



Research Repository UCD

Title	Enabling End-to-End Secure Connectivity for Low-Power IoT Devices with UAVs
Authors(s)	Rajakaruna, Archana, Manzoor, Ahsan, Porambage, Pawani, Liyanage, Madhusanka
Publication date	2019-04-18
Publication information	Rajakaruna, Archana, Ahsan Manzoor, Pawani Porambage, and Madhusanka Liyanage. "Enabling End-to-End Secure Connectivity for Low-Power IoT Devices with UAVs." IEEE, 2019.
Conference details	The 2019 IEEE Wireless and Networking Conference Workshops, Marrakech, Morocco, 15-18 April 2019
Publisher	IEEE
Item record/more information	http://hdl.handle.net/10197/11693
Publisher's statement	© 2019 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
Publisher's version (DOI)	10.1109/WCNCW.2019.8902746

Downloaded 2024-04-17 09:24:12

The UCD community has made this article openly available. Please share how this access benefits you. Your story matters! (@ucd_oa)



© Some rights reserved. For more information

Enabling End-to-End Secure Connectivity for Low-Power IoT Devices with UAVs

Archana Rajakaruna*, Ahsan Manzoor*, Pawani Porambage*, Madhusanka Liyanage*[†],
Mika Ylianttila*, Andrei Gurtov[†]

*Centre for Wireless Communications, University of Oulu, Finland

[†]School of Computer Science, University College Dublin, Ireland.

[†]Department of Computer and Information Science, Linköping University, Sweden

*{firstname.lastname}@oulu.fi, [†]madhusanka@ucd.ie [†]gurtov@acm.org

Abstract—The proliferation of the Internet of Things (IoT) technologies have strengthen the self-monitoring and autonomous characteristics of the sensor networks deployed in numerous application areas. The recent developments of the edge computing paradigms have also enabled on-site processing and managing the capabilities of sensor networks. In this paper, we introduce a system model that enables end-to-end secure connectivity between low-power IoT devices and UAVs, that helps to manage the data processing tasks of heterogeneous wireless sensor networks. The performance of proposed solution is analyzed by using simulation results. Moreover, in order to demonstrate the practical usability of the proposed solution, the prototype implementation is presented using commercial off-the-shelf devices.

Index Terms—Internet of Thing (IoT), Sensor Nodes, Bluetooth Low Energy (BLE), Unmanned Aerial Vehicle (UAV)

I. INTRODUCTION

The world of Internet of Things (IoT) allows the data retrieved by multiple smart devices to transmit to different cloud servers, in order to build a more comprehensive picture of the whole ecosystem [1]. However, this needs seamless connectivity between the IoT sensor and the central cloud (i.e., end-to-end connectivity), which is hard to be guaranteed every time [2]. Edge computing paradigms (eg., Fog computing, cloudlets) have appeared to bridge the gap between remote clouds and the IoT devices [3], [4].

Typically, low power IoT devices are equipped with unlicensed band short-range radio access technologies, including Bluetooth Low Energy (BLE), HaLow, ZigBee, and Smart Utility Networks (SUNs) [5]. BLE is a commonly used stateless protocol where the requests are independently transmitted. Moreover, BLE allows a flexible topology that can be adjusted to accommodate in many applications [6]. The IoT sensor nodes that use standalone BLE for communication purposes require dedicated nodes that serve as local gateways (GWs) to provide back-end connectivity with the central cloud servers. In our previous work, we presented a mobile-based relay assistance solution for establishing secure End-to-End (E2E) connectivity between low-power IoT sensors and cloud servers without using a dedicated gateway [6], [7].

