Rapid Deployment of 5G Services Using Drones and other Manned and Unmanned Aerial Vehicles

Riccardo Bassoli, Fabrizio Granelli

Abstract 5G Networks are expected to introduce several breakthroughs and a big step forward towards a flexible and effective mobile network. An interesting requirement for the 5th generation of cellular networks is indeed the possibility to deploy a network in a very short time frame, indicatively 90 minutes. The purpose of this unprecedented design goal is to address scenarios of dynamic coverage requirements, especially targeted at unexpected or emergency situations.

In this framework, a research proposal is being developed at the CNIT Research Unit at the University of Trento in collaboration with Technion in Israel to define and prototype a suitable architecture to provide on-demand 5G coverage for border monitoring and disaster scenarios.

1 Introduction

5G is expected to provide a big step forward in enabling fast deployment of networks, shifting the time scale from days to hours or less. Indeed, 3GPP requirements for 5G cellular networks propose a nominal deployment time of 90 minutes. This feature will enable 5G to offer connectivity and services in novel relevant scenarios, such as border monitoring and surveillance and disaster scenarios.

In this framework, several works in the literature outlined the possibility to integrate moving BSs within the 5G infrastructure, using Manned or Unmanned Vehicles - in several cases Aerial Vehicles. Aerial vehicles provide several advantages over land vehicles due to their agility, freedom of operation and potential coverage, at the cost of limited lifetime and range of operation.

Riccardo Bassoli
DISI - University of Trento, Via Sommarive 9, Trento, ITALY, e-mail: riccardo.bassoli@unitn.it

Fabrizio Granelli
Consorzio Nazionale Interuniversitario per le Telecomunicazioni - Sede di Trento, Via Sommarive 9, Trento, ITALY, e-mail: fabrizio.granelli@unitn.it

Despite the potential benefits of unmanned aerial vehicles in applications like disaster recovery, environmental monitoring, flood area detection, and aerial surveillance of public areas, there are still several open issues to be addressed. These are mainly related to their effective usage for data/information collection, communication and processing. Moreover, regulation about data access requires an efficient selection of authorized personnel to manage sensitive information. Finally, a network of unmanned vehicles needs to adapt to unpredictable events, attacks and network dangerous states to guarantee optimal quality of monitoring experience: eventually, the network should be capable not only to detect but also to prevent dangerous network situations.

In this context, the research activities of the Dynamic Architecture based on UAVs Monitoring for border Security and Safety (DAVOSS) project (nato-davoss.org), funded by the NATO in the framework of the Science for Peace and Security Programme (funding period: 2018-2021), aim at advancing the current monitoring networks based on unmanned aerial vehicles to help to overcome some of their technological limitations, and focusing on system reliability. The project will study and design a virtualized cloud-based architecture to enhance capabilities of current border surveillance and counter-terrorist operational networks based on sensors, cameras and unmanned aerial vehicles. The DAVOSS solution will consider different kind of environments. Moreover, given its dynamic network structure and adaptability, it will provide higher security against physical attacks and natural catastrophes. The centralized structure of the architecture will allow for easier implementation of traffic measurement and anomaly detection processes, even in case of disaster forecast: its dynamic reconfiguration will optimize network performance, information management and processing, by ensuring optimal coverage to sensors and monitoring peripherals. Finally, the architecture will define and develop an appropriate wide-range connectivity functionality to provide the most suitable communication paradigm for connecting with the remote control center, via 4G/5G cellular backhaul, through the intervention of an Ultra Light aerial Vehicle (UVL) - such a small airplane, nano-satellite or blimp, multi-hop wireless mesh networking or, in a possible future scenario, the usage of satellites. In particular, lightweight flying platforms such as ULV or small satellites will represent a viable alternative to terrestrial backhaul in terms of easy and low cost deployment and robustness against attack and environmental disruption. The proposed solution will also prevent information leakage, since no sensitive military/security data will be processed at unsecure network entities. It will also possible to easily monitor the effectiveness and the efficiency of network updates since they will be performed in a centralised manner.

This chapter will present the architecture and current status of the DAVOSS 5G Testbed in Trento.

2 Related Works

The usage of advanced communication and networking infrastructures for border monitoring and emergency scenario is commonly found in the literature. In this section we review some of the most interesting approaches, focusing on the cases including WAN connectivity in addition to local coverage.

