Journal of Internet Services and Applications

RESEARCH Open Access

Networking architectures and protocols for smart city systems

Imad Jawhar[1*], Nader Mohamed[2] and Jameela Al-Jaroodi[3]

Abstract

The smart city model is used by many organizations for large cities around the world to significantly enhance and improve the quality of life of the inhabitants, improve the utilization of city resources, and reduce operational costs. This model includes various heterogeneous technologies such as Cyber-Physical Systems (CPS), Internet of Things (IoT), Wireless Sensor Networks (WSNs), Cloud Computing, and Unmanned Aerial Vehicles (UAVs). However, in order to reach these important objectives, efficient networking and communication protocols are needed to provide the necessary coordination and control of the various system components. In this paper, we identify the networking characteristics and requirements of smart city applications, and identify the networking protocols that can be used to support the various data traffic flows that are needed between the different components. In addition, we provide illustrations of networking architectures of selected smart city systems, which include smart grid, smart home energy management, smart water, UAV and commercial aircraft safety, and pipeline monitoring and control systems.

Keywords: Smart city, Cyber-physical systems (CPS), Networking architectures, Unmanned aerial vehicle (UAV), Wireless sensor networks (WSNs)

1 Introduction

A number of large cities around the world are investigating applying the smart city model to heighten the living quality of their inhabitants and enhance the utilization of the city infrastructure and resource s. Various advanced technologies and techniques supporting such models provide smart services to improve the performance and operations in healthcare, transportation, energy, education, and many other fields. At the same time these services reduce operational costs and resource consumption in smart cities. Examples of these technologies are Wireless Sensor Networks (WSNs), the Internet of Things (IoT), Cyber-Physical Systems (CPS), robotics, Unmanned Aerial Vehicles (UAVs), fog computing, cloud computing, and big data analytics. Utilizing these technologies provides many advantages and services for smart cities. WSNs are used to provide real-time monitoring of the conditions of smart city resources, and infrastructures [1]. The IoT facilitates the integration of the physical objects in a city network [2]. CPS are used to provide useful interactions between the cyber world and the physical world in smart cities [3]. Robotics and UAVs are used to provide automation and offer useful services for smart cities [4]. Such services include enhancement delivery of services, environmental monitoring, traffic monitoring, security and safety controls, and telecommunication services [5]. Fog computing is used to provide low latency support, location awareness, better mobility support, and streaming and real-time support for smart city applications [6]. Cloud computing provides a scalable and cost effective computation and data storage platform to support smart city applications [7]. Big data analytics is used to provide intelligent and optimized short and long term decisions based on collected data to enhance smart city services [8].

These advanced technologies are used to implement a number of smart city services [9–11]. Examples of these smart services are intelligent transportation services that can be used to enhance route planning and congestion avoidance in city streets, provide intelligent traffic light controls and parking services, enhance vehicular safety, and enable self-driving cars. Other examples are smart energy services that provide better energy decisions for more efficient energy consumption in smart cities.

*Correspondence: ihjawhar@gmail.com; imad.jawhar@mu.edu.lb
[1]Al Maaref University, Old Airport Avenue, P.O. Box 25-5078, Beirut, Lebanon
Full list of author information is available at the end of the article

Applications of these smart energy services are used to support smart grids, and smart buildings, as well as provide better utilization of renewable energy. Other smart services involve structural health monitoring as well as real-time monitoring of water networks, bridges, tunnels, train and subway rails, and oil and gas pipelines. Additional services include smart services for environmental monitoring and smart services for public safety and security.

These smart city services do not only need the various advanced technologies discussed here, but also need reliable and robust networking and communication infrastructures to enable efficient exchange of messages among the different components of the systems that provide a particular service. Smart city services are designed at different scales, which require various networking and communication technologies for their implementation and operations. Furthermore, different network and communication models and approaches can be utilized for smart city services. This paper investigates the communication and network issues of smart city systems. It also investigates networking technologies, architectures, and communication requirements for such systems. The suitability of existing network protocols for different smart city services will be discussed. Although there are significant research efforts to investigate different issues in smart cities and provide solutions for these issues, very little research has been done to investigate the networking and communication parts of smart city systems, which constitute the main objective of this paper.

The rest of the paper is organized as follows. Section 2 provides an overview of related work in this field. Section 3 includes an overview of some smart city applications. Section 4 presents networking architectures and communication requirements for smart city applications. Section 5 offers an illustration of selected smart city systems. Section 6 discusses open issues in the area of networking and communication for smart city systems. Finally, Section 7 concludes the paper and provides some future research directions.

2 Related work

There are a few papers published addressing the network and communication issues for smart cities. In this section we discuss some of the work presented in these papers. Zanella et al. [2] provided an interesting study that analyzed the current technologies available for deploying IoT for a smart city. In addition, the authors presented and discussed a proof-of-concept implementation of IoT in the city of Padova, Italy. There are generally two common approaches to offer data access to things in IoT. The first is using multi-hop mesh networks with short-range communication in the unlicensed spectrum among the network nodes. The second is using long-range cellular technologies in the licensed frequency band. A new communication technology is introduced to provide alternative connectivity for IoT named LPWAN (Low-Power Wide Area Network) [12]. From its name, this communication technology can provide low-rate, long-range transmission in the unlicensed frequency bands using star topology. These features can be very useful for some smart city applications. Leccese et al. [13] introduced a smart city application of fully controlled street lighting using a ZigBee Sensor Network and WiMAX while the application is controlled by Raspberry-Pi Card. Sanchez et al. [14] introduced a smart city testbed for IoT experimentation named SmartSantander.

Some work more related to our contribution in this paper is investigating network architectures for smart cities. Wan et al. [15] presented an event-based communication architecture that helps manage and facilitates cooperation among Machine to machine (M2M) components in smart cities. The authors also conducted a case study using this architecture for vehicular applications. Gaur et al. [16] proposed a multi-level smart city architecture based on semantic web technologies. This architecture is mainly for wireless sensor networks applications in a smart city. It consists of 4 levels: Data Collection, Data Processing, Integration and Reasoning, and Device Control and Alerts. Jin et al. [17] studied distinct IoT network architectures with focus on Quality of Service (QoS) for different smart city applications.

The last paper [17] is the closest to our contributions in the paper, thus we will elaborate on it. The authors presented five different IoT network architectures: (1) Autonomous Network Architecture, (2) Ubiquitous Network Architecture, (3) Application-Layer Overlay Network Architecture, (4) Service-Oriented Architecture, and (5) Participatory Sensing. The autonomous network architecture is usually not directly linked to public networks such as the Internet. It can be connected though gateways if this link is needed. This network architecture is suitable for some smart city applications such as automatic parking management in which most of the network connections are mainly to support the application. The QoS requirements in this network architecture are mainly dependent on the requirements of the application.

In the ubiquitous network architecture, smart objects including the sensors and actuators are part of the Internet. Information from these smart objects can be obtained by authorized users and applications through the Internet directly or through intermediate servers which serve as sinks that gather data from the connected smart objects. The servers' option can provide better scalability and resource efficiency than the direct access option. The smart objects can be connected to the Internet through multitier and multiradio. This network architecture is suitable for smart city applications such as structure

health monitoring in which multiple software applications can collect and analyze different structures' health in a city. The QoS of such network architecture can be challenging due to the level of heterogenous network components used. The application layer overlay network architecture is suitable for large scale networks with a large number of distributed nodes. These nodes can be logically structured in clusters with cluster heads that can run in-network data processing task to reduce network traffics. In this network architecture ad hoc and/or mesh are used. One application of this network architecture is using a wireless sensor network (WSN) for environmental monitoring. The QoS for applications suitable for such architecture is generally tolerable to some level. The service-oriented network architecture is based on an innovative network architecture, called Information Driven Architecture (IDRA) [18]. In this architecture different network functions such as addressing, naming, forwarding, and routing are provided as network services. These network services can be utilized to provide different network configurations to suit different applications. Although, this approach can be very useful, flexible and can provide advanced network features, it requires new network components technology. The participatory sensing network architecture is considered a special case and a new model of IoT. In this model, residents through their consumer devices collect, analyze, and share sensor data. This can be called "human-as-a-sensor". In this mode, wireless communications such as WiFi, GPRS, and 3G are used. Some possible applications of this architecture are environmental monitoring, intelligent transportation, and healthcare. QoS in such network can be challenging as humans are the main source of data and humans can be lazy, privacy-worried, error-prone, and misbehaving.

