# A VNF-Chaining Approach for Enhancing Ground Network with UAVs in a Crowd-Based Environment

Davide Montagno Bozzone
*Department of Computer Science, University of Pisa*
Pisa, Italy
d.montagnobozzone@studenti.unipi.it

Stefano Chessa
*Department of Computer Science, University of Pisa*
*Institute of Information Science and Technologies, CNR*
stefano.chessa@unipi.it

Michele Girolami
*Institute of Information Science and Technologies, CNR*
Pisa, Italy
michele.girolami@isti.cnr.it

Federica Paganelli
*Department of Computer Science, University of Pisa*
Pisa, Italy
federica.paganelli@unipi.it

***Abstract*—In the context of a 5G and beyond network operating in a smart city, in which the fixed network infrastructure is supported by a flock of unmanned aerial vehicles (UAV) operating as carriers of Virtual Network Functions (VNF), we propose a Mixed Integer Linear Programming (MILP) model to place chains of VNFs on a hybrid UAV-terrestrial infrastructure so to maximize the UAV lifetime while considering resource constraints and by taking into account the network traffic originated by crowds of people assembling in the city at given hotpoints. We formalize the UAV deployment problem and we test our solution with a practical scenario based on DoS detection system. The experimental results assess the deployment in a practical scenario of a DoS detection system and show that the proposed solution can effectively enhance the capability of the system to process the input flows under a DoS attack.**

***Index Terms*—Virtual Network Functions, Network Function Virtualization, UAV, Mobility**

## I. Introduction

The convergence of edge computing and Internet of Things (IoT) in the context of wireless communications is considered a key factor to enable novel applications. However extremely complex and mutable domains like those of the smart cities, in which a very large number of IoT sensing devices coexists with increasing traffic demand of the citizens which require huge data rate with low latency requirements and wide and flexible network coverage, are unveiling the limits of current network infrastructures. To cope with these limitations, a promising approach consists in complementing terrestrial networks with resources provided by aerial devices, like small Unmanned Aerial Vehicles (UAVs) [1], [2].

Such integration would enhance 5G and Beyond networks (5GB) [3] with high mobility, fast deployment, global availability, and dynamic reconfiguration of the network. Network Function Virtualization (NFV) is another pillar of modern networks, which consists in decoupling network functions from proprietary hardware, thus allowing to flexibly deploy and execute them as Virtual Network Functions (VNFs), i.e., as software bundles on general purpose hardware through a virtualization process. The NFV concept and related technologies provide models and tools for uniformly modelling heterogeneous infrastructure resources and orchestrate them to setup network services.

Recently, the increasing performance of embedded devices equipping UAV, which also supports increasingly complex software organization to deal with multiple tasks in real-time [4], enables the adoption of NFV in hybrid UAV and terrestrial networks [5]–[7] to support the flexible deployment of application and network functions [8], [9]. Such features enable an UAV to provide VNFs to users roaming on a bounded region, so that to extend the performance of the network infrastructure.

In this context, the problem of the deployment of software functions, such as those governing security like firewalls, or those than control access and mobility, session management or the network data analytics [10], over a hybrid UAV and terrestrial distributed edge infrastructure becomes critical as it may enhance connectivity and resilience by providing alternative options for deploying network functions. However, this deployment should operate so to take into account the limited computational capacity and memory of network nodes and the finite resources of UAVs.

To tackle with this challenge, we present a Mixed Integer Linear Programming (MILP) optimization problem that aims at determining the placement of VNF chains by taking into account the limited resources on board of UAVs, including energy, and that aims at maximizing the UAVs operational lifetime. We evaluate our solution by simulation, by using a traffic generator that models crowd assembled at an hotpoint in a city, and which is based on a synthetic extension of mobility data taken from the GeoLife crowdsensed dataset [11], [12]. More specifically, we generate three types of users' workload (low, medium and high), and we configure the simulator with parameters of commercially available UAV. The experimental results assess the deployment in a practical scenario of a DoS detection system and show that the proposed solution can effectively enhance the capability of the system to process the input flows under a DoS attack.

The remainder of this paper is organized as follows: Section II introduces the reference scenario and the addressed problem. Section III formalizes the problem and the proposed solution, Section IV details our experimental settings and the obtained results. Section V draws the conclusions.

