communicate from various domains	How to ensure connectivity in a wide range of IoT devices during no communication network and high mobility?	1) Efficient usage of spectrum for IoT devices to communicate 2) Intelligent usage of every possible communication medium (e.g., WLAN, 3G, LTE, WiMAX) 3) Development of gossip-based algorithms to provide connectivity to IoT devices in the absence of a communication network

Table 3. Future research challenges.

Big Data Analytics

Big data analytics is one of the major research directions in the IoT-based smart cities paradigm [15]. Smart cities connecting billions of devices will provide a massive amount of information and data for analysis. This data can include information from surrounding environments (ITS) and user private data (smart hospitals). To analyze this data, intelligent techniques and algorithms are required. For instance, deep learning algorithms can be adopted to efficiently analyze immense information produced by locally connected devices. The major issues that must be addressed are:

- To respect user privacy during data analysis
- To provide data anonymity for sensitive data
- To provide infrastructure to collect, store, and analyze the huge amount of data
- To provide the required computation power to extract new knowledge from the data

Connectivity in IoT

An IoT-based smart city includes billions of devices in the network. The concept of smart cities can succeed only if it has the ability to provide connectivity to every available IoT device with sensing capabilities that produce significant information. In smart cities, IoT devices can use any available communication networks such as public Wi-Fi, Bluetooth, cellular networks (LTE/LTE-Advanced), and satellites to communicate with the cloud-based application center. However, ensuring connectivity in smart cities poses several challenges such as:

- Providing connectivity to devices with high mobility (e.g., high-speed trains and vehicles)
- Connectivity transition from device to network level and vice versa
- Ensuring connectivity to massively deployed devices in the absence of communication networks

Conclusions

This article has presented recent trends and advancements in the IoT-enabled smart cities paradigm. We have devised a taxonomy for IoT-based smart cities based on communication protocols, major service providers, network types, standard bodies, and major service requirements for the understanding of the reader. Based on the conducted study, we have concluded that smart city applications rely on several wireless technologies such as IEEE 802.11p, WAVE, SIGFOX, 6LoWPAN, and LTE/LTE-A. Furthermore, we have studied major open IoT platforms for the ease of researchers. In addition, a number of reported case studies of several of the newest IoT deployments and research projects have been presented to reveal an increasing trend of IoT deployments. In the end, we have unearthed several open research issues such as multi-vendor interoperability, low cost, low power consumption, and security, which demand considerable attention from our research community.

Acknowledgements

We especially thank the late Prof. Dr. Carmelita Görg, former head of ComNets, University of Bremen, Germany, for all her support and guidance. Furthermore, we thank the International Graduate School for Dynamics in Logistics, the doctoral training group of LogDynamics, University of Bremen, for financial support of this work. M. Imran's work is supported by the Deanship of Scientific Research at King Saud University through Research Group No. (RG # 1435-051).

References

[1] A. Zanella *et al.*, "Internet of Things for Smart Cities," *IEEE Internet of Things J.*, vol. 1, no. 1, 2014, pp. 22–32.
[2] J. Gubbi *et al.*, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, 2013, pp. 1645–60.
[3] A. Gluhak *et al.*, "A Survey on Facilities for Experimental Internet of Things Research," *IEEE Commun. Mag.*, vol. 49, no. 11, Nov. 2011, pp. 58–67.
[4] J. Jin *et al.*, "An Information Framework for Creating a Smart City Through Internet of Things," *IEEE Internet of Things J.*, vol. 1, no. 2, 2014, pp. 112–21.
[5] N. Mitton *et al.*, "Combining Cloud and Sensors in a Smart City Environment," *EURASIP J. Wireless Commun. and Net.*, vol. 2012, no. 1, 2012, pp. 1–10.
[6] I. Ganchev, Z. Ji, and M. O'Droma, "A Generic IoT Architecture for Smart Cities," *25th IET Irish Signals & Systems Conf. 2014 and 2014 China-Ireland Int'l. Conf. Info. and Commun. Technologies*, 2013, pp. 196–99.
[7] R. Ratasuk *et al.*, "Narrowband LTE-M System for M2M Communication," *IEEE VTC-Fall*, 2014, pp. 1–5.
[8] P. Papadimitratos *et al.*, "Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation," *IEEE Commun. Mag.*, vol. 47, no. 11, Nov. 2009, pp. 84–95.
[9] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A Comparative Study of Wireless Protocols: Bluetooth, Uwb, Zigbee, and Wi-fi," *33rd Annual Conf. IEEE Industrial Electronics Society*, 2007, pp. 46–51.
[10] X. Lin, A. Adhikary, and Y.-P. E. Wang, "Random Access Preamble Design and Detection for 3GPP Narrowband IoT Systems," arXiv preprint arXiv:1605.05384, 2016.
[11] A. Botta *et al.*, "Integration of Cloud Computing and Internet of Things: A Survey," *Future Generation Computer Systems*, vol. 56, 2016, pp. 684–700.
[12] S. Sicaria *et al.*, "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Computer Networks*, vol. 76, 2015, pp. 146–64.
[13] C. Levy-Bencheton and E. Darra, "Cyber Security and Resilience of Intelligent Public Transport," tech. rep., ENISA, Dec. 2015.
[14] World Economic Forum Industrial Internet Survey, "Industrial Internet of Things: Unleashing the Potential of Connected Products and Services," tech. rep., Jan. 2015.
[15] I. Vilajosana *et al.*, "Bootstrapping Smart Cities through a Self-Sustainable Model Based on Big Data Flows," *IEEE Commun. Mag.*, vol. 51, no. 6, June 2013, pp. 128–34.

