Possibility of Using Existed WLAN Infrastructure as an Emergency Network for Air-to-Ground Transmissions: The Case of WebRTC-Based Flying IoT System

Agnieszka Chodorek[1(✉)], Robert R. Chodorek[2], and Krzysztof Wajda[2]

[1] Kielce University of Technology, Al. 1000-lecia P.P. 7, Kielce 25-314, Poland
a.chodorek@tu.kielce.pl
[2] The AGH University of Science and Technology, Al. Mickiewicza 30, Krakow 30-059, Poland
chodorek@agh.edu.pl, wajda@kt.agh.edu.pl
http://www.kt.agh.edu.pl

Abstract. In many urban and industrial areas, there exist wireless network infrastructures - usually complex, covering large public buildings (often with adjacent parking lots and green areas). In the case of emergency situations, such infrastructure could be used as a production network (i.e. a network dedicated to the transmission of user data) for creating ad-hoc flying monitoring systems, composed of one or more air stations (drones equipped with specialized sensors and detectors, as well as a high resolution camera), and corresponding ground station(s). This paper proves that the existing network architecture is able to play a significant role in the casual assurance of suitable air-to-ground transmission of monitoring data. Transmissions are carried out between two WebRTC applications of IoT brokers, placed on the air station, and on the ground one. The stations are connected through the IEEE 802.11ac (Wi-Fi) production network. During experiments, two different wireless local area networks were used as a production network. The first one was dedicated to transmissions coming from the flying monitoring system. The second one was the private network of the AGH University of Science and Technology, available for the academic community. Results of experiments show that although a dedicated network better fits the needs of the flying monitoring system, a well-dimensioned public network that has good coverage of the monitored area is able to effectively replace it in an emergency.

Keywords: Internet of Things · Performance evaluation · Real-time multimedia · Unmanned aerial vehicle · WebRTC

This work was supported by the Polish Ministry of Science and Higher Education with the subvention funds of the Faculty of Computer Science, Electronics and Telecommunications of AGH University.

H. Gao et al. (Eds.): BROADNETS 2020, LNICST 355, pp. 3–21, 2021.
https://doi.org/10.1007/978-3-030-68737-3_1

1 Introduction

In many places, especially in strongly urbanized environments, there exist complex network infrastructures. In urban areas extensive local network infrastructures have been built, based on cellular telephony (LTE[1], GSM[2]/EDGE[3] or UMTS[4]/HSPA[5]) and (or) IEEE[6] 802.11 wireless local area network (wireless LAN, or WLAN) technology (also known as Wireless Fidelity, or Wi-Fi). Large companies and institutions have built complex IEEE 802.11 networks, which include anything from a few to a large number of access points. Complex IEEE 802.11 networks have also been created by network service providers. In many cities, there are large public IEEE 802.11 networks available to a large group of users.

All these networks are usually designed considering the local propagation of radio signals to obtain full coverage of a given area. As a result, they could be used, in emergency situations, as data transmission networks for the purpose of ad-hoc installed flying monitoring systems. Such systems consist of one or more air station(s), i.e., flying drones equipped with high resolution cameras and specialized sensors and detectors, and corresponding ground station(s), connected with the air one through a wireless local area network.

The Authors believed that the use of existing network infrastructure could facilitate and accelerate the process of the construction of flying monitoring systems, although there are some unknowns, such as the behaviour of flying monitoring systems when non-dedicated, not-optimized (in terms of a flying monitoring system), typically configured user channel will be used for the transmission of monitoring data. This paper sheds a light on these aspects through the experimental evaluation of the air-to-ground transmission of environmental data from sensors and video from a 4K UAV camera.

1.1 WebRTC and WebRTC-Based Flying Monitoring System

The World Wide Web real-time communications (WebRTC) [15,24,32] is a novel technology, not fully standardized yet [25], which assures real-time transmission of media (audio and/or video) in a non-real-time Web environment. The media are streamed using the Real-time Transport Protocol (RTP) version 2 [34], which uses the classic Audio Video Profile (RTP/AVP) [35] and the security extension to this profile, namely RTP/SAVP [3] (Secure RTP, or SRTP). Cryptographical protection of the SRTP is performed with the use of the Advanced Encryption Standard (AES) algorithm. The WebRTC technology also offers data transmission, which uses symmetric Data Channels [19], enabling transmissions of non-real-time data flows with the use of the Stream Control Transmission Protocol

[1] Long-Term Evolution.
[2] Global System for Mobile Communications.
[3] Enhanced Data rates for GSM Evolution.
[4] Universal Mobile Telecommunications System.
[5] High Speed Packet Access.
[6] Institute of Electrical and Electronics Engineers.

(SCTP) [37]. SCTP transmissions are secured using the Datagram Transport Layer Security (DTLS) protocol [31,38].

Both audio/video streams and data flows are congestion controlled. The SCTP congestion control is a slightly modified TCP Congestion Control [1]. Streaming media congestion control is mainly based on the TCP-friendly Rate Control (TFRC) [14] and the Google Congestion Control (GCC) [17] (both used as sender-side congestion control). Additionally, stream replication simulcast and layered simulcast can be used as node-side congestion control. Performance evaluation of the sender-side congestion control is presented in [7,36], and the node-side one in [8,16].

One of the possible applications of the WebRTC technology is the Internet of Things (IoT) broker [9,10], which was one of the main parts of the flying IoT system, designed to monitor parking lots.

The flying IoT system consists of an air station and a ground station. The air station is composed of the IoT carrier, which is an Unmanned Aerial Vehicle (UAV), and the flying IoT system, which is composed of a 4K video camera, a set of environmental sensors, and a single-board computer, on which the WebRTC application of an IoT broker is run. Streaming media from the camera and non-media data from sensors are aggregated into one stream and transmitted to the ground, where they are received by the other WebRTC application of an IoT broker, run at the ground station. The ground station also is composed of the two parts (as the air station is): the WebRTC multimedia and monitoring station (WMMS), and the command and control console (CCC). The WMMS is the WebRTC-based IoT broker run on a computer device (e.g.. desktop computer, laptop or even smartphone on which WebRTC-capable web browser is run). The CCC is used for piloting the UAV.

Due to reliability and quality of service (QoS) issues, the network connecting the air station and the ground station has been physically divided into two separate parts: the production network, used for the communication between the IoT system on board the UAV and the WMMS, and the management and control network, used for communication between the UAV and the CCC.

1.2 Complex Infrastructure-Based Production Network

The example of a complex infrastructure-based variant, based on an IEEE 802.11 network, is shown in Fig. 1. The flying IoT system uses a set of available access points AP1, AP2, AP3, which are connected to a central controller to authorize future clients of the successive access points and to allow for fast roaming between access points. In practice, in a given instant of time, usually only a subset of this set is being used. Which available access points belong to the subset of currently used access points varies in time.

