Abstract: This paper introduces both a hardware and a software system designed to allow low-cost electronic monitoring of social insects using RFID tags. Data formats for individual insect identification and their associated experiment are proposed to facilitate data sharing from experiments conducted with this system. The antenna’s configuration and their duty cycle ensure a high degree of detection rates. Other advantages and limitations of this system are discussed in detail in the paper.

Keywords: RFID, social insects, Apis, Melipona, insect behaviour

1. Introduction

Pollinators play an important role in our ecosystem. Amongst them, social insects are particularly interesting not only because of their diversity of caste structure or because they forage around their nests, but also as they respond to environmental changes. In some cases, such as bees, can also be domesticated.

European honey bees (Apis mellifera) play a vital role in maintaining the world’s agricultural production [1]. A large proportion of the food we eat relies on pollination, with honey bees providing the majority of these pollination services [2,3]. However, bee populations around the world are in decline [4,5]. Potential reasons for this decline include pesticides, pathogens, parasites, diet, and changes to their natural habitat, or a combination of these.

A number of other factors are also thought to be having an impact upon honey bee populations. These include agricultural intensification, seed pesticide treatments [6–9], electromagnetic radiation [10], changes occurring in foraging conditions resulting from losses of biodiversity, and increases in the frequency of extreme climatic events attributed to global climate change [11].

Over the past decade beekeepers in the US, Europe, and Japan have reported even steeper declines in honey bee numbers than had previously been experienced, finding many of their hives without adult bees but still containing abandoned food supplies and brood populations [12]. In the absence of any identifiable cause this phenomenon is known as Colony Collapse Disorder [13].

A better understanding of bee behaviour will give farmers, fruit growers, seed producers, and apiarists improved pollinator management knowledge, enabling them to increase the benefit they receive from pollination services provided by these insects and minimizing the impact on hive health.

Since the pioneering research by Nobel-prize winner Karl von Frisch [14] on the exceptional dance-based communication capabilities of the European honey bee, this insect has been the primary species used in the study of social insect behaviour. Much work has been done on studying and modelling bee behaviour and this has revealed sophisticated cognitive, sensory and navigational
capabilities, given the relatively small size of their brains [15–21]. Other efforts to monitor bees include the use of harmonic radar [16,22–24].

Concerns about colony collapse disorder and other threats to European honey bee populations in recent years have also led to the development of a number of colony dynamics models, in an effort to determine the causes underlying these population declines [25–27].

Marking social insects is an effective way to identify some individuals in the colony and monitor their behaviour as they return to their nest after foraging activities. Social insect behaviour is known to be driven by resource needs of the colony, defense, and reproduction, and is highly influenced by weather conditions. Common ways to mark individuals for identification include the use of ink (where colour and patterns are limited), wing trimming, or micro-dots. The entomologist will record when the marked insects arrive at and leave the nest, and later correlate their observations with other parameters. More recently, image-processing based systems have been used in making this a less labour-intensive process. Limitations in physical marking persist, like the finite variations of patterns and colours that can be used, affecting the number of insects that can be uniquely marked.

More recently, electronic tagging based on RFID (radio frequency identification) technology has been used for social insects (e.g., [6,28,29]). RFID tags have proven to be valuable as they can be small enough to be glued onto insects, and unique encoding in each tag can support identification of thousands of animals in a single experiment. While RFID tags have unique identifiers from the factory, this could restrict capturing experimental details in each deployment. For this reason a specific data format has been developed and adopted (see Section 2.3.2 for details). Some disadvantages of RFID tags include:

- Cost of the tags and the supporting electronics;
- Power usage requirements, which in some cases limits the application in remote areas;
- Extra weight of the tags may disturb bees, limiting their capacity to carry pollen, nectar, and water. This might also change their behaviour;
- Disturbance to the hive, including to bees without tags. As a consequence of the short communication range of the RFID tags, bees must be forced to approach electronic antennas through restrictive channels installed at the hive entrance. This certainly disturbs the hive behaviour on warmer days.

While the RFID tags may disturb bees carrying them, the technology will continue to be useful for analyzing the effects of bees’ exposure to specific stressors (such as exposure to chemicals).
2. System Architecture

We have developed both a hardware and a software system that allows the electronic detection of bees in their natural environment, or in the lab, producing useful data about their behaviour. The architecture of the system is described in terms of its hardware components, embedded software, proposed data formats and data storage schema, and an overarching quality assurance and quality control framework. The following sections provide detail on all components of the system architecture, their importance and how they work together.

2.1. Hardware

The hardware components are the electronic tags, reader units, antennas, printed circuit board, and housing.

2.1.1. Electronic Tags

The RFID tags used in these experiments are 2.5 mm × 2.5 mm × 0.4 mm in size, weigh 5.4 g and are manufactured by Hitachi Chemicals [30]. The operating temperature of these tags is between −20°C and 70°C, and the storage temperature is between −30°C and 75°C. Both of these temperature ranges are valid between 10% and 80% relative humidity. We operated these tags under higher humidity conditions in the Amazon without noticeable degradation of performance. The tags respond optimally at frequencies between 860 MHz and 920 MHz.