Unlike other related work, our contributions in this paper is mainly in investigating networking architectures focusing on the communication characteristics and requirements of the main smart city applications including smart buildings, smart grids, gas and oil pipeline monitoring and control, smart water network, intelligent transportation, manufacturing control and monitoring, and unmanned aerial vehicle applications for smart cities. The works we studied usually focus on a single attribute or characteristic such as quality of service in [17]. We considered several communication characteristics and requirements including bandwidth, delay tolerance, power consumption, reliability, security, heterogeneous network support, network type, and mobility support. In addition, we studied the suitability of different networking protocols for different smart city applications. These protocols are IEEE 802.15.4 (Zigbee), IEEE 802.15.1 (Bluetooth), IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.16 (WiMAX), Cellular 3G, Cellular 4G/LTE, and Satellite. With this, we are providing a comprehensive study in networking architectures and protocols for smart city systems.

3 Smart city applications

Development and operation of smart city applications can face many challenges. To identify and understand these challenges, we discuss some important smart city applications used or proposed for different domains. We highlight their benefits as well as their development and operational challenges. This will help us identify the type of support needed by the networking platforms designed for smart city applications.

In the energy domain, smart city applications are used to add values such as efficiency, reliability, and sustainability of the production and distribution of electric power in smart grids [19]. A smart grid is a renovated electrical grid system that uses information and communication technology (ICT) to collect and act on available information about the behavior of suppliers and consumers in an automated fashion. A smart grid uses CPS to provide self-monitoring and advanced control mechanisms for power productions and consumer needs to increase grid efficiency and reliability. In addition, CPS systems are used to control the processes of generating renewable energy from hydropower plants [20] and wind power plants [21]. Furthermore, some applications are used to monitor and control energy consumptions in smart buildings [3]. The buildings' equipment such as HVAC (Heating, Ventilating, and Air-Conditioning) systems, appliances, and lighting systems are controlled with CPS. Smart building systems are usually equipped with different types of sensor nodes that monitor the current energy usage and environmental conditions. These sensors report their observations and measurements to a centralized monitoring and control system. The control system implements intelligent algorithms to control the sub-systems used in the buildings to optimize energy usage based on the sensed observations and current operational and environmental conditions.

In the transportation domain, an important smart city application area that recently received high attention is intelligent transportation. Vehicular safety applications constitute one of the most important classes of such applications. There are many safety applications for vehicles including lane change warning messages, emergency breaking, collision avoidance mechanisms, and blind spot monitoring. These applications provide fully automatic or semi-automatic actions to enhance driving safety. The most important features of such applications are the real-time and reliability support in detection and response. All aspects of vehicular safety applications including threat observations, decision making, communication, and actions must be reliable and able to run in real-time. This imposes a serious restriction on how the software

is designed and how well it supports high levels of integration across all the devices involved to ensure real-time and reliable responses. In addition, self-driving cars are considered as important smart city applications [22]. Since they practically integrate all the mentioned features in addition to vision and monitoring components to allow the vehicle to navigate the roads based on sensed data and intelligent software that interprets and responds to this data in real-time. Another intelligent transportation application include intelligent traffic light controls, which include monitoring devices across multiple locations to accurately predict traffic patterns and adjust traffic lights to optimize flow. One example of such domain is discussed in [23].

In addition, smart city systems can be used to protect water networks and to make them smarter, more efficient, more reliable, and more sustainable. CPS systems can be embedded within water networks to provide some monitoring and control mechanisms and to add smart features to the operations of water distribution [24]. One of these functions is to provide early warning mechanisms to identify problems in water networks. For examples, leaks and pipe bursts can be easily detected while fast and temporary solutions can be applied to reduce water waste and to minimize further risks or damages to the network.

Other smart city applications include greenhouse monitoring that aims to provide efficient control for suitable climate, soil, lighting, and water level in greenhouses [25]. In addition, some applications involve autonomous operation of unmanned vehicles using CPS systems. Such systems provide networks that connect the payloads on the unmanned vehicles like sensors, actuators, cameras, storage, communication devices, and microcontrollers [26]. Additional smart city systems are also used to automate, control, monitor, and enhance manufacturing processes [27]. Finally, monitoring and controlling oil, and gas pipelines is another one of the applications for smart cities. We discuss the corresponding architecture and features of this and other important applications in the section illustrating selected smart city systems later in this paper.

4 Smart city networking architectures and communication requirements

In this section, we investigate the different networking and communication requirements of the various smart city applications, as well as the protocols that can be used to connect the components used to support such applications.

4.1 Networking characteristics, requirements, and challenges of smart city systems

Table 1 describes the various smart city applications along with the appropriate networking protocols that can be used, the bandwidth requirements, the delay tolerance, power consumption level, reliability and security requirements, heterogeneity of the networking links, whether they use wired communication, wireless communication, or both, and the mobility characteristics for each of these applications.

4.1.1 Network protocols

As shown in the table, applications with short range communication such as smart buildings, and smart water networks can use protocols from the personal area network (PAN) class such as IEEE 802.15.4 (Zigbee), and 801.15.1 (Bluetooth). These protocols are generally characterized by lower bandwidth, low energy consumption, and short range. Applications requiring longer ranges such as intelligent transportation, and manufacturing and control use protocols, which are in the local area network (LAN) class, such as IEEE 802.11 (WiFi). Applications requiring wide range communication such as UAVs and smart grid can use protocols that are in the wide area network (WAN) class such as IEEE 802.16 (WiMAX), cellular, and satellite. All of these protocols have provisions to support asynchronous and synchronous data connections. The former can be used with smart city applications with best effort traffic, which can tolerate delay, while the latter can be used with applications that generate traffic requiring more stringent quality of service (QoS) requirements such as larger bandwidth and limited delay. Such applications involve real-time and multimedia communication. In addition, these protocols have reliability and security services. However, most of the security features require more processing, and can cause added delay and energy consumption. Consequently, these considerations should be taken into account before enabling such features.

4.1.2 Bandwidth

Also, the table shows that certain applications, such as intelligent transportation, have low bandwidth requirements. Others, such as smart buildings, gas and oil pipeline monitoring, and UAVs require more bandwidth. However, even inside the same type of applications, the bandwidth requirements can range from low to medium or even high, depending on the type of data that is generated. For example, telemetric and control data such as UAV ground-to-air control commands only require small bandwidth, while UAVs taking images and videos, and transmitting them to ground base units require considerably larger bandwidth.

4.1.3 Delay tolerance

In addition, it is shown that some applications have low tolerance for end-to-end delay. Such applications include intelligent transportation. This is the case, since

Table 1 Networking characteristics and requirements of smart city applications

Smart city application	Appropriate Net. Prot.	Band- width	Delay tolerance	Power Consump.	Reliabil- ity	Security	Het. Net.	Wired / wireless	Mobility
Smart buildings [3]	IEEE 802.15.4, IEEE 802.15.1	L, M, H	L	L, M	M, H	H	H	WD/WL	M
Smart grid [19]	IEEE 802.16 , Cellular	L, M	L, H	M, H	H	H	M, H	WD/WL	L
Gas and oil pipeline monitoring and control [22]	IEEE 802.16 , Cellular	L, M, H	L, H	L	M, H	H	M	WL	L
Smart water networks [24]	IEEE 802.15.4 , IEEE 802.11, IEEE 802.16	L, M	L, H	L	M	H	M	WL	L
Intelligent transportation [54]	IEEE 802.16, IEEE 802.11, IEEE 802.15.4, Cellular	L, M	L, H	L, M	M, H	H	H	WD/WL	H
Manufacturing control and monitoring [27]	IEEE 802.15.4 , IEEE 802.15.1 , IEEE 802.11	L, M	L, H	L, M	M	M	M	WD/WL	M
Unmanned aerial vehicle [5]	IEEE 802.11 , IEEE 802.16, Satellite	L, M, H	L, H	L	M, H	M, H	M	WD/WL	H

IEEE 802.15.1: Bluetooth, IEEE 802.15.4: Zigbee, IEEE 801.11: WiFi, IEEE 802.16: WiMAX, H: High, M: Medium, L: Low. WD: Wired, WL: Wireless

the data that is being transmitted needs to arrive within microseconds in order to allow the control systems to react within an acceptable time frame to avoid car imminent danger or life-threatening collisions. On the other hand, other smart city applications have higher tolerance for delay. These applications include ones that rely on the collection of information and monitoring data for later analysis. Examples of such applications include UAVs taking images for later processing.