In contrast to the simple infrastructure-based variant, where a single access point is a kind of relay station that receives application data and resends them directly to the WMMS, the solution shown in Fig. 1 allows the data transmission

In the case of a simple infrastructure-based variant, a single intermediate device (access point) is used. It acts as a kind of relay station that receives

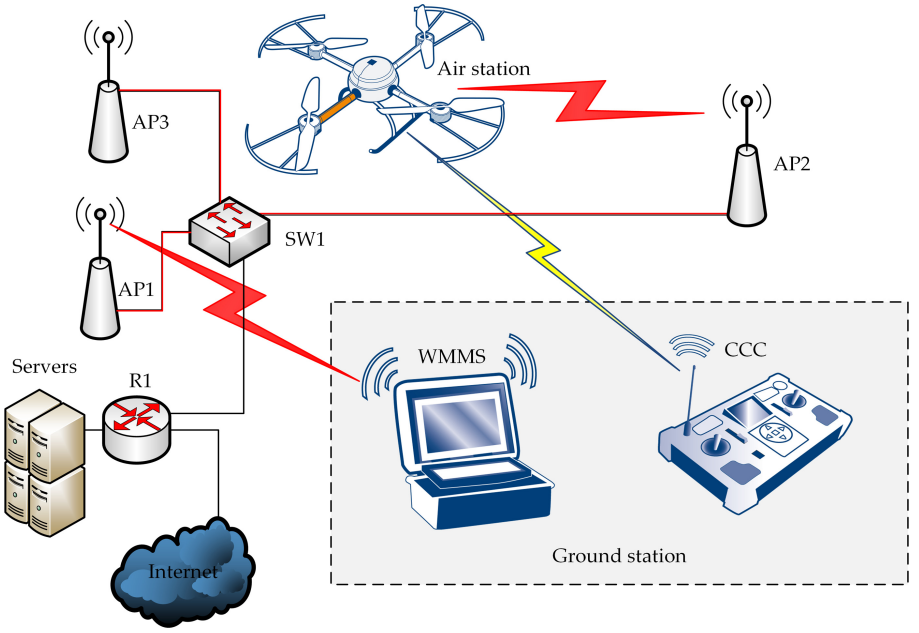

Fig. 1. General architecture of the flying IoT system: infrastructure-based variant with multiple APs (red - production network, yellow - management and control network). (Color figure online)

application data and resends them directly to the WMMS. The complex infrastructure-based variant extends the simple one with multiple (two or more) intermediate devices. Example of such a solution is shown in Fig. 1. In contrast to the simple infrastructure-based variant, the complex one allows the data transmission path to travel through a set of access points.

In the situation depicted in Fig. 1, one access point (AP2) receives the application data from the IoT system mounted on the UAV, and sends them using the infrastructure of the distribution network (the so-called Distribution System, or DS, which can be implemented as a wired or wireless one) to the other access point (AP1), which broadcasts data directly to the WebRTC multimedia and monitoring station. AP1 and AP2 belong to the subset of currently used access points.

This situation may change over time. The range of an average drone is greater than the range of an average IEEE 802.11 connection. Areas monitored by flying IoT systems will often be large enough to display a significant deterioration of the signal-to-noise ratio when IoT systems are connected to single access points. In the case of the availability of multiple access points, if the quality of connections between IoT systems and the currently connected access points become poor, the current points of attachment to the IEEE 802.11 network will be changed (e.g.. from AP2 to AP3). Thus, the subset of currently used access points will change (here: from {AP1, AP2} to {AP1, AP3}).

An essential condition of the IEEE 802.11 network connectivity is that all access points connected to a given network (and so belonging to a given set of available access points) must provide the same extended set of services. They must create an Extended Service Set (ESS) and be identified by the same identifier (the same ESSID). In practice it means that classic roaming consists of several steps, which take time and causes some more or less serious breaks in transmission. This is usually unnoticeable during reliable data transfer, but can be seen during media streaming.

The use of a seamless handover allows streaming media to be transferred during the changing of their point of attachment from one access point to another, without significant degradation of the quality of the transmission service (QoS parameters should not fall below a level acceptable by a streaming application). So, in the case depicted in Fig. 1, fast roaming (standardized as the IEEE 802.11r) is recommended. For purposes of the flying IoT system, both the IEEE 802.11r over-air roaming and the IEEE 802.11r over-ds (over Distribution System) roaming can be used.

Large companies and institutions build IEEE 802.11 networks working in so-called enterprise mode, in which central databases based on the 802.1x protocol and RADIUS servers are used for authentication. The use of this infrastructure for the flying IoT system requires registration of all used network devices (here: network adapters of IoT systems and of WMMSs) within the authentication server.

The complex infrastructure-based variant of the flying IoT system has two general advantages, common for both infrastructure-based variants: easy access to additional services provided by the external infrastructure, and the ability for transmissions between a WMMS and multiple UAVs. However, the main advantages of the complex infrastructure-based variant are the increased range of communication within large areas, and the high performance of the communication, which is optimized to a given area.

The main disadvantages of the complex infrastructure-based variant is a complex setup and a longer time to start gathering data, when compared with the simple infrastructure-based variant. Additionally, if the production network is attached to the public Internet, cyber threats that are coming from any site of this global network may appear in the production network nodes.

The complex infrastructure-based variant of the flying IoT system assumes that the production networks may or may not be dedicated. In particular, it may be built in whole as a dedicated network, or it may be constructed (partially or in whole) using fragments of existing network infrastructures.

1.3 Motivations, Main Contributions and Organization of This Paper

In the paper [9] a WebRTC-based flying Internet of Things system to monitor a parking lot was introduced. The presented system consists of an air station, a ground station, and two wireless local area networks that connect stations. The first WLAN is a management and control network, intended for the pilotage

of a UAV, which serves as the carrier of a WebRTC-based IoT. The second is a production network, used for WebRTC transmissions of video from the UAV camera and environmental data from sensors.

The aim of this paper is to discuss performance of the flying IoT system, when the production network has a relatively complex topology, i.e. transmission paths lead through more than one intermediate node. The question is: must such a network be built as a dedicated one, or is possible to use existing infrastructure, covering the whole monitoring area but not being under the administrative control of the owners of the flying IoT system? The latter is especially important in the case of emergency situations, where there is no time for the ad-hoc building of complex networks, and in the case of occasional events, where the building of complex networks may not be economically feasible. The main contributions of this paper are:

- Discussion of the architectural issues of the flying monitoring system in the context of the building of a complex production network.
- Evaluation of the prototype flying monitoring system in terms of the performance of air-to-ground communication carried out in a dedicated 802.11ac WLAN.
- Evaluation of the prototype flying monitoring system in terms of the performance of air-to-ground communication using an existing, general-purpose 802.11ac WLAN infrastructure, which is a functional equivalent of the dedicated one.