The tags have three memory addresses: a 96-bit tag identifier (TID), a 128-bit Electronic Product Code (EPC), and a 64-bit password. Each tag is registered with a unique hexadecimal identifier written into the tag’s EPC. Metadata about the bees is encoded into the EPC, capturing information about the location where the bee was tagged, what kind of platform the bee was tagged at, and species and type information about the bee. The metadata is described in more detail in Section 2.3.2.

2.1.2. Printed Circuit Board

The printed circuit board (PCB) integrates the following components into a single platform: HP-SiP module1 (RFID reader), IoT module (Intel® Edison), GNSS receiver (Global Navigation Satellite System), micro-SD card, micro-USB I/O, and power regulator. Figure 2 shows the PCB and its major components.

The HP-SiP module supports up to 4 antennas that are multiplexed through dwell settings (see Section 3.3.2 for further details), with power levels up to 31.5 dBm, and is capable of reading hundreds of tags per second. The reader’s command set provides many commands for controlling the ISO 18000-6C2 compatible HP-SiP module. The operator can configure the module for various operations such as:

- **Inventory**: Allows the module to gather the EPC data for any tags of interest.
- **Read**: A lower-level operation that allows any specified memory bank on tags of interest to be read.
- **Write**: An operation that allows the module to write a single 16-bit word to a specified memory bank on tags of interest.
- **Kill**: An operation that allows the module to render tags of interest inoperable.
- **Lock**: Allows the permissions for the memory banks on tags of interest to be read or adjusted.

The permissions are for each memory bank and include read only access, password protection, ability to adjust the settings after they have been set, and the visibility of the passwords.

---

1 Hi-Power System in Package
2 https://www.iso.org/standard/46149.html
Intel® Edison is a small computer system previously manufactured by Intel for Internet of Things (IoT) development. This computer system is powered by a 500 MHz Intel® Atom dual-core processor, 1 GiB DDR3 RAM, 4 GiB eMMC Flash memory, and it runs Poky³ Linux as its operating system. It supports Python, C/C++, NodeJS, Java, and other programming languages. For network connectivity support, the Intel® Edison is bundled with Bluetooth 4.0 and Wi-Fi.

The compact GNSS receiver unit from u-blox (Max 7Q module) integrates GPS, GLONASS, GZSS and SBAS ⁴. The GNSS function provides location of the platform, updates local time, and confirms the HP-SiP module is operating within the ISM (industrial-scientific-medical) band, which does not require a licence, for the region where it is installed. According to the International Telecommunication Union [31], the decision on frequencies used for the ISM band is a national matter. The HP-SiP module has to be set up for each allowed frequency in the country in which it operates, and the GNSS can help to confirm the unit is operating in the allowed band. This prevents the risk of a kit configured for one country being operated using prohibited RF bands in another country.

The micro-USB I/O provides access to the IoT module. It is an efficient gateway to communicate via wired serial connection with a field laptop. It also provides safe access to stored data in case the wireless communication fails. The micro-SD card can be used to store large amounts of data and effectively work as a backup. If other communication gateways fail (Bluetooth, Wi-Fi or via micro-USB) physical access to the card will ensure data from the experiments can be recovered.

The power regulator enables the system to work from a variety of DC power sources ranging from 6 V up to 60 V without any additional configuration.

---

³ [http://git.yoctoproject.org/cgit/cgit.cgi/poky/about/](http://git.yoctoproject.org/cgit/cgit.cgi/poky/about/)

⁴ GPS, GLONASS, GZSS and SBAS are different global network satellite systems
2.1.3. RFID antennas

The antennas, as seen in Figure 3, are RFIT 2DBI-1: 2 dBi ceramic patch antennas with TNC male connectors. The ceramic patch is 40 mm × 40 mm × 5 mm, centered on a 50 mm × 50 mm × 1 mm ground plane. These antennas have been used with 50 cm, 75 cm, and 100 cm cables. The system can also work with other antennas such as the Taoglas 49.5 mm × 49.5 mm × 7.5 mm ISPC.86A 868 MHz Ceramic Patch Antenna, 92 mm RG-178 which has been used in Europe.

2.1.4. Housing

The two-part housing for the PCB is manufactured from aluminum. It includes a built-in heat sink as part of the enclosure to provide cooling for the PCB and electronics. It also provides a number of external connectors including:

- Four TNC antenna connectors
- An SMA antenna connector for GNSS
- An SMA antenna connector for Wi-Fi
- A Micro-USB Type B connector
- A 4-pin power connector

![Figure 3. Aluminum housing (18.5 cm × 10.5 cm × 5.5 cm) and peripherals. 1) 4-pin power inlet; 2) micro-USB port; 3) Wi-Fi antenna, and 5) RFID antennas and ports.](image)

2.1.5. Power Requirements

The system can operate with a solar panel of 120 W, with a 12 V 33 Ah battery. A 12 V regulator and a 12 V to 5 V converter are used for powering other lower-voltage instruments.

The specification provided by the manufacturer (MTI) of the HP-SiP module indicates a peak power draw of 15 W - 20 W when the RFID is running at maximum power (transmitting at 2 W RF). We have observed (0.2 A - 0.9 A at 12 V when the inventory cycle is running) a need for no more than

---

10.8 W, amounting to an absolute maximum of 10.8 W × 24 h = 259.2 Wh per day. This energy can be provided by commercially available solar panels, which allows the system to operate in remote areas.

2.2. Software

In this section we describe three major components of the software system: the embedded software, communication gateways and watchdog system.