Recently, Unmanned Aerial Vehicle (UAV) systems or drones received great attention for autonomous monitoring applications [8]. However, to the best of our knowledge there is still no sufficient work available to show the synergies between UAV systems and low power IoT devices and their cooperative

applicability with practical implications in sensor networks. To describe the concept of integrating end-to-end secure connectivity between low power IoT devices and UAVs in a real world problem, we contemplate a smart agriculture use case which consists of deployed wireless sensors. Therefore, we propose this system to a remote agricultural site which is difficult to reach and monitored by humans frequently. A drone can be sent to the farm site to collect sensed data and perform actions (e.g. apply water or fertilizer, activate crop monitoring sensors). These actions can be activated based on the data received by the sensors, which are then processed already at the drone. The user can control the drone, send control commands, or program the flight route whenever needed. Similar setup can be used for environmental monitoring, disaster detection, anomaly detection in sensor networks or mobile crowd sensing applications. This setup can be extended for dew computing [9] based applications.

We present a novel edge computing based architecture which entails an UAV to assist data retrieving, data processing, and data management in a heterogeneous Wireless Sensor Network (WSN) located in a remote area. The proposed system supports edge computing architecture to provide both insight and remote processing capabilities to the remotely located IoT sensor networks. Instead of using mobile phone as the relay in [6], here we use a drone accompanied by a Raspberry Pi to perform as an edge processor. We have proven the viability of the proposed solution by providing the comprehensive analysis of the simulation results. Finally, a prototype implementation is presented using commercial off-the-shelf devices to demonstrate the practical viability.

The remainder of the paper is organized as follows: Section II describes the proposed architecture and the communication protocols. Section III and IV present the simulation and implementation results of the proposal. Finally, Section V concludes the paper by drawing the future research directions.

II. THE PROPOSED ARCHITECTURE

A. System Model

As illustrated in Figure 1, we consider heterogeneous IoT devices which contain diversified sensor nodes with different capabilities whereas the drone is performing as the edge server. It will perform as a lightweight server and serves one sensor at a time. Drone can provide end-to-end connectivity from

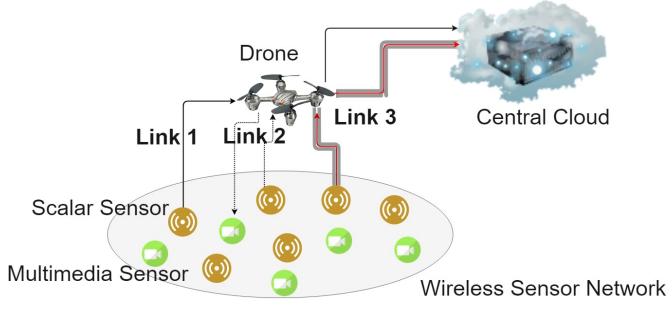


Fig. 1: Use case scenario

the sensor to cloud when there is Internet connectivity or allow offline accessibility otherwise. The drone will perform on site data processing and take the control functions of the IoT sensor network. These can be sensor nodes that monitors the environmental conditions and collect data or the actuator devices that perform given actions based on the received commands. We consider three types of links that can exist in this particular setting.

- **Link 1:** Sensors collect data and send to the central cloud via the drone, when the drone is returned to home location. Drone can access and process the retrieved data.
- **Link 2:** Sensors collect data and send to drone for further processing. Drone controls the actuator nodes based on the retrieved data. No data is transferred to the central cloud. As in edge computing paradigm, the drone will provide offline data accessibility to the actuator nodes, even though without real-time access to the central cloud.
- **Link 3:** Sensors collect data and send to the central cloud via the drone in the encrypted format. Drone is acting as a relay and cannot decrypt the data. Data offloading from the drone to cloud can be performed once the drone returns to home location.

B. Communication Protocol

Two communication protocols are used in the proposed architecture. First protocol is used to upload the data from sensor node to the drone and second protocol is used to download the data from the drone to the sensor node.

