Emergency communications leveraging decentralized swarm computing

Michail Alexandros Kourtis, Georgios Xylouris, Anastasios Kourtis
National Center of Scientific Research "Demokritos", Athens, Greece

Michael Batistatos
Department of Informatics and Telecommunications, University of Peloponnese, Tripolis, Greece

Albertos Markakis
Adrestia Private Company, Heraklion, Greece

ABSTRACT

Abstract—Reliable and ubiquitous communications, offering high data rates, low latency and supporting large numbers of connected devices, are critical requirements for modern emergency rescue missions. Multiple teams of First Responders, operating at remote areas, on rough terrain or under harsh conditions (e.g. wildfires, earthquakes, flooding etc.) need seamless connectivity to send/receive mission data and organize their operations. Decentralized swarm computing architectures offer a wide range of capabilities to enhance and accelerate edge processing for critical use case scenarios. This paper presents a converged approach on swarm computing and intelligence using Decentralized Autonomous Organizations for emergency communications, and how a swarm of drones can leverage different edge accelerators for different applications.

KEYWORDS

Keywords— Emergency communications, drones, swarm intelligence, decentralized computing, blockchain, DAO

ACM Reference Format:
Michail Alexandros Kourtis, Georgios Xylouris, Anastasios Kourtis, Michael Batistatos, and Albertos Markakis. 2023. Emergency communications leveraging decentralized swarm computing. In *Cyber-Physical Systems and Internet of Things Week 2023 (CPS-IoT Week Workshops '23), May 09–12, 2023, San Antonio, TX, USA.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3576914.3588019

1 INTRODUCTION

Aimed at addressing concurrently multiple requirements coming from different services and operational objectives, 5G introduces the concept of network slicing [1], allowing network operators and carriers to split the resources of physical, or virtualized infrastructure and assign them to different applications/tenants with pre-determined criteria. More specifically, 3GPP standards define three service slice types (SST), based on the underlying services' requirements, and demands [2], [3]. These are broadly known as: (i) Enhanced Mobile Broadband (eMBB), which addresses the human-centric use cases for access to multi-media content, services and data.; (ii) Ultra-reliable and low latency communications (uRLLC): This network slice type sets stringent requirements for key performance indicators such as throughput, latency and reliability. Some examples for emergency communications include UAV control, remote assistance, transportation safety, etc.; (iii) Massive machine-type communications (mMTC): The latter network slice type is characterized by the ability to service very large number of connected devices typically transmitting relatively low data volume of non-delay-sensitive data. With respect to FRs requirements, it provisions the enhanced operation for multiple communication devices, and sensor aggregation [4], commonly required when a large number of FRs is deployed in the area of incident.

This scope in conjunction with the massive increase in device connectivity and generated data has resulted in the proliferation of intelligent processing services to create insights, exploit data in a multi-modal manner and can greatly benefit emergency communications [5]. Currently, the most powerful data processing operates in a centralized manner at the cloud, which provides the ability to scale and allocate resources on demand and efficiently. Centralized processing and cloud hosting, bound and limit their services and applications to operate in a resource restricted manner, relying usually on large single entities to provide, i) Authentication, ii) Data storage, iii) Data processing, iv) Connectivity, v) Vendor-locked environments for development and orchestration [6]. This significantly limits the user from its data governance and even identity management. Similarly, existing solutions for edge device authentication require a centralized entity to trust them and authenticate them, rendering a non-portable identification paradigm [7].

The paper presents a converged work from two European funded projects, i.e., RESPOND-A and OASEES from the respective fields, that develop a 5G-based emergency communications system for FRs and an open, decentralized, programmable edge framework for Swarm architectures. The paper is organized as follows: Section I provided an introduction and main incentive behind the research of the manuscript. Section II and III provide an overview of different modules of the OASEES and RESPOND-A architectures and a brief description. Next, Section IV provides a high layer analysis of the emergency communication design and security analysis. Finally, Section V, concludes the paper and draw future lines.