2.2.1. Embedded Software

This component is the software that controls and communicates with:

- HP-SiP module:
  - issuing commands (e.g., initialization of the module including the region specification, duty cycle (described in greater detail in Section 3.3.3))
  - antenna configuration and receiving responses (e.g., detections of RFID tags, data on temperature of the module, signal strength indicators of each antenna).
- GNSS unit: initializes the unit, reads responses and makes use of the data as needed. Experiments with movable feeders or hives could also be supported with this component.
- Memory storage devices:
  - writing data into memory and retrieving when required, such as by the QA/QC framework
  - Data management including compression and transmission.
- Power regulator: checking battery levels.
- Other hardware components: verifying the operational status of the hardware including communication gateways and registered its status in log files and provides input to the QA/QC framework.

The embedded software, written in Python 2.7, utilizes multiprocessing as the Edison® IoT module has a dual-core processor. The embedded software generates daily log files containing detailed information about the operation of each unit of the hardware and other relevant information. This software can be further customized to accommodate specific user needs.

2.2.2. Communication Channels

The availability of Wi-Fi allows the system to be accessible remotely via SSH (secure shell) or SCP (secure copy) and the data to be retrieved as needed by users. For example, a user might want to receive experimental data every day via e-mail or if a specific bee is detected. During field inspections the user can access data via Bluetooth and this communication channel can also support visualization tools such as augmented reality (e.g., [32] and [33]). To operate communication channels the user can use the embedded software, Linux commands or external devices.

2.2.3. Watchdog

To ensure the continued operation of the embedded software, a system watchdog is enabled. The watchdog listens for a notification from the embedded software arriving within a specified interval. If the notification is not received within the interval, the watchdog restarts the system service for the embedded software. The watchdog provides assurance that, should the embedded software fail, it will be restarted promptly. This re-initializes the hardware as part of the start-up process for the embedded software and recommences regular operation. The watchdog is configured for a 30 s interval.

2.3. Data Format

Tagged bees passing by antennas at hives or feeders are registered by the reading platform. Consider a bee detected leaving its hive, and a few minutes later arriving at a feeder; there are separate registered events for the detection of this bee at each location. A file is created daily for each platform,
containing the time each bee visits that platform. The following sections describe the data formats used for the reading platforms and for the RFID tags, as well as the strategy for the data storage and the database schema. This section describes the data format for both reading platforms and RFID tags.

2.3.1. Data Format for Reading Platforms

Each platform creates a **CSV** (comma-separated values) file every day, containing the times at which each bee was detected. The name of the file has the following format: `YYYYMMDD_CCSSSTTNNN.csv`, as described in Table 1.

<table>
<thead>
<tr>
<th>Field</th>
<th># Characters</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>YYYY</td>
<td>4</td>
<td>Year</td>
</tr>
<tr>
<td>MM</td>
<td>2</td>
<td>Month</td>
</tr>
<tr>
<td>DD</td>
<td>2</td>
<td>Day</td>
</tr>
<tr>
<td>CC</td>
<td>2</td>
<td>Country</td>
</tr>
<tr>
<td>SSS</td>
<td>3</td>
<td>Site</td>
</tr>
<tr>
<td>TT</td>
<td>2</td>
<td>Platform Type</td>
</tr>
<tr>
<td>NNN</td>
<td>3</td>
<td>Platform Number</td>
</tr>
</tbody>
</table>

Some examples of file names are given in Table 2:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Date</th>
<th>Country</th>
<th>Site</th>
<th>Platform Type</th>
<th>Platform Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>20171022_0A00101001.csv</td>
<td>22th October 2017</td>
<td>Argentina</td>
<td>Tucumán</td>
<td>Hive</td>
<td>1st Hive</td>
</tr>
<tr>
<td>20170317_0D00B02001.csv</td>
<td>17th March 2017</td>
<td>Australia</td>
<td>Sandy Bay</td>
<td>Feeder</td>
<td>1st Feeder</td>
</tr>
<tr>
<td>20150519_1D00201006.csv</td>
<td>19th May 2015</td>
<td>Brazil</td>
<td>EMBRAPA</td>
<td>Hive</td>
<td>6th Hive</td>
</tr>
</tbody>
</table>

2.3.2. Data Format for RFID tags

Each RFID tag has a unique code that, when detected at a given time, is recorded in a file named as described in section 2.3.1. Each RFID tag is programmed, prior to being fitted on a bee, with a unique 24-digit hexadecimal code in the format `CCSSSTTNNNXXXYYZ****BBBB` as described in Table 3. There is one exception; a special-case testing tag that uses the code `FFFFFFFFFFFFFFFFFFFFFFF`. This tag is used manually to verify that the system is operational and to create a persistent registry of user visits to the units. Details are provided in Section 3.2.