In [1], a solution based on the integration of Ku-band radar systems installed on UAVs and GNSS localization is proposed for patrolling of sea borders in the Mediterranean area. In [2], the use of aquatic drones is considered for marine safety. In these works, the focus is on the optimal sensor deployment and on the best routing approach, exploiting state-of-the-art technology and standard network configuration. Other papers, like e.g. [3] and [4] consider the use of UAVs in combination with ground sensors in order to foster and optimize the border monitoring and minimizing the false alarms. However, such approaches are not based on an effective integration of the different network infrastructures involved and still rely on human operators' intervention to work.

In [5], Kim, Mokdad and Ben-Othman analyze the design of UAV-based surveillance networks in two different scenarios: the smart city and the extensive ocean. Differentiated UAV typologies and network configurations are proposed in [5] for the two scenarios, evidencing a substantial weakness of UAV-based monitoring in terms of lack of adaptation to potential modifications of the test field.

The DAVOSS approach represents a step forward with respect to the current state-of-the-art about the use of avionic networks for environmental and border monitoring. Indeed, the flexibility and reconfigurability introduced by the DAVOSS network architecture in terms virtualization and softwarization is expected to provide a viable yet effective solution to adapt to dynamic changes of the application scenario.

3 The DAVOSS Network Concept

The DAVOSS project proposes to define a virtualized cloud-based architecture based on different types of manned and unmanned aerial vehicles, to enhance the capabilities and the reliability of current border surveillance and disaster management systems.

3.1 Global Architectural Overview

Figure 1 depicts the proposed DAVOSS architecture. The system can be divided into four main layers:

- *Layer 1* consists of the ground-level sensors and peripherals, which are devoted to different kind of sensing procedures according to the application scenario and the environment.
- *Layer 2* represents the fleet of UAVs equipped with a camera and hardware for data transmission/reception. The UAVs provide network connectivity (by acting as mobile gateways) and further monitoring functionalities both in case of disasters and border security/terrorist attacks.
- *Layer 3* provides network and resources virtualisation, and manages virtual network function assignment and slicing. This layer will implement a Software Defined Networking approach to control the connectivity and performance of the underlying mobile nodes (e.g. the UAVs), and well as Network Function Virtualization to assign or re-locate relevant processing and security functionalities.
- *Layer 4* (Wide-Area connectivity) is responsible to collect information from UAVs and to transmit it securely to the cloud servers located at the remote control center. Different solutions for communication with cloud servers will be analyzed, tested and experimented, including direct usage or mesh-based solutions for efficient usage of the existing 4G/5G cellular infrastructure as backhaul, usage of a manned ULV to collect data by the virtualized network of UAVs and sensors in a delay-tolerant paradigm, usage of satellite communication (CubeSat scenario). This layer will be the key to guarantee coverage, security, availability and reliability, in case of both disasters and terrorists threats.

The project testbed will implement a subset of the solutions at Layer 4, considered to be the best ones, but will also investigate future extension of the architecture through CubeSat or other advanced solutions.

3.2 Sensor Network Deployment Solutions

The project will study optimal Sensor Network Deployment solutions, mainly based on Low Power Wide Area Network (LPWAN) wireless telecommunication technologies [6]. The basic characteristics of this technology are: (a) ability to inter-connect battery-powered end-devices over long ranges, (b) the end-devices must operate at low power, (c) downlink and uplink traffic is at low bit rate (0.3 kbit/s to 200 kbit/s) per frequency channel, (d) the frequencies used are licensed or unlicensed , (e) proprietary or open standard protocols are used. The following technologies are the most popular: Sigfox, LoRa, NB-IOT (Narrowband IOT) , LTE-M. We examined closely Sigfox and LoRaWAN and found the main characteristics as described in Tab. 1.

