UbiComp'15 Proof-of-Concept: Aerial Detection of Wireless Signals using low-cost RPA

Jeffrey Putka
IUPUI School of Informatics
535 W Michigan St
Indianapolis, IN 46202
jputka@umail.iu.edu

Joshua Ward
IUPUI School of Informatics
535 W Michigan St
Indianapolis, IN 46202
wardje@umail.iu.edu

Pankaj Avhad
IUPUI School of Informatics
535 W Michigan St
Indianapolis, IN 46202
pvavhad@umail.iu.edu

Steven Voida
IUPUI School of Informatics
535 W Michigan St
Indianapolis, IN 46202
svoida@iupui.edu

Abstract
Shrinking computer form-factors, and the advancement of battery and brushless motor technology have allowed multi-rotor copters to become popular for hobbyists and enthusiasts. Ground control software enables the ability for such aircraft to fly pre-planned routes with automated behavior. In this demo, we show a concept of using such remotely piloted aircraft as a platform to perform contextual sensing of wireless access points and their associated data traffic.

Author Keywords
RPA, Remotely Piloted Aircraft, Drone, War-droning, War-driving, Wireless detection, mesh-networks, drone, civilian use, Contextual sensing, Packet Sniffing

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

General Terms
Design, Experimentation, Measurement, Security

Introduction
Technology is becoming increasingly ubiquitous in nature as has been the trend for several decades now. Technologies today are becoming increasingly dependent on knowing the environment which they are being deployed and used in. Furthermore, knowing what specific people are doing in the environment

and/or the general activities of that environment are becoming increasingly important for the ubiquity and usefulness of devices and applications. This awareness is often coined as “context aware computing.” One segment of the available data to gather such context that seems largely untapped is analysis of existing wireless signals.

Remotely Piloted Aircraft (RPA), or “drones” as often coined by news media or the public, have become small and cost effective enough to be accessible in large scale deployment situations by small businesses and the general public. The trend, like most technologies, has been smaller, cheaper, and more powerful and shows little signs of slowing anytime soon. RPAs offer many unique advantages in terms of ubiquitous applications over other devices. They can avoid obstacles by flying over and around them as they move through three dimensional space. They are flexible in both design and application and can be integrated into existing systems and outfitted for a variety of applications easily and inexpensively.

RPAs have the flexibility to add equipment to aid in detection and mapping of the environment around it, including various wireless signals. Having knowledge of the types of wireless devices in use at any given location gives numerous contextual indications. These include, but are by no means limited to: what other devices are in range that are broadcasting signals as various details about those signals; what their use is; whom is using them; when they are being used; and where they are located. This information may be used to help derive the context of surrounding activities and provide support to other applications such as acting as network relay nodes expanding the range and capacities of existing networks, while using those same networks to receive control instructions and transmit sensed data [2, 18].

“An obvious challenge of context-aware computing is making it truly ubiquitous.” “Although a complete definition of context remains an elusive research challenge, it is clear that in addition to who and where, context-awareness involves when, what, and why [1].” Combining contextual information to represent context accurately and in a meaningful way is key to solving this challenge. Implicit and explicit information are combined to define the context of interactions between the human and the environment. Presence and natural interactions in an environment combined with information such as their identity, location, effect, and identified activity are currently used to define context in many context-aware applications.

The information provided by such aerial systems could significantly aid in determination of contextual human activity. Population density in a particular area can be reasonably determined by detection of mobile signals. Using rapidly-deployable aerial platform sensing 802.11 emitters activities of mobile devices can capture and track particular device's' current locations and activities, population density, crowd movement patterns, among numerous others that can be used to aid in determining general context.

Our study builds upon the existing research by further exploring the ubiquitous nature of wireless data networks for integration with RPA operations. We intend to show RPAs can be introduced to existing environments where wireless communication is already present without the need for dedicated command and control equipment. This would reduce cost in both capital and human labor when RPAs as a platform for sensing and data relay, while increasing range beyond line of sight to ground control stations.

By demonstrating this ability and identifying and addressing challenges, numerous other uses can be derived based on the same setup. This includes both the transmittal of data by acting as a network node, and the use existing network nodes by employing them as relay points for command and control elements. We intend to show RPA based sensor systems can be built inexpensively with off the shelf components and software. Those systems can be augmented with existing networks. Such augmentation could be used to expand existing affordances and ranges. While this has been shown to be effective in terms of expanding and building mesh networks to supplement existing infrastructure [6], we will be demonstrating it using much smaller drones with off the shelf hardware and software. While expanding the network's capabilities the RPA can use the same networks for flight control.