<table>
<thead>
<tr>
<th>Field</th>
<th>Digits</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC</td>
<td>2</td>
<td>Country</td>
</tr>
<tr>
<td>SSS</td>
<td>3</td>
<td>Site</td>
</tr>
<tr>
<td>TT</td>
<td>2</td>
<td>Platform Type</td>
</tr>
<tr>
<td>NNN</td>
<td>3</td>
<td>Platform Number</td>
</tr>
<tr>
<td>XXX</td>
<td>3</td>
<td>Bee Species</td>
</tr>
<tr>
<td>YY</td>
<td>2</td>
<td>Bee Strain</td>
</tr>
<tr>
<td>Z</td>
<td>1</td>
<td>Bee Type</td>
</tr>
<tr>
<td>****</td>
<td>4</td>
<td>Reserved</td>
</tr>
<tr>
<td>BBBB</td>
<td>4</td>
<td>Bee Number</td>
</tr>
</tbody>
</table>

Some examples of RFID tag codes are given in Table 4:
Table 4. The table shows two examples of identification codes and their interpretation.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example 1</th>
<th>Example 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID Tag Code</td>
<td>0D0110200100103300000005</td>
<td>1D002100600202300000019</td>
</tr>
<tr>
<td>Country</td>
<td>00 Australia</td>
<td>1D Brazil</td>
</tr>
<tr>
<td>Site</td>
<td>011 Sandy Bay</td>
<td>002 EMBRAPA</td>
</tr>
<tr>
<td>Platform Type</td>
<td>02 Feeder</td>
<td>01 Hive</td>
</tr>
<tr>
<td>Platform Number</td>
<td>001</td>
<td>006</td>
</tr>
<tr>
<td>Bee Species</td>
<td>001 <em>Apis mellifera</em></td>
<td>002 <em>Melipona fasciculata</em></td>
</tr>
<tr>
<td>Bee Strains</td>
<td>03 Golden Italian</td>
<td>02 No Strain</td>
</tr>
<tr>
<td>Bee Type</td>
<td>3 worker</td>
<td>3 worker</td>
</tr>
<tr>
<td>Reserved Digits</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>Bee Number</td>
<td>0005</td>
<td>0019</td>
</tr>
</tbody>
</table>

2.4. Data storage

Reader recordings are stored one per line. Each line registers the detection time in UTC (coordinated universal time) in seconds (or at higher resolution if required), the bee visiting that platform (as described in Section 2.3.2), and the detecting antenna. Table 5 presents a sample of CSV file content.

Table 5. The first three lines of sample content in the first file show the detection of three different bees (#1130, #5, #3) on the 17th of March 2017 at 1:41:07 (UTC). The second file shows two different bees (#15, #19) detected on the 19th of May 2015 between 9:04:17 (UTC) and 9:33:01am (UTC).

<table>
<thead>
<tr>
<th>Time in UTC</th>
<th>Bee Tag Data</th>
<th>Antenna ID*</th>
</tr>
</thead>
<tbody>
<tr>
<td>20170317T014107Z</td>
<td>0D0080100100103300001130</td>
<td>2</td>
</tr>
<tr>
<td>20170317T014107Z</td>
<td>0D0110200100103300000005</td>
<td>4</td>
</tr>
<tr>
<td>20170317T014107Z</td>
<td>0D0110200100103300000003</td>
<td>4</td>
</tr>
<tr>
<td>20170317T014108Z</td>
<td>0D008010010010330000130</td>
<td>2</td>
</tr>
<tr>
<td>20170317T014108Z</td>
<td>0D0080100100103300000003</td>
<td>4</td>
</tr>
</tbody>
</table>

File: 20170317_0D00802001.csv

<table>
<thead>
<tr>
<th>Time in UTC</th>
<th>Bee Tag Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>20150519T090417Z</td>
<td>1D0020100600202300000019</td>
</tr>
<tr>
<td>20150519T090455Z</td>
<td>1D0020100100202300000015</td>
</tr>
<tr>
<td>20150519T090457Z</td>
<td>1D0020100100202300000015</td>
</tr>
<tr>
<td>20150519T092035Z</td>
<td>1D0020100600202300000019</td>
</tr>
<tr>
<td>20150519T093301Z</td>
<td>1D0020100100202300000015</td>
</tr>
</tbody>
</table>

Details on antenna configuration are given in Sections 3.3.2 and 3.3.3, and Figure 5. The “Antenna ID” field is optional.

This experiment involving stingless bees in Brazil used a single antenna in the entrance housing, because direction of movement of bee activity was not required.

These data, providing information on the activity of bees leaving and returning to the hives, and visiting an artificial feeder, were processed in time-order and analyzed to reconstruct foraging behaviour [29].

The system offers internal storage for the files and logs that are produced. The micro-SD card provides extended external storage that can be used in place of the internal storage. A timed script runs daily to compress the data files and the log files that are more than two days old. This reduces the likelihood of the system running out of storage space, although it has occurred when the user has not
cleared the memory. For that reason memory status has been included in the QA/QC framework (see section 2.5).

An alternative approach to reduction of storage requirements is the use of a SQLite version 3 database, implemented within the embedded software, to consolidate and filter tag data before writing to the SD Card. After tag records are written to the SQLite database, a consolidated and filtered version of the data is written to the SD card.

The combination of two internal locations to store files, an SD Card, and access to external data-stores through online services (when Wi-Fi is available to the system) offers flexibility in data storage. The current status of memory resources is reported through the QA/QC process as described at Section 2.5.

The data can be accessed via Wi-Fi, Bluetooth, and direct cable connection. When the system is connected to Wi-Fi with a known IP address, the data can be recovered using a secure protocol such as Secured Copy (SCP). This technique has been used successfully, with an automated script running on a daily schedule fetching any new files found on the system. A SCP client on a laptop, and a cable connection to the system, also allows the data to be recovered directly by an operator. The system also offers a smaller storage area that is exposed as a USB drive when a cable is connected to the system. This can be used as an alternative way to recover the data using a cable connection.

