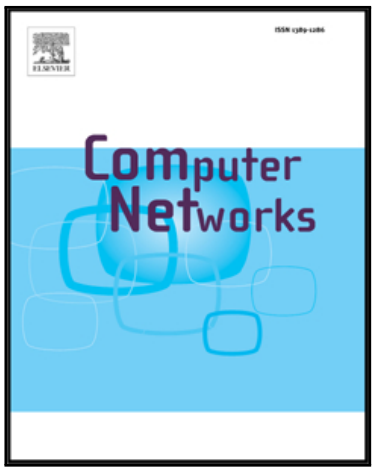
Accepted Manuscript



A Survey of the Sensing, Communication, and Security Planes in Smart City System Design

Hadi Habibzadeh, Tolga Soyata, Burak Kantarci,
Azzedine Boukerche, Cem Kaptan

PII: S1389-1286(18)30653-4
DOI: https://doi.org/10.1016/j.comnet.2018.08.001
Reference: COMPNW 6560

To appear in: *Computer Networks*

Received date: 26 March 2018
Revised date: 8 July 2018
Accepted date: 2 August 2018

Please cite this article as: Hadi Habibzadeh, Tolga Soyata, Burak Kantarci, Azzedine Boukerche, Cem Kaptan, A Survey of the Sensing, Communication, and Security Planes in Smart City System Design, *Computer Networks* (2018), doi: https://doi.org/10.1016/j.comnet.2018.08.001

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

A Survey of the Sensing, Communication, and Security Planes in Smart City System Design

Hadi Habibzadeh [a], Tolga Soyata [a], Burak Kantarci [b1], Azzedine Boukerche [b], Cem Kaptan [b]

[a] *Electrical and Computer Engineering, University at Albany Albany, NY, 12222, USA*
[b] *School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON, K1N 6N5, Canada*

Abstract

The Internet of Things (IoT) era is evolving into sensor initiated, actuation-driven, and machine intelligence-based decision making platform for smart cities. A smart city system aims at seamless and secure interconnection of sensors, actuators, and data processing resources to ensure digital, efficient, and reliable services. In this article, we present a brief planar overview of a smart city system architecture by introducing the application, sensing, communication, data, and security/privacy planes. Tailoring existing communication protocols and infrastructures to bridge massively deployed sensors and data processing/storage resources introduces unique communication challenges for smart cities. Furthermore, co-existence, integration, and control of dedicated and non-dedicated sensors is a grand challenge while IoT sensors continuously push sensory data through the communication medium towards data processing and analysis planes. While pervasiveness and ubiquity of smart city services are ensured by the interaction of communication and sensing technologies, their robustness and resilience calls for customized security and privacy solutions. With these in mind, we focus on sensing/actuation, communication, and security planes of a smart city system and present a comprehensive survey of the challenges and state-of-the-art solutions in each plane. Furthermore, we provide insights for open issues and opportunities in these planes.

Keywords: Smart Cities; Smart Spaces; Security; 5G Networks and Communication; Edge Networks; Internet of Things, Dedicated sensing; Non-dedicated Sensing.

1. Introduction

Increasing individual use of connected smart devices, rapid growth of worldwide urban population, gradual aging of society in many countries as well as the rising demand for sustainable energy resources have given momentum to the emergence of smart cities and smart spaces [1]. Smart city services span a wide spectrum of applications ranging from smart utilities, to smart health, smart transportation, smart governance, and smart environment [2], which Utilize real-time sensing, knowledge engineering, and presentation of the analyzed data in an interpretable format.

To fulfill the requirements of diverse applications and services, a smart city architecture consists of five planes as illustrated in Fig. 1 in a minimalist manner. The *application plane* provides services to the end users for any relevant application such as smart utilities, energy, transportation, health, environment and safety. Serving mobile, home, and corporate sectors, these applications rely on an underlying substrate, which encompasses sensing, communication, data, and security planes as the core of a smart city architecture [3]. The data acquisition (sensing) networks—implemented by utilizing either hard sensors or soft sensors—form the *sensing and actuation plane*; whereas processing, analysis, and storage of data shape the main functionality of the *data plane*. These two planes are bridged by the *communication and aggregation plane*.

Addressing users' growing cognizance about smart city cybersecurity, each component shown in Fig. 1 calls

☆This work was supported in part by the U.S. National Science Foundation grant CNS-1239423, and the Natural Sciences and Engineering Research Council of Canada (NSERC) under Grant RGPIN/2017-04032.

Email addresses: hhabibzadeh@albany.edu (Hadi Habibzadeh [a]), tsoyata@albany.edu (Tolga Soyata [a]), burak.kantarci@uottawa.ca (Burak Kantarci [b]), boukerch@uottawa.ca (Azzedine Boukerche [b]), ckaptan@uottawa.ca (Cem Kaptan [b])

[1]Corresponding author: Burak Kantarci.

ACCEPTED MANUSCRIPT

for security and privacy assurance mechanisms. The challenging task of satisfying these requirements is relegated to the *security and privacy plane*. As shown in Fig. 1, a comprehensive and effective security and privacy plane must be implemented adjacent to every individual building block of this architecture.

The Internet of Things (IoT) is a major enabler for diverse smart applications that involve massive data acquisition and intelligent decision making [4]. Therefore, in the realization of smart cities, the IoT is a bridging component between the sensing devices and the data plane [5, 6]. Indeed, in order for the IoT concept to operate thoroughly, its interface with the local wireless networks, backhaul networks, as well as local wired networks needs to be addressed properly. Furthermore, protocols for reliable and efficient data acquisition methodologies for fusing data are of paramount importance particularly to ensure a robust communication back-end in a smart city infrastructure.

In a smart city architecture, communication back-end is one of the most crucial components, which is responsible for pre-processing and aggregation of the sensory data. Reliability, usefulness and trustworthiness of the data acquired by the communication back-end depends on the effectiveness of the sensing plane. As studied in [2], sensors in a smart city setting can be deployed in either a dedicated or non-dedicated manner; each deployment strategy has its own pros and cons.

Based on the observations above, in this paper, we present a smart city architecture by briefly introducing its building blocks (termed *planes*), namely the *application*, *communication*, *sensing*, *data*, and *security* planes. Upon brief introduction of the architectural building blocks, we move to our main foci, which are the sensing, communication and security planes. In the study of the sensing plane, we present the dedicated and non-dedicated sensing paradigms from the standpoint of various smart city applications. We thoroughly investigate the sensor types, problems experienced by the corresponding smart city applications, existing solutions and the communication technologies used by the sensors. Sensing plane is followed by the communication plane, which is studied in terms of the requirements, implications, and common solutions. We partition the communication plane into several sub-planes to study the communication infrastructure and protocol design for a smart city with fine granularity. These sub-planes include data aggregation, protocol adaptation, and application sub-planes. Besides the back-end functionality, we further review the in-field communication front-end, with an emphasis on the Wireless Body Area Networks (WBAN), Wireless Personal Area Networks (WPAN),

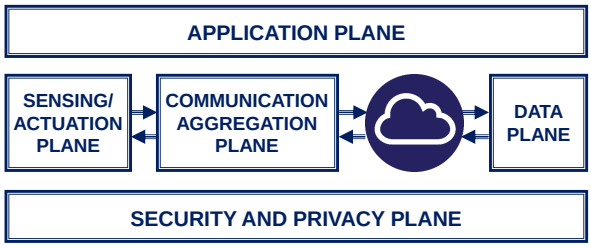


Figure 1: A high-level representation of smart city applications architecture, consisting of five planes: application, sensing, communication, data, and security and privacy. Application and security planes are spread over the other three, indicating their inclusiveness. Although this figure abstracts each plane as a single block, the actual implementation can be distributed.

heterogeneous cellular networks, visible light communications, power line communications, and various existing standards. Lastly, the security plane, as the gluing component among these planes, is presented under two sub-planes, namely crypto-level and system-level security solutions. For each of these three planes, a thorough discussion on the open issues, challenges, and opportunities for future research are presented.

The rest of the paper is organized as follows. In Section 2, we introduce the smart city architecture, consisting of its five planes, and we define the requirements and functionality of each plane. In Section 3, we study the sensing plane, followed by the communication plane in Sections 4 and 5. In Section 6, we review the security plane and its interaction with the other four planes in the smart city architecture. Finally, in Section 7, we give future directions and concluding remarks in Section 8.

2. Smart City System Architecture

As shown in Fig. 2, an assembly of five collaborative (yet independent) planes form the complex organism of modern smart cities; sensing, communication, data, and security and privacy planes shape the backbone of the system, while the application plane brings the benefits of smart cities to their citizens via a rich variety of services such as smart health, smart transportation and driving, smart lighting, etc. To take advantage of the existing synergies among various applications, most recent implementations of smart cities now incorporate a sixth abstraction plane that ensures interoperability among individual applications, thereby taking a major step toward realization of a uniform smart city *ecosystem*. In this section, however, we focus our investigation on (now classic) architecture depicted in Fig. 2 as the fundamental framework of any smart city system.

ACCEPTED MANUSCRIPT

2.1. Application Plane

Gluing all components of a smart city together, the application plane determines to what end resources and data must be utilized in a modern city. Designing smart city services typically begins by defining the applications; other planes are then configured and tweaked to meet the requirements of this plane. The design process, however, is not limited to these technical considerations. Being the highest level (and most abstract) component of the architecture, application plane inexorably involves multiple exogenous social aspects as well. It is within this context, where perceived entertainment, educational, security, and safety value of an application can be evaluated. Furthermore, the imminent fusion of smart city applications into a uniform framework is chiefly fueled by these social variables, although technical breakthroughs in other planes have also contributed to this transition. In this section, we study a select number of applications to investigate their interplay with social and technical aspects of the architecture shown in Fig. 2.

Smart environment (not to be confused with environmental monitoring) aims to facilitate the interaction between humans and their surroundings by imparting machine intelligence into an environment, thereby creating a responsive and adaptive ambiance. For example, by feeding data collected from microphones and cameras into an emotion recognition algorithm, a *Smart Classroom* can help instructors and students adjust their presentation to the mood of the audience [7]. Smart environment applications typically embody a diverse range of sensing devices, which further gives rise to heterogeneity in sensing, communication, data, and security planes. Guaranteeing interoperability among these components as well as intertwining them with existing infrastructure are the major challenges in these applications [8].

Smart home and smart building are two representative applications within the smart environment, which use an ensemble of sensors and actuators that are employed in homes to improve energy consumption [9], promote healthy lifestyles [10], ensure security [11], etc, which inevitably ties smart homes with other smart city applications such as **smart grid** and **smart healthcare**. For example, as discussed in [10], force sensors incorporated into floor tiles can help with detecting fall incidents, counting steps, and monitoring resident's weights and gaits. Aside from their many advantages, smart homes are sometimes perceived by citizens as a invasion to their privacy and security [12, 13].

Smart surveillance has also been subject to impressive progress in the recent years, mostly due to advancements in image processing and growing ubiquity of low power communication techniques. For example, being compatible with IBM Db2 [14] and IBM WebSphere [15], IBM Smart Surveillance System (S3) can automatically extract information from surveillance cameras and issue alerts and notification when an anomaly is detected. In a different approach, the study conducted in [16] uses low-power and inexpensive BLE tags to track individuals. Utilizing low power demand of BLE, each tag can operate for a year when powered by a coin-battery.

Smart transportation establishes connectivity among vehicles, citizens, and infrastructure to improve road safety, reduce traffic, and increase fuel efficiency [17]. Reliability, low-delay connectivity and processing, mobility support, and robustness to noise and interference are major requirements of smart transportation applications. Consequently, the authors in [18] select BLE over ZigBee for their implementation of an Intra-Vehicular Wireless Sensor Network (IVWSN), which can decrease production costs and fuel consumption of vehicles by reducing weight. An emerging trend in smart transportation can be ascribed to the proliferation of electric vehicles (EVs), which links this domain to smart grid and renewable energy sources [19]. Particularly, within the context of smart parking, the authors in [20] propose an online intelligent demand coordination for plug-in electric vehicles (PEVs) in distributed systems. To achieve this goal, the authors employ a fuzzy expert system for parking lots, which maximizes driver satisfaction without violating the operational constraints of the power grid under coordinated demand.

In response to challenges such as population aging and widespread outbreak of chronic diseases such as diabetes and obesity, smart healthcare applications employ noninvasive, accurate, and inexpensive sensors to provide *personalized* and *continuous* monitoring. The proposed system in [21] collects body heat data using RFID body temperature sensors. As battery limitation of sensors is a major challenge in continuous monitoring, the authors incorporate ambient energy harvesting in the sensors, thereby enabling them to harvest a portion of their power. Another study [22] describes a glucose monitoring system based on implantable electrochemical sensors that communicate using the 13.56 MHz RFID frequency band. Backscattering can be used to power RFID sensors [23], which addresses the intractable problem of low power availability for in-vivo sensors. Smart healthcare is one of the fastest growing fields in smart city; nonetheless, the path toward realization of such systems is obstructed

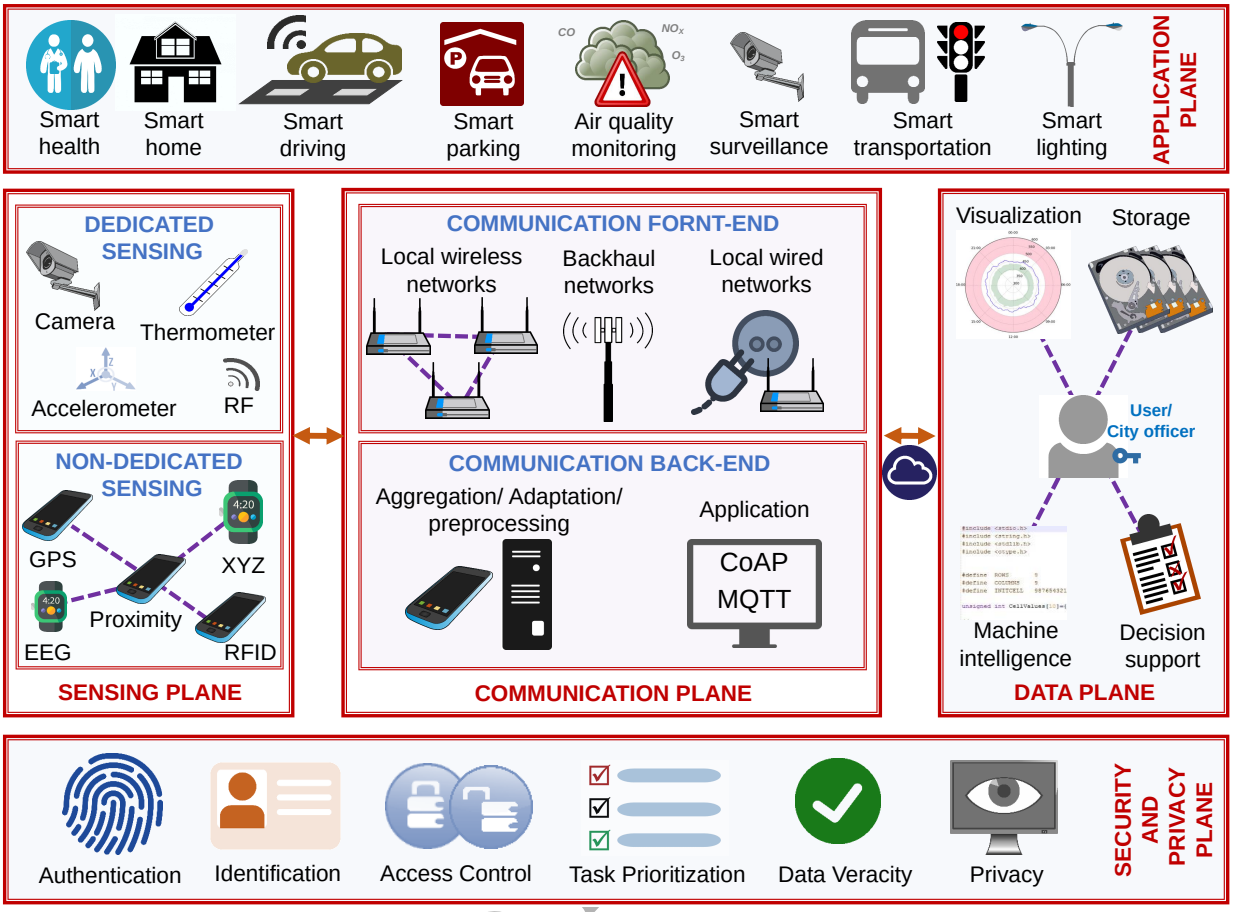


Figure 2: An expanded depiction of Fig. 1, which demonstrates smart city architecture comprising five planes. **(i) Application plane** is the social link between smart city systems and city's citizens. **(ii) Sensing plane** involves data acquisition through either dedicated or non-dedicated sensing. **(iii) Communication plane**, bridges the gap between data transmission to the cloud. **(iv) Data plane** performs various data processing techniques to obtain useful information from the bulk of raw data. **(v) Security plane** objective is to ensure security and privacy of every single plane.

with security and privacy concerns [24, 25, 26].

Being the precursor of smart city services, smart grid employs machine intelligence to improve grid's manageability and reliability, while reducing wastes and expenses. Smart microgrids are an important component of smart grids. A microgrid can operate in the islanded or non-islanded mode depending on available energy capacity as well as availability of distribution lines. A reliable overlay topology design to interconnect the microgrids in the islanded mode is proposed in [27], in which the authors formulate a mixed integer linear programming model depending on the predicted demand profile during a day; their objective is to maximize the duration of remaining disconnected from the power grid while possibly trading energy among the interconnected microgrids. The growth of smart grids is also closely tied to proliferation of Advanced Metering Infrastructure (AMI) fueled by novel communication breakthroughs such as Low Power Wide Area Networks (LPWAN).

2.2. *Sensing Plane*

Evolution of smart city sensing has completed three milestones [28]. The first generation involved a limited number of sensing devices in each application. The emergence of the second generation was mostly fueled by the introduction of *data fusion*, where valuable insight could be gained by combing data from a wide spectrum of sensors. The latest (third) generation now fuses information from external sources such as databases and research as well as exogenous applications. Although this evolution could be partly associated with advances in data processing and communication techniques, the sensing plane itself has been

ACCEPTED MANUSCRIPT

subject to major breakthroughs. More eminent than other, advances in VLSI design have been constantly reducing the energy consumption and the cost of sensors, while increasing their on-node computation capability. Other available technologies such as flexible circuit boards [29], bio-compatible sensing materials [30], and RF-based sensing [31] have also paved the path for the evolution of smart city sensing. However, nothing has revolutionized this plane more than the introduction of crowd-sensing, where participating volunteers use non-dedicated sensors of their portable devices such as smartphones to record a variety of parameters [2, 32, 33], substantially decreasing recurring and non-recurring expenses.

Sensing in smart cities faces numerous challenges, many of which stem from the limitation of traditional Wireless Sensors Networks (WSNs). Insufficient power availability is the root cause of many of these challenges. Although energy harvesting techniques can mitigate this problem [34, 35, 36], their efficacy remains limited to satisfy other requirements such as cost, portability, and size. Additionally, sensing plane suffers from high fragmentation and heterogeneity, which, in turn, complicates guaranteeing interoperability and expandability. Maturing crowd-sensing solutions can satisfy many of these requirements; nonetheless, incentivizing participants still remains a moot problem [37, 33]. **Indeed, mobile-crowd-sensing experiences further challenges. Amongst these are ensuring battery efficiency of smart mobile devices, dependability of crowd-sensed data, privacy of participants, and effective incentives to promote user participation. Furthermore, from an architectural standpoint, new networking paradigms such as network function virtualization and mobile edge computing are considered to be among the enablers of mobile crowd-sensing [38].** We provide a detailed discussion of this plane in Section 3.

2.3. *Communication Plane*

Communication plane provides a conduit for data to channel from the in-field sensing plane to the cloud-based data plane and vice versa—when commands and firmware updates are streamed from the cloud to field devices. As depicted in Fig. 2, we have divided the functionality of the communication plane into two sub-planes: **(i)** *Communication Front-End* establishes a connection between every sensing device and a concentrating point (typically, an Access Point (AP) or a gateway), and **(ii)** *Communication Back-End* provides a backhaul link between these concentrating points and the cloud. It is evident that this architecture implies a hierarchal approach, which is now the de facto standard for smart city communication. This multi-level implementation, however, is more mature than classic clustering methods developed for traditional WSNs [39]. This non-flat approach relies on relatively more powerful field devices to provide a variety of services such as data aggregation, pre-processing, and protocol adaptation. Communication plane is the focus of this paper and we investigate the requirements and enabling technologies of this plane in further detail in Section 4 (in-field front-end) and Section 5 (back-end).

2.4. *Data Plane*

In a modern smart city application, data plane provides a hardware/software framework to host machine intelligence, which assists city officers and citizens with decision-making within the context of an application (for example, providing recommendations for saving energy in a smart home implementation [40] or helping physicians to detect the onset of a heart failure [41]). Therefore, while maintaining compliance with requirements pertaining to big data 5Vs (veracity, velocity, volume, value, and variety) [42], the data plane must offer at least three services to its corresponding planes: data analytics and machine intelligence, data storage and processing, and data visualization.

Lumping the functionality of the data plane into single component, as shown in Fig. 2, does not necessarily imply centralized implementation. In fact, both centralized cloud-based and distributed edge-based implementations are fairly common in smart cities. The former oftentimes offer superior manageability, applicability, and reliability, while the latter typically excels in scalability and latency by reducing the physical distance between the field devices and the data plane [43]. For example, the infrastructure monitoring system proposed in [44] adopts a cloud-based architecture to satisfy its prime requirements such as large-scale data, real-time processing, and reliability. To further increase the robustness of the system against occasional failures, the authors use replication techniques; however, such solutions can adversely affect resource requirements of the application. Alternatively, research conducted in [45] proposes an edge-based platform with embedded scheduling techniques, which reduce energy demand and provide Quality of Service (QoS) assurance. This solution allows participants to share their storage and processing resources over a Peer-to-Peer (P2P) network. While such an edge-based implementation can dynamically adjust to ever-changing demands of the network, it introduces a wide array of challenges such as heterogeneous device

ACCEPTED MANUSCRIPT

properties, free riders, security and privacy concerns, etc [46, 47].

After structuring either a cloud-based or edge-based (or hybrid) architecture, machine learning and deep learning algorithms can be applied to raw data to extract useful information. For example, the authors in [48] use Support Vector Machine (SVM), as a supervised learning technique to distinguish various physical activities (e.g., walking, running, and standing) based on features obtained from Received Signal Strength Indicator (RSSI) of RF signals. Considering that SVM is typically used for binary classification, authors adopt Winner-Takes-All (WTA) to extend the outcome set of their classifier. A Random Forest (RF) comprising 400 trees is grown in [49] to provide highly localized Air Quality (AQ) monitoring in smart cities. It correlates historical data with status of traffic and topology of the area to classify AQ into six categories. Taking advantage of many benefits of emerging deep learning, the study in [50] applies Convolutional Neural Networks (CNN) to license-plate recognition problem. The proposed system can address a multitude of challenges associated with image-based plate recognition including heavy traffic, ambient occlusion, and plates' physical damages and imperfections.

Finally, unless through an effective visualization methodology, extracted information from bulk of raw data cannot be of assistance to city officers and residents. Representing the interwoven dynamics of data, however, is proven to be a difficult task, particularly considering the impressive size of the data collected and processed in the data plane. Indeed, knowing how the requirements of applications differ and different users seek different information, effective visualization techniques must be *personalized* and be made *hierarchal*.

2.5. Security Plane

A stream of attacks targeting various applications such as smart healthcare and smart transportation have recently given rise to discussions regarding the security and privacy considerations of IoT and smart cities [51, 52, 53]. These attacks can be mostly attributed to developers failing to create comprehensive security preserving mechanisms spread over all other planes of the architecture. Instead, they often emphasize the security of the communication plane (as off-the-shelf security solutions are already available and expedient to employ), while neglecting sensing and data planes. With ever growing influence of smart cities in our lives, the repercussions of such cyber-threats can soon go beyond their usual "extortion" scope and lead to catastrophic outcomes, paralyzing the city and even endangering the lives and safety of citizens. We provide an in-depth discussion of security and privacy aspects of smart cities in Section 6.

3. Sensing Plane

In a smart city application, a set of sensors are deployed within the city to facilitate the collection of data for that application; these sensors are *dedicated* to that application and are not typically shared with any other application. Alternatively, in the emerging mobile crowd-sensing concept [32], a set of participants (e.g., smartphone users) can perform the required sensing for an application, which significantly reduces the amount of investment that the city has to make for that application. Since the sensors that are embedded into the users' smartphones are not dedicated to any specific application, the users are free to participate any time they want. The usage of sensors in this way is termed *non-dedicated sensing* [2]. Despite its advantages in reducing the recurring and non-recurring expenses, this type of sensing brings about challenges in incentivizing the users [54, 33], as well as guaranteeing a certain coverage area. **Moreover, user privacy and data trustworthiness in mobile crowd-sensing are still two important barriers that impede a large scale adoption of mobile crowd-sensing [55].** The sensing plane consists of either one (or a combination of) these two types of sensors. In this section, we study both dedicated (Section 3.1) and non-dedicated (Section 3.2) sensing.

3.1. Dedicated Sensing

While many different types of dedicated sensors exist, we investigate six different categories here.

3.1.1. Traffic Sensors

Traffic sensors are used in various applications such as drive support, traffic monitoring, vehicle monitoring and even pedestrian monitoring. All of these applications fall under the umbrella of intelligent transportation systems.

In [56], a Cooperative Road Infrastructure Systems for Drive Support, namely iRoad, is proposed that aims at improving road safety. In the proposed infrastructure, road marking units (RMUs) are deployed over the road surface to sense several phenomena such as directional surveillance of the moving vehicles, tracking critical distances between the cars and the queue end. The system consists of sensors, actuators, a processing module, radio communication unit, and an energy supply block. The transmission unit utilizes IEEE 802.15.4

ACCEPTED MANUSCRIPT

transceivers. Road surface based sensors (e.g. inductive loop detectors) can also be used for traffic flow prediction. In a follow-up work, the authors in [57] use fuzzy neural networks for flow prediction by using the sensory data acquired from inductive loop detectors. Another study that also uses on-road loop detectors aims to find the statistical links between turbulent traffic conditions with the ultimate goal of minimizing the crash events [58].

Detection and classification of the vehicles is another application area that requires multimedia traffic sensors in the sensing plane [59, 60, 61]. The authors in [59] present an application that is executed in six stages, namely segmentation, region tracking, dimensional recovery of the vehicle, identification of a vehicle, tracking of a vehicle, and finally the classification of a vehicle. In another similar application, the authors in [62] estimate vehicle density in a region by utilizing a Kalman filter-driven approach on data that is acquired from multimedia sensors (e.g., cameras). In [63], the authors aim to estimate the density of a crowd by using the same method. The usage of cameras and infrared sensors are reported to be sensitive to traffic and weather conditions whereas piezoelectric sensors and inductive loops require high installation and maintenance costs. Therefore, for the same application of vehicle classification, the study conducted in [64] propose to use accelerometers to detect vibrations and magnetometers to measure the speed of vehicles. Furthermore, by running an Axle Detection algorithm on the cloud, the authors aim to estimate the number and spacing of the axles.

As for driver assistance, detecting stress levels of the drivers in real time during driving utilizes ECG, EMG, skin conductivity, and respiration sensors [65]. By using the data acquired from these sensors, two types of analysis are conducted: **(i)** classifying the stress level of the driver through a machine learning algorithm, **(ii)** continuous quantification of the driver's stress level.

In [66], a computer vision-based system is presented to automatically monitor and analyze the status of an intersection. The sensor plane requires multimedia sensors (e.g., cameras), and a Hidden Markov Model (HMM) is utilized to analyze various event patterns of behavior for each vehicle in order to detect/classify events such as bumping, passing, and jamming.

As mentioned earlier, traffic sensors are also used to detect and track pedestrian behavior. This requires the use of multimedia sensors so that a combination of the shape, texture, and depth can be used to acquire data that can be fed into a classifier [67].

3.1.2. Smart Environment Sensors

Smart environment sensors measure the environmental conditions (living conditions) of a user's living environment (e.g., home). As an example smart environment application, the MavHome project in [68] employs a dedicated sensor network to detect light, humidity, temperature, smoke, gas, and motion to ensure user comfort. Besides sensors to measure ambient data, infrared sensors are also deployed to track inhabitant localization.

Aiming to implement a human recognition system, the work in [69] estimates the health condition and lifestyle of individuals by running data mining algorithms on the data acquired from accelerometers, RFID tags, and multimedia sensors. A similar problem is investigated in [70] by deploying RFID tags and a dedicated wireless sensor network in a smart home setting.

To ensure smart environments, actuators can also be deployed along with sensors. For instance, the authors [71] introduce a smart environment system using three building blocks as follows: **(i)** Smart objects with RFID tags and appliances with sensor network functionality; **(ii)** a home server connecting all smart devices; and **(iii)** robots (i.e. actuators) collaborating with the environment.

Smart environment applications can also utilize external dedicated sensors. CitiSense is a typical application to improve geospatial environmental assessment of air quality using wearables [72]. The wearables use three electrochemical gas sensors, which are hardwired to monitor exposure to CO, NO_2, and O_3. Additionally, sensors for measuring humidity, temperature, and barometric pressure are also included. The sensor board communicates with the user's smartphone via Bluetooth Low Energy (BLE).

3.1.3. Smart Water Sensors

Water sustainability is crucial in a smart city. The authors in [73] investigate the impact of smart metering on water management and planning. Furthermore, an integrated knowledge management system that brings together smart metering, water consumption data, wireless communication networks, and information management systems is also crucial to provide information to consumers and utilities. Tracking water consumption through smart metering can also be used for water leakage detection by applying intelligent sensory data analysis techniques [74]. The underlying communication technology to handle smart metering communication in such scenarios is also a research concern; the authors in [75] show that a Radio Frequency (RF)-based mesh system using frequency hopping spread

ACCEPTED MANUSCRIPT

spectrum (FHSS) and routing the information via geographic routing can ensure reliable delivery of the smart metering data in these scenarios.

3.1.4. Smart Metering Sensors

Smart metering was presented in Section 3.1.3 for smart water management. However, smart metering can also be used for smart power management, e.g., in smart grids and smart microgrids. The data that is collected by smart metering is mainly the real-time or near-time measurement of the electricity usage and generation. An example for an automated meter reading system is the QUNDIS AMR, which was introduced in 2009, and was capable of metering in the following three levels: **(i)** Field devices level, **(ii)** LAN-level, and **(iii)** WAN-level [76]. In smart metering, the main challenges include the possibility of an existing sensor network being hampered by communication interfaces, lack of programmability, and insufficient adaptability to novel scenarios because of the availability of the aggregate consumption values, rather than individual meter values. To cope with these challenges, the authors in [77] propose a sensor platform that is based on low-power hardware and a reprogrammable microcontroller; due to the compatibility of the radio receivers of the platform with IEEE 802.15.4, integration with smart buildings is also possible in this proposal.

Smart metering sensors and smart grid sensors are highly related. In [78], the authors study the integration of smart meters and smart grid sensors with the objective of an Automatic Voltage Control Strategy combined with the wireless communication systems in smart metering.

Another application area of smart meter sensors is the monitoring of household assets that use home area networks and the smart meter infrastructure. In [79], a holistic system that consists of a microcontroller unit, a motion sensor unit, and a communication unit registered to a home network is presented. The system tracks module location and raises alerts in the presence of a module move.

3.1.5. Smart Grid Sensors

Application, opportunities, and challenges of WSNs for electricity power systems have been comprehensively studied in [80]; this study also presents experimental research on the statistical characterization of wireless channels under various environments including a 500-kV substation, an industrial power control room, and an underground network transformer vault. The smart grid sensors used in the study are IEEE 802.15.4-compliant operating in the 2.4-GHz frequency band. An empirical evaluation and field tests reveal the spatiotemporal impacts of electric power system environments on low-power wireless communication and show that LQI (link quality indicator) can be a reliable metric for link-quality assessment.

Partial discharge (PD) monitoring is crucial in the implementation of the smart grid in order to effectively assess the insulation conditions of high voltage equipment. The authors in [81] present a PD measurement method which is used to collect data from an electricity distribution substation, and show that integration of Fast Fourier Transform (FFT)-based de-noising into the smart PD sensors can enable effective remote monitoring of the smart grid.

Electrification of transportation is another smart grid aim. To integrate the transportation system with the smart grid, the authors in [82] introduce a new type of sensor called the smart "stick-on" sensors, which are low-cost, self-powered, and universal. Stick-on sensors can be used to monitor various smart grid assets such as cables, conductors, transformers, disconnect switches, and so on. Furthermore, ambient energy harvesting is also possible with stick-on sensors.

Demand management is one of the earliest problems studied in smart grid research. The authors in [83] propose a wireless power meter sensor network to monitor the power consumption of household appliances and provide predictions for the next day. Note that the same approach can be extended from a household to the power grid to achieve automated reconfiguration.

3.1.6. Smart RFID Sensors

RFID devices can contain one or more sensors to sense data and can also receive data transmitted from a remote concentration device; they can also log and store data [84]. There are many application areas of RFID sensors in smart environments. For instance, smart labeling of products is a very popular application area. To accomplish this goal, printed sensors on flexible polymeric foil can be used for radio frequency identification. The authors in [85] argue that flexible foil with multi sensors can be low-cost, low power, and can be used for environment monitoring including gases, humidity, and temperature. Another example use case for passive and semi-active RFID tags is in food logistics.

The use of passive RFID tags can also enable the smart skin technology, which incorporates cognition and intelligence to monitor environmental parameters as presented in [86]. Passive RFID-based sensors are capable of power harvesting, sensor integration, processing, and modulation/demodulation without requiring a

ACCEPTED MANUSCRIPT

power supply, such as a battery [23]. In [86], the authors conceptualize a nanotechnology-enabled gas sensing platform that uses passive RFID tags, which leads to zero-power operation and high sensitivity.

Tracking the real time movements of people is also possible via RFID sensing. The authors in [87] present a sensor network based on RFID wireless communication, which enables the acquisition of user movement information in a transparent and reliable way in a dynamic environments.

3.2. Non-dedicated Sensing

With the wide adoption of smart mobile devices, mobile phone sensing has appeared as a viable solution to complement the dedicated sensor networks; smartphones are equipped with accelerometers, gyroscopes, GPSs, microphones, cameras and several other sensors that can be used for applications such as health care, environmental, and traffic monitoring and management [91]. For instance, Google's Science Journal application [92] is a typical example of using built-in smartphone sensors for real time monitoring of environmental parameters such as light and sound. Based on the mobile phone sensing concept, Sensing as a Service (S^2aaS) was first introduced by Sheng et al. in [93] as a cloud-inspired distributed sensing model. In [94], Cardone et al. provided a processing core of smartphone-based Mobile Sensing Technology (MoST); they particularly focused on activity detection, geo-localization, and geo-fencing in smart cities. Ericsson's consumer insight summary study [95] reported smart citizens as the major drivers of smart cities. In [96], the authors defined smart citizens as mobile device users who actively contribute to the collection of sensor data for smart city monitoring by dedicating the sensing and processing resources of their mobile devices. Khan et al. classify city-wide non-dedicated sensing under two categories, namely *participatory sensing* and *opportunistic sensing* [91]. The former denotes active user involvement in the sensing process including accepting/declining the application requests to access their mobile phone sensors, while the latter does not require any intervention during all stages of sensing.