4.1.4 Power consumption

Power consumption is also an important requirement for smart city applications. However, as shown in the table, some applications that have local high energy sources such as smart grid systems, can tolerate protocols with higher power consumption levels. Other applications, which have energy sources with limited capacities have medium power requirements. Such applications include intelligent transportation. Other applications have very limited energy sources and require protocols with low or very low energy consumption characteristics. Such applications include gas and oil pipeline monitoring, smart water networks, and UAVs.

4.1.5 Reliability

Reliability is another important parameter in smart city applications, and the table shows that most applications either have medium reliability requirements such as smart water networks, while others have high reliability requirements such as smart grid, and intelligent transportation.

4.1.6 Security

With respect to security, most applications require medium to high security. For example, applications such as manufacturing control and monitoring require medium security, while others such as smart grid have high security requirements due to the sensitivity of the data and criticality of the functions that are performed.

4.1.7 Heterogeneity of network protocols

Most smart city systems include networking protocols, which connect the various components within the system. Examples of such systems include include smart buildings, and intelligent transportation. In such cases, these protocols must be able to co-exist without interfering with each other. In addition, appropriate mapping of the various control information inside the headers at the various layers of the networking stack of the different heterogeneous protocols and networks must be done to ensure seamless and efficient operation.

4.1.8 Wired/wireless connectivity

The table also shows that some smart city applications such as gas and oil pipeline monitoring, and UAVs mostly involve wireless communication. Others, such as smart buildings and intelligent transportation involve both wired as well as wireless communication. In such

cases, communication within a particular physical system can use wired networking (e.g. inside a UAV), while wireless communication can be used to connect the physical system with other similar physical systems, or backbone and infrastructure networks.

4.1.9 Mobility

Finally, mobility is another important characteristic of smart city applications. The table shows that some systems have low or medium mobility such as smart grid, gas and oil pipeline monitoring, and smart water networks. Other systems have high mobility such as intelligent transportation, and UAVs. Consequently, the networking protocols that are used to connect medium to high mobility smart city systems must be robust and adapt well to node mobility without consuming too much bandwidth on control messages and related processing to readjust to changes in the network topology.

4.2 Additional issues and challenges

In addition to the requirements and characterization of the links between nodes in smart city systems, we identify the following additional issues and challenges, which must be considered.

4.2.1 Interoperability

Smart city systems rely on various heterogeneous networking protocols at the physical and data link layers, which use different medium access control (MAC) strategies Interoperability between these protocols is important in order to provide seamless integration of the underlying technologies. The IEEE 1905.1 protocol, which was designed to provide convergent interface between physical/data link layers and the network layer is intended to play such a role for digital home networks [28]. Development of similar protocols to expand the support mechanism for smart city systems is a good area for future research.

4.2.2 Availability

Software and hardware availability are essential components of smart city systems due to the criticality and real-time nature of a lot of the related applications. Software availability can be achieved by ensuring that the various services are available to the corresponding applications. On the other hand, hardware availability is obtained by ensuring that the various devices that are needed to provide networking contestability and efficient performance are readily available anytime and anywhere. One way to accomplish these objectives is through redundancy of both software and hardware components and systems. This was already considered and studied for IoT devices [29, 30]. Furthermore, considerations to attain availability need to be incorporated as a part of the design objectives of networking and communication protocols for smart city systems.

4.2.3 Performance

Performance is always an important consideration for any type of architecture, and this is also the case for smart city systems. In order to achieve this essential objective, more evaluation needs to be done for the various networking protocols at the various layers of the architecture, especially at the data link, network and transport layers. These three layers are critical components in order to support traffic of various QoS requirements. In addition, the middleware layer can be used to provide proper interface and convergence services between these layers and the application layer.

4.2.4 Management

Another important aspect of smart city system networking is management of the thousands or even millions of devices that are involved in many applications. For example, to achieve energy management in smart buildings thousands of sensor and actor devices can be deployed in each building. Efficient protocols are needed to provide effective management of fault, configuration, accounting, performance, and security (FCAPS) aspects of these devices. The Light-weight machine-to-machine (LWM2M) [31] standard is being done by the Open Mobile Alliance to specify the interface between M2M devices and servers. On the other hand, the NETCONF Light protocol [32] is designed by IETF to provide mechanisms to install, manipulate and delete the configuration of network devices. Similar efforts are encouraged for smart city systems in order to offer standard mechanisms and services to efficiently manage and control the communication of devices at the various levels of the architecture.

4.2.5 Scalability

It is important for smart city systems to be able to accommodate new devices without appreciable loss in the quality of the provided services and associated network traffic flows. This can be accomplished through virtualization and extensibility in the platforms and their operations. An extensible IoT architecture was proposed in [33], which consists of three layers: Virtual object, Composite virtual object, and Service layer. The design must have objectives of automation, intelligence, and zero-configuration for objects and related devices in order to achieve scalability and interoperability. More research is desirable in order to extend this strategy to smart city systems.

4.2.6 Big data analytics

Huge amounts of data is collected by smart city systems and the corresponding IoT devices that are spread out over a considerably larger geographic area. Analyzing and extracting useful information from this data can provide

considerable advantages for businesses and government institutions. In addition, communication and collection of a very large number of messages in a timely fashion according to their priority, delay-tolerance, and size is vital to the efficient operation of smart city systems. In order to reduce the amount of exchanged traffic, local processing, compression, and aggregation of the generated messages need to be done at the lower and intermediate levels of the node hierarchy and geographic areas. Consequently, More research is needed to provide proper convergence and mapping of the networking parameters between the various layers of the networking stack at the data-generating nodes (e.g. sensors, IoT devices, etc.), the intermediate routers, processing servers (typically in the cloud), and actor nodes at the other end of the communication cycle.

4.2.7 Cloud computing

Cloud computing is an important component of any smart city as it can provide scalable processing power and data storage for different smart city applications [34]. Cloud computing has powerful processing capabilities, large and scalable data storage, and advanced software services that can be utilized to build different support services to provision diverse smart city applications. Cloud computing can be used as the main control and management platform used to execute smart city applications. Different sensors and actuators of smart city applications can be connected to the city's cloud computing services to collect, process, store the sensors' data and perform management tasks for different smart city applications. As the collected data from a smart city can also become big data as huge amounts of data are collected throughout the city. Cloud computing can provide the necessary powerful platforms for storing and processing this big data to enhance operations and planning.

The communication between city sensors and actuators and cloud computing can involve different communication requirements to smoothly support smart city applications. These requirements should be supported by the network architectures deployed in the smart city. Smart applications rely on the integration between sensors and actuators on one side and the cloud on the other and cannot performed well unless there is a good network that provides good communication services connecting both sides. Another issue that arises when using cloud computing for a smart city is that the cloud services are either offered at a centralized location or across multiple distributed platform in various locations. The distributed cloud computing approach can provide better quality and reliability support for different cloud applications [35]. However, there is usually a need to provide good communication links among the distributed cloud computing facilities available in different places. Another issue arising when using the cloud is the reliability and performance of the networks connecting all components on both sides. With the Internet in the mix, there are problems with delays, lost packets and unstable connections. Careful planning and management of network resources and communication models in addition to the design and architecture of the smart city application is necessary to account for these issues. Yet, there are some unavoidable aspects such as the transmission delays.

4.2.8 Fog computing

While cloud computing can provide many advanced and beneficial services for smart city applications, it cannot provide good provisions for distributed applications that need real-time, mobility, low-latency, data streaming, synchronization, coordination, and interaction support services. This is mainly due to the transmission delays imposed by the large distances to be covered between the smart city censors and devices and the cloud platforms. In addition, it is difficult for cloud computing to manage and deal with a large number of heterogenous sensors, actuators, and other devices distributed over a large-area. Fog computing was lately introduced to offer more localized, low latency, and mobility services. Fog computing allows to move some functionalities from the cloud closer to the devices [36]. This approach aims to enable different IoT applications through distributed fog nodes that provide localized services to support these IoT applications. In a smart city, fog computing can complement cloud computing to support smart city applications [37]. While cloud computing can provide powerful and scalable services for smart city applications, fog computing can provide more localized, fast-response, mobility, and data streaming services for smart city applications. Furthermore, integrating IoT, fog computing, and cloud computing as shown in Fig. 1 can provide a powerful platform to support different smart city applications. Figure 2 shows a hierarchical representation where the IoT devices use a multihop topology to reach the gateway connecting to the fog server. This integrated platform needs good networking and communication support to efficiently handle the communication between all these components. This also includes a good network security support to avoid any threat vulnerability issues in the integration and in supporting smart city applications.

