Preventive Maintenance of Critical Infrastructures using 5G Networks & drones

Prof. Theodore Zahariadis,
Ass. Prof. Lambros Sarakis
Eleftherios Tsampasis, MSc
TEI of Sterea Ellada
Pscahna, Chalkida, Greece
Zahariad|sarakis@teiste.gr

Dr. Artemis Voulkidis
Power Operations Ltd
1st King Av., London, UK
voulkidis@power-ops.com

Dr. Panagiotis Karkazis
Dr. Panagiotis Trakadas
Synelixis Solutions
157 Perissou, N.Chalkidona, Greece
pkarkazis|ptrak@synelixis.com

Abstract

The massive deployment of IoT devices, broadband and mission critical services are paving the way for 5G communication networks, which will enable massive capacity, zero delay, elasticity and optimal deployment, enhanced security, privacy by design and connectivity to billions of devices with less predictable traffic patterns. This paper targets a very important and demanding application the Preventive Maintenance as a Service in Critical Infrastructures and more precisely in the energy (electricity and gas) transmission and distribution network that combines the 5G technology with secure IoT and drones flight control. In more details, it addresses the 5G advances at the edge network and proposes a number of VNFs to support surveillance using swarms of drones.

1. Introduction

The massive deployment of IoT devices, broadband and mission critical services along with a huge variety of scenarios, ranging from smart city to factory automation, are paving the way for a novel and disruptive 5G communication network, which will enable massive capacity, zero delay, faster service development, elasticity and optimal deployment, less energy consumption, enhanced security, privacy by design and connectivity to billions of devices with less predictable traffic patterns. Accordingly, the next generation network should be capable of handling the complex context of operations and support the increasingly diverse set of new and yet unforeseen services, all of them with extremely diverging requirements, which will push mobile network performance and capabilities to their extremes. Additionally, it should provide flexible, yet smart and scalable adaptation and/or association of the available network resources to the specific requirements of the supported services, enabling a dramatic paradigm shift from CAPEX to the OPEX "Everything as a Service" driven business models [1].

Despite a variety of software frameworks and reference architectures have already made available for 5G enabling technologies, there is still a clear gap to bridge for 5G seamless deployment within a number of "vertical" sectors, which pose significant new requirements. Among others, the energy "vertical" represents one of the most demanding "use/test case" for 5G enabling technologies, mainly due to the need of addressing a huge range of very diverse requirements across a variety of applications (stringent capacity for massive smart metering/AMI services versus stringent latency for supervisory control and fault localization). In particular "last mile" of the smart energy network has the highest potential for demonstrating the added value of the 5G unified approach.

This paper targets a very interesting application that combines the 5G communication networks technology with drones flight control and visual analysis in order to provide Preventive Maintenance as a Service (PMaaS) in the energy (electricity and gas) transmission and distribution network. In more details, it addresses the 5G advances at the edge network and proposes a number of VNFs (Virtual Network Functions) to support surveillance using swarms of drones.

1.1. Critical Infrastructures' Predictive Maintenance

Distributed generation plants, energy transmission and distribution networks, like electricity cables and electrical isolators, and natural gas/ Liquefied Natural Gas (LNG) tanks, pumps and pipelines, are considered critical infrastructures that need extensive surveillance. Predictive Maintenance of critical infrastructures is an activity of utmost importance not only due to the high accompanying cost, but also in achieving extended protection including highest power network reliability [2].

Recently, the Energy industry started to adopt manually driven UAVs/Drones to perform visual inspections, but special flight control certification has been necessary and the time required for such operations is, still, hindering wide adoption; using manually driven drones, an electricity transmission network may need to be traversed three or four times as each electricity transmission

978-1-5386-2939-0/17/$31.00 © IEEE

network has at least one power line for each electrical phase and a safety lightning protection cable, often with fibre optics inside, for communication purposes.

Low-delay, 5G-enabled PMaaS using swarms of drones may significantly help in more efficient operation, accidents avoidance and fast restoration of energy networks, leading to reduced maintenance costs and increasing the QoE offered by the Utilities to the citizens.

However, controlling drones' swarms require complex, bandwidth demanding, computationally heavy and time critical applications, meeting a) *operational requirements*, such as to define the flight plan for each drone in a swarm, so that they have optimal coverage with minimal resources, taking into account the flight capability of each UAV/drone and the remaining energy, b) *communication requirements*, either by cellular or satellite links controlling the drones flight and uploading captured video and c) *mission requirements*, such as object (i.e. lines, pipes, tanks, blades, towers) video analysis and inspection.