The rest of this paper is as follows. The next, second Section describes related work. The third Section briefly describes the analyzed system and the test environment. The fourth Section presents the results of the experiments that were carried out. The last, fifth Section summarizes our experiences and concludes this paper.

2 Related Work

Several aspects of communication (routing, various communications technologies) in the context of UAVs were presented in paper [2]. Literature reearch carried out in the paper [39] shows that advanced high-bandwidth UAV communication can be carried out mainly with the use of the IEEE 802.11 technology.

The transmission from a drone to a ground station using LTE was analyzed in [6,27,29]. In [6] is presented a system in which the mobile phone supporting LTE was installed on the drone. Only data generated by the application which runs on the mobile phone are sent to the ground station using the LTE network. The transmission of both the video live stream and the control data between the drone and the ground station using the LTE network was presented in [27]. The LTE network used for the video transmission from the UAV for the surveillance a crowd of people was presented in [29]. It is worth remarking that experiments were carried out only in private LTE network, fully administrated by persons which conducted experiments.

In [5] usage of a Narrow Band IoT (NB-IoT) for collecting data from underground sensors in potato crops was presented. The base station of the NB-IoT using the 716 MHz band was mounted on a UAV.

Analysis of the usage of a UAV as a gateway between IoT devices which uses LoRaWAN technology and a LTE network was presented in [4].

Very small drones with only a few sensors onboard (humidity, temperature, light intensity) were analyzed in [18]. For communication dedicated RF working in the 900 MHz ISM band was used. Data are sent using ON-OFF keying modulation.

In [28] the integration of a UAV IoT communication platform which minimized both energy consumption and the time to handle events was analyzed. The performance of the presented system was validated using simulation.

In several applications, IoT devices are being located not on the drone but on the ground. In those solutions drones work as a communication relay [11–13]. In the paper [12] the performance of air-to-ground communication between the drone and multiple wireless IoT devices in a WiFi 2,4 GHz test environment was analyzed. Paper [13] analyzes two problems of the communication between the drone and multiple wireless IoT devices: different numbers of devices in different areas and potential traffic congestion in those areas. To avoid those problems the concept of load balancing is proposed. The concept was evaluated in a simulator. An analysis of the usage of multiple UAVs in a dynamic environment to cover multiple regions was presented in [11]. The proposed solution was evaluated using the numerical simulations which were performed in the Matlab.

3 Analyzed System and Experimental Environment

This Section outlines a WebRTC-based flying monitoring system, build as reported in [9], describes the environment of experiments that were carried out at a parking lot of the AGH University of Science and Technology, and overviews practical aspects related to these experiments.

3.1 WebRTC-Based Flying Monitoring System

The WebRTC-based flying monitoring system, introduced in the paper [9], includes an air station and a ground one. The air station is composed of a WebRTC-based IoT system, which performs a monitoring service, and a flying carrier (here: a UAV), on which the IoT system is mounted. The ground station is composed of two consoles:

- CCC, which is the remote control console,
- WMMS, which is the IoT console.

The WMMS is also the destination point of the air-to-ground transmissions coming from the IoT system.

The important part of the analyzed system is an emulator of an IoT broker, written as a WebRTC application. This software implements full encapsulation

and decapsulation of non-real-time data in/from messages of the Message Queue Telemetry Transport (MQ Telemetry Transport, MQTT) protocol. The MQTT is used as an application layer protocol for the transmission of data coming from sensors. For transmission of video frames no application layer protocol is used.

On the air station, the WebRTC application of the IoT broker is run on the Chromium browser, which, in turn, is run on a single-board computer (SBC) working under the control of the Raspbian operating system. On the ground station, the application of the IoT broker is run on the Chrome browser.

The broker running on the air station collects data from sensors and from a 4K video camera, and then sends that data to the WMMS. Video data are transmitted as a media stream, using the RTP. Environmental data from sensors are transmitted as non-media flow, using the SCTP. The media stream and non-media flow are aggregated before being sent to the WMMS. The broker running on the WMMS disaggregates the received stream, decapsulates video frames from RTP packets and non-media data from SCTP packets and MQTT receivers. Then the broker processes the obtained information (if needed) and displays it on the dashboard. The video is displayed in the form of moving pictures, and the environmental data from sensors are displayed as successive points of time graphs and/or numerical values.

As was mentioned in the Introduction, the air station and the ground station are connected through two networks:

- the management and control network, which connects the IoT carrier and the CCC,
- the production network, which connects the WebRTC-based IoT system and the WMMS.

In the prototype implementation [9], the production network was built according to the IEEE 802.11ac standard. Thus, at least three variants of the production network are possible:

- the infrastructure-less variant, implemented as the simplest Independent Basic Service Set (IBSS), which is composed of only two stations,
- the simple infrastructure-based variant, implemented as two Basic Service Sets (BSSs) connected through a shared access point,
- the complex infrastructure-based variant, implemented as a single Extended Service Set (ESS).

In the case of the infrastructure-less variant, transmissions between the air station and the ground station are carried out using a single, direct path, and no intermediate devices are used. This variant offers high mobility and great simplicity, although it suffers from a limited range of communication.

Both the infrastructure-based variants offers indirect transmissions, which lead through one (the simple infrastructure-based variant) or more (the complex infrastructure-based variant) intermediate access points. The use of infrastructure-based variants results in an increased range of communication when compared to the infrastructure-less one.

3.2 Test Environment

Experiments were carried out at one of the parking lots of the AGH University of Science and Technology. During experiments, the flying IoT system described in the paper [9] and briefly characterized in the previous Section, was used.

Experiments were conducted with the use of a complex infrastructure-based variant of the production network, depicted in the Fig. 2, and according to following scenarios:

- the use of a portable, temporary network infrastructure (scenario S1),
- the use of the existing permanent network infrastructure (scenario S2).

To realize the above scenarios, three access points were used. Devices AP1, AP2 and AP3 (Fig. 2) belonged to the portable infrastructure that was built for the purpose of the experiments described in the next Section. The access points were NETGEAR Nighthawk X4 R7500 AC2350 devices. As the DS, a 1 Gbps Ethernet network was used. The SW1 Ethernet switch, which belonged to the DS, was an HP 3500-24G-PoE+ yl Switch, with 24 ports, 1 Gbps each.