Also known as *crowd-sensing*, non-dedicated sensing applications in smart city settings are various. Magnetometers in smartphones can be used to detect available parking spots in a populated area, and can be crowd-sensed to inform drivers; a simple testbed to verify this idea was Ciudad Real, Spain [88]. Indeed, one of the most common non-dedicated city-wide sensing application areas is public transportation. GPS sensors in smartphones are used to acquire accurate location data that is used over Google Maps in order to obtain spatio-temporal traffic information in the city [89]. Smart tourism is another field that can be improved by utilizing crowd-sensed data from non-dedicated sensors. In [90], a framework called Tresight is introduced for the city of Trento in Italy. Tresight deploys wearable bracelets to sense visitor activity (via accelerometers), environmental conditions (through temperature and humidity sensors), and location information for each monitored region. By using the multidimensional crowd-sensed data from visitors, as well as the information collected from WiFi hotspots, Tresight builds a context-aware recommendation system. **Community health is another field that crowd-sensing can benefit. For instance in [97], Allergymap, an integrated mobile health-crowdsensing platform is presented to investigate and manage diseases that are the consequences of allergic reactions. To this end, Allergymap consists of four planes, namely the crowdsourcing plane to acquire subjective inputs from users, the crowd-sensing plane to acquire environmental sensory data in large scale, and the analytics and visualization planes to investigate allergens, irritants and methods to improve patient experience and well-being.**

The authors in [98] identify three primary components for crowd-sensing systems: (i) *tasks*, (ii) *servers*, and (iii) *crowd*; they provide a qualitative classification of crowd-sensing tasks under three categories: tasks whose marginal contribution is proportional to their size, tasks whose marginal contribution is proportional to the progress, and tasks whose marginal contribution is reversely proportional to their progress. With these in mind, the authors propose a crowd-task matching policy that aims at the efficiency of task execution and effective budget management. They conclude that to meet the budgetary and task execution efficiency targets, quantitative optimization of participants with the highest quality, the progress of task execution, and the impact of communication network have to be taken into account.

Development of user centric approaches are of paramount importance. The authors in [99] tackle the utility and dependability effects of delegating finalization of user-task matching to participating devices. Indeed, this is expected to be supported by edge computing functionality. Battery limitation of smart mobile devices is one of the barriers against a wide adoption of crowd-sensing systems. In [100], the authors propose to consolidate continuous user profiling with effective incentives to ensure maximum platform utility and minimum

ACCEPTED MANUSCRIPT

Table 1: Overview of Sensing Plane Applications, Sensor Types and Communication Interfaces

Sensing Application: Sensor Type	**Example Objectives and Problem**	**Communication**
Smart Transportation: Road Marking Units (RMU) [56] Inductive Loop Detector (ILD) [57] On-Road Loop Detector [58] Multimedia Traffic Sensor [59, 60] Infrared Sensors [62] Accelerometers/ Magnetometers [64] ECG/ EMG/ Respiration Sensor [65] Non-Dedicated Availability: ✗	Road Safety [56, 57, 58] Vehicle Classification and Identification [59, 61, 62] Driver Assistance [65] Intersection Monitoring [66] Pedestrian Behavior [67]	IEEE 802.15.4 [56, 57, 58] / Hard-wired [65, 66, 67]
Smart Environment: IR, RFID, Multimedia Sensors [68] Electrochemical Gas Sensors, Humidity, Temperature, Barometric Pressure [72] Non-Dedicated Availability: ✗	Localization/Activity Recognition [68] Smart Home Monitoring [71] Environmental Monitoring [72]	Common Object Request Broker Arch. RFID and Hard-Wired [68] / RFID Tags [71] Bluetooth [72]
Smart Water: Smart Metering Sensors [74, 75] Non-Dedicated Availability: ✗	Water Leakage Detection	RF-Based Mesh
Smart Metering: Smart Metering Sensors [76, 79] Non-Dedicated Availability: ✗	Automatic Voltage Control [76] Monitoring Household Assets [79]	Ethernet, WLAN, IEEE 802.15.4 [76] / IEEE 802.16, Satellite, RF [79]
Smart Grid: Partial Discharge Sensor [81] Smart Stick-On Sensors [82] ACmes [83] Non-Dedicated Availability: ✗	Partial Discharge Monitoring [81] Transportation Electrification [82]	Coax, Cellular [81] IEEE 802.15.4 [82]
Smart RFID Sensor: Printed Gas, Humidity, Temperature Sensors [85] Gas Sensors, RFID Tags [86, 87] Non-Dedicated Availability: ✓	Environment Monitoring [85] Smart Skin Technology [86] Tracking People [87]	RFID
Smart Parking and Driving: Magnetometers Smartphone GPS Sensor Non-Dedicated Availability: ✓	Available Parking Spots Detection In A Populated Area [88] Spatiotemporal Traffic Data Acquisition [89]	Cellular / WiFi
Smart Tourism: Wearable Accelerometers, Temperature, Humidity Sensors [90] Non-Dedicated Availability: ✓	Visitor Activity Sensing, Environmental Monitoring, Location Recommender [90]	WiFi

battery drain. The proposed scheme, Sociability-Oriented and Battery Efficient Recruitment for Mobile Crowd-Sensing (SOBER-MCS) exploits social activity signatures of the participants to predict a map of battery usage-social activity for every participant so as to make wiser decisions in the recruitment process.

It is worth noting that building a federation of

ACCEPTED MANUSCRIPT

crowd-sensing platforms experiences several *human-in-the-loop* challenges. These include security of the crowd-sensed data, privacy of the participants, and anonymity of participation. The study in [101] presents a clear roadmap for the integration of different crowd-sensing platforms by considering these parameters. This integrative vision is introduced as Testbed as a Service in [102], particularly as a key enabler for IoT experiments.

4. Communication Plane

The communication plane provides the link between in-field data sensing and the data plane. Functionality of this plane can be divided into three categories: **(i)** *In-field communication front-end* embodies resource-constrained sensing nodes that collect raw data from various types of sensors and forward them to in-field gateways or Access Points (APs) over either a wireless or wired connection. **(ii)** *Aggregation and adaptation* involves cluster heads, gateways, cloudlets, and APs, which are relatively more computationally-capable than the field sensors. In certain cases, with the assistance of a *cloudlet*, cluster heads perform preliminarily pre-processing and aggregation to further decrease energy consumption and facilitate the fulfillment of QoS objectives. *Adaptation* functionality interfaces heterogeneous network technologies that co-exist in a typical smart city implementation. It ensures interoperability with the internet, through which the accessibility to the cloud and its numerous services is established. Finally, **(iii)** *Network application* component standardizes message exchange among centralized or distributed cloud-based servers and field devices, regardless of their vendor, topology, and functionality.

We analyze the fundamental requirements of smart city communication plane in Section 4.1 and discusses how IoT communication is differentiated from legacy WSNs. In Section 4.2, we elaborate on the implementation details of smart city communication architecture. Data aggregation, adaptation, and communication functionalities are detailed in Section 4.3, Section 4.4, and Section 4.5, respectively. We dedicate Section 5 to a detailed study of the in-field network front-end.

4.1. Communication Requirements

Communication plane bridges the gap between sensing and data processing. This functionality evidently resembles the objectives of traditional Wireless Sensor Networks (WSN). However, unlike WSNs, smart city communication platforms must ensure that every single device in the network is uniquely *identifiable* and *addressable* through the internet, which makes internet compatibility the underlying requirement of this plane. Aside from this, smart cities' scale and dynamism also entail additional requirements. The former poses interference and co-existence challenges, while the latter complicates the implementation by necessitating complementary services such as plug-and-play and mobility. Particularly, co-existence among a wide spectrum of protocols and implementations is proven a festering complication. The first generation of smart city applications neglected expandability and compatibility to generate a set of working applications rather quickly. The absence of a universal standard has exacerbated the situation, leaving the smart city communication plane an amalgamation of incompatible protocols and standards. The diffusion of deep learning and machine learning techniques has made overcoming this non-uniformity even more critical, as they allow the fusion of seemingly unrelated data —collected from sensors designed for independent applications with different requirements— to obtain invaluable information, laying the foundation for a a new generation of smart city applications.

In-field deployment of communication front-ends implies their constant interaction with both residents and the city environment. These interactions create an intensely dynamic context, where communication modules are subject to frequent changes. This makes *mobility* and *plug-and-play* the key requirements of many smart city communication planes. Intuitively, mobility plays an integral role in applications such as smart transportation and smart healthcare —which involve tracking moving objects and individuals. However, seemingly stationary sensing —in applications such as smart grid and smart metering— might also be subject to occasional movements as a result of changes in their environment; this introduces a distinction among highly mobile, mobile, and stationary communication. The plug-and-play feature is also required to further facilitate a network's potential adaptations; the smart city communication plane must automatically detect and integrate new devices. It must also be able to resume its normal operation unhindered upon exclusion of some nodes.

Due to the inherent characteristics of M2M communication, data traffic patterns within the smart city communication plane are known to be more sophisticated than legacy WSNs. A vast range of smart city applications are event-based, where data tends to arrive in bursts rather than in a constant stream. Controlling bursty data involves more sophisticated in-field pre-processing, routing, and QoS management. Ensuring QoS standards is further complicated by the delay sensitivity of many smart city services, such as smart

ACCEPTED MANUSCRIPT

Table 2: The list of primary requirements of the smart city communication plane. Each requirement can be associated directly with others, implying intricate tradeoffs among them.

Requirements	Implications	Common Solutions
Low Power Consumption	Cost TCP/IP Compatibility Plug-and-Play Mobility Interoperability QoS (Various) Expandability	• Energy Harvesting [103] • Hierarchal Structuring [104]
TCP/IP (v6) Compatibility	Power Consumption QoS (Adaptation Delay) Expandability	• Hierarchal Structuring [105]
Mobility	Power Consumption Plug-and-Play QoS (Routing Delay) Expandability	• Mesh Topology [106]
Inter-operability	Power Availability TCP/IP Compatibility Mobility QoS (Adaptation Delay) Expandability	• Adaptation Layer [107]
QoS (Various)	Power Availability TCP/IP Compatibility Mobility Interoperability Expandability	• Aggregating [108] • Prioritizing [109]

transportation and smart health, which calls for additional techniques for traffic prioritizing and redundancy reduction. From another perspective, smart city data traffic can be categorized into *scalar* and *multimedia*. The former involves information that can be represented in small chunks of data, with each chunk being independent from others. For example, temperature, pressure, and air quality monitoring sensors typically generate scalar traffic. In contrast, the prevalence of a new family of smart city applications that revolve around voice commands and video processing services has increased the share of multimedia traffic in communication load. It can be expected that entanglement of these two types of data will continue to increase in the foreseeable future. Table 2 summarizes the primary requirements of the smart city communication plane. Due to their intricate interplay, addressing each requirement often affects others.

4.2. Communication Architecture

Establishing a universal framework capable of satisfying the requirements of smart city communication is a non-trivial task. Since the advent of IoT, various networking architectures have been experimented with, ranging from single-hop flat topologies, to more resilient multi-hop hierarchal architectures. A rising star in this arena, crowd-sensing seems a viable solution for a wide spectrum of smart city applications. By leaving the communication burden on volunteering individuals, crowd-sensing solutions effectively reduce the complexity of this plane, inducing a substantial reduction in RE and NRE [2]. **Furthermore, by exploiting mobile edge computing, it is possible to improve the effectiveness of crowd-sensing campaigns and the efficiency of recruitment, as well as the data acquisition process [110, 99].** Nonetheless, whether the network is formed by independent volunteers or managed by a centralized administration, the continuous evolution of smart city communication has gradually contributed to the obsolescence of flat implementations in favor of hierarchal architectures. Multiple impetuses have expedited this transition. Most noticeably, borrowed from traditional WSNs, hierarchal implementations [111] (e.g., LEACH [112]) are proven effective to manage/reduce power consumption in large-scale networks. Furthermore, considering that the adoption of the TCP/IP protocol for IoT applications faces numerous challenges, satisfying internet compatibility and ensuring interoperability implicitly necessitate a multi-level architecture. The unsuitability of the TCP/IP protocol for smart city communication stems from its inherent characteristics: **(i)** TCP/IP is not originally tweaked for power consumption optimizations, hence failing to meet the most important requirement of smart city communication, **(ii)** fragmenting and re-assembling packets complicate the protocol, degrade the performance, and raise security and privacy concerns, and **(iii)** lack of built-in security measures must be offset by the addition of sub-layers, which further reduces the performance [107]. Multi-level architectures also facilitate complementary services such as aggregation, preprocessing, outliers detection, etc., paving the way for improved QoS management.

Figure 3 depicts the high-level implementation of the smart city communication architecture. The communication functionality is typically divided among three components: The *in-fiend communication front-end* collects raw data from sensors and transmits them to local aggregators for further analysis. *Data adaptation and aggregation* is relatively less constrained by stringent

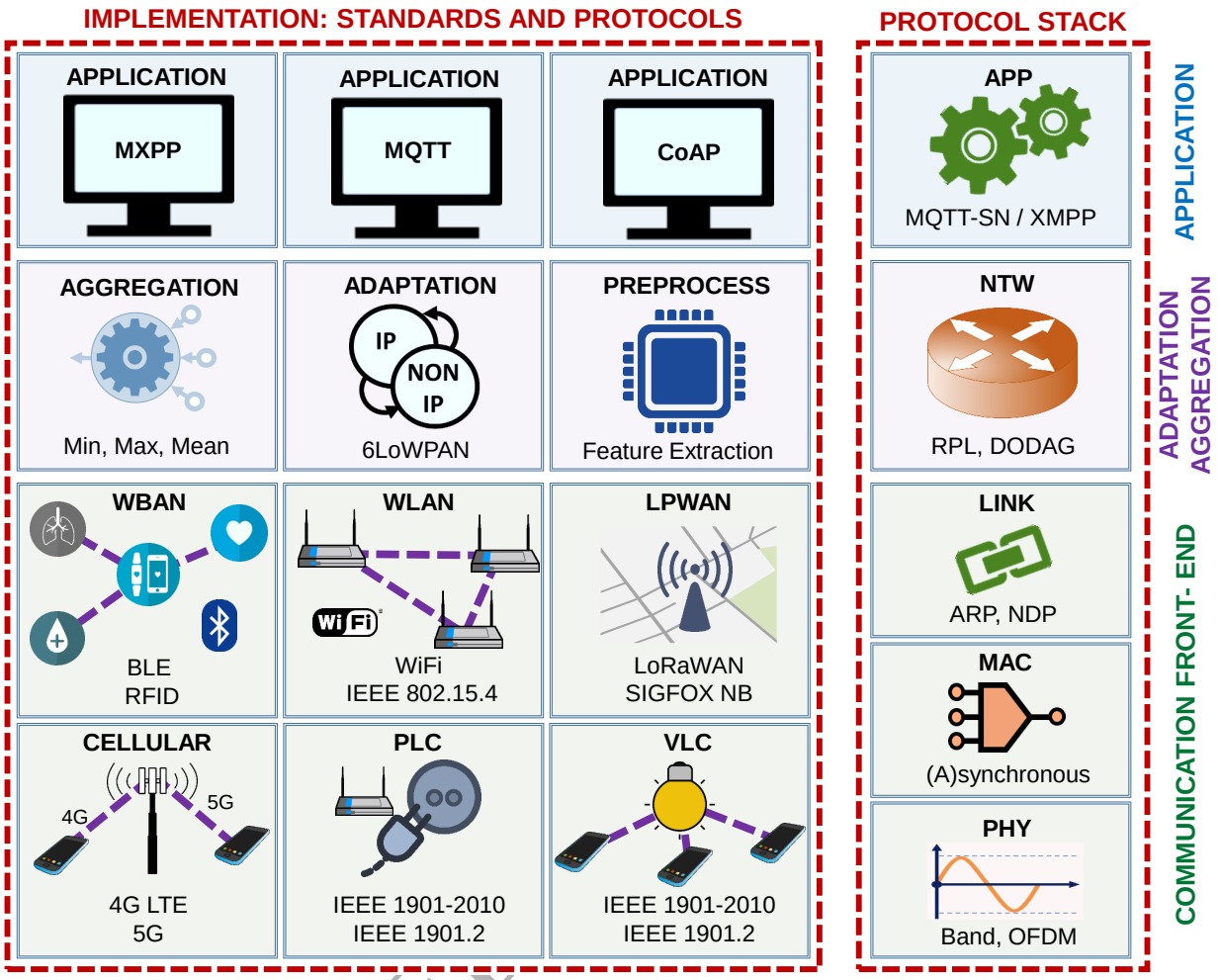


Figure 3: High-level architecture of a hierarchal smart city communication platform. The communication apparatus consists of three components: **(i)** in-field front-end, **(ii)** aggregation and adaptation, and **(iii)** application. This distribution of functionality reduces power consumption, while facilitating interoperability and internet compatibility.

power limitations, which enables it to provide more reliable communication and perform rudimentary data processing as well as interface the Internet with the local in-field network via its IP/non-IP adaptation functionality. This interface opens the door to a vast range of cloud-based services, where sophisticated and demanding data analytics can be employed virtually free of any power availability concerns. Finally, bringing together all constituents of a smart city, the *application component* provides higher level services to facilitate various types of message exchange within the network, e.g., device-to-device, device-to-server, and server-to-server.

In-field front-end encompasses a multitude of communication modules, which are hosted within sensing devices. The networking approaches suggested in the literature can be broadly categorized into **(i)** Wireless Body Area Networks (WBAN), **(ii)** Wireless Personal Area Networks and Wireless Local Area Networks (WPAN/WLAN), **(iii)** cellular networks, **(iv)** Low Power Wide Area Networks (LPWAN), **(v)** Visible Light Communication (VLC), and **(vi)** Power Line Communication (PLC). These networking frameworks are evolved by tweaking different tradeoffs among various requirements of IoT communication (see Table 2); consequently, whether to choose one over another depends on the target application and its requirements. Each of these front-end data acquisition networks includes multiple standards, many of which leverage a hierarchal implementation. Therefore, each level of the architecture, shown in Fig. 3, is often structured as a multi-level multi-dimension platform. Due to its broad context, we detail the most common protocols used in

ACCEPTED MANUSCRIPT

the communication front-end in a separate section (Section 5).

Data aggregation and adaptation plays a pivotal role in seamlessly bridging IoT and the internet, while facilitating the fulfillment of QoS goals. Three major services can be associated with this sub-plane. **(i)** *Data aggregation* involves algorithms that can reduce network traffic, thereby enhancing communication performance at the expense of increased complexity and computation energy consumption. **(ii)** *Cloudlets* are sufficiently powerful devices placed closer to the front-end. They can perform demanding computation on collected raw data. Relegating some of the cloud services to the cloudlets effectively decreases the distance between the cloud and field devices. This has proven effective against multiple challenges in smart city communication. We provide the details of data aggregation and cloudlets in Section 4.3. **(iii)** *Adaptation* involves the link layer and the network layer services that ensure interoperability among various protocols and the TCP/IP architecture, which is the underlying platform of the Internet. We study adaptation in Section 4.4. Although these three aforementioned services are logically distinct, many network implementations combine all these services into a single device, thereby reducing the physical complexity of the network. Alternatively, a hierarchically-distributed implementation of these services can also enhance the performance in certain implementations [108].

Application sub-plane aims to enhance interoperability by standardizing communication between various parts of the system, as the diversity and heterogeneity of smart city communication cannot be fully addressed by merely relying on adaptation and front-end sub-planes. The majority of the proposed protocols such as MQTT, XMPP, and AMQP are originally designed for the TCP/IP stack and are tuned for H2H communication. MQTT-SN is an amendment of MQTT protocol that is particularly optimized for M2M message exchange. While applying these protocols to smart city services can be beneficial in some implementations, it can be detrimental in others. Addressing the needs of the smart city community, IETF has recently developed CoAP for IoT applications. CoAP is available publicly. It is lightweight and compatible with popular HTTP, which paves the way for integration of smart city and the web. However, its limitations and shortcomings must be fully considered before choosing CoAP over its alternatives. We provide a comparative study of major smart city protocols in Section 4.5.

4.3. Data Aggregation and Pre-Processing Sub-Plane

Data aggregation and pre-processing aim to improve smart city communication performance by minimizing data redundancy. In data aggregation, a subset of field devices (typically those that are relatively more resourceful, either in terms of energy availability or computational power) are selected as *aggregators*. Being a local convergent node for other sensing devices, aggregators perform rudimentary data processing algorithms to compress, combine, and summarize raw data. To further improve the scalability of the network, aggregators can also be implemented in a hierarchal fashion. These services reduce network traffic, which in turn, leads to more relaxed requirements for the communication infrastructure, consequently reducing both recurring and non-recurring expenses. However, delegating additional computation tasks to aggregators increases their energy consumption. This *computation-vs-communication* tradeoff is the underlying enabler for data aggregation.

Redundancy typically exists in an application's sensed data as a result of sensor density, where a large number of sensors measure and report the same physical parameters. For example, all sensors measuring the temperature in a room often report the same value. Transmitting that single value instead of multiple copies can substantially reduce network burden, provided that an *aggregator* compares the incoming traffic and drops duplicates before transmission. Furthermore, a vast variety of smart city applications are event based, where data tend to arrive in burst with substantial amount of redundancy. Applying simple event-detection algorithms can significantly reduce long-range transmission to the cloud. Because communication consumes orders of magnitude more power than computation, this mechanism can substantially contribute to overall energy efficiency. However, communication/computation tradeoff typically provides diminishing returns, implying that running complex algorithms on resource-constrained devices might not be beneficial. To address this limitation, the authors in [113] develop models that can analyze gain and losses of data aggregation in a particular network. Aside from eliminating duplicates, aggregators combine and compress the payload of multiple packets into a single frame, hence reducing packet overhead.

Simple operations such as maximum value, minimum value, average, and median can be executed on raw data to significantly reduce data traffic, without employing demanding and complicated algorithms. However, two drawbacks can be associated with these techniques: First, *lossy* operations such as min, max, and

ACCEPTED MANUSCRIPT

average eliminate a bulk of the information. Second, even small number of defective nodes can severely affect the accuracy of the entire network. For example, a maximum-value aggregating technique can drop correct measurements of healthy sensors in favor of data generated by a faulty —or uncalibrated— device. Studies conducted in [114] propose an adaptive weighted average based on spatial correlation that can alleviate these problems. Nonetheless, such solutions often complicate the system and may not be applicable to highly dynamic and mobile networks. Furthermore, although aggregation is proven to be an effective method to reduce network traffic, it can negatively affect QoS by introducing additional latency. Processing raw information inevitability entails decrypting data, which poses security and privacy concerns. Homomorphic encryption techniques have been proposed as a solution [115, 116, 117], however, considering computational power limitations of the sensing devices, practicability of such methods remains limited for a foreseeable future [117, 116].

Cloudlets have recently received attention as a new approach to multi-level network architecture. Cloudlets are often defined as substantially resourceful devices, in comparison to field sensing nodes, with broadband internet connectivity. Being orders of magnitude simpler than cloud-based servers [118], yet incorporating computationally-capable hardware (e.g., GPUs [119]), cloudlets can be deployed in the vicinity of the sensing networks, typically at a single hop distance, thereby bridging the distance between the cloud and sensing nodes. Authors in [120, 118] enumerate application offloading, data storage and caching, and network management services as the main functionality of a cloudlet. In application offloading, field devices can delegate a portion or the entirety of the execution to a local cloudlet. The result of the operation can be sent back to end-devices for further execution, visualized and stored in the cloudlet, or forwarded to the cloud for multi-user access and sharing purposes. The vast storage resources of cloudlets can also be used as a proxy between users and the servers. When augmented with intelligent behavior prediction algorithms, cloudlets can download and cache the required information of the users. Cloudlets can also supervise network operation by providing services such as VPNs, firewalls, traffic monitoring and optimization [121]. Multiple aspects of smart city communication benefit from bringing the services of the cloud to the field-networks. First, cloudlets can reduce the latency imposed by the core network. Second, decreasing the communication range sometimes allows system developers to employ higher bandwidth communication standards (by trading off coverage for throughput). More importantly, cloudlets can provide offline services independent from the cloud. They can also reduce costs by eliminating subscription fees for the cloud processing and cloud connectivity [122].

4.4. Protocol Adaptation Sub-Plane

As discussed in Section 4.1, heterogeneity in networking technologies is an inherent characteristics of smart city applications. It is therefore crucial to ensure interoperability among these diverse range of technologies. Particularly, almost all smart city applications must be compatible with the TCP/IP protocol, as IoT nodes are differentiated from legacy WSN devices through their internet accessibility. In many scenarios, interoperability is assigned to the *adaptation* subplane. For technologies such as BLE and WiFi (star topologies), this adaptation is conducted by the Operating System (OS) and their specific drivers. Distributed resource-constraint implementations, however, require a more efficient and more standardized solution. IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) is particularly designed for the IEEE 802.15.4 standard (and its variants) to address this problem. In this section, we study the main characteristics concerning a 6LoWPAN-based adaptation subplane.

The incompatibility of IEEE 802.15.4 with IPv6 can be traced back to the differences in their Maximum Transmission Unit (MTU) sizes. While IEEE 802.15.4 sets the MTU to 127 bytes (up to 25 bytes of it can be used for the header), IPv6 allows packet sizes to reach as large as 1280 bytes. Consequently, the majority —but not all— of the IPv6 packets cannot be fit in IEEE 802.12.5 frames. 6LoWPAN specifies two procedures to circumvent MTU differences in these two architectures: **(i)** Header Compression (HC) and **(ii)** Fragmentation and Re-Assembly (FRA). *HC* is mostly achieved by omitting some of the IPv6 header fields such as Traffic Class (8-bits), Payload Length (16-bits), and Flow Label (20-bits) [123]. If the packet still fails to fit in IEEE 802.15.4 frames, FRA procedure breaks IPv6 packets into multiple *fragments*. This process is typically referred to as *fragmentation*. Similarly, multiple fragmented frames can be *re-assembled* into a single IPv6 packet before forwarding to the TCP/IP network. Although HC and FRA allow IPv6 traffic over an IEEE 802.15.4 network, they contribute to packet delivery delays. This contribution is twofold. First, FRA adds packet processing delays. Second, transmitting multiple packets instead of a single one increases the overall latency (because the latency of each fragmentation is added to the overall delay). Furthermore, FRA increases

ACCEPTED MANUSCRIPT

packet loss incidents, as the loss of only a single fragmentation can render the entire packet invalid. The latter drawback can be alleviated by the method proposed in [124], where authors intentionally add redundancy to fragmentation. This enables the adaptation layer to recover the entire packet from even a subset of fragments. As the authors discuss in [125], 6LoWPAN is also susceptible to multiple security attacks targeting addressing, mesh routing, and neighbor discovery. Considering the scant amount of resources available to IoT WSNs, 6LoWPAN does not adopt the IPSec protocol.

Adaptation layer can also provide routing protocols compatible with IPv6. Particularly, IETF developed a Routing Protocol for Low Power and Lossy Networks (RPL) to satisfy this requirement. RPL is compatible with 6LoWPAN and is designed for low-power, large-scale, and multi-hop mesh topologies. Routing is conducted by employing Destination Oriented Acyclic Graphs (DODAG), which establishes an optimum loop-free route between every node and a *sink*. Multiple DODAGs can be established in a network with multiple sinks. The suitability of a route is determined by an *Objective Function* based on parameters such as hop-count, expected transmission count (ETX), and even energy consumption [126]. *Hop count* describes the number of nodes a packet passes through before it reaches the sink, whereas *ETX* denotes the expected number of retransmission for a packet to successfully reach the destination. Due to the dynamic nature of large-scale WSNs, ETX is typically preferred to hop count, especially considering that interference and fading constantly change the status of links [127].

4.5. Application Sub-Plane

Seamless end-to-end communication among nodes in smart city services cannot be attained without standardized application layer protocols. Parallel efforts are being undertaken by various organizations and research communities to provide an IoT-friendly application layer protocol, capable of satisfying the requirements discussed in Table 2. We overview the status of a select number of these protocols below, such as Constraint Application Protocol (CoAP), Message Queue Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP), an Advanced Message Queuing Protocol (AMQP).

CoAP: Constraint Application Protocol (CoAP) is developed by the Internet Engineering Task Force as a simplified and IoT-friendly replica of the popular HTTP. CoAP utilizes the same Representational State Transfer (REST) architecture, where a client and server can transfer resources by using familiar GET, PUT, POST, and DELTE commands. As the study conducted in [128] shows, CoAP interoperability with HTTP bridges IoT and the Web through transparent CoAP proxies. CoAP relies on 6LoWPAN for IPv6 compatibility, which not only facilitates Internet access for IoT nodes, but also improves interoperability with HTTP. Packet fragmentation and assembly of 6LoWPAN, however, substantially impacts the performance of the network. Considering the inherent resource limitations of IoT devices, CoAP significantly reduces message overhead to alleviate this problem (header size is decreased to 4 bytes). Unlike HTTP, CoAP adopts User Datagram Protocol (UDP) in its Transportation layer. Multiple advantages can be associated with UDP in the context of smart city and IoT applications. First, its inherent simplicity —when compared to TCP— makes it suitable for resource-constrained devices. UDP can also provide multicasting, a crucial requirement for many IoT applications. Furthermore, CoAP allows applications with stringent security requirements to adopt Datagram Transport Layer Security (DTLS) protocol as well. Substituting TCP with UDP, however, has multiple drawbacks. Most noticeably, UDP does not provide a strong congesting control mechanism. Congestion in smart city services can be associated with the large number of devices and event-based characteristics of some applications, where data tends to arrive in bursts. The built-in Retransmission Timeout (RTO) mechanism of CoAP is proven ineffective in many scenarios. IETF is developing Congestion Control/Advanced (CoCoA) to address this issue [129, 130]. Using the UDP DTLS protocol also eliminates the protocol's ability to multicast. Diversifying its QoS management, CoAP supports both *confirmable* (CON) and *non-confirmable* (NON) messages [131].

MQTT-SN: Message Queue Telemetry Transport for Sensor Networks (MQTT-SN) [132] is an open communication technique designed specifically for resource-constrained devices, which operates in lossy networks with limited throughput. Instead of the REST protocol used in CoAP, MQTT-SN adopts a Publish/Subscribe (Pub/Sub) mechanism due to its superior scalability and improved compatibility with dynamic WSNs. MQTT-SN embodies multiple modifications aiming at IoT device requirements. For example, unlike MQTT, this protocol does not necessarily require TCP/IP communication (i.e., it is UDP-compatible), it includes message overhead reduction, and provides a new sleeping mode mechanism tailored to battery-powered IoT devices. MQTT-SN is originally developed for ZigBee-based WSNs; however, it is also compatible with any bi-directional communication technology. An MQTT-

ACCEPTED MANUSCRIPT

SN-based WSN is formed by three components: *clients*, *forwarders*, and *gateways* (*GWs*). Clients use MQTT-SN to send their message to GWs either directly or in a multi-hop connection consisting of one or more forwarders. Gateways bridge clients to MQTT servers by converting the MQTT-SN syntax to MQTT and vice versa. A gateway can be implemented either as a standalone device or be integrated into the server. Two types of GWs are defined in MQTT-SN specifications. *Transparent* GWs create a one-to-one connection between every client and a server. For example, a GW associated with five clients establishes five simultaneous connections to the server. Transparent GWs are simple to implement; however, some MQTT servers have limitations in the number of simultaneous connections. In this case, MQTT-SN suggests *aggregating* GWs, which encapsulates all communication among clients into a single connection between the GW and the MQTT server, which reduces the number of concurrent connections. Aggregating GWs, however, are more complicated than transparent ones. MQTT-SN also includes a new sleeping mode, where clients can inform the gateway of their sleeping period through a DISCONNECT message. During this period, all data destined to a *sleeping* client is buffered in the GW.

XMPP: Extensible Messaging and Presence Protocol (XMPP) is an open protocol originally designed to facilitate real-time exchange of structured data, which can be encapsulated in small packages (XML stanza). XMPP uses a distributed server-client architecture, where clients must establish a connection to a server prior to exchanging any information with other clients. Overall, XMPP architecture includes three types of devices: *clients*, *servers*, and *gateways*. Clients cannot exchange messages directly. Instead, all communications must pass through XMPP servers. These servers are interconnected to allow message exchange between clients associated with different servers. Protocol gateways are used by the servers to provide interoperability with other Instant Messaging (IM) protocols. Although IM can be considered as an XMPP main target application, the aforementioned characteristics coupled with its remarkable extensibility and flexibility renders this protocol suitable for delay-sensitive IoT networks with scalar traffic. Particularly, the decentralized nature of the XMPP seems applicable to distributed and heterogeneous smart city applications. XMPP utilizes TCP to provide lossless communication between either servers or servers and clients. Despite its reliability and embedded congestion control mechanisms, TCP can increase the overhead for smart city devices. Transport Layer Security (TLS) is also available as an optional choice to meet security and privacy requirements [133]. In spite of its many desirable characteristics, XMPP is not originally designed for IoT applications; therefore, it cannot be deployed in its current form on resource-constrained WSNs, which typically involve periodic data collection (in contrast to event-based data interaction of instant messaging) [134]. Consequently, extensive research in the literature has been conducted to provide lightweight, IoT-friendly variations of XMPP [134, 135]. XMPP does not support acknowledged communication either.

AMQP: Advanced Message Queuing Protocol (AMQP) is an open standard developed for reliable point-to-point communication. It is originally designed for banking services, which involve queuing a large number of transactions and reliably delivering them later. This emphasize on reliability coupled with built-in support for scalability makes AMQP suitable for mission-critical smart city applications. Overall, the protocol consists of a *transport* layer, which provides connection between two *nodes*, and a *message* layer, which facilitates message exchange among nodes. Nodes can assume one of the three defined roles in the AMQP architecture: *Producers*, *consumers*, and *queues*. Producers and consumers are application layer processes that respectively generate and receive messages, while queues provide store-and-forward services. The Transport layer connects a producer/consumer pair through full-duplex bidirectional *connections*. Each connection embodies a group of unidirectional *channels*, which provide reliable communication over lossy links. The frame header is defined to have an 8-bit wide fixed field and an extensive field, which is reserved for future use. AMQP utilizes TCP and the communication is secured by employing Transport Layer Security (TLS) and Simple Authentication and Security Layer (SASL) [136].

5. In-field Communication Front-End

Being the first tier in the smart city networking hierarchy, field communication front-end involves collecting raw data from a diverse range of devices and forwarding them to the data aggregation and adaptation sub-planes. Its physical connection with the sensing devices often entails a distributed deployment in a smart city, where reliable communication must be provided over an unreliable infrastructure. Although the networking society has been remarkably successful in fulfilling this objective via the implementation of a mature TCP/IP protocol stack (and its sub-layers), fledgling smart city front-end protocols often struggle to catch up. Thus, the designers are forced to make trade-offs, which is the fact that

ACCEPTED MANUSCRIPT

caused the introduction of a wide spectrum of protocols, where *variety* is viewed as a trade-off to counterbalance non-ideality. Even in the absence of a perfect communication solution, system developers can still browse through existing protocols to choose ones that match the requirements of the target application almost perfectly. However, utilizing this impressive diversity and selecting the most compliant implementation burdens developers with the task of analyzing and comparing the advantages and disadvantages of every proposed solution and makes it crucial for them to gain knowledge about the most recent advances in the field. In this section, we compare existing protocols. Numerous comprehensive surveys exist in the literature that delve into low-level implementation of these protocols [137, 138, 139]. Therefore, instead of focusing on technical aspects, we investigate every protocol from an application-oriented perspective, concentrating on the strengths and shortcomings of available solutions in practical deployments.

Smart city communication infrastructure can be categorized either retrospectively or based on their coverage. First generation of protocols are directly borrowed from legacy WSNs. These protocols (e.g., ZigBee, Z-Wave, WirelessHART, etc.) are proven adequate in many smart city applications as an off-the-shelf and easy-to-deploy solution. Nonetheless, the emergence of IoT coupled with its ever-increasing complexity has dictated a new set of rules that cannot be fulfilled unless alternative communication protocols are introduced. Hence, a new category of protocols such as LoRa, Bluetooth Low Energy (BLE), and IEEE 802.11ah have emerged to addressed these challenges and potentially open the door to a new era of smart city services.