Based on the above considerations, DAVOSS focuses on LoRa technology and to use LoRaWAN as the MAC protocol for the Network Deployment solution.
The technical specification of LoRa/LoRaWAN is:

- LoRa ISM Band : 868MHz - 900MHz (EU) , 902MHz - 928MHz (US);
- Ranges: 5 km (Urban) - 15 km (LoS);
- Security: Authentication and Encryption AES-128;

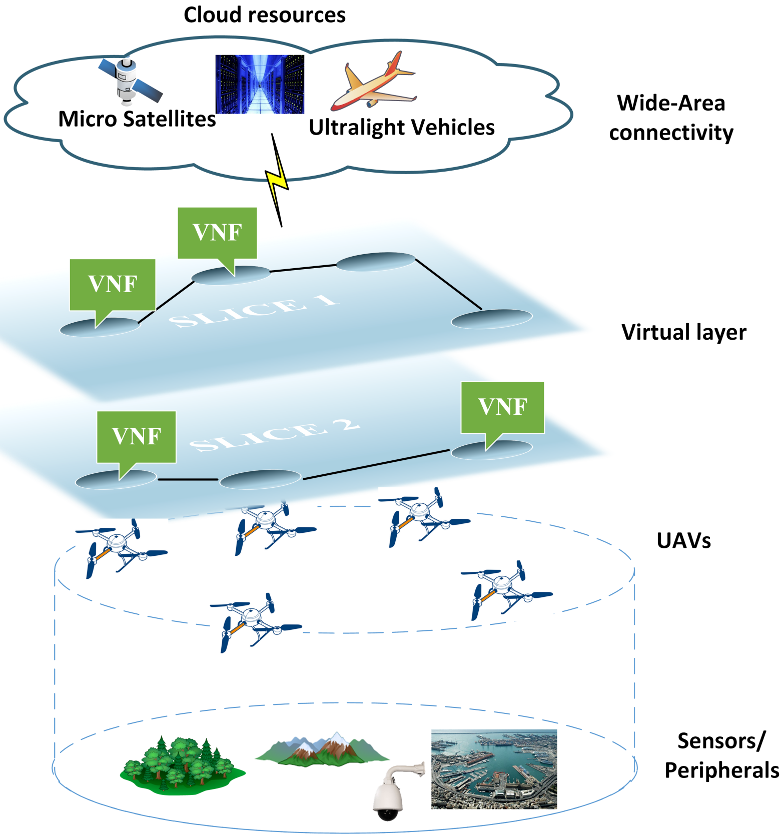

Fig. 1 Structure of the DAVOSS proposed system.

Table 1 Sigfox and LoRa standard comparison

Sigfox	**LoRa**
Narrowband (or ultra-narrowband) technology	Wide band (125Khz or more) Spread-Spectrum technology
Uses a standard radio transmission method (BPSK)	Uses on frequency-modulated chirp Wide band (125Khz or more)
Requires an inexpensive End node radio, but expensive HW at the Gateway	Both the End node and the Gateway are relatively inexpensive
Uplink quality: good, Downlink quality: Limited	Looks at a wider amount of spectrum than SigFox so can get more Interference. The larger receiver frequency bandwidth is mitigated by the coding gains
Technology and protocols from the end node to the server are not open.	Anyone can join the LoRa Alliance. LoRa Gateway spec is open. LoRaWAN which is the MAC protocol above LoRa is an open standard developed by committee. Network management spec is open.

- Data Rates: 0.3Kbps – 50Kbps.

The LoRaWAN specification version 1.1 defines 3 device classes:

- Class A devices have the lowest power consumption by opening two short receive windows after transmission.
- Class B devices extend Class A by adding slotted communication.
- Class C devices extend Class A by keeping the receive windows open unless they are transmitting.

3.3 Software Defined Networking and Network Function Virtualization

Layer 3 will aim at maximising system automation and autonomy, by providing centralised configuration, quick, reliable and secure access to information, and encapsulating information at different user's levels – thanks to key 5G technologies of SDN and slicing.

Software Defined Networking represents an emerging paradigm which enables the separation of control functionalities from traditional Internet routers in order to transform them into dumb "Switches" controlled by a central entity (namely: the SDN controller) [7]. SDN demonstrated its effectiveness in improving the control and programmability of the current packet networks. Indeed, the SDN controller, having a central and global vision of the whole network, is capable of optimizing the performance, managing in effective manner the various traffic flows and finally guaranteeing a satisfactory Quality of Service (QoS) to the users.