1) *Data upload process:* Figure 2 illustrates the message sequence between the sensor node, BLE module and the drone for the data upload process. Drone initiates the connection establishment process by sending connection request to the BLE module of the sensor node. Then BLE module acknowledges the connection request and connects with the drone. Next, BLE module requests data from sensor node, which has already been saved inside the sensor node. Then, sensor node writes data on BLE modules local attribute. After that, BLE module notifies the drone that it has data to be transferred to the drone. Drone then sends attribute read request to the BLE module. Once the attribute request is acknowledged by BLE module, drone starts reading data and sends acknowledgment to the BLE module to ensure a reliable communication between the drone and the BLE module. This process continues until the drone retrieves required information and then the drone

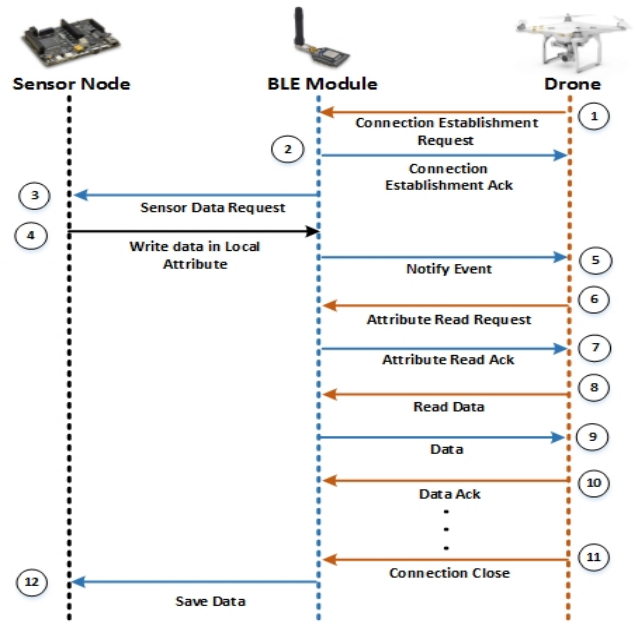


Fig. 2: Communication Protocol for data upload process

terminates the connection. Once the drone has terminated the connection, BLE module sends a command to the sensor node to save the data until it makes another connection with the drone in its next flying cycle.

2) *Data download process:* Figure 3 illustrates the message sequence between drone, BLE module and the sensor node during data download. Similar to the upload procedure, drone initiates the connection process by sending connection request to the BLE module of the sensor node. BLE module acknowledges this request and connects with drone. Then the drone begins data download by requesting attribute writing permission from BLE module. Afterwards, BLE module acknowledges the request from the drone and starts retrieving data from drone. At the same time, BLE module sends the command to the sensor node to save those data in flash memory. Drone also receives an acknowledgement so that it knows the data has been successfully transferred. After the successful completion of data transfer, drone terminates the connection.

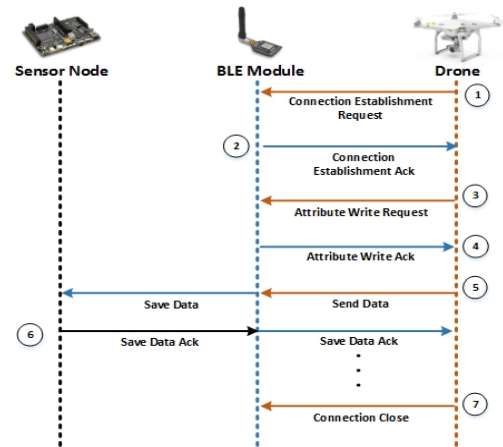


Fig. 3: Communication Protocol for data download process

III. NUMERICAL ANALYSIS

To measure the performance of the proposed system, we implemented a simulation using MATLAB simulator. Simulation steps are explained below. Results of the simulation provide the number of sensor nodes, for which the drone can fly and collect its data, during one flying cycle.

In the simulation setup, we considered three main sensor node arrays as depicted in Figure 4, which can be practically deployed in the environment. Therefore we contemplated the linear, circular and square orientations of sensor node arrays. For each array, we observe the number of sensor nodes in the array supported during drones one flying cycle, assuming that the drone starts flying from the first sensor node of the array.

We consider that the sensor node array is comprised of n sensor nodes as depicted in Figure 4. For the square sensor node array i. e. $(\sqrt{n} \times \sqrt{n})$ where we consider (\sqrt{n}) as an odd number.