## II. System model

In this work we consider a scenario where a set of UAVs can provide VNFs at the edge, thus complementing the computation capacity available at ground base stations. For instance, UAVs can be used to deploy security appliances realized as chains of network functions (e.g vFirewall, vIDS) [13]–[15]). The whole set of VNF chains to be placed is referred to as a set $R$ of requests. The requests can be satisfied by executing the VNFs on the ground $BS$, which has a maximum processing capacity of $C_{BS}^{max}$ $Gb/s$ or on a set $D$ of UAVs. Each UAV has a limited processing capacity as well as limited energy resources.

Each request $r \in R$ is defined as a sequence of VNFs of length $L^r$ as follows: $\{v_1^r, \ldots, v_{L^r}\}$. Due to its processing behaviour (e.g., compression, filtering, encapsulation), each $v_h^r$ VNF with $h \in \{1, ..., L^r\}$ may provide an output bitrate that is a fraction $\gamma_h^r$ of the input bit rate. For example, the value of $\gamma_h^r$ can be less than 1 for a firewall or 1 for a monitoring VNF. Therefore, given $w_0^r$ the initial input rate of the flow to be processed by request $r$, the input rate of $v_h^r$ will be given by:

$$w_{h-1}^r = w_0^r \prod_{h=1}^{h-1} \gamma_h^r \tag{1}$$

and its output rate will be given by $w_h^r = w_{h-1}^r \cdot \gamma_h^r$.

We assume that each drone $i \in D$ has a processor on board with a computational capacity of $CC_i$ $Gb/s$. We also define the instantaneous power consumption to keep the processor active and idle as $C_i^{proc-active}$ and $C_i^{proc-idle}$, respectively. Both powers are fixed and expressed in Watts. We define the instantaneous power to execute the $h-th$ VNF for a request $r \in R$ in drone $i$ as:

$$P_{i,h}^{proc,r} = C_i^{proc-active} \cdot d_{i,h,r}^{proc-active} \tag{2}$$

where $d_{i,h}^{proc-active}$ is the percentage of active use of the processor to execute $v_h^r$, which, given $w_{h-1}^r$ the input workload that must be processed, is defined as follows:

$$d_{i,h,r}^{proc-active} = \frac{w_{h-1}^r}{CC_i} \tag{3}$$

We define $d_i^{proc-active}$ as the overall percentage of active use of the processor, thus the percentage of idle use of the entire processor is:

$$d_i^{proc-idle} = 1 - d_i^{proc-active} \tag{4}$$

We also assume that each drone has a radio on board with maximum capacity $CR_i$ $Gb/s$. We define the power consumption to keep the radio active in transmission and reception and idle as $C_i^{TX}, C_i^{RX}$ and $C_i^{radio-idle}$, respectively. These powers are fixed and expressed in Watts. We now define the instantaneous power to transmit the $h-th$ workload (i.e., $w_h^r$ $Gb/s$) as follows:

$$P_{i,h}^{TX,r} = C_i^{TX} \cdot d_{i,h,r}^{TX} \tag{5}$$

where $d_{i,h,r}^{radio-TX}$ is the percentage of active use of the radio in transmission and it is defined as:

$$d_{i,h,r}^{TX} = \frac{w_h^r}{CR_i} \tag{6}$$

Similarly, we define the instantaneous power to receive the the $h-th$ workload as:

$$P_{i,h}^{RX,r} = C_i^{RX} \cdot d_{i,h,r}^{RX} \tag{7}$$

where $d_{i,h,r}^{radio-RX}$ is the percentage of active use of the radio in reception and it is defined as:

$$d_{i,h,r}^{RX} = \frac{w_h^r}{CR_i} \tag{8}$$

Given $d_i^{radio-active}$ the overall percentage of active use of the radio for receiving and transmitting packets, we define the percentage of idle state of the radio as follows:

$$d_i^{radio-idle} = 1 - d_i^{radio-active} \tag{9}$$

## III. Problem formulation

In this section, we provide a mathematical formulation of the considered system and propose a VNF chain placement that maximizes the lifetime of the drone that discharge first. Main notation is shown in Table I.