In short their applications for context and helping overcome and aid in challenges existing when deploying technology in ubiquitous environments is vast. We intend to show through proof of concept that collection of such data can be done with off the shelf components at a low cost. Then we discuss the challenges we faced, and potential future applications.

Related Work

Currently, there are a number of studies focusing on the new affordances that Remotely Piloted Aircraft bring into the fold. They focus on single applications with specific purposes [6, 12, 17]. One looking to deliver content via portable displays, has already demonstrated the need for being able to detect and use wireless networks [16]. Studies have shown applications on larger more expensive RPA setups. For instance, one showed successfully that RPAs can be deployed to monitor signal strength of cellular towers. Using this information they showed success in guiding placement of additional aerial vehicles carrying cellular routing equipment to form an ad-hoc, in-air mesh network augmenting the cellular infrastructure based on dynamic and changing needs [18]. Similarly, another study showed traffic monitoring RPAs could use existing cellular networks both for data connection and command and control, eliminating the need for dedicated ground stations to be employed for RPA operations [2]. This has also been applied to post-disaster assessment and management as well as infrastructure development in disaster situations [3].

Design

An aerial platform was chosen for this task due to the unique affordances offered by RPAs as to sensing mobile and wireless data. Due to the aircraft's mobility, it can track signal strengths and associate them with its current location, in effect triangulating the precise positions of devices. This can be used to create an accurate mapping of the ground-based wireless environment quickly. Additionally, the mobile/aerial affordances render the platform unobstructed by obstacles, and with the aid of altitude; allows the platform to cover a wider area of collection coverage than a ground-based system. This allows sensing operations to take place where ground vehicles cannot travel, and reduces the cost of establishing permanent infrastructure when relaying data. The platform can travel to where it is needed most, dynamically.

Core Components

Remotely Piloted Aircraft (RPA) - "Multi-rotor copter"

The RPA we are using is a multi-rotor copter design which gives great flexibility to the aircraft's ability to perform complex maneuvers, hover in-place, and carry a wide variety of attached payloads due to its natural lifting capabilities and agnosticism to aerodynamic control surfaces needed for flight.

RPA Features

The RPA is controlled by a 3D Robotics 'Pixhawk' flight controller to enable remote operation, which is based from previous Arduino reference designs [19]. The flight controller uses a series of embedded and attached sensors including a barometer for altitude sensing, accelerometers for automated control pitch and yaw control, GPS and magnetometer for location and direction sensing, and a 900 MHz wireless modem for communication with a ground control station.

Figure 1. RPA Design

Payload

High gain Wi-Fi Antenna and receiver
Included in design for low cost, effective reception of the surrounding 802.11 standard Wi-Fi signals.

GPS receiver
Additional GPS receiver was included for ease of construction and to better fit our data needs.

Raspberry Pi
Low cost, credit-card sized small programmable fully functioning computer capable of plugging into a monitor or TV, interfacing with a standard keyboard and mouse [14].

Figure 2. Raspberry Pi Circuit Board

'Kismet wireless'
Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet also supports plugins which allow sniffing other media such as DECT [9].
Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, de-cloaking) hidden networks, and inferring the presence of non-beaconing networks via data traffic [9].

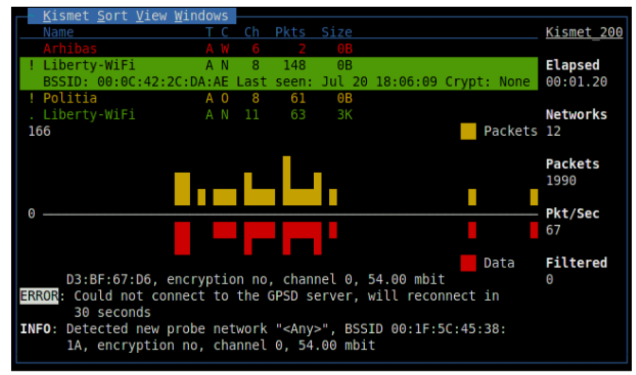

Figure 3. Kismet Wireless

Ground Control

Laptop computer
Standard laptop computer running windows 8.1 for centralized management of software and hardware needed to control the RPA as well as later analyze the results.

900 MHz wireless modem
Enables communication directly with the RPA.
'Mission Planner' - Open-source ground control software enabling the ability to plan mission routes using GPS waypoints [10].