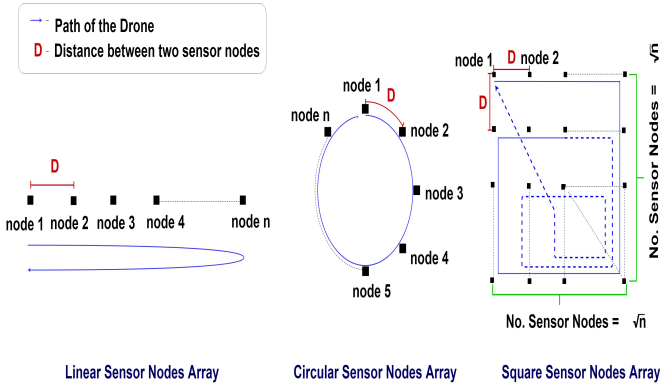


Fig. 4: Orientation of Sensor Arrays

Following (3), (4) and (5) equations illustrate the relationship between drones maximum hovering time and number of sensor nodes that can be covered during data collection procedure. Those equations were derived using the general flying time equation depicts in equation (1), where n is the number of sensor nodes in a particular array.

$$T_F = (n \times T_W) + \frac{\text{Distance between all nodes}}{S} \quad (1)$$

$$T_W = \frac{T_P}{60} + \frac{T_{DL}}{60} + \frac{R_S(T_C + T_F)}{R_{BLE}} \quad (2)$$

$$n_1 = \frac{T_F + \frac{D}{30S}}{T_W + \frac{D}{30S}} \quad (3)$$

$$n_2 = \frac{T_F}{T_W + \frac{D}{30S}} \quad (4)$$

$$n_3 = \left\{ \frac{\frac{-D}{\sqrt{2}} + \sqrt{\frac{D^2}{2} + 4A \times \left(1 + \frac{1}{\sqrt{2}}\right)D + 60ST_F}}{2A} \right\}^2 \quad (5)$$

$$A = (60ST_W) + D \quad (6)$$

Where, T_W is the drone's waiting time near a sensor node. n_1, n_2, n_3 are the number of sensor nodes in linear sensor node array, circular sensor node array and square sensor node array respectively that can be covered during data collection procedure. T_F is the total flying time of the drone, assuming that the drone starts flying from the first sensor node of the array. T_C is the battery charging time of the drone, T_P is the data processing time of Raspberry Pi, T_{DL} is the data download time from Raspberry Pi to sensor node and S is the speed of the drone. R_{BLE} is the data transfer rate between Raspberry Pi and sensor node, R_S is the data generation rate of sensor node and D is the distance between two sensor nodes. A is used for simplify the equation (5).

Table I summarizes parameters we used in the experiments in order to obtain the simulation results. Moreover, we have evaluated how significantly each parameter contributes to decide the number of sensor nodes serviced by the drone.

TABLE I: General simulation parameters

Parameter	Value
Total flying time (T_F)	25 minutes [10]
Battery charging time of the drone (T_C)	90 minutes [10]
Data processing time of the drone (T_P)	1 second
Data download time from drone to node (T_{DL})	10 seconds
Data generation rate of the sensor node (R_S)	20 B/min [11]
BLE data rate between drone and node (R_{BLE})	10.5×10^4 B/min [12]
Speed of the drone (S)	12 m/s
Distance between two sensor nodes (D)	100 m

Figure 5 illustrates the results of the experiment obtained using MATLAB simulator.

A. Impact of BLE Data Rate

In our proposed system, we use BLE communication protocol between the drone and the sensor nodes. Data rate of BLE communication has a significant impact on waiting time of the drone near the location of sensor node. Waiting time of the drone at a sensor node decreases as BLE data rate increases. Therefore, with lower waiting time spent at a particular sensor node, drone can collect data from more sensor nodes throughout its maximum flying time.

In order to illustrate the relationship between the BLE data rate and the number of sensor nodes supported at each BLE data rate, we considered different values for BLE data rate and executed the simulation. We considered BLE data rate (R_{BLE}) as 2 kbps, 4 kbps, 8 kbps, 12 kbps, 16 kbps while keeping the other parameters fixed. These parameters are depicted in Table I. This experiment has been carried out for all three sensor node arrays i.e. linear, circular and square.

