T.A.A.G

Tamper Automated Alert Gadget

Critical Design Review

Group 7

Aiman Salih	EE
Daniel Gibney	CpE
Leaphar Castro	EE

Funding

Dr. Yuan, Co-Director of MIST research center at UCF.

Motivation

With the ever expanding use of IoT sensor systems, the vulnerability of these systems must be evaluated. This project serves as a platform to demonstrate how IoT security can be implemented.

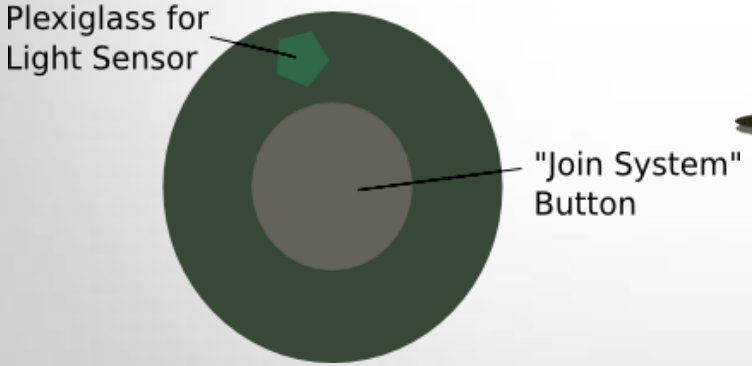
Concept

What is T.A.A.G?

- Senses motion and light
- Wi-Fi messages to mobile app
- Place on door, gun case, etc.

User Interface

Detector



Detectors

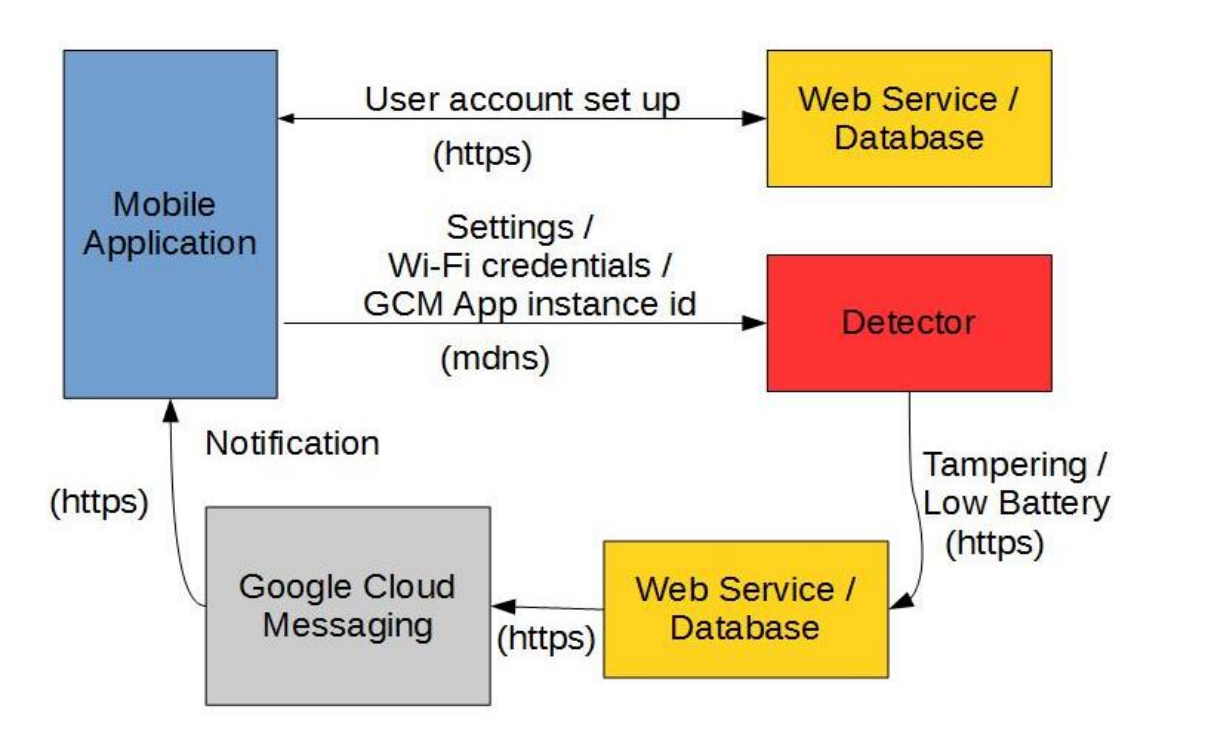
Goals & Objectives

- Secure transmission of data between device and user
- Lightweight & compact
- Easy to use and set up
- Adjustable light and motion thresholds
- Long lasting battery life
- Allows for multiple detectors

Requirement Specifications

Parameter of interest	Specification
Battery life	50 days or more with normal operation
Charging time	1 hour or less
Weight	50 grams or less
Dimensions	55 mm X 45 mm or less
Mobile application	Android mobile app
Notification	Given network connectivity detector sends notification to user when sensor thresholds are crossed -Provides low battery notification before battery is fully depleted
Security	Use of AES (American Encryption Standard) algorithm
Range of light sensing threshold	0 lux – 10,000 lux
Acceleration detection	Be able to detect a magnitude of 0.2g or greater in all directions

System Overview