Analysis Components

'Google Earth'

Geographical information program represented by a globe used to display aerial imagery and examine collected data by use of overlays [5].

'netxml2kml.py'

Python script used to format .netxml files output from Kismet wireless into a geo-rectified .kml for representation in Google Earth [11].

'kisheat'

Python script that renders temperature-map style overlays for Google Earth from Kismet wireless collection data [8].

Plan

The initial plan was to fly the RPA in a circular pattern in a suburban setting which would avoid tall buildings, obstacles, and other devices in the air. We will restrict our flight to under 500 feet above the ground and have no commercial interests in the use of the device as to keep within the limited regulatory framework that exists. These constraints also free us from consideration of most of the human factors that may have an impact on the research. Both of these issues have taken research directions of their own and take away from our overall research goals [4, 6, 7, 13, 15]. Using a suburban environment, we also take advantage of the commonality of wireless devices located in suburban households. The device will then collect and store information which will be downloaded after the flight. The data will then be reviewed manually. Finally the data will be uploaded into heat mapping software.

Results

A 2-minute flight revealed 122 unique devices; 39 of which were non-beaconing, as well as associated data traffic, signal strength, and GPS coordinates of detection and loss. Wireless Access points from the launch location that could be traditionally detected by native wireless connection applications on laptops and mobile phones were no more than twelve.

GPS signal data was later found to be incomplete shortly into main flight. Hand cleansing of the data so that it would be usable for heat map were required. Heat map contained a small subset of information. Despite the limited dataset it is included for demonstration purposes.


```
   <datasize>0</datasize>
  <snr-info>
    <last_signal_dbm>-63</last_signal_dbm>
    <last_noise_dbm>0</last_noise_dbm>
    <last_signal_rssi>0</last_signal_rssi>
    <last_noise_rssi>0</last_noise_rssi>
    <min_signal_dbm>-81</min_signal_dbm>
    <min_noise_dbm>0</min_noise_dbm>
    <min_signal_rssi>1024</min_signal_rssi>
    <min_noise_rssi>1024</min_noise_rssi>
    <max_signal_dbm>-57</max_signal_dbm>
    <max_noise_dbm>-256</max_noise_dbm>
    <max_signal_rssi>0</max_signal_rssi>
    <max_noise_rssi>0</max_noise_rssi>
  </snr-info>
  <gps-info>
    <min-lat>39.992920</min-lat>
    <min-lon>-86.178398</min-lon>
    <min-alt>270.471008</min-alt>
    <min-spd>0.000000</min-spd>
    <max-lat>39.993233</max-lat>
    <max-lon>-86.177933</max-lon>
    <max-alt>277.776001</max-alt>
    <max-spd>2.161000</max-spd>
    <peak-lat>39.993027</peak-lat>
    <peak-lon>-86.178192</peak-lon>
    <peak-alt>270.947998</peak-alt>
    <avg-lat>-177.342663</avg-lat>
    <avg-lon>-179.321990</avg-lon>
    <avg-alt>-175665.895200</avg-alt>
  </gps-info>
  <bsstimestamp>766577254789</bsstimestamp>
  <cdp-device></cdp-device>
  <cdp-portid></cdp-portid>
  <seen-card>
   <seen-uuid>43a3ec98-e61c-11e4-93c9-98086a627a0
   <seen-time>Sat Apr 18 22:51:59 2015</seen-time
   <seen-packets>83</seen-packets>
  </seen-card>
  <wireless-client number="1" type="fromds" first
```