We believe that the envisioned 5G network architecture and the described extended Mobile Edge Computing (xMEC) device addresses these requirements. Yet, it is fundamental to understand how security and privacy solutions are able to support the lifecycle of Critical Infrastructures IoT applications. Particularly, how different security and privacy solutions or components, which are defined in their respective systems or contexts, can be used in a harmonised way to support the design and deployment of secure IoT applications. To this, H2020 project ARMOUR[1] has created procedures to test and validate the migration and the extendibility of IoT applications from the security and privacy viewpoints especially considering uses in a large-scale IoT, e.g. considering various sensor types (from static nodes to robots), the migration aspects (from one release to another of the IoT application) or the level of crypto-agility.

2. Envisioned Network Architecture for 5G

In order to realize the PMaaS scenario along with a number of other mission critical applications, we foresee the 5G Network Architecture shown in Figure 1. At the lower level, we may see the smart energy (electricity & gas) layer, composed of varying energy infrastructure assets. This layer covers the complete energy network on one hand from electricity production, transmission and distribution down to the smart meters and EV chargers and on the other hand, the GAS/LNG network of pipes and critical infrastructures (storage, vaporization, reticulation). Over this layer, we consider the telecommunications network, compiled of cellular and mini-cells, IoT and satellite communications. Finally at the higher layer, we consider the 5G architectural and application layers.

Following the 5G Architecture vision, we propose a number of VNFs offering Infrastructure as a Service (IaaS), Self* functions (such as self-discovery, self-configuration, self-healing etc.) and smart energy specific VNFs. At the higher later, we introduce mechanisms such as xMEC routers for offloading computationally heavy functions, elastic VNF sizing and chaining, Machine-to-Machine (M2M) and Machine-Cloud-Machine (MCM) communications and trusted Plug 'n' Play functions.