4.3 Links between nodes in smart city systems

Table 2 describes the various networking protocols that can be used in smart city systems [38–40]. The table shows their main characteristics, the physical and data link layer specifications, their data rates, and transmission range.

We can see that the applications requiring short range such as smart buildings, smart grid and smart water, generally can use the IEEE 802.15.4 (Zigbee) protocol, which is a very short range protocol that is mainly designed

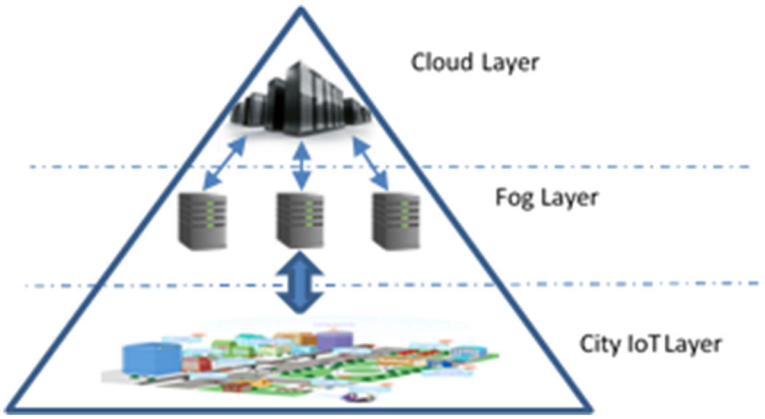

Fig. 1 An Illustration of the integration of IoT, fog computing, and cloud computing to support smart city applications

for very small devices that have very limited energy. It is intended to allow these devices to last up to several years using the same battery. In addition, the IEEE 802.15.1 (Bluetooth) protocol can be used by such applications. It is a WPAN protocol, which uses the 2.4 GHz band. It employs a master/slave time division duplex (TDD) strategy, with a 1 Mbps data rate, and a range of 10 to 100 m.

The IEEE 802.11a/b/g/n protocol can be used with almost all smart city systems. The IEEE 802.11n protocol, which is the later version, works in the 2.4 GHz and 5.1 GHz ranges, uses direct sequence spread spectrum (DSSS) and orthogonal frequency division multiplexing (OFDM). It employs a carrier sense multiple access with collision avoidance (CDMA/CA) MAC strategy. It allows best effort operation using the distributed coordination function (DCF) as well as reservation-based operation using the point coordination function (PCF). The latter service is useful for multimedia audio, video, and real-time data traffic, which require QoS guarantees of certain parameters such as bandwidth, delay and delay jitter. It supports data rates from 15 to 150 Mbps, and has a communication range up to 25 m.

The cellular 3G and 4G protocols can be used with applications such as smart grid, smart water, UAVs and pipeline monitoring. They use packet switching for data communication and optional packet or circuit switching for voice communication. They use frequencies in the 800 MHz to 1900 MHz, 700 MHz, and 2500 MHz ranges. They also use code division multiple access (CDMA) and

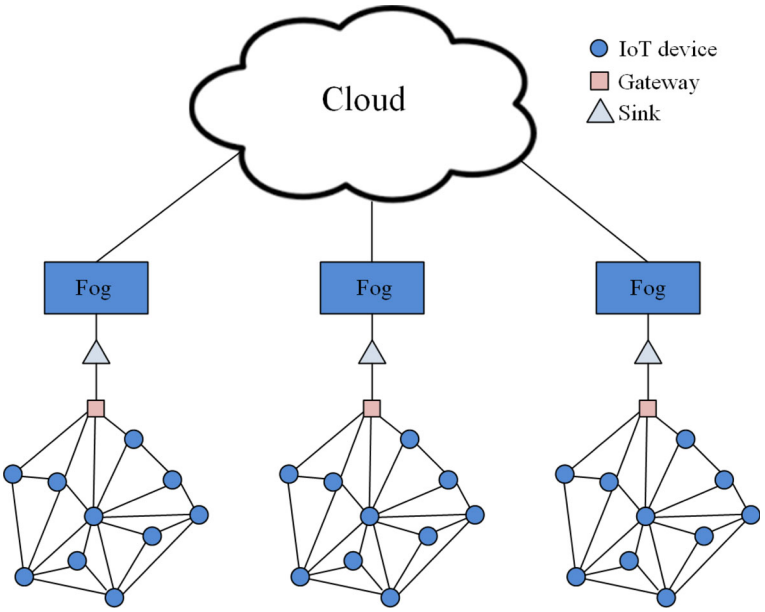

Fig. 2 An hierarchical representation showing the integration of IoT, fog computing, and cloud computing to support smart city applications

Table 2 The various networking protocols that are useful for smart city applications

Protocol	Main characteristics	Physical layer specs	Data link layer specs	Data rate	Transmission range	Smart city application
IEEE 802.15.4 (Zigbee)	Energy saving, very short range	2.4 GHz Band, DSSS	CSMA/CA	20 Kbps to 250 Kbps	10 to 20 m	Smart Buildings, Smart Grid, Smart Water
IEEE 802.15.1 (Bluetooth)	Cable replacement	2.4 GHz Band, FHSS/FSK	Master/Slave, TDD	1 Mbps	10 to 100 m	Smart Buildings, Smart Grid, Smart Water
IEEE 802.11a	Data networking, local area network	5 GHz Band, OFDM	CSMA/CA, DCF/PCF	6, 9, 12, 18, 24, 36, 48, 54 Mbps	120 m outdoors	All
IEEE 802.11b	Data networking, local area network	2.4 GHz Band, DSSS	CSMA/CA, DCF/PCF	1, 2, 5.5, 11 Mbps	140 m outdoors	All
IEEE 802.11g	Data networking, local area network	2.4 GHz Band, DSSS, OFDM	CSMA/CA, DFS/PFS	6, 9, 12, 18, 24, 36, 48, 54 Mbps	140 m outdoors	All
IEEE 802.11n	Data networking, local area network	2.4 GHz and 5 GHz Band, DSSS, OFDM	CSMA/CA, DFS/PFS	15, 30, 45, 60, 90, 120, 135, 150 Mbps	250 m outdoors	All
IEEE 802.16 (WiMAX)	Metropolitan area network	2 to 66 GHz Band, OFDMA	TDD, FDD	2 to 75 Mbps	Up to 35 miles (56 Km)	Smart Grid, Smart Water, UAVs, Pipeline Monitoring
Cellular 3G	Wide area network connectivity. Digital, packet switched for data	800 MHz to 1900 MHz	CDMA, HSDPA	144 Kbps (mobile) to 42 Mbps (stationary)	Depends on cell radius (1 Km to several Km's)	Smart Grid, Smart Water, UAVs, Pipeline Monitoring
Cellular 4G/LTE	Same as 3G	700 MHz to 2500 MHz	LTE and LTE Advanced	300 Mbps to 1 Gbps	Depends on cell radius (1 Km to several Km's)	Smart Grid, Smart Water, UAVs, Pipeline Monitoring
Satellite	Wide area network	1.53 GHz to 31 GHz	FDMA and TDMA	10 Mbps (upload) and 1 Gbps (download)	Satellie can cover 100's of Km's to entire earth	UAVs, Pipeline Monitoring, Intelligent Transportation

high-speed downlink packet access (HSDPA) as well as long term evolution (LTE) advanced technology. The data rates that are supported are 300 Mbps to 1 Gbps. The geographic area that is covered is the entire city or country without roaming, and it has world-wide coverage if roaming is used.

Satellite communication can also be used with applications such as UAVs, pipeline monitoring, and intelligent transportation. They typically use frequencies in the range of 1.53 GHz to 31 GHz. They also employ frequency division multiple access (FDMA) and time division multiple access (TDMA) at the data link layer. The data rate is between 10 Mbps (download) and 1 Gbps (upload). Geographically, satellite communication covers the entire earth since handoff between satellites can be used to achieve such continuous coverage.

5 Illustration of selected smart city systems

In this section, five selected smart city systems are briefly presented in order to illustrate some possible networking and communication models that are used.