The AP1 was placed in a corner of the rectangular parking lot, at the place marked as the point B. Access points AP2 and AP3 were placed, respectively, 30 meters from point A, and 28,3 m from the point A'. The placement of AP1, AP2 and AP3 was chosen so that:

- the change of the access point location after the scenario changed to S2 was as small as possible,
- access point locations were safe for both access points and users of the parking lot.

Note that the Fig. 2 is an explanatory figure (not shown to scale).

In tests carried out according to the S2 scenario, three access points (AP1', AP2' and AP3') belonging to the permanent infrastructure of the AGH University of Science and Technology were used. The IEEE 802.11 university network covers the entire campus, and connects local IEEE 802.11 networks built by some university departments. The access point chosen to be the AP1' belongs to WLAN administrated by Department of Telecommunications, while AP2' and AP3' are administrated by the University. This allowed the air station to use an account with its transfer rate unlimited administratively.

AP1', AP2' and AP3' were placed in nearby buildings, a bit further from the parking lot than AP1, AP2 and AP3. AP1' was located 16.2 m in a straight line from the point B, AP2' was 37.2 m from point A, and AP3' was 34,4 m from point A'.

The ground station was equipped with a IEEE 802.11 Intel®Dual Band Wireless-AC 7260 network adapter, and the air station was equipped with an IEEE 802.11ac dual band (2.4 GHz and 5 GHz) network adapter embedded in the Raspberry Pi 4 B single-board computer. The ground station was placed about 1 to 1.5 m from point B.

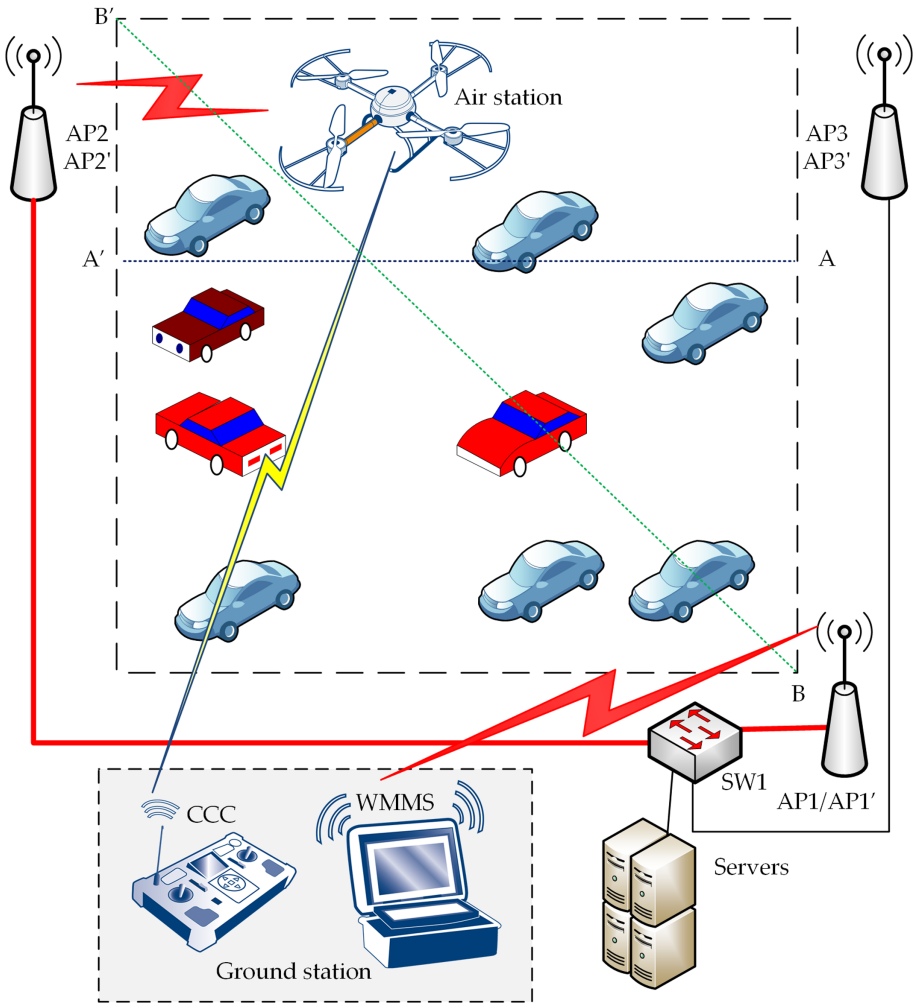

Fig. 2. Test environment.

During the WebRTC session establishment three auxiliary servers must be used (the WWW server, the signalling server, and the NAT traversal server). In both S1 and S2 scenarios, all three servers were run on external machines (see Fig. 2).

3.3 Experiments

During the experiments, the air station flew 15 m over the parking lot on the course shown in Fig. 2 as lines A-A' and B-B'. The line A-A' crosses the parking lot horizontally, in the place where the strength of the signal coming from the ground station becomes small enough to possibly cause transmission problems

and the air station should change its point of attachment to the production network. The line B-B' leads diagonally across a rectangular parking lot, passing through expected areas of weak and strong signal. Note that signal strength all time was high enough to keep the air station and the ground station connected. The distance between points A and B was 50 m.

After ascending to the cruising altitude of 15 m (measured with an accuracy of 10 cm by the on-board barometric altimeter), the UAV flew to the measurement starting point, i.e. point A or point B. Then it followed trajectories, respectively, of A-A' or B-B'. Every 5 m the UAV hovered in the air, enabling measurements of total throughput (expressed in megabits per second, or Mbps) and readings of the parameters set by the network adapter mounted on the air station (available data rate, expressed in Mbps, and the Received Signal Strength Indicator, or RSSI, expressed in decibel-milliwatts, or dBm) at fixed positions. The five-meter distances were measured horizontally, using the accuracy of the on-board NSS[7] (up to 0.5 m), in a straight line between the starting point (A or B) and the current position of the air station. The total length of trajectory A-A' was 70 m, and trajectory B-B' was 100 m.

Experiments were carried out over a few days, at approximately the same time and the same weather conditions. The RSSI, the available data rate, and the total throughput were averaged over 5 times. The available data rate was computed as a dominant, and other quantities as an arithmetic mean. Results of experiments are shown and discussed in the next Section.

4 Experimental Results

The results of the experiments are depicted in figures from Fig. 3 to Fig. 5. Quantities shown in these figures are presented as functions of the horizontal distance between the air station and the beginning of a trajectory: point A (d_{aA}) and point B (d_{aB}). During experiments the air station followed trajectories A-A' and B-B', and at about the fortieth meter (A-A') or the fiftieth meter (B-B') from the starting point of each trajectory (A or B, respectively) the air station changed its point of attachment to the DS.

