

Sobhi, Salma; Ali, Maged A.; Abdelkader, Mohamed F.

Conference Paper

Combining Fog Computing and LoRaWAN Technologies for Smart Cities Applications

2nd Europe - Middle East - North African Regional Conference of the International Telecommunications Society (ITS): "Leveraging Technologies For Growth", Aswan, Egypt, 18th-21st February, 2019

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Sobhi, Salma; Ali, Maged A.; Abdelkader, Mohamed F. (2019) : Combining Fog Computing and LoRaWAN Technologies for Smart Cities Applications, 2nd Europe - Middle East - North African Regional Conference of the International Telecommunications Society (ITS): "Leveraging Technologies For Growth", Aswan, Egypt, 18th-21st February, 2019, International Telecommunications Society (ITS), Calgary

This Version is available at:

<https://hdl.handle.net/10419/201754>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

Combining Fog Computing and LoRaWAN Technologies for Smart Cities Applications

Salma Sobhi¹, Maged A. Ali², Mohamed F. Abdelkader^{1,2}

¹ Wireless Communication Engineering, Information Technology Institute,
Ismailia, EGYPT

²Electrical Engineering Department Faculty of Engineering,
Port Said, EGYPT

Abstract- With the growing need for smart services and internet of things (IoT) devices in smart cities, the cloud paradigm might not be able to accommodate the increasing data traffic and the various latency-aware applications. Meanwhile, as smart cities grow bigger and wider, finding a communication protocol that fully supports the nature of smart cities application becomes essential, with the need for a secure and privacy protecting paradigm is more than ever. In this paper, we investigate the potential of combining the recently introduced fog computing and loRaWAN communication standard to attain more sustainable smart cities. We present a case study for using the proposed network architecture for smart water distribution networks.

Index Terms – Fog-computing, Smart-Cities, LoRaWAN, IoT, Water distribution networks.

I. INTRODUCTION.

The merge to smart cities is becoming essential due to the rapid increase in internet of things (IoT) applications and their introduction into most of daily services such as health care, finance and billing, systems monitoring and management, smart grids, and smart metering. Smart cities applications rely on smart devices connected to each other and exchanging data and information over the internet. A setup which can result in a wide range of heterogeneous devices communicating via various communication protocols. This categorizes applications of smart cities into groups on the basis of scalability, coverage, flexibility, heterogeneity, and end-user involvements [1].

Meanwhile, as smart cities continue to grow, they require millions of smart devices including sensors, RFIDs, monitoring cameras, and communication devices. This massive deployment of smart devices will result in communication challenges in both end devices and core network domains. Those challenges include congestion, service delay, data privacy and security and lack of interoperability [2], [3]. Most of the core network domain challenges are downsides of

depending heavily on cloud computing. Sending all the data collected all the time to cloud has high costs in terms of bandwidth, storage, latency, and energy consumption [4]. To address the weaknesses inherited by the cloud computing paradigm, fog computing has been proposed by Cisco in 2005 encouraging a shift of handling everything in the core of cloud computing to handling at the edges of a network [2].

On the other side, the challenges in the end devices domain lies in choosing the wireless technologies used to provide data access to these devices. Several standards such as ZigBee and Bluetooth, have been used to implement IoT services due to their low power consumptions. However, their limited coverage constitutes a major obstacle, in particular when the application scenario involves services that require urban-wide coverage, as in typical smart city. A promising alternative, standing in between short-range technologies operating and long-range cellular-based is provided by the so-called Low-Power Wide Area Networks (LPWANs) [5].

Several papers have been devoted to discussing the future of smart cities, and many researchers proposed potential solutions to the challenges facing scalability and sustainability of these cities. The authors in [6] introduced eight principles for sustainable and healthy smart cities. In [7], the authors discuss the enabling communication and networking technologies used in smart cities, and a taxonomy is devised by classifying the literature based on future and emerging technologies.

Fog computing was proposed for sustainable smart cities in [2]. The authors in [8] proposed a multi-tiered framework that relies on fog computing to save energy and reduce delays. The authors in [9] suggested that a fog-based approach is the most suitable architecture for IoT applications and proposed a distributed dataflow programming model as a basis for fog based IoT applications.

In this paper, we highlight the potential of combining fog computing and LoRaWAN communications in smart cities. We also, discuss the proposed benefits on the case study of IoT monitoring of water distribution networks.

The rest of the paper is organized as follows: in the next section we outline some of the challenges facing current cloud based smart city applications. Section III discusses fog computing definition and characteristics and the benefits and applications of fog computing for smart cities. An introduction to LoRaWAN and its usages for smart cities is discussed in section IV. Section V present our case study of using fog and LoRaWAN for smart water monitoring applications.

II. CURRENT CHALLENGES OF SMART CITIES DEPLOYMENT.

Although cloud computing is widely used in smart city applications, it still shows some limitations. The fundamental limitation is caused by the nature of the connectivity link between the cloud and the end devices due to the centralized nature of cloud-based solutions. A model which is no longer sufficient to incorporate all the needs and demands of the users. As the number of users increases, the continuously growing traffic loads the core network, resulting in some serious challenges [10].