The database schema has been designed with components, samples, and annotations as the central elements. Examples of components are weather stations, hive scales, in-hive sensors such as humidity and temperature sensors, and our system. Data recorded by a component is, for the database schema, a sample. Annotations are notes made by users that are associated to the experiment, the components, or the samples. Examples of annotations are the consumption of fluids in a feeder, the presence of other insects around the hives, weather events, calibration of sensors and simple comments on the data.

This schema provides a flexible and extensible design that allows additional features to be added while facilitating complex searches on the data. It has also been used in the design of a collaborative framework for immersive analytics [33]. This schema allows for assets, experiments, and data to be recorded, annotated, and searched.

A PostgreSQL 9.4 implementation of the schema is used to store the experimental data. The live implementation includes tables to capture any changes, and their source (who/what), made to the core tables in the schema via SQL Triggers. This allows users to review changes and roll back to previous versions where required or desirable. The ability to roll back is particularly applicable to annotations and observation descriptions.

A data storage strategy implemented in the system is important because it allows data to be recorded, compressed, transmitted and stored effectively. As a result the device will not lose data or run out of memory, and the data management will be efficient.

2.4.1. Data Curation

Data curation is an important part of the experimental process. Human mistakes in the conduct of experiments can occur. This include, for example, tags designated for one hive being fitted to bees from another hive. Such errors can be noted and corrected during the curation process. It is important to process any data to ensure that the correct values are being stored. The raw data is retrieved from the system and written to a data-store. These files are kept as the ground truth. Once collected, the data follows a three step curation process:

---

6 https://www.postgresql.org/
• **Data Verification** confirming the operator has used the correct tags in the correct hive, checking expected tag times, assessing any potential misreadings, verifying if any bee with a tag is dead near an antenna causing spurious detections.

• **Injection into a Database** scripts write the processed data into a database to facilitate ease of search.

• **Data Archival** data is made available as a collection of verified CSV files via a data repository.

2.5. **Quality Assurance & Quality Control (QA/QC)**

A quality assurance and quality control system runs autonomously to ensure integrity of the experiment and flag potential issues with the system. Its architecture is divided into two major components that assess the quality of engineering data and of the scientific data [34]. As an outcome it reports the working status of the system and if the quality of the experiment could be compromised at the current moment or in a near future.

2.5.1. **Engineering Data**

Engineering data includes information about the working status of some components like:

- **GNSS:** Verifies if the GNSS is operational and ensures there is no clock discrepancy between the microcomputer and the GNSS. Also verifies if the RFID reader is operating within the allowed local ISM-band.
- **RFID reader unit:** The unit has a number of low-level error reports that can be interpreted and addressed at a higher level.
- **Wi-Fi:** Confirms if this gateway is operating as expected.
- **Memory:** Assesses the amount of memory used, that is still available, and when it is likely to become an issue estimated from the reading frequencies.

The key advantages of having QA/QC for engineering data is to assure the user the system is operational and any issues are detected and promptly reported.

2.5.2. **Scientific Data**

The QA/QC of scientific data allows the operator to verify that their experiment is recording data as expected, and produces warnings about anomalous data and behaviour. This component automatically analyzes the data produced by the system, including:

- **Anomalous detection of bees:** An example is a bee that is detected leaving the hive twice without returning. It could occur when the bee finds another entry to the hive (which should be immediately fixed) or if the RFID readers stop working for some time. Another potential cause is a less than ideal duty cycle, which could allow bees to move on the antennas without being detected (see Section 3.4.3).
- **Bee mingling:** bees visiting neighbour hives is an expected behaviour, but ideally this should be highlighted.
- **Detection within antennas:** for the honey bee configuration, two pairs of antennas are recommended (see Figure 5a). The number of detections of tags is highly dependent upon bee behaviour, and hives equipped with the system should present similar results as they are subjected to similar environmental conditions. It is acceptable for bees to be detected more frequently in one antenna pair than in the other, but all hives should show similar results.

The QA/QC framework for engineering or scientific data can be updated and expanded depending on specific needs of users. The main advantage of having a QA/QC framework is that issues can be promptly identified, prioritized based on the consequences and addressed.
3. Operating Methods

This section describes how to operate the system, including how to fit bees with RFID tags, how to set up and test the system, its antenna configuration, and expected issues.

3.1. Tagging Bees

RFID chips are dipped in one-component cyanoacrylate (Cyberbond® 2610) and, while holding the bee lightly with a pair of forceps at the upper abdomen (holding down the wings), the RFID chip is placed between the wings at the top of the thorax. The bee is released after a few seconds (Figure 4). More aggressive bee strains like the Africanized honey bee make it nearly impossible to work around open hives. In that case bees are collected and held manually during the RFID fitting or a number of bees are brought to the laboratory where CO₂ or cooling can be used to decrease bee movement. Depending on the nature of the study, such as checking longevity of bees, it will be ideal to tag bees as they hatch in their first day of life as an adult. This is done using incubators. Forager bees can be tagged directly on feeders, but in that case the bee could be from a wild hive.