4.1 Received Signal Strength Indicator

The RSSI represents the power of the received signal, and is used by IEEE 802.11 standard as a relative signal strength quantity.

Nearly symmetric placement of access points causes that end-points of each trajectory are characterized by a very good (if the dedicated network was used: S1 scenario) or good (if the public network was used: S2 scenario) relative signal strength. In detail, if the dedicated network was used (S1 scenario, figures Fig. 3a and Fig. 3c), end-points of A-A' trajectory were characterized by the RSSI of −45 dBm (point A) and −46 dBm (point A'). And both end-points of B-B'

[7] Navigation Satellite System.

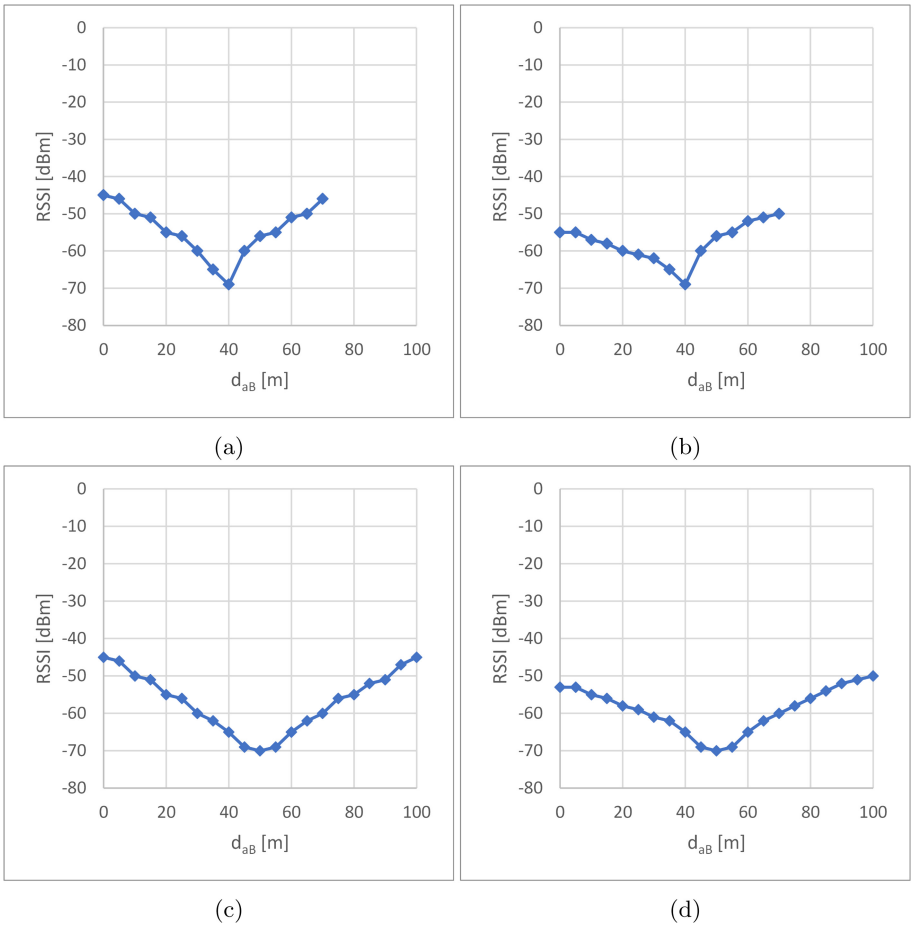

Fig. 3. Relative signal strength (RSSI) measured in scenario: (a) S1, trajectory A-A'; (b) S2, trajectory A-A'; (c) S1, trajectory B-B'; (d) S2, trajectory B-B'.

trajectory were characterized by the RSSI of −45 dBm. The use of the public network (S2 scenario, figures Fig. 3b and Fig. 3d) allows the RSSI to achieve −55 dBm (point A), −53 dBm (point B), and −50 dBm (points A' and B').

The closer to the mid-point of each trajectory, the smaller the Received Signal Strength Indicator. A small asymmetry of the placement of pairs of access points AP2 and AP3, and AP2' and AP3' causes that the switching of the point of attachment of the air station to the DS (from AP3/AP3' to AP2/AP2') occurs 40 m from point A and 30 m from point A'. The placement of pairs of access points AP1 and AP2, and AP1' and AP2' is more symmetric about the trajectory B-B', so switching from AP1/AP1' to AP2/AP2' is observed exactly at the middle of the B-B' (50 m from the point B and 50 m from the point B'). The values of the RSSI observed at the point of switching between access points

are the smallest values of the RSSI read at a given trajectory. In the case of the testbed presented in the Fig. 2, the minimum value of the RSSI did not depend on the type of network (a dedicated one or public), but on the length of trajectory only, and was:

- −69 dBm at the shorter trajectory (A-A'),
- −70 dBm at the longer trajectory (A-A').

Note that in the case of both trajectories, and of both scenarios, the −67 dBm limit for the minimal signal strength required by real-time media streaming was exceeded. The next, −70 dBm limit of applicability of non-real time non-media reliable transmission service was not exceeded, although in the case of the A-A' trajectory the minimum RSSI was equal to this limit. This means that the production network was at the limit of use (in terms of IoT transmissions). However, in the case of both S1 and S2 scenarios, the RSSI never exceeds the limit of basic connectivity (−80 dBm).

Comparative analysis of the RSSI obtained for dedicated and public production networks shows that in the case of both trajectories the RSSI achieved by a well-dimensioned, dedicated network, designed to optimize a flying monitoring system, was larger than or equal to the values of the RSSI observed in the case of the use of an existing, multi-purpose infrastructure. The largest differences were observed at end points of trajectories, and ranges from 22% (point A), through 18% (point B) and 11% (point B') to 9% (point A') in favor of the dedicated network. However, at close to the middle of each trajectory, this difference was smaller. As a result, on the last 20 m of the 70 m of the A-A' trajectory and on the last 35 m of the 100 m of the B-B' trajectory, the RSSI read in the dedicated network equals the RSSI read when the public network was used for transmission of monitoring data.

4.2 Available Data Rate and Total Throughput

The signal strength has an impact on the performance of the wireless communication. In the case of the evaluation of communication between stations of the flying monitoring system, two performance parameters were used:

- available data rate (a parameter of the network card), which is maximum data rate that can be obtained on a given network circumstances; this parameter is read from the settings of network card mounted at the air station,
- total throughput of the aggregated WebRTC stream, measured at the ground station.