Following a similar idea as in [16], we use an auxiliary layered-graph $G^r = (N^r, E^r)$, for each request $r \in R$. Specifically, $G^r$ has a layer for each VNF in $r$ (numbered from 1 to $L^r$), and two additional layers: layer 0 hosting the origin node which receives the traffic from the users, and layer $L^r + 1$ hosting the destination node $d^r$. We assume that for all requests the destination node is the ground BS. Each layer contains the nodes of our system (UAVs and BS) and arcs linking each node in level $h$ to a subset of nodes in level $h+1$. In this work we make the simplifying assumption that each UAV is connected to the ground BS but no UAV-to-UAV connection exists (i.e. we assume a star topology). Thus, this implies that in the construction of the graph each node $i$ in level $h$ is connected to the same node $i$ and to the BS at level $h+1$ through two outgoing links. Moreover, we assume that if a VNF is assigned to a BS the subsequent VNFs in the chain will be assigned to the same BS.

We define the following decision variables corresponding to path design variables, representing the allocation of VNFs to nodes, as follows:

$$x_{\langle i,h\rangle\langle i,h+1\rangle}^r = \begin{cases} 1 & \text{if the arc linking node } i \text{ in level } h \text{ and} \\ & \text{node } i \text{ in level } h+1 \text{ is in the path} \\ & \text{relative to } r \in R \\ 0 & \text{otherwise} \end{cases}$$

$\forall\, r \in R, \forall i \in D, \forall h \in \{0, \ldots, L^r - 1\}$

$$x^r_{\langle i,h\rangle\langle BS,h+1\rangle} = \begin{cases} 1 & \text{if the arc linking node } i \text{ in level } h \text{ and the BS in level } h+1 \text{ is in the path relative to } r \in R \\ 0 & \text{otherwise} \end{cases}$$
$\forall\ r \in R,\ \forall i \in D \cup \{BS\},\ \forall h \in \{0,\dots,L^r\}$

Since our goal is to maximize the lifetime of the drone that discharges first, we write the objective function as follows:

$$\max \min_{i \in D} \quad LG_i \tag{10}$$

where $LG_i$ represents the lifetime of drone $i$ and is expressed as:

$$LG_i = \frac{BJ_i - CA_i - CB_i}{P_i^{flight} + P_{i,tot}} \tag{11}$$

$BJ_i$ is the initial energy of the drone's battery and is expressed in Joules, $CA_i$ and $CB_i$ are the costs to go and come back to the base (these costs are fixed and are expressed in Joules), $P_i^{flight}$ is the instantaneous power consumption of the drone for flight (this cost is fixed and is expressed in Watts), $P_{i,tot}$ refers to the overall power consumption of a drone in Watts. $P_{i,tot}$ is computed as the sum of the power consumed during processing and radio communication activities and idle status:

$$P_i^{tot} = P_i^{proc} + P_i^{radio} + P_i^{proc-idle} + P_i^{radio-idle} \tag{12}$$

where $P_i^{proc}$ represents the power consumption for executing the VNFs assigned to drone $i$, $P_i^{radio}$ is the power consumed for radio communication activity (i.e. for receiving traffic and transmitting it to the BS), and $P_i^{proc-idle}$ and $P_i^{radio-idle}$ account for the power consumed in idle status:

$$d_i^{proc-active} = \sum_{r \in R} \sum_{h=1}^{L^r} d_{i,h,r}^{proc-active} x^r_{<i,h-1><i,h>} \tag{13}$$

$$P_i^{proc} = C_i^{proc-active} d_i^{proc-active} \tag{14}$$

$$P_i^{proc-idle} = C_i^{proc-idle}(1 - d_i^{proc-active}) \tag{15}$$

TABLE I
MAIN NOTATION

| | |
|---|---|
| **Sets and Nodes** | |
| $D$ | set of drones in the network |
| $R$ | set of all service requests |
| $BS$ | Base Station |
| **Network Parameters** | |
| $CC_i$ | computational capacity of drone $i \in D$ |
| $CR_i$ | radio capacity of drone $i \in D$ |
| $C_i^{proc-active}$ | power consumed to keep the processor active |
| $C_i^{proc-idle}$ | power consumed to keep the processor in idle state |
| $C_i^{TX}$ | power consumed to keep the radio active in transmission |
| $C_i^{RX}$ | power consumed to keep the radio active in reception |
| $C_i^{radio-idle}$ | power consumed to keep the radio in idle state |
| $C_{BS}^{max}$ | maximum processing capacity of the BS |
| **Request parameters** | |
| $\{v_1^r, v_2^r, .., v_{L^r}^r\}$ | ordered sequence of VNFs composing $r$ |
| $Lr$ | length of the chain in $r$ |
| $w_0^r$ | input traffic rate for request $r$ |