The least of the observed challenges is the repeated congestion. The vast and rapidly growing number of connected things is creating data at an exponential rate, devices such as connected cars and traffic monitoring cameras could generate tens megabytes worth of data per one second. Sending all the data to the cloud will require prohibitively high network bandwidth. That is often unnecessary and sometimes even prohibited due to regulations and data privacy concerns. Also, many smart applications, such as vehicle-to-vehicle communications, virtual reality applications, gaming applications, and real-time financial trading applications, require latencies below a few tens of milliseconds, a requirement that falls far outside what mainstream cloud services can achieve. Finally, Cloud services have difficulty providing uninterrupted services to devices and systems that have intermittent network connectivity to the cloud [11].

Another major challenge is that the existing security paradigm will no longer be adequate for addressing many new security challenges in the emerging IoT applications of smart cities. Such as, keeping security credentials and software up to date on large number of devices, protecting resource-constrained device and responding to security compromises without causing intolerable disruption

On the other hand, the communication requirements for smart city systems considerable vary among the different applications. As smart cities offer wide range of services, some are localized such as smart homes, e-health care and smart shopping carts, and others are spread on wide geographical areas, such as wireless sensor networks, monitoring services like traffic cameras, and smart metering. Each group of services has different communication requirements, while the first could deploy low power low range protocols such as WiFi, RFID, near field communication NFC or Bluetooth low energy BLE. The later needs longer range and uses technologies such as cellular networks or IoT LPWAN supporting protocols such as SigFox or LoRa. This wide range of applications and protocols makes it a challenge to incorporate all protocols in one paradigm and ensure flexible connectivity with the cloud.

III. FOG COMPUTING.

Fog computing has been defined in several ways in the literature. Some definitions are found in [12], [13], [14] and [15]. The one we find most comprehensive is: “*Fog computing is a distributed computing platform where most of the processing will be done by virtualized and non-virtualized end or edge devices. It is also associated with the cloud for non-latency-aware processing and long-term storage of useful data by residing in between users and the cloud*” [16]. In This section we present the fog system architecture and highlight and discuss some of the main benefits Fog computing introduced to the existing smart cities.

A. Fog system architecture

The system architectures of fog systems adopt a three-tier architecture similar to other large-scale distributed computing systems. An illustrative model of such architecture is shown in Figure1.

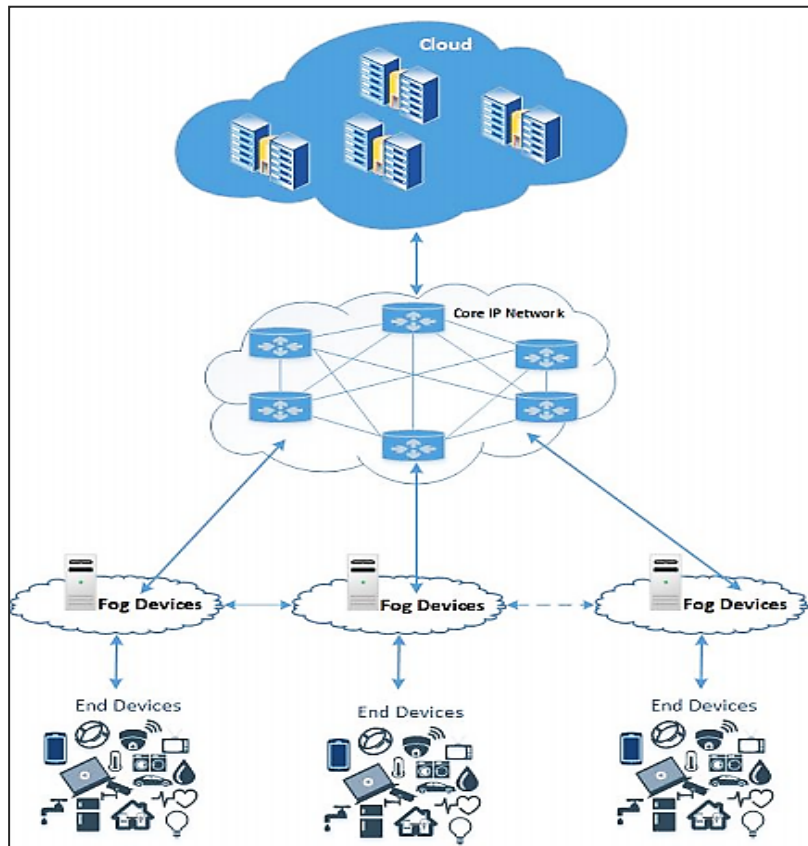


Figure 1. A model of Fog computing [16]

The three layers are: cloud layer, fog layer, and the IoT device/end-user layer. The fog layer can be formed by one or more fog nodes, controlled by the same or different providers. These fog nodes include edge routers, switches, gateways, access points, PCs, smartphones, set-top boxes, etc. The IoT/end-user layer is formed of IoT/smart devices and/or end user devices.