5.1 Smart grid system

Figure 3 shows the general architecture of a smart grid system, which is one of the essential applications in a smart city. As shown in the figure, smart grid systems are divided into three categories: (1) generation, (2) transportation, and (3) consumer. In turn, the consumer systems are separated into three sub-categories: (1) commercial, (2) residential, and (3) industrial. Each of these sites usually contains sensing and acting devices that are deployed to monitor and control the different mechanisms and machines that are located on the premises. These devices form nodes in a mobile ad hoc network (MANET) or a wireless sensor and actor network (WSAN). The nodes can communicate using multihop networking protocols specifically designed for MANETs and WSANs [41, 42]. Usually, one (or more) of the nodes plays the role of a gateway and it provides connectivity to the network at that site with the infrastructure LAN or the Internet. Cloud computing platforms can also be used to provide storage, analysis, processing and decision making services to the smart grid network system [43]. In addition, the control center and various users can collect information and issue

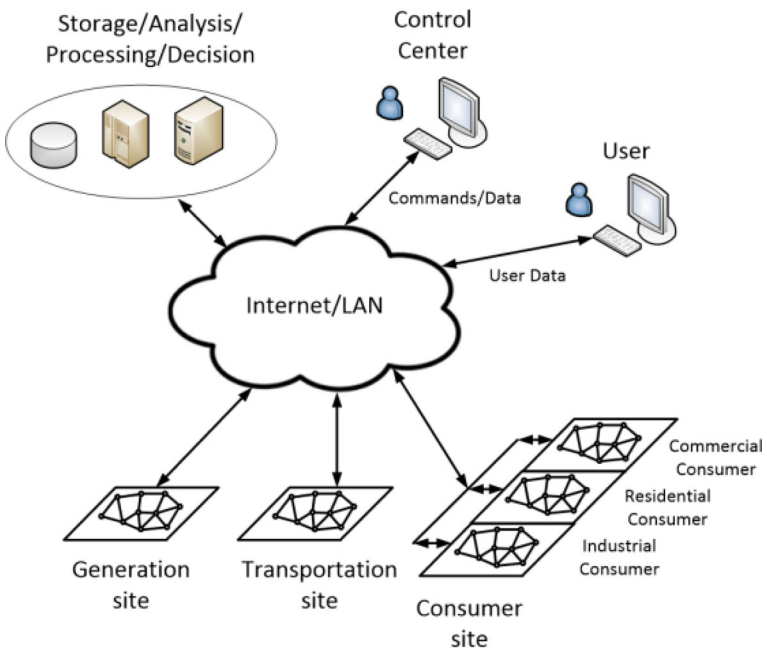

Fig. 3 The general architecture for a smart grid system used in a smart city

requests and commands to provide real-time control of the corresponding systems.

5.2 Smart home energy management

In a typical smart city, the electric company will have different rates for different time periods. Typically these periods would be three: *Peak*, *Mid-Peak*, and *OFF-Peak*. Also, most homes would be equipped with environment-friendly local energy generation sources such as windmills, solar panels, or photovoltaic cells (PVC). In Fig. 4, a general architecture of a smart home energy management system is shown. In this model, when a specific service is requested from a particular appliance (e.g. wash the laundry, run the dishwasher, use a robot to clean the pool, etc.), the energy management unit (EMU) is used to decide which energy source is used to supply the requested power and the time to turn ON the corresponding electric appliance. The user enters the requested task (or service) to be carried out by a particular appliance along with a deadline (or an amount of acceptable delay) by which the task needs to be accomplished. This allows the EMU to calculate the amount of maximum delay that can be tolerated for the performance of the task. Then it performs an algorithm, which determines the source of the energy and the time for executing the desired task by the indicated appliance. The algorithm consists of the following logic. If the amount of energy that is needed by the task is available in the locally generated/stored energy, then it runs the appliance immediately using the local energy storage as a source. Otherwise, it tries to shift the time of running the appliance to the *OFF-Peak* period, with the electric company as a source, using the maximum tolerable delay that is calculated based on the user input. If the delay does not allow such shifting, it tries to shift the task executing to the *Mid-peak* period. Otherwise, if the shifting is not possible, it executes the task during the current time period. This type of energy management system provides considerable environmental benefits. It also lowers the cost of energy for both the user as well as the electric company.

5.3 Smart water systems

Figure 5 shows the general architecture of a smart water system, which is another important smart city application. The system is used to monitor and control the irrigation of the soil with various types of crops using an optimized process. In general, sensing devices are placed in selected areas in the farm in order to monitor different parameters such as temperature, and moisture of the soil. Actor devices are used to control different activities such as the time and amount of water that is provided by the system. Both sensor and actor devices constitute nodes in a WSAN. The nodes can have various topologies including mesh and star configurations. In either case, one of the nodes acts as a gateway to provide connectivity to the sink, which in turn connects the WSANs to the backbone LAN or the Internet. Cloud computing platforms can also be used to provide storage, analysis, processing, and decision making services. The figure also shows that different databases can be used to provide plant and weather related information to the system. Such information is

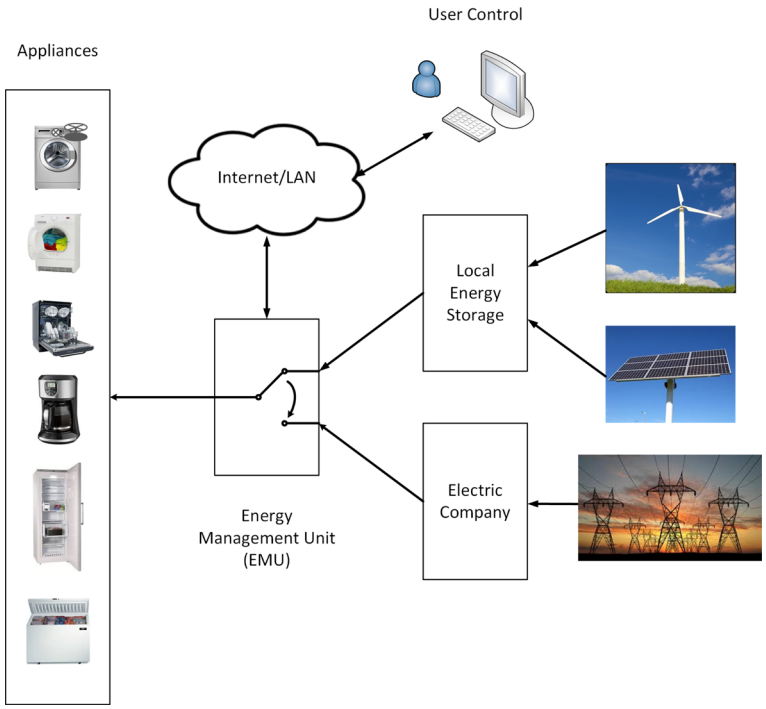

Fig. 4 The architecture of a home-based energy management system used in a smart city

typically combined with the collected sensing data to make optimized decisions related to the time, location, and amount of water that is released by the system. The system is also capable of issuing alert notifications to the users whenever it is appropriate. In addition, the network is connected to the control center, which oversees the operations. It also issues different configuration and command requests to supervise and manage the network.

5.4 UAV and Commercial Aircraft Safety Communication

Due to the several challenges of the new aeronautical applications including emerging UAV applications for

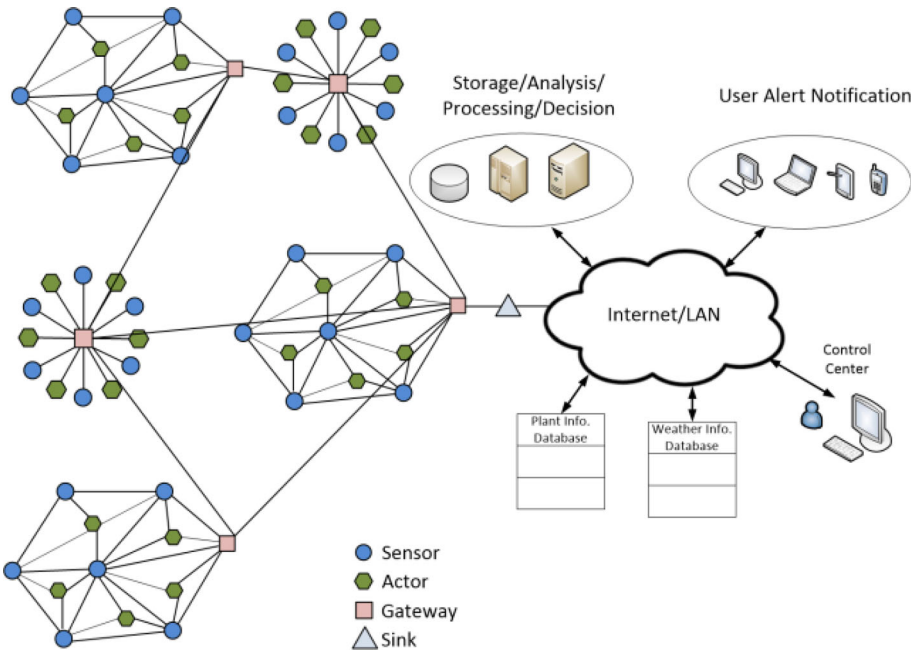

Fig. 5 The general architecture for a smart water system used in a smart city

smart cities, there are high needs to define new communication solutions, which can effectively support these new applications. The National Aeronautics and Space Administration (NASA) in the United States and the European Organization for the Safety of Air Navigation (EUROCONTROL) are leading the development of new communication systems. A standard for UAS Control and Non-Payload Communication (CNPC) links is being developed in the United States to enable safe integration of UAS operations within the National Airspace System (NAS) [44]. NAS is the main aviation system in the United States that involves, the US airspace, airports, and monitoring and control equipment and services that implement the enforced rules, regulations, policies, and procedures. This system covers the airspace of the United States and large portions of the oceans. Some of its components are also shared with the military air force. For safe integration of UAS operations in NAS, sense and avoid techniques, aircraft-human interface, air traffic management policies and procedures, certification requirements, and CNPC are being studied [45]. This integration allows UAVs to function within the airspace used for manned aircrafts used for carrying passengers and cargo.