Figure 5(A) illustrates the results of the simulation. It is clear that, with a higher BLE data rate, drone is capable to collecting data from more nodes and this observation is valid for all three sensor node arrays. Results further demonstrated that circular and square arrays yield better performance than the linear array of sensor nodes.

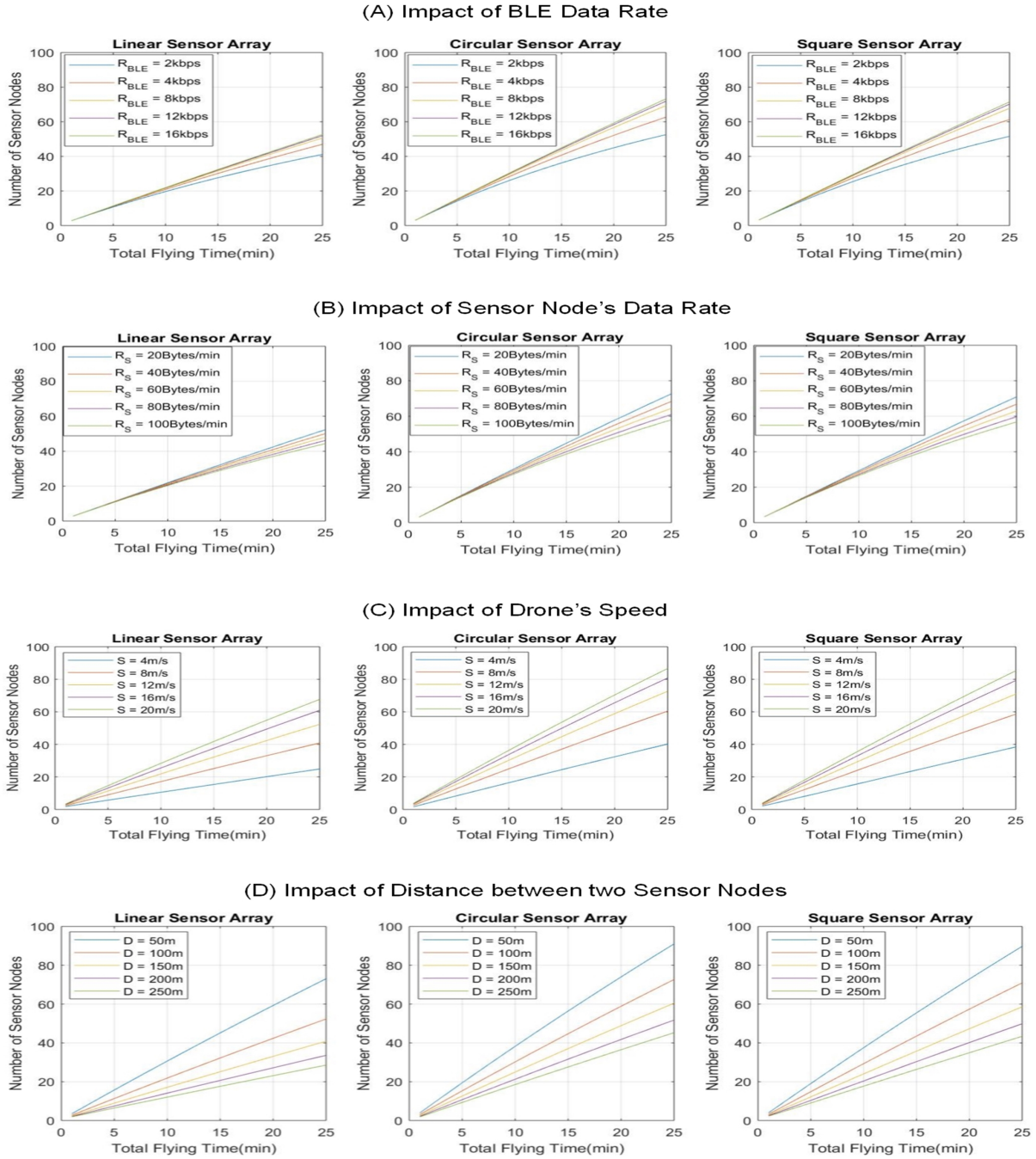


Fig. 5: Simulation Results

B. Impact of Sensor Data Rate

Sensor node data rate, also has a substantial impact on the performance of the system. With lower sensor node data rate, drone can collect data from more sensor nodes than having higher data rates. This behaviour is opposite to the behaviour we considered for BLE data rate. When the sensor data rate is low, the amount of data that the drone has to collect is low, thereby requiring a less amount of time to retrieve the data. Figure 5(B) illustrates the simulation results for this scenario. Here we have changed sensor node's data rates(R_S) as 20

Bytes/min, 40 Bytes/min, 60 Bytes/min, 80 Bytes/min, 100 Bytes/min while keeping other parameters in Table I fixed. Also we assumed one in-built sensor generates 20 Bytes/min. In this case also, circular and square arrays provided better performance than linear sensor node array.

C. Impact of Drone's Speed

In our prototype implementation, we used DJI Phantom 3 SE drone which is capable of flying at maximum 16 m/s [10]. For the simulation experiments we used 12 m/s as

average speed(S) considering the time taken to accelerate and decelerate. By using a drone with a higher maximum flying speed, the performance of the system can be enhanced. In order to validate this phenomenon, we carried out our simulation experiments from lower drone speeds to higher speeds. We changed speed values as 4, 8, 12, 16, 20 m/s while keeping other parameters fixed as in Table I. Figure 