Although a retrospective review reveals valuable information about the technological trends, choosing a protocol primarily depends on its ability to address the key requirements of the target application (see Table 2). Therefore, considering the application-focused orientation of this section, we classify these protocols based on their practicality for each set of applications. Since the scale of a network substantially affects its other fundamental characteristics (such as rate, range, power consumption, and traffic propagation), we investigate the existing protocols in the following categories: **(i)** WBAN, **(ii)** WLAN, **(iii)** LPWAN, **(iv)** cellular networks, **(v)** VLC, and **(vi)** PLC.

5.1. Wireless Body Area Network (WBAN)

WBANs are designed to connect multiple sensors in a range of ≈100 meters. Smart healthcare is the niche application of WBAN. Low power consumption, mobility, ubiquity, user-friendliness, security, and privacy are the main requirements of such networks, particularly when they are used within the context of smart healthcare. Different protocols have been experimented with as the primary ingredient of WBANs, beginning from ZigBee and Bluetooth to the more refined and more IoT-compliant Bluetooth Low Energy (BLE). Exclusively targeting IoT, BLE is known to be adequate for numerous smart city applications. Owing to its constantly expanding market share, BLE can eventually become the universal standard for WBAN by making its competitors, such as WiFi and ZigBee, obsolete. Therefore, we investigate BLE in this section, while leaving the discussion for ZigBee and WiFi for Section 5.2.

Bluetooth Low Energy (BLE): BLE is designed to provide short-range, low-power, low-delay, and low-rate connectivity. Like many of its competitors, BLE operates in the 2.4 GHz frequency band, which makes it prone to interference with existing wireless protocols such as WiFi and ZigBee. Adaptive (dynamic) frequency hopping is therefore implemented in its MAC layer to reduce the probability of interference. Two types of communication are supported by this protocol: **(i)** *piconet*, in which multiple nodes (slaves) can be connected to a single master, and **(ii)** *broadcasting*, in which a node can broadcast its data to every device within its range. In the piconet scenario, slaves cannot communicate directly, making it a star topology. BLE frequency band is divided into forty 2 MHz-wide channels, out of which 3 are used for advertising (broadcasting) and 37 are used for data transfer after a connection is established. The coverage area can be adjusted based on power availability, with a maximum radius of ≈70 m [9]. The latest version of BLE (version 5 [145]) can support data transfer rates up to 2 Mbps.

The fundamental advantages of BLE emanate from its IoT-centric design. BLE is inexpensive and requires only 40% of ZigBee's power demand [146], while providing higher data transfer rates [18]. These two characteristics of BLE alone make it a suitable choice for a vast range of smart city applications. For example, authors in [16] use inexpensive coin battery-powered BLE tags, which last up to a year, to track the movements of individuals; this is an application that is typically considered a niche market for passive RFID tags. Furthermore, BLE star topology can *theoretically* include an unlimited number of slaves, which addresses the scalability requirement of many smart city services. The built-in low-latency characteristic of BLE also satisfies the low-delay requirement of many IoT applications. Unlike WiFi, which uses 50 frequency channels to adver-

ACCEPTED MANUSCRIPT

Table 3: A summary of the BLE technology and its applications in the smart city arena. *Example applications* includes some of the widely used services in which BLE is used; this column includes non-WBAN implementations as well. The data represented in this paper is not exhaustive, meaning that there may applications and sensors compatible with BLE not listed in the table.

Technology/ Characteristics	**Advantages/ Disadvantages**	**Example Applications**	**Suggested Application**
Bluetooth Low Energy (BLE) / 2.4 GHz ISM Band Low-Rate ($\leq$ 2 Mbps) Low-Range ($\leq$ 100 m) Low-Energy	$\Uparrow$ Low Power $\Uparrow$ Inexpensive $\Uparrow$ Ubiquitous $\Uparrow$ Low Delay $\Uparrow$ Scalability $\Downarrow$ No Multi-Hop $\Downarrow$ Limited Scalability $\Downarrow$ No Mesh/Cluster $\Downarrow$ No Multi-Casting $\Downarrow$ MAC Layer Inflexibility $\Downarrow$ Utilizing 2.4 GHz Band	Location Fingerprinting [140] Smart Home (HVAC) [18] Crowd Tracking [16] Smart Vehicle (IVWSN) [18] Smart Healthcare (WBAN) [141] Smart Environment[142] Driver Assist [143] Activity Recognition [144]	Human-Centric Stationary/ Quasi-Stationary Networks (Scalar Traffic)

tise its SSID, BLE utilizes only three channels for pairing purposes. This utilization of fewer number of advertising channels, coupled with a low-complexity pairing mechanism, substantially reduces advertising delay [140]. Complementing these offerings, BLE's remarkable ubiquity translates to user-friendliness, non-invasiveness, and compatibility with existing and potential implementations. In contrast to ZigBee, almost all portable smart devices, such as smartphones, laptops, and smart wearables are shipped with built-in BLE-compatible chips.

Multiple shortcomings of BLE have been noted in the literature. For example, aside from broadcasting, BLE is only compatible with the *star* topology, which can restrict its scalability and introduce various security and privacy concerns [107]. Other competitors such as ZigBee support alternative topologies including *mesh* and *cluster*. Additionally, the single-hop master-slave implementation of BLE limits its expandability and makes it difficult to provide a wide-area coverage. Multi-casting (a crucial requirement for many smart city applications) is not supported, which complicates QoS management [107]. Although the specifications do not impose a maximum on number of connections to a master, the *practical* size of the network is typically determined by interference and the computational capability of the master. Finally, BLE's MAC layer flexibility is inferior to its competitors, since it only supports time-division multiple access (TDMA) [18].

Despite its drawbacks, BLE seems to be a viable solution for short-range communication among *relatively* stationary sensors. Aside from WBAN —which is the traditional domain of BLE— authors in [18] utilize this technology to reduce the costs and weights of Intra-Vehicular WSNs (IVWSN). BLE is suitable for IVWSNs since it can effectively address its main requirements by providing low-rate, delay-sensitive, and prioritized communication for stationary sensors even in harsh deployment environments. BLE can also be used for networking non-stationary sensors, for example in crowd and individuals tracking applications [16, 142]; in these settings, the nodes are typically configured to operate only in advertisement mode to reduce power consumption and avoid pairing delays. BLE is also shown to be compatible with a wide spectrum of sensors that generate different types of data traffic; these include **(i)** event-based sensors such as Infra Red (IR) presence detectors, temperature, and humidity sensors [9], which generate discrete samples and **(ii)** sensors that generate continuous streams of real-time data such as photoplethysmogram (PPG) [143]. Intuitively, BLE is not suitable for applications that require wide bandwidth such as high frame-rate real-time video recording. Table 3 summarizes BLE and its main characteristics.

ACCEPTED MANUSCRIPT

5.2. Wireless Personal Area Networks (WPAN)

WPAN protocols are designed to provide wireless connectivity in a radius of ≈100 meters. Unlike WBAN, WPAN protocols allow a multi-hop implementation, extending their coverage area to hundreds of meters. Having its roots in legacy WSN, the transition from WSN to IoT has contributed to the emergence of new adaptations, making WPAN protocols more IoT-friendly. They typically emphasize co-existence with existing technology, management of heterogeneous traffic, and addressing security and privacy considerations. In this section, we investigate the most commonly used protocols along with their strengths and shortcomings in their target applications.

IEEE 802.15.4: This protocol is designed to provide low-power, low-range (≈ 10 m) and low-rate (≈ 250 kbps) communication, although practical data rates are typically lower [147]. Targeting simplicity, IEEE 802.15.4 is implemented on top of a 2-layer protocol stack. Although this simplified implementation fails to offer higher level services, it provides a robust basis for more advanced protocols such as ZigBee and WirelessHART (both of which utilize IEEE 802.15.4 PHY and MAC layers), thereby fortifying its omnipresence in the smart city field. Like many of its competitors, IEEE 802.15.4 operates in the 2.4 GHz ISM frequency band, which leaves it exposed to interference and fading effects. Multiple amendments have been added to IEEE 802.15.4 (i.e., IEEE 802.15.4a, IEEE 802.15.4c, IEEE 802.15.4d, and IEEE 802.15.4e), which incorporate a wider frequency band, add support for additional modulation techniques, and improve the MAC layer performance [125]. IEEE 802.15.4 MAC layer regulates channel sharing using either synchronous or asynchronous access. The latter involves a limited contention period, which is broadcasted by a beacon, while the latter is based on a CSMA/CA mechanism. By dividing the communicating nodes to Full Function Devices (FFD) and Reduced Function Devices (RFD), IEEE 802.15.4 implements a hierarchal topology; RFDs require minimal communication capability to forward their data to relatively more resourceful FFDs in either star, peer-to-peer, or tree topologies. By outsourcing their functionality to FFDs, this hierarchal implementation enables RFDs to substantially reduce their power consumption.

Although BLE is proven superior in terms of low-energy consumption and low cost, IEEE 802.15.4 (and its variants) can still be considered a viable alternative even for state-of-the-art smart city implementations. IEEE 802.15.4 boasts a more predictable behavior due to its maturity, because numerous studies and implementations have revealed its strengths and weaknesses since its introduction in 2003. In contrast, behavior of the fledgling BLE in complex settings still requires more research [148]. Furthermore, being one of the oldest standards in WSN and the IoT networking realms, IEEE 802.15.4 lends itself well to inclusion of higher-level layers. This has led to the introduction of customized complementary standards such as 6LoWPAN, RPL, UDP, and CoAP that can substantially enhance the applicability of this protocol. Particularly, 6LoWPAN ensures IPv6 compatibility, opening the doors of local WPANs to the global Internet. Another major advantage of IEEE 802.15.4 comes from simplicity. The study conducted in [148] shows that the IEEE 802.15.4 protocol stack implementation requires approximately 4 times less memory than its competitors, giving it a competitive edge in resource-constrained smart city network implementations. Additionally, supporting various networking topologies such as peer-to-peer, mesh, tree, and star enhances the flexibility and applicability of this protocol. For example, mesh topology can be selected to implement multi-hop networks that can cover a wide area, making IEEE 802.15.4 ideal for environmental monitoring.

Despite multiple attempts to make IEEE 802.15.4 more IoT-compliant, the majority of the disadvantages of this protocol emanate from the discrepancies between IoT and WSNs. Particularly, considering the coexistence issue, IEEE 802.15.4 cannot compete with its main alternatives, thereby failing to satisfy a major requirement of smart city applications. Lacking a powerful priority-based packet delivery mechanism further restricts the applicability of IEEE 802.15.4 in IoT and smart city applications. Additionally, collision prevention techniques employed in its MAC layer are not effective in handling dynamic (typically event-based) traffic of a smart city. Particularly, non-adaptive selection of back-off period is known to degrade network performance during congestion, when the collision rate increases substantially [149]. Selecting a back-off period regardless of the status of the network also decreases the throughput of the network, because it may lead to an occasional low utilization rate of the medium. IEEE 802.15.4 does not include a PHY layer security mechanism and suffers from the *hidden terminal problem*. Furthermore, peer-to-peer communication is only supported in asynchronous operating mode, which has an inferior performance to the synchronous mode in terms of power consumption [127]. Finally, although this protocol can become compatible with IPv6 using standardized adaptation layers, 6LoWPAN is known to impact the performance of a network negatively, particularly, in terms of latency [150].

ACCEPTED MANUSCRIPT

Original IEEE 802.15.4 is not widely used in state-of-the art applications, since its variants such as ZigBee can offer superior performance while providing the advantages of basic IEEE 802.15.4. These two protocols are interwoven to the extent where many system developers use the terms IEEE 802.15.4 and ZigBee interchangeably. In this paper, although we make a distinction between the two when describing the strengths and advantages of each protocol, we group both protocols into a single summary table. Aside from the popularity of ZigBee, some relatively recent papers investigate the use of IEEE 802.15.4 in various branches of smart city, including smart transportation [151], smart healthcare [152], smart structural health monitoring [153], and smart agricultural applications [154]. Being a mature WSN protocol, IEEE 802.15.4 has proven itself a low-cost and low-power solution for static and stationary (or quasi-stationary [151]), networks, in which a substantial portion of the network traffic consists of scalar data.

ZigBee: Utilizing the PHY and MAC layers of IEEE 802.15.4-2006, the ZigBee Alliance [155] (a consortium of several companies including Samsung, Texas Instruments, and Motorola) offers an inexpensive, low-range (≤ 100 m), low-rate (up to 250 kbps using Direct Sequence Spread Spectrum (DSSS)), and low-energy technology for PANs. ZigBee operates in the 2.4 GHz ISM frequency band and adopts the same synchronous (beacon-based) and asynchronous communication; its PHY and MAC layers have the same characteristics as IEEE 802.15.4. Similar to its ancestor, ZigBee nodes are categorized into Reduced Function Devices (RFD) and Full Function Devices (FFD). The former support basic functionality and are typically used as leaves in the network hierarchy. The latter are mostly used as parents and host additional NTW and APL layers atop IEEE 802.15.4 PHY and MAC. Although this increases their resilience and augments their applicability, it also increases the power consumption of FFDs. Each ZigBee device can undertake one of the three responsibilities defined in this standard: **(i)** ZigBee End Devices (ZED) are used as the leaves of networks to collect and forward raw data from field sensors, **(ii)** ZigBee Routers (ZR) can be used to extend the coverage of ZigBee networks, and **(iii)** ZigBee Coordinators (ZC) are used as the central nodes to provide centralized control. ZRs can have up to 12 children, whereas ZCs cannot have more than 10 children. Overall, ZigBee networks can encompass up to 65000 nodes.

The addition of the NTW layer to the IEEE 802.15.4 protocol stack enables ZigBee to perform more robust routing. Particularly, the MAC layer executes the Ad hoc On-demand Distance Vector (AODV) algorithm, which makes ZigBee suitable for mobile and dynamic connectivity. The NTW layer also uses acknowledgement packets to enhance reliability. Furthermore, data transmission is secured using AES-128 encryption to address both security and privacy concerns. Application profiles are added to the APL layer of ZigBee to provide support for interoperability and distributed processing. These predefined application profiles standardize message formats and processing actions, which enables communication among ZigBee-compatible devices manufactured by different vendors [156].

Benefiting from the same PHY and MAC layers of IEEE 802.15.4, ZigBee retains major strengths of its ancestor; it surpasses cellular networks in terms of cost and power consumption, provides considerably lower power consumption than IEEE 802.11, and unlike BLE, it can be structured to offer wide area coverage. Furthermore, implementing the AODV routing algorithm results in a self-healing feature, which increases network reliability and adds support for mobility. The NTW layer also uses ACK packages, supports mesh topology, and employs 128-AES encryption to improve both reliability and security even further [157]. The implementation of application profiles in the APL layer boosts the interoperability of the system. Additionally, unlike BLE, ZigBee supports multi-casting, which can facilitate QoS management [107].

The shortcomings of ZigBee in practical deployments have been well documented in the literature (which can be counted as one of the advantages of ZigBee due to its maturity). A portion of these limitations are inherited from IEEE 802.15.4. For example, non-adaptive selection of the back-off period imposes the same performance impact [158]. Additionally, depending on the requirements of their target applications, smart city services —particularly applications which solely involve scalar traffic— should be able to reduce networking power consumption by either lowering data rate or limiting communication range. Such functionality, however, is not implemented in ZigBee [159]. Although ZigBee can be used in Wireless Dynamic Sensor Networks (WDSN), its deployment is such networks faces multiple challenges; studies in the literature [160] show that ZigBee suffers from performance degradation as the number of mobile nodes increases. Furthermore, due to its 10-second refreshment delay, AODV routing algorithm fails to efficiently re-route the network in highly-mobile networks. Relying on ACK packages to improve reliability leads to an inexorable increase in network traffic (when ACK packages are lost during transmission), affecting delay and other QoS parameters. ZigBee also suffers from significant performance penalties

ACCEPTED MANUSCRIPT

when deployed in coexistence with WiFi, particularly because transmission power of WiFi is orders of magnitude higher than ZigBee. (While ZigBee/WiFi interferences significantly reduce ZigBee performance, their effects are less detrimental to WiFi, as ZigBee transmissions are not strong enough to interfere with WiFi signals.) Regarding the omnipresence of WiFi in a modern city, this drawback substantially affects the applicability of ZigBee in smart city applications. Numerous solutions are suggested in the literature to abate this problem [161, 162, 163]. These proposed solutions, however, negatively impact the performance and power consumption of ZigBee and WiFi communication [164]. Finally, although a multi-hop architecture can be used to substantially extend the coverage area of ZigBee, such implementations typically suffer from unbalanced distribution of traffic; nodes closer to the gateways are flooded with numerous converging streams of data, which degrades the network throughput.

The maturity, reliability, low cost, and low-power consumption of ZigBee have made it a natural choice for a variety of smart city applications, including smart grid [165, 166, 167], smart transportation [168], smart healthcare[169, 170], environmental monitoring [157, 171], smart home [172] and surveillance [173]. ZigBee communication is suitable for mission-critical harsh industrial applications which mostly involve scalar data transmission. Extending the coverage area of the ZigBee networks or increasing the density of the nodes can degrade their network performance; therefore, alternative solutions must be considered in these scenarios. Table 4 summarizes ZigBee and other IEEE 802.15.4-based protocols.

WirelessHART: WirelessHART is the wireless extension of Highway Addressable Remote Transducer (HART) protocol, which was debuted in 2007. It is designed to provide a low-power (maximum transmit power of 10 mW), short-range ($\approx$ 100 m), and low-rate (250 kbps) wireless connectivity for industrial applications. Generally, these applications tend to be mission critical and delay-sensitive, where a failure to meet these requirements can lead to catastrophic outcomes, endangering the safety of personnel and incurring substantial financial cost. Ensuring reliability in industrial wireless communications, however, is a daunting task, especially considering their harsh deployment environment. WirelessHART meets this requirement by defining complementary functionality atop the IEEE 802.15.4 PHY layer. It leverages a centralized hierarchal structure, because such architectures surpass flat and distributed networks in terms of reliability. WirelessHART defines six major types of devices: *field devices* are in-field sensing nodes that collect raw data and forward them to a *gateway*, which interfaces host applications with field devices. A centralized *network manager* supervises the entire network providing services such as transmission scheduling, routing, traffic priority control, etc. Network managers typically host a *security manager* to control key sharing (join, session, and network [174]). In-field operators can use their *handheld* devices to configure, calibrate, and diagnose field devices. Finally, non-wireless HART devices can be interfaced with WirelessHART using *network adapters*. The MAC layer utilizes TDMA, where the centralized network manager assigns each node a dedicated time slot to transmit its package. Each time slot is 10 ms long, which is enough for a node to send its 133-byte packet and receive its associated ACK. This approach improves the reliability of the network by making it more predictable. Dedicated time slots also enable each node to remain in sleep mode for a pre-defined period of time, which helps reduce the overall power consumption of the network [175]. The NTW layer uses graph and source routing [176, 177], allowing it to support both mesh and star topologies. Although not mandatory, packet delivery can be confirmed using ACK packages. WirelessHART application layer standardizes a set of mandatory and optional commands, which facilitate the inter-operation of devices manufactured by different vendors.

Although WirelessHART was originally designed for process automation applications, its low-power consumption coupled with its outstanding reliability makes it suitable for some mission-critical smart city applications. In order to reduce the noise and interference effects of the crowded 2.4 GHz ISM band, this technology leverages frequency hopping and channel blacklisting. Unlike other IEEE 802.15.4-based standards such as ZigBee, the centralized approach to the TDMA technique substantially improves predictability, manageability, and reliability of the network. Furthermore, NTW layer support for multi-path routing and inclusion of mesh and star topologies augment the performance of WirelessHART [178]. The inclusion of multi-hop topology also implies that the network can be extended to cover relatively wide areas. Using network adapters, any HART-capable device can be integrated into a WirelessHART network, which provides backward-compatibility and facilitates the transition from wired network to wireless implementations.

WirelessHART suffers from multiple drawbacks that limit its applicability to a small set of smart city applications. Although it boasts higher reliability, the centralized management of the network inexorably leads

ACCEPTED MANUSCRIPT

to an unbalanced load problem, where nodes closer to the central sink are often flooded with converging traffic from the remaining nodes [179]. Limited coexistence capability can further limit the applicability of this technology, where the network performance is known to degrade in presence of other wireless standards, such as IEEE 802.11 variants. WirelessHART is even incompatible with other IEEE 802.15.4-based protocols that use less centralized beaconing techniques (such as ZigBee [174]). More importantly, WirelessHART fails to match its competitors in terms of scalability. Practical considerations including limited computation capability of the central nodes and unbalanced traffic load problem restrict the maximum number of field devices to ≈100. To resolve this problem, system designers are typically compelled to either reduce the sampling rate of field devices [180] in order to reduce the traffic load or use multi-network hierarchal approaches, which inevitability increases interference [181]. Mandatory inclusion of security features reduces the flexibility of the network; in cases when security is not a concern, system developers cannot disable security features to improve the battery life of the nodes. Additionally, concentrating the security management into a single device leaves the entire network susceptible to cyberattacks as soon as the *security manager* is compromised [180]. WirelessHART also does not support multi-casting [174], making it less friendly to QoS management in the smart city context.

Although WirelessHART was originally designed for industrial applications, the emergence of a new generation of hybrid smart city services has increased its acceptance in the IoT and smart city arenas. For example, the system developed in [182] employs WirelessHART-based communication in a smart transportation to measure the vibration of rail roads. Authors in [183] utilize WirelessHART for in-vehicle networking, reducing the cost and weight of vehicles and improving their efficiency. Alternatively, authors in [184] use WirelessHART for localization, i.e., estimating the location of operators in a process plant. When aiming at mission-critical small to medium scale applications, smart city service providers may choose WirelessHART over its competitors as a viable alternative.

IEEE 802.11 ah (HaLow): Various amendments of IEEE 802.11 have long been an integral part of a smart city. The latest amendment, the IEEE 802.11ac, is capable of supporting data rates of up to 6.9 Gbps, making it ideal for real-time multi-media content delivery. However, despite their ubiquity and impressive data transfer rate, classic variations of IEEE 802.11 are not particularly suitable for smart city applications; they fail to meet the major requirements pertaining to scalability and power consumption. To make IEEE 802.11 IoT-friendly, Task Group 802.11 ah (TGah) introduced IEEE 802.11ah amendment in 2017 [187], which is designed to provide low-power, low-data rate (150 kbps), and relatively long range (≈1 km) connectivity; IEEE 802.11ah can either be used in a sensor or a backhaul network (due to its relatively broader coverage). Scaling down the PHY level implementation of IEEE 802.11ac by a factor of ten, IEEE 802.11ah operates in the sub-GHz (902–928 MHz in the US) ISM frequency band. The narrower frequency band (26 MHz vs. 100 MHz, and 150 MHz in 2.4 GHz and 5 GHz ISM frequency bands, respectively) implies limited throughput. Nonetheless, its superior propagation characteristics result in reduced power consumption and wider range. The 26 MHz-wide band can be divided into 1 MHz, 2 MHz, 4 MHz, 8 MHz, and 16 MHz channels, providing support for throughputs of 150kbps to 346Mbps [188], although, compatibility with channels wider than 2 MHz is optional. The MAC layer of IEEE 802.11ah supports a single-hop start topology with the exception of relays, which can be inserted between stations and the AP to increase the coverage of the network [189]. 6000 stations (STAs) can be connected to each AP, addressing the scalability requirement of IoT applications. Medium access is controlled using CSMA/CA techniques. A specific contention mechanism, called Restricted Access Window (RAW) is employed by TGah to limit collision probability. AP periodically broadcasts RAW frames, each of which encompasses multiple *time slots*. Only a portion of the STAs can compete for the channel access during a time slot. Time slots are assigned to STAs based on their Association Identifier (AID). This divide-and-conquer strategy reduces collision and extends the sleep time of STAs.

Similar to BLE, targeting smart city and IoT applications exclusively arms IEEE 802.11ah with various advantages over its classic competitors such as ZigBee and WirelessHART. Specifically, operating in the sub-GHz frequency band, where signals possess superior propagation characteristics and a +10 dB higher SNR as compared to the 2.4 GHz band, enables IEEE 802.11ah to offer extended coverage for outdoor or alternatively low power consumption for indoor implementations [190]. It demonstrates improved efficiency when coexisting with other wireless standards such as BLE, ZigBee, and classic WiFi. Additionally, IEEE 802.11ah is designed with flexibility as a built-in feature, where power consumption, coverage range, and throughput can be tuned according to the requirements of an application. This allows its data transfer rate to range from 150 kbps

Table 4: A summary of WPAN technologies and their applications in the smart city arena. *Example applications* includes some implementations, in which each technology is widely used (this column includes non-WPAN implementations as well). The information represented in this table is not exhaustive. Although WirelessHART is mentioned in numerous papers as a viable solution for a wide range of smart city applications, its actual implementation in this area is rarely investigated.

Technology/ Characteristics	**Advantages/Disadvantages**	**Example Applications**	**Suggested Application**
IEEE 802.15.4 (ZigBee) / 2.4 GHz ISM Band Short Range (≤ 100 m) Low Rate (≤ 250 kbps) Low Power	⇑ Low Power Consumption ⇑ Inexpensive ⇑ Maturity/Simplicity ⇑ IPv6 Compatibility (6LoWPAN) ⇑ P2P and Mesh Topologies ⇑ Self-Healing/Reliability ⇑ Multi-Cast Support ⇓ Static Power Management ⇓ High Routing Delay ⇓ Poor WiFi Coexistence ⇓ Unbalanced Traffic Distribution ⇓ Dense Network Incompatibility ⇓ Hidden Terminal Problem ⇓ Utilizing 2.4 GHz Band	Smart Grid [167] Smart Road [168] Smart Healthcare [170] Smart Utility [185] Smart Home Smart Surveillance	Industrial Stationary/ Quasi-Stationary Networks (Scalar Traffic) / Low Density Wide Area Monitoring (Scalar Traffic)
WirelessHART / 2.4 GHz ISM Band Short Range (≤ 100 m) Low Rate (≤ 250 kbps) Centralized Management	⇑ Low Power Consumption ⇑ Inexpensive ⇑ Backward Compatibility ⇑ Star and Mesh Topologies ⇑ Self-Healing/Reliability ⇓ No Multi-Cast Support ⇓ Inflexible/Unscalable ⇓ Poor WiFi Coexistence ⇓ Unbalanced Traffic Distribution ⇓ Utilizing 2.4 GHz Band	Process Automation [186] Smart Road [182] Localization [184] Smart Vehicle (IVWSN) Smart Grid	Medium Scale Industrial Stationary Networks (Scalar Traffic) / Mission-Critical Monitoring (Scalar Traffic)
IEEE 802.11 ah (HaLow) / sub-GHz ISM Band Medium Range (≤ 1 km) Centralized Management	⇑ Low Power Consumption ⇑ Inexpensive ⇑ Superior Coexistence Behavior ⇑ Dense Network Compatibility ⇑ Multi-Cast Support ⇑ Flexible/Scalable ⇑ Relatively Wide Coverage ⇓ Hidden Terminal Problems ⇓ Flat Fading Susceptibility ⇓ No Backward-Compatibility ⇓ Stringent Sub-GHz Regulations	Smart Grid Smart Transportation Smart Environment Smart Utilities Smart Metering	Dense, Stationary Networks With Large Packet Size (Multimedia Traffic) / Large Scale Backhaul Networks (Scalar Traffic)

(when utilizing 1 MHz channels) to 346 Mbps. Controlling medium access using Restricted Access Window (RAW) coupled with a hierarchal implementation of AID ensures scalability, particularly for the dense smart city oriented networks [191]. Considering the small payload size of IoT packets, IEEE 802.11ah MAC layer employs various techniques to reduce the overhead of the network, including abridged MAC headers (Frame Control field of the header determines if the header is abridged or not) and short AP beacons [192]. Additionally, its MAC layer utilizes Null Data Packets (NDP) to reduce the overhead of ACK packet exchanges. Reduction in overhead oftentimes translates to decreased power consumption. IEEE 802.11ah prioritizes medium access by categorizing STAs into Traffic Indication Map (TIM), Non-TIM, and unscheduled devices, which are

ACCEPTED MANUSCRIPT

suitable for heavy, low, and sporadic traffic, respectively [193]. Further extending its compatibility with IoT, IEEE 802.11ah encompasses a wide range of power saving features such as extended sleep time (up to ≈ 5 years), bi-direction Transmit Opportunity (TXOP), and Target Wakeup Time (TWT). Bidirectional TXOP is inherited from classic IEEE 802.11 amendments, where multiple frames can be transmitted after the medium access is won by a STA. However, IEEE 802.11ah allows both transmission and reception of the frames during TXOP. By agreeing on a pre-defined wakeup time, TWT allows an AP to prefetch the data and contend for the medium access, while STA is still in sleep mode, which reduces STA idle time and increases its sleep time [190].

One major drawback of the sub-GHz frequency band is associated with its stringent regulations, which govern PHY layer characteristics. For example, authors in [194] investigate the impact of duty cycling (the duration of time for which an STA can hold the channel and transmit data) on the performance of the network. Their study confirms that duty cycling can significantly affect the performance of networks, particularly in sparse implementations. Duty cycling effect seems to be alleviated as the networks get denser. Operating in the sub-GHz frequency band makes IEEE 802.11ah incompatible with existing amendments of IEEE 802.11, which curbs its ubiquity [195]. Furthermore, due to its utilization of a narrower channel width, IEEE 802.11ah is susceptible to multi-path fading [190]. Extending the communication range in a CSMA-based networks such as IEEE 802.11ah inevitably deteriorates *hidden terminal* problems, which can lead to occasional "chain of collisions," which degrades both the throughput and power consumption [196]. Additionally, although the implementation of RAW improves the performance in dense network scenarios, the efficacy of this mechanism significantly lays upon algorithms that assign STAs to the time slots of RAWs. Studies conducted in the literature confirm that an effective grouping must be conducted dynamically and in accordance with the status of the network traffic and its QoS requirements [197]. IEEE 802.11ah also fails to compete with emerging Low Power Wide Area Network (LPWAN) networks in terms of power efficiency and communication range [198]; however, it can provide substantially higher throughput. Finally, considering that the standard has been finalized recently, to our best knowledge, no commercial IEEE 802.11ah-compatible device is yet available in the market. Consequently, all related research in the literature is carried out based on simulations and theoretical analyses. Although these studies provide insight to numerous aspects of the standard, their initial assumptions may not always be consistent with real-world deployments [191].

IEEE 802.11ah targets IoT and smart city communication front-end, where its advanced MAC features make it particularly suitable for dense networks. In contrast to its competitors such as IEEE 802.15.4-based standards, flexible data rates renders IEEE 802.11ah a viable option for some real-time multi-media traffic handling as well. Alternatively, its extended coverage can be utilized to provide a low-cost and low-power backhaul network for scalar data traffic. This technology is *expected* to become the de facto standard in many smart city applications such as smart grid, smart environment, and smart transportation.

5.3. Cellular Networks

By operating in licensed spectrum, cellular networks present a unique opportunity for smart city applications, as they can better ensure various QoS requirements in comparison to already-congested license-free frequency bands. However, cellular networks are traditionally designed for human-centric VoIP services, with the support for high-definition multimedia content recently added to the latest generations. Consequently, regardless of their many strengths, traditional cellular networks are impractical for typical smart city and IoT applications, because their Human-to-Human (H2H) communication model deviates from addressing IoT's major requirements pertaining to its scale, heterogeneity, power consumption, and QoS policies. With the smart city paradigm gaining momentum, industry and academia have recently undertaken substantial efforts towards designing IoT-friendly cellular communication. This points to a new era for cellular networks to the extent that they can dominate smart city expansion during the next decade. In this section, we review recent developments in IoT-centric cellular communication and study the their main enablers. The summary of our discussion about these transitions is tabulated in Table 5.

4G/LTE: First introduced in 2008, Long Term Evolution (LTE) Release-8 (R-8) operates in the licensed spectrum (between 600 MHz to 3.5 GHz) and originally targets high-throughput Human Type Communication (HTC). Since its inception, LTE has been subject to major HTC-oriented improvements, where newer releases have been constantly adding gradual efficiency enhancements and complementary features such as public warning and Voice over LTE (VoLTE). Although LTE has been proven to be effective for HTC communication, its applicability to IoT implementations remained limited to high-throughput low-latency backhaul networks

ACCEPTED MANUSCRIPT

tuned for multimedia services. Even Category-1 (CAT-1) devices with reduced data rates of up to 10 Mbps for downlink (connection form evolved NodeB (eNB) to User Equipment (UE)) and 5 Mbps for uplink (connection from UE to eNB) could not satisfy low-power and low-complexity requirements of many smart city applications.

LTE R-12: The first major development toward Machine Type Communication (MTC—a term used by Third Generation Partnership Project (3GPP) to describe machine-to-machine communication) transpired in Release 12 (R-12) by defining Category 0 (CAT-0) devices with low-power and low-rate (up to 1 Mbps for both uplink and downlink) capability. To provide simplicity and low implementation cost, CAT-0 devices utilize single-chain antennas and provide Frequency Division Duplex. With the release of R-12, the carrier bandwidth was reduced to 20 MHz to trade off QoS for reduced complexity, cost, and energy consumption. R-12 also introduces LTE Proximity Services (ProSe, also called LTE Direct), which allows device-to-device (D2D) communication, with or without the intervention of eNB. *Sidelinks* (direct connections between two UEs), use Physical Uplink Shared Channel (PUSCH) resources and are supported through a new interface referred to as PC5 [199]. Original specifications of LTE ProSe emphasize public safety services as the main application; note the efforts to investigate social and economic aspects of ProSe [200]. The most important step taken toward making LTE more IoT-friendly in LTE R-12, however, can be associated with introduction of Narrow Band-IoT (NB-IoT); a major overhaul to make LTE a viable candidate for Low Power Wide Area Networks (LPWAN). Although NB-IoT is defined as a subset of LTE, we dedicate a separate section to it due to its importance.

LTE Advanced Pro: Further enhancing LTE compatibility for IoT, LTE Advanced Pro (R-13 and beyond) define CAT-M1 devices for enhanced MTC (eMTC). While reducing device bandwidth to 1.4 MHz, CAT-M1 devices offer half-duplex FDD connectivity. Reducing the transmission power simplifies the hardware implementation of an IoT device, which not only decreases deployment costs but also improves power efficiency. To further reduce latency and power consumption, R-13 MTC includes simplified handshaking and semi-persistent scheduling [201]. Employing a Multiple Input Multiple Output (MIMO)-based beam-forming, R-13 uses spatial multiplexing to substantially improve spectrum efficiency and support a larger number of devices per cell; a maximum of 16 antennas are supported [202]. R-13 MTC also deploys signal repetition and frequency hopping in Physical Random Access Channel (PRACH) to trade off latency for reduced path loss and extended range. Regarding ProSe, R-13 MTC includes modifications that allow multi-hop D2D connectivity [203]. CAT-M1 devices benefit from extended sleep durations (for days) without losing their network registration [198]. New in R-13, LTE MTC can opportunistically utilize unlicensed 5 GHz frequency bands to further improve the performance of its downlink channel. Considering that the popular IEEE 802.11ac also operates in this frequency band, the *Listen Before Talk (LBT)* mechanism is employed to address coexistence-related issues and ensure fair medium access. This *Licensed Assisted Access (LAA)* can be utilized to extend LTE range in indoor deployments [202].