2 EMERGENCY COMMUNICATIONS ARCHITECTURE

2.1 System Concept

During large scale emergencies communications may suffer from failure, because of network overload or infrastructure damages. So, not only the citizens of the affected area cannot reach the emergency

CPS-IoT Week Workshops '23, May 09–12, 2023, San Antonio, TX, USA

ACM ISBN 979-8-4007-0049-1/23/05…$15.00
https://doi.org/10.1145/3576914.3588019

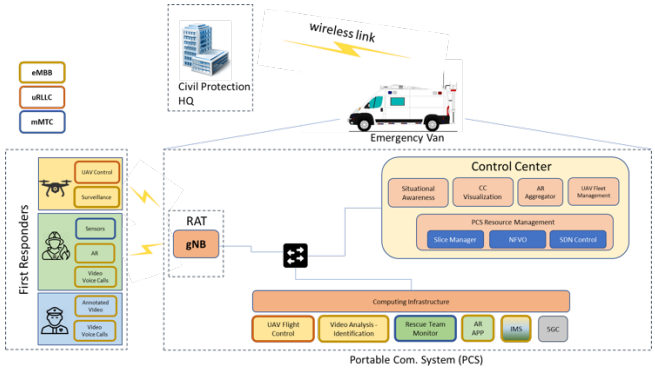

Figure 1: 5G emergency communications architecture

units and provide them with important first information about the incident, but the FR teams may also face communication problems, as the public network is likely also employed by them. On top of this, there are cases that FRs have to operate in harsh and dangerous environment, like low visibility conditions (e.g. because of smoke, dust, low light etc), toxic gas leakage or collapsed buildings, putting their life in great danger. Last but not least, when the rescue teams locate victims, they need to act fast, evaluate the victims' condition and either offer the first aids or transfer them to the hospital.

The proposed platform, depicted in Fig. 1, utilizing 5G network services and a centralized Command Center (CC) answers to the needs of FR teams. The platform is loaded on a dedicated emergency van so to quickly approach the incident area and to provide the FRs with the necessary services. The platform is not isolated in the emergency area, but it is connected to the central civil protection headquarters for better mission management. The system architecture presented in the figure depicts the key components of proposed platform, beginning from the First Responders' teams in the action field, to the PCS, which delivers on-site various Radio Access Technologies (RATs), a 5G core, a virtualized service infrastructure, and a mobile Control Center with several capabilities, e.g., Slice Manager, NFVO, Situational Awareness, etc. The communication chain is finalized with the link to the Civil Protection HQ, which provides upper layer management and coordination of the First Responder teams. Specifically the components are:

- Situational Awareness: Situation awareness is the basis for an efficient Common Operational Picture (COP), it provides required interfaces for the Command and Control Centers to display imageries and videos in control rooms using projectors, AR glasses and headsets, and also present mission specific data.
- CC Visualization: It provides the means for First Responders to explore, present and communicate visually large information spaces. By visualizing the mission space First Responders can improve their analytical reasoning and decision making through integrated and highly interactive visual interfaces and creative visualization of complex and dynamic data.
- AR Aggregation: This module collects feeds from the AR interfaces of the First Responders in the field. The AR displays various field and unit information from various sensors. The aggregation module helps to monitor the current state of on field uni
- ts.
- UAV F leet Management: The management module coordinates the UAV flight plan and operation. Dedicated UAV fleets are considered for the execution of Search and Rescue (SAR) operations. UAVs offer the capabilities for faster location of missing persons within the Regions of Interest (ROIs).
- PCS Resource Management: The resource management module is the core of the PCS platform, as it contains the orchestration services of the infrastructure. The PCS Resource Management, comprises of:
- Slice Manager : The Slice manager creates and provisions specific network slices for corresponding services required at any given scenario. In the frame of 5G, Slice Manager acts as the Network Slice Management Functions (NSMF) requesting the provision of resources from the underlying MANO (management and orchestration) components at the RAN domain, the WAN and the Computing ones. During the operation, the slice manager can intervein and re-allocate resources fulfilling the real-time needs and the objectives of the mission,
- NFVO: Orchestrates the deployment of virtualized service components according to Network Function Virtualization provisions
- SDN Control: Controls the provision of the network resources within the PCS, based on the slice type.

The computing infrastructure is exploited for the deployment of all the network applications and services, required for the particular operations. The infrastructure resources are, assigned and allocated to each specific slice serving the particular application or FR team, fulfilling their requirements:

- UAV Flight Control: At the PCS UAV communication stand at the edge of the system where different operations can take place. This specific function operates over a uRLLC slice in order to minimize control latency and optimize UAV response times.
- Video Analysis Identification: This virtualized service processes video feeds from UAVs, and other units, and performs Machine Learning powered object detection. The detected objects and subjects are automatically annotated in order to facilitate the situation assessment in the Control Center.
- Rescue Team Monitor: Each First Responder group is equipped with sensors that monitor their current health state, position, etc. This module operates over an mMTC slice as it collects and aggregates the data from multiple sensors and performs post processing in order to assess each group's state.
- AR App: AR for First Responders incorporates various enablers in a dynamic rich media interface for the responder i.e., thermal image streaming, sensor monitoring. The immersive stream is also transmitted back to the Control Center for further assessment.
- IP M ultimedia S ubsystem (IMS): This component provides the connectivity for group communication over voice and