![Figure 4. RFID tag being fitted to the thorax of a honey bee. This process can be done in the hive with non-aggressive bees.](image)

3.2. Testing the System

An efficient way to verify if the system is reading RFID tags and processing the data accordingly is to use one RFID with a known identity code different from those used for bees. For this purpose all experiments are using a tag with a hexadecimal sequence of 24 Fs (FFFFFFFFFFFFFFFFFFFFFFFF) in the EPC memory. This tag is mounted on a non-metallic rod which is inserted manually at the hive entry, triggering a messaging task. Alternatives tested are:

- **micro-USB connection**: Using a laptop the operator can confirm the system is working by using the testing tag and verifying if the file was updated. In this case, the Wi-Fi and the Bluetooth connection will not be tested.
- **Bluetooth**: an augmented reality system, MelissAR [32], has been developed for visual analytics of Honey bee behaviour in the field. The implementation was realized on a Sony Xperia Z4 which utilizes Bluetooth to communicate with the system to recover hive data.
- **e-mail**: an electronic message can be sent from the system via Wi-Fi either directly to recipients, as an email, or to a RESTful service, which then generates email messages to subscribers, to confirm the system is operational.
- **SMS**: an electronic message is sent from the system via Wi-Fi to a RESTful service which then generates SMS messages to subscribers.
3.3. System Set up

The system set up will depend on the bee species under study. In this paper we will describe the set up for the honey bee (*Apidae*). Their hive entrances are wider than for other bee species like *Bumbus*, *Xylopcopa*, *Euglossini* or *Melipona*.

3.3.1. Antenna Physical Arrangement

The direction of bee movement (in or out of their nest or feeders) can only be determined by using at least two antennas. The use of only two antennas must be associated with some constraints in bee path to ensure a minimum distance between the antenna and the tag attached to the bee allowing its detection. Using two pairs of antennas has proven to be more efficient as a result of cross antenna excitation. Details of this feature are described in Section 3.3.3.

The patch antenna with coaxial feed was designed with CST Microwave Studio\(^7\). The antenna parameters are optimized to achieve a resonant frequency at 875 MHz. A substrate with high permittivity is selected to reduce the size of the antenna and the substrate thickness is increased to increase the antenna bandwidth. The spacing between the pairs of patch antennas in y-direction was varied to simulate mutual coupling between pairs of patch antennas placed on the antenna housing (Figures 5a and 5b).

The simulated coupling between Port 1 and Port 3 versus distance Dy is shown in Figure 7. The spacing between the antennas increased from 70 mm to 340 mm, or 0.2 \(\lambda_0\) to \(\lambda_0\) calculated at 875 MHz. As expected, the coupling between Port 1 and Port 3 has maximum value close to resonance frequency of the patch antennas and it reduces by increasing distance Dy. The coupling between Port 1 and Port 4 shows similar trend and it is on average by 3 dB lower than the coupling between Ports 1 and 3. The coupling between Port 1 and Port 2 is strong since the corresponding patch antennas are facing each other and it is close to -8.5 dB.

In this experiment, the antennas are spaced by 170 mm in order to reduce the coupling between them. In future, other options for reducing mutual while keeping the spacing between will be considered. For example, the mutual coupling may be reduced below 45 dB for centre to centre spacing of 0.33\(\lambda_0\), by introducing simple resonant slots on the common ground plane between two microstrip antennas [35,36].

3.3.2. Antenna Electronic Configuration

The MTI HP-SiP module supports up to 16 logical antennas mapped to 4 physical transmit/receive ports. The HP-SiP module may retrieve status and configure several parameters on a per-logical-antenna-port basis. This allows for flexible configuration of the antennas through enabled/disabled states, power levels, dwell times, number of inventory cycles, and logical to physical antenna port mapping.

The module allows the antenna power level to be set in 0.1 dBm increments in the range 0 dBm to 33 dBm. This range represents the programmatic specification for the HP-SiP module, however the highest level is not guaranteed and it allows for a ‘calibration factor’ so that a guaranteed and equal level is presented on each port. Allowing for up to 1.5 dBm in cable and connector loss gives the module an effective limit of 31.5 dBm on each antenna port. The experimental configuration uses 27 dBm to help reduce antenna cross-talk and as a result improve the quality of detections. The antennas used are a 2 dBi ceramic patches, meaning the antenna has a RF gain of 2 dBm. When the power has been set to 27 dBm, the ERP (measured at a specific point) is 29 dBm.

---

(a) External view of entrance housing. The structure is 38.5 cm × 12.5 cm × 4 cm.

(b) Internal view of entrance housing. This is mirrored by the opposite layer of the housing to provide matching pairs of antennas. The centers of the highlighted squares (where the antennas are mounted) are 17 cm apart.

Figure 5. Model of a 3D-printed housing for the RFID patch antennas. This particular model has proven to be useful for *Apis mellifera*. Other bee species may require different arrangements.

Figure 6. Four patch antennas placed on the entrance housing. Patch antennas are fed by a coaxial probe. The antenna size is 50 mm x 50 mm X 6.5 mm.