5(C) illustrates the simulation results for this scenario. According to Figure 5(C), drones with higher speed are capable of collecting data from more sensor nodes than drones with lower speeds. In this case also, circular and square array provided better performance compared to linear array.

D. Impact of Distance Between Sensors

In order to analyze how the distance between two sensor nodes affects the number of sensor nodes supported, we used 50 m, 100 m, 150 m, 200 m, 250 m as distance(D) and carried out the simulations. In this case also we kept other parameters fixed as in Table I. Based on the results as depicted in Figure 5(D), the lower the distance between two sensor nodes, the higher the number of sensor nodes supported by the drone during data collection. Moreover, circular and square arrays provided better system performance than the linear array.

IV. PROTOTYPE IMPLEMENTATION

To establish the prototype implementation we used five Wasmotes with BLE modules, a Raspberry Pi 3 and a DJI phantom 3 SE [10] drone as core instruments of the setup.

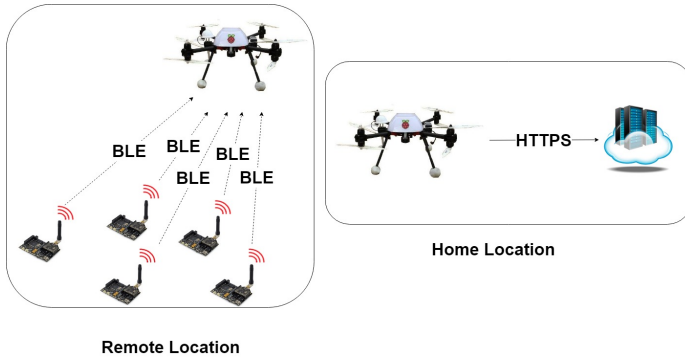


Fig. 6: Prototype

Figure 6 illustrates system model of the prototype implementation. For the prototype implementation, we first implemented the Wasmote sensor network. To setup the BLE communication capability of Wasmote we used Wasmote BLE module introduced by Llibelium [11]. For the implementation, we considered Wasmote's in-built accelerometer generated data. This data is then transferred to Raspberry Pi over BLE. Raspberry Pi is coupled with the drone. Generally, Raspberry Pi 3 is powered by a +5.1V micro USB supply and recommended input current is 2.5A [13]. To cater these specifications we used a portable external power source coupled with Raspberry Pi. This prototype implementation was basically based on two scenarios, real time and non-real time.