$$d_i^{radio-active} = \sum_{r \in R} d_{i,0,r}^{RX}(x^r_{<i,0>,<i,1>} + x^r_{<i,0>,<BS,1>}) + \sum_{r \in R} \sum_{h=0}^{L^r} d_{i,h,r}^{TX} x^r_{<i,h>,<BS,h+1>} \tag{16}$$

$$P_i^{radio} = C_i^{RX} d_i^{radio-active} \tag{17}$$

$$P_i^{radio-idle} = C_i^{radio-idle}(1 - d_i^{radio-active}) \tag{18}$$

To preserve linearity, we transform the problem by considering the inverse of lifetime:

$$\min \max_{i \in D} \quad \frac{1}{LG_i} \tag{19}$$

and, by introducing an auxiliary variable $z$, we re-write the problem as follows:

$$\min z \tag{20}$$

$$z \geq (P_i^{flight} + P_{i,tot})/(BJ_i - CA_i - CB_i), \forall i \in D \tag{21}$$

Finally, we introduce the following constraints:

$$d_i^{proc-active} \leq 1 \quad \forall i \in D \tag{22}$$

$$d_i^{radio-active} \leq 1 \quad \forall i \in D \tag{23}$$

$$\sum_{r \in R} \sum_{i \in D \cup \{BS\}} \sum_{h=0}^{L^r-1} x^r_{<i,h><BS,h+1>} w_h^r \leq C_{max}^{BS} \tag{24}$$

$$\sum_{i \in D} x^r_{\langle i,0\rangle\langle i,1\rangle} + x^r_{\langle i,0\rangle\langle BS,1\rangle} + x^r_{\langle BS,0\rangle\langle BS,1\rangle} = 1 \quad \forall r \in R \tag{25}$$

$$\sum_{i \in D \cup \{BS\}} x^r_{\langle i,L^r\rangle\langle BS,L^r+1\rangle} = 1 \quad \forall r \in R \tag{26}$$

$$x^r_{\langle i,h-1\rangle\langle i,h\rangle} = x^r_{\langle i,h\rangle\langle i,h+1\rangle} + x^r_{\langle i,h\rangle\langle BS,h+1\rangle}$$
$$\forall h \in \{1,\dots,L^r 1\}, \forall i \in D, \forall r \in R \tag{27}$$

$$x^r_{\langle i,h-1\rangle\langle BS,h\rangle} - x^r_{\langle BS,h\rangle\langle BS,h+1\rangle} \leq 0$$
$$\forall h \in \{1,\dots,L^r - 1\} \quad \forall i \in D \cup \{BS\}, \forall r \in R \tag{28}$$

$$x^r_{\langle i,h\rangle\langle i,h+1\rangle} \in \{0,1\} \quad \forall r \in R, \forall i \in D, \forall h \in \{0,\dots,L^r - 1\} \tag{29}$$

$$x^r_{\langle i,h\rangle\langle BS,h+1\rangle} \in \{0,1\} \quad \forall r \in R, \forall i \in D \cup \{BS\},$$
$$\forall h \in \{0,\dots,L^r\} \tag{30}$$

$$z \geq 0 \tag{31}$$

Constraints (22) and (23) guarantee that the percentage of active use of the processor and radio does not exceed 100%. Constraint (24) ensures that the BS utilization is lower than its maximum processing capacity. Constraints (25),(26) and (27) refer to flow conservation conditions. Constraint (25) ensures that for each request one unit of flow leaves the origin node in level 0. In other words, each request uses either at most one drone or the Base Station $BS$. Constraint (26) states that for each request one unit of flow enters the destination node (the BS). Constraint (27) states that for each node $i$ belonging to any intermediate level $h$ and for each request $r \in R$, the quantity of flow entering node $i$ coincides with the one leaving node $i$. Constraint (28) ensures that if the $h$ VNF of request

$r$ is assigned to the BS, the remaining VNFs $(v^r_{h+1}, \ldots, v^r_{L^r})$ are also assigned to that BS. Finally, constraints (29),(30) and (31) define the variable domains.

## IV. Experimental Settings and Results

We now detail the experimental settings and the results to validate the proposed solution. The objective is to emulate the use of commercial UAVs to accommodate a specific traffic flow generated by users. To this end, we first describe the adopted mobility dataset and we detail how we determine the user's requests (see Section IV-A). Secondly, we report the experimental results (see Section IV-B).