Virtualisation technologies will efficiently handle different kinds of traffic, with different priority. DAVOSS will provide the necessary centralised-cloud communications system. When available, other networks such as cellular networks or the Internet will also provide the required connectivity and infrastructure. Based on these communication technologies, DAVOSS also aims to exploit adaptive slicing. That will be used to bring rich computational and network resources to authorized UAVs. Authorized end users will have more information by increasing the number of information gathering nodes, real-time availability, and interoperability among systems: that is made possible by deploying dynamic slicing. With the amount and quality of information available in real-time, action will be immediately steered to the location of interest. A centralized analysis of network status, and of data about border surveillance will prevent network monitoring to fail because of attacks and lack of resources. Last, but not the least, UAVs, cameras and sensors with dynamic virtualisation and slicing will significantly reduce intensive human interaction and control.

DAVOSS virtualization approach with adaptive slicing represents a novelty with respect to the state-of-the-art. A very recent work [8] considered the use of SDN and virtualization in UAV networks. However, the SDN architecture of [8] is targeted at managing multi-path routing only, by searching for the best available path. In

DAVOSS approach, SDN and virtualization are regarded as complementary tools capable of dynamically and adaptively manage the overall link and processing resources involved in the border patrolling tasks, while ensuring the maximum possible reliability and network lifetime.

3.4 Satellite- or blimp-based Backhauling

The backhaul plays a key role in the DAVOSS network architecture. Indeed, the information acquired by the ground sensors and processed by the drone layer should be forwarded in real time to remote control stations, that may be considerably far from the monitored area. Moreover, the DAVOSS system considers scenarios where the terrestrial network connection may not be available (e.g. desert/mountain areas or open sea). For this reason, effective and reliable backhauling pays a key role in the architecture.

In this framework, the use of satellite links for long-range data transmission in emergency recovery and public safety applications is regarded as a resilient solution, whose deployment costs are limited and convenient [9]. Geostationary (GEO) satellites present very favorable coverage and availability, but, as drawback, they are characterized by high latency due to the very long distance from Earth. Low-Earth-Orbit (LEO) satellites placed at orbital heights of 500-700 Km offer reduced coverage with respect to the GEO counterparts, but also acceptable latency.

In the framework of DAVOSS research, different alternatives will be studied, involving the usage of blimps, Ultra Light Aerial vehicles or small satellites.

One of the novel solutions for long-distance backhaul will be based on the use of the CubeSat picosatellites. Nowadays, CubeSats are raising a lot of interest in the aerospace research community thanks to the reduced development and launch costs. Despite to their small amount of available volume, CubeSat missions have been proven to be very effective in high added-value applications like scientific data gathering, educational purposes and small-scale industrial equipment testing [14]. The on-board processing capabilities of CubeSats are not so limited as one can expect. Indeed, the use of dedicated processors, based e.g. on FPGA technology [15], allows to perform on-board image processing [14] [15] with fully-affordable power consumption. As far as communication aspects are considered, considerable research efforts have been done in order to overcome the bottleneck of low-rate standard radio interfaces, like e.g. AX-25 or similar variants [16], capable of providing small throughput of the order of 9.6 Kb/s. In [16], an X-band CubeSat communication system, compatible with the NASA Near Earth Network,offering a downlink data rate of 12.5 Mb/s has been implemented and tested. In [17], a prototype of 2.4 GHz High-Data Rate (HDR) radio for CubeSat has been implemented, able at supporting a topic data rate of 60 Mb/s. We believe that these last numbers and consideration can fully justify the CubeSat solution for DAVOSS long-range communication, thus solving the tradeoff between costs and coverage (the footprint diameter of a single CubeSat is well enough for DAVOSS purposes).

Nevertheless, CubeSats will be considered in the design and simulation phases of the project, and for future implementations of the project. DAVOSS testbed and proof-of-concept will be based on locally available alternatives for backhauling, including LTE/5G, Ultra Light Aerial Vehicle and Helium-based Blimps.

4 DAVOSS Network Design Preliminary Assessments

This section presents some preliminary results of the model used for analyzing the DAVOSS networking infrastructure, focusing on the key aspects of energy consumption and virtualization of BBUs. In particular, the analysis is focused on comparing the different alternatives of re-location of BBUs: at UAVs, at geostationary satellites, or at CubeSats. The model is based on stochastic geometry, in order to calculate the variation of the average number of v-BBUs and the impact of virtualisation on the power consumption of the system.