High-throughput, long range, low-latency, and reliability that arises from the utilization of licensed frequency bands have created a niche market for traditional LTE in smart city applications that utilize LTE as the backhaul network for high-bandwidth multi-media traffic cameras. Except LTE, none of the Radio Access Technologies (RATs) discussed so far are capable of satisfying the requirements of such applications, which renders LTE an indispensable constituent of IoT, even without considering numerous MTC-oriented enhanced services introduced in R-13 and R-14. eMTC CAT-M devices target the in-field communication front-end, directly challenging technologies such as IEEE 802.11ah and emerging LPWANs; CAT-M devices are superior to traditional CAT-1 devices, as they can offer: **(i)** reduced complexity (80% less complex than CAT-1 devices), which leads to reduced implementation costs (as low as $1 USD, which is around 20% less expensive than Enhanced GPRS [204]), **(ii)** additional Power Saving Modes (PSMs) that can prolong the battery life of smart city devices [205], **(iii)** full backward compatibility with 2G, 3G, and 4G technologies, **(iv)** mobility support of up to 150 km/h, and **(v)** wider coverage due to increased SNR [204], while maintaining a throughput of 1 Mbps for both uplink and downlink channels. Additionally, built-in compatibility with IP arms LTE with another advantage over its competitors [206]. Furthermore, D2D connectivity introduced in R-12 enhances throughput and spectrum efficiency. Bypassing eNB and Evolved Packet Core (EPC) substantially improves network latency as well [207]. Calibrating LAA parameters (such as energy threshold and freeze period) precisely not only increases the coverage of macro cells, but also enables LTE to support dense networks and larger number of devices [208]. LTE also benefits from robust security and privacy measures.

Leaving aside its niche market, major obstacles hin-

ACCEPTED MANUSCRIPT

der the widespread employment of HTC LTE in IoT and smart city applications. Most notable than others, LTE Advanced (R-10 and beyond) devices are known to be power-hungry and cost an order of magnitude more than their competitors (even in comparison to older 3G and 3G technologies) [209]. Furthermore, LTE-A suffers from limited scalability and fails to maintain a large number of simultaneous connections [210]. Even MTC and eMTC fail to fully address requirements of smart city front-ends. A major limitation can be associated with the heterogeneity of IoT; merely categorizing devices to CAT-0 and CAT-1 is insufficient to satisfy the diverse QoS requirements of smart city applications. Hence, more complicated grouping techniques are necessary [211]. Furthermore, although the Random Access Channel (RACH) mechanism employed in MTC effectively avoids the coordination overhead of centralized techniques, its performance degrades as the number of contending nodes increases [212]. Additionally, in spite of overhead reductions in the latest releases, eMTC still suffers from substantial packet overheads. This overhead takes its toll on network performance in large-scale smart city applications, where nodes tend to transmit a large number of small size packets (in contrast to HTC multimedia traffic patterns) [213]. LTE is also vulnerable to DoS, Access priority indicator, and device trigger attacks [205]. LTE is not recommended for delay-sensitive applications, as both Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and EPC substantially increase the latency of the network [214].

Traditional LTE is suitable for backhaul networks, where power consumption and cost are of not primary concern. MTC and eMTC support relatively high data rates (up to 1 Mbps) and are, therefore, suitable for sparse mobile networks that deliver multimedia traffic. For example, authors in [215] use LTE for crowd surveillance applications using Unmanned Aerial Vehicles (UAVs). Authors in [216, 217] introduce a framework named AXaaS (Acceleration as a Service), in which Telecom Service Providers (TSPs) sell high-intensity computation services over LTE, LTE Advanced, or 5G.

Due to its extended coverage, LTE is also a viable solution for Advanced Metering Infrastructures (AMIs) [218]. In addition to public safety and emergency management applications, LTE Direct is applicable to wide range of smart city services. It can discover thousands of devices in a radius of 500 m in less than a second, without collecting personal and identity information and endangering the privacy of users, which makes it ideal for crowd-sensing applications [219]. Finally, R-14 includes multiple modifications, facilitating the application of LTE D2D connectivity to Vehicle-to-Everything (V2X) connectivity. Unsupervised implementation of LTE D2D coupled with the LAA technique implies numerous advantages: **(i)** it reduces delay and latency, **(ii)** improves reliability of the network by preventing eNB to become the single point of failure, **(iii)** better supports MTC as opposed to HTC [220].

NB-IoT: First introduced in 3GPP Release 13 (R-13), Narrowband-IoT (NB-IoT) can be viewed as a simplified LTE targeting Low Power Wide Area Networks (LPWANs) applications. NB-IoT operates in the 7 MHz–900 MHz licensed frequency band. It uses Orthogonal Frequency Division Multiple Access (OFDMA) for downlink and Single-Carrier FDMA (SC-FDMA) modulation for uplink. Receive channel width in NB-IoT is reduced to one Physical Resource Block (PRB) or equivalently 180 kHz (in contrast to 20 MHz channel width for CAT-1 and 1.4 MHz for CAT-M devices), which reduces network throughput to 20 kbps and 60 kbps for downlink and uplink, respectively [204]. Using shorter channels along with signal repetition techniques increases the coverage up to 30 km in rural areas (20 dB higher gain than LTE) [221]. Inheriting its implementation from LTE, NB-IoT can coexist with multiple cellular services such as GPRS, GSM, 3G, and 4G, without causing significant interference. However, compatibility with these technologies remain fairly limited. Aside from the extended range, the main advantages of reducing receive channel include superior energy consumption profile, lower complexity (and hence lower cost), and better scalability. For devices transmitting 200 bytes a day, a battery life of 10 years can be expected [222]. Compatible devices benefit from an approximately ten-fold reduction in complexity (in comparison to CAT-1 devices), achieved by reducing sampling rates, utilization of a single antenna and a single transmission stream, half-duplex FDD support, and non-parallel processing due to sequential nature of procedures [221]. From a scalability standpoint, each cell can provide connectivity for more than 50,000 devices [198]. From a coexistence standpoint with LTE, NB-IoT can operate in three modes: **(i)** in *in-band* operation, the required PRB is allocated within LTE carriers, **(ii)** in *guard-band* operation, resources are allocated within the LTE guard band. This operation mode reduces the impact of NB-IoT on LTE; however, LTE guard ban is fairly limited, **(iii)** in *standalone* operation, resources are allocated outside the LTE carrier (within GMS carriers). This minimizes the interaction with LTE, but requires dedicated bandwidth to be allocated to NB-IoT. R-14 (completed in Jun 2017) introduced

ACCEPTED MANUSCRIPT

multiple enhancements to NB-IoT including positioning services and multi-casting. Most importantly, it defines category-NB2 (CAT-NB2) devices with enhanced data rates, 120 kbps and 160 kbps for downlink and uplink, respectively [223].

Operating in a licensed frequency band, NB-IoT outperforms its LPWAN competitors, such as LoRa and SIGFOX, in terms of reliability, which renders it a better choice for mission-critical applications. Furthermore, it provides higher data rates in comparison to LoRa. NB-IoT also benefits from complete IP and non-IP network compatibility, built into the architecture of the technology [224]. Recycling various components of the LTE technology introduces multiple advantages to the system. First, it enables operators to add NB-IoT compatibility to their Public Land Mobile Network (PLMN) through mere software updates, thereby substantially reducing deployment costs [225]. UE producers also benefit from this feature as they can readily tweak their LTE device manufacturing processes to build CAT-NB1 and CAT-NB2 devices. Additionally, it reduces LTE coexistence-related complications [222]. Finally, NB-IoT extends Discontinuous Reception (DRX) sleep periods to 175 minutes, as opposed to 2.56 s in LTE. Furthermore, newly defined Power Saving Modes (PSMs) make it possible for a device to remain in sleep mode for several months, hence decreasing energy consumption and extending battery life [223].

Signal repetition (a maximum of 2048 and 128 repetitions are allowed for downlink and uplink, respectively [226]) is used by NB-IoT to extend coverage and enhance reliability. However, it typically adds to network's latency and power consumption [227]. NB-IoT fails to meet latency requirements of delay sensitive applications, as latencies lower than 10 s cannot be not guaranteed [222]. Due to the overhead of network synchronization, NB-IoT offers an inferior energy consumption profile than its LoRa competitor. Authors in [228] study the negative impact of handshaking overhead in NB-IoT—particularly when used along with higher level protocols such as CoAP and DTLS, which introduce additional handshaking activity—and offer solutions to improve the energy efficiency. Such solutions, however, have negative impact on network performance. Additionally, in-band operation of NB-IoT may reduce the performance of LTE [229]. Because it runs on LTE infrastructure, providing NB-IoT services to rural and remote areas not covered by LTE remains challenging and financially prohibitive. Due to these disadvantages, NB-IoT deployment rate and market penetration has been quite unimpressive.

Due to its relatively low throughput, NB-IoT is not suitable for handling multimedia traffic. However, its remarkable coverage, low power consumption, low cost, and scalability make it ideal for large-scale dense sensing and crowd-sensing networks [221]. NB-IoT supports limited mobility. It is not suitable for delay-sensitive applications, since NB-IoT does not guarantee low-latency delivery. Furthermore, as of now, the coverage of NB-IoT in the US remains quite limited.

5G: Currently undergoing development, 5G is expected to be finalized by 2020. In comparison to the older generation, 4G, multiple design goals are defined for 5G including: **(i)** achieving data rates as high as 10 Gbps, **(ii)** reducing power consumption by 90%, **(iii)** supporting a significant number connections per cell, and **(iv)** targeting latencies lower than 1 ms and improving network availability [237]. 5G employs the latest communication techniques such as deployment of millimeter waves (mmWaves), small cells, Space Division Multiple Access (SDMA), and Cloud-Radio Access Network (C-RAN) to satisfy these daunting requirements. By utilizing the high frequency (3–300 GHz) licensed spectrum, 5G not only avoids already-congested macrowave bands, but also paves the way to support substantially higher data rates and larger number of connections (in the order of millions per cell). Regardless of their desirable characteristics, mmWaves suffer from path loss and limited Line Of Sight (LOS) problems. These limitations are tackled by the deployment of small size cells such as phantom, micro, pico, and femtocells. Centered around Relay Stations (RSs), which are substantially less complicated than Base Stations, small cells help mmWave signals propagate further and reach out of LOS ares and indoor environments. RSs typically cover an area of around 200 meters in radius [238]. Based on their functionality, RSs can be categorized as *amplify and forward*, *demodulation and forward*, *decode and forward*, and *buffer aided*, which demodulate, decode, and buffer received signals until the status of the channel allows re-modulation and retransmission [159].

Complementing small cells, SDMA is implemented in 5G by substituting omni-directional antennas with directional transceivers. Relying on beam-forming and MIMO increases spectrum efficiency and mitigates the LOS drawback of mmWaves. C-RAN physically and virtually separates Baseband Units (*BBUs*) from *Remote Radio Heads* (*RRHs*), allowing centralized allocation of BBUs and paving the way toward RAN as a Service (RANaaS) [159]. The connection between BBUs and RRHs is maintained through high-speed low-latency fiber optic cables. Additionally, 5G is outfitted with D2D, unlicensed spectrum access, and non-

ACCEPTED MANUSCRIPT

Table 5: A summary of Cellular technologies and their applications in smart city arena. *Example applications* includes implementations, in which each technology is widely used. The information represented in this table is not exclusive. Although LTE and NB-IoT belong to the same technology, they are considered as separate due to the differences in their target applications. Furthermore, as 5G is yet to be finalized, no actual 5G sensor network currently exists.

Technology / Characteristics	**Advantages/ Disadvantages**	**Example Applications**	**Suggested Application**
4G/LTE (eMTC) / 600 MHz–3.5 GHz Licensed Band 5 GHz LAA High Data Rate (≥ 1 Mbps) Long Range (≥ 500 m)	⇑ High Throughput/Long Range ⇑ Low Complexity/Low Cost ⇑ Fully IP Compatible ⇑ Advanced PSMs/ Increased SNR ⇑ Backward Compatible ⇑ Multi-Cast Support ⇑ Licensed Assisted Access (LAA) ⇓ High Power Consumption ⇓ Poor Scalability ⇓ Poor Heterogeneity Support ⇓ Communication Overhead ⇓ Long EUTRAN/EPC Delay ⇓ Limited Coverage In Rural Areas	Smart Metering [218] V2X [220] Air Quality Monitoring [230] Emergency Management [231] Crowd-sensing [219] Smart Surveillance [215]	High Traffic Backhaul Networks (Multimedia Traffic) / Delay Tolerant Wide Area Mobile Networks (Multimedia Traffic)
Narrowband-IoT (NB-IoT) / 7 MHz–900 MHz Licensed Band Low Data Rate (≤ 160 kbps) Long Range (≤ 30 km)	⇑ Long Range ⇑ Low Complexity/Low Cost ⇑ Fully IP Compatible ⇑ Extended PSM Duration ⇑ Good Coexistence With 3G/4G ⇑ Reusing LTE Infrastructure ⇑ Multi-Cast Support ⇓ Indeterministic Latency ⇓ Synch./Handshaking Overhead ⇓ Unimpressive Market Penetration ⇓ Low Energy Efficiency (vs LoRa) ⇓ Limited Coverage In Rural Areas	AMI Air Quality Monitoring Environment Monitoring Smart Transportation Smart Utilities Smart Grid	Large Scale Dense Network (Scalar Traffic) / Delay-Tolerant Wide-Area Outdoor Networks (Scalar Traffic)
5G / 30 GHz–300 GHz Licensed Band Sub-30 GHz LTE Licensed Band High Throughput (≤ 10 Gbps) Long Range	⇑ Long Range/Scalable ⇑ Mobility Support (500 kmph) ⇑ Fully IP Compatible ⇑ Good Coexistence With Other RATs ⇑ Multi-Cast Support ⇑ Reliability/Low Latency ⇑ SDR-Oriented Design/Virtualization ⇓ mmWave-Related Uncertainties ⇓ Higher Power Consumption ⇓ Limited Coverage In Rural Areas ⇓ Dependence On Operators	Process Automation [232] V2X [233] Smart Grids [234] Environment Monitoring [235] Smart Health [236] Smart Metering Smart Surveillance	Large Scale Dense Networks (Multimedia Traffic) / Delay-Sensitive Mission-Critical Networks (Scalar Traffic) / Long-Range Backhaul Networks (Multimedia Traffic)

orthogonal access. In terms of HTC, these advances translate to breakthroughs in QoS and Quality of Experience (QoE), while motivating a new family of applications and services such as location-based services, Virtual and Augmented reality, and HD multimedia traffic. Regarding MTC, 5G targets two types of networks: **(i)** Massive MTC (mMTC), which refers to networks with relaxed QoS requirements encompassing a large number of devices and **(ii)** Ultra Reliable Low Latency Communication (URLLC), which is used in mission critical scenarios such as industrial process automations.

Owing to its modern technology and partly due to its ongoing development status, 5G is often portrayed as a panacea for IoT and MTC. Numerous strengths

ACCEPTED MANUSCRIPT

and improvements of the next generation mobile technology rest upon 5G; it provides remarkable throughput, unseen in any other RAT; it is designed for highly mobile networks (up to 500 km/h); and includes built-in mechanisms to ensure outstanding coexistence with other RATs such as LTE, WiFi, and BLE. For example, authors in [239] propose a *multi-connection* technique, where 5G devices can dynamically assess and switch among multiple RATs such as LTE, LoRa, ZigBee, etc., improving the reliability of communication for mission-critical industrial applications. Another track of research focuses on the ability of 5G for Simultaneous Wireless Information and Power Transfer (SWIPT), investigating the possibility of 5G-powered perpetual smart city sensing networks [240]. Decreasing cell size and shifting the network architecture towards a UE-centric implementation (as opposed to the BS-centric architecture of LTE) augments the connectivity in multiple aspects. First, it prevents the BS from becoming a single point of failure, hence reducing its dependence on the BS. It adds scalability and helps distribute the traffic among RSs evenly in dense networks. Using Full Duplex communication, 5G increases network efficiency and avoids the hidden-terminal problem [237]. Furthermore, multiple studies investigate the benefits of utilizing small cells to separate the control and data transmission plane, which can potentially improve coverage and spectrum efficiency. Furthermore, 5G implementation leans towards Software Defined Networks (SDR), allowing the network to be adjusted using application layer APIs [241]. Finally, employing C-RAN and RANaaS allows resource pooling, increases resource utilization, reduces deployment costs, adds support for enhanced mobility and increased scalability, and can potentially lead to new applications in smart cities.

Although it is difficult to discuss the shortcomings of 5G—as it is still under active development—it is still possible to investigate some of the challenges it faces. For example, authors in [242] study the power consumption of a 5G network and propose MIMO-based techniques and local caching of data to improve energy efficiency. 5G is not expected to be fully backward compatible with LTE and 3G, which can stymie its diffusion rate [243]. Another challenge 5G development faces can be associated with mmWave characteristics. Modeling the propagation of these signals involves numerous uncertainties and is still the subject of ongoing research [244, 245, 246]. Finally, like other cellular networks, any 5G deployment involves third party service providers and operators. Aside from these challenges, network *uniformity* promised by 5G seems to be one of its most important advantages. Impressive scalability coupled with good coexistence with incumbent RATs makes 5G ideal for large-scale and dense networks. Its built-in mechanisms to simultaneously satisfy various QoS requirements, make this technology friendly to heterogeneous networks. Enhanced mobility along with the remarkable ≤ 1 ms delay provides a solid solution for mission-critical systems. Consequently, it is expected that 5G is adopted by a wide range of smart city applications and in the meantime provide a seamless interface between MTC and HTC, thereby reducing technology heterogeneity and facilitating inter-application services.

5.4. Low Power Wide Area Networks (LPWANs)

Low Power Wide Area Networks (LPWANs) aim to bridge the gap between wide area coverage of cellular networks and low power consumption of WPANs and WLANs. Unfortunately, fulfilling this objective and preserving the simplicity of the network and its devices—in order to optimize recurring and non-recurring expenses—oftentimes results in the degradation of both throughput and latency. Utilization of Narrow Band (NB) and Ultra NB (UNB) in the license-free sub-GHz ISM band is the major enabler of these technologies; since sub-GHz signals possess path loss resistance and they do not suffer from narrow LOS problem, their application directly translates to extended coverage. Furthermore, the sub-GHz frequency band is not congested, which reduces the possibility of collision and interference, consequently enhancing the performance of the network. However, the Sub-GHz ISM band is subject to stringent regulations, which steered some LPWAN technologies, such as INGENU's RPMA, toward the alternative 2.4 GHz ISM band [198]. In this section, we investigate and compare a selected set of LPWAN technologies.

LoRaWAN: Operating in the sub-GHz frequency band (902–928 MHz ISM in the US), LoRaWAN targets *Lo*ng-*Ra*nge (≈15 km), low-power, and low-data rate (37.5 kbps) communication. LoRaWAN is a modified technology, which is based on the physical layer of LoRa®, a proprietary technology developed by Semtech [247]. However, other layers of LoRaWAN are open [210] and are sponsored by the LoRaAlliance™ [248]. LoRaWAN architecture has similarities to cellular networks and is typically described as *star-of-stars*. It is centered around three types of devices: **(i)** *end-devices*, **(ii)** *gateways*, and **(iii)** *network server*. End-devices are the sensing nodes that collect data from the environment and forward it to one or more gateways using the LoRa physical layer. Approximately 10,000 end devices can be connected to a gateway [210]. Gateway(s) are connected to one centralized

ACCEPTED MANUSCRIPT

network server, over an IP-based communication, which provides application layer APIs to interact with the data and the network [249]. Gateways do not perform any data processing on the received data and merely forward them to the network server. An end-device is allowed to transmit its data to multiple gateways, thereby improving the odds of packet delivery. Packet duplicates must be handled by the network server [107].

LoRaWAN PHY layer provides bi-directional communication, which makes it applicable to both sensors and actuators. It uses *m*-ary Frequency Shift Keying (FSK) and Chirp Spread Spectrum (CSS) modulation to extend its communication range by trading off the data rate. Spreading Factor (SF) of CSS determines the data rate (DR) of the communication (according to the following formula: $DR = Bandwidth/2^{SF}$, where SF changes between 7 and 12); therefore, the effective data rate of the nodes farther from the gateway is decreased to make up for signal propagation losses. Because SFs are orthogonal, multiple signals can be received by a gateway simultaneously [250]. The MAC layer is based on an ALOHA-like medium access method and is designed to be compatible with higher level layers such as 6LoWPAN and CoAP [210].

To address the heterogeneity of QoS in many IoT application to some extent, LoRaWAN defines three types of devices based on their downlink access priority. *Class A* devices can only receive downlink traffic during two receive windows, which are reserved for them after each data transmission. *Class B* devices can receive downlink traffic either during receive windows (similar to Class A end-devices) or during pre-defined reception periods. Their access to the channel is coordinated through beacons transmitted by gateways. *Class C* devices can request receive channel access in any moment (except during data transmission). Class A devices suffer from long downlink latency, while offering superior energy efficiency. Class C devices enjoy relatively lower receive delays at the expense of higher energy consumption and complexity [250].

LoRaWAN outperforms its competitors in terms of complexity. Authors in [251] note that each LoRaWAN module costs around $2–5 USD, which is considerably cheaper than its cellular competitor, eMTC, which is priced at around $8–12 USD per piece. The reduction in cost is partly due to the relaxation of frequency offset (up to 20% is tolerated), which reduces crystal expenses [249]. Furthermore, unlike NB-IoT and eMTC, LoRaWAN deployment does not involve complying with policies of third party operators. Although the LoRa PHY layer is proprietary, LoRaWAN specifications are available to public, which makes its study and deployment easy. Compatible devices are already available in the market and LoRaWAN deployment rates have surpassed comparable cellular solutions such as NB-IoT. Downlink channel support makes LoRaWAN applicable to actuator-based networks, albeit in a limited fashion. The technology also supports ACK packets to enhance communication reliability. Counter-intuitively, study conducted in [250] shows that acknowledgement transmission improves the performance of the network in terms of energy efficiency. This is because the end-devices can remain in sleep mode during the second receive window if they receive the ACK packet in the first one.

Defining three device classes alleviates QoS heterogeneity, particularly, considering that device classes can be changed dynamically. In [250], authors show that a device transmitting data every five minutes can achieve a lifetime of approximately one year when powered by a 2400 mAh battery. To secure data integrity, LoRaWAN utilizes Cyclic Redundancy Check (CRC) and 128-bit AES for all communication between end-devices and the network server. Finally, it is recently shown in [252] that *Concurrent Transmission* (*CT*) techniques can be applied to LoRaWAN to create a multi-hop CT LoRa technology for indoor deployment. CT is an innovative transmission technique that enhances latency, energy consumption, and throughput of the network by relaxing collision-avoidance mechanisms of wireless standards.

Because of its operation in the sub-GHz band, LoRaWAN is subject to strict regulations and duty cycling limitations. These regulations impact both end-devices and gateways; gateway duty cycling disrupts transmission of ACK packets, thereby, practically making LoRaWAN unsuitable for mission-critical applications [251]. In general, increasing downlink traffic substantially decreases the performance of the LoRaWAN technology [253]. Regarding end-device power consumption, LoRaWAN falls behind primary WLAN technologies such as BLE and ZigBee. For instance, the study conducted in [250] shows that LoRaWAN end-devices draw approximately seven times more current than WLANs in sleep mode. Aside from the CT techniques, leveraging a star topology translates to limited suitability for indoor (multi-building) applications. Employing a channel access mechanism similar to ALOHA poses a practical limitation to the maximum load the network can handle [249]. LoRaWAN does not support D2D connectivity.

LoRaWAN low-rate data transfer capability makes it only applicable to low-load networks, which encompass a wide range of applications such as smart grid and smart metering. Its remarkable coverage coupled with

ACCEPTED MANUSCRIPT

support for tens or hundreds of thousands end-devices per gateway makes LoRaWAN the natural selection for wide-area outdoor applications. However, this technology cannot fulfill the timing requirements of mission-critical and delay-sensitive services, nor can it be used in applications that involve substantial downlink traffic.

Sigfox: Ultra Narrow Band (UNB) Sigfox was introduced in 2009. It is a proprietary long-range low-power RAT with very limited data rates. It operates in the sub-GHz ISM frequency band and supports data rates of 100 bps. The frequency band is divided into 400 channels, each 100 Hz wide, hence practically becoming an ultra narrowband technology. Utilizing UNB channels in parallel to Binary PSK modulation (downlink modulation is conducted using the GPSK technique) enables coverage of around 50 km in rural areas [198]. Packet sizes are limited to 12 bytes; as a result of stringent regulations that govern sub-GHz frequency band, each device can only transmit up to a maximum of 140 messages a day [249]. Sigfox adopts a client-server architecture, which resembles LoRaWAN and cellular networks, where up to a million end-devices can transmit their data to a *Base Station* (*BS*) [256]. Packets received by the BS are forwarded to a server through an IP-based network. A *cooperative reception* mechanism is built-into Sigfox, which allows a signal to be received with multiple BSs in range, thereby increasing packet delivery chances. Sigfox was originally designed for uplink-only data transfer, however, recent updates have added support for downlink traffic. Each device scans the channel for downlink traffic after transmission [257]. Downlink opportunity window is 10 s and each message cannot be more than eight bytes.

The primary strengths of Sigfox are low power consumption, impressive coverage in urban and rural areas, and low deployment costs. Particularly, the adoption of a client-server model has eliminated the synchronization overhead (unlike cellular RATs, where devices must periodically wake up for paging), thereby reducing costs and enhancing energy efficiency. Furthermore, utilization of UNB improves the scalability of the network as well as its robustness against noise [257]. Finally, Sigfox enhances the probability of successful packet delivery by requiring each device to repeat its transmissions three times, in different frequencies using different encoding schemes, as well as implementing *cooperative* reception mechanism, where a signal can be received by multiple BSs [258].

The primary drawback of Sigfox is its limited data rate. In comparison to LoRaWAN, Sigfox suffers from an $\approx 10\times$ reduction in throughput [258]. Particularly, scant downlink opportunities render important services such as *over-the-air updates* and *command-and-control*, impractical [249]. Strict regulations of the sub-GHz frequency band translate to prolonged latencies most of the time, exacerbating the low data rate disadvantage. For example, considering a duty cycle of 1%, each device cannot hold the channel for longer than 3.6 s in an hour (enough time to send 37 messages at 100 bps). Therefore, a latency of at least one hour is imposed on every device that needs to send more than 37 messages in a single transmission. Finally, in the absence of encryption mechanisms, Sigfox merely relies on frequency hopping and an indeterministic payload format to safeguard the communication between the device and BS [259].

Overall, application uses of Sigfox and LoRaWAN are alike; both target outdoor wide area networks with an extremely limited downlink traffic. This limitation, however, does not prevent Sigfox from becoming an inexpensive and effective solution for smart homes, environment monitoring, air quality monitoring, and smart metering. These applications are inherently sensor-based (as opposed to sensor/actuator-based) and involve very limited downlink traffic. Sigfox is particularly enjoying an impressive growth in Europe, while offering acceptable coverage in the big cities of North America, Australia, and Japan [260]. Sigfox is not the best option for mission-critical and latency-sensitive applications and its performance is shown to suffer as data size increases [258]. Table 6 contrasts the foregoing LPWAN technologies from the standpoint of their strengths, shortcomings, and typical applications.

5.5. Visible Light Communication (VLC)

Visible Light Communication (VLC), or alternatively Light Fidelity (LiFi), is an emerging short-range and *potentially* high-throughput communication technique for next generation smart city applications. The emergence of VLC can be mostly attributed to the gradual substitution of power-hungry incandescent light bulbs with efficient Light Emitting Diodes (LEDs), which is fueled by advances in solid-state electronics. Unlike their predecessors, LEDs are intrinsically compatible with high-frequency switching (in the order of multiple MHz), thereby making them compatible with high-speed data communication (up to $\approx$10 Gbps, under ideal circumstances). In this section, we study the IEEE 802.15.7 standard as the most promising VLC protocol.

IEEE 802.15.7: IEEE 802.15.7 was published in 2011 as a VLC standard, designed to provide high data rate connectivity for (mostly) indoor WPANs. The standard includes the specification of PHY and MAC layers. The PHY layer operates in the visible light frequency

ACCEPTED MANUSCRIPT

Table 6: A summary of Low Power Wide Area Networks (LPWANs) and their applications in smart city arena. *Example applications* includes some implementations in which each technology is either used or recommended to be used.

Technology/ Characteristics	**Advantages/ Disadvantages**	**Example Applications**	**Suggested Application**
LoRaWAN / 902–928 MHz ISM Band (US) Narrowband (NB) Low Data Rate ($\leq$ 50 kbps) Long Range ($\leq$ 15 km) Low Power	$\Uparrow$ Inexpensive/Extensive Range $\Uparrow$ Open Specifications $\Uparrow$ Acknowledged Transmission $\Uparrow$ Dynamic Class Selection $\Uparrow$ Concurrent Transmission $\Uparrow$ Available In Market $\Downarrow$ Very Low Data Rate $\Downarrow$ Limited Downlink Capacity $\Downarrow$ Sub-GHz Band Regulations $\Downarrow$ High Latency $\Downarrow$ No D2D Support $\Downarrow$ Practical Traffic Limit	Environmental Monitoring [210] Smart Lighting [251] Smart Grid [254] Smart Home (HVAC) [254] Smart Metering [254] Industrial Automation (Limited) [254] Smart Waste Management [255]	Low Traffic Delay-Tolerant Networks (Scalar Traffic) / Outdoor Large-Scale Uplink-Only Networks (Scalar Traffic)
Sigfox / 902–928 MHz ISM Band (US) Ultra Narrowband Low Data Rate ($\leq$ 100 bps) Long Range ($\leq$ 50 km) Low Power Proprietary	$\Uparrow$ Inexpensive/Extensive Range $\Uparrow$ Low Synchronization Overhead $\Uparrow$ Robustness to Noise $\Uparrow$ Cooperative Reception $\Uparrow$ Impressive Coverage (Europe) $\Downarrow$ 10$\times$ Lower Rate Than LoRaWAN $\Downarrow$ Scant Downlink Capacity $\Downarrow$ Sub-GHz Band Regulations $\Downarrow$ High Latency/No D2D Support $\Downarrow$ No Encryption $\Downarrow$ Practical Traffic Limit	Environmental Monitoring Smart Grid Smart Home Smart Metering Air Quality Monitoring	Extremely Low Traffic Delay-Tolerant Networks (Scalar Traffic) / Outdoor Large-Scale Uplink-Only Networks (Scalar Traffic)

band (400–800 THz) and supports three modes of operation.

- *PHY I* targets LEDs with limited switching capabilities and provides data rates ranging from 11.67–266.6 kbps,
- *PHY II* throughput can be adjusted between 1.25–96 Mbps and is typically suggested for portable devices such as smartphones, and
- *PHY III* provides the maximum data rate of 96 Mbps using MIMO technique (for white lights encompassing an array of RGB LEDs) [261].

Medium access is controlled using Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism with support for broadcasting, star, and peer-to-peer topologies. Similar to other Optical Communication Systems such as fiber optic and Infra Red (IR) wireless communication, IEEE 802.15.7 implementations typically involve two types of devices. An Access Point (AP, also referred to as the *coordinator*) transmits visible light signals modulated using Intensity Modulation (IM) techniques—where digital content of the signal is represented by different levels of light intensity. A Photo Diode (PD) receives and demodulates the signals using Direct Detection (DD)—where the incident of photons generates an electric current proportional (almost linearly) to the number of received photons. IEEE 802.15.7 is developed to add communication capabilities atop the illumination functionality of normal LED lights. This double-purpose implementation introduces additional complications in *flicker mitigation* and *dimming support*. The former is associated with the side-effects of light intensity fluctuations on humans' health, while the latter mandates that IEEE 802.15.7 devices must be able to resume their operation unhindered when users dim light intensity of their lighting systems (for example, to save energy or to adjust the light for a specific activity such as reading or watching TV). Any solution to satisfy these two requirements must deliver light intensity controlling and energy saving without negatively impacting communication performance. Flicker mitigation can be satisfied by imposing Maximum Flickering Time Period (MFTP), which defines a threshold for the highest flick-

ACCEPTED MANUSCRIPT

ering frequency detectable by human eyes (typically around 200 Hz). Dimming support solutions in IEEE 802.15.7 can be categorized into modulation-based and coding-based techniques [262]. In modulation-based solutions, On-Off Keying (OOK) and Variable Pulse Positioning Modulation (VPPM) are employed to modulate data according to the *dimming target*. In OOK, different light intensity levels are used to represent the data. For example, OFF can be associated with logic 0 and ON can represent logic 1. To ensure dimming support, OOK uses Inter-Pulse Padding, where a group of redundant 0s and 1s are added to the signal to achieve the dimming target [263]. OOK can also adjust the intensity levels allocated to 1s and 0s to meet dimming goals, thereby avoiding the negative impact on performance caused by inserting redundant bits. This solution, however, under-drives LEDs leading to chromaticity shifts [262]. Alternatively, VPPM meets dimming requirements by adjusting the duty cycle of the modulated data using Pulse Width Modulation (PWM). Coding-based techniques such as Inverse Source Coding (ISC) can be utilized to minimize the impact of dimming support on communication performance. In ISC, coding schemes are used to control the ratio (or probability) of 1s to 0s based on the desired light intensity. IEEE 802.15.7 channel access is controlled by *beacons*, which the coordinator periodically broadcasts in the beginning of each superframe. End devices can use the CSMA/CA technique to compete for channel access during Contention Access Period (CAP). Superframes also include a Contention-Free Period (CFP) for latency-sensitive communications that require guaranteed bandwidth. Alternatively, non-Beacon-Enabled Network (non-BEN) is also defined to provide asynchronous unslotted random channel access [264].

Utilizing the visible light spectrum for communication has multiple advantages. First, it does not involve health-related or safety concerns associated with RF signals. Furthermore, outsourcing some of the communication traffic to VLC reduces the load on the already-congested 2.5 GHz and 5 GHz frequency bands. This reduces interference and collision, which leads to increased efficiency (in terms of latency, throughput, and energy consumption) for both VLC and RF techniques. Utilizing the visible light spectrum does not require licensing or meeting strict regulations, which results in a reduction in expenses. Additionally, visible light possesses the same characteristics as IR and the principles of VLC resemble the fundamentals of fiber optics, which further reduces research and development costs. In particular, IEEE 802.15.7 is designed to be compatible with regular lighting applications. Therefore, normal LED lights can be easily adjusted to act as coordinators, implying that unlike RF-based technologies, LiFi does not require an extensive infrastructure. For example, authors in [265] show that existing LEDs can be readily modified as coordinators and PDs to form a low-rate connectivity between objects, as well as objects and users. (With smartphone camera and flash acting as PD and coordinator, respectively.) MIMO compatibility is added to IEEE 802.15.7 by including Color Shift Keying (CSK). This allows white lights (which incorporate an array of RGB LEDs) to achieve higher data rates [261]. Additionally, spatial confinement of visible light improves not only the security robustness of the communication but also the re-usability of the frequency band. Finally, as discussed in [266], reliance on visible light for communication creates a unique opportunity for VLC backscattering, which motivates the realization of a wide array of smart city devices.