CNPC links are defined to provide communication connections to be used for aircraft safety applications and to enable remote pilots and other ground stations to control and monitor the UAVs. Figure 6 show an illustration of required communication links between the UAVs, commercial airlines, and the control center. This involves several issues including communication architecture types as well as rate, bandwidth, frequency spectrum allocation, security, and reliability requirements. Two communication architecture types were proposed including line-of-sight (LOS) communication, which provides communication with unmanned aircrafts through ground-based communication stations and beyond-line-of-sight (BLOS) communication, which provides communication with unmanned aircrafts through satellites. The communication rates requirements for both uplink (ground-to-air) and downlink (air-to-ground) were defined based on the size of unmanned aircrafts as shown in Table 3. The uplink rates are much lower than downlink rates as the uplink communication will be mainly used to send small messages to control the unmanned aircrafts while the downlink communication is used for different types of communication including video transmission. The uplink rate was determined to support transmission of 20 individual control messages per second. This rate is required to provide a complete real-time ground control for a UAV using a joystick [44].

The supported density requirements of unmanned aircrafts that use CNPC to the year 2030 are also specified [45] and shown in Table 4. The third column shows the numbers of unmanned aircrafts (of different sizes) that can be supported if a terrestrial-based communication link of radius 100 Km is used.

Based on the defined UAV density, the required bandwidth for CNPC links is 90 MHz divided into 34 MHz for the terrestrial-based LOS CNPC links and 56 MHz for the BLOS CNPC links [44]. Two frequency spectrum ranges were assigned by the 2012 International Telecommunications Union World Radio Communications Conference (WRC-12) to be used by CNPC to provide reliable and real-time data transmissions. These frequency spectrums are from 960 MHz to 1164 MHz (L-Band) and from 5030 MHz to 5091 MHz. However, a portion of the first range will be shared with other legacy applications

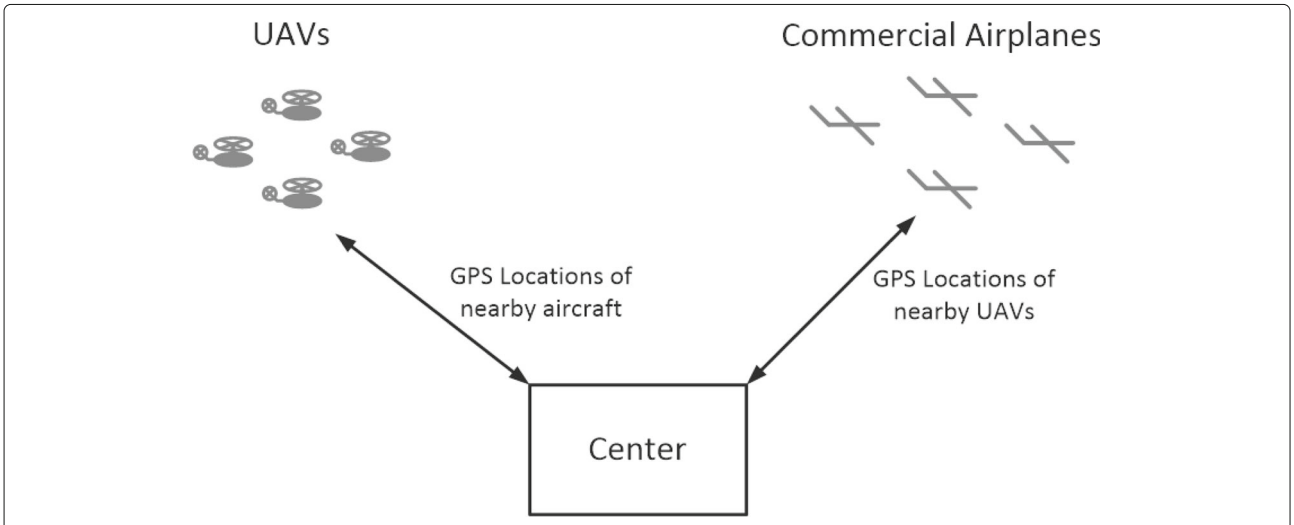

Fig. 6 UAV and commercial aircraft safety communication

Table 3 CNPC data communication rates

Aircraft size	Uplink rate	Downlink usages	Downlink rate
Small (<=55 kg)	2424 bps	Basic services only	4008 bps
Medium and Large (>55 kg)	6925 bps	Basic services only	13,573 bps
Medium and Large (>55 kg)	6925 bps	Basic and weather radar	34,133 bps
Medium and Large (>55 kg)	6925 bps	Basic, weather radar and video	234,134 bps

for surveillance and navigation purposes. Another issue of CNPC links is the high security requirements. Good security mechanisms should be used on CNPC links to avoid any possibility of spoofed control or navigation signals that may allow unauthorized persons to control the UAVs [46]. For meeting future communication capacity requirements in aeronautical communications, a new air-ground communication system, called L-Band Digital Aeronautical Communication System (L-DACS), is being developed in Europe with funding from EUROCONTROL. L-DACS is the system in the Future Communication System (FCS) for L-band, 960-1164 MHz. L-DACS comprises of L-DACS1 [47] and L-DACS2 [48]. L-DACS1 is multi-carrier broadband Orthogonal Frequency-Division Multiplexing (OFDM)-based system while L-DACS2 is narrow band single-carrier with Gaussian Minimum Shift Keying (GMSK) modulation system. More information about L-DACS1 and L-DACS2 including their benefits with the current aeronautical system and their physical and medium access layers can be found in [49].

5.5 Pipeline monitoring and control

In this section, we provide further discussion and illustration of the smart city application of monitoring pipelines systems as an example of infrastructure monitoring. Figure 7 shows a CPS system for pipeline monitoring and control. In our previous work in [50, 51], we present a framework for monitoring oil, gas, and water pipelines using linear sensor networks (LSNs). We defined an LSN to be a WSN where the sensors are aligned in linear form due to the linearity of the structure or geographic area that is being monitored, such as pipelines, borders, rivers, sea coasts, railroads, and more. In the system illustrated in the figure, the sensor nodes (SNs) are placed on the pipeline in order to monitor various important parameters such as temperature, pressure, fluid velocity, chemical substances, leaks, etc. The collected data could either be routed to the sink, which is placed at the end of the pipeline or pipeline segment using a multihop strategy [51], or it could be collected using a mobile node such as a low flying UAV [52]. In the latter case, the SN transmits its stored data to the UAV when it comes within its range. The UAV, which flies along the pipeline, delivers the collected data to the sink at the other end. Once the data arrives at the sink using either one of these strategies, it transmits the data to the infrastructure network using any one of the communication networks that are available in the area such as IEEE 802.16 (WiMAX), cellular, and satellite.