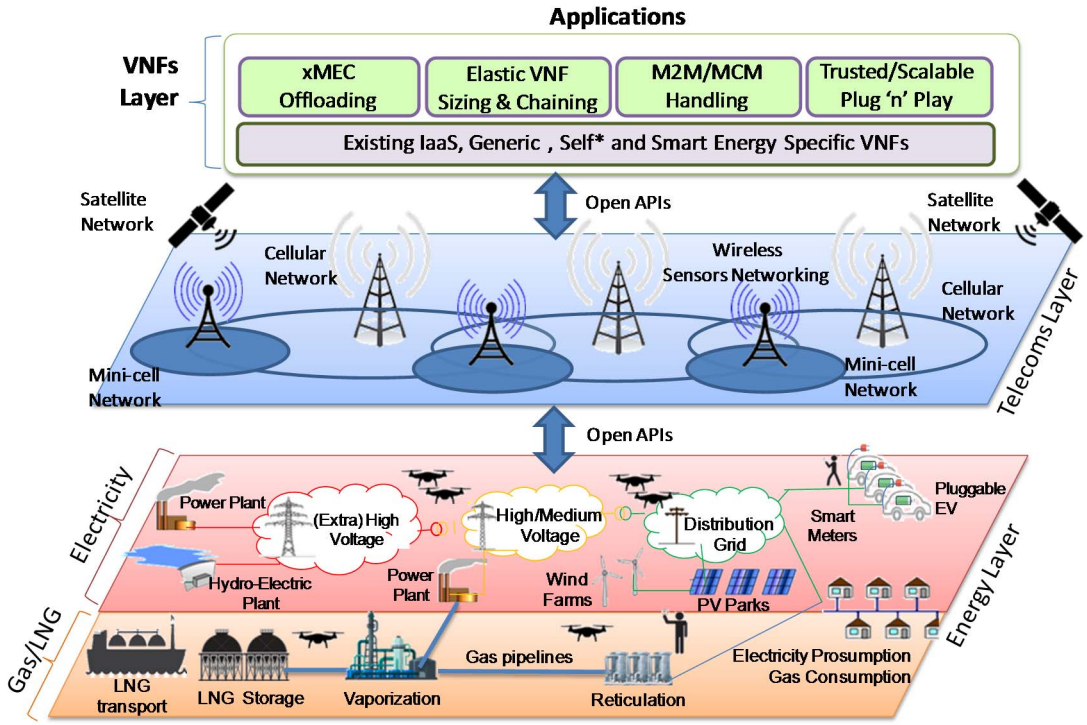

Figure 1: 5G Network Architecture for Predictive Maintenance as a Service

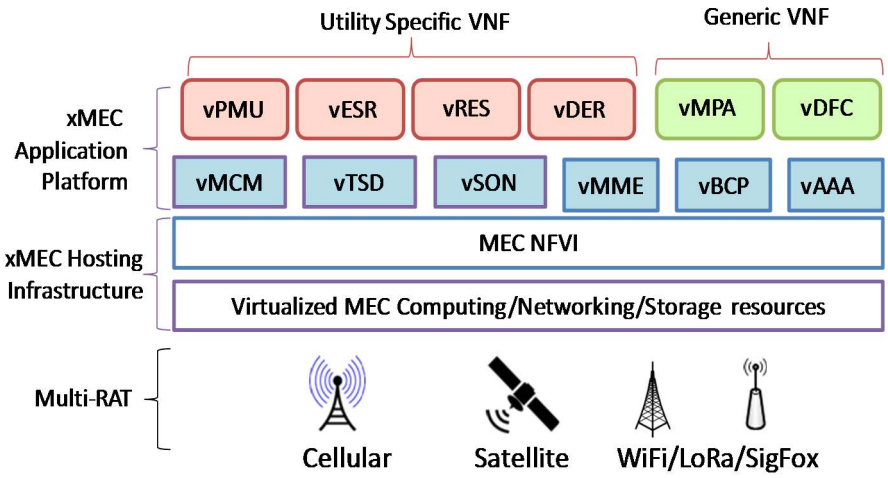

Figure 1: The proposed xMEC protocol stack

2.1. The 5G xMEC device

Controlling a drone (or even a swarm of drones) is a quite complex and processing intensive task. Moreover, automatic surveillance of the electricity network in order to follow the wiring needs extensive video processing. To enable the PMaaS, we propose to expand the ETSI Mobile Edge Computing (MEC) [3] concept create a trusted Multi-RAT extended MEC (xMEC) enabling process offloading from hardware constrained devices to the edge-cloud infrastructure. At execution time, an offloading decision will be taken, based on the remote node and xMEC status (e.g. CPU load, memory, network delay, etc), policies and license agreements. xMEC will employ fault-tolerant replication techniques, to re-execute any failing task execution, if this is feasible due to time constraints. Likewise, the xMEC system will be able to recall any incident, and modify the permissions granted to a migrated service or even revoke access to previously stored data.

As shown in Figure 2, the proposed xMEC will realize as a collection of basic VNFs that enable Machine Cloud Machine communications and virtual resource representation (vMCM), Terminal Self-Discovery (vTSD), Self-Organizing Networking (vSON), while VNFs such as the virtual Mobile Management Entity (vMME) will provide for idle mobile devices paging and tagging. Other application platform VNFs will offer Blockchains Processing (vBCP) and Authentication, Authorization and Accounting (vAAA) services, which we consider quite important for the provision of 5G based services.

The xMEC will also support utility specific VNFs such as virtual Phasor Measurement Unit (vPMU) to provide measurements of the energy network health, virtual Renewable Energy Sources (vRES) and virtual Distributed Energy Storage (vDES) to control the relevant generation and storage resources and virtual Electricity Substation & Rerouting (vESR) to offer energy rerouting in case of energy network unbalance or need to maintain the network.

Last but not least we consider a Virtual Drone Flight Control (vDFC) VNF to remotely control the drone (or the drones swarm) and a virtual Media Processing & Analysis (vMPA) on one hand to support the drones flight control and follow the energy network and on the other to support the PMaaS service,by providing feedback to the Utility control centre.

3. Offloading Drones flight control

It has been showcased [4] the capability for an drone to sense the surrounding, compute its trajectory that avoids nearby obstacles while flying towards the original destination using a real-time trajectory generation layer based on model predictive control schemes. We will continue to take on the challenging topics by providing solutions to real world problems that require more than one autonomous system to perform their missions with minimal human intervention. Such goals require the capability of the autonomous systems to sense, reason, and act in a highly intelligent manner. Moreover, the formation flight is the primary movement technique for the drone teams: it establishes a coordinated formation to achieve flight integrity with less power consumption, increasing the possibility of a mission's success [5]. Finally, system identification techniques and control of rotorcraft-based unmanned aerial vehicles (RUAVs) enhance autonomous formation flight [6]. Yet, these techniques are quite complex leading to significant energy consumption and quite expensive CPUs on the drones.