Unlike IR, VLC relies on visible light. Therefore, manipulating these signals directly affects users. Mechanisms used in OOK modulation and VPPM are effective to provide flickering mitigation and dimming support. Nonetheless, the increased communication overhead of these techniques degrades the performance of the network. The impact on performance is considerable when dimming targets deviate from the ideal level of 50%. (Statistically, logical 1s and 0s follow a uniform 50% distribution, which implies that the dimming level of 50% can be achieved without any modulation). Intensity domain solution—where a DC component is added to the intensity of the signal based on the dimming goal—can address the redundancy of OOK and VPPM; however, calculating the correct value of the DC component often involves nonlinear computations, which increases the complexity of the LED driver circuitry [263]. Ensuring dimming support also poses challenges regarding the design of LED circuitry, as they must be compatible with both high-frequency modulation and low-frequency dimming signals. This directly translates to increased complexity and cost. PDs are also susceptible to noise induced by virtually any other light source in the environment. A portion of the noise contribution can be related to the non-ideality of the LED driver circuitry. This type of noise typically manifests itself as a nonlinear component, which is difficult to detect and suppress [270]. Limited range coupled with reliance on CSMA/CA leaves IEEE 802.15.7 susceptible to the *hidden terminal problem*. Considering that some devices can remain in sleep mode, classic solutions such as inclusion of Clear To Send (CTS) and Request to Send (RTS) cannot fully address this problem. Experiments conducted in [271] show that the

ACCEPTED MANUSCRIPT

Table 7: A summary of main characteristics, advantages, and disadvantages of IEEE 802.15.7 as a smart city oriented VLC standard. *Example applications* includes example implementations or suggested applications of this technology.

Technology / Characteristics	**Advantages/ Disadvantages**	**Example Applications**	**Suggested Application**
IEEE 802.15.7 / 400–800 THz Visible Light Spectrum Broadband High Throughput (≤ 96 Mbps) Broadcasting, P2P, Star Topologies CSMA/CA Channel Access	⇑ Safe (No Health-Related Concerns) ⇑ No Interference with Other RATs ⇑ No Licensing or Strict Regulation ⇑ Compatible with Typical LEDs ⇑ MIMO Support/ VLC Backscattering ⇑ Reusable (Spatial Confinement) ⇑ Secure (Spatial Confinement) ⇓ Dimming Impact On Performance ⇓ Increased Circuit Complexity ⇓ Complicated Noise Profile ⇓ Hidden Node/ Syncing Problems ⇓ Limited QoS Diversity ⇓ Limited IPv6 Compatibility	Smart Home [264, 267] Smart Transportation [268] Smart Healthcare [269] Smart Lighting	High Traffic Indoor Networks (Stationary and Quasi-Stationary) / Small Cell Last-Mile Indoor Connectivity (HetNets)

hidden terminal problem can substantially affect multiple parameters of the network, including a substantial reduction in Goodput, a sharp increase in packet loss rate, and energy consumption (by an order of approximately 10× under 100% load). Additionally, employing simple modulation techniques such as OOK poses synchronization challenges; utilizing more sophisticated modulation techniques such as OFDM can alleviate this problem, however, underlying characteristics of VLC, such as IM and DD, make it incompatible with OFDM (as OFDM creates non-real and bipolar signals). To address synchronization considerations, the authors in [272] propose various frame detection techniques for Direct Current biased Optical OFDM (DCO-OFDM). Finally, IEEE 802.15.7 fails to address diverse QoS requirements of the IoT applications. Compatibility with IPv6 and the Internet is also limited.

With the increasing share of LED lighting, VLC is becoming increasingly more relevant for short-range indoor communication. This includes home networks and in-vehicle communication for cars, trains, planes, etc. [264]. This implies that VLC is viable for smart home and smart transportation applications. For example, authors in [267] propose a VLC-based system for 3D posture detection of the residents of a house. The aforementioned limitations of VLC, however, coupled with its limited mobility support, reduces its applicability to many smart city applications. Alternatively, major benefits can be gained by utilizing its coexistence with prevalent RATs such WiFi. Offloading a substantial portion of communication to VLC can substantially improve the performance of WiFi and its QoS and QoE (Particularly, considering that 80% of the network load is generated by indoor mobile traffic) [273]. Including VLC in a multi-level heterogeneous network can circumvent its major limitations, including IPv6 incompatibility, limited mobility, and lack of QoS management diversity. Table 7 tabulates our discussion about IEEE 802.15.7 standard.

5.6. Power Line Communication (PLC)

Power Line Communication (PLC) refers to techniques that utilize the existing electric power lines as a communication medium. PLC can provide either reliable narrowband (below 500 kHz) or high-speed broadband (up to 100 MHz, reaching data rates as high as 1 Gbps) connectivity for many IoT applications [274]. In deployment areas where the required power line infrastructure already exists, PLC can outperform many wireless technologies in terms of reliability and cost. Additionally, it can readily pass through obstacles and reach enclosed indoor environments [275]. In this section, we overview some of the most notable efforts undertaken toward PLC implementations.

IEEE 1901-2010/ IEEE 1901.2: IEEE 1901-2010 technology is a broadband (BB) PLC technique, designed particularly for multimedia home traffic and select smart city applications such as smart grid and Au-

ACCEPTED MANUSCRIPT

tomatic Measuring Infrastructure (AMI). IEEE 1901-2010 operates in the 2–30 MHz frequency band and can deliver throughputs up to 500 Mbps. This technology is developed for low and medium voltage power transmission lines and is not compatible with Digital Subscriber Line (DSL) or coax cables. The overall architecture of the network includes a service provider, which typically provides a single *Access Network* (*AN*) over a specific PLC infrastructure. An AN can be divided into multiple *cells* (or equivalently, *Basic Service Sets*). Each cell consists of one or more stations (STAs), *Repeaters* (RPs), *Network Termination Units* (*NTUs*), and a single *Head End* (*HE*). STAs within a cell can communicate with each other either directly or through the HE. However, all communication with the backhaul network must be directed to the HE.

Considering that the maximum distance a signal can travel over power lines is determined by various—and uncontrollable—parameters such as noise, medium quality, and even weather, IEEE 1901-2010 uses RPs to regenerate and re-transfer packets, thereby increasing the coverage of the network. NTUs bridge IEEE 1901 PLC communication with other *In Home* (*IH*) networks such as WiFi and Ethernet. The number of cells in an AN is typically determined by the QoS requirements of STAs, where STAs with the same QoS requirements must be grouped in the same cell [276]. Only PHY and MAC layers are specified in IEEE 1901-2010. The PHY level uses either Fast Fourier Transform (FFT) OFDM or Wavelet OFDM. The MAC layer allows both synchronous and asynchronous medium access, based on TDMA and CSMA/CA mechanisms, respectively. In an AN, HEs are assigned a 6-bit Short Network Identification (SNID), allowing a total of 63 to be defined (SNID zero is reserved). Similarly, a 12-bit Terminal Entity Identification (TEID) is used to address STAs. Therefore, over 4000 Stations can be defined in a single cell [277]. For applications that do not require broadband connectivity, IEEE 1901.2 is a narrowband PLC alternative, which can provides data rates as high as 234 kbps [278]. This technology was first standardized in 2013 and it operates in the 10–490 kHz frequency band (in the US) and uses OFDM modulation to improve robustness against noise. Similar to IEEE 1901.1, IEEE 1901.2 is compatible with low voltage ($\leq$1 kV) and medium voltage (between 1 kV and 73 kV) power lines. Only PHY and MAC layers are specified in this standard. The latter is based on IEEE 802.15.4-2016 and uses the same CSMA/CA medium access mechanism. However, various modifications are included to improve efficiency and add priority-based medium access.

The primary strengths of the IEEE 1901-2010 protocol are its extended coverage, reliable communication over a non-reliable power line infrastructure, and impressive throughput. Additionally, this protocol is capable of supporting thousands of nodes, which addresses the scalability requirement of smart city applications. Furthermore, this technology can be used in a wide range of topologies such mesh, tree, ring, and hybrid. Utilizing both CSMA/CA and Transmission Opportunities (TXOPs) provides the foundation for QoS diversification, thereby addressing the QoS heterogeneity requirement of smart city applications. STAs can coordinate their medium access with their associated HE to receive *differentiated* and *reserved* access, which allows prioritization of STAs based on the application. However, only two priority levels (high and normal) are defined to avoid complicating the network [279].

Security and privacy concerns in IEEE 1901-2010 are mostly addressed by using Robust Security Network Association (RSNA) [276]. IEEE 1901.2 can cater to applications that value simplicity and cost reduction. Utilizing the MAC layer of IEEE 802.15.4-2006 makes IEEE 1901.2 compatible with 6LoWPAN, thereby adding IPv6 compatibility to the protocol [280]. However, unlike IEEE 802.15.4, this standard includes modifications to include both ACK and NACK packages. Furthermore, Automatic Repeat Request (ARQ) is also implemented to improve reliability.

IEEE 1901-2010 suffers from multiple drawbacks. First, 500 Mbps throughput is proven to be unnecessary for many AMI and smart grid applications. Therefore, a substantial gain could be achieved by trading off the throughput for simplicity, power consumption, and cost. Additionally, limiting the compatibility of IEEE 1901-2010 to low and medium voltage power line infrastructures restricts its applicability to environments with an existing Coax or DSL infrastructure [281]. Although priority-based medium access techniques are effective against high latency in delay-sensitive applications, they can potentially lead to resource starvation for nodes with lower priority [275]. Despite great opportunities to substantially enhance the MAC layer efficiency (through adjusting medium access contention parameters, as discussed in [282]), the performance of the network is known to decrease as the number of STAs increases. IEEE 1901.2 does not support multi-casting, which reduces its energy efficiency.

Both IEEE 1901 and IEEE 1901.2 are developed particularly for applications such as smart grid, AMI, and electric vehicles, where power line infrastructure is assumed to be available. The high throughput of IEEE 1901 and its good coexistence for in-home networks

ACCEPTED MANUSCRIPT

Table 8: A summary of Power Line Communication (PLC) technologies and their applications in smart city arena. *Example applications* includes example implementations or suggested applications of this technology.

Technology / Characteristics	**Advantages/ Disadvantages**	**Example Applications**	**Suggested Application**
IEEE 1901 (IEEE 1901.2) / 2–30 MHz (10–490 kHz) Frequency Band (US) Broadband (Narrowband) High Throughput (≤ 500 Mbps) (Low Throughput (≤ 240 kbps)) Indoors and Outdoors	⇑ Various Available Data Rates ⇑ Low Cost Guided Connectivity ⇑ Acknowledged Transmission ⇑ Support for Numerous STAs ⇑ Flexible QoS Management ⇑ IPv6 Compatibility (1901.2) ⇑ RSNA Security ⇑ Mesh, Tree, Ring Topologies ⇓ Coax/DSL Incompatibility ⇓ Potential Medium Access Starvation ⇓ Poor Performance in Large Networks ⇓ Limited Prioritizing Options (1901.2) ⇓ No Multi-Casting	Home Networks [276] Smart Lighting [279] Smart Grid [276, 279] HVAC [276] AMI [276, 279] Electric Vehicles [279]	High Traffic Delay-Tolerant Networks (Multimedia Traffic) / Large-Scale Stationary Low Traffic Networks (IEEE 1901.2)

also make it a good candidate for home and building automation. Due to the inherent characteristics of wired networks, applications of PLC technologies remain limited to stationary and static networks. Underlying characteristics of these two technologies are tabulated in Table 8.

5.7. Other Standards

Z-Wave: This technology is a low-power low-cost WPAN/WLAN solution, which is supported by Z-Wave Alliance [283] and primarily targets smart homes and building automation. The PHY and MAC layers are based on the ITU G9959 standard. Z-Wave operates in the sub-GHz frequency band and provides the data rates of 9.6 kbps and 40 kbps, by using FSK modulation, and 100 kbps by using GFKS modulation. Z-Wave MAC layer provides half-duplex asynchronous (contention-based) communication, allows mesh topologies, and supports acknowledged communication. Although the mesh topology is supported, the number of hops cannot exceed 4 and the total number of nodes in a network must be lower than 232 [284]. Specifications of the NTW layer are not open to public; consequently, not much is known about the Z-Wave routing mechanism [285]. Z-Wave compatible devices can either assume the role of a *control* or a *slave* node. Control nodes perform routing algorithms and control other nodes through command messages, while slave nodes either respond to the command messages or forward them to their neighbor nodes. Considering the limited number of devices in a network and the pairing mechanism of Z-Wave (which is similar to BLE) [285], this technology is not suitable for large-scale and mobile communication and is typically used for home automation, HVAC, power management, security monitoring, etc. Z-Wave uses AES-128, however, encryption is not mandatory and is determined by the vendor based on the target application.

ISA 100.11a: This open-source WLAN technology is designed by the International Society of Automation (ISA), particularly for mission-critical and delay sensitive industrial automation applications. ISA 100.11a is developed atop the IEEE 802.15.4-2006 PHY and MAC layers. Therefore, it operates in the 2.4 GHz ISM frequency band and can provide data rates of up to 250 kbps. ISA 100.11a leverages synchronous (TDMA) medium access in order to improve latency predictability and packet delivery reliability. The protocol supports mesh, star, and hybrid mesh-star topologies [286]. *Infield* wireless subnet typically consists of

- *Input/Output,* which are the sensors and actuators,
- *Routers,* which execute routing algorithms,
- *Provisioning,* which controls network joining and leaving activity,
- *System Manager,* which interfaces the ISA 100.11a network with the backbone network,

ACCEPTED MANUSCRIPT

- *Security Manager,* and a
- *Time Source application*.

Reusing the IEEE 802.15.4-2006 protocol stack automatically makes ISA 100.11a compatible with 6LoWPAN adaptation [180].

WIA-PA: Wireless Networks for Industrial Automation–Process Automation (WIA-PA) is another alternative for mission-critical and delay-intolerant applications for industrial and process automation. Similar to its competitors (ZigBee, ISA100.11a, and WirelessHART), this technology utilizes the PHY and MAC layers of IEEE 802.15.4-2006. WIA-PA networks are typically implemented in a mesh-star hybrid topology, where an in-field data collecting mesh subnet—consisting of *Host Computers*, *Gateways*, *Routing Devices*, *Field Devices*, and *Handheld Devices*—is controlled by a higher level Network Manager (NM) and Security Manager (SM), in either a centralized or decentralized fashion. NM carries out network status and health monitoring, network resource allocation, and mesh routing, while the SM handles authorization and network key management. NM and SM are typically hosted by a single physical component [287].

DECT ULE: Digital Enhanced Cordless Telecommunication Ultra Low Energy (DECT ULE) is developed by European Telecommunication Standard Institute and is a WLAN technology designed for mission-critical and delay-intolerant networks. DECT ULE operates in the 1880 MHz–1900 MHz licensed frequency band (in Europe). The 20 MHz-wide frequency is divided into ten channels [288], allowing this technology to achieve data rates as high as 1.153 Mbps. Therefore, DECT ULE outperforms almost all its competitors in terms of throughput. Its MAC layer uses FDMA, TDMA, and TDD and supports the star topology [107]. DECT ULE architecture involves two types of devices: *Portable Parts* (*PPs*), which typically refers to sensors and actuators with severe resource constraints, and *Fixed Parts* (*FPs*), which are more resourceful and act as APs and gateways for PPs. In addition to its remarkable throughput, which results in satisfactory QoS, DECT ULE provides competitive coverage (75 m and 300 m in indoor and outdoor deployments, respectively [288]), while maintaining low energy consumption (battery-powered devices in sleep mode can last up to ten years [289]). Furthermore, operating in the licensed 1900 MHz translates to limited interference with existing RATs such as WiFi, ZigBee, BLE, etc., thereby reducing collisions and increasing energy efficiency. However, DECT ULE cannot be implemented in a mesh topology and does not provide multi-casting. Furthermore, DECT ULE is not available in the US due to frequency band regulations. Typically, this technology is suggested for home automation, AMI, industrial and process automation, and health monitoring [107].

EC-GSM: Extended Coverage for Global System for Mobile communication (EC-GSM) is developed by 3GPP in Release 13 as an LPWAN solution. EC-GSM involves modifications to reduce complexity, cost, and energy consumption of GSM devices, thereby making this technology more IoT-friendly. EC-GSM uses Gaussian Minimum Shift Keying (GMSK) and 8PSK modulation. Data rates can reach as high as 240 kbps and ≈5000 devices can be serviced in each cell [107]. This technology introduces new low-power classes and message overhead reduction [290]. Existing GSM infrastructures can be brought to compliance with EC-GSM through mere software updates, which not only simplifies the deployment process, but also makes EC-GSM an alternative to NB-IoT in locations with limited 4G coverage.

RFID: Radio Frequency Identification has been traditionally used for identification purposes. However, recent studies have shown the potential of RFID in sensors, where properties of an antenna changes with specific physical parameters (such as acceleration) [291]. RFID is generally associated with short-range WBAN communication, where the maximum achievable range remains lower than tens of meters. Operating frequency of RFID is device-dependent and is typically between 135 kHz to 2.45 GHz. Increasing the operating frequency not only increases the data rate but also reduces the antenna size; nonetheless, higher frequency signals are more prone to path loss. RFID is favorable in cost-sensitive, delay-tolerant and low-traffic applications. Particularly, passive RFID devices outperform their competitors in terms of unobtrusiveness, making RFID a viable solution for smart healthcare applications [292].

INGENU RPMA: INGENU (formerly On-Ramp Wireless) developed Random Phase Multiple Access (RPMA) as a proprietary LPWAN solution. Unlike its main competitors, INGENU RPMA operates in the 2.4 GHz ISM frequency band, thereby avoiding strict regulations of the sub-GHz spectrum. The coverage can reach up to 18 km, while offering data rates as high as 624 kbps for uplink and 156 kbps for downlink [290]. INGENU PRMA is compatible with the IEEE 802.15.4(k) standard. RPMA medium access is based on the Code Division Multiple Access (CDMA) mechanism, where multiple devices can transmit simultaneously in one time slot. Based on their distance to

ACCEPTED MANUSCRIPT

the base station, RPMA devices can adjust their transmit power, thereby providing power saving opportunities for devices near a base station.

Weightless: An open standard for LPWAN, *Weightless* provides an option for UNB, NB, and DSSS communication through *Weightless-N*, *Weightless-P*, and *Weightless-W*, respectively. UNB Weightless-N operates in the sub-GHz ISM spectrum and provides data rates of 30 kbps. Similarly, NB Weightless-P operates in the sub-GHz frequency band. Using a channel width of 12.5 kHz, Weightless-P can achieve data rates up to 100 kbps. Unlike Weightless-N, Weightless-P supports bidirectional communication. Weightless-W operates in TV white space, providing data rates of up to 10 Mbps. Weightless technology supports multiple QoS management services such acknowledged transmission, ARQ, Forward Error Correction, and Auto-retransmission [293].

G3-PLC: Standardized in ITU G.9903 and ITU G.9904, G3-PLC is an NB PLC communication, which targets smart grid and AMI applications. The PHY layer operates in the 9 kHz–490 kHz frequency spectrum (in the US) and provides data rates of up to 141 kbps. The MAC layer is based on IEEE 802.15.4, which implies compatibility with 6LoWPAN. The standard only supports star topology and allows multi-casting along with various QoS services such as ARQ, acknowledge communication, and MAC-layer prioritization (4 different priority levels are defined).

6. Security Plane

The security plane of smart cities faces unique challenges, which are in part inherited from the security challenges of conventional information and communication systems. Each plane in Fig. 2 contains an assembly of interacting heterogeneous embedded cyber physical systems, shared communication and computing infrastructures, and distributed systems. This heterogeneity is the primary cause of weak links in the security and privacy management of smart cities; due to this complex nature of a smart city system, attacks can be originated by insiders or outsiders, as well as a collaboration of both entities [294]. Studies of recent efforts against potential security threats in smart city settings can be found in [295, 296, 297]. The design of an effective security plane requires holistic solutions that address the unique challenges of each plane outside the security plane. To start with, the data plane deals with a highly heterogeneous, unstructured and massive amount of data, which is handled either in the cloud or at the mobile edge; therefore, the data plane inherits the security issues of cloud-based systems. The communication plane, on the other hand, requires security solutions that take into account the interoperability and coexistence of various communication technologies. The sensing plane is vulnerable to attacks that aim at limited power capacity of sensors [298, 299], as well as the lack of trustworthiness of the data acquired through non-dedicated sensors [300, 301]. The application plane is vulnerable to identity spoofing attacks since end devices play the role of data acquisition and usage. It is worth mentioning that conventional security solutions can overcome most of these challenges however the ubiquity, quality and robustness requirements of smart city services call for solutions that are able to make a trade-off between performance and security. In this section, we investigate the security plane challenges and solutions under two categories, namely the *crypto-level security* (Section 6.1), which is primarily concerned with the sensing and communication planes, and *system-level security* (Section 6.2), which is primarily concerned with the application and data planes.

6.1. Crypto-level security

Addressing cybersecurity at lower levels of smart city communication (which we term *crypto-level security*) is a multi-faceted and a complicated problem. The complications of this task stem from the fundamental characteristics of smart city services. Guaranteeing the privacy, integrity, authenticity, and correctness of information, which is acquired by the sensing plane and transmitted by the communication plane, must be fulfilled under extreme power availability constraints (See Fig. 2). Other characteristics of smart city including its large scale, mobility, heterogeneity, and dynamism further convolute the task; for example, *forward and backward security* poses multiple challenges as a consequence of mobility. The goal is to prevent recently added devices from using decryption keys to decipher messages generated in the network prior to their joining the network. Similarly, discharged devices must be unable to decrypt messages immediately after leaving the network [123]. Due to their availability, smart city security requirements are typically addressed by employing off-the-shelf encryption protocols, many of which are not originally designed for IoT applications. Although these solutions considerably improve robustness, they occasionally fail to address every peculiarity of smart city systems. Therefore, these challenges are typically impossible to overcome without a thorough understanding of application requirements, available options, and characteristics of both the sensing and communication planes.

ACCEPTED MANUSCRIPT

A majority of the attacks on the communication plane target user privacy. These attacks can be conducted by either *active* or *passive* (privacy leakage) adversaries with "extortion" as their typical goal, e.g., ransomware. Indeed, privacy concerns are application-dependent. For example, smart healthcare and smart home inherently involve sensitive information. In contrast, privacy leakage in a public air quality monitoring system can rarely endanger the privacy of citizens. Nonetheless, the advances in data communication (particularly in data fusion) have been constantly blurring the meaning of data privacy; due to the continuous data sharing among different applications, data that is considered *insensitive* now, can become critical in the near future. For healthcare applications that involve gathering private data about users, Health Insurance Portability and Accountability Act (HIPAA) mandates application administrators to protect and ensure the privacy of their users [115, 302]. Failing to comply with HIPAA requirements can be interpreted as violation of the law, which introduces another *legal* dimension to the already-existing *technical* dimension for the challenges surrounding the security plane.

Communication plane is subject to a broad range of cyberthreats. Many of these attacks target *sensitive information*, such as user actual identities and location-related data. Particularly, Radio Access Technology (RAT) devices are known to be vulnerable against message injection, jamming, and eavesdropping. For example, the authors in [303] show that BLE security can be compromised by eavesdropping and injection attacks. ZigBee also suffers from a breakable key sharing procedure. Furthermore, the lack of a strong mechanism for checking the freshness of packages renders it vulnerable to reply attacks [304]. WiFi is susceptible to Denial of Service (DoS) and man-in-the-middle attacks, which can practically cripple the entire network. Cellular networks typically outperform RATs operating in ISM bands. However, as discussed in [305], Licensed Assisted Access (see Section 5.3) can potentially undermine the security of such networks and increase the possibility of privacy leakage. Mostly due to weak random number generation procedures, the study conducted in [306] shows that LoRaWAN joining procedure can lead to potential DoS attacks.

Almost all security solutions in smart city communication plane are *software-based*, where data encryption is used as the only tool to ensure both the integrity (to detect potential communication-induced changes in data) and the authenticity (to detect data manipulation attacks such as spoofing) of the information. Encryption techniques, using either public keys or digital signatures, are the backbone of these solutions, as they are not only easy to deploy, but can also address both the security and privacy concerns simultaneously. Many communication standards such as ZigBee, BLE, and WiFi are shipped with embedded encryption mechanisms. *Advanced Encryption Standard (AES)* has for long been considered to be the de facto encryption solution for WSN and IoT communication [307], particularly because of its simplicity, which makes it resource efficient and consequently suitable for resource-constrained microcontroller-based devices. Furthermore, a majority of the sensing and communication modules are equipped with built-in AES encryption/decryption accelerators, which further improves its energy efficiency and latency footprint, while boosting the robustness of the AES against various types of attacks (particularly *side-channel* attacks) [307].

In terms of robustness, AES is not on par with RSA, which can provide superior security at the expense of increased resource requirements. Relatively more recent than both RSA and AES, *Elliptic Curve Cryptography* (*ECC*) has been gaining continuous momentum as a solution that can dovetail resource efficiency of the AES with the robustness of RSA for resource-constrained devices. By employing the *Elliptic Curve Digital Signature Algorithm (ECDSA)*, both Transport Layer Security (TLS) and Datagram TLS (DTLS, which is used in CoAP) are now compatible with ECC. The benefits of ECC are rooted in utilization of smaller keys, which reduces both the memory usage and communication overhead. However, due to computational complexity of the verification process, ECDSA is known to subject servers to heavy load. The prevalence of IoT has increased the awareness of this problem. For example, the authors in [308] propose IoT-centric hardware architectural improvements that can alleviate this drawback. Based on the Twisted Edwards Curve, the proposed solution allows tweaking the system according to the availability of resources and latency/scale requirements of the applications.

Network layer IPSec protocol can also be used to further improve the security of communication, regardless of the transport and application layers. Therefore, IPSec can provide some level of security even in absence of secured application (e.g., CoAP) and transport layer protocols (e.g., TLS, and DTLS). 6LoWPAN also provides flexible AES-based cryptography that can be configured to provide various levels of security according to the requirements of applications. Particularly, Auxiliary Security Header (ASH) field can be setup to provide authentication, confidentiality, and both [123].

Although these traditional cryptography solutions en-

ACCEPTED MANUSCRIPT

hance the security of data communication, they fail to protect data during processing. Data decryption during processing temporarily exposes data to the opportunistic attackers, thereby undermining the entire security mechanism by creating a weak link. As explained in Section 6.2, this vulnerability mostly affects cloud-based data processing. Nonetheless, it can also compromise higher levels of communication architecture that involve in-field data processing, including cloudlets and aggregators (See Section 4.3). Similar to the data plane, security and privacy concerns in data aggregation plane can be addressed by employing *Fully Homomorphic Cryptography* (*FHC*) [309, 310]. Applying FHC to resource-constrained data aggregators, however, is rife with challenges and limitations, as FHC algorithms are notoriously resource-hungry and demanding [311].

Software-based security and privacy solutions used in the communication plane are effective against network breaches and leakages. However, they are vulnerable against both hardware-level intrusions and attacks carried out by insiders. Side channel attacks including timing, power analysis, and cache attacks can effectively circumvent software-based cryptography, once the attacker gains access to the decryption key. Side-channel attacks typically involve analyzing timing of executions, memory and cache access patterns, and energy consumption footprint to acquire revealing information about cryptographic methods and the keys [307]. Randomizing computations and utilizing data processing techniques that are independent of key size (such as Montgomery's multiplication) can increase the robustness of the system against side-channel threats. Nonetheless, these solutions often add to the computational overhead, which is critical to resource-constrained sensing devices [23]. In addition to data, it is also crucial to protect command and control messages as well as over-the-air firmware updates. Particularly, insiders can use debugging pins available in many sensing devices to upload Trojans or malicious firmware [312]. The inter-operation of smart city communication with non-IoT networks further deteriorates this problem, as a compromised IoT node can endanger the entire network [313].

6.2. System-level security

Distributed and embedded cyber-physical systems that interact with each other over shared infrastructures and communicate via heterogeneous platforms form the smart city infrastructure. This setting results in vulnerabilities in the security and privacy of smart cities. As previously mentioned, the source of an attack that targets the system security of smart cities can be insiders, outsiders, or a collaboration of both [294]. Several studies have proposed countermeasures against the security challenges in smart city settings [295, 296, 297]. Although existing techniques for security and privacy management of information systems can be adopted, they need to be tailored to fulfill the requirements of secure, robust and resilient smart city systems, because they were not originally designed to be used in smart city applications. In this section, we present security threats at the system level under three categories, along with solutions to mitigate these threats: 1) Man-in-the-middle attacks, 2) intrusion detection in the communication infrastructure, and 3) authentication on the end devices based on hard and soft approaches.

6.2.1. Man-in-the-middle attacks

Manipulation of messages from a sender to a receiver, with the action being noticed by neither end, is termed a *Man-in-the-Middle attack* [314]. Recently, with the advent of the IoT concept, man in the middle attacks have also been called *manipulation attacks* [315]. The most effective type of manipulation attacks aim at manipulating the network layer immediately at the time when a new device is introduced to the network. As IoT is implemented in a distributed mobile environment, this makes IoT networks especially vulnerable to man-in-the-middle attacks [316]. This increased vulnerability in IoT networks particularly arises from the complicated nature of a successful verification of the end devices.

In smart city applications, session key establishment procedure is an open target for Man-in-the-Middle attacks. To address this vulnerability, a secure access control method is proposed in [317], with the objective of session key establishment based on a mutual-authentication between a sender and a receiver. At the lower layer, ECC is used for encryption (see Section 6.1); the use of ECC disables data transmission to the nodes that cannot be identified as genuine at the end of a two-step authentication procedure.

Network layer security issues under smart city settings have been studied in [318] along with possible solutions. Network encryption, authentication and key management, identity verification, symmetric or asymmetric data encryption and digest algorithms are the most effective solutions that have been reported.

6.2.2. Intrusion detection

Intrusion detection in IoT is based on the immune theory and thus adopts the principles of artificial immune systems. In [319], the authors discuss the self and non-self antigens in an IoT network through simulations. In that study, the immature detector, mature

ACCEPTED MANUSCRIPT

detector, and memory detector define the threat exposition. The efficacy of the detectors against both the mutated and totally unknown IoT attacks is performed by evolution with the ultimate goal of adaptation to the IoT settings. An information library is required for proper execution of the proposed method. The library contents and the attacks that have been detected are used for alarming the system manager [319].

SVELTE [320], a real-time intrusion detection system (IDS) for the IoT to detect sinkhole and selective forwarding attacks, was initially designed for a Low-power Wireless Personal Area Networks with IPv6 (6LoWPAN) [321] to ensure end-to-end message security. A 6LoWPAN Mapper (6Mapper) to collect information about the low power and lossy network, an intrusion detection component to process the mapped data, and a distributed mini-firewall form the SVELTE framework.

Resource limitations of IoT devices introduce the fundamental challenge in the IoT-centric systems in smart cities. With this motivation in mind, the authors in [314] propose a hybrid IDS to co-operate with the Constrained Application Protocol (CoAP) in public transport systems. The proposed IDS is based on the analysis of communication patterns. The experiments show that the integration of the anomaly-based IDS with machine learning approaches such as neural networks can meet the system level security requirements of applications in smart cities.

6.2.3. Authentication

Continuous authentication and verification has appeared as an inevitable functionality for participating devices in smart city applications. To address this challenge, hybrid solutions which combine behavioral pattern mining/recognition with the conventional biometrics-based hard authentication techniques have gained popularity.

The socialization of smart objects concepts was first introduced in [331] The integration of the IoT and social networks was presented in [332]. These two studies are important to acknowledge since they have the potential to form a basis of the concept of continuous and/or behavioral authentication in smart city applications. Shortly after the introduction of the social IoT concept, social network-based behavioral study for the mobile nodes in an IoT system was presented in [333].

It is worth noting that soft-authentication solutions (e.g., behavioral authentication) are not expected to replace biometric authentication, which is still the most promising method in end user authentication. However, biometric authentication also suffers from few vulnerabilities and more importantly performance penalties. Biometrics-based authentication can be categorized into hard and soft biometric authentication groups. As stated in [334], the former denotes authentication methods using physiological features such as fingerprints, facial image, and iris scanning whereas the latter denotes habitual signature such as including handwriting, keystroke dynamics, and social networking. Soft-biometric-based continuous authentication methodologies use behavioral patterns of users or nodes by aiming at improved robustness and non-intrusiveness during the authentication procedure. Hence, recent research on continuous authentication uses behavioral features such as SMS, phone calls, browser history, location, gestural patterns on touch screens to address these aims through implicit and continuous procedures [324, 325, 326, 327, 328].

Smart environments such as smart homes offer rich contextual information regarding the interaction of the users with the environment. Thus, the contextual information helps the platform define behavioral biometrics that can be used for continuous authentication of the users [335]. An example of interaction-based behavioral biometrics is the gestural patterns on touch-screens [329].

As smart cities can be considered as a superset of smart environments, behavioral biometrics can be considered as a well-suited method for system-level security of smart city applications [336, 337]. The applicability of behavioral biometrics in smart environments has been investigated by the comprehensive survey in [330] by considering smart homes, smart media devices, smart traffic systems and smart health.

In [323], continuous verification on mobile devices is based on the behavioral patterns of smart mobile device users on various social network platforms. The idea behind continuously authenticating the users on smart mobile devices is that smart devices can be used in participatory sensing campaigns [33]. A minimalist view of the continuous verification to ensure system level security is illustrated in Fig. 4. Conventional verification schemes such as pin codes/passwords or fingerprints/face recognition may lead to disruption and performance reduction. Many researchers have pointed out the security vulnerabilities of pin code/password-based authentication [338], where the security assurance by biometrics introduce a security-implementation cost trade-off [339, 340, 341, 342]. To address this trade-off, a mobile behaviometric framework can monitor and assess the social activity on the mobile devices, which is introduced as the sociability signature.

Table 9 summarizes our discussion about system-

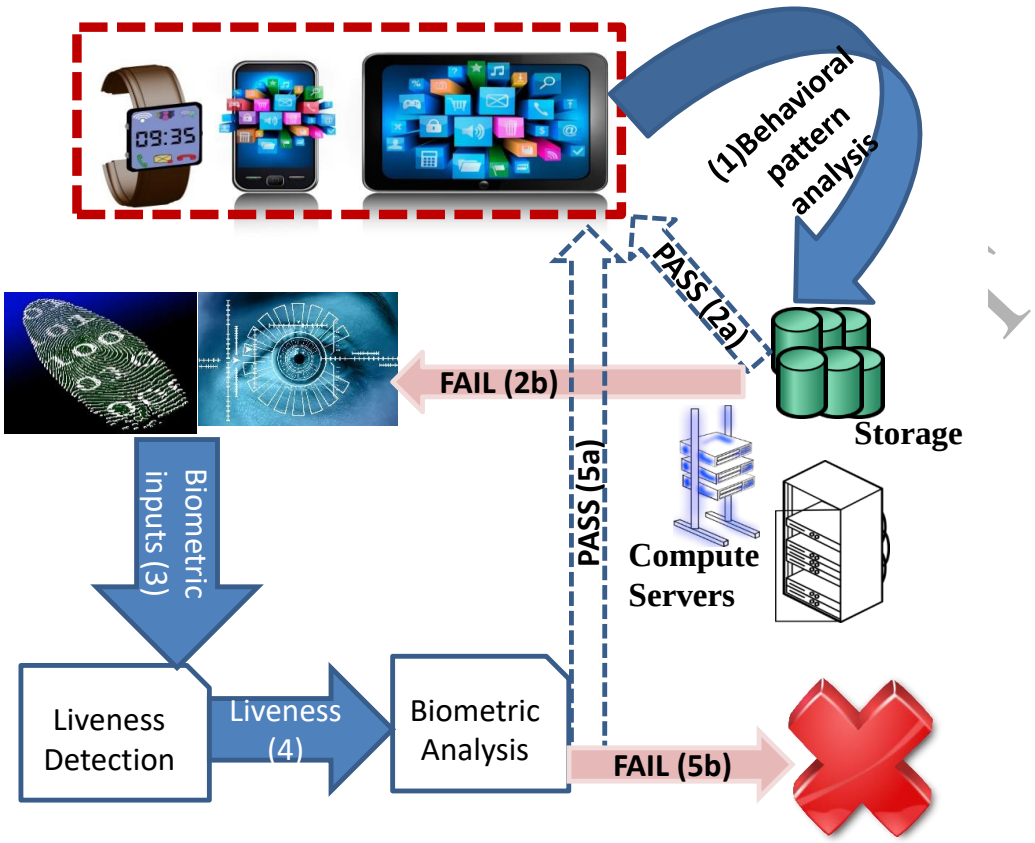


Figure 4: Continuous authentication scheme proposed in [322][323]. The proposed approach aims to strengthen the biometrics authentication through behaviometric properties. The motivation is that biometric authentication cannot be called on continuous basis whereas behaviometrics can be adopted as soft-biometrics to overcome system-level security attacks, particularly aiming at identity spoofing.

level security concerns and select number of proposed solution.