### A. Mobility Dataset and User Requests

The dataset adopted for the experiments is obtained using data of the GeoLife [11], [12] dataset. The dataset has been collected by Microsoft Research Asia, and it involves about 182 participants recruited on a volunteer basis. The collected data include GPS traces of users. The dataset spans from April 2007 to August 2012, but the quality and the amount of traces strictly depends on the selected time period. We restrict the analysis to the interval 2008-07-01 to 2009-09-30. The dataset adopted for our experiments is obtained with a simulation process. In particular, we execute two steps: (i) determining the users' workload (ii) building the set of requests $R$. The first step is achieved by tiling the geographical region of the GeoLife's dataset with tiles of equal size. More specifically, we build a grid of equal-size tiles as reported in Fig. 1.

Then, we assign to each cell a workload type: low, medium and high, reproducing different user's behaviours in terms of networks usage. The second step consists of using the assigned workload to generate requests $R$, as follows:

1) The number of requests that need to be generated, denoted as $|R|$, is equal to the sum of the different workload types;
2) We assume the initial workload for each request $r \in R$ as: $w^r_0 = \frac{tot}{|R|}$;
3) We create a number of requests equal to the count of *low* workload type. For each generated request, the corresponding chain of Virtual Network Functions (VNFs) consists of 1 VNF, so we have $r = \{v^r_1\}$.
4) We create a number of requests equal to the count of *medium* workload type. For each generated request, the corresponding chain of VNFs consists of 2 VNFs, so we have $r = \{v^r_1, v^r_2\}$.
5) We create a number of requests equal to the count of *high* workload type. For each generated request, the corresponding chain of VNFs consists of 3 VNFs, so we have $r = \{v^r_1, v^r_2, v^r_3\}$.
6) The requests generated in steps 3, 4, and 5 compose the final set $R$ for a unique row $i$ within the dataset.

### B. Metrics and Results

The evaluation metrics are selected to provide a quantitative measure of the performance and efficiency of the system in handling and processing VNFs using a combination of Base Station $BS$s and drones. The presented metrics are also adopted in [13], [17], [18] and they are described in the following:

- $TP$: The total traffic processed by VNFs within the network (TP) expressed in Gbps;
- $E$: The enhancement measures the improvement in performance when drones assist in processing VNFs. $E$ is calculated by subtracting the total processed traffic from the maximum capacity of the Base Station divided by the maximum capacity of the Base Station: $\frac{TP - C^{BS}_{max}}{C^{BS}_{max}}$;
- $|D|$: The number of drones used;
- $LG_i$: Final lifetime of each drone after executing a set of VNFs measured in seconds.

Experiments are obtained by considering some hardware and software features for the Base Stations and UAV. In particular, we used the Nokia Flexi Multiradio 10 system module as reference Base Station. It supports multiple radio access technologies, including 5G, 4G LTE, 3G, and 2G. The maximum capacity of the base station is configured according to the technical specifications of the OBSAI RP3-01 interface, with $C^{BS}_{max}$ up to 6.144 Gbps. Concerning the technical specification of UAVs, we rely on authors of [19] which detail the power consumption value of a small quadrotor in hover flight mode. We assume a power required to fly $P^{flight} = 100W$. Data concerning the active power consumption for the radio ($C^{TX}_i$, $C^{RX}_i$) and processor ($C^{proc-active}_i$) are reported in [19]. In particular, we set $C^{TX}_i = C^{RX}_i = 8W$ and $C^{proc-active}_i = 8.5W$. We also set the idle power consumption $C^{radio-idle}_i$ and $C^{proc-idle}_i$ to 1/3 of the active values. The initial battery capacity is obtained considering the use of the DJI Mavic 3 drone battery, with a nominal voltage of 15.4 volts and a capacity of 5000 milliampere-hours (mAh). Based on the technical specifications of this drone, we assume that our ideal drone has Wifi-6 technology operating at 2.4GHz, with a maximum uplink speed of 100Mbps for receiving/transmitting data ($CR_i$) and 100 for the resource processor to process ($CC_i$).

To solve the optimization problem, we adopt the widely-used CPLEX v12.10 [20] tool developed by IBM, that offers an extensive range of solvers designed for linear programming, quadratic programming, mixed-integer programming, and more.