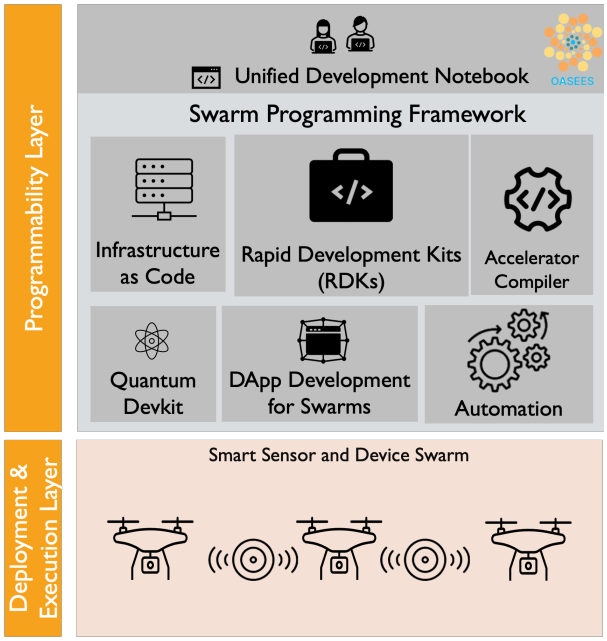

Figure 2: OASEES decentralized framework.

video among each responder group. It is the backbone of emergency communications for First Responders. As it can be deducted from the figure, it operates over the eMBB slice to address the high bandwidth requirements of the communication.

- 5G Core (5GC): This module implements the virtualized core component for 5G communications and is the basis for providing the connectivity service for multiple slices. The 5GC may be shared among slices or use separate instances per slice in case isolation is of importance.

All these different types of services are usually packaged in a centralized manner and controlled by a main entity. This may lead to service disruption in case where edge provision of services is not available. In order to address these cases the decentralized approach of another framework is presented in the next section.

3 OPEN DECENTRALIZED EDGE FRAMEWORK FOR SWARM ARCHITECTURES

OASEES aims to create an open, decentralized, intelligent, programmable edge framework for Swarm architectures and applications, leveraging the Decentralized Autonomous Organization (DAO) paradigm [8] and integrating Human-in-the-Loop (HITL) processes for efficient decision making.

The OASEES decentralized framework, shown in Fig. 2, is to provide the open tools and secure environments for swarm programming and orchestration for numerous fields, in a completely decentralized manner [9]. An important aspect in this process is identification and identity management, in which OASEES targets the implementation of a portable and privacy preserving ID federation system, for edge devices and services, with full compliance and compatibility to GAIA-X federation and IDSA trust directives and specifications [10]. This situation solidifies the need for an integrated enabler framework tailored to the edge's extreme data processing demands, using different edge accelerators, i.e. GPU, NPU, SNN and Quantum.

Another gap to be addressed is related to the ease of access from the side of the data scientists and engineers [11]. Public clouds already provide user-friendly abstractions (notebooks, simplified administration interfaces, graphical workflow designers, etc.) to data experts, so that the latter can concentrate on the management of the data and the selection and optimisation of the ML/AI algorithms, rather than on the management of the physical and virtual resources which are needed and committed. This is a feature currently missing from edge orchestration solutions.

3.1 OASEES System Concept

The OASEES stack is expected to enable the user to i) discover and select available platforms, services and capabilities pertinent to their needs; ii) develop AI services as well as automate lifecycle management operations; iii) deploy and manage AI workflows across the compute continuum; iv) configure service performance constraints; v) interactively explore data and exercise MLOps; vi) verify the integrity of infrastructure and services across the continuum.

3.1.1 *Programmability Layer.*

Unified Development Notebook OASEES. OASEES will expose a graphical User Interface / Dashboard, mainly targeting at lifecycle management operations. Through the UI, end users will be able to express their requirements, select and deploy service templates (mathing their requirements), configure data sources and sinks, monitor and terminate their services. Also, system administrators will be able to use the UI to monitor the status and health of the overall infrastructure and onboard/configure edge nodes and smart devices. All these operations will also be offered through an authenticated API to allow programmatic control and automation of OASEES functionalities. In addition to service management, OASEES will facilitate collaboration between developers by offering an interactive web-based environment (notebooks, based e.g., on Jupyter or Zeppelin platforms) to support a wide range of analytics workflows, boosted with maintainable and collaborative pipelines, tab completion and collaborative editing functionalities. This is expected to encourage third party developers to reproduce and build upon the existing work, in order to create customized applications that can be reused, shared and monetized via the EOSC Marketplace.