7. Open Issues and Challenges

This section presents open issues, challenges, and opportunities for future research in smart cities by focusing on the sensing, communication and security planes.

7.1. Sensing Plane

First and foremost, wireless sensors are powered by batteries, which introduces the most important challenge to the research in this field. While there are few studies on RF energy harvesting for wireless powered sensors [23, 343, 344], energy harvesting for IoT sensors will remain an open issue for the next few years as efficiency objectives have yet to be met. Direct integration of sensing devices on passive and semi-passive RFID tags by printing sensors on flexible plastic RFID labels, as well as integration of sensors with energy scavengers to extend the applications have been presented in [85]. Thus, besides architectural, hardware and software design for sensors, fabrication of sensing devices based on electrical properties remains a challenge in the sensing plane of a smart city system. Additionally, because of their low power budget, IoT sensors cannot readily implement encryption into their operation; this fact makes them vulnerable to attacks that aim to steal their data [298]. **As mentioned earlier, mobile crowd-sensing is a revolutionary paradigm to enable non-dedicated sensing in smart cities. While testbeds are being implemented, in order to test new techniques and methodologies for effective incentives, energy efficient crowd management, and privacy of participants, availability of realistically designed simulators is crucial [345]. As currently available simulators and platforms assume that the IoT devices in a mobile crowd-sensing system are equipped with 3G/LTE, WiFi and Bluetooth communication capability, in the 5G Era and beyond,**

ACCEPTED MANUSCRIPT

Table 9: The list of system-level security solutions in smart city applications

Smart City Application	Problem	Solution
Generic	Man-In-the-Middle-Attack Network-Layer Security Intrusion Detection Sinkhole and Selective Forwarding Attacks	Secure Session Key +ECC [317] Encryption, Authentication, Key Management [318] Artificial Immune Systems [319] SVELTE [320]
Smart Transportation	Intrusion Detection	Communication Pattern Analysis [314]
Soft Biometrics	Authentication	Behavioral Pattern Analysis [324, 325, 326, 327, 328]
Smart Environments	Continuous Authentication	Gestural Pattern Analysis [329]
Smart Homes, Smart Traffic Systems, Smart Health	Implicit Authentication	Behavioral Biometrics [330]
Participatory and Opportunistic Sensing	Continuous Authentication	Sociability Analysis [323]

the presence of augmented reality and virtual reality (AR/VR) devices will need to be integrated with the crowd-sensing campaigns. Therefore, existing testbeds as well as simulators call improvements that consider the integration of AR/VR devices in the IoT ecosystem.

7.2. *Communication Plane*

Heterogeneous nature of the communication plane introduces many challenges that remain unaddressed to this date. A universal architecture that can address IoT communication fragmentation is urgently needed. Since majority of sensing and data acquisition is performed through IoT nodes, congestion control in IoT needs to be addressed to cope with the data explosion in IoT networks. Conventional TCP-based congestion control introduces a significant overhead on the IoT nodes, while choosing UDP over TCP will not solve congestion control effectively. As for next generation wireless communication systems, 5G mmWave requires careful modeling. Various studies have been presented in the literature [346, 347], however a final model to characterize mmWave propagation is yet to be developed.

When WSNs are used in certain applications, antenna placement and link quality assurance appear as two important challenges. For instance, as described in [348], when WSNs are used in smart parking applications, antennas should be placed only a few centimeters above the ground to be able to be catch passing vehicles, although such placement reduces communication range. Moreover, the antenna is covered by the metal body of the car, which further degrades the performance. Therefore, the traditional topology discovery and routing algorithms in WSNs cannot guarantee high performance under dynamic arrival/departure patterns of vehicles. Furthermore, interference-driven link quality degradation and consequent high packet losses have to be overcome by novel solutions.

7.3. *Security Plane*

Challenges in the security plane are highly dependent on the smart city applications and services. For instance, smart meters are vulnerable to attacks that manipulate energy costs or leak energy usage information, which may reveal unique behavioral patterns [349]. Therefore, novel solutions to hide sensitive patterns in energy usage are required.

As mentioned earlier, continuous authentication is still in its infancy; however it is envisioned to be an integral part of the security plane of smart city systems. Therefore, novel schemes that take benefit of machine learning, deep learning, and statistical signal processing

ACCEPTED MANUSCRIPT

techniques are emerging to achieve system-level security in the smart cities.

As majority of the sensing infrastructure operates on batteries, DDoS attacks may also raise serious threats for the sensing infrastructure. Detection and defense mechanisms against DDoS attacks on the sensing infrastructure, —especially in the presence of a heterogeneous sensing environment— are necessary.

8. Summary and Concluding Remarks

The advent of Internet of Things (IoT) and data analytics have paved the way to realize fully digitized, sustainable, resilient, and effectively-serving smart cities. The ultimate goal of digitization is to minimize human intervention. Smart city applications and services in the areas of healthcare, transportation, energy, public safety, and environment require ubiquitous, pervasive, resilient and efficient communication infrastructure to ensure the highest quality of service and quality of experience. Internet of Things (IoT) bridges the communication between sensory data acquisition and decision making over massive, heterogeneous and unstructured data. Indeed security and privacy are the utmost important design parameter for each individual component of a smart city system.

This article studies the building blocks (i.e. *planes*) of a smart city system by providing an architectural overview and special emphasis on the sensing, communication, and security planes. Smart city architecture consists of the following five components; *1. Application plane* enables interaction with the end users through various services, *2. Sensing Plane* is solely responsible for data acquisition through dedicated and/or non-dedicated sensors, *3. Communication Plane* is responsible for ensuring efficiency and high quality of service in the transmission of sensory data from the sensing plane to the data plane, *4. Data plane* is where the ultimate processing and storage services are provisioned for the data acquired/generated in the sensing plane, and *5. Security Plane* ensures confidentiality, integrity, authenticity, and resiliency of the entire system through crypto-level or system-level security solutions.

The survey is centered around sensing, communication and security planes considering the unique requirements of smart city applications. A detailed survey of the state of the art for each of these planes is followed by a thorough discussion on the open issues and challenges. Moreover, in order to stimulate future research, the survey provides insights to address the interplay among these planes to ensure ubiquity, pervasiveness, robustness, resiliency, and security of smart city systems.

References

[1] T. Guelzim, M. Obaidat, B. Sadoun, Chapter 1 - Introduction and Overview of Key Enabling Technologies for Smart Cities and Homes, in: M. S. Obaidat, P. Nicopolitidis (Eds.), Smart Cities and Homes, Morgan Kaufmann, Boston, 2016, pp. 1 – 16.

[2] M. Habibzadeh, Z. Qin, T. Soyata, B. Kantarci, Large Scale Distributed Dedicated- and Non-Dedicated Smart City Sensing Systems, IEEE Sensors Journal 17 (23) (2017) 7649–7658. doi:10.1109/JSEN.2017.2725638.

[3] C. E. A. Mulligan, M. Olsson, Architectural Implications of Smart City Business Models: An Evolutionary Perspective, IEEE Communications Magazine 51 (6) (2013) 80–85. doi:10.1109/MCOM.2013.6525599.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, IEEE Communications Surveys Tutorials 17 (4) (2015) 2347–2376. doi:10.1109/COMST.2015.2444095.

[5] B. Hammi, R. Khatoun, S. Zeadally, A. Fayad, L. Khoukhi, IoT Technologies for Smart Cities, IET Networks 7 (1) (2018) 1–13. doi:10.1049/iet-net.2017.0163.

[6] P. Barsocchi, P. Cassara, F. Mavilia, D. Pellegrini, Sensing a City's State of Health: Structural Monitoring System by Internet-of-Things Wireless Sensing Devices, IEEE Consumer Electronics Magazine 7 (2) (2018) 22–31. doi:10.1109/MCE.2017.2717198.

[7] Y. Kim, T. Soyata, R. F. Behnagh, Towards Emotionally-Aware AI Smart Classroom: Current Issues and Directions for Engineering and Education, IEEE Accessdoi:10.1109/ACCESS.2018.2791861.

[8] L. Catarinucci, D. de Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi, L. Tarricone, An IoT-Aware Architecture for Smart Healthcare Systems, IEEE Internet of Things Journal 2 (6) (2015) 515–526. doi:10.1109/JIOT.2015.2417684.

[9] M. Collotta, G. Pau, A Novel Energy Management Approach for Smart Homes Using Bluetooth Low Energy, IEEE Journal on Selected Areas in Communications 33 (12) (2015) 2988–2996. doi:10.1109/JSAC.2015.2481203.

[10] M. Daher, A. Diab, M. E. B. E. Najjar, M. A. Khalil, F. Charpillet, Elder Tracking and Fall Detection System Using Smart Tiles, IEEE Sensors Journal 17 (2) (2017) 469–479. doi:10.1109/JSEN.2016.2625099.

[11] J. Zhang, Y. Shan, K. Huang, ISEE Smart Home (ISH): Smart Video Analysis for Home Security, Neurocomputing 149 (2015) 752 – 766. doi:https://doi.org/10.1016/j.neucom.2014.08.002.
URL http://www.sciencedirect.com/science/article/pii/S092523121401011X

[12] E. Zeng, S. Mare, F. Roesner, End User Security & Privacy Concerns with Smart Homes, in: Symposium on Usable Privacy and Security (SOUPS), 2017.

[13] C. Cakebread, Consumers Are Holding Off on Buying Smart-Home Gadgets Thanks to Security and Privacy Fears, http://www.businessinsider.com/consumers-holding-off-on-smart-home-gadgets-thanks-to-privacy-fears-2017-11, accessed: 03-13-2018 (2017).

ACCEPTED MANUSCRIPT

[14] IBM Corp., IBM Db2 Database, Database Software, IBM Analytics, https://www.ibm.com/analytics/us/en/db2/, Accessed 09 March 2018 (2017).

[15] IBM Corp., Application Server, IBM Cloud, https://www.ibm.com/cloud/websphere-application-platform, accessed 09 March 2018 (2017).

[16] A. Basalamah, Sensing the Crowds Using Bluetooth Low Energy Tags, IEEE Access 4 (2016) 4225–4233. doi:10.1109/ACCESS.2016.2594210.

[17] C. Kaptan, B. Kantarci, T. Soyata, A. Boukerche, Emulating Smart City Sensors Using Soft Sensing and Machine Intelligence: a Case Study in Public Transportation, in: IEEE International Conference on Communication, Kansas City, MO, 2018.

[18] J.-R. Lin, T. Talty, O. K. Tonguz, On the Potential of Bluetooth Low Energy Technology for Vehicular Applications, IEEE Communications Magazine 53 (1) (2015) 267–275.

[19] K. M. Tan, V. K. Ramachandaramurthy, J. Y. Yong, Integration of Electric Vehicles in Smart Grid: A Review on Vehicle to Grid Technologies and Optimization Techniques, Renewable and Sustainable Energy Reviews 53 (2016) 720 – 732. doi:https://doi.org/10.1016/j.rser.2015.09.012. URL http://www.sciencedirect.com/science/article/pii/S136403211500982X

[20] E. Akhavan-Rezai, M. F. Shaaban, E. F. El-Saadany, F. Karray, Online Intelligent Demand Management of Plug-In Electric Vehicles in Future Smart Parking Lots, IEEE Systems Journal 10 (2) (2016) 483–494. doi:10.1109/JSYST.2014.2349357.

[21] I. Jauregi, H. Solar, A. Beriain, I. Zalbide, A. Jimenez, I. Galarraga, R. Berenguer, UHF RFID Temperature Sensor Assisted With Body-Heat Dissipation Energy Harvesting, IEEE Sensors Journal 17 (5) (2017) 1471–1478. doi:10.1109/JSEN.2016.2638473.

[22] Z. Xiao, X. Tan, X. Chen, S. Chen, Z. Zhang, H. Zhang, J. Wang, Y. Huang, P. Zhang, L. Zheng, H. Min, An Implantable RFID Sensor Tag toward Continuous Glucose Monitoring, IEEE Journal of Biomedical and Health Informatics 19 (3) (2015) 910–919. doi:10.1109/JBHI.2015.2415836.

[23] T. Soyata, L. Copeland, W. Heinzelman, RF Energy Harvesting for Embedded Systems: A Survey of Tradeoffs and Methodology, IEEE Circuits and Systems Magazine 16 (1) (2016) 22–57. doi:10.1109/MCAS.2015.2510198.

[24] Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication, https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm, accessed: 03-12-2018.

[25] S. Balasubramanlan, The Global Cyberattack And The Need To Revisit Health Care Cybersecurity, https://www.huffingtonpost.com/entry/lessons-learned-the-global-cyberattack-the-need_us_591a1ac5e4b086d2d0d8d1ed, accessed: 03-12-2018.

[26] B. Barrett, Hack Brief: Hackers Are Holding an LA Hospital's Computers Hostage, https://www.wired.com/2016/02/hack-brief-hackers-are-holding-an-la-hospitals-computers-hostage/, accessed: 03-12-2018.

[27] M. Erol-Kantarci, B. Kantarci, H. T. Mouftah, Reliable Overlay Topology Design for the Smart Microgrid Network, IEEE Network 25 (5) (2011) 38–43. doi:10.1109/MNET.2011.6033034.

[28] J. Andreu-Perez, D. R. Leff, H. M. D. Ip, G. Z. Yang, From Wearable Sensors to Smart Implants–Toward Pervasive and Personalized Healthcare, IEEE Transactions on Biomedical Engineering 62 (12) (2015) 2750–2762. doi:10.1109/TBME.2015.2422751.

[29] H.-L. Peng, J.-Q. Liu, H.-C. Tian, B. Xu, Y.-Z. Dong, B. Yang, X. Chen, C.-S. Yang, Flexible Dry Electrode based on Carbon Nanotube/Polymer Hybrid Micropillars for Biopotential Recording, Sensors and Actuators A: Physical 235 (2015) 48 – 56. doi:https://doi.org/10.1016/j.sna.2015.09.024. URL http://www.sciencedirect.com/science/article/pii/S0924424715301412

[30] R. K. Pal, A. A. Farghaly, C. Wang, M. M. Collinson, S. C. Kundu, V. K. Yadavalli, Conducting Polymer-Silk Biocomposites for Flexible and Biodegradable Electrochemical Sensors, Biosensors and Bioelectronics 81 (2016) 294 – 302. doi:https://doi.org/10.1016/j.bios.2016.03.010. URL http://www.sciencedirect.com/science/article/pii/S0956566316301993

[31] S. Kianoush, S. Savazzi, F. Vicentini, V. Rampa, M. Giussani, Device-Free RF Human Body Fall Detection and Localization in Industrial Workplaces, IEEE Internet of Things Journal 4 (2) (2017) 351–362. doi:10.1109/JIOT.2016.2624800.

[32] M. Pouryazdan, B. Kantarci, T. Soyata, L. Foschini, H. Song, Quantifying User Reputation Scores, Data Trustworthiness, and User Incentives in Mobile Crowd-Sensing, IEEE Access 5 (2017) 1382–1397. doi:10.1109/ACCESS.2017.2660461.

[33] M. Pouryazdan, C. Fiandrino, B. Kantarci, T. Soyata, D. Kliazovich, P. Bouvry, Intelligent Gaming for Mobile Crowd-Sensing Participants to Acquire Trustworthy Big Data in the Internet of Things, IEEE Access 5 (1) (2017) 22209–22223. doi:10.1109/ACCESS.2017.2762238.

[34] M. Habibzadeh, M. Hassanalieragh, A. Ishikawa, T. Soyata, G. Sharma, Hybrid Solar-Wind Energy Harvesting for Embedded Applications: Supercapacitor-based System Architectures and Design Tradeoffs, IEEE Circuits and Systems Magazine 17 (4) (2017) 29–63. doi:10.1109/MCAS.2017.2757081.

[35] M. Habibzadeh, M. Hassanalieragh, T. Soyata, G. Sharma, Solar/Wind Hybrid Energy Harvesting for Supercapacitor-based Embedded Systems, in: IEEE Midwest Symposium on Circuits and Systems, Boston, MA, 2017, pp. 329–332. doi:10.1109/MWSCAS.2017.8052927.

[36] M. Habibzadeh, M. Hassanalieragh, T. Soyata, G. Sharma, Supercapacitor-Based Embedded Hybrid Solar/Wind Harvesting System Architectures, in: Proceedings of the 30th IEEE International System-on-Chip Conference, Munich, Germany, 2017.

[37] X. Zhang, Z. Yang, W. Sun, Y. Liu, S. Tang, K. Xing, X. Mao, Incentives for Mobile Crowd Sensing: A Survey, IEEE Communications Surveys Tutorials 18 (1) (2016) 54–67. doi:10.1109/COMST.2015.2415528.

[38] B. K. V. S. Dasari, M. Pouryazdan, Selective versus non-selective acquisition of crowd-solicited iot data and its dependability, in: IEEE International Conference on Communications Workshops (ICCW), 2018, pp. 1–6.

[39] W. B. Heinzelman, A. P. Chandrakasan, H. Balakrishnan, An Application-Specific Protocol Architecture for Wireless Microsensor Networks, IEEE Transactions on Wireless Communications 1 (4) (2002) 660–670. doi:10.1109/TWC.2002.804190.

[40] E. Fotopoulou, A. Zafeiropoulos, F. Terroso-Sáenz, U. Şimşek, A. González-Vidal, G. Tsiolis, P. Gouvas, P. Liapis, A. Fensel, A. Skarmeta, Providing Personalized Energy Management and Awareness Services for Energy Efficiency in Smart Buildings, Sensors 17 (9) (2017) 2054.

[41] A. Page, M. K. Aktas, T. Soyata, W. Zareba, J. Couderc,

ACCEPTED MANUSCRIPT

QT Clock to Improve Detection of QT Prolongation in Long QT Syndrome Patients, Heart Rhythm 13 (1) (2016) 190–198. doi:10.1016/j.hrthm.2015.08.037.

[42] M. Habibzadeh, A. Boggio-Dandry, Z. Qin, T. Soyata, B. Kantarci, H. Mouftah, Soft Sensing in Smart Cities: Handling 3Vs Using Recommender Systems, Machine Intelligence, and Data Analytics, IEEE Communications Magazine 56 (2) (2018) 78–86. doi:10.1109/MCOM.2018.1700304.

[43] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, Edge Computing: Vision and Challenges, IEEE Internet of Things Journal 3 (5) (2016) 637–646. doi:10.1109/JIOT.2016.2579198.

[44] J. Yin, I. Gorton, S. Poorva, Toward Real Time Data Analysis for Smart Grids, in: 2012 SC Companion: High Performance Computing, Networking Storage and Analysis, 2012, pp. 827–832.

[45] D. Neumann, C. Bodenstein, O. F. Rana, R. Krishnaswamy, STACEE: Enhancing Storage Clouds Using Edge Devices, in: Proceedings of the 1st ACM/IEEE Workshop on Autonomic Computing in Economics, ACE '11, ACM, New York, NY, USA, 2011, pp. 19–26. doi:10.1145/1998561.1998567. URL http://doi.acm.org/10.1145/1998561.1998567

[46] J. Stößer, D. Neumann, C. Weinhardt, Market-Based Pricing in Grids: On Strategic Manipulation and Computational Cost, European Journal of Operational Research 203 (2) (2010) 464–475.

[47] R. Buyya, H. Stockinger, J. Giddy, D. Abramson, Economic Models for Management of Resources in Peer-to-Peer and Grid Computing, in: Commercial Applications for High-Performance Computing, Vol. 4528, International Society for Optics and Photonics, 2001, pp. 13–26.

[48] Y. Geng, J. Chen, R. Fu, G. Bao, K. Pahlavan, Enlighten Wearable Physiological Monitoring Systems: On-Body RF Characteristics Based Human Motion Classification Using a Support Vector Machine, IEEE Transactions on Mobile Computing 15 (3) (2016) 656–671. doi:10.1109/TMC.2015.2416186.

[49] R. Yu, Y. Yang, L. Yang, G. Han, O. A. Move, RAQA Random Forest Approach for Predicting Air Quality in Urban Sensing Systems, Sensors 16 (1). doi:10.3390/s16010086. URL http://www.mdpi.com/1424-8220/16/1/86

[50] R. Polishetty, M. Roopaei, P. Rad, A Next-Generation Secure Cloud-Based Deep Learning License Plate Recognition for Smart Cities, in: 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), 2016, pp. 286–293.

[51] K. Liao, Z. Zhao, A. Doupe, G. J. Ahn, Behind Closed Doors: Measurement and Analysis of CryptoLocker Ransoms in Bitcoin, in: 2016 APWG Symposium on Electronic Crime Research (eCrime), 2016, pp. 1–13. doi:10.1109/ECRIME.2016.7487938.

[52] K. Cabaj, W. Mazurczyk, Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall, IEEE Network 30 (6) (2016) 14–20. doi:10.1109/MNET.2016.1600110NM.

[53] S. Mohurle, M. Patil, A Brief Study of Wannacry Threat: Ransomware Attack 2017, International Journal 8 (5).

[54] M. Pouryazdan, C. Fiandrino, B. Kantarci, D. Kliazovich, T. Soyata, P. Bouvry, Game-Theoretic Recruitment of Sensing Service Providers for Trustworthy Cloud-Centric Internet-of-Things (IoT) Applications, in: Globecom Workshops, Washington, DC, 2016, pp. 1–6. doi:10.1109/GLOCOMW.2016.7848915.

[55] D. He, S. Chan, M. Guizani, User privacy and data trustworthiness in mobile crowd sensing, IEEE Wireless Communications 22 (1) (2015) 28–34.

[56] W. Birk, E. Osipov, J. Eliasson, iRoad-Cooperative Road Infrastructure Systems for Driver Support (2009).

[57] K. Y. Chan, T. S. Dillon, On-Road Sensor Configuration Design for Traffic Flow Prediction Using Fuzzy Neural Networks and Taguchi Method, IEEE Trans. on Instrumentation and Measurement 62 (1) (2013) 50–59.

[58] M. Abdel-Aty, A. Pande, ATMS Implementation System for Identifying Traffic Conditions Leading to Potential Crashes, IEEE Trans. on Intelligent Transportation Systems 7 (1) (2006) 78–91.

[59] S. Gupte, O. Masoud, R. F. K. Martin, N. P. Papanikolopoulos, Detection and Classification of Vehicles, IEEE Trans. on Intelligent Transportation Systems 3 (1) (2002) 37–47.

[60] C. C. R. Wang, J. J. J. Lien, Automatic Vehicle Detection Using Local Features- A Statistical Approach, IEEE Trans. on Intelligent Transportation Systems 9 (1) (2008) 83–96.

[61] M. S. Shehata, J. Cai, W. M. Badawy, T. W. Burr, M. S. Pervez, R. J. Johannesson, A. Radmanesh, Video-Based Automatic Incident Detection for Smart Roads: The Outdoor Environmental Challenges Regarding False Alarms, IEEE Trans. on Intelligent Transportation Systems 9 (2) (2008) 349–360.

[62] M. Balcilar, A. C. Sonmez, Extracting Vehicle Density from Background Estimation using Kalman Filter (Oct 2008).

[63] J. Zhang, B. Tan, F. Sha, L. He, Predicting Pedestrian Counts in Crowded Scenes With Rich and High-Dimensional Features, IEEE Trans. on Intelligent Transportation Systems 12 (4) (2011) 1037–1046.

[64] R. Bajwa, R. Rajagopal, P. Varaiya, R. Kavaler, In-Pavement Wireless Sensor Network for Vehicle Classification, in: Proceedings of the 10th ACM/IEEE International Conference on Information Processing in Sensor Networks, 2011, pp. 85–96.

[65] J. A. Healey, R. W. Picard, Detecting Stress During Real-World Driving Tasks using Physiological Sensors, IEEE Trans. on Intelligent Transportation Systems 6 (2) (2005) 156–166.

[66] S. Kamijo, Y. Matsushita, K. Ikeuchi, M. Sakauchi, Traffic Monitoring and Accident Detection at Intersections, IEEE Trans. on Intelligent Transportation Systems 1 (2) (2000) 108–118.

[67] S. Munder, C. Schnorr, D. M. Gavrila, Pedestrian Detection and Tracking Using a Mixture of View-Based Shape-Texture Models, IEEE Trans. on Intelligent Transportation Systems 9 (2) (2008) 333–343.

[68] D. J. Cook, M. Youngblood, , S. K. Das, A multi-Agent Approach to Controlling a Smart Environment, in: Designing smart homes, 2006, pp. 165–182.

[69] P. Rashidi, D. J. Cook, L. B. Holder, M. Schmitter-Edgecombe, Discovering Activities to Recognize and Track in a Smart Environment, IEEE Trans. on knowledge and data engineering 23 (4) (2011) 527–539.

[70] S. Hussain, S. Schaffner, D. Moseychuck, Applications of Wireless Sensor Networks and RFID in a Smart Home Environment, in: CNSR, 2009, pp. 153–157.

[71] S. Baeg, J. Park, J. Koh, K. Park, M. Baeg, Building a Smart Home Environment for Service Robots based on RFID and Sensor Networks, in: ICCAS, 2007, pp. 1078–1082.

[72] N. Nikzad, N. Verma, C. Ziftci, E. Bales, N. Quick, P. Zappi, K. Patrick, S. Dasgupta, I. Krueger, S. Š. Rosing, et al., Citisense: Improving Geospatial Environmental Assessment of Air Quality Using a Wireless Personal Exposure Monitoring System, in: Proceedings of the conference on Wireless Health, ACM, 2012, p. 11.

[73] R. A. Stewart, R. Willis, D. Giurco, K. Panuwatwanich, G. Capati, Web-Based Knowledge Management System: Linking Smart Metering to the Future of Urban Water Planning, Australian Planner 47 (2) (2010) 66–74.

[74] G. Hauber-Davidson, E. Idris, Smart Water Metering, Water

ACCEPTED MANUSCRIPT

33 (3) (2006) 38–41.

[75] B. Lichtensteiger, B. Bjelajac, C. Mueller, C. Wietfeld, RF Mesh Systems for Smart Metering: System Architecture and Performance, in: International Conference on Smart Grid Communications, 2010, pp. 379–384.

[76] F. Derbel, Trends in Smart Metering, in: Systems, Signals and Devices, 2009. SSD'09. 6th International Multi-Conference on, IEEE, 2009, pp. 1–4.

[77] A. Reinhardt, D. Burkhardt, P. S. Mogre, M. Zaheer, R. Steinmetz, SmartMeter.KOM: A Low-cost Wireless Sensor for Distributed Power Metering, in: Local Computer Networks (LCN), 2011 IEEE 36th Conference on, IEEE, 2011, pp. 1032–1039.

[78] C. Gao, M. Redfern, A Review of Voltage Control in Smart Grid and Smart Metering Technologies on Distribution Networks, in: UPEC, 2011, pp. 1–5.

[79] C. W. Chen, M. T. Mohn, F. Aybar, S. V. Lopez, W. S. Du, N. K. Pandya, System and Method for Utilization of Smart Meter Infrastructure, uS Patent App. 12/458,370 (Jul. 9 2009).

[80] V. C. Gungor, B. Lu, G. P. Hancke, Opportunities and Challenges of Wireless Sensor Networks in Smart Grid, IEEE Trans. on industrial electronics 57 (10) (2010) 3557–3564.

[81] R. Ambikairajah, B. Phung, J. Ravishankar, T. Blackburn, Z. Liu, Smart Sensors and Online Condition Monitoring of High Voltage Cables for the Smart Grid, in: MEPCON, 2010, pp. 19–21.

[82] R. Moghe, F. C. Lambert, D. Divan, Smart "Stick-On Sensors for the Smart Grid, IEEE Trans. on Smart Grid 3 (1) (2012) 241–252.

[83] A. Barbato, A. Capone, M. Rodolfi, D. Tagliaferri, Forecasting the Usage of Household Appliances Through Power Meter Sensors for Demand Management in the Smart Grid, in: SmartGridComm, 2011, pp. 404–409.

[84] L. Beauvillier, M. J. Brady, D. Duan, D. J. Friedman, P. A. Moskowitz, P. Murphy, Method and Apparatus for Testing RFID Tags, uS Patent 6,104,291 (Aug. 15 2000).

[85] D. Briand, F. Molina-Lopez, A. V. Quintero, G. Mattana, N. F. de Rooij, Printed Sensors on Smart RFID Labels for Logistics, in: NEWCAS, 2012, pp. 449–452.

[86] B. S. Cook, T. Le, S. Palacios, A. Traille, M. Tentzeris, Only Skin Deep: Inkjet-Printed Zero-Power Sensors for Large-Scale RFID-Integrated Smart Skins, IEEE Microwave Magazine 14 (3) (2013) 103–114.

[87] H. Mora-Mora, V. Gilart-Iglesias, D. Gil, A. Sirvent-Llamas, A Computational Architecture based on RFID Sensors for Traceability in Smart Cities, Sensors 15 (6) (2015) 13591–13626.

[88] F. J. Villanueva, D. Villa, M. J. Santofimia, J. Barba, J. C. Lpez, Crowdsensing Smart City Parking Monitoring, in: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015, pp. 751–756.

[89] K. Farkas, G. Feher, A. Benczur, C. Sidlo, Crowdsending based Public Transport Information Service in Smart Cities, IEEE Communications Magazine 53 (8) (2015) 158–165.

[90] Y. Sun, H. Song, A. J. Jara, R. Bie, Internet of Things and Big Data Analytics for Smart and Connected Communities, IEEE Access 4 (2016) 766–773.

[91] W. Z. Khan, Y. Xiang, M. Y. Aalsalem, Q. Arshad, Mobile Phone Sensing Systems: A Survey, IEEE Communications Surveys Tutorials 15 (1) (2013) 402–427.

[92] Google, Science Journal, `https://makingscience.withgoogle.com/science-journal`.

[93] S. Xiang, T. Jian, X. Xuejie, X. Guoliang, Sensing as a Service: Challenges, Solutions and Future Directions, IEEE Sensors Journal 13 (10) (2013) 3733–3741.

[94] G. Cardone, A. Cirri, A. Corradi, L. Foschini, R. Ianniello, R. Montanari, Crowdsensing in Urban Areas for City-Scale Mass Gathering Management: Geofencing and Activity Recognition, IEEE Sensors Journal 14 (12) (2014) 4185–4195.

[95] Ericsson Consumer Lab, How the Internet Facilitates Smart Choices in City Life, Nov2014, `www.ericsson.com/res/docs/2014/consumerlab/ericsson-consumerlab-smart-citizens.pdf`.

[96] M. Pouryazdan, B. Kantarci, The Smart Citizen Factor in Trustworthy Smart City Crowdsensing, IT Professional 18 (4) (2016) 26–33.

[97] L. Kalogiros, K. Lagouvardos, S. Nikoletseas, N. Papadopoulos, P. Tzamalis, A hybrid mhealth mobile crowdsensing system for allergic diseases epidemiology, in: 5th International Workshop on Crowd Assisted Sensing, Pervasive Systems and Communications, (CASPer), 2018.

[98] C. M. Angelopoulos, S. Nikoletseas, T. P. Raptis, J. D. P. Rolim, Characteristic utilities, join policies and efficient incentives in mobile crowdsensing systems, in: 2014 IFIP Wireless Days (WD), 2014, pp. 1–6. `doi:10.1109/WD.2014.7020795`.

[99] B. K. V. S. Dasari, M. Pouryazdan, On the impact of selective data acquisition in mobile crowd-sensing performance, in: IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), 2018, pp. 1–6.

[100] F. Anjomshoa, B. Kantarci, Sober-mcs: Sociability-oriented and battery efficient recruitment for mobile crowd-sensing, Sensors 18 (5) (2018) 1593.

[101] C. M. Angelopoulos, G. Filiosy, S. Nikoletseas, T. P. Raptis, J. D. P. Rolim, K. Veroutis, S. Ziegler, Towards a holistic federation of secure crowd-enabled iot facilities, in: IEEE International Conference on Communications (ICC), 2015, pp. 555–560.

[102] P. Alexandrou, C. M. Angelopoulos, O. Evangelatos, J. Fernandes, G. Filios, M. Karagiannis, N. Loumis, S. Nikoletseas, A. Rankov, T. P. Raptis, J. Rolim, A. Souroulagkas, A service based architecture for multidisciplinary iot experiments with crowdsourced resources, in: N. Mitton, V. Loscri, A. Mouradian (Eds.), Ad-hoc, Mobile, and Wireless Networks, Springer International Publishing, Cham, 2016, pp. 187–201.

[103] S. Ulukus, A. Yener, E. Erkip, O. Simeone, M. Zorzi, P. Grover, K. Huang, Energy Harvesting Wireless Communications: A Review of Recent Advances, IEEE Journal on Selected Areas in Communications 33 (3) (2015) 360–381. `doi:10.1109/JSAC.2015.2391531`.

[104] K. Gai, M. Qiu, H. Zhao, L. Tao, Z. Zong, Dynamic Energy-Aware Cloudlet-Based Mobile Cloud Computing Model for Green Computing, Journal of Network and Computer Applications 59 (Supplement C) (2016) 46 – 54. `doi:https://doi.org/10.1016/j.jnca.2015.05.016`. URL `http://www.sciencedirect.com/science/article/pii/S108480451500123X`

[105] J. Montavont, D. Roth, T. Nol, Mobile IPv6 in Internet of Things: Analysis, Experimentations and Optimizations, Ad Hoc Networks 14 (Supplement C) (2014) 15 – 25. `doi:https://doi.org/10.1016/j.adhoc.2013.11.001`. URL `http://www.sciencedirect.com/science/article/pii/S1570870513002357`

[106] M. Bouaziz, A. Rachedi, A Survey on Mobility Management Protocols in Wireless Sensor Networks based on 6LoWPAN Technology, Computer Communications 74 (Supplement C) (2016) 3 – 15, current and Future Architectures, Protocols, and Services for the Internet of Things. `doi:https://doi.org/10.1016/j.comcom.2014.10.004`. URL `http://www.sciencedirect.com/science/article/pii/S0140366414003338`

ACCEPTED MANUSCRIPT

[107] O. Bello, S. Zeadally, M. Badra, Network Layer Inter-Operation of Device-to-Device Communication Technologies in Internet of Things (IoT), Ad Hoc Networks 57 (Supplement C) (2017) 52 – 62, special Issue on Internet of Things and Smart Cities security, privacy and new technologies. doi:https://doi.org/10.1016/j.adhoc.2016.06.010.
URL http://www.sciencedirect.com/science/article/pii/S1570870516301597

[108] P. Jesus, C. Baquero, P. S. Almeida, A Survey of Distributed Data Aggregation Algorithms, IEEE Communications Surveys Tutorials 17 (1) (2015) 381–404. doi:10.1109/COMST.2014.2354398.

[109] M. Yigit, V. C. Gungor, E. Fadel, L. Nassef, N. Akkari, I. F. Akyildiz, Channel-Aware Routing and Priority-Aware Multi-Channel Scheduling for WSN-Based Smart Grid Applications, Journal of Network and Computer Applications 71 (Supplement C) (2016) 50 – 58. doi:https://doi.org/10.1016/j.jnca.2016.05.015.
URL http://www.sciencedirect.com/science/article/pii/S1084804516301114

[110] L. Ma, X. Liu, Q. Pei, Y. Xiang, Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing, IEEE Transactions on Services Computing (2018) 1–1doi:10.1109/TSC.2018.2825986.