The fog system architectures can be classified into application agnostic or application specific as shown in the survey work in [17]. The architecture for fog-based smart cities is defined in the same paper as follows:

The IoT/end-user layer is comprised of smart objects such as sensors and laptops. Application components deployed in the fog layer are responsible for filtering the collected data from the smart objects and ensuring real-time interactions. The fog layer consists of two types of fog nodes: The fog server and the fog edge nodes. The fog server includes modules that are responsible for management functionalities such as application deployment, network configuration, and billing.

The fog edge node provides computing, storage, and communication capabilities to smart objects, and communicates with the fog server. Meanwhile, the communications between the fog edge nodes and the cloud nodes are routed through the fog servers. The cloud layer includes components that are responsible for functionalities such as storing the data received from the fog layer as a backup.

The main advantages of fog computing can be exemplified as CEAL as explained in [11]. CEAL stands for cognition, efficiency, agility and latency. Cognition means the awareness of the client objectives. Due to the close proximity of fog to the end users, fog devices could be fully aware of the nature of the customer requirements and be able to adapt to these requirements. Efficiency appears in the interoperability between fog and cloud, as fog can distribute computing, storage, and control functions anywhere between the cloud and the endpoint to take full advantage of the resources available anywhere on the network. Moreover, the closer proximity of the fog to the endpoints enable it to be more closely integrated with the end-user systems to enhance overall system efficiency and performance.

Agility enables rapid innovation and affordable scaling as it is usually much feasible to experiment with client edge devices rather than waiting for large networks migration to a new or updated technology. While, latency is the main benefit of processing at the network edge. As fog can support time-sensitive functions such as alarming systems, vehicle to vehicle communication and augmented reality applications.

More advantages appear in [12] and [13], including the geographical distribution which will provide better support for user mobility; heterogeneity and interoperability as fog nodes coming from different vendors and operate under different protocols; and, support for big data analytics.

One of the most important advantages of fog computing is protecting data privacy and enhancing the overall security of the network. This will be discussed in more details throughout the paper.

B. Fog Computing for Smart Cities.

The presented fog architecture offers many compelling benefits for computing, storage, as well as for networking in smart city scenarios. This architecture is based on fog clusters where multiple fog devices participate to cooperate in the processing. On the other hand, datacenters are the main physical components of cloud paradigm. Because of this, cloud computing has high operational costs and energy consumption. By comparison, energy consumption and operation costs in the Fog computing paradigm is low. The Fog is located closer to the user, so the distance between users and fog devices could be one or a few hops [18].

Fog computing can also ensure higher availability. Connecting to the cloud is less reliable due to a variety of different connectivity issues, and, considering cost, fog computing will cost more than deploying dumb devices at the edge and thus it would increase the total cost of a fog-based IoT solution. However, in the long term such additional costs will become justified due to potential savings and other benefits [16].

Some of the main benefits Fog computing introduction into existing smart cities are as follows:

- *Interoperability between Fog and Cloud:*

Fog nodes fill the gap between the cloud and the end-devices “things” to enable a service continuum. Meaning, that if you rely on the cloud for a certain service and you lose connectivity, your nearest fog node could act as a backup server for this service. Fog and Cloud Are Interdependent: For example, cloud services may be used to manage the fog. Conversely, Fog can act as the proxy of the cloud to deliver cloud services to endpoints, and act as the proxy of the endpoints to interact with the cloud.

In cloud computing paradigm, events or data are transmitted to the data center inside the core network. Results are sent back to the end users after a series of processing, which puts high load on the core network. By designing module-based data analytical components that can be remotely

pushed into fog devices on demand, fog can insure uninterrupted services, by acting as a backup for the cloud or by splitting the traffic and processing load of the cloud’s core network by handling acquisition, aggregation and preprocessing, reducing the data transportation and storage and, balancing computation power on data processing [2].

- *Bandwidth and Power consumption:*

Being in the near proximity to the end users, fog avoids the back-and-forth traffic between cloud and mobile users. This not only saves the backbone bandwidth, but also significantly reduces the energy consumption of both the connected things and the core networks. This close proximity of fog nodes to users reduces the latency effectively. In [19], Shanhe Yi et al, constructed an experiment comparing between fog and cloud performances in terms of latency and bandwidth consumption. They build a proof-of-concept fog computing platform, consisting of two fog subsystems with a network link between them and both are connected to the Amazon EC2 cloud through WAN as shown in figure 2, all of which were equipped with access points so that the mobile devices they used can access the fog as well as the Amazon EC2 cloud.