To initialize the connection between Raspberry Pi and Wasmote sensors, we defined Wasmote as the master and Raspberry Pi as the slave. Therefore Wasmote sends advertising packets to Raspberry Pi through advertising attribute and then Raspberry Pi sends the connection request to Wasmote to establish the connection. Moreover, Raspberry Pi uses the MAC addresses of Wasmotes to establish the connection.

The real time scenario has implemented to collect the data when the drone is within the range of sensor network. Hence, in the real time scenario we created a local attribute in Wasmote for data transferring process. Therefore we programmed a handler in BLE user services profile of Wasmote to send the accelerometer sensed data to Raspberry Pi attached to the drone.

Non-real time scenario has proposed and implemented to maintain the continuity of data collection while drone was away from the sensor network. In the non-real time scenario Wasmote generates the accelerometer data and saves them into a text file in its SD memory. When, the drone arrives Wasmote sends those text files through pre-defined handler as in the real time scenario.

After extracting the sensed data (real time and non-real time) from Wasmotes, Raspberry Pi saves all sensed data into a SQLite database. Hence when the drone comes to its home location, Raspberry Pi sends those saved data from SQLite database to the cloud server over HTTPS protocol. The prototype setup with equipment is illustrated in Figure 7.

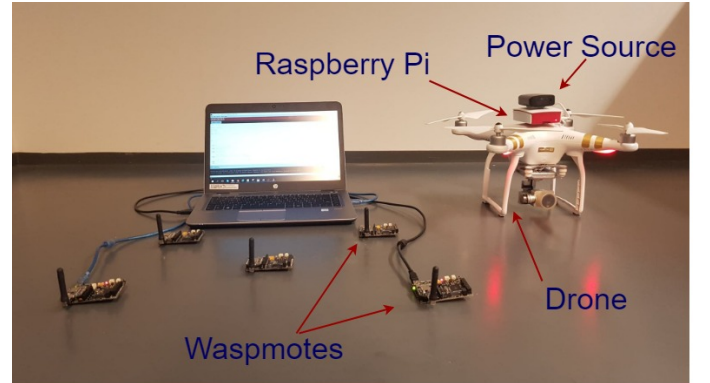


Fig. 7: Prototype Implementation

A. Cloud Integration

The last part of the implementation was to deploy the cloud storage server. As the drone arrives at the docking station after extracting the data from sensors, Raspberry Pi 3 coupled with the drone connects to 802.11 WLAN router with internet access; to upload the locally saved sensor data. The cloud server is implemented on Google Firebase¹ where Raspberry Pi first authenticates itself using its private key. After authentication, Raspberry Pi starts uploading the sensed data to cloud and stores in the database. The Firebase Real-time Database is a cloud-hosted database. Data is stored as JSON and synchronized in real-time to every connected client.

¹<https://firebase.google.com/>

Moreover, Firebase uses HTTPS connection over Transport Layer Security for secure communications between Raspberry Pi and cloud server along with real-time database security. The database provides a flexible, expression-based rules language, to define how your data should be structured and when data can be read from or written to the database. It is capable of defining who has access to what data, and how they can access it. After successful transferring of the data, Raspberry Pi deletes the stored data from the local database.

B. Performance Results

We used handler 0x0038 from BLE user services profile of Waspnote to send the accelerometer sensor data to the Raspberry Pi. Handler 0x0038 is capable of creating a reliable BLE communication between Raspberry Pi and Waspnote, because it caters the master with read/write and indication operations. Maximum data size that can be transferred during a particular transmission attempt is 20 bytes. Waspnote sends those accelerometer sensor data in an encoded format which has to be decoded at Raspberry Pi to make it readable. After the decoding process, it extracts to 112 Bytes at Raspberry Pi. Hence, we consider this 112 Bytes as maximum data that can be send within one particular transmission. To obtain the performance results, we fixed the drone's flying altitude as 10 m above the ground level.

For the data download scenario (i. e. the transmission from Raspberry Pi to Waspnote) we used handler 0x0029. Here we considered 10 seconds time duration to send the data packets over BLE from Raspberry Pi to Waspnote. The following Table II summarizes the results obtained from the experiment.