Table 4 CNPC supported aircraft density

Aircraft size	Density of UAVs in Space (km^3)	No. of UAVs within Radius of 100 km
Small	0.000802212	1680
Medium	0.000194327	407
Large	0.00004375	91

The storage and processing servers that are used by the CPS system can be a part of the cloud computing environment. The results are then sent in appropriate format to the network control center (NCC), where they can be presented to the NCC personnel using applications that allow visualization of the pipeline structure. The graphic representation that is displayed can show the pipeline's current status as well as any anomalies that need more attention and further inspection. The NCC officers can then issue certain commands back to the SNs in a particular *hot spot*. Alternatively, such commands might be automatically issued by the CPS system in accordance with algorithms and configurations that are programmed by the system administrators. The command messages intended to reach the target SNs are communicated via the network, the sink, and other SNs (if the multihop routing strategy is used) or the UAV (if UAV-based communication is used). An example of such commands could be: (1) increase the quantity and/or quality of the collected data, (2) turn ON more SNs in the hot spot, and (3) turn ON additional sensing or monitoring devices (that might be in sleep-mode to save energy) such as higher resolution cameras, as well as audio or video monitoring equipment. Also, the NCC might dispatch specialized UAVs and/or quick response teams for further inspection, or to take remedial emergency actions (put out fire, etc.) In other cases, the collected data can be used to generate appropriate maintenance schedules, which could result in the service of various parts of the pipeline according to a pre-set priority strategy.

6 Open issues

In this section, we identify some of the most important open issues that need further research and investigation in the area of networking and communication in smart city systems.

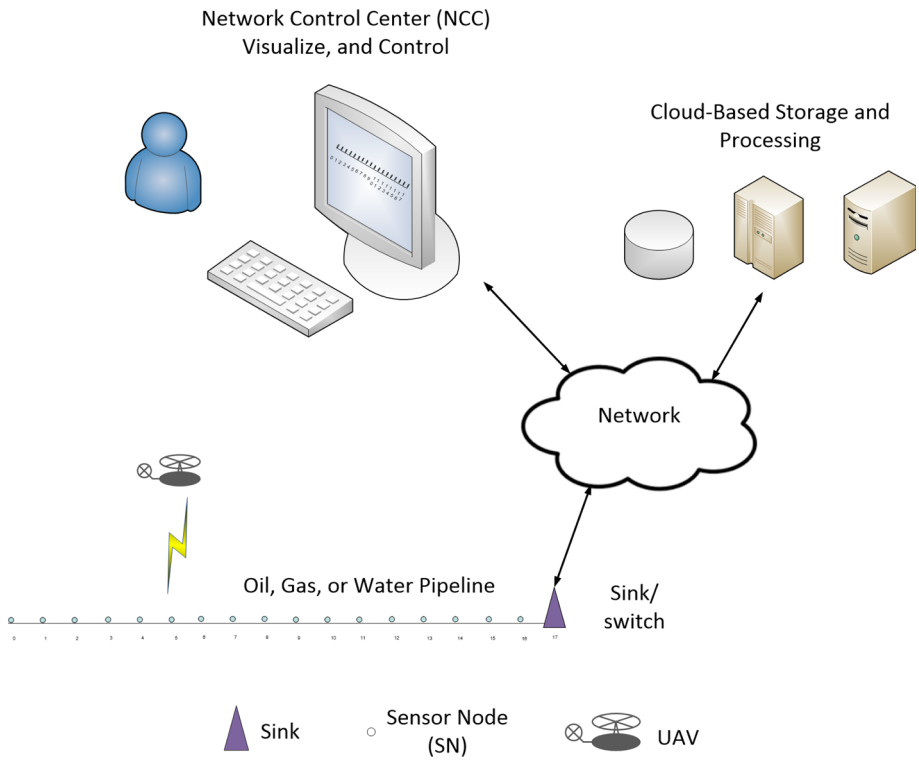

Fig. 7 CPS for pipeline monitoring and control

6.1 Communication middleware for smart city applications

As a smart city network can consist of different devices, communication technologies, and protocols, managing such a network can be very complex. One of the possible approaches to relax this complexity is to use a specialized communication middleware capable of abstracting these communication details. In addition, this middleware can offer value-added features that are commonly needed for different smart city applications and are not fully supported by existing network technologies. These features can include provisions and services for security, reliability, scalability, and quality of service provisioning.

6.2 Software defined network support for smart city applications

Software defined networking (SDN) is an approach to enable flexible and efficient network configuration to enhance a network. SDN can provide many advantages for configuring city networks to support different applications. While there are some efforts in investigating this approach for supporting smart city applications [37], there is room for developing more advanced management and networking mechanisms in SDN for efficient, reliable, and secure network configurations in smart cities.

6.3 New networks and network protocols

Most of the current communication infrastructure uses the Internet infrastructure or the cellular networks. Although these have proven to be efficient and usable, they often lack some necessary requirements for smart city applications. Issues in real-time responses, mobility support and the ability to handle huge volume of network traffic. When a smart city application is deployed city-wide and collects find grain data, it will generate massive traffic, which could cause serious performance problems for the underlying network infrastructure. Some work is underway to add more capabilities such as the progression from 3G, to 4G and now 5G cellular networks [53], advances in MESH networks and investigation of more efficient protocols on the existing networks. However, there is a lot to be done in this regard.

6.4 Modeling and simulation

There are limited efforts in studying modeling and simulation of the communication performance of different smart city applications on different network architectures. It is important to develop different models and simulation tools to be able to design, evaluate, and plan for such networks. In addition, more detailed traffic patterns of different smart applications need to be comprehensively studied. Modeling and simulation of both the

traffic of smart city applications and the used networks' capabilities may lead to better end results for the smart city applications.

7 Conclusions and future research

Significant advancements in various technologies such as CPS, IoT, WSNs, cloud computing, and UAVs have taken place lately. The smart city paradigm combines these important new technologies in order to enhance the quality of life of city inhabitants, provide efficient utilization of resources, and reduce operational costs. In order for this model to reach its goals, it is essential to provide efficient networking and communication between the different components that are involved to support various smart city applications. In this paper, we investigated the networking requirements for the different applications and identified the appropriate protocols that can be used at the various system levels. In addition, we illustrated networking architectures for five different smart city systems. This area of research is still in its initial stages. Future studies can focus on important requirements including routing, energy efficiency, security, reliability, mobility, and heterogeneous network support. Consequently, more investigations and studies need to be done, which should lead to the design and development of efficient networking and communication protocols and architectures to meet the growing needs of the various important and rapidly expanding smart city applications and services.

Abbreviations

CPS: Cyber-physical systems; UAV: Unmanned aerial vehicle; WSN: Wireless sensor networks

Acknowledgments

Not applicable.

Funding

This research was not supported by any external funding source.

Authors' contributions

IJ wrote the main sections of the paper. NM contributed to the section on smart city applications, and illustration of smart city systems. JA contributed to the introduction and related work content. All authors read, and approved the final manuscript, and contributed to various sections in the paper according to their background.

Ethics approval and consent to participate

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Author details

[1] Al Maaref University, Old Airport Avenue, P.O. Box 25-5078, Beirut, Lebanon.
[2] Middleware Technologies Laboratory, Pittsburgh, Pennsylvania, USA.
[3] Robert Morris University, Moon Township, Pennsylvania, USA.

Received: 24 April 2018 Accepted: 11 October 2018
Published online: 20 December 2018