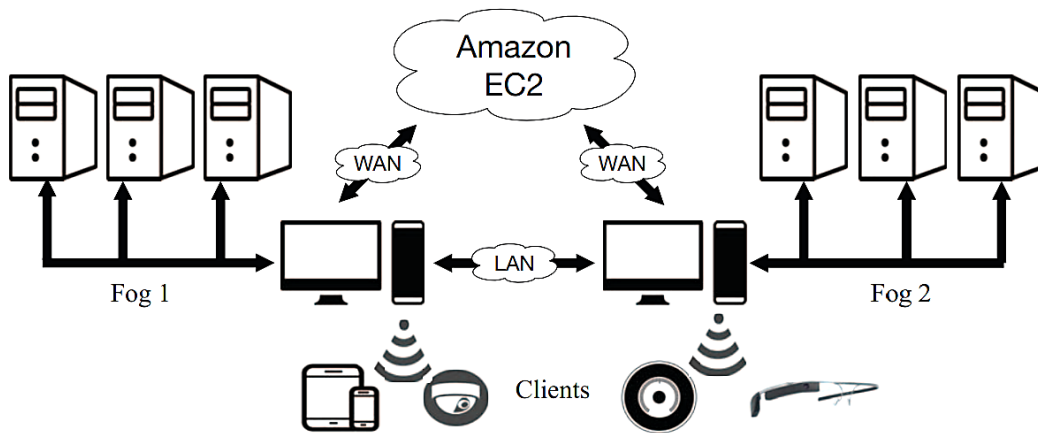


Figure 2 Experiment setup comparing fog and cloud latency performance [19].

Then they measured both uplink and downlink bandwidth while connecting to each system showing that, the bandwidth consumption for connecting to the cloud is almost fifty times more the consumption of fog.

Another experiment was conducted by the authors in [8] to test the power consumption of their fog-supported smart city network architecture. They implemented their architecture on an *iFogSim*

simulator, which provides real-time scenarios for Fog-based networks in a smart city. *iFogSim* evaluated the resulting average total consumed power for each fog node under a web-based application and, comparing between their fog-based and web-based networks in a smart city, under various settings and using different networking protocols, showing that fog networking substantially decreases power consumption.

- *Real Time services and Low latency capabilities:*

Real-time Interaction is one of the main service requirements in many smart city application domains. Applications such as vehicle-to-vehicle communications require latency below a few tens of milliseconds. Which fall far outside what mainstream cloud services can achieve. A problem which can be easily resolved by fog computing, through allowing processing to take place at the network edge near the end devices, by the fog nodes and the ability to enable processing at specific locations. This reduces the delay significantly and allow for location aware real time services.

The experiment conducted in [19] measured fog and cloud based network performances in terms of latency. They used use RTT (round trip time) as their metric and, implemented a face recognition application running across a smartphone and a fog or a cloud. The app on the smartphone sends a picture of someone face to the remote server and, the remote server will then try to recognize the face by matching it in the local face photo database of size 1521. They compared the RTT for both systems showing that the latency of cloud is twelve times more than fog, while the processing time on both servers was almost the same. The response time of the fog server was almost eight times faster than that of a cloud server.

- *Data Privacy and Security in Fog Paradigm:*

Data privacy and security remains the main concern of most users which poses a national security threat for large scale smart city applications. According to HP, 70 percent of IoT devices in a smart city were at risk of attack due to sufficient vulnerabilities such as insufficient authorization, inadequate software protections, and weak encrypted communication protocols [20]. Moreover, the open nature of smart cities and its dependency on wireless communication between the smart cities three elements; devices, fog and, cloud causes more vulnerabilities.

Three different types of security need to be ensured: network connection security, data security, and user privacy [21]. Fog's proximity to end users and locality on the edge enable it to

help address certain IoT security challenges such as updating security checks and credentials on a large number of physical devices. If an update is available, it will be much more feasible and reliable for the devices to get this update through its nearest fog server instead of connecting to the cloud all at once.

The fog nodes also can work as an authentication layer between the end devices and the cloud to apply some sort of access control over the services and data. On the other hand, fog layer could be used as an extra layer of protection to source limited devices which cannot execute complex security algorithms.

More importantly, using fog ensure that users will take possession of their own data locally, and eliminate the need of transmitting sensitive data for processing. If remote processing is needed, these data could be always processed at a secure local fog server. The authors in [22] proposed a layered security architecture where, security related decisions are taken at various levels depending on their complexity. IoT devices collect data from the physical surroundings, and takes basic security decisions, while the middleware take more advanced decisions on whether data should be processed on fog or cloud. The middleware is responsible of access control, authentication, security profiles and data privacy and protection.