The OASEES SDK is built on top of an extensible set of development modules abstracting different parts of the IoT-to-edge-to-cloud spectrum, and results into a set of modules building upon them. Interaction between components will follow a message-passing paradigm (e.g., pub|sub architecture). Each of the services and components implements the interaction with particular hardware or functionality interacting with the APIs of a different cloud, network and/or edge systems. The OASEES orchestration framework is responsible for abstracting the interaction with cloud APIs (e.g., OpenStack, Kubernetes, KubeEdge), the network provision module

will abstract network system APIs (e.g., Cloud-Fog-Edge interaction), and blockchain (EVM, IoTA). Enablers for data-rich services in OASEES are dedicated hardware accelerated aware endpoints for the management and interaction with AI acceleration hardware and smart devices (via the dedicated agents). The AI acceleration and smart device interfacing will abstract the APIs as provided by highly specialized acceleration hardware such as FPGAs, AI ASICs, Quantum processors, etc.

RDKs. In addition to the Notebook approach, and complementing it, the OASEES SDK will provide a suite of tools that enables developers to create edge applications tailored to their needs. Developers will be able to select from pre-configured connectors and templates for faster integration and connectivity across their existing infrastructure. The SDK will provide Libraries in at least two languages (e.g., Python, Go) for interfacing with OASEES, as well as Data management libraries to accelerate the creation of distributed ML apps. An App Developer Guide will be provided, containing Guidelines, Patterns or Tutorials. The abstraction of the underlying hardware and capabilities will accelerate development and facilitate interoperability and portability.

Quantum Devkit. Quantum acceleration and processing for retail and IoT services and application still remains an open challenge and opportunity for different fields. Currently, a noteworthy issue in the pathway towards wider adoption remains the communication and data exchange, between quantum systems and vendor cloud and edge frameworks. OASEES in this aspect aims to develop Quantum APIs along the Edge-Fog-Cloud continuum, targeting the following stages: i) Placing of Quantum Middleware nodes, ii) Realization of a high-level programming language for Quantum Computing - programming without gates, iii) Integration of the higher-level programming language with the Quantum APIs along the Edge-Fog-Cloud continuum, iv) Realization of hybrid Quantum Machine Learning algorithms on the base of the high-level programming language for Quantum Computing, v) Tools for the systematic and Model-Driven Development of Quantum Computing algorithm. In this respect, FOKUS bringing its own Quantum processor will delve into the integration of a Quantum Devkit for Swarm applications and services at the edge. The main goal of this effort will be computation of optimized paths and interconnections (DAGs) between the different devices and swarm topologies across the different scenarios and their respective requirements.

DApp Development for Swarms. A DApp implementation framework consists of three key building elements, which we dubbed the DApp triplet. These elements are (i) a trusted decentralized ledger (i.e., network connecting a swarm in OASEES case), (ii) trusted decentralized execution of program logic, and (iii) decentralized applications. An example of a DApp triplet is a DAO network, smart contracts (SC) implemented in this network, and blockchain enabled front end applications, which provide user interfaces and run embedded IoT devices and edge/cloud accelerators. The DApp to be developed will also support natively the smart contract inference for different use case scenarios and parameters. Different technology monitoring endpoints will consume heterogeneous raw data (health vital sensors, building monitoring, electric vehicle observation, etc.) and different events and alarms will be triggered automatically through the smart contract adoption. DAO in this case will also involve the HITL decision making where for sensitive and critical events a specialist will be involved, i.e., medical practitioner, civil engineer, etc. Overall, this module will involve the convergence of different technologies and tools from blockchain, e.g., Remix, to edge device programming, e.g., Node-RED.

Edge Package Rollup. This module will focus on the packaging of the DApp to be deployed across the entire swarm in an efficient manner and its respective security. Its aim is to provide a step-by-step workflow to minimize the risks of deploying decentralized behaviours: a low-resource simulator to iterate quickly on the design and test thousands of units, followed by a more realistic full-stack software-in-the-loop environment, extended whenever available to hardware-in-the-loop validation and finally to the deployment of the behaviour in the field. Additionally, regarding the security and fortification of this process the ZK-Rollups will be integrated, a paradigm from the blockchain sector, ZK-Rollups vastly reduce the computing and storage resources required to validate blocks, by decreasing the amount of data in a transaction. This is made possible through cryptographic zero-knowledge proofs (ZKPs), whereby a party can prove that they know or have something without surrendering any information about what it is they know or have.