Biographies

Yasir Mehmood (ym@comnets.uni-bremen.de) received his Master's in electrical (telecommunications) engineering from the Military College of Signals (MCS), National University of Science and Technology (NUST) Islamabad, Pakistan. He is currently a doctoral researcher at the Sustainable Communication Networks (ComNets) research group, University of Bremen, Germany, in the framework of the International Graduate School (IGS) for Dynamic in Logistics (a doctoral training group at the University of Bremen). His major research area includes cellular communications, mobile M2M communications, and the cellular Internet of Things.

Farhan Ahmad (f.ahmad@derby.ac.uk) received his B.Sc. degree in electronics engineering from COMSATS Institute of Information Technology, Abbottabad, Pakistan, and his M.Sc. degree in communication and information technology from the University of Bremen in 2009 and 2014, respectively. He is currently a final year Ph.D. student in computer science and a postgraduate teaching assistant at the College of Engineering and Technology, University of Derby, United Kingdom. His research focuses on cyber security, risk-assessment, and trust in vehicular networks, M2M communications, and the Internet of Things.

Ibrar Yaqoob (ibraryaqoob@siswa.um.edu.my) received his B.S. (Hons.) degree in information technology from the University of the Punjab, Gujranwala campus, Pakistan, in 2012. He has been pursuing his Ph.D. degree in computer science at the University of Malaya, Malaysia, since November 2013. He won a scholarship for his Ph.D. and is also a Bright Spark Program research assistant. He has published a number of research

In smart cities, the IoT devices can use any available communication networks such as public Wi-Fi, Bluetooth, cellular networks (LTE/LTE-Advanced) and satellites to communicate with the cloud-based application center. However, ensuring connectivity in smart cities poses several challenges.

articles in refereed international journals and magazines . His numerous research articles are very famous and most downloaded in top journals. His research interests include big data, mobile cloud, the Internet of Things, cloud computing, and wireless networks.

ASMA ADNANE (a.adnane@derby.ac.uk) joined the University of Derby as a full-time senior lecturer in Networks and Security from the University of Leicester, United Kingdom, where she was a Knowledge Transfer Partnership (KTP) associate with CrowdLab as their database and security expert. She received her Ph.D. in computer science from the University of Rennes, France. She has published several papers in renowned conferences and journals focusing on ad hoc network security and trust management. She also worked as a research associate/lecturer in France at the University of Rennes, University of Nantes, and ENSI-Bourges. Her research interests include trust management in intelligent transport systems, smart cities, and network security.

MUHAMMAD IMRAN (dr.m.imran@ieee.org) has been an assistant professor in the College of Computer and Information Sciences, King Saud University (KSU), since 2011. He worked as a postdoctoral associate on joint research projects between KSU and the University of Sydney, Australia. He is a visiting scientist at Iowa State University. His research interests include mobile ad hoc and sensor networks, WBANs, M2M, IoT, SDN, fault-tolerant computing, and security and privacy. He has published a number of research papers in refereed international conferences and journals. His research is financially supported by several grants. Recently, the European Alliance for Innovation (EAI) appointed him Co-Editor-in-Chief of *EAI Transactions on Pervasive Health and Technology*. He also serves as an Associate Editor for *IEEE Access*, *IEEE Communications Magazine*, the *Wireless Communication and Mobile Computing Journal* (SCIE, Wiley), the *Ad Hoc & Sensor Wireless Networks Journal* (SCIE), *IET Wireless Sensor Systems*, the *International Journal of Autonomous and Adaptive Communication Systems* (Inderscience), and the *International Journal of Information Technology and Electrical Engineering*. He has served/serves as a Guest Editor for *IEEE Communications Magazine*, *Computer Networks* (SCIE, Elsevier), *MDPI Sensors* (SCIE), the *International Journal of Distributed Sensor Networks* (SCIE, Hindawi), the *Journal of Internet Technology* (SCIE), and the *International Journal of Autonomous and Adaptive Communications Systems*. He has been involved in more than 50 conferences and workshops in various capacities such as Chair, Co-Chair, and Technical Program Committee member. These include IEEE ICC, GLOBECOM, AINA, LCN, IWCMC, IFIP WWIC, and BWCCA. He has received a number of awards such as Asia Pacific Advanced Network fellowship.

SGHAIER GUIZANI (sguizani@alfaisal.edu) received his Ph.D. degree from the University of Quebec, Canada, in 2007. He is currently an assistant professor in the Electrical Engineering Department at Alfaisal University, Riyadh, Saudi Arabia. His research interests include communication networks and security (particularly wireless ad hoc, sensor networks, QoS, wireless sensor network security, and RFID/NFC application and security) and the Internet of Things. He has published a number of research papers in refereed international conferences and journals. He has served/is serving as an Associate Editor for *Security and Communication Networks* (Wiley), the *International Journal of Sensor Networks* (Inderscience), and the *Journal of Computer Systems, Networking, and Communications*. He has been involved in a number of conferences and workshops in various capacities.