IV. LoRAWAN COMMUNICATION AND SMART CITY APPLICATIONS

The whole smart cities functionality depends on the wireless technologies that are used to provide data access to the end devices. This is particularly crucial when the application scenario involves services that require urban-wide coverage, as in typical smart city. Initially, wireless cellular networks were used since they are able to provide reliable coverage. Lately, cellular standardization bodies such as the third-generation partnership project (3gpp) is attempting to support IoT applications by implementing cellular IoT (CIoT) architecture and standardizing protocols such as LTE-M and LTE-NB. However, the cellular network standards, were not designed to provide machine-type services to a massive number of devices. The potentially huge number of IoT devices asking for connectivity through a single Base Station (BS) would raise new issues related to the signaling and control traffic, which would affect the existing users and the quality of the original services provided by the cellular networks. The all-IP architecture of the latest generations of cellular standards result in the same set of issues discussed related to cloud architecture.

A promising alternative solution is Low-Power Wide Area Networks (LPWANs). These kinds of networks exploit sub-GHz, unlicensed frequency bands and are characterized by long-range radio links and star topologies. The end devices, indeed, are directly connected to a unique collector node, generally referred to as gateway, which also provides the bridging to the IP world. The architecture of these networks is designed to provide wide area coverage and ensure the connectivity also to nodes that are deployed in very harsh environments [5].

On the other hand, IoT devices are typically, small in nature and equipped with a group of sensors. In order to operate these devices, a continuous source of energy is constantly required, which poses a significant challenge in terms of battery life and cost. To address these issues in IoT-based smart cities, the devices must feature low power consumption at very low cost. And, one of the major challenges in connectivity in smart cities is ensuring connectivity to massively deployed devices in the absence of communication networks [1].

LoRa was first introduced as a new physical (PHY) layer LPWAN solution [23]. It has been designed and patented by Semtech Corporation. Its PHY is a derivative of *Chirp Spread Spectrum* (CSS) where the innovation consists in ensuring the phase continuity between different chirp symbols in the preamble part of the physical layer packet, thus enabling a simpler and more accurate timing and frequency synchronization, without requiring expensive components that generate a stable local clock in the LoRa node.

The technology employs a spreading technique, according to which a symbol is encoded in a *longer sequence of bits*, thus reducing the signal to noise and interference ratio required at the receiver for correct reception without changing the frequency bandwidth of the wireless signal. The length of the spreading code can be varied, thus making it possible to provide variable data rates, giving the possibility to trade throughput for coverage range, or link robustness, or energy consumption. The system has been designed to work in the 169 MHz, 433 MHz and 915 MHz bands in the USA, but in Europe it works in the 868 MHz band [24].

LoRa protocol lies in the Low-Power Wide Area Networks (LPWANs) category. And, the rest of the protocol stack, known as LoRaWAN, is open, and its development is carried out by the LoRa Alliance, led by IBM, Actility, Semtech, and Microchip.

The LoRa network is typically laid out in a star-of-tars topology, where the end devices are connected via a single-hop LoRa link to one or many gateways that, in turn, are connected to a common network server over IP protocol. Figure 3.

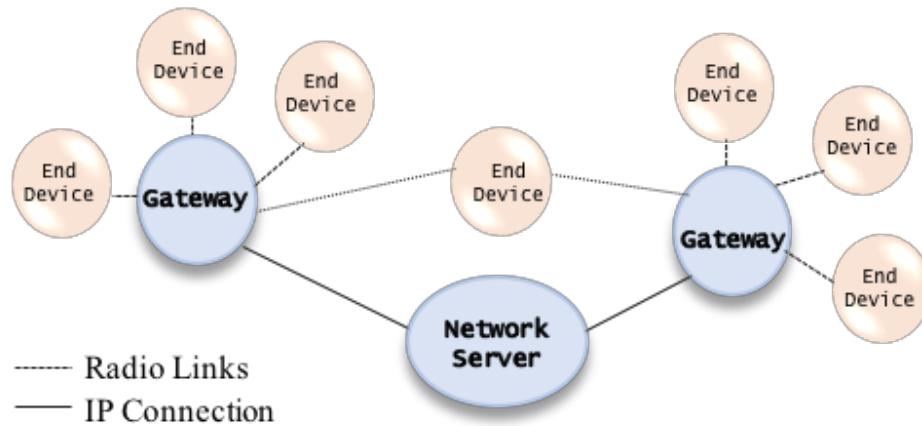


Figure 3. LoRaWAN network Architecture

LoRa end devices could operate in three different transmission profiles, denoted as A, B, and C. The key difference between these profiles is the trade-off between latency and power consumption as shown in Figure 4. Class A defines the default functional mode of the LoRa networks and is mandatorily supported by all LoRa devices. Class A networks are mainly intended for monitoring applications. In a Class A network, transmissions are always initiated by the end devices, in a totally asynchronous manner. After each uplink transmission, the end device will open two reception windows, waiting for any command or data packet returned by the server.

Class B is for battery powered actuators where uplink and downlink transmissions are equally needed. Class B end devices synchronize with the server by beacon packets which are broadcasted by Class B gateways and can hence receive downlink data or command packets in specific time windows. Finally, Class C is defined for end devices with no energy constraints. Which means that such devices can keep their receive window open at all times.