[111] L. Xu, R. Collier, G. M. P. OHare, A Survey of Clustering Techniques in WSNs and Consideration of the Challenges of Applying Such to 5G IoT Scenarios, IEEE Internet of Things Journal 4 (5) (2017) 1229–1249. doi:10.1109/JIOT.2017.2726014.

[112] W. R. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy-Efficient Communication Protocol for Wireless Microsensor Networks, in: System sciences, 2000. Proceedings of the 33rd annual Hawaii international conference on, IEEE, 2000, pp. 10–pp.

[113] Y. Lu, P. Kuonen, B. Hirsbrunner, M. Lin, Benefits of Data Aggregation on Energy Consumption in Wireless Sensor Networks, IET Communications 11 (8) (2017) 1216–1223. doi:10.1049/iet-com.2016.0990.

[114] P. Sridhar, A. M. Madni, M. Jamshidi, Hierarchical Aggregation and Intelligent Monitoring and Control in Fault-Tolerant Wireless Sensor Networks, IEEE Systems Journal 1 (1) (2007) 38–54. doi:10.1109/JSYST.2007.900244.

[115] A. Page, O. Kocabas, T. Soyata, M. K. Aktas, J. Couderc, Cloud-Based Privacy-Preserving Remote ECG Monitoring and Surveillance, Annals of Noninvasive Electrocardiology 20 (4) (2014) 328–337. doi:10.1111/anec.12204.

[116] A. Page, O. Kocabas, S. Ames, M. Venkitasubramaniam, T. Soyata, Cloud-based Secure Health Monitoring: Optimizing Fully-Homomorphic Encryption for Streaming Algorithms, in: Globecom Workshops, Austin, TX, 2014, pp. 48–52. doi:10.1109/GLOCOMW.2014.7063384.

[117] A. Ara, M. Al-Rodhaan, Y. Tian, A. Al-Dhelaan, A Secure Privacy-Preserving Data Aggregation Scheme Based on Bilinear ElGamal Cryptosystem for Remote Health Monitoring Systems, IEEE Access 5 (2017) 12601–12617. doi:10.1109/ACCESS.2017.2716439.

[118] T. Soyata, H. Ba, W. Heinzelman, M. Kwon, J. Shi, Accelerating Mobile Cloud Computing: A Survey, in: H. T. Mouftah, B. Kantarci (Eds.), Communication Infrastructures for Cloud Computing, IGI Global, 2013, Ch. 8, pp. 175–197. doi:10.4018/978-1-4666-4522-6.ch008.

[119] T. Soyata, GPU Parallel Program Development Using CUDA, Taylor and Francis, 2018.

[120] U. Shaukat, E. Ahmed, Z. Anwar, F. Xia, Cloudlet Deployment in Local Wireless Networks: Motivation, Architectures, Applications, and Open Challenges, Journal of Network and Computer Applications 62 (Supplement C) (2016) 18 – 40. doi:https://doi.org/10.1016/j.jnca.2015.11.009.
URL http://www.sciencedirect.com/science/article/pii/S1084804515002817

[121] Y. Chen, Y. Chen, Q. Cao, X. Yang, PacketCloud: A Cloudlet-Based Open Platform for In-Network Services, IEEE Transactions on Parallel and Distributed Systems 27 (4) (2016) 1146–1159. doi:10.1109/TPDS.2015.2424222.

[122] O. Kocabas, R. Gyampoh-Vidogah, T. Soyata, Operational Cost of Running Real-Time Mobile Cloud Applications, in: T. Soyata (Ed.), Enabling Real-Time Mobile Cloud Computing through Emerging Technologies, IGI Global, 2015, Ch. 10, pp. 294–321. doi:10.4018/978-1-4666-8662-5.ch010.

[123] C. Hennebert, J. D. Santos, Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis, IEEE Internet of Things Journal 1 (5) (2014) 384–398. doi:10.1109/JIOT.2014.2359538.

[124] W. Xiong, X. Hu, T. Jiang, Measurement and Characterization of Link Quality for IEEE 802.15.4-Compliant Wireless Sensor Networks in Vehicular Communications, IEEE Transactions on Industrial Informatics 12 (5) (2016) 1702–1713. doi:10.1109/TII.2015.2499121.

[125] J. Granjal, E. Monteiro, J. S. Silva, Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues, IEEE Communications Surveys Tutorials 17 (3) (2015) 1294–1312. doi:10.1109/COMST.2015.2388550.

[126] T. C. Arcadius, B. Gao, G. Tian, Y. Yan, Structural Health Monitoring Framework Based on Internet of Things: A Survey, IEEE Internet of Things Journal PP (99) (2017) 1–1. doi:10.1109/JIOT.2017.2664072.

[127] O. Iova, F. Theoleyre, T. Watteyne, T. Noel, The Love-Hate Relationship between IEEE 802.15.4 and RPL, IEEE Communications Magazine 55 (1) (2017) 188–194. doi:10.1109/MCOM.2016.1300687RP.

[128] A. Ludovici, A. Calveras, A Proxy Design to Leverage the Interconnection of CoAP Wireless Sensor Networks with Web Applications, Sensors 15 (1) (2015) 1217–1244. doi:10.3390/s150101217.
URL http://www.mdpi.com/1424-8220/15/1/1217

[129] A. Betzler, C. Gomez, I. Demirkol, J. Paradells, CoAP Congestion Control for the Internet of Things, IEEE Communications Magazine 54 (7) (2016) 154–160. doi:10.1109/MCOM.2016.7509394.

[130] A. P. Castellani, M. Rossi, M. Zorzi, Back Pressure Congestion Control for CoAP/6LoWPAN Networks, Ad Hoc Networks 18 (Supplement C) (2014) 71 – 84. doi:https://doi.org/10.1016/j.adhoc.2013.02.007.
URL http://www.sciencedirect.com/science/article/pii/S1570870513000279

[131] Z. Shelby, RFC 7252-The Constrained Application Protocol (CoAP). Internet Engineering Task Force (IETF)(2014) (2016).

[132] A. Stanford-Clark, H. L. Truong, MQTT for Sensor Networks (MQTT-SN) Protocol Specification, International business machines (IBM) Corporation version 1.

[133] P. Saint-Andre, Extensible Messaging and Presence Protocol (XMPP): Address Format.

[134] H. Wang, D. Xiong, P. Wang, Y. Liu, A Lightweight XMPP Publish/Subscribe Scheme for Resource-Constrained IoT Devices, IEEE Access 5 (2017) 16393–16405. doi:10.1109/ACCESS.2017.2742020.

[135] A. Celesti, M. Fazio, M. Villari, Enabling Secure XMPP Communications in Federated IoT Clouds Through XEP 0027 and SAML/SASL SSO, Sensors 17 (2). doi:10.3390/

ACCEPTED MANUSCRIPT

s17020301.
URL http://www.mdpi.com/1424-8220/17/2/301

[136] Link to AMQP V1.0 Specifications, http://www.amqp.org/sites/amqp.org/files/amqp.pdf, accessed 26 Dec. 2017 (2017).

[137] Z. Sheng, S. Yang, Y. Yu, A. V. Vasilakos, J. A. Mccann, K. K. Leung, A Survey on The IETF Protocol Suite for The Internet of Things: Standards, Challenges, and Opportunities, IEEE Wireless Communications 20 (6) (2013) 91–98. doi:10.1109/MWC.2013.6704479.

[138] L. Atzori, A. Iera, G. Morabito, The Internet of Things: A survey, Computer Networks 54 (15) (2010) 2787 – 2805. doi:https://doi.org/10.1016/j.comnet.2010.05.010.
URL http://www.sciencedirect.com/science/article/pii/S1389128610001568

[139] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, IEEE Communications Surveys Tutorials 17 (4) (2015) 2347–2376. doi:10.1109/COMST.2015.2444095.

[140] R. Faragher, R. Harle, Location Fingerprinting With Bluetooth Low Energy Beacons, IEEE Journal on Selected Areas in Communications 33 (11) (2015) 2418–2428. doi:10.1109/JSAC.2015.2430281.

[141] F. Lin, A. Wang, Y. Zhuang, M. R. Tomita, W. Xu, Smart Insole: A Wearable Sensor Device for Unobtrusive Gait Monitoring in Daily Life, IEEE Transactions on Industrial Informatics 12 (6) (2016) 2281–2291. doi:10.1109/TII.2016.2585643.

[142] P. M. Varela, T. O. Ohtsuki, Discovering Co-Located Walking Groups of People Using iBeacon Technology, IEEE Access 4 (2016) 6591–6601. doi:10.1109/ACCESS.2016.2615863.

[143] D. S. Lee, T. W. Chong, B. G. Lee, Stress Events Detection of Driver by Wearable Glove System, IEEE Sensors Journal 17 (1) (2017) 194–204. doi:10.1109/JSEN.2016.2625323.

[144] G. Mokhtari, Q. Zhang, G. Nourbakhsh, S. Ball, M. Karunanithi, PBLUESOUND: A New Resident Identification Sensor–Using Ultrasound Array and BLE Technology for Smart Home Platform, IEEE Sensors Journal 17 (5) (2017) 1503–1512. doi:10.1109/JSEN.2017.2647960.

[145] Bluetooth Special Interest Group (SIG), Core Specifications - Bluetooth Technology Website, https://www.bluetooth.com/specifications/bluetooth-core-specification, accessed 17 Oct 2017 (2017).

[146] M. Siekkinen, M. Hiienkari, J. K. Nurminen, J. Nieminen, How Low Energy Is Bluetooth Low Energy? Comparative Measurements with ZigBee/802.15. 4, in: Wireless Communications and Networking Conference Workshops (WCNCW), 2012 IEEE, IEEE, 2012, pp. 232–237.

[147] C. Pham, Communication Performances of IEEE 802.15.4 Wireless Sensor Motes for Data-Intensive Applications: A Comparison of WaspMote, Arduino MEGA, TelosB, MicaZ and iMote2 for Image Surveillance, Journal of Network and Computer Applications 46 (Supplement C) (2014) 48 – 59. doi:https://doi.org/10.1016/j.jnca.2014.08.002.
URL http://www.sciencedirect.com/science/article/pii/S108480451400188X

[148] K. Mikhaylov, N. Plevritakis, J. Tervonen, Performance Analysis and Comparison of Bluetooth Low Energy with IEEE 802.15.4 and SimpliciTI, Journal of Sensor and Actuator Networks 2 (3) (2013) 589–613. doi:10.3390/jsan2030589.
URL http://www.mdpi.com/2224-2708/2/3/589

[149] M. Khanafer, M. Guennoun, H. T. Mouftah, A Survey of Beacon-Enabled IEEE 802.15.4 MAC Protocols in Wireless Sensor Networks, IEEE Communications Surveys Tutorials 16 (2) (2014) 856–876. doi:10.1109/SURV.2013.112613.00094.

[150] Y. H. Zhu, S. Qiu, K. Chi, Y. Fang, Latency Aware IPv6 Packet Delivery Scheme over IEEE 802.15.4 Based Battery-Free Wireless Sensor Networks, IEEE Transactions on Mobile Computing 16 (6) (2017) 1691–1704. doi:10.1109/TMC.2016.2601906.

[151] J. A. Nazabal, F. Falcone, C. Fernndez-Valdivielso, I. R. Matas, Development of a Low Mobility IEEE 802.15.4 Compliant VANET System for Urban Environments, Sensors 13 (6) (2013) 7065–7078. doi:10.3390/s130607065.
URL http://www.mdpi.com/1424-8220/13/6/7065

[152] A. Babu, K. Dube, S. Mukhopadhyay, H. Ghayvat, J. K. M. V, Accelerometer Based Human Activities and Posture Recognition, in: 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE), 2016, pp. 367–373. doi:10.1109/SAPIENCE.2016.7684120.

[153] T. Torfs, T. Sterken, S. Brebels, J. Santana, R. van den Hoven, V. Spiering, N. Bertsch, D. Trapani, D. Zonta, Low Power Wireless Sensor Network for Building Monitoring, IEEE Sensors Journal 13 (3) (2013) 909–915. doi:10.1109/JSEN.2012.2218680.

[154] C. T. Kone, A. Hafid, M. Boushaba, Performance Management of IEEE 802.15.4 Wireless Sensor Network for Precision Agriculture, IEEE Sensors Journal 15 (10) (2015) 5734–5747. doi:10.1109/JSEN.2015.2442259.

[155] ZigBee Alliance, ZigBee Alliance Web page, http://www.zigbee.org/, accessed 10 Nov. 2017 (2017).

[156] T. Zillner, S. Strobl, ZigBee Exploited: The Good the Bad and the Ugly (2015).

[157] R. I. Gomaa, I. A. Shohdy, K. A. Sharshar, A. S. Al-Kabbani, H. F. Ragai, Real-Time Radiological Monitoring of Nuclear Facilities Using ZigBee Technology, IEEE Sensors Journal 14 (11) (2014) 4007–4013. doi:10.1109/JSEN.2014.2357803.

[158] E. D. N. Ndih, S. Cherkaoui, On Enhancing Technology Coexistence in the IoT Era: ZigBee and 802.11 Case, IEEE Access 4 (2016) 1835–1844. doi:10.1109/ACCESS.2016.2553150.

[159] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, L. Ladid, Internet of Things in the 5G Era: Enablers, Architecture, and Business Models, IEEE Journal on Selected Areas in Communications 34 (3) (2016) 510–527. doi:10.1109/JSAC.2016.2525418.

[160] T. de Almeida Oliveira, E. P. Godoy, ZigBee Wireless Dynamic Sensor Networks: Feasibility Analysis and Implementation Guide, IEEE Sensors Journal 16 (11) (2016) 4614–4621. doi:10.1109/JSEN.2016.2542063.

[161] P. Yang, Y. Yan, X. Y. Li, Y. Zhang, Y. Tao, L. You, Taming Cross-Technology Interference for Wi-Fi and ZigBee Coexistence Networks, IEEE Transactions on Mobile Computing 15 (4) (2016) 1009–1021. doi:10.1109/TMC.2015.2442252.

[162] Y. Kim, S. Lee, S. Lee, Coexistence of ZigBee-Based WBAN and WiFi for Health Telemonitoring Systems, IEEE Journal of Biomedical and Health Informatics 20 (1) (2016) 222–230. doi:10.1109/JBHI.2014.2387867.

[163] Z. Zhao, W. Dong, G. Chen, G. Min, T. Gu, J. Bu, Embracing Corruption Burstiness: Fast Error Recovery for ZigBee under Wi-Fi Interference, IEEE Transactions on Mobile Computing 16 (9) (2017) 2518–2530. doi:10.1109/TMC.2016.2630696.

[164] Y. Yan, P. Yang, X. Y. Li, Y. Zhang, J. Lu, L. You, J. Wang, J. Han, Y. Xiong, WizBee: Wise ZigBee Coexistence via Interference Cancellation with Single Antenna, IEEE Transac-

ACCEPTED MANUSCRIPT

tions on Mobile Computing 14 (12) (2015) 2590–2603. doi:10.1109/TMC.2014.2359673.

[165] H. R. Chi, K. F. Tsang, K. T. Chui, H. S. H. Chung, B. W. K. Ling, L. L. Lai, Interference-Mitigated ZigBee-Based Advanced Metering Infrastructure, IEEE Transactions on Industrial Informatics 12 (2) (2016) 672–684. doi:10.1109/TII.2016.2527618.

[166] M. A. Setiawan, F. Shahnia, S. Rajakaruna, A. Ghosh, ZigBee-Based Communication System for Data Transfer Within Future Microgrids, IEEE Transactions on Smart Grid 6 (5) (2015) 2343–2355. doi:10.1109/TSG.2015.2402678.

[167] F. Shariff, N. A. Rahim, W. P. Hew, ZigBee-Based Data Acquisition System for Online Monitoring of Grid-Connected Photovoltaic System, Expert Systems with Applications 42 (3) (2015) 1730 – 1742. doi:https://doi.org/10.1016/j.eswa.2014.10.007.
URL http://www.sciencedirect.com/science/article/pii/S0957417414006307

[168] M. Tolani, Sunny, R. K. Singh, K. Shubham, R. Kumar, Two-Layer Optimized Railway Monitoring System Using Wi-Fi and ZigBee Interfaced Wireless Sensor Network, IEEE Sensors Journal 17 (7) (2017) 2241–2248. doi:10.1109/JSEN.2017.2658730.

[169] L. H. Wang, T. Y. Chen, K. H. Lin, Q. Fang, S. Y. Lee, Implementation of a Wireless ECG Acquisition SoC for IEEE 802.15.4 (ZigBee) Applications, IEEE Journal of Biomedical and Health Informatics 19 (1) (2015) 247–255. doi:10.1109/JBHI.2014.2311232.

[170] A. Kumar, G. P. Hancke, A Zigbee-Based Animal Health Monitoring System, IEEE Sensors Journal 15 (1) (2015) 610–617. doi:10.1109/JSEN.2014.2349073.

[171] C. Peng, K. Qian, C. Wang, Design and Application of a VOC-Monitoring System Based on a ZigBee Wireless Sensor Network, IEEE Sensors Journal 15 (4) (2015) 2255–2268. doi:10.1109/JSEN.2014.2374156.

[172] A. C. Jose, R. Malekian, Improving Smart Home Security: Integrating Logical Sensing Into Smart Home, IEEE Sensors Journal 17 (13) (2017) 4269–4286. doi:10.1109/JSEN.2017.2705045.

[173] J. Niu, B. Wang, L. Shu, T. Q. Duong, Y. Chen, ZIL: An Energy-Efficient Indoor Localization System Using ZigBee Radio to Detect WiFi Fingerprints, IEEE Journal on Selected Areas in Communications 33 (7) (2015) 1431–1442. doi:10.1109/JSAC.2015.2430171.

[174] Q. Wang, J. Jiang, Comparative Examination on Architecture and Protocol of Industrial Wireless Sensor Network Standards, IEEE Communications Surveys Tutorials 18 (3) (2016) 2197–2219. doi:10.1109/COMST.2016.2548360.

[175] O. Khader, A. Willig, An Energy Consumption Analysis of the Wireless HART TDMA Protocol, Computer Communications 36 (7) (2013) 804 – 816. doi:https://doi.org/10.1016/j.comcom.2012.12.008.
URL http://www.sciencedirect.com/science/article/pii/S0140366413000029

[176] M. Boushaba, A. Hafid, M. Gendreau, Source-Based Routing in Wireless Mesh Networks, IEEE Systems Journal 10 (1) (2016) 262–270. doi:10.1109/JSYST.2014.2317453.

[177] M. Sha, D. Gunatilaka, C. Wu, C. Lu, Empirical Study and Enhancements of Industrial Wireless Sensor-Actuator Network Protocols, IEEE Internet of Things Journal 4 (3) (2017) 696–704. doi:10.1109/JIOT.2017.2653362.

[178] M. Nobre, I. Silva, L. A. Guedes, Performance Evaluation of WirelessHART Networks using A New Network Simulator 3 Module, Computers & Electrical Engineering 41 (Supplement C) (2015) 325 – 341. doi:https://doi.org/10.1016/j.compeleceng.2014.05.005.
URL http://www.sciencedirect.com/science/article/pii/S0045790614001311

[179] H. Zhang, P. Soldati, M. Johansson, Performance Bounds and Latency-Optimal Scheduling for Convergecast in WirelessHART Networks, IEEE Transactions on Wireless Communications 12 (6) (2013) 2688–2696. doi:10.1109/TWC.2013.050313.120543.

[180] S. Petersen, S. Carlsen, WirelessHART Versus ISA100.11a: The Format War Hits the Factory Floor, IEEE Industrial Electronics Magazine 5 (4) (2011) 23–34. doi:10.1109/MIE.2011.943023.

[181] X. Jin, F. Kong, L. Kong, W. Liu, P. Zeng, Reliability and Temporality Optimization for Multiple Coexisting WirelessHART Networks in Industrial Environments, IEEE Transactions on Industrial Electronics 64 (8) (2017) 6591–6602. doi:10.1109/TIE.2017.2682005.

[182] K. Das, P. Zand, P. Havinga, Industrial Wireless Monitoring with Energy-Harvesting Devices, IEEE Internet Computing 21 (1) (2017) 12–20. doi:10.1109/MIC.2017.2.

[183] Z. Bi, D. Chen, C. Wang, C. Jiang, M. Chen, Adopting WirelessHART for In-vehicle-Networking, in: 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems, 2015, pp. 1027–1030. doi:10.1109/HPCC-CSS-ICESS.2015.244.

[184] X. Zhu, W. Dong, A. K. Mok, S. Han, J. Song, D. Chen, M. Nixon, A Location-Determination Application in WirelessHART, in: 2009 15th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, 2009, pp. 263–270. doi:10.1109/RTCSA.2009.36.

[185] N. A. Cloete, R. Malekian, L. Nair, Design of Smart Sensors for Real-Time Water Quality Monitoring, IEEE Access 4 (2016) 3975–3990. doi:10.1109/ACCESS.2016.2592958.

[186] L. Ascorti, S. Savazzi, G. Soatti, M. Nicoli, E. Sisinni, S. Galimberti, A Wireless Cloud Network Platform for Industrial Process Automation: Critical Data Publishing and Distributed Sensing, IEEE Transactions on Instrumentation and Measurement 66 (4) (2017) 592–603. doi:10.1109/TIM.2016.2640579.

[187] IEEE Standard for Information Technology–Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Sub 1 GHz License Exempt Operation, IEEE Std 802.11ah-2016 (Amendment to IEEE Std 802.11-2016, as amended by IEEE Std 802.11ai-2016) (2017) 1–594doi:10.1109/IEEESTD.2017.7920364.

[188] V. Baos-Gonzalez, M. S. Afaqui, E. Lopez-Aguilera, E. Garcia-Villegas, IEEE 802.11ah: A Technology to Face the IoT Challenge, Sensors 16 (11). doi:10.3390/s16111960.
URL http://www.mdpi.com/1424-8220/16/11/1960

[189] N. Ahmed, H. Rahman, M. Hussain, A Comparison of 802.11ah and 802.15.4 for IoT, ICT Express 2 (3) (2016) 100 – 102, special Issue on ICT Convergence in the Internet of Things (IoT). doi:https://doi.org/10.1016/j.icte.2016.07.003.
URL http://www.sciencedirect.com/science/article/pii/S2405959516300650

[190] M. Park, IEEE 802.11ah: Sub-1-GHz License-Exempt Operation for the Internet of Things, IEEE Communications Magazine 53 (9) (2015) 145–151. doi:10.1109/MCOM.2015.

ACCEPTED MANUSCRIPT

7263359.

[191] G. C. Madueo, . Stefanovi, P. Popovski, Reliable and Efficient Access for Alarm-Initiated and Regular M2M Traffic in IEEE 802.11ah Systems, IEEE Internet of Things Journal 3 (5) (2016) 673–682. doi:10.1109/JIOT.2015.2496418.

[192] E. Khorov, A. Lyakhov, A. Krotov, A. Guschin, A Survey on IEEE 802.11ah: An Enabling Networking Technology for Smart Cities, Computer Communications 58 (Supplement C) (2015) 53 – 69, special Issue on Networking and Communications for Smart Cities. doi:https://doi.org/10.1016/j.comcom.2014.08.008.
URL http://www.sciencedirect.com/science/article/pii/S0140366414002989

[193] T. Adame, A. Bel, B. Bellalta, J. Barcelo, M. Oliver, IEEE 802.11ah: The WiFi Approach for M2M Communications, IEEE Wireless Communications 21 (6) (2014) 144–152. doi:10.1109/MWC.2014.7000982.

[194] A. Hazmi, L. F. Del Carpio, A. Goekceoglu, B. Badihi, P. Amin, A. Larmo, M. Valkama, et al., Duty Cycle Challenges of IEEE 802.11ah Networks in M2M and IoT Applications, in: European Wireless 2016; 22th European Wireless Conference; Proceedings of, VDE, 2016, pp. 1–7.

[195] W. Sun, M. Choi, S. Choi, IEEE 802.11 ah: A Long Range 802.11 WLAN at Sub 1 GHz, Journal of ICT Standardization 1 (1) (2013) 83–108.

[196] W. Damayanti, S. Kim, J.-H. Yun, Collision Chain Mitigation and Hidden Device-Aware Grouping in Large-Scale IEEE 802.11ah Networks, Computer Networks 108 (Supplement C) (2016) 296 – 306. doi:https://doi.org/10.1016/j.comnet.2016.09.006.
URL http://www.sciencedirect.com/science/article/pii/S1389128616302882

[197] L. Tian, J. Famaey, S. Latr, Evaluation of the IEEE 802.11ah Restricted Access Window Mechanism for Dense IoT Networks, in: 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2016, pp. 1–9. doi:10.1109/WoWMoM.2016.7523502.

[198] U. Raza, P. Kulkarni, M. Sooriyabandara, Low Power Wide Area Networks: An Overview, IEEE Communications Surveys & Tutorials 19 (2) (2017) 855–873.

[199] S. Y. Lien, C. C. Chien, F. M. Tseng, T. C. Ho, 3GPP Device-to-Device Communications for Beyond 4G Cellular Networks, IEEE Communications Magazine 54 (3) (2016) 29–35. doi:10.1109/MCOM.2016.7432168.

[200] Qualcomme Inc., LTE Direct, https://www.qualcomm.com/invention/technologies/lte/direct, accessed 12 Dec. 2017 (2017).

[201] C. Hoymann, D. Astely, M. Stattin, G. Wikstrom, J. F. Cheng, A. Hoglund, M. Frenne, R. Blasco, J. Huschke, F. Gunnarsson, LTE Release 14 Outlook, IEEE Communications Magazine 54 (6) (2016) 44–49. doi:10.1109/MCOM.2016.7497765.

[202] J. Lee, Y. Kim, Y. Kwak, J. Zhang, A. Papasakellariou, T. Novlan, C. Sun, Y. Li, LTE-Advanced in 3GPP Rel-13/14: An Evolution toward 5G, IEEE Communications Magazine 54 (3) (2016) 36–42. doi:10.1109/MCOM.2016.7432169.

[203] S. Y. Lien, C. C. Chien, G. S. T. Liu, H. L. Tsai, R. Li, Y. J. Wang, Enhanced LTE Device-to-Device Proximity Services, IEEE Communications Magazine 54 (12) (2016) 174–182. doi:10.1109/MCOM.2016.1500670CM.

[204] M. Elsaadany, A. Ali, W. Hamouda, Cellular LTE-A Technologies for the Future Internet-of-Things: Physical Layer Features and Challenges, IEEE Communications Surveys Tutorials 19 (4) (2017) 2544–2572. doi:10.1109/COMST.2017.2728013.

[205] C. Zhao, L. Huang, Y. Zhao, X. Du, Secure Machine-Type Communications toward LTE Heterogeneous Networks, IEEE Wireless Communications 24 (1) (2017) 82–87. doi:10.1109/MWC.2017.1600141WC.

[206] S. Abdelwahab, B. Hamdaoui, M. Guizani, T. Znati, Replisom: Disciplined Tiny Memory Replication for Massive IoT Devices in LTE Edge Cloud, IEEE Internet of Things Journal 3 (3) (2016) 327–338. doi:10.1109/JIOT.2015.2497263.

[207] J. Liu, N. Kato, J. Ma, N. Kadowaki, Device-to-Device Communication in LTE-Advanced Networks: A Survey, IEEE Communications Surveys Tutorials 17 (4) (2015) 1923–1940. doi:10.1109/COMST.2014.2375934.

[208] L. Falconetti, D. H. Kang, R. Karaki, E. Obregon, J. F. Cheng, H. Koorapaty, A. Mukherjee, S. Falahati, D. Larsson, Design and Evaluation of Licensed Assisted Access LTE in Unlicensed Spectrum, IEEE Wireless Communications 23 (6) (2016) 24–30. doi:10.1109/MWC.2016.1600049WC.

[209] Y. Gao, Z. Qin, Z. Feng, Q. Zhang, O. Holland, M. Dohler, Scalable and Reliable IoT Enabled by Dynamic Spectrum Management for M2M in LTE-A, IEEE Internet of Things Journal 3 (6) (2016) 1135–1145. doi:10.1109/JIOT.2016.2562140.

[210] M. Centenaro, L. Vangelista, A. Zanella, M. Zorzi, Long-Range Communications in Unlicensed Bands: The Rising Stars in the IoT and Smart City Scenarios, IEEE Wireless Communications 23 (5) (2016) 60–67. doi:10.1109/MWC.2016.7721743.

[211] N. Ksairi, S. Tomasin, M. Debbah, A Multi-Service Oriented Multiple Access Scheme for M2M Support in Future LTE, IEEE Communications Magazine 55 (1) (2017) 218–224. doi:10.1109/MCOM.2016.1500689CM.

[212] K. Zheng, S. Ou, J. Alonso-Zarate, M. Dohler, F. Liu, H. Zhu, Challenges of Massive Access in Highly Dense LTE-Advanced Networks with Machine-to-Machine Communications, IEEE Wireless Communications 21 (3) (2014) 12–18. doi:10.1109/MWC.2014.6845044.

[213] F. Ghavimi, H. H. Chen, M2M Communications in 3GPP LTE/LTE-A Networks: Architectures, Service Requirements, Challenges, and Applications, IEEE Communications Surveys Tutorials 17 (2) (2015) 525–549. doi:10.1109/COMST.2014.2361626.

[214] P. Schulz, M. Matthe, H. Klessig, M. Simsek, G. Fettweis, J. Ansari, S. A. Ashraf, B. Almeroth, J. Voigt, I. Riedel, A. Puschmann, A. Mitschele-Thiel, M. Muller, T. Elste, M. Windisch, Latency Critical IoT Applications in 5G: Perspective on the Design of Radio Interface and Network Architecture, IEEE Communications Magazine 55 (2) (2017) 70–78. doi:10.1109/MCOM.2017.1600435CM.

[215] N. H. Motlagh, M. Bagaa, T. Taleb, UAV-Based IoT Platform: A Crowd Surveillance Use Case, IEEE Communications Magazine 55 (2) (2017) 128–134. doi:10.1109/MCOM.2017.1600587CM.

[216] N. Powers, T. Soyata, AXaaS (Acceleration as a Service): Can the Telecom Service Provider Rent a Cloudlet ?, in: Proceedings of the 4th IEEE International Conference on Cloud Networking, Niagara Falls, Canada, 2015, pp. 232–238. doi:10.1109/CloudNet.2015.7335314.

[217] N. Powers, A. Alling, K. Osolinsky, T. Soyata, M. Zhu, H. Wang, H. Ba, W. Heinzelman, J. Shi, M. Kwon, The Cloudlet Accelerator: Bringing Mobile-Cloud Face Recognition into Real-Time, in: Globecom Workshops, San Diego, CA, 2015, pp. 1–7. doi:10.1109/GLOCOMW.2015.7414055.

[218] E. Inga, S. Cespedes, R. Hincapie, C. A. Cardenas, Scalable Route Map for Advanced Metering Infrastructure Based on Optimal Routing of Wireless Heterogeneous Networks, IEEE

ACCEPTED MANUSCRIPT

Wireless Communications 24 (2) (2017) 26–33. doi:10.1109/MWC.2017.1600255.

[219] J. D. Benedetto, P. Bellavista, L. Foschini, Proximity Discovery and Data Dissemination for Mobile Crowd Sensing using LTE Direct, Computer Networks 129 (Part 2) (2017) 510 – 521, special Issue on 5G Wireless Networks for IoT and Body Sensors. doi:https://doi.org/10.1016/j.comnet.2017.08.002.
URL http://www.sciencedirect.com/science/article/pii/S1389128617303092

[220] L. Gallo, J. Haerri, Unsupervised Long- Term Evolution Device-to-Device: A Case Study for Safety-Critical V2X Communications, IEEE Vehicular Technology Magazine 12 (2) (2017) 69–77. doi:10.1109/MVT.2017.2669346.

[221] V. Petrov, A. Samuylov, V. Begishev, D. Moltchanov, S. Andreev, K. Samouylov, Y. Koucheryavy, Vehicle-Based Relay Assistance for Opportunistic Crowdsensing over Narrowband IoT (NB-IoT), IEEE Internet of Things Journal PP (99) (2017) 1–1. doi:10.1109/JIOT.2017.2670363.

[222] Y. P. E. Wang, X. Lin, A. Adhikary, A. Grovlen, Y. Sui, Y. Blankenship, J. Bergman, H. S. Razaghi, A Primer on 3GPP Narrowband Internet of Things, IEEE Communications Magazine 55 (3) (2017) 117–123. doi:10.1109/MCOM.2017.1600510CM.

[223] R. Ratasuk, N. Mangalvedhe, Z. Xiong, M. Robert, D. Bhatoolaul, Enhancements of Narrowband IoT in 3GPP Rel-14 and Rel-15, in: 2017 IEEE Conference on Standards for Communications and Networking (CSCN), 2017, pp. 60–65. doi:10.1109/CSCN.2017.8088599.

[224] R. S. Sinha, Y. Wei, S.-H. Hwang, A Survey on LPWA Technology: LoRa and NB-IoT, ICT Express 3 (1) (2017) 14 – 21. doi:https://doi.org/10.1016/j.icte.2017.03.004.
URL http://www.sciencedirect.com/science/article/pii/S2405959517300061

[225] Y. D. Beyene, R. Jantti, O. Tirkkonen, K. Ruttik, S. Iraji, A. Larmo, T. Tirronen, a. J. Torsner, NB-IoT Technology Overview and Experience from Cloud-RAN Implementation, IEEE Wireless Communications 24 (3) (2017) 26–32. doi:10.1109/MWC.2017.1600418.

[226] Y. D. Beyene, R. Jantti, K. Ruttik, S. Iraji, On the Performance of Narrow-Band Internet of Things (NB-IoT), in: 2017 IEEE Wireless Communications and Networking Conference (WCNC), 2017, pp. 1–6. doi:10.1109/WCNC.2017.7925809.

[227] C. Yu, L. Yu, Y. Wu, Y. He, Q. Lu, Uplink Scheduling and Link Adaptation for Narrowband Internet of Things Systems, IEEE Access 5 (2017) 1724–1734. doi:10.1109/ACCESS.2017.2664418.

[228] J. Lee, J. Lee, Prediction-Based Energy Saving Mechanism in 3GPP NB-IoT Networks, Sensors 17 (9). doi:10.3390/s17092008.
URL http://www.mdpi.com/1424-8220/17/9/2008

[229] S. Liu, F. Yang, J. Song, Z. Han, Block Sparse Bayesian Learning-Based NB-IoT Interference Elimination in LTE-Advanced Systems, IEEE Transactions on Communications 65 (10) (2017) 4559–4571. doi:10.1109/TCOMM.2017.2723572.

[230] Y. C. Wang, G. W. Chen, Efficient Data Gathering and Estimation for Metropolitan Air Quality Monitoring by Using Vehicular Sensor Networks, IEEE Transactions on Vehicular Technology 66 (8) (2017) 7234–7248. doi:10.1109/TVT.2017.2655084.

[231] M. Habibzadeh, W. Xiong, M. Zheleva, E. K. Stern, B. H. Nussbaum, T. Soyata, Smart City Sensing and Communication Sub-Infrastructure, in: IEEE Midwest Symposium on Circuits and Systems, Boston, MA, 2017, pp. 1159–1162. doi:10.1109/MWSCAS.2017.8053134.

[232] O. N. C. Yilmaz, Y. P. E. Wang, N. A. Johansson, N. Brahmi, S. A. Ashraf, J. Sachs, Analysis of Ultra-Reliable and Low-Latency 5G Communication for A Factory Automation Use Case, in: 2015 IEEE International Conference on Communication Workshop (ICCW), 2015, pp. 1190–1195. doi:10.1109/ICCW.2015.7247339.