Our experiment tests our model under a DoS attack scenario. According to authors of [21], a system failure occurs when the initial throughput exceeds 9Gbps. To achieve our objective, we split 6000 users into 3 groups of 2000 users each, with various types of generated traffic in 1 hour, as illustrated in Table II. The first group generates textual traffic at an average data rate of 1.5Mbps per user, while the second group browses social media sites at an average data rate of 3Mbps per user. The third group consists of users attempting to overload the entire network, and generating traffic at an average data rate of 6.5Mbps per user. Concerning Group 1, we assume a workload split as follows: 100 Mbps of low workload type, 500Mbps of medium workload type and 2400Mbps of high workload

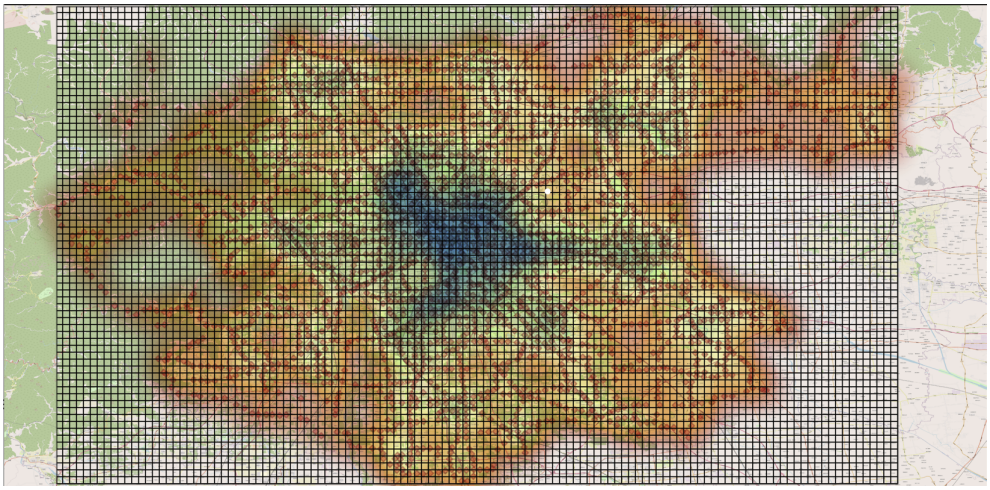

Fig. 1. Tessellation of Geolife's geographical region.

type for a total of 3000Mbps of traffic generated by users in Group 1. Concerning Group 2 the traffic is split as follows: 500 Mbps of low workload type, 2500Mbps of medium workload type and 3000Mbps of high workload type for a total of 6000Mbps of traffic generated by users in Group 2. Lastly, concerning Group 3 the traffic is split as follows: 350Mbps of low workload type, 600Mbps of medium workload type and 4900Mbps of high workload type for a total of 13000Mbps of traffic generated by users in Group 3.

TABLE II
DATASET'S REQUESTS.

| Group | users | Avg rate user (Mbps) | Tot rate (Mbps) | low | medium | high |
|---|---|---|---|---|---|---|
| 1 | 2000 | 1.5 | 3000 | 10 | 10 | 40 |
| 2 | 2000 | 3 | 6000 | 50 | 50 | 50 |
| 3 | 2000 | 6.5 | 13000 | 250 | 150 | 50 |

The randomly generated VNF chains, based on the total number of assumed traffic types, consist of various VNFs. For low traffic type, a Traffic Analyzer VNF detects common patterns or traffic spikes indicating a possible DoS attack. For medium traffic type, a Traffic Analyzer VNF is followed by a Load Balancer VNF that reduces the load on each resource and prevents resource overload. Finally, for high traffic type, the VNF chain comprises a Traffic Analyzer VNF, a Load Balancer VNF, and a Firewall VNF that filters out unwanted traffic and blocks malicious requests commonly used in DoS attacks.

Results of the DoS scenario are reported in Table III. Group 0 achieves a throughput of 7328.28 Mbps with an increase of the performance of 22%, thanks to the UAV deployment. Group 1 results with a processed traffic of 5968 Mbps, including 101 Mbps of traffic directly processed by the $BS$ and 2004.94 Mbps of traffic partially processed by 98 drones before being sent to the $BS$ for further processing. The base station processes a total of 153 VNFs, comprising 101 VNFs directly processed by the $BS$ and 52 VNFs partially processed by the drones. The total throughput achieved is 11828 Mbps.