According to the results depicted in Table II, Raspberry Pi to Waspnote data download rate is higher than Waspnote to Raspberry Pi data upload rate. With the buffer size limitation in Waspnote, Raspberry Pi is only allowed to send a maximum of 74 data packets (each 20 Bytes) to Waspnote. This maximum data transmission causes to fill the buffer size at Waspnote and then stops retrieving data from Raspberry Pi.

TABLE II: Experimental Data Rates

Data Rate Parameter	Value
Data transfer rate from Waspnote to Raspberry Pi R_{UL}	672 Bytes/min
Data transfer rate from Raspberry Pi to Waspnote R_{DL}	148 Bytes/s

V. CONCLUSIONS

The widespread of low-power IoT technologies and their sensing and monitoring applications may demand processing power at the edge of the network, rather than accessing the remote central cloud. Throughout this paper, we have addressed how to provide edge processing power in a similar manner as in edge computing architecture, for the low-power BLE sensors with the help of UAVs such as drones. We have described the protocol in detail along with the simulation and prototyping results. The key findings of the simulations are as follows: the number of served sensor nodes by the drone is

directly proportional to the speed of the drone; The distance between two sensor nodes is the most dominant parameter that defines the overall performance of the system; Circular and square array type sensor node topologies always outperform the linear array topology. The prototyping caused some problems due to the hardware limitations of the Waspnotes.

We intend to extend the research by implementing a fully working prototype and measuring energy consumption in an actual WSN where the sensors are deployed in a higher density. The current experimental results are taken in an ideal situation assuming a constant drone speed by taking the wind speed as zero. In the future, we plan to investigate how the drone speed and the wind speed will impact on the proposed system model.

ACKNOWLEDGEMENT

This work is supported by Business Finland in Towards Digital Paradise, Academy of Finland in SECUREConnect, 6Genesis Flagship (grant no. 318927), 5GEAR projects, and European Union in RESPONSE 5G (Grant No: 789658) project. A. Gurtov was supported by CENIT project 17.01. The authors would also like to acknowledge the contribution of the COST Action CA15127 (RECODIS) and CA16226 (SHELD-ON) projects.

REFERENCES

- [1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.
- [2] O. Bello and S. Zeadally, "Intelligent Device-to-Device Communication in the Internet of Things," *IEEE Systems Journal*, vol. 10, no. 3, pp. 1172–1182, 2016.
- [3] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and Challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.
- [4] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on Multi-Access Edge Computing for Internet of Things Realization," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2961–2991, 2018.
- [5] N. Xia, H.-H. Chen, and C.-S. Yang, "Radio Resource Management in Machine-to-Machine Communications A Survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 791–828, 2018.
- [6] P. Porambage, A. Manzoor, M. Liyanage, A. Gurtov, and M. Ylianttila, "Managing mobile relays for secure e2e connectivity of low-power iot devices," in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2019, pp. 1–7.
- [7] A. Manzoor, P. Porambage, M. Liyanage, M. Ylianttila, and A. Gurtov, "Mobile Relay Architecture for Low-Power IoT Devices," in *IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, 2018, pp. 14–16.
- [8] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless Communications with Unmanned Aerial Vehicles: Opportunities and challenges," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 36–42, 2016.
- [9] P. P. Ray, "An Introduction to Dew Computing: Definition, Concept and Implications," *IEEE Access*, vol. 6, pp. 723–737, 2018.
- [10] "DJI Specs." [Online]. Available: <https://www.dji.com/phantom-3-se/info?lang=cn#specs>
- [11] "Libelium." [Online]. Available: <http://www.libelium.com/development/waspnote>
- [12] "Practical BLE Throughput." [Online]. Available: <https://rigado.zendesk.com/hc/en-us/articles/226824267-Practical-BLE-Throughput>
- [13] "Raspberry Pi Power." [Online]. Available: <https://www.raspberrypi.org/documentation/hardware/raspberrypi/power/README.md>