Figure 4. Sample Kismet .netxml data

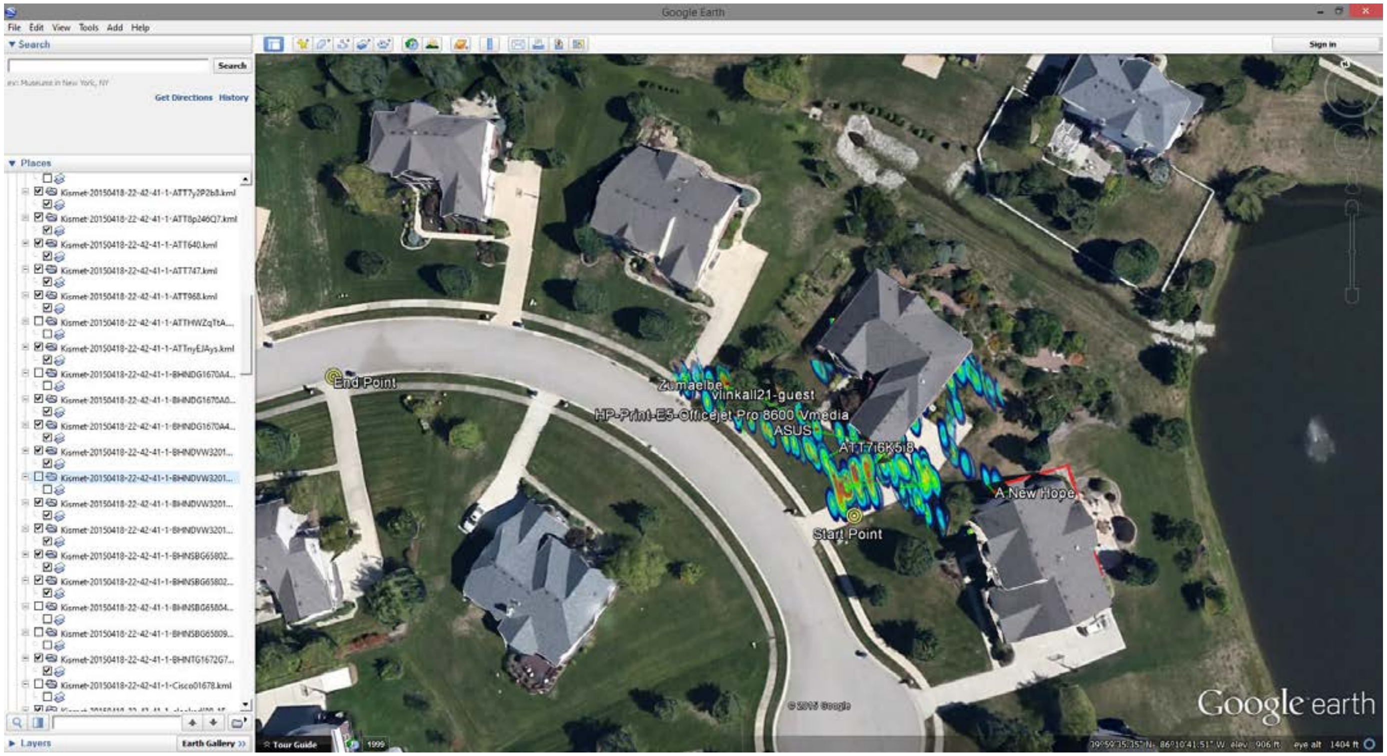

Figure 5. Heat Map

Issues and Challenges

Our vision to use Mission planner to plan the flight route ahead of time and let the device operate autonomously during the flight, and then return to the launch point failed. Shortly into the flight it was apparent that the device was not properly using the flight data, as at ascended to an unanticipated altitude.

We switched the remote piloting capabilities on through manual piloting of the aircraft using remote control. Navigating the RPA in terms of both finding the flight plan and then struggling with the mission planner software was the largest challenge we faced.

The largest issue we foresaw facing others looking to deploy such technologies is in terms of the user interface. The interfaces that are used to program and interrupt the RPA, and the individual components that we added to it are not relatively user friendly. Deployment to a larger audience such as small businesses or the general public will demand a friendlier user interface and the ability to both gather the information needed as well as well as present it in a useful manner. This issue manifested it further when enabling GPS functionality with Kismet Wireless on the Raspberry Pi, as the status of the logging could not be determined until after flight. After completion of the first successful long-duration flight, it was discovered that the GPS failed to log upon initial examination of the logging data. This failure led to a subsequent test flight of significantly shorter duration.

During our short test we collected a large amount of data. We found various devices including small devices such as streaming media players and printers. While as researchers we found this plethora of information to be exciting in its application the collection, storage, and broadcasting of such information in real time is costly in terms of energy and hardware needed to handle this.

Our recording of the GPS signal also failed early on in our test flights, leading to a short duration flight to validate integrity of the RPA's onboard sensors. Due to the shortened duration of the flight as well as limited GPS coordinates, creating a heat map that was accurate and provided useful information was both challenging and ineffective.

In order to provide useful knowledge from the data collected real time processing of this information will need to occur. Communication of data from the RPA to ground control provides a unique set of challenges. The environment in which the RPA operates varies widely and is subject to interference, failure, and corruption. We worked around these by using the RPA to store the data during the flight and then uploading it after the fact for processing.