TABLE III
RESULTS OF THE EVALUATION METRICS.

| Group | TP (Gbps) | E | $\|D\|$ |
|---|---|---|---|
| 0 | 7328 | 0.22 | 17 |
| 1 | 11828 | 0.97 | 98 |
| 2 | 15954 | 1.65 | 230 |

With Group 2, the traffic received directly from the crowd and processed by the Base Station ($C2B$) is close to the maximum capacity of the Base Station of 5988 Mbps. The total throughput achieved is 15954.95 Mbps. Moreover, the number of drones used to partially process the traffic before sending it to the Base Station for further processing ($D2B$) is 290. Overall, Group 2 results with the highest enhancement metric out of the three groups, suggesting that the addition of drones can significantly improve the system's processing capacity when the Base Station is overloaded in the case of DoS attack.

We also analyze the lifetime of different groups, as shown in Figure 2. The boxplot for Group 1 shows a lifetime spanning from roughly 2287s to 2341s, with a median value of 2325s. The boxplot for Group 2 spans approximately from 2329s to 2375s, with a median at value of 2364s, and some outliers present on the lower end. The boxplot for Group 3 has a box spanning from approximately 2364s to 2364s, with a median value of 2364s, and no outliers. The results indicate that drones are effective not only in enhancing network performance, but also in terms of their instantaneous power consumption. As previously indicated, the initial lifetime is 2661s, and this is also applicable in this case. Upon comparing these outcomes to the acquired data, it is apparent that although drones make a considerable contribution to network performance, they still have sufficient lifetime to satisfy further requests.

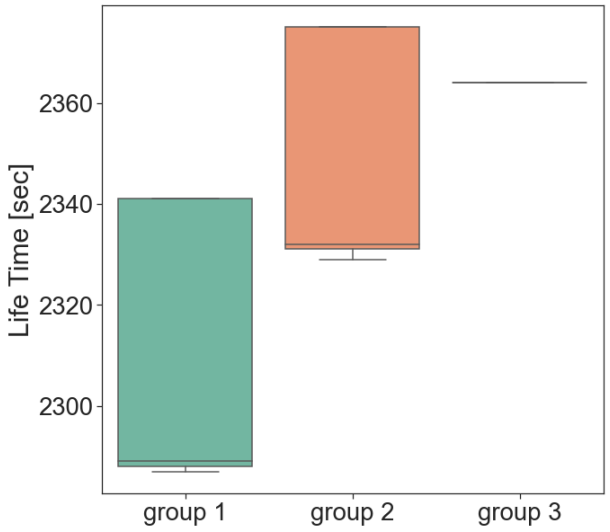


Fig. 2. Distribution of drones' lifetime for the three user groups.

## V. Conclusions

In this work, we investigate the possibility of deploying VNFs on commercial UAVs. More specifically, we study how detecting a Denial of Service attack, based on VNFs deployed on a number of UAVs. To this purpose, we present a MILP problem to optimize the placement of VNF chains, considering the hardware features of commercial UAVs. Experiments are based on technical specifications of commercially available Base Stations and UAVs. In particular, we adopt the Nokia Flexi Multiradio 10 system and the DJI Mavic 3 UAV as reference hardware. We measure a number of metrics, evaluating the quality of the deployment solution we found, i.e. the total traffic processed, the enhancement obtained with the UAV deployment and the number of UAVs used for hosting VNFs. The experiment provides valuable insights on how UAVs can potentially enhance network security by providing computation and communication resources for the operation of VNF chains, while also considering their capacity and energy constraints. Experimental results demonstrate that the integration of UAVs with the system can effectively enhance the system's processing capacity in the event of a DoS attack.

As future work we plan to extend the scenario considered in the experimentation to generalize to other contexts, also considering a comparison against an established baseline. We also plan to further extend the work by considering other infrastructure topologies beyond the star topology. A further line of investigation consists of extending the optimization model proposed in this work to consider specific features of drone networks (such as high-speed mobility and link instability), flying dynamics, which might possibly affect the optimal number of required UAVs and leveraging a UAV network simulator for validating the model.

## References

[1] Q.-V. Pham, R. Ruby, F. Fang, D. C. Nguyen, Z. Yang, M. Le, Z. Ding, and W.-J. Hwang, "Aerial computing: A new computing paradigm, applications, and challenges," *IEEE Internet of Things Journal*, 2022.

[2] M. Bacco, S. Chessa, M. Di Benedetto, D. Fabbri, M. Girolami, A. Gotta, D. Moroni, M. A. Pascali, and V. Pellegrini, "Uavs and uav swarms for civilian applications: communications and image processing in the sciadro project," in *Wireless and Satellite Systems: 9th International Conference, WiSATS 2017, Oxford, UK, September 14-15, 2017, Proceedings 9*. Springer, 2018, pp. 115–124.