In order to provide a realistic data of BBUs, the technical specifications of the Ericsson-Baseband-5212-5216 [10] are used. However, the generality of the model allows the correct use of any BBUs' data sheet. The average traffic provided constantly by peripheral sensors is set to 500 kb/s.

The deployment of virtualisation allows proper optimization in a dynamic networking scenario, in which only v-BBUs are considered, which are activated according to network and traffic requirements. This does not happen in current monitoring networks based on 4G/LTE, where each active mobile base station must always host an active BBU or the split between BBUs and RRHs is performed a-priori.
Given $\lambda_{bs} = 30$ AP/km^2 and $\lambda_s = 900$ peripherals/km^2, this means that a 4G/LTE-based monitoring network maintains active 30 BBUs/km^2. The energy consumption of a BBU can be estimated to be 3 W for pico cells mobile BSs [11].

Fig. 2 shows the Voronoi tessellation of a unit of area to depict the properties related to coverage.

Given these premises, the value of peripherals that a mobile BS has to serve, with higher probability, is 22.

The resulting relationship between weight of the drone (mobile BS) and the power consumption is depicted in Fig. 3. In particular, the gain is calculated in respect of mobile BSs, which carry BBU weighting less than 4 kg.

Let's consider the possibility to re-locate the BBUs within geostationary satellites. For the considered border area, it has to handle $\lambda_{bs} A_u$, where A_u is the unitary area. That means 41340 mobile BSs. Given the limited capacity of a v-BBU [10] at the geostationary and CubeSat satellites, the datacentre processors will serve mobile BSs according to a queueing model. Detailed analysis of this aspect of the scenario will be considered in future works.

Regarding latency, the total delay of the two approaches can be modelled as

$$t_{totnoV} = t_{prop} + t_{BBUproc} + t_{RRH} \tag{1}$$

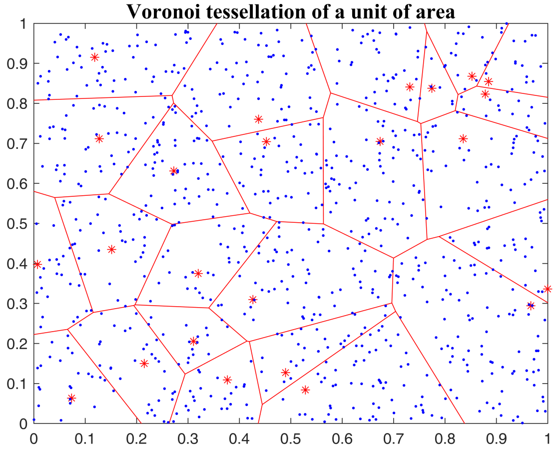

Fig. 2 Voronoi tessellation, which provides a snapshot of the coverage of a unit of area. The red stars are the mobile BSs while the blue dots are the peripherals.

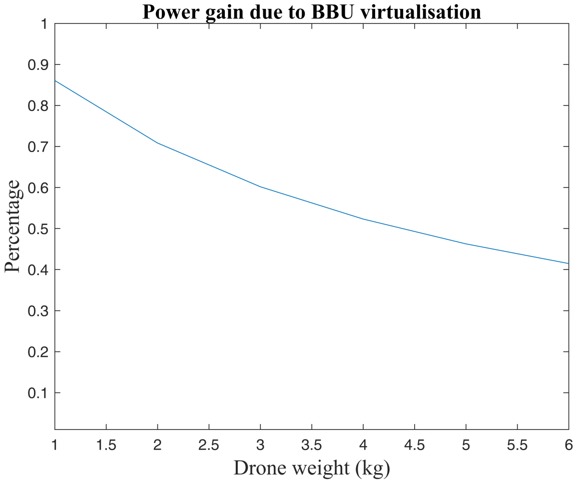

Fig. 3 Power gain at the mobile BSs (drones) when BBU is virtualised. Obviously, by increasing the load of the drone, the impact of the weight of the BBU decreases.

and

$$t_{totV} = t_{prop} + t_{Cloudproc} + t_{RRH} + t_{back} \tag{2}$$

where t_{totnoV} and t_{totV} are the total latency without virtualisation and with BBU virtualisation respectively. In particular, t_{prop} is the propagation delay, $t_{BBUproc}$ is the processing time of a physical BBU, $t_{Cloudproc}$ is the processing time in the cloud (i.e. the satellite) of v-BBUs, t_{RRH} [13] is the remote radio head (RRH) delay and t_{back} is the backhaul latency.