Generally, the curve of the available data rate depends on the RSSI curve. In the case of the dedicated production network, at the very beginning and very end of trajectory A-A' (Fig. 4a) and B-B' (Fig. 4c) the maximal available data rate was set at 540 Mbps (points A, A', B, and B'). Then, according to the declining curve of the RSSI, it falls down until the air station changed its point of attachment. Then the curve of the available data rate rises, as does the RSSI

curve. The smallest values of the maximal available data rate were observed where the point of attachment changed. They values were 54 Mbps for A-A' trajectory and 26 Mbps for the B-B' trajectory.

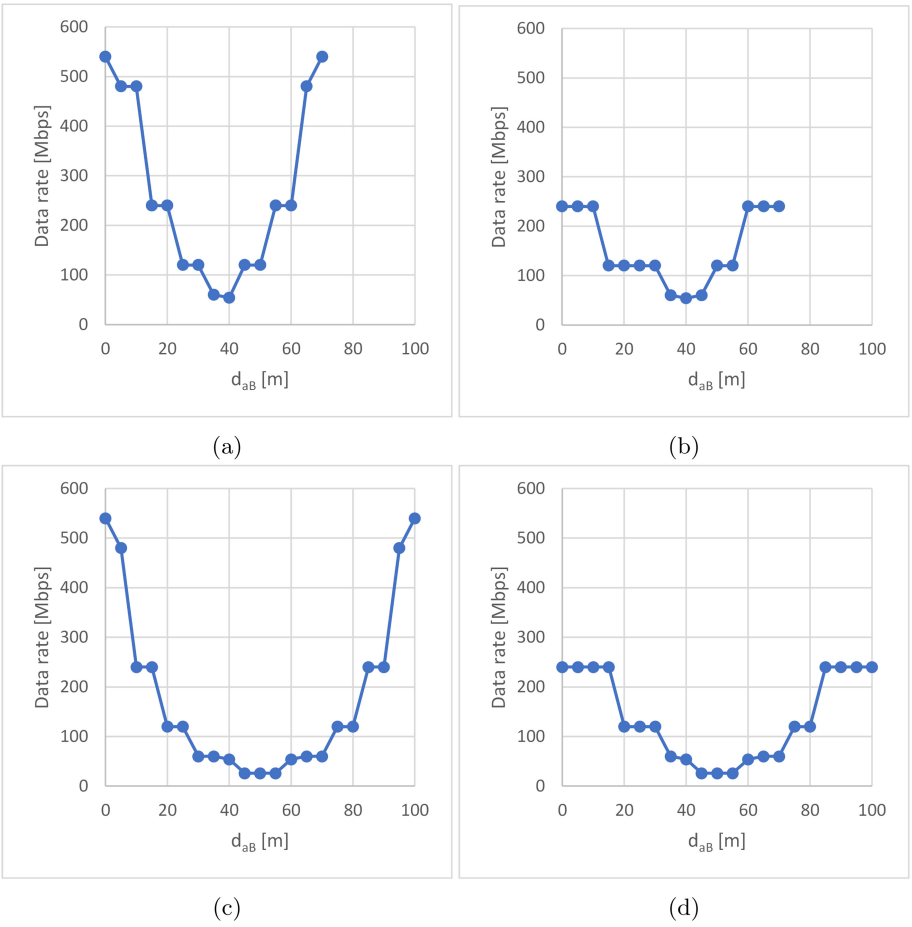

Fig. 4. Available data rate read in scenario: (a) S1, trajectory A-A'; (b) S2, trajectory A-A'; (c) S1, trajectory B-B'; (d) S2, trajectory B-B'.

In the case of a production network that uses an existing infrastructure, the curve of the available data rate is flatter than is drawn for a dedicated production network. At the very beginning of trajectory A-A' (Fig. 4b) and B-B' (Fig. 4d) the maximal available data rate was set at 240 Mbps (points A, A', B, and B'). However, the smallest values of the available data rate are the same as read for the dedicated network: 54 Mbps read when the air station follows the A-A' trajectory and 26 Mbps read for the B-B' trajectory.

The comparative analysis of the available data rate obtained for dedicated and public production networks shows that in the case of the A-A' trajectory, when the air station is close to the end points A and A', the available data rate set for the public network was two times smaller than the available data rate set for the dedicated one. And if the air station was exactly over the points A and A', the available data rate obtained for the public network was a little more than two times smaller. However, at 6 of 15 points of measurements established on this trajectory, there were no difference between the available data rate observed for the dedicated production network and the public one.

In the case of measurement points established along the B-B' trajectory, at almost the entire trajectory the differences between the available data rate read for the dedicated production network and the public one equals zero. Only if the air station was exactly over the points B and B', this difference was more than 100% in favor of the dedicated network. And five meters away towards the middle of the B-B' trajectory it was exactly 100% in favor of the dedicated network. As a curiosity at one of the measurement points this trend has been reversed: the available data rate read for the dedicated production network was two times smaller than read for the public network.

Despite the changes to the RSSI and the maximal available data rate, the curve of the total throughput of the aggregated WebRTC stream (Fig. 5) is almost completely flat whatever the trajectory is followed by the air station and however the production network is used. Almost all the time the throughput is 20 Mbps, and it falls to from 19.8 to 19.4 Mbps only when the air station changes its point of attachment to the DS.

Comparative analysis of the dedicated production network and the production network that uses an existing infrastructure shows that in the majority of the measurement points established along the trajectory A-A' and the trajectory B-B' the total throughput of the aggregated WebRTC stream measured for the dedicated production network was the same as measured for the public one. Only in two points of each trajectory, situated near the middle of this trajectory, were observed differences between total throughput. These differences were in favor of the dedicated network, and were about 1% of measured throughput. As a result, if the public network is well dimensioned, differences in the RSSI and the available data rate do not necessarily entails large differences in total throughput of aggregated WebRTC stream transmitted between the air station of the flying monitoring system and the ground one.