The combination of the configuration for dwell time, which specifies the number of milliseconds that tag protocol operations (as described in Section 2.1.2) may spend before switching to the next enabled antenna port, and inventory cycles, determines the conditions under which the port switch will occur. The dwell time can be set between 0 ms and 65535 ms. Likewise, the number of inventory cycles can be set between 0 and 65,535 cycles. In all combinations of dwell time and number of inventory cycles, the logical antenna will remain active until the maximum number of tags have had the protocol applied, or the operation is explicitly cancelled. If the dwell time is set to 0 ms the logical antenna must be configured with at least 1 inventory cycle. Under this configuration the logical antenna will remain active until one of the general conditions is met or until the specified number of inventory cycles has completed. If the dwell time is not 0 ms but the number of inventory cycles is, then the logical antenna remains active until one of the general conditions is met or the dwell time expires. If both the dwell time is above 0 ms and the number of cycles is 1 or more, any of the previously mentioned conditions will end the logical antenna activity.

3.3.3. Duty Cycle

The experimental configuration uses dwell times of 0.125 s on 8 logical antennas activity times mapped to 4 physical antenna ports. The logical antennas are alternately set with a 27 dBm or 0 dBm power level, i.e. logical antenna (LA) 1: 27 dBm, LA 2: 0 dBm, LA 3: 27 dBm, LA 4: 0 dBm, LA 5: 27 dBm, LA 6: 0 dBm, LA 7: 27 dBm, LA 8: 0 dBm. Logical antennas 9 - 15 are disabled. The resulting signals from this configuration can be seen in Figure 8.
3.4. Known Issues

While RFID is a useful technology to follow bee activity, it has some important issues the user must pay attention to including how to fit RFID tags onto bees, the consequences of dead bees with tags at the entry, reading-frequency setup and details on data interpretation. This section discusses these issues in some detail.

3.4.1. Fitting RFID on Bees

During the placement of the RFID tag on a bee it is possible that a misplacement of the tag will prevent the bee from being able to fly (e.g., RFID tag touching one of the wings), a tag could impair the bee’s navigation (if it is covering their eyes) or adding the tag could hurt the bee when pressing on its thorax. Some bee species (e.g., *Melipona seminigra*) are very sensitive to the glue’s smell. Once the bee receives the RFID tag it will immediately be attacked by its own nest. In this case, it is only possible to work with these bees by placing them overnight in a separate box and releasing them the next morning. There are different strategies to be used while attaching the RFID tags to the bees. These are a result of lessons learned from entomologists and beekeepers using this and previous generations of this system, and include:

- **Bees tagged at the hive**: distress to the entire hive, no guarantee the bee will survive many days, and there is no knowledge of the role of that bee in the colony.
- **Bees tagged at the feeder**: Bees from non-instrumented hives from the neighborhood could visit the feeder. It is very likely the bee will return to the feeder, as long as quality sugar water solution is continuously provided.
- **Bees tagged in the lab**: stress to the individuals.
- **Bees tagged as they hatch**: ideal scenario for most studies. The issue will be the uncertain future of that bee. Young bees usually remain in the hive for about three weeks until they start flying.

3.4.2. Dead bees at the entry

A common behaviour of *Apis mellifera* is to dispose of dead bees near the entry of the hive. As a consequence, dead bees with RFID tags are at times deposited near the reader and detected continuously. Large files will be recorded as a consequence of the presence of a dead bee with a RFID on an antenna.

3.4.3. Reading Frequency

A duty cycle that is not well-designed could lead to bees passing by the antennas undetected. Ideally, the reading frequency should allow multiple detections of a passing bee. This will result in
Figure 8. The structure of a duty cycle of the RFID reader operation. It is only possible to power one antenna at a time and all antennas must be off for a given time as well. The time span during which each pair of antennas (Figure 5) operate can be tailored to how fast the bee species under study moves.

a desired redundancy which ensures the bee presence is recorded and then confirmed by a second detection. However, higher reading frequency will consume more power and memory. It is also possible to implement an adaptive reading frequency that takes into account the weather conditions and likelihood of bee activity (e.g., [37]).

3.4.4. Data Interpretation

While RFIDs provide an accurate way to determine bee movements, individual bees may respond to specific hive needs such as air cooling, cleaning, and defense. These activities are usually conducted at the entry of the hive, which could lead to a large number of readings as the bees stay in the vicinity of an antenna for some time, or move intensively across the hive entry. As a consequence, data interpretation can be difficult and would require the assistance of an entomologist who has observed bees during that period of time or who is familiar with those behaviours. Post-experiment data processing could facilitate cleansing or lead to misinterpretations. While it is tempting to process the data, it is important to confirm the cleansing has produced desired results.

4. Discussion

4.1. Features

The hardware can be installed in hives as well as in feeders. Observing the behaviour of bees in hives could provide insights into whole-of-colony response to specific needs, changes in individual role as the insects mature, foraging force of the hive, drone behaviour, and if the queen is away from the hive (e.g., nuptial flight or swarming).

Monitoring bees in feeders allows the observation of foraging bees, independent of their hives. Bees, visiting feeders usually filled with sugar water solution, can come from any hive nearby and bees from different species could also be present (e.g., *Apis mellifera* and *Apis cerana* in Queensland, or *Apis mellifera* and *Bombus terrestris* in Tasmania, both in Australia). In this case bees will be fitted with...
RFID tags when visiting the feeders and special care should be taken to avoid mixing the tags from one species with the those prepared for another species. Feeders also allow the exposure of bees to chemicals (e.g., pesticides) in controlled doses, and multiple feeders distributed over a region could contain different doses of chemicals, with control feeders containing none. In this case environmental factors will be nearly identical for all bees within the region.