LoRaWAN utilizes two layers of security: one for the network and one for the application. The network security ensures authenticity of the node in the network while the application layer of security ensures the network operator does not have access to the end user's application data. AES encryption is used, with the key exchange utilizing an IEEE EUI64 identifier.

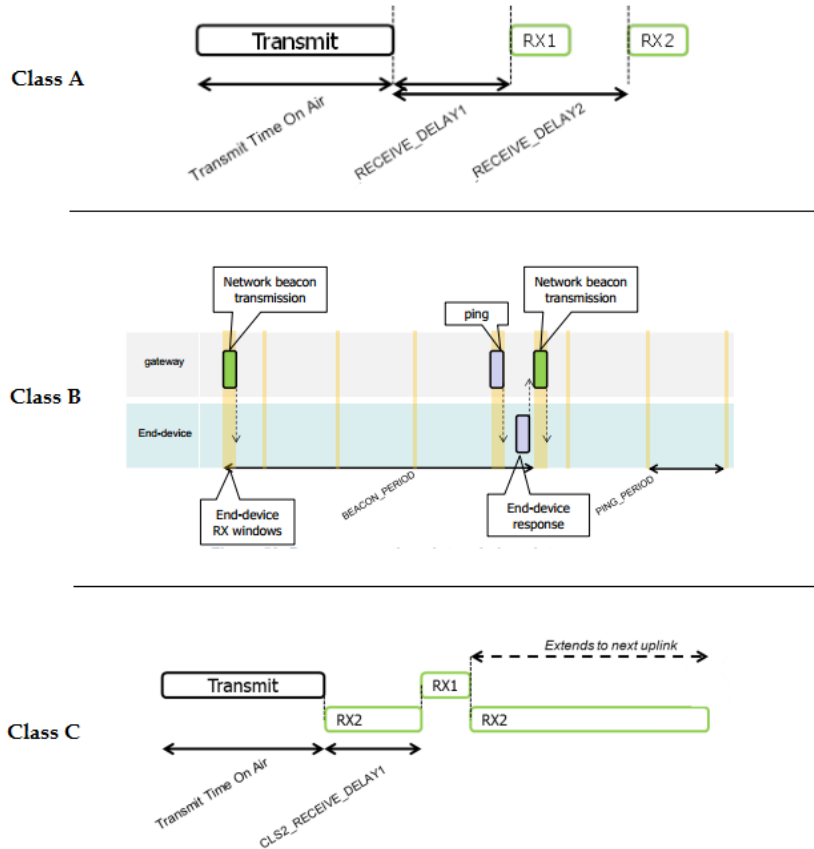


Figure 4 LoRa end-devices reception slot timing in different classes

LoRaWAN technology, as appears in the taxonomy in [25] is the fundamental modern technologies that enables connectivity among heterogeneous smart devices, with very low power, secure bidirectional communication and for the longest range among its group of protocols. Deploying LoRaWAN in smart cities employs a spreading technique, which reduces the signal to noise and interference ratio required at the receiver for correct reception. Also, LoRaWAN covers a cell of 2 km radius, using the lowest bit rate at cell edge.

LoRaWAN was used for device to device (D2D) communication scenario in [26], the authors noted that using LoRaWAN reduces the time and energy for data transfers between the involved devices. Another scenario was proposed in [27] where the authors established an experiment to evaluate the latency and coverage performance of their proposed latency and coverage optimized data collection (LCODC) scheme based on a LoRaWAN network of vehicle to vehicle communication. The authors showed that LoRaWAN reduces the latency while guaranteeing an acceptable coverage rate. The authors in [5] deployed a private LoRaWAN network in a large and tall building of nineteen floors in Italy for a proof of concept of the capabilities of LoRaWAN

networks. The installation included the integration of a LoRa network server with a monitoring application and with the databases already in use.

The authors tested the network performance in terms of coverage, data rates, security and power consumption and have shown that the LPWAN paradigm should be intended to complement current IoT standards as an enabler of smart city applications, which can greatly benefit from long-range links.

V. CASE STUDY: FOG COMPUTING AND LORAWAN IN WATER DISTRIBUTION NETWORKS

Smart water management is considered one of most important application of future smart cities [2]. A smart water system is expected to help monitor city-wide water consumption, distribution, and prediction of future water use. Such systems can ensure more sustainable management of one of our most precious natural resource. More specifically, monitoring of the city-wide water distribution networks can reduce non-revenue water losses that accounts for around 40% of the water pumped in water networks [28]. This can be achieved by a combination of real-time hydraulic parameter monitoring and leakage and burst detection algorithms [29].

The structure of a typical water distribution network is composed of multiple isolated District Metering Areas (DMAs). Figure 5 shows a typical DMA area in Hurghada Egypt. The monitoring of the network is achieved via installing hydraulic sensing nodes at different valve chambers across the DMA. Data analytics algorithms are applied to the real-time measurements of the sensors in order to optimize network operation and detect any abnormal events.