By considering the values of latency for Legacy long term evolution (LTE) uplink in [12], equation (1) and equation (2) becomes respectively $t_{totnoV} = x + 2.5$, $t_{totV} = x + 121.5$ (GEO satellite) and $x + 4 \leq t_{totV} \leq x + 4.66$ (CubeSat). The latencies of these formulas are measured in ms.

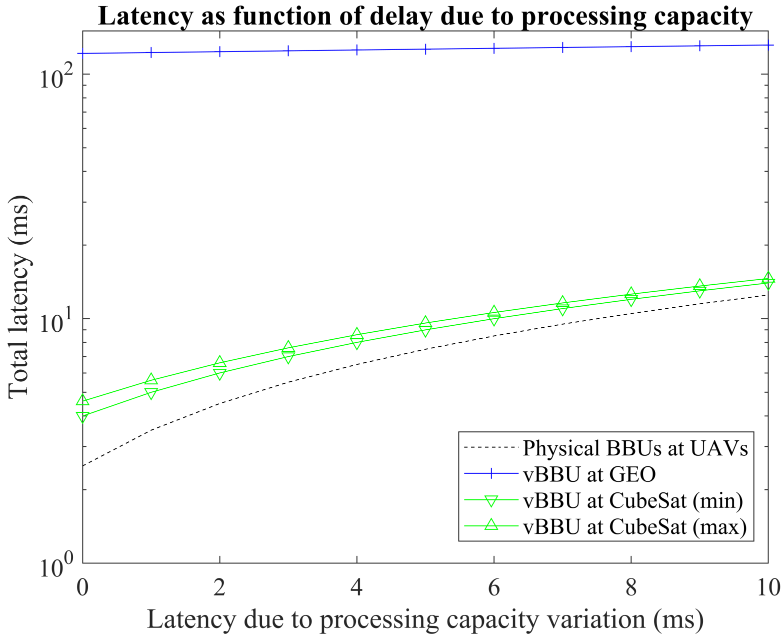

Fig. 4 Behaviour of total latency functions depending on the increase in processing time at physical BBUs or vBBUs at satellites.

As clearly appears by Fig. 4, the trade-off between reduction in energy consumption and latency becomes significant when satellites are involved in the Cloud RAN realisation. Furthermore, it also becomes clear that the choice of CubeSats is fundamental to have reasonable response time in case of data transmissions whose quality is hardly affected by latency. In that sense, a possible vision of DAVOSS to choose ultralight aerial vehicles or remotely operated blimps as an alternative to satellites to host cloud computing shows its importance.

On the other hand, the deployment of physical BBUs at the UAVs is an optimal choice in terms of latency but it increases a lot the energy cost at the drones. That would probably involve, given that a fleet of UAVs have very short flight time and require very frequent charging time, an extremely dynamic and challenging networking environment.

For more information on the model, please refer to [18].

Ongoing work is focused on analyzing the different solutions of backhauling, that will be reported on the project website: nato-davoss.org

5 Conclusions

5G design will include the possibility of fast deployment of the networking infrastructure. This would represent a great advantage in application scenarios, such as border monitoring and disaster situations.

This chapter analyzed an ongoing project activity at the Research Unit of Trento in order to design, implement and demonstrate a 5G architecture able to provide connectivity and advanced services using network virtualization and UAVs/aerial communication platforms. The results of this project will provide useful suggestions about the possibility of generating and managing reliable yet fast connectivity solutions using drones and 5G technology.

For additional information and updates related to the project, please visit the DAVOSS project website: nato-davoss.org

Acknowledgements This work has been partially funded by NATO Science for Peace and Security (SPS) Programme, in the framework of the project SPS G5428 "Dynamic Architecture based on UAVs Monitoring for Border Security and Safety".