Accelerator Compiler. On top of the abstractions provided by the different hardware accelerators, OASEES SDK provides a collection of dedicated services to support intelligent and trusted IoT-to-edge-to-cloud services. The first step will be resource discovery, registration and pooling. This will require a hardware model and taxonomy to categorise potential acceleration mechanisms and involved hardware (e.g., FPGA, AI accelerators, smartNICs, Quantum processor), providing potential support for a wide range of "execution units", incl. containers, VMs, serverless functions, switch configurations or AI models. This task will re-investigate and possibly extend existing protocols such as OCCI , TOSCA , CloudML or ontologies models such as CoCoOn as infrastructure modelling languages.

Following, based on an enriched service model, including meta-information regarding security, QoS and intelligence requirements, these edge services provide a management component or set of system calls for: i) federation of resources, ii) monitoring of infrastructure or service resources, iii) enforcing trust and security in application services, iv) the global management of resources and platforms, and most importantly v) the lifecycle management of application services.

This set of modules and decentralized governance can be leveraged in the case of emergency and critical use cases in order to ensure continuous connectivity and leverage different capabilities deployed at the edge. An indicative convergence of both frameworks would be the creation of a critical mission DAO, where the different emergency infrastructure and connectivity enablers would be integrated in a decentralized SDK.

4 CONCLUSIONS

The paper presented a convergence approach for how emergency and critical mission applications can leverage decentralized intelligence for swarm architectures in order to enhance and accelerate

their operation. A set of two prototype frameworks was presented where the different modules of each system is detailed in each relevant scenario.

Additionally, the paper presented a set of technologies that each module utilizes and how it can enhance the operation of the entire system. As future steps, a preliminary implementation of an integrated DAO for emergency communications could operate over an SDK and assign and utilize different enablers based on the scenario of a use case.

ACKNOWLEDGMENTS

The research leading to these results has been supported by the OASEES project (no. 101092702), H2020 RESPOND-A project (G.A. no.883371) and H2020 SANCUS project (no. 952672).

REFERENCES

[1] European Commission, "5G: Challenges, Research Priorities, and Recommendations – Joint White Paper". European Commission, Strategic Research and Innovation Agenda.

[2] International Telecommunication Union – Radiocommunications Sector (ITU-R), "Recommendation ITU-R M.2083-0 (09-2015): IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond."Available at: https://www.itu.int/rec/R-REC-M.2083- 0-201509-I/en Accessed Date: 1/12/2020

[3] S. E. Elayoubi, S. Ben Jemaa, Z. Altman, and A. Galindo-Serrano, "5G RAN Slicing for Verticals: Enablers and Challenges, IEEE Communications Magazine, Institute of Electrical and Electronics Engineers (IEEE), 2019, 57, 28-34.

[4] Carlberg, K.; Burger, E. W. & Jover, R. P., "Dynamic 5G Network Slicing for First Responders", Principles, Systems and Applications of IP Telecommunications (IPTComm), IEEE, 2019.

[5] Kourtis M-A, Sarlas T, Xilouris G, Batistatos,M.C, Zarakovitis C.C, Chochliouros I.P, Koumaras H, "Conceptual Evaluationof a 5G Network Slicing Technique for Emergency Communications and Preliminary Estimate of Energy Trade-off", Energies 2021,14(21): 6876

[6] Fowler, K.: "Best practices in mission-assured, mission-critical, and safety-critical systems" in "Mission-critical and safety-critical systems handbook", pp. 1-82, Elsevier, 2010

[7] Shah Khalid Khan, Usman Naseem, Haris Siraj, Imran Razzak, Muhammad Imran, "The role of unmanned aerial vehicles and mmWave in 5G: Recent advances and challenges", Transactions on Emerging Telecommunications Technologies, Vol. 32, Issue 7, July 2021, pp e4241

[8] S. Filipčić, "Web3 & DAOs: an overview of the development and possibilities for the implementation in research and education," 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 2022, pp. 1278-1283, doi: 10.23919/MIPRO55190.2022.9803324.

[9] L. Liu, S. Zhou, H. Huang and Z. Zheng, "From Technology to Society: An Overview of Blockchain-Based DAO," in IEEE Open Journal of the Computer Society, vol. 2, pp. 204-215, 2021, doi: 10.1109/OJCS.2021.3072661.

[10] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F. -Y. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266-2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.

[11] I. Mehdi, M. Sbai, M. Mazlin and K. Azghiou, "Data Centric DAO: When blockchain reigns over the Cloud," 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 2022, pp. 1-7, doi: 10.1109/IEMTRONICS55184.2022.9795753.