Discussion

The largest challenge that will need to be addressed before adoption on a larger scale will be in terms of a programmable interface that is user friendly. Most of the tools available today are created with functionality and hobbyists in mind. They are not intuitive, standardized, or easy to use. This is what we believe to be the largest barrier behind only regulatory issues. Solutions to this could include both making such interfaces more user friendly and also creating deployable RPAs designed with the capture, broadcast, and processing of this information in mind. For instance a dedicated winged RPA platform that is designed to loiter in circles could be an effective alternative for reading and reporting signals that are within a fixed area. The area has much opportunity for further design and research.

The largest challenge that we faced as researchers in terms of this project was error correction. Loss of the GPS signal early on in our test flights was undetected until after the main series of flights were conducted. Superficially everything appeared well until we ran into struggles attempting to port information over for processing into the heat map. While we had a redundant GPS sensor, the reasoning was for ease of programming. The main GPS sensor would require physical wiring and coding into in order to get information into the logs. We disabled it and used the secondary one for simplicity/ease.

To achieve a truly ubiquitous state of operation, the need for human intervention will have to be designed around. The potential loss of device or loss of the RPA's ability to pilot itself as well as any other errors that such a device may run into are going to be a reality even under situations where common problems in design and function are worked through. In this short testing period we lost two critical functions to our project. The ability to switch from an automatic to manual mode requires both that a human directly in control of the device to be present, as well the hardware needed to receive remote commands. Both of these are costly in terms of labor, energy, and hardware that the device must support. Designing solutions that take these issues into consideration, with failure as the rule and not the exception, will be critical components in realizing the true opportunities that such technologies afford.

To truly realize the opportunities that such technologies present solutions will need to be developed that account for both real time collection and processing of this information. Due to the constraints of energy availability, we believing that the RPA will need to broadcast this information and the reception and analysis of such information will need to occur on the ground. We believe such information should be broadcast in its pure form and what is done with it determined on the ground. In order for this to work seamlessly over a greater distance than our testing the RPAs will either need to be efficient at communicating and cooperating with each other or investment and research into a ground infrastructure may be needed. Likely, the most effective solutions may involve a combination of these factors.

When developing solutions based on collection and the forwarding of data collected by the RPA, designers need to be aware of the energy and hardware resources needed to collect and use such a wide variety of information that such devices are capable of intercepting. Depending on the particular application, what information is captured and broadcast as well as what form, provides a unique set of design challenges. Any decision making occurring at the device level and the energy requirements to make such decisions making will need to be balanced with the cost savings realized by broadcasting this information to the ground infrastructure. We believe there is opportunities for such information decision making to be hard coded into the hardware such that the decision making could be both energy efficient and saving in terms of the energy requirements of communicating this information. This is an area of future research, design, and development.

Conclusions and Future Work

The largest challenges that are in the immediate future still remain technical challenges, regulatory challenges, and user friendliness. Advances over the last years has made the technology possible, available, and inexpensive. The user friendliness of the applications we use to interface with these devices are largely designed around functionality and not deployment over a larger scale. Significant opportunity exists for businesses and developers to create platforms that are easy to use and are designed for specific application of the technologies. Despite this battery life and challenges in regards to technical issues currently pose some of the greatest limitations upon their widespread use. Legal and regulatory uncertainties as well as the current ban against using RPAs for any for profit purpose in the US are stifling significant investment in the field. We remain optimistic once some of this uncertainty is cleared up and businesses have less risk to absorb in terms of investment into this market that many of these challenges will be resolved through innovation.

The next step for this research directly would be to either switch out or amend to the 802.11 wireless detection system with one that can detect various signals being broadcasted from cellular phones and other devices. We believe there is significant opportunity in regards to the detection of cell phones as the application of such data in real time. Thanks to existing research in the field it has already been useful in large scale deployments to supplement existing networks especially in cases of disaster or other non-normal conditions, such as large gathering crowds for events. While large military style deployments of these systems have large scale infrastructure and emergency uses; the ability to deploy them at low cost could allow for a less centralized or more flexibility by introducing opportunity for smaller businesses and civilians.

Most of these applications also point to another issue that will need more research, work, and cooperation into which is the ability for these RPAs to detect, communicate, share, and protect themselves from each other. Opportunities and difficulties in this area provide significant challenges to both designers, business, and regulatory agencies.