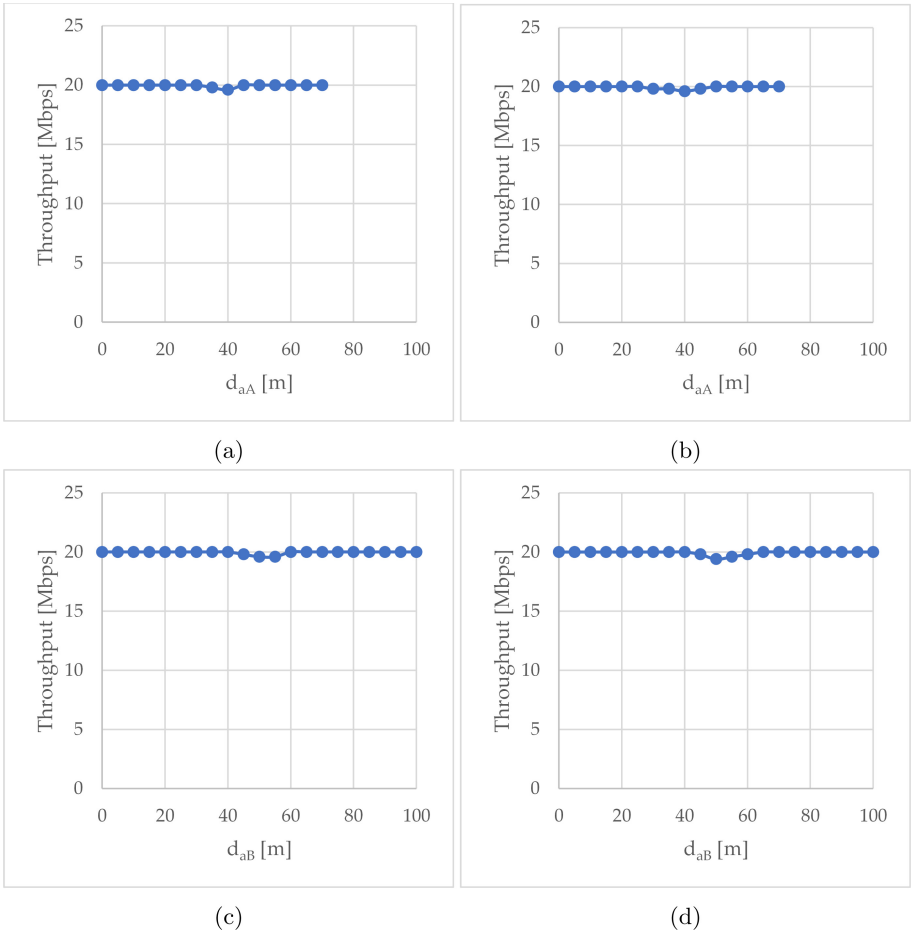

Fig. 5. Total throughput measured in scenario: (a) S1, trajectory A-A'; (b) S2, trajectory A-A'; (c) S1, trajectory B-B'; (d) S2, trajectory B-B'.

5 Conclusions

In the flying monitoring system, introduced in the authors' previous paper [9], to multiplex the data coming from the IoT devices and aggregate it with the video stream WebRTC technology was used. In this paper the performance evaluation of the aggregated WebRTC air-to-ground transmissions was carried out, and two implementations of the IEEE 802.11 network infrastructure connecting the air station and the ground one were taken into consideration.

The first one (S1 scenario) uses a dedicated IEEE 802.11 network infrastructure, which was designed and built especially for this flying monitoring system. The second (S2 scenario) uses an existing infrastructure covering the monitored area.

To analyze the performance of the air-to-ground transmissions the test trial was carried out at one of the parking lots of the AGH University of Science and Technology. Both the measurements of the total throughput of the aggregated WebRTC stream and the readings of the parameters set by the network adapter mounted on the air station (the RSSI and available sending rate) were analyzed.

Experimental results show that a dedicated network gives a little bit better performance at the cost of both the complicated physically building of and setup of the network, and the longer time to reach operational readiness (due to the necessity of performing practical tests of the area coverage). The usage of existing infrastructure, which is designed to work in a given area for ground-to-ground operation (not air-to-ground), gives not as good, but still satisfactory results.

References

1. Allman, M., Paxson, V., Stevens, W.: TCP congestion control. In: RFC2581, IETF (1999). https://doi.org/10.17487/RFC2581
2. Alzahrani, B., Oubbati, O.S., Barnawi, A., Atiquzzaman, M., Alghazzawi, D.: UAV assistance paradigm: state-of-the-art in applications and challenges. J. Netw. Comput. Appl. **166**, 102706 (2020). https://doi.org/10.1016/j.jnca.2020.102706
3. Baugher, M., McGrew, D., Naslund, M., Carrara, E., Norrman, K.: The secure real-time transport protocol (SRTP). In: RFC 3711, IETF (2004). https://doi.org/10.17487/RFC3711
4. Carrillo, D., Seki, J.: Rural area deployment of internet of things connectivity: LTE and LoRaWAN case study. In: 2017 IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON), pp. 1–4. IEEE (2017). https://doi.org/10.1109/INTERCON.2017.8079711
5. Castellanos, G., Deruyck, M., Martens, L., Joseph, W.: System assessment of WUSN Using NB-IoT UAV-aided networks in potato crops. IEEE Access **8**, 56823–56836 (2020). https://doi.org/10.1109/ACCESS.2020.2982086
6. Chen, L., Huang, Z., Liu, Z., Liu, D., Huang, X.: 4G network for air-ground data transmission: a drone based experiment. In: 2018 IEEE International Conference on Industrial Internet (ICII), pp. 167–168 (2018). https://doi.org/10.1109/ICII.2018.00028
7. Chodorek, A., Chodorek, R. R., Wajda, K.: An analysis of sender-driven WebRTC congestion control coexisting with QoS assurance applied in IEEE 802.11 wireless LAN. In: 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1–5. IEEE, Split, Croatia (2019). https://doi.org/10.23919/SOFTCOM.2019.8903749
8. Chodorek, A., Chodorek, R.R., Wajda, K.: Comparison study of the adaptability of layered and stream replication variants of the WebRTC simulcast. In: 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1–6. IEEE, Split, Croatia (2019). https://doi.org/10.23919/SOFTCOM.2019.8903887
9. Chodorek, A., Chodorek, R.R., Wajda, K.: Media and non-media WebRTC communication between a terrestrial station and a drone: the case of a flying IoT system to monitor parking. In: 2019 IEEE/ACM 23rd International Symposium on Distributed Simulation and Real Time Applications (DS-RT), pp. 1–4. IEEE, Cosenza, Italy (2019). https://doi.org/10.1109/DS-RT47707.2019.8958706