References

1. Watteyne T, Pister KSJ (2011) Smarter cities through standards-based wireless sensor networks. IBM J Res Dev 55(1.2):1–7
2. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M (2014) Internet of things for smart cities. IEEE Internet Things J 1(1):22–32
3. Gurgen L, Gunalp O, Benazzouz Y, Gallissot M (2013) Self-aware cyber-physical systems and applications in smart buildings and cities. In: Proceedings of the Conference on Design, Automation and Test in Europe, pages 1149–1154. EDA Consortium
4. Ermacora G, Rosa S, Bona B (2015) Sliding autonomy in cloud robotics services for smart city applications. In: Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction Extended Abstracts. ACM. pp 155–156
5. Mohammed F, Idries A, Mohamed N, Al-Jaroodi J, Jawhar I (2014) Uavs for smart cities: Opportunities and challenges. In: Unmanned Aircraft Systems (ICUAS), 2014 International Conference on. IEEE. pp 267–273
6. Giordano A, Spezzano G, Vinci A (2016) Smart agents and fog computing for smart city applications. In: International Conference on Smart Cities. Springer. pp 137–146
7. Clohessy T, Acton T, Morgan L (2014) Smart city as a service (scaas): a future roadmap for e-government smart city cloud computing initiatives. In: Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing. IEEE Computer Society. pp 836–841
8. Al-Nuaimi E, Al-Neyadi H, Mohamed N, Al-Jaroodi J (2015) Applications of big data to smart cities. J Internet Serv Appl 6(1):25
9. Mohamed N, Lazarova-Molnar S, Al-Jaroodi J (2017) Cloud of things: Optimizing smart city services. In: Proceedings of the International Conference on Modeling, Simulation and Applied Optimization. IEEE. pp 1–5
10. Erol-Kantarci M, Mouftah HT (2012) Suresense: sustainable wireless rechargeable sensor networks for the smart grid. IEEE Wirel Commun 19(3)
11. Gutiérrez J, Villa-Medina JF, Nieto-Garibay A, Porta-Gándara MÁ (2014) Automated irrigation system using a wireless sensor network and gprs module. IEEE Trans Instrum Meas 63(1):166–76
12. Centenaro M, Vangelista L, Zanella A, Zorzi M (2016) Long-range communications in unlicensed bands: The rising stars in the iot and smart city scenarios. IEEE Wirel Commun 23(5):60–7
13. Leccese F, Cagnetti M, Trinca D (2014) A smart city application: A fully controlled street lighting isle based on raspberry-pi card, a zigbee sensor network and wimax. Sensors 14(12):24408–24
14. Sanchez L, Muñoz L, Galache JA, Sotres P, Santana JR, Gutierrez V, Ramdhany R, Gluhak A, Krco S, Theodoridis E, et al. (2014) Smartsantander: Iot experimentation over a smart city testbed. Comput Netw 61:217–38
15. Wan J, Di L, Zou C, Zhou K (2012) M2m communications for smart city: An event-based architecture. In: Computer and Information Technology (CIT), 2012 IEEE 12th International Conference on. IEEE. pp 895–900
16. Gaur A, Scotney B, Parr G, McClean S (2015) Smart city architecture and its applications based on iot. Procedia Comput Sci 52:1089–94
17. Jin J, Gubbi J, Luo T, Palaniswami M (2012) Network architecture and qos issues in the internet of things for a smart city. In: Communications and Information Technologies (ISCIT), 2012 International Symposium on. IEEE. pp 956–961
18. De Poorter E, Moerman I, Demeester P (2011) Enabling direct connectivity between heterogeneous objects in the internet of things through a network-service-oriented architecture. EURASIP J Wirel Commun Netw 2011(1):61
19. Karnouskos S (2011) Cyber-physical systems in the smartgrid. In: Industrial Informatics (INDIN), 2011 9th IEEE International Conference on. IEEE. pp 20–23
20. Miclea L, Sanislav T (2011) About dependability in cyber-physical systems. In: Design & Test Symposium (EWDTS), 2011 9th East-West. IEEE. pp 17–21
21. Sridhar S, Hahn A, Govindarasu M (2012) Cyber–physical system security for the electric power grid. Proc IEEE 100(1):210–24
22. Berger C, Rumpe B (2014) Autonomous driving-5 years after the urban challenge: The anticipatory vehicle as a cyber-physical system. arXiv preprint arXiv:1409.0413

23. Cunningham R, Garg A, Cahill V, et al. (2008) A collaborative reinforcement learning approach to urban traffic control optimization. In: Web Intelligence and Intelligent Agent Technology, 2008. WI-IAT'08. IEEE/WIC/ACM International Conference on. IEEE Vol. 2. pp 560–566
24. Kartakis S, Abraham E, McCann JA (2015) Waterbox: A testbed for monitoring and controlling smart water networks. In: Proceedings of the 1st ACM International Workshop on Cyber-Physical Systems for Smart Water Networks. ACM. p 8
25. Gonda L, Cugnasca CE (2006) A proposal of greenhouse control using wireless sensor networks. In: Proceedings of 4thWorld Congress Conference on Computers in Agriculture and Natural Resources, Orlando, Florida, USA. p. 229
26. Mohamed N, Al-Jaroodi J, Jawhar I, Lazarova-Molnar S (2014) A service-oriented middleware for building collaborative uavs. J Intell Robot Syst 74(1-2):309–21
27. Lee J, Bagheri B, Kao H-A (2015) A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manuf Lett 3:18–23
28. López P, Fernández D, Jara AJ, Skarmeta AF (2013) Survey of internet of things technologies for clinical environments. In: Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on. IEEE. pp 1349–1354
29. Macedo D, Guedes LA, Silva I (2014) A dependability evaluation for internet of things incorporating redundancy aspects. In: Networking, Sensing and Control (ICNSC), 2014 IEEE 11th International Conference on. IEEE. pp 417–422
30. Silva I, Leandro R, Macedo D, Guedes LA (2013) A dependability evaluation tool for the internet of things. Comput Electr Eng 39(7):2005–18
31. (2014) Oma lightweight m2m. Available: http://technical.openmobilealliance.org/technical/technical-information/release-program/current-releases/oma-lightweightm2m-v1-0-2
32. Perelman V, Ersue M, Schönwälder J, Watsen K (2012) Network Configuration Protocol Light (NETCONF Light). Network
33. (2013) Commercial building automation systems. Navigant Consulting Res, Boulder
34. Suciu G, Vulpe A, Halunga S, Fratu O, Todoran G, Suciu V (2013) Smart cities built on resilient cloud computing and secure internet of things. In: Control Systems and Computer Science (CSCS), 2013 19th International Conference on. IEEE. pp 513–518
35. Bolodurina I, Parfenov D (2017) Development and research of models of organization distributed cloud computing based on the software-defined infrastructure. Procedia Comput Sci 103:569–76
36. Bonomi F, Milito R, Zhu J, Addepalli S (2012) Fog computing and its role in the internet of things. In: Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM. pp 13–16
37. Liu J, Li Y, Chen M, Dong W, Jin D (2015) Software-defined internet of things for smart urban sensing. IEEE Commun Mag 53(9):55–63
38. Olenewa JL (2014) Guide to Wireless Communications. Cengage Learn
39. Stallings W (2005) Wireless Communications and Networks. Prentice Hall, Pearson Education, Inc., Upper Saddle River
40. IEEE 802.11, IEEE 802.16. http://en.wikipedia.org/wiki, viewed December 10, 2014
41. Goyal D, Tripathy MR (2012) Routing protocols in wireless sensor networks: A survey. In: Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on. IEEE. pp 474–480
42. Jawhar I, Mohamed N, Agrawal DP (2011) Linear wireless sensor networks: Classification and applications. J Netw Comput Appl 34(5):1671–82
43. Nunes BAA, Mendonca M, Nguyen X-N, Obraczka K, Turletti T (2014) A survey of software-defined networking: Past, present, and future of programmable networks. IEEE Commun Surv Tutor 16(3):1617–34
44. Kerczewski RJ, Griner JH (2012) Control and non-payload communications links for integrated unmanned aircraft operations. In: Report, NASA Glenn Research Center, Cleveland, Ohio, USA
45. (2012) Unmanned aircraft systems (uas) integrated in the national airspace system (nas) technology development project plan. In: National Aeronautics and Space Administration
46. Zeng Y, Zhang R, Lim TJ (2016) Wireless communications with unmanned aerial vehicles: opportunities and challenges. IEEE Commun Mag. arXiv preprint arXiv:1602.03602 54(5)
47. Sajatovic M, Haindl B, Ehammer M, Graupl T, Schnell M, Epple U, Brandes S (2009) L-dacs1 system definition proposal: Delivrable d2. EUROCONTROL, Tech. Rep. Version 1.0
48. Fistas N (2009) L-dacs2 system definition proposal: Delivrable d2. EUROCONTROL, Tech. Rep. Version 1.0
49. Neji N, De Lacerda R, Azoulay A, Letertre T, Outtier O (2013) Survey on the future aeronautical communication system and its development for continental communications. IEEE Trans Veh Technol 62(1):182–91
50. Jawhar I, Mohamed N, Agrawal DP (2011) Linear wireless sensor networks: Classification and applications. Elsevier J Netw Comput Appl (JNCA) 34:1671–82
51. Jawhar I, Mohamed N, Shuaib K (2007) A framework for pipeline infrastructure monitoring using wireless sensor networks. In: The Sixth Annual Wireless Telecommunications Symposium (WTS 2007), IEEE Communication Society/ACM Sigmobile, Pomona, California, U.S.A. pp 1–7
52. Jawhar I, Mohamed N, Al-Jaroodi J, Zhang S (2014) A framework for using unmanned aerial vehicles for data collection in linear wireless sensor networks. J Intell Robot Syst 74(1-2):437–453
53. Andrews JG, Buzzi S, Choi W, Hanly SV, Lozano A, Soong ACK, Zhang JC (2014) What will 5g be? IEEE J Sel Areas Commun 32(6):1065–82
54. Fallah YP, Huang C, Sengupta R, Krishnan H (2010) Design of cooperative vehicle safety systems based on tight coupling of communication, computing and physical vehicle dynamics. In: Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems. ACM. pp 159–167