Autonomous navigation, obstacle avoidance, landing, and flight formation in the context of PMaaS should be considered from several factors: accurate positioning, sensor fusion, sensing arbitrary terrain, and real-time operation. Yet, the objective of this paper is not to report

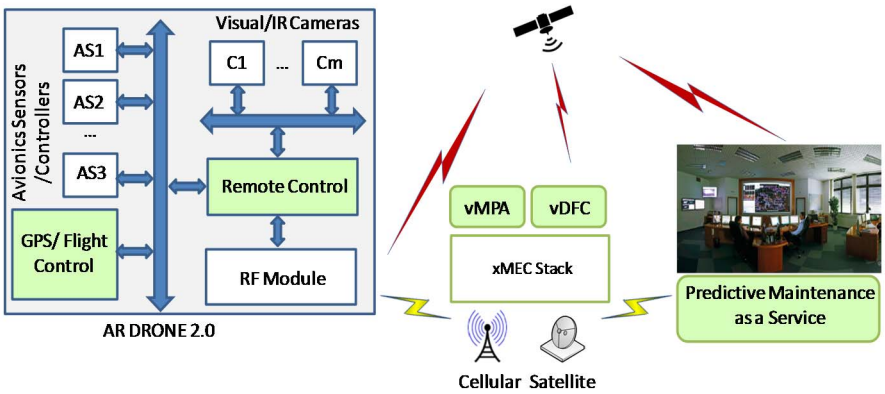

Figure 2: Predictive Maintenance as a Service Architecture Reference implementation

on these areas, but instead to focus on the off-loading of drone's on-board computer, migrate the visual and ultra-sonic analysis at the MEC using relevant media analysis VNFs (vMPA), continually evaluate and analyze the observed terrain to determine sites tolerable for landing or performing flight from a constant attitude.

3.1. Reference Implementation

Figure 3 shows an initial design and reference implementation of the PMaaS as proof of concept. As drone, the Parrot AR Drone 2.0 GPS Edition has been preselected. Though low-cost, Parrot AR Drone offers great stability and remote video streaming of flight. Moreover, it is an open source solution that offers SDKs for IoS, Android, Linux and Windows, both for the flight control and for the on board video camera.

We propose to modify the GPS/Flight Control and the Remote Control module so that computing complexity tasks to be offloaded to a reference xMEC, while vMPA and vDFC VNFs will also run on the xMEC.

In more details we consider:

- a virtual ***Media Processing & Analysis (vMPA) VNF*** able to perform real time video streams processing and analysis. Though this VNF will be specialized for energy infrastructures-related video processing, it will be generic enough to be used for generic video processing and analysis, complementing existing VNFs such CISCO's Virtualized Video Processing VNF [7].

- A ***virtual Drones Flight Control (vDFC)*** VNF able to perform real time autonomous control of drones. This VNF will also be quite generic, as it may be used for applications such as precision agriculture, security monitoring of critical infrastructures and crown management.

Both VNFs will reside at the xMEC so that applications hosted on drones may migrate tasks from their embedded processor to the edge cloud accelerator, sense the traffic demand and the mobility/distribution of the drone swarms. Additional vMPA and vDFC instances may be deployed and/or their resources may be dynamically scaled-up in locations where there is an increased traffic processing demand. In this way, the access and especially the backhaul network capacity is preserved, thus offering the capability to the network infrastructure to allow remote control and conserve more users/terminals, while mobile operators monetize on their access/edge resources.

4. Conclusions

This paper proposes a 5G architecture to offer PMaaS in Critical Infrastructures utilizing drones remote control, processes offloading and media processing. Part of the work has been implemented under the European Commission (EC) funded project H2020 ICT-644852 ARMOUR (http://www.armour-project.eu), while the proposed architecture will be implemented under the 5G Public Private Partnership (5G-PPP) framework and the EC funded project H2020 ICT-762013 NRG-5 (http://www.nrg5.eu). The complete framework will be validated in laboratory environment and in real life trials offered by ASM Terni (electricity network) and ENGIE (Gas/LNG network)

References

[1] 5G-PPP whitepaper: 5G Empowering Verticals (February 2016) https://5g-ppp.eu/wpcontent/ uploads/2016/02/BROCHURE_5PPP_BAT2_PL.pdf

[2] E. Tsampasis, L. Sarakis, H. C. Leligou, Th. Zahariadis, J. Garofalakis, "Novel Simulation Approaches for Smart Grids" Journal of Sensor and Actuator Networks, Vol. 5, Issue 11, June 2016, doi:10.3390/jsan5030011

[3] http://www.armour-project.eu/

[4] http://www.etsi.org/deliver/etsi_gs/NFV-EVE/001_099/005/01.01.01_60/gs_nfv-eve005v010101p.pdf

[5] A. Nemra, N. Aouf, "Robust INS/GPS Sensor Fusion for UAV Localization Using SDRE Nonlinear Filtering", IEEE Sensors Journal, vol.10, no.4, pp.789-798, April 2010

[6] D. Mellinger,N. Michael, V. Kumar. "Trajectory generation and control for precise aggressive maneuvers with quadrotors". Int. J. Rob. Res. 31, 5 (April 2012), 664-674.

[7] http://www.cisco.com/c/en/us/solutions/service-provider/virtualized-video-processing/index.html