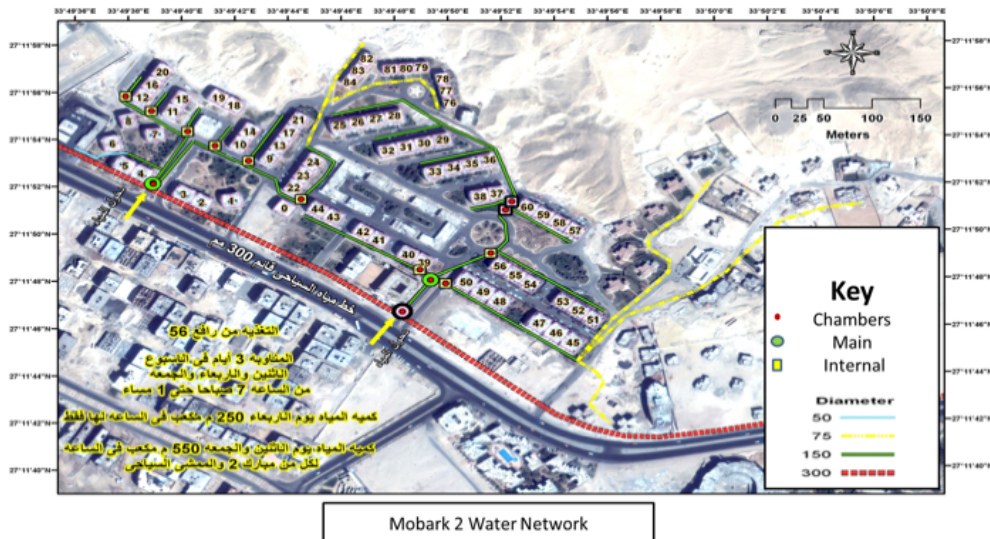


Figure 5. A pilot District metered area (DMA) in Hurghada, Egypt [29]

In the case of smart water networks, combining fog computing and LoRaWAN paradigms can offer an integrated solution that can enhance the performance, and solve few problems that face current deployment of such systems.

In such scenario, the proposed network architecture is a simple version of the LoRaWAN architecture in addition to edge node servers. It follows a star of stars topology, where the sensing nodes of each DMA group are connected to a single DMA LoRa gateway and an Edge server. All the DMA gateways are connected to a LoRa network server that is connected to a local database and communicates with an application server located on the cloud.

The sensing nodes consist of hydraulic sensors equipped with LoRa interface. They are limited resources nodes that are responsible for sensing hydraulic parameters such as pressure, flow, and water quality, in addition to simple data compression and communication with the DMA LoRa gateway using a class A profile. The DMA gateways collect data from their associated sensing nodes and send it to its associated edge node server. The edge servers are responsible for data reconstruction and local storage. It performs local DMA data processing and use secure transmission to transfer to the cloud any data crucial for the network.

The LoRaWAN network-server component, responsible for managing the state of the network. It has knowledge of devices active on the network and is able to handle join-requests when devices want to join the network. LoRa network server provides an API which can be used for integration or when implementing your own application-server. Finally, the application cloud server provides a web-interface and APIs for management of users, organizations, applications, gateways and devices, it also provides the water utility users with the required performance monitoring and event alarms.

The aforementioned architecture can offer several advantages over existing smart networks systems as follows:

- *Sensing node structure*

A major advantage of the proposed architecture is the reduction of the power, storage, and computational requirements of the IoT sensing nodes. Such nodes are usually installed at underground manholes and valve chambers, which may not be easily accessible. The isolated structure of these locations poses a connection problem for general cellular services. Using LoRaWAN communication protocol instead of accessing the cloud through cellular modules is expected to reduce the nodes power consumption significantly. The sense and forward architecture

of the nodes also eliminate the need for local storage of the measurements, and thus reduce the computational needs of the node.

- *Security and Privacy*

One of the main advantages of fog computing is its potential to eliminate the need for continuous transmission of sensitive data on cloud servers. Real-time water usage pattern is considered private consumer data that can reveal many information about the DMA residents. Through using fog computing, the user and DMA real-time measurements are stored and analyzed at the DMA fog server. Only critical events are transmitted to the cloud server, ensuring the network privacy.

From security point of view, it is much easier to deploy complicated security protocols on the connection between the fog and cloud servers as compared to establishing direct connections between the sensing nodes and the cloud. With the fog layer acting as an authentication center between the nodes and the cloud

- *Low Latency burst detection*

In classical IoT water monitoring, it is typical for the sensing nodes to store periodic measurements and then transmit the data once a day for cloud processing. A business scenario arising from the need to reduce the power consumption of the nodes, However, such model results in delayed burst detection. The low latency characteristics of the proposed fog-LoRaWAN architecture provides better alarming performance in case of burst. It also features a buffer that balances between low latency services at the fog node and high processing demanding services at the cloud.

CONCLUSION.