The number of bees to receive RFID tags will depend on the nature of the experiment. For example, to observe the behaviour of a small honey bee hive (with some 15,000 individuals), at least 200 bees should be fitted with RFID tags. Hive replication is always desired, if collective behaviour of the colony is relevant.

Additional hardware such as weather stations and hive scales can be relevant and their installation should be considered. If the user is visiting the site regularly to deploy additional RFIDs on bees or for site maintenance (e.g., grass cutting), it is always good to record observations on bee activity, presence of other insects such as wasps, ants or other bee species, pests such as varroas or hive beetles, movement of drones, and colour of pollen foraging bees are carrying. All this information can be relevant later on when the user is trying to interpret the data on individual or collective behaviour of bees with RFIDs.

4.2. Limitations

Scientists working with RFID-based technologies are making assumptions that must be understood as they are also common to all similar electronic monitoring systems.

4.2.1. Disturbing bees

Bees could be impacted by the process of attaching RFID tags to their thorax. As discussed previously in this paper, these impacts are the smell from the glue affecting the acceptance of the bees in their own hives or their ability to properly forage, the stress on bees receiving the tag, glue spilling on bee’s eyes or wings, effects on bee mobility within the hive, to mention a few. Also, there are studies (e.g., [10], and references therein) suggesting the interference of electromagnetic radiation in bee behaviour.

While studies with electronic tagging of bees are designed to compare bees carrying the same tags exposed to stressors with those not exposed to those particular stressors, it is assumed that the behaviour of bees without tags exposed to and not exposed to those stressors can be translated without further analysis. This assumption will fail if bees carrying electronic tags will suffer differently to the effects of stressors than bees exposed to the same stressors and not carrying tags.

4.2.2. Hive entry modification

The hive entrance and antenna housing (as illustrated in Figure 5a) can impact the behaviour of the bees when they are trying to regulate the internal conditions of the hive such as humidity and temperature. The distance between pairs of antennas should be at least 17 cm which makes the entry relatively long. If the distance is shorter than that there will be interference across pairs of antennas. This long entry can be prohibitive to some experiments in very hot environments. The distance between a pair of antennas may be reduced by optimizing a pair of antennas which share the same substrate and ground plane.

4.2.3. Vulnerability to predators

Bees with RFID tags could be more visible to predators such as other insects and birds. Depending on bird species in the region, ethics application could be needed because of the potentially hazardous ingestion of RFID tags. If bees with RFIDs are more vulnerable this could affect the accuracy of the studies of bee longevity.
5. Conclusions

One of the key challenges in using RFID-based systems for social insect monitoring is the occurrence of misreadings, i.e. when the insects pass by check-points without being detected. This was addressed in our system by a combination of multiple antennas, designed to operate to their maximum performance without undesirable interference; and the application of duty cycles that provides some redundancy in detection of tags. Duty cycles can be also adapted to minimize power consumption.

The system is energy efficient, it can be powered with solar panels. The system has been used in remote areas with frequent cloud coverage such as in the Amazon and in places with long hours at dark such as the winter in Tasmania (42°S).

The data formats adopted for both the system and RFID tags captures most of the high-level metadata required for an efficient data exchange. The data management within the system and with data base schema facilitates data storage.

While the cost of the system is important, it is equally relevant to provide the user with hardware that is easy to operate, to assess the health conditions of the electronics and the quality of the data and provide ways the data can be accessed and curated. While entomologists and beekeepers have deep expertise with hive management and bees, they are still developing their capability with electronics and ICT. Therefore, user experience is important to ensure adoption of the technology.

Acknowledgments:

PdS would like to thank CSIRO for his OCE Science Leader appointment and the Vale Institute of Technology for its financial and technical contribution to this research. We wish to thank Intel for supplying us with the Intel Edison platform and acknowledge technical support from Hitachi Chemical. The authors would like to thank the Tasmanian Beekeeping Association, Fruit Growers Tasmania and past and current members of the Swarm Sensing Team. The authors would like to thank Dr Giorgio Venturieri for providing the image of the *Melipona mellanoventer* with the RFID tag (Figure 1b). The authors would like to thank Assoc. Prof. Geoff Allen and Dr Stephen Quarrell both from Tasmanian Institute of Agriculture and University of Tasmania for their support with field experiments with bees and Simon Hills from IMBROS Pty Ltd. for his assistance with the hardware assembly. SB and PH would like to thank CSIRO’s OCE Program for their top-up PhD scholarship. KB would like to thank Vale Institute of Technology for her Academic Scholarship for her Master studies. Previous versions of this system were used by scientists and beekeepers worldwide as part of the Global Initiative for Honeybee Health. Their feedback and constant encouragement were instrumental to the development of the current version of this system, which is originally reported in this paper.

Author Contributions:

In this manuscript, PdS contributed with the experimental design and work, data analysis, system checking, and manuscript writing. PM contributed with the work, data analysis, system checking, and manuscript writing. KB, SB, NN, TG, PH, GP and AD contributed with the work and data analysis.

Conflicts of Interest:

The authors declare no conflict of interest.

1. Levine, R. Is it Honey Bee or Honeybee? Beg Bug or Bedbug? House Fly or Housefly? *Entomology Today* 2014, —, —. doi:—.


doi:10.1016/j.ecolmodel.2013.06.005.


doi:10.1109/BDVA.2016.7787044.

doi:10.1109/OCEANSSYD.2010.5603582.