[3] B. Li, Z. Fei, and Y. Zhang, "Uav communications for 5g and beyond: Recent advances and future trends," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2241–2263, 2019.

[4] A. Kocian and S. Chessa, "Iterative probabilistic performance prediction for multiple iot applications in contention," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13 416–13 424, 2022.

[5] G. Wang, S. Zhou, S. Zhang, Z. Niu, and X. Shen, "Sfc-based service provisioning for reconfigurable space-air-ground integrated networks," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 7, pp. 1478–1489, 2020.

[6] O. S. Oubbati, M. Atiquzzaman, T. A. Ahanger, and A. Ibrahim, "Softwarization of uav networks: A survey of applications and future trends," *IEEE Access*, vol. 8, pp. 98 073–98 125, 2020.

[7] A. Kocian, M.-A. Badiu, B. H. Fleury, F. Martelli, and P. Santi, "A unified message-passing algorithm for mimo-sdma in software-defined radio," *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, no. 1, p. 4, Jan 2017. [Online]. Available: https://doi.org/10.1186/s13638-016-0786-y

[8] R. Zhang, F. Zeng, X. Cheng, and L. Yang, "Uav-aided data dissemination protocol with dynamic trajectory scheduling in vanets," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 2019, pp. 1–6.

[9] L. F. Gonzalez, I. Vidal, F. Valera, V. Sanchez-Aguero, B. Nogales, and D. R. Lopez, "Nfv orchestration on intermittently available suav platforms: challenges and hurdles," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2019, pp. 301–306.

[10] O. Bekkouche, K. Samdanis, M. Bagaa, and T. Taleb, "A service-based architecture for enabling uav enhanced network services," *IEEE Network*, vol. 34, no. 4, pp. 328–335, 2020.

[11] Y. Zheng, Q. Li, Y. Chen, X. Xie, and W.-Y. Ma, "Understanding mobility based on GPS data," in *Proc. 10th Int. Conf. Ubiquitous Computing*, ser. UbiComp '08. ACM, 2008, p. 312–321.

[12] Y. Zheng, L. Zhang, X. Xie, and W.-Y. Ma, "Mining interesting locations and travel sequences from GPS trajectories," in *Proc. 18th Int. Conf. WWW*. ACM, 2009, p. 791–800.

[13] H. Li, H. Hu, G. Gu, G.-J. Ahn, and F. Zhang, "vnids: Towards elastic security with safe and efficient virtualization of network intrusion detection systems," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 17–34.

[14] A. Hermosilla, A. M. Zarca, J. B. Bernabe, J. Ortiz, and A. Skarmeta, "Security orchestration and enforcement in nfv/sdn-aware uav deployments," *IEEE access*, vol. 8, pp. 131 779–131 795, 2020.

[15] U. Fattore, M. Liebsch, and C. J. Bernardos, "Upflight: An enabler for avionic mec in a drone-extended 5g mobile network," in *2020 IEEE 91st Vehicular Technology Conf. (VTC2020-Spring)*. IEEE, 2020, pp. 1–7.

[16] P. Cappanera, F. Paganelli, and F. Paradiso, "Vnf placement for service chaining in a distributed cloud environment with multiple stakeholders," *Computer Communications*, vol. 133, pp. 24–40, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366418303104

[17] J. Lyu, Y. Zeng, and R. Zhang, "Uav-aided offloading for cellular hotspot," *IEEE Transactions on Wireless Communications*, vol. 17, no. 6, pp. 3988–4001, 2018.

[18] G. Mountaser, E. Pardo, and T. Mahmoodi, "Graphical modelling and optimization of ran function split deployed through uavs," *Computer Networks*, vol. 217, p. 109266, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128622003309

[19] H. V. Abeywickrama, B. A. Jayawickrama, Y. He, and E. Dutkiewicz, "Empirical power consumption model for uavs," in *IEEE Vehicular Technology Conference*, vol. 2018-August, 2018.

[20] I. I. Cplex, "V12. 1: User's manual for cplex," *International Business Machines Corporation*, vol. 46, no. 53, p. 157, 2009.

[21] G. Wangen, A. Shalaginov, and C. Hallstensen, "Cyber security risk assessment of a ddos attack," in *Information Security: 19th International Conference, ISC 2016, Honolulu, HI, USA, September 3-6, 2016. Proceedings 19*. Springer, 2016, pp. 183–202.