[233] F. Camacho, C. Cárdenas, D. Muñoz, Emerging Technologies and Research Challenges for Intelligent Transportation Systems: 5G, HetNets, and SDN, International Journal on Interactive Design and Manufacturing (IJIDeM) (2017) 1–9.

[234] A. Osseiran, F. Boccardi, V. Braun, K. Kusume, P. Marsch, M. Maternia, O. Queseth, M. Schellmann, H. Schotten, H. Taoka, H. Tullberg, M. A. Uusitalo, B. Timus, M. Fallgren, Scenarios for 5G Mobile and Wireless Communications: the Vision of the METIS Project, IEEE Communications Magazine 52 (5) (2014) 26–35. doi:10.1109/MCOM.2014.6815890.

[235] M. Taha, L. Parra, L. Garcia, J. Lloret, An Intelligent Handover Process Algorithm in 5G Networks: The Use Case of Mobile Cameras for Environmental Surveillance, in: 2017 IEEE International Conference on Communications Workshops (ICC Workshops), 2017, pp. 840–844. doi:10.1109/ICCW.2017.7962763.

[236] D. M. West, How 5G Technology Enables the Health Internet of Things, Brookings Center for Technology Innovation 3 (2016) 1–20.

[237] M. Agiwal, A. Roy, N. Saxena, Next Generation 5G Wireless Networks: A Comprehensive Survey, IEEE Communications Surveys Tutorials 18 (3) (2016) 1617–1655. doi:10.1109/COMST.2016.2532458.

[238] N. Saxena, A. Roy, B. J. R. Sahu, H. Kim, Efficient IoT Gateway over 5G Wireless: A New Design with Prototype and Implementation Results, IEEE Communications Magazine 55 (2) (2017) 97–105. doi:10.1109/MCOM.2017.1600437CM.

[239] O. Galinina, S. Andreev, M. Komarov, S. Maltseva, Leveraging Heterogeneous Device Connectivity in A Converged 5G-IoT Ecosystem, Computer Networks 128 (Supplement C) (2017) 123 – 132, survivability Strategies for Emerging Wireless Networks. doi:https://doi.org/10.1016/j.comnet.2017.04.051.
URL http://www.sciencedirect.com/science/article/pii/S1389128617301822

[240] A. Costanzo, D. Masotti, Energizing 5G: Near- and Far-Field Wireless Energy and Data Trantransfer as an Enabling Technology for the 5G IoT, IEEE Microwave Magazine 18 (3) (2017) 125–136. doi:10.1109/MMM.2017.2664001.

[241] Y. Mehmood, N. Haider, M. Imran, A. Timm-Giel, M. Guizani, M2M Communications in 5G: State-of-the-Art Architecture, Recent Advances, and Research Challenges, IEEE Communications Magazine 55 (9) (2017) 194–201. doi:10.1109/MCOM.2017.1600559.

[242] D. Zhang, Z. Zhou, S. Mumtaz, J. Rodriguez, T. Sato, One Integrated Energy Efficiency Proposal for 5G IoT Communications, IEEE Internet of Things Journal 3 (6) (2016) 1346–1354. doi:10.1109/JIOT.2016.2599852.

[243] A. Orsino, A. Ometov, G. Fodor, D. Moltchanov, L. Militano, S. Andreev, O. N. C. Yilmaz, T. Tirronen, J. Torsner, G. Araniti, A. Iera, M. Dohler, Y. Koucheryavy, Effects of Heterogeneous Mobility on D2D- and Drone-Assisted Mission-Critical MTC in 5G, IEEE Communications Magazine 55 (2) (2017) 79–87. doi:10.1109/MCOM.2017.1600443CM.

[244] S. Hur, S. Baek, B. Kim, Y. Chang, A. F. Molisch, T. S. Rappaport, K. Haneda, J. Park, Proposal on Millimeter-Wave

ACCEPTED MANUSCRIPT

Channel Modeling for 5G Cellular System, IEEE Journal of Selected Topics in Signal Processing 10 (3) (2016) 454–469. doi:10.1109/JSTSP.2016.2527364.

[245] M. K. Samimi, T. S. Rappaport, 3-D Millimeter-Wave Statistical Channel Model for 5G Wireless System Design, IEEE Transactions on Microwave Theory and Techniques 64 (7) (2016) 2207–2225. doi:10.1109/TMTT.2016.2574851.

[246] J. Huang, C. X. Wang, R. Feng, J. Sun, W. Zhang, Y. Yang, Multi-Frequency mmWave Massive MIMO Channel Measurements and Characterization for 5G Wireless Communication Systems, IEEE Journal on Selected Areas in Communications 35 (7) (2017) 1591–1605. doi:10.1109/JSAC.2017.2699381.

[247] Semtech Corporation, LoRa Family, Wireless & RF ICs for ISM Band Application, http://www.semtech.com/wireless-rf/lora.html, accessed 15 Dec. 2017 (2017).

[248] LoRa Alliance, LoRa Alliance, About the Alliance, https://www.lora-alliance.org/about-the-alliance, accessed 15 Dec. 2017 (2017).

[249] A. Augustin, J. Yi, T. Clausen, W. M. Townsley, A Study of LoRa: Long Range & Low Power Networks for the Internet of Things, Sensors 16 (9) (2016) 1466.

[250] L. Casals, B. Mir, R. Vidal, C. Gomez, Modeling the Energy Performance of LoRaWAN, Sensors 17 (10). doi:10.3390/s17102364.
URL http://www.mdpi.com/1424-8220/17/10/2364

[251] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, T. Watteyne, Understanding the Limits of LoRaWAN, IEEE Communications Magazine 55 (9) (2017) 34–40. doi:10.1109/MCOM.2017.1600613.

[252] C. H. Liao, G. Zhu, D. Kuwabara, M. Suzuki, H. Morikawa, Multi-Hop LoRa Networks Enabled by Concurrent Transmission, IEEE Access 5 (2017) 21430–21446. doi:10.1109/ACCESS.2017.2755858.

[253] F. V. den Abeele, J. Haxhibeqiri, I. Moerman, J. Hoebeke, Scalability Analysis of Large-Scale LoRaWAN Networks in ns-3, IEEE Internet of Things Journal 4 (6) (2017) 2186–2198. doi:10.1109/JIOT.2017.2768498.

[254] M. Rizzi, P. Ferrari, A. Flammini, E. Sisinni, Evaluation of the IoT LoRaWAN Solution for Distributed Measurement Applications, IEEE Transactions on Instrumentation and Measurement 66 (12) (2017) 3340–3349. doi:10.1109/TIM.2017.2746378.

[255] P. Fedchenkov, A. Zaslavsky, A. Medvedev, T. Anagnostopoulos, I. Sosunova, O. Sadov, Supporting Data Communications in IoT-Enabled Waste Management, Springer International Publishing, Cham, 2017, pp. 163–174. doi:10.1007/978-3-319-67380-6_15.
URL https://doi.org/10.1007/978-3-319-67380-6_15

[256] A. Augustin, J. Yi, T. Clausen, W. M. Townsley, A Study of LoRa: Long Range & Low Power Networks for the Internet of Things, Sensors 16 (9). doi:10.3390/s16091466.
URL http://www.mdpi.com/1424-8220/16/9/1466

[257] W. Yang, M. Wang, J. Zhang, J. Zou, M. Hua, T. Xia, X. You, Narrowband Wireless Access for Low-Power Massive Internet of Things: A Bandwidth Perspective, IEEE Wireless Communications 24 (3) (2017) 138–145. doi:10.1109/MWC.2017.1600298.

[258] É. Morin, M. Maman, R. Guizzetti, A. Duda, Comparison of the Device Lifetime in Wireless Networks for the Internet of Things, IEEE Access 5 (2017) 7097–7114. doi:10.1109/ACCESS.2017.2688279.

[259] R. Sanchez-Iborra, M.-D. Cano, State of the Art in LP-WAN Solutions for Industrial IoT Services, Sensors 16 (5). doi:10.3390/s16050708.
URL http://www.mdpi.com/1424-8220/16/5/708

[260] Sigfox Corporation, Sigfox Geolocation, https://www.sigfox.com/en/sigfox-geolocation, accessed 16 Dec. 2017 (2017).

[261] S. Rajagopal, R. D. Roberts, S. K. Lim, IEEE 802.15.7 Visible Light Communication: Modulation Schemes and Dimming Support, IEEE Communications Magazine 50 (3) (2012) 72–82. doi:10.1109/MCOM.2012.6163585.

[262] F. Zafar, D. Karunatilaka, R. Parthiban, Dimming Schemes for Visible Light Communication: The State of Research, IEEE Wireless Communications 22 (2) (2015) 29–35. doi:10.1109/MWC.2015.7096282.

[263] S. H. Lee, S. Y. Jung, J. K. Kwon, Modulation and Coding for Dimmable Visible Light Communication, IEEE Communications Magazine 53 (2) (2015) 136–143. doi:10.1109/MCOM.2015.7045402.

[264] A. C. Boucouvalas, P. Chatzimisios, Z. Ghassemlooy, M. Uysal, K. Yiannopoulos, Standards for Indoor Optical Wireless Communications, IEEE Communications Magazine 53 (3) (2015) 24–31. doi:10.1109/MCOM.2015.7060515.

[265] G. Corbellini, K. Aksit, S. Schmid, S. Mangold, T. R. Gross, Connecting Networks of Toys and Smartphones with Visible Light Communication, IEEE Communications Magazine 52 (7) (2014) 72–78. doi:10.1109/MCOM.2014.6852086.

[266] S. Shao, A. Khreishah, H. Elgala, Pixelated VLC-Backscattering for Self-Charging Indoor IoT Devices, IEEE Photonics Technology Letters 29 (2) (2017) 177–180. doi:10.1109/LPT.2016.2631946.

[267] T. Li, C. An, Z. Tian, A. T. Campbell, X. Zhou, Human Sensing Using Visible Light Communication, in: Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, MobiCom '15, ACM, New York, NY, USA, 2015, pp. 331–344. doi:10.1145/2789168.2790110.
URL http://doi.acm.org/10.1145/2789168.2790110

[268] J.-H. Yoo, J.-S. Jang, J. K. Kwon, H.-C. Kim, D.-W. Song, S.-Y. Jung, Demonstration of Vehicular Visible Light Communication based on LED Headlamp, International Journal of Automotive Technology 17 (2) (2016) 347–352. doi:10.1007/s12239-016-0035-8.
URL https://doi.org/10.1007/s12239-016-0035-8

[269] V. P. Rachim, Y. Jiang, H.-S. Lee, W.-Y. Chung, Demonstration of Long-Distance Hazard-Free Wearable EEG Monitoring System using Mobile Phone Visible Light Communication, Opt. Express 25 (2) (2017) 713–719. doi:10.1364/OE.25.000713.
URL http://www.opticsexpress.org/abstract.cfm?URI=oe-25-2-713

[270] A. Tsiatmas, C. P. M. J. Baggen, F. M. J. Willems, J. P. M. G. Linnartz, J. W. M. Bergmans, An Illumination Perspective on Visible Light Communications, IEEE Communications Magazine 52 (7) (2014) 64–71. doi:10.1109/MCOM.2014.6852085.

[271] C. Ley-Bosch, I. Alonso-Gonzlez, D. Snchez-Rodrguez, C. Ramrez-Casaas, Evaluation of the Effects of Hidden Node Problems in IEEE 802.15.7 Uplink Performance, Sensors 16 (2). doi:10.3390/s16020216.
URL http://www.mdpi.com/1424-8220/16/2/216

[272] Y. Jiang, Y. Wang, P. Cao, M. Safari, J. Thompson, H. Haas, Robust and Low-Complexity Timing Synchronization for DCO-OFDM LiFi Systems, IEEE Journal on Selected Areas in Communications 36 (1) (2018) 53–65. doi:10.1109/JSAC.2017.2774419.

[273] M. Ayyash, H. Elgala, A. Khreishah, V. Jungnickel, T. Little, S. Shao, M. Rahaim, D. Schulz, J. Hilt, R. Freund, Co-

ACCEPTED MANUSCRIPT

existence of WiFi and LiFi toward 5G: Concepts, Opportunities, and Challenges, IEEE Communications Magazine 54 (2) (2016) 64–71. doi:10.1109/MCOM.2016.7402263.

[274] A. Pittolo, M. D. Piante, F. Versolatto, A. M. Tonello, In-Vehicle Power Line Communication: Differences and Similarities Among the In-Car and the In-Ship Scenarios, IEEE Vehicular Technology Magazine 11 (2) (2016) 43–51. doi:10.1109/MVT.2015.2480098.

[275] C. Cano, A. Pittolo, D. Malone, L. Lampe, A. M. Tonello, A. G. Dabak, State of the Art in Power Line Communications: From the Applications to the Medium, IEEE Journal on Selected Areas in Communications 34 (7) (2016) 1935–1952. doi:10.1109/JSAC.2016.2566018.

[276] IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications, IEEE Std 1901-2010 (2010) 1–1586doi:10.1109/IEEESTD.2010.5678772.

[277] S. Goldfisher, S. Tanabe, IEEE 1901 Access System: An Overview of Its Uniqueness and Motivation, IEEE Communications Magazine 48 (10) (2010) 150–157. doi:10.1109/MCOM.2010.5594690.

[278] B. Masood, S. Baig, Standardization and Deployment Scenario of Next Generation NB-PLC Technologies, Renewable and Sustainable Energy Reviews 65 (Supplement C) (2016) 1033 – 1047. doi:https://doi.org/10.1016/j.rser.2016.07.060.
URL http://www.sciencedirect.com/science/article/pii/S1364032116303884

[279] IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications, IEEE Std 1901.2-2013 (2013) 1–269doi:10.1109/IEEESTD.2013.6679210.

[280] S. Galli, T. Lys, Next Generation Narrowband (under 500 kHz) Power Line Communications (PLC) Standards, China Communications 12 (3) (2015) 1–8. doi:10.1109/CC.2015.7084358.

[281] M. M. Rahman, C. S. Hong, S. Lee, J. Lee, M. A. Razzaque, J. H. Kim, Medium Access Control for Power Line Communications: An Overview of the IEEE 1901 and ITU-T G.hn Standards, IEEE Communications Magazine 49 (6) (2011) 183–191. doi:10.1109/MCOM.2011.5784004.

[282] C. Vlachou, A. Banchs, P. Salvador, J. Herzen, P. Thiran, Analysis and Enhancement of CSMA/CA With Deferral in Power-Line Communications, IEEE Journal on Selected Areas in Communications 34 (7) (2016) 1978–1991. doi:10.1109/JSAC.2016.2566078.

[283] Z-Wave: Safer Smarter Homes Start With Z-Wave, http://www.z-wave.com/, accessed 18 Dec. 2017 (2017).

[284] J. D. Fuller, B. W. Ramsey, Rogue Z-Wave Controllers: A Persistent Attack Channel, in: 2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops), 2015, pp. 734–741. doi:10.1109/LCNW.2015.7365922.

[285] C. W. Badenhop, S. R. Graham, B. W. Ramsey, B. E. Mullins, L. O. Mailloux, The Z-Wave Routing Protocol and Its Security Implications, Computers & Security 68 (Supplement C) (2017) 112 – 129. doi:https://doi.org/10.1016/j.cose.2017.04.004.
URL http://www.sciencedirect.com/science/article/pii/S0167404817300792

[286] A. K. I. Yasari, L. A. Latiff, R. A. Dziyauddin, M. A. Lilo, Y. Aljeroudi, H. A. Atee, Flexible Online Multi-Objective Optimization Framework for ISA100.11a Standard in Beacon-Enabled CSMA/CA Mode, Computers & Electrical Engineering 64 (Supplement C) (2017) 537 – 551. doi:https://doi.org/10.1016/j.compeleceng.2017.02.024.
URL http://www.sciencedirect.com/science/article/pii/S0045790617304007

[287] W. Liang, X. Zhang, Y. Xiao, F. Wang, P. Zeng, H. Yu, Survey and Experiments of WIA-PA Specification of Industrial Wireless Network, Wireless Communications and Mobile Computing 11 (8) (2011) 1197–1212.

[288] K. Das, P. Havinga, Evaluation of DECT for Low Latency Real-Time Industrial Control Networks, in: 2013 IEEE International Conference on Sensing, Communications and Networking (SECON), 2013, pp. 10–17. doi:10.1109/SAHCN.2013.6644954.

[289] D. Bodson, Standardization Roadmap for Electric Vehicles [Standards], IEEE Vehicular Technology Magazine 8 (3) (2013) 114–116. doi:10.1109/MVT.2013.2269199.

[290] H. S. Dhillon, H. Huang, H. Viswanathan, Wide-Area Wireless Communication Challenges for the Internet of Things, IEEE Communications Magazine 55 (2) (2017) 168–174. doi:10.1109/MCOM.2017.1500269CM.

[291] M. M. Islam, J. Song, K. Rasilainen, V. Viikari, Optimization of RFID Sensor With Frequency Modulation, IEEE Sensors Journal 16 (15) (2016) 5993–6002. doi:10.1109/JSEN.2016.2577378.

[292] A. Wickramasinghe, D. C. Ranasinghe, Ambulatory Monitoring Using Passive Computational RFID Sensors, IEEE Sensors Journal 15 (10) (2015) 5859–5869. doi:10.1109/JSEN.2015.2449862.

[293] W. Ltd., Weightless-P Standard is Designed for High Performance, Low Power, 2-Way Communication For IoT , http://www.weightless.org/news/weightlessp-standard-is-designed-for-high-performance-low-power-2way-communication-for-iot, accessed 20 Dec. 2017 (2017).

[294] S. Ijaz, M. A. Shah, A. Khan, M. Ahmed, Smart Cities: A Survey on Security Concerns, Int. J. Adv. Comput. Sci. Appl 7 (2016) 612–625.

[295] A. Balte, A. Kashid, B. Patil, Security Issues in Internet of Things (IoT): A Survey, International Journal of Advanced Research in Computer Science and Software Engineering 5 (4).

[296] A. S. Elmaghraby, M. M. Losavio, Cyber Security Challenges in Smart Cities: Safety, Security and Privacy, Journal of advanced research 5 (4) (2014) 491–497.

[297] Y. L. Zhao, Research on Data Security Technology in Internet of Things, in: Applied Mechanics and Materials, Vol. 433, Trans Tech Publ, 2013, pp. 1752–1755.

[298] A. Page, M. Hassanalieragh, T. Soyata, M. K. Aktas, B. Kantarci, S. Andreescu, Conceptualizing a Real-Time Remote Cardiac Health Monitoring System, in: T. Soyata (Ed.), Enabling Real-Time Mobile Cloud Computing through Emerging Technologies, IGI Global, 2015, Ch. 1, pp. 1–34. doi:10.4018/978-1-4666-8662-5.ch001.

[299] T. Soyata, Enabling Real-Time Mobile Cloud Computing through Emerging Technologies, IGI Global, 2015. doi:10.4018/978-1-4666-8662-5.

[300] G. Honan, A. Page, O. Kocabas, T. Soyata, B. Kantarci, Internet-of-Everything Oriented Implementation of Secure Digital Health (D-Health) Systems, in: Proceedings of the 2016 IEEE Symposium on Computers and Communications, Messina, Italy, 2016, pp. 718–725. doi:10.1109/ISCC.2016.7543821.

[301] A. Page, S. Hijazi, D. Askan, B. Kantarci, T. Soyata, Research Directions in Cloud-Based Decision Support Systems for Health Monitoring Using Internet-of-Things Driven Data Acquisition, International Journal of Services Computing 4 (4) (2016) 18–34.

[302] O. Kocabas, T. Soyata, J. Couderc, M. K. Aktas, J. Xia,

ACCEPTED MANUSCRIPT

M. Huang, Assessment of Cloud-based Health Monitoring using Homomorphic Encryption, in: Proceedings of the 31st IEEE International Conference on Computer Design, Ashville, VA, USA, 2013, pp. 443–446. doi:10.1109/ICCD.2013.6657078.

[303] M. Ryan, et al., Bluetooth: With Low Energy Comes Low Security, WOOT 13 (2013) 4–4.

[304] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, R. Kuhn, Learning Internet-of-Things Security "Hands-On", IEEE Security Privacy 14 (1) (2016) 37–46. doi:10.1109/MSP.2016.4.

[305] X. Yang, X. Wang, Y. Wu, L. Qian, W. Lu, H. Zhou, Small-Cell Assisted Secure Traffic Offloading for Narrow-Band Internet of Thing (NB-IoT) Systems, IEEE Internet of Things Journal PP (99) (2017) 1–1. doi:10.1109/JIOT.2017.2779820.

[306] S. Tomasin, S. Zulian, L. Vangelista, Security Analysis of LoRaWAN Join Procedure for Internet of Things Networks, in: 2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2017, pp. 1–6. doi:10.1109/WCNCW.2017.7919091.

[307] O. Kocabas, T. Soyata, M. K. Aktas, Emerging Security Mechanisms for Medical Cyber Physical Systems, IEEE/ACM Transactions on Computational Biology and Bioinformatics 13 (3) (2016) 401–416. doi:10.1109/TCBB.2016.2520933.

[308] Z. Liu, J. Großschädl, Z. Hu, K. Järvinen, H. Wang, I. Verbauwhede, Elliptic Curve Cryptography with Efficiently Computable Endomorphisms and Its Hardware Implementations for the Internet of Things, IEEE Transactions on Computers 66 (5) (2017) 773–785. doi:10.1109/TC.2016.2623609.

[309] S. Tonyali, A. K, N. Saputro, A. S. Uluagac, M. Nojoumian, Privacy-Preserving Protocols for Secure and Reliable Data Aggregation in IoT-Enabled Smart Metering Systems, Future Generation Computer Systems 78 (Part 2) (2018) 547 – 557. doi:https://doi.org/10.1016/j.future.2017.04.031.
URL http://www.sciencedirect.com/science/article/pii/S0167739X17306945

[310] O. Kocabas, T. Soyata, Towards Privacy-Preserving Medical Cloud Computing Using Homomorphic Encryption, in: T. Soyata (Ed.), Enabling Real-Time Mobile Cloud Computing through Emerging Technologies, IGI Global, 2015, Ch. 7, pp. 213–246. doi:10.4018/978-1-4666-8662-5.ch007.

[311] O. Kocabas, T. Soyata, Utilizing Homomorphic Encryption to Implement Secure and Private Medical Cloud Computing, in: IEEE 8th International Conference on Cloud Computing, New York, NY, 2015, pp. 540–547. doi:10.1109/CLOUD.2015.78.

[312] O. Arias, J. Wurm, K. Hoang, Y. Jin, Privacy and Security in Internet of Things and Wearable Devices, IEEE Transactions on Multi-Scale Computing Systems 1 (2) (2015) 99–109. doi:10.1109/TMSCS.2015.2498605.

[313] J. Zhou, Z. Cao, X. Dong, A. V. Vasilakos, Security and Privacy for Cloud-Based IoT: Challenges, IEEE Communications Magazine 55 (1) (2017) 26–33. doi:10.1109/MCOM.2017.1600363CM.

[314] J. Krimmling, S. Peter, Integration and Evaluation of Intrusion Detection for CoAP in Smart City Applications, in: Communications and Network Security (CNS), 2014 IEEE Conference on, IEEE, 2014, pp. 73–78.

[315] H. Suo, J. Wan, C. Zou, J. Liu, Security in the Internet of Things: A Review, in: Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on, Vol. 3, IEEE, 2012, pp. 648–651.

[316] M. J. Covington, R. Carskadden, Threat Implications of the Internet of Things, in: Cyber Conflict (CyCon), 2013 5th International Conference on, IEEE, 2013, pp. 1–12.

[317] N. Ye, Y. Zhu, R.-c. Wang, R. Malekian, L. Qiao-min, An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things, Applied Mathematics & Information Sciences 8 (4) (2014) 1617.

[318] D. Puthal, S. Nepal, R. Ranjan, J. Chen, Threats to Networking Cloud and Edge Datacenters in the Internet of Things, IEEE Cloud Computing 3 (3) (2016) 64–71.

[319] C. Liu, J. Yang, Y. Zhang, R. Chen, J. Zeng, Research on Immunity-Based Intrusion Detection Technology for the Internet of Things, in: Natural Computation (ICNC), 2011 Seventh International Conference on, Vol. 1, IEEE, 2011, pp. 212–216.

[320] S. Raza, L. Wallgren, T. Voigt, SVELTE: Real-Time Intrusion Detection in the Internet of Things, Ad hoc networks 11 (8) (2013) 2661–2674.

[321] N. Kushalnagar, G. Montenegro, C. Schumacher, IPv6 Over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals, Tech. rep. (2007).

[322] B. Kantarci, M. Erol-Kantarci, S. Schuckers, Towards Secure Cloud-Centric Internet of Biometric Things, in: 2015 IEEE 4th International Conference on Cloud Networking (CloudNet), 2015, pp. 81–83. doi:10.1109/CloudNet.2015.7335286.

[323] F. Anjomshoa, M. Aloqaily, B. Kantarci, M. Erol-Kantarci, S. Schuckers, Social Behaviometrics for Personalized Devices in the Internet of Things Era, IEEE Access.

[324] H. Gascon, S. Uellenbeck, C. Wolf, K. Rieck, Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior., in: Sicherheit, Citeseer, 2014, pp. 1–12.

[325] H. Khan, A. Atwater, U. Hengartner, Itus: An Implicit Authentication Framework for Android, in: Proceedings of the 20th annual international conference on Mobile computing and networking, ACM, 2014, pp. 507–518.

[326] H. Khan, U. Hengartner, Towards Application-Centric Implicit Authentication on Smartphones, in: Proceedings of the 15th Workshop on Mobile Computing Systems and Applications, ACM, 2014, p. 10.

[327] A. D. Luca, A. Hang, F. Brudy, C. Lindner, H. Hussmann, Touch Me Once and I Know It's You!: Implicit Authentication Based on Touch Screen Patterns, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2012, pp. 987–996.

[328] T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunar, Y. Jiang, N. Nguyen, Continuous Mobile Authentication using Touchscreen Gestures, in: Homeland Security (HST), 2012 IEEE Conference on Technologies for, IEEE, 2012, pp. 451–456.

[329] A. B. Budurusubmi, S. S. Yau, An Effective Approach to Continuous User Authentication for Touch Screen Smart Devices, in: IEEE International Conference on Software Quality, Reliability and Security (QRS), 2015, pp. 219–226.

[330] C. Ziegler, Implicit Authentication 2.0: Behavioural Biometrics in Smart Environments, in: E. von Zezschwitz et al. (Ed.), Human Computer Interaction in the Internet of Things Era, University of Munich, 2015, pp. 100–107.

[331] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, H.-W. Gellersen, Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts, in: international conference on Ubiquitous Computing, Springer, 2001, pp. 116–122.

[332] L. Ding, P. Shi, B. Liu, The Clustering of Internet, Internet of Things and Social Network, in: Knowledge Acquisition and Modeling (KAM), 2010 3rd International Symposium on, IEEE, 2010, pp. 417–420.

[333] J. An, X. Gui, W. Zhang, J. Jiang, Nodes Social Relations Cognition for Mobility-Aware in the Internet of Things, in: Inter-

ACCEPTED MANUSCRIPT

ACCEPTED MANUSCRIPT

national Conference on Internet of Things (iThings/CPSCom), 4th International Conference on Cyber, Physical and Social Computing, IEEE, 2011, pp. 687–691.

[334] M. Sultana, P. P. Paul, M. Gavrilova, A Concept of Social Behavioral Biometrics: Motivation, Current Developments, and Future Trends, in: International Conf. on Cyberworlds, IEEE, 2014, pp. 271–278.

[335] A. S. Crandall, D. J. Cook, Behaviometrics for Identifying Smart Home Residents, in: Human Aspects in Ambient Intelligence, Springer, 2013, pp. 55–71.

[336] M. Batty, K. W. Axhausen, F. Giannotti, A. Pozdnoukhov, A. Bazzani, M. Wachowicz, G. Ouzounis, Y. Portugali, Smart Cities of the Future, The European Physical Journal Special Topics 214 (1) (2012) 481–518.

[337] R. Khatoun, S. Zeadally, Smart Cities: Concepts, Architectures, Research Opportunities, Communications of the ACM 59 (8) (2016) 46–57.

[338] H. Zhang, M. Li, Security Vulnerabilities of an Remote Password Authentication Scheme with Smart Card, in: Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on, IEEE, 2011, pp. 698–701.

[339] W. Meng, D. S. Wong, S. Furnell, J. Zhou, Surveying the Development of Biometric User Authentication on Mobile Phones, IEEE Communications Surveys & Tutorials 17 (3) (2015) 1268–1293.

[340] A. Dantcheva, P. Elia, A. Ross, What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics, IEEE Transactions on Information Forensics and Security 11 (3) (2016) 441–467.

[341] A. Poursaberi, J. Vana, S. Mracek, R. Dvora, S. N. Yanushkevich, M. Drahansky, V. P. Shmerko, M. L. Gavrilova, Facial Biometrics for Situational Awareness Systems, IET biometrics 2 (2) (2013) 35–47.

[342] J. Liu-Jimenez, R. Sanchez-Reillo, B. Fernandez-Saavedra, Iris Biometrics for Embedded Systems, IEEE transactions on very large scale integration (vlsi) systems 19 (2) (2011) 274–282.

[343] W. Lu, Y. Gong, X. Liu, J. Wu, H. Peng, Collaborative Energy and Information Transfer in Green Wireless Sensor Networks for Smart Cities, IEEE Transactions on Industrial Informatics PP (99) (2017) 1–1. doi:10.1109/TII.2017.2777846.

[344] J. Liu, K. Xiong, P. Fan, Z. Zhong, RF Energy Harvesting Wireless Powered Sensor Networks for Smart Cities, IEEE Access 5 (2017) 9348–9358. doi:10.1109/ACCESS.2017.2703847.

[345] C. Fiandrino, A. Capponi, G. Cacciatore, D. Kliazovich, U. Sorger, P. Bouvry, B. Kantarci, F. Granelli, S. Giordano, Crowdsensim: a simulation platform for mobile crowdsensing in realistic urban environments, IEEE Access 5 (2017) 3490–3503.

[346] C. T. Neil, M. Shafi, P. J. Smith, P. A. Dmochowski, J. Zhang, Impact of Microwave and mmWave Channel Models on 5G Systems Performance, IEEE Transactions on Antennas and Propagation 65 (12) (2017) 6505–6520. doi:10.1109/TAP.2017.2759958.

[347] T. S. Rappaport, Y. Xing, G. R. MacCartney, A. F. Molisch, E. Mellios, J. Zhang, Overview of Millimeter Wave Communications for Fifth-Generation (5G) Wireless Networks-With a Focus on Propagation Models, IEEE Transactions on Antennas and Propagation 65 (12) (2017) 6213–6230. doi:10.1109/TAP.2017.2734243.

[348] J. P. Benson, T. O'Donovan, P. O'Sullivan, U. Roedig, C. Sreenan, J. Barton, A. Murphy, B. O'Flynn, Car-Park Management using Wireless Sensor Networks (Nov 2006).

[349] P. McDaniel, S. McLaughlin, Security and Privacy Challenges in the Smart Grid, IEEE Security & Privacy 7 (3).

ACCEPTED MANUSCRIPT

ACCEPTED MANUSCRIPT

Hadi Habibzadeh received his B.S. in Computer Engineering from Isfahan University of Technology in Iran in 2015 and his M.S. degree in Technical Entrepreneurship and Management (TEM) from University of Rochester, USA in 2016. He is currently pursing his PhD degree in the Electrical and Computer Engineering department of University at Albany, State University of New York (SUNY Albany), under the supervision of Dr. Tolga Soyata. His current research interests include Cyber Physical systems and embedded systems with applications in Internet of Things and Smart Cities.

Tolga Soyata received his B.S. degree in Electrical and Communications Engineering from Istanbul Technical University in 1988, M.S. degree in Electrical and Computer Engineering from Johns Hopkins University in 1992 and Ph.D. in Electrical and Computer Engineering from University of Rochester in 2000. He joined the University of Rochester ECE Department in 2008. He was an Assistant Professor – Research at UR ECE when he left to join SUNY Albany, Department of ECE as an Associate Professor in 2016. His teaching interests include CMOS VLSI ASIC Design, FPGA-based High Performance Data Processing System Design, and GPU Parallel Programming. His research interests include Cyber Physical Systems, Digital Health, and GPU-based high-performance computing. He is the author of the book "GPU Parallel Program Development Using CUDA." He is a senior member of both IEEE and ACM.

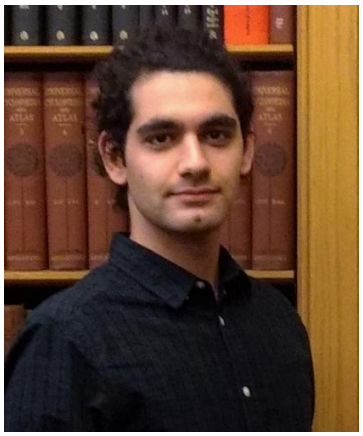
Burak Kantarci is an Assistant Professor with the School of Electrical Engineering and Computer Science at the University of Ottawa. From 2014 to 2016, he was an assistant professor at the ECE Department at Clarkson University, where he currently holds a courtesy appointment. Dr. Kantarci received the M.Sc. and Ph.D. degrees in computer engineering from Istanbul Technical University, in 2005 and 2009, respectively. He received the Siemens Excellence Award in 2005 for his studies in optical burst switching. During his Ph.D. study, he studied as a Visiting Scholar with the University of Ottawa, where he completed the major content of his thesis. He has co-authored over 130 papers in established journals and conferences, and contributed to 11 book chapters. He is the Co-Editor of the book entitled Communication Infrastructures for Cloud Computing. He has served as the Technical Program Co-Chair of seven international conferences/symposia/workshops. He is an Editor of the IEEE Communications Surveys and Tutorials. He also serves as the Vice-Chair of the IEEE ComSoc Communication Systems Integration and Modeling Technical Committee. He is a member of the ACM and a senior member of the IEEE.

Azzedine Boukerche is a full professor and holds a Canada Research Chair Tier-1 position with the University of Ottawa. He is founding director of the PARADISE Research Laboratory and the DIVA Strategic Research Centre, University of Ottawa. He has received the C. Gotlieb Computer Medal Award, Ontario Distinguished Researcher Award, Premier of Ontario Research Excellence Award, G. S. Glinski Award for Excellence in Research, IEEE Computer Society Golden Core Award, IEEE CS-Meritorious Award, IEEE TCPP Leaderships Award, IEEE ComSoc ASHN Leaderships and Contribution Award, and University of Ottawa Award for Excellence in Research. He serves as an associate editor for several IEEE transactions and ACM journals, and is also a Steering Committee Chair for several IEEE and ACM international conferences. His current research interests include wireless ad hoc and sensor networks, wireless networking and mobile computing, wireless multimedia, QoS service provisioning, performance evaluation and modeling of large-scale distributed and mobile systems, and large scale distributed and parallel discrete event simulation. He has published extensively in these areas and received several best research paper awards for his work. He is a fellow of the Engineering Institute of Canada, the Canadian Academy of Engineering, the American Association for the Advancement of Science, and the IEEE.

Cem Kaptan received his B.S. in Computer Engineering from Marmara University in Turkey in 2015. He worked as a software engineer at Accenture prior to starting his graduate studies. He is currently working towards his MSc degree in Computer Science at the University of Ottawa under the supervision of Dr. Kantarci and Dr. Boukerche. His areas of research are smart transportation, machine learning, smart environments and large-scale sensing systems.

ACCEPTED MANUSCRIPT

Author Photo



Hadi Habibzadeh

Tolga Soyata

Burak Kantarci

ACCEPTED MANUSCRIPT

Azzedine Boukerche

Cem Kaptan

ACCEPTED MANUSCRIPT