In this paper, we have addressed some of the challenges facing cloud-enabled sustainable smart cities, and the potential solutions offered by the emerging fog computing and LoRaWAN technologies. We proposed a combined fog-LoRa network architecture that combines the advantages of the two technologies for smart cities applications. We customized the proposed paradigm for a case study of smart monitoring of water distribution networks.

REFERENCES

- [1] Yasir Mehmood, et. al, "Internet-of-Things-Based Smart Cities:Recent Advances and Challenges," *IEEE Communications Magazine* , 2017.
- [2] Perera Charith, et. al, "Fog Computing for Sustainable Smart Cities: A Survey," *ACM Computing Surveys*, 2017.
- [3] H. Ahvenniemi, et. al, "What are the differences between sustainable and smart cities?," *Elsevier*, 2016.

- [4] S. Talari, "A Review of Smart Cities Based on the Internet of Things Concept," *Energies* , 2017.
- [5] Marco Centenaro, et. al, "Long-Range Communications in Unlicensed Bands: the Rising Stars in the IoT and Smart City Scenarios," *IEEE Wireless Communications*, 2016.
- [6] Anu Ramaswami, et. al, "Meta-principles for developing smart, sustainable, and healthy cities," *Science*, 2016.
- [7] Ibrar Yaqoob, et. al, "Enabling Communication Technologies for Smart Cities," *IEEE Communications Magazine*, 2017.
- [8] Paola G. Vinueza Naranjo, et. al, "FOCAN: A Fog-supported Smart City Network Architecture for Management of Applications in the Internet of Everything Environments," *Journal of Parallel and Distributed Computing*, 2018.
- [9] Nam Ky Giang, et. al, "Developing IoT Applications in the Fog: a Distributed Dataflow Approach," in *IEEE IoT*, 2015.
- [10] Mattias Höjer and, Josefin Wangel "Smart Sustainable Cities: Definition and Challenges," *Springer*, 2015.
- [11] Mung Chiang and, Tao Zhang "Fog and IoT: An Overview of Research Opportunities," *IEEE Internet Of Things Journal*, 2016.
- [12] Flavio Bonomi, et. al, "Fog Computing and its Role in the Internet of Things," *Cisco Systems Inc.*, 2012.
- [13] Shanhe Yi, et. al, "A Survey of Fog Computing: Concepts, Applications and Issues," in *IEEE Xplore*, 2015.
- [14] Luis M. Vaquero and, Luis Rodero-Merino, "Finding your Way in the Fog: Towards a Comprehensive Definition of Fog Computing," *ACM SIGCOMM*, 2014.
- [15] Charith Perera, et. al, "Fog Computing for Sustainable Smart Cities: A Survey," *ACM Computing Surveys*, 2017.
- [16] Ranesh K. Naha, et. al, "Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions," *IEEE Access*, 2018.
- [17] Carla Mouradian, et. al, "A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges".
- [18] Pengfei Hu, et. al, " Survey on fog computing: architecture, key technologies, applications and open issues," *Journal of Network and Computer Applications*, 2017.
- [19] Shanhe Yi, et. al, "Fog Computing: Platform and Applications," in *3rd Workshop on Hot Topics in Web Systems and Technologies*, 2015.
- [20] Alessio Botta, et. al, "Integration of Cloud Computing and Internet of Things: A Survey," *Future Generation Computer Systems*, 2016.
- [21] Ivan Stojmenovic and, Sheng Wen, "The Fog Computing Paradigm: Scenarios and Issues," in *Federated Conference on Computer Science and Information Systems*, 2014.
- [22] Wissam Razouk, et. al, "A New Security Middleware Architecture Based on Fog Computing and Cloud To Support IoT Constrained Devices," in *International Conference on Internet of Things and Machine Learning* , 2017.
- [23] F. Sforza, "Communications system". US Patent 8,406,275, Mar. 2013.
- [24] LoRa Alliance, Inc., LoRaWAN™ 1.1 Specification, 2017.
- [25] Ibrar Yaqoob, et. al, "Enabling Communication Technologies for Smart Cities," *IEEE Communications Magazine*, 2017.
- [26] Marine LORIOT, et. al, "Analysis of the use of LoRaWan technology in a Large-Scale Smart City Demonstrator," *IEEE Xplore*, 2017.
- [27] Yixuan Xu, et. al, "A Latency and Coverage Optimized Data Collection Scheme for Smart Cities Based on Vehicular Ad-Hoc Networks," *Sensors*, 2017.

- [28] Food and A. organization of the United Nations. The state of food security and nutrition in the world 2017. [Online]. Available: <http://www.fao.org/economic/ess/ess-home/en/>
- [29] M. Afifi, M. F. Abdelkader and A. Ghoneim, "An IoT system for continuous monitoring and burst detection in intermittent water distribution networks," 2018 International Conference on Innovative Trends in Computer Engineering (ITCE), Aswan, 2018, pp. 240-247.
doi: 10.1109/ITCE.2018.8316632