RPA's deployed on a small scale also open up a Pandora's Box in regards to privacy. We were able, using software that is easily obtained and equipment that is already relatively inexpensive and affordable to gather a plethora of information about devices around the RPA. This information was collected in just a matter of minutes and given enough time could have afforded us an opportunity to use this information potentially malicious ways without the realization of those around us knowing we had even collected this information or acted on it. Even malicious intent aside, as researchers having collected this data opened up the possibility for it to be exposed, stolen, or otherwise used by parties outside our control. All of these issues and many more face the use of this technology. These problems demand more extensive research and attention then they have gotten as this proof of concept demonstrates, these are not tomorrow's problems or some future consideration. These privacy concerns are already here and it's not just possible but likely probable that they are being deployed and used by people whose intentions are not merely for research and demonstration.

Ultimately, the potential applications and benefits to these technologies are vast. The ability to put these in the hands of the general public, small businesses, and various levels of government at a low cost in a way that could be productive is already here.

Acknowledgements

We appreciate the opportunities afforded to us by Indiana University and the IUPUI campus. Special thank you to Dr. Stephen Voida for his guidance and support in this project. This couldn't also have been possible without researchers from around the globe, some cited below, but in numerous other areas from battery research to military development. True innovation and opportunity lie in this field and without the participation and support of each and every one our project would not have been possible in the manner that it was currently. Finally, thank you to our friends and family which support us both in helping with elements of this project and general support.

References

[1] Abowd, G.D., Mynatt, E.D., & Rodden, T. (2002). The human experience. IEEE Pervasive Computing, 1 (1), 48–57

[2] Chen, Y. M., Dong, L., & Oh, J. S. (2007, March). Real-time video relay for uav traffic surveillance systems through available communication networks. In Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE (pp. 2608-2612). IEEE.

[3] Ezequiel, C. A. F., Cua, M., Libatique, N. C., Tangonan, G. L., Alampay, R., Labuguen, R. T., ... & Palma, B. (2014, May). UAV aerial imaging applications for post-disaster assessment, environmental management and infrastructure development. In Unmanned Aircraft Systems (ICUAS), 2014 International Conference on (pp. 274-283). IEEE.

[4] Goodman, E., & Paulos, E. (2004). The familiar stranger: anxiety, comfort, and play in public places.

[5] Google Earth. https://www.google.com/earth/

[6] He, D., Ren, H., Hua, W., Pan, G., Li, S., & Wu, Z. (2011, September). FlyingBuddy: augment human mobility and perceptibility. In Proceedings of the 13th international conference on Ubiquitous computing (pp. 615-616). ACM.

[7] Hobbs, A., & Shively, R. J. Human Factor Challenges of Remotely Piloted Aircraft.

[8] Kisheat. https://code.google.com/p/kisheat/

[9] Kismet Wireless. https://www.kismetwireless.net/

[10] Mission Planner Ground Station. http://planner.ardupilot.com/

[11] Netxml2kml. http://www.salecker.org/software/netxml2kml/en

[12] Nozaki, H. (2014, April). Flying display: a movable display pairing projector and screen in the air. In CHI'14 Extended Abstracts on Human Factors in Computing Systems (pp. 909-914). ACM.

[13] Quaritsch, M., Stojanovski, E., Bettstetter, C., Friedrich, G., Hellwagner, H., Rinner, B., ... & Shah, M. (2008, September). Collaborative microdrones: applications and research challenges. In Proceedings of the 2nd International Conference on Autonomic Computing and Communication Systems (p. 38). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[14] Raspberry Pi Micro Computer. https://www.raspberrypi.org/

[15] Schmidt, A., Pfleging, B., Holz, C., & Holmquist, L. E. (2014). From Photography to Ubiquitous Capture Systems. Pervasive Computing, IEEE, 13(1), 10-13.

[16] Schneegass, S., Alt, F., Scheible, J., Schmidt, A., & Su, H. (2014, April). Midair displays: Exploring the concept of free-floating public displays. In CHI'14 Extended Abstracts on Human Factors in Computing Systems (pp. 2035-2040). ACM.

[17] Tei, K., Aizawa, K., Suenaga, S., Takahashi, R., Lee, S., & Fukazawa, Y. (2014, September). HoppingDuster: self-adaptive cleaning robot based on aerial vehicle. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (pp. 271-274). ACM.

[18] Wei, P., Gu, Q., & Sun, D. (2013, June). Wireless sensor network data collection by connected cooperative UAVs. In American Control Conference (ACC), 2013 (pp. 5911-5916). IEEE.

[19] 3D Robotics Pixhawk Flight Controller. http://3drobotics.com/kb/pixhawk/