References

1. D. Tarchi and G. Guglieri and M. Vespe and C. Gioia and F. Sermi and V. Kyovtorov, "Search and Rescue: Surveillance support from RPAs radar". 2017 European Navigation Conference (ENC), 256–264 (2017).
2. D. Moura and L. Guardalben and M. Luis and S. Sargento, "A Drone-Quality Delay Tolerant Routing Approach for Aquatic Drones Scenarios". 2017 IEEE Globecom Workshops (GC Wkshps), 1–7 (2017).
3. D. Bein and W. Bein and A. Karki and B. B. Madan, "Optimizing Border Patrol Operations Using Unmanned Aerial Vehicles". 2015 12th International Conference on Information Technology - New Generations, 479–484 (2015).
4. L. L. Coulter and D. A. Stow and Y. H. Tsai and C. M. Chavis and R. W. McCreight and C. D. Lippitt and G. W. Fraley, "A new paradigm for persistent wide area surveillance". 2012 IEEE Conference on Technologies for Homeland Security (HST), 51–60 (2012).
5. H. Kim and L. Mokdad and J. Ben-Othman, "Designing UAV Surveillance Frameworks for Smart City and Extensive Ocean with Differential Perspectives". IEEE Communications Magazine, Vol. 56, No. 4, pp. 98–104 (2018).

6. U. Raza and P. Kulkarni and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview". IEEE Communications Surveys Tutorials, Vol. 19, No. 2, pp. 855–873 (2017).
7. D. B. Rawat and S. R. Reddy, "Software Defined Networking Architecture, Security and Energy Efficiency: A Survey". IEEE Communications Surveys Tutorials, Vol. 19, No. 1, pp. 325–346 (2017).
8. G. Secinti and P. B. Darian and B. Canberk and K. R. Chowdhury, "SDNs in the Sky: Robust End-to-End Connectivity for Aerial Vehicular Networks". IEEE Communications Magazine, Vol. 56, No. 1, pp. 16–21 (2018).
9. M. Panizza and C. Sacchi and J. Varela-Miguez and S. Morosi and L. Vettori and S. Digenti and E. Falletti, "Feasibility study of a SDR-based reconfigurable terminal for emergency applications". 2011 Aerospace Conference, 1–18 (2011).
10. Ericsson, *Baseband Description – Baseband 5216, Baseband 5212*, 2016, http://www.1com.net/wp-content/uploads/2017/03/Ericsson-Baseband-5212-5216-datasheet-specs.pdf
11. G. Auer and V. Giannini and I. Godor and P. Skillermark and M. Olsson and M. A. Imran and D. Sabella and M. J. Gonzalez and C. Desset and O. Blume, "Cellular Energy Efficiency Evaluation Framework". IEEE 73rd Vehicular Technology Conference (VTC Spring), 1–6 (2011).
12. S. Nagata and L. H. Wang and K. Takeda, "Industry Perspectives". IEEE Wireless Communications, Vol. 24, No. 3, pp. 2–4 (2017).
13. L. Zhang and A. U. Quddus and E. Katranaras and D. Wübben and Y. Qi and R. Tafazolli, "Performance Analysis and Optimal Cooperative Cluster Size for Randomly Distributed Small Cells Under Cloud RAN". IEEE Access, Vol. 4, pp. 1925–1939 (2016).
14. E. Baceski and S. Gokcebag and A. Erdem and C. G. Erbay and M. Akyol and K. Arslankoz and I. Arslan and M. A. Agca and Y. B. Aydin and A. R. Aslan and O. Ceylan, "HAVELSAT: A software defined radio experimentation CubeSat". 2015 7th International Conference on Recent Advances in Space Technologies (RAST), 831–834 (2015).
15. D. L. Bekker and T. A. Werne and T. O. Wilson and P. J. Pingree and K. Dontchev and M. Heywood and R. Ramos and B. Freyberg and F. Saca and B. Gilchrist and A. Gallimore and J. Cutler, "A CubeSat design to validate the Virtex-5 FPGA for spaceborne image processing". 2010 IEEE Aerospace Conference, 1–9 (2010).
16. S. E. Palo, "High rate communications systems for CubeSats". 2015 IEEE MTT-S International Microwave Symposium, 1–4 (2015).
17. B. Butters and R. Raad, "A 2.4 GHz High Data Rate radio for pico-satellites". 2014 8th International Conference on Telecommunication Systems Services and Applications (TSSA), 1–6 (2014).
18. R. Bassoli, C. Sacchi, F. Granelli, I. Ashkenazi, "A Virtualized Border Control System based on UAVs: Design and Energy Efficiency Considerations". 2018 IEEE Aerospace Conference (2018).