10. Chodorek, R.R., Chodorek, A., Rzym, G., Wajda, K.: A comparison of QoS parameters of WebRTC videoconference with conference bridge placed in private and public cloud. In: 2017 IEEE 26th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), pp. 86–91. Poznan, Poland (2017). https://doi.org/10.1109/WETICE.2017.59
11. Dai, H., Zhang, H., Li, C., Wang, B.: Efficient deployment of multiple UAVs for IoT communication in dynamic environment. China Commun. **17**(1), 89–103 (2020). https://doi.org/10.23919/JCC.2020.01.007
12. Duangsuwan, S., Chusongsang, A., Promwong, S.: Performance analysis of power outage probability for drone based IoT connectivity network. In: 2019 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), pp. 1–4 (2019). https://doi.org/10.1109/ISPACS48206.2019.8986314
13. Fan, Q., Ansari, N.: Towards traffic load balancing in drone-assisted communications for IoT. IEEE Internet of Things J. **6**(2), 3633–3640 (2018). https://doi.org/10.1109/JIOT.2018.2889503
14. Floyd, S., Handley, M., Padhye, J., Widmer, J.: TCP Friendly Rate Control (TFRC): protocol specification. In: RFC 5348. IETF (2008). https://doi.org/10.17487/RFC5348
15. García, B., Gortázar, F., Gallego, M., Hines, A.: Assessment of QoE for video and audio in WebRTC applications using full-reference models. Electronics **9**(3), 462 (2020). https://doi.org/10.3390/electronics9030462
16. Grozev, B., Politis, G., Ivov, E., Noel, T., Singh, V.: Experimental evaluation of simulcast for WebRTC. IEEE Commun. Stand. Mag. **1**(2), 52–59 (2017). https://doi.org/10.1109/MCOMSTD.2017.1700009
17. Holmer, S., Lundin, H., Carlucci, G., Cicco, L.D., Mascolo, S.: A Google congestion control algorithm for real-time communication. Internet-Draft, draft-ietf-rmcat-gcc-02, IETF (2016)
18. Iyer, V., Nandakumar, R., Wang, A., Fuller, S.B., Gollakota, S.: Living IoT: a flying wireless platform on live insects. In: The 25th Annual International Conference on Mobile Computing and Networking, pp. 1–15 (2019). https://doi.org/10.1145/3300061.3300136
19. Jesup, R., Loreto, S., Tuexen, M.: WebRTC data channels. Internet Draft, draft-ietf-rtcweb-data-channel-13, IETF (2015)
20. Jesup, R., Loreto, S., Tuexen, M.: WebRTC data channel establishment protocol. Internet Draft, draft-ietf-rtcweb-dataprotocol-09, IETF (2015)
21. Kim, J., Yun, J., Choi, S.C., Seed, D.N., Lu, G., Bauer, M., Al-Hezmi, A., Campowsky, K., Song, J.: Standard-based IoT platforms interworking: implementation, experiences, and lessons learned. IEEE Commun. Mag. **54**(7), 48–54 (2016). https://doi.org/10.1109/MCOM.2016.7514163
22. Kobayashi, T., Matsuoka, H., Betsumiya, S.: Flying communication server in case of a largescale disaster. In: 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), vol. 2, pp. 571–576 (2016). https://doi.org/10.1109/COMPSAC.2016.117
23. Lea, P.: Internet of Things for Architects: Architecting IoT Solutions by Implementing Sensors, Communication Infrastructure, Edge Computing, Analytics, and Security. Packt Publishing Ltd, Birmingham (2018)
24. Loreto, S., Romano, S.P.: Real-Time Communication with WebRTC: Peer-to-Peer in the Browser. O'Reilly Media, Inc., United States (2014)
25. Loreto, S., Romano, S.P.: How far are we from WebRTC-1.0? an update on standards and a look at what's next. IEEE Commun. Mag. **55**(7), 200–207 (2017). https://doi.org/10.1109/MCOM.2017.1600283

26. McGrew, D.: The Use of AES-192 and AES-256 in Secure RTP. RFC 6188. IETF (2011). https://doi.org/10.17487/RFC6188
27. Mohamed, A.M.A., AbuElgasim, A.E.: Controlling drone-using IOT platform. In: 2019 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), pp. 1–4 (2019). https://doi.org/10.1109/ICCCEEE46830.2019.9071087
28. Motlagh, N.H., Bagaa, M., Taleb, T.: UAV selection for a UAV-based integrative IoT platform. In: 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE (2016). https://doi.org/10.1109/GLOCOM.2016.7842359
29. Motlagh, N.H., Bagaa, M., Taleb, T.: UAV-based IoT platform: a crowd surveillance use case. IEEE Commun. Mag. **55**(2), 128–134 (2017). https://doi.org/10.1109/MCOM.2017.1600587CM
30. Park, J.H., Choi, S.C., Ahn, I.Y., Kim, J.: Multiple UAVs-based surveillance and reconnaissance system utilizing IoT platform. In: 2019 International Conference on Electronics, Information, and Communication (ICEIC), pp. 1–3. IEEE (2019). https://doi.org/10.23919/ELINFOCOM.2019.8706406
31. Rescorla, E., Modadugu, N.: Datagram Transport Layer Security Version 1.2. RFC 6347. IETF (2012). https://doi.org/10.17487/RFC6347
32. Roy, R.R.: Handbook of SDP for Multimedia Session Negotiations: SIP and WebRTC IP Telephony. CRC Press, Boca Raton, FL, United States (2018)
33. Saputro, N., Akkaya, K., Uluagac, S.: Supporting seamless connectivity in drone-assisted intelligent transportation systems. In: 2018 IEEE 43rd Conference on Local Computer Networks Workshops (LCN Workshops), pp. 110–116. IEEE (2018). https://doi.org/10.1109/LCNW.2018.8628496
34. Schulzrinne, H., Casner, S., Frederick, R., Jacobson, V.: RTP: A Transport Protocol for Real-Time Applications. RFC 3550. IETF (2003). https://doi.org/10.17487/RFC3550
35. Schulzrinne, H., Casner, S.: RTP profile for audio and video conferences with minimal control. RFC 3551. IETF (2003). https://doi.org/10.17487/RFC3551
36. Singh, V., Lozano, A.A., Ott, J.: Performance analysis of receive-side real-time congestion control for WebRTC. In: 2013 20th International Packet Video Workshop, pp. 1–8. San Jose, CA, USA (2013). https://doi.org/10.1109/PV.2013.6691454
37. Stewart, R.: Stream control transmission protocol. RFC 4960. IETF (2007). https://doi.org/10.17487/RFC4960
38. Tuexen, M., Seggelmann, R., Rescorla, E.: Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP). RFC 6083. IETF (2011). https://doi.org/10.17487/RFC6083
39. Van den Bergh, B., Chiumento, A., Pollin, S.: Ultra-reliable IEEE 802.11 for UAV video streaming: from network to application. In: El-Azouzi, R., Menasché, D.S., Sabir, E., Pellegrini, F.D., Benjillali, M. (eds.) Advances in Ubiquitous Networking 2. LNEE, vol. 397, pp. 637–647. Springer, Singapore (2017). https://doi.org/10.1007/978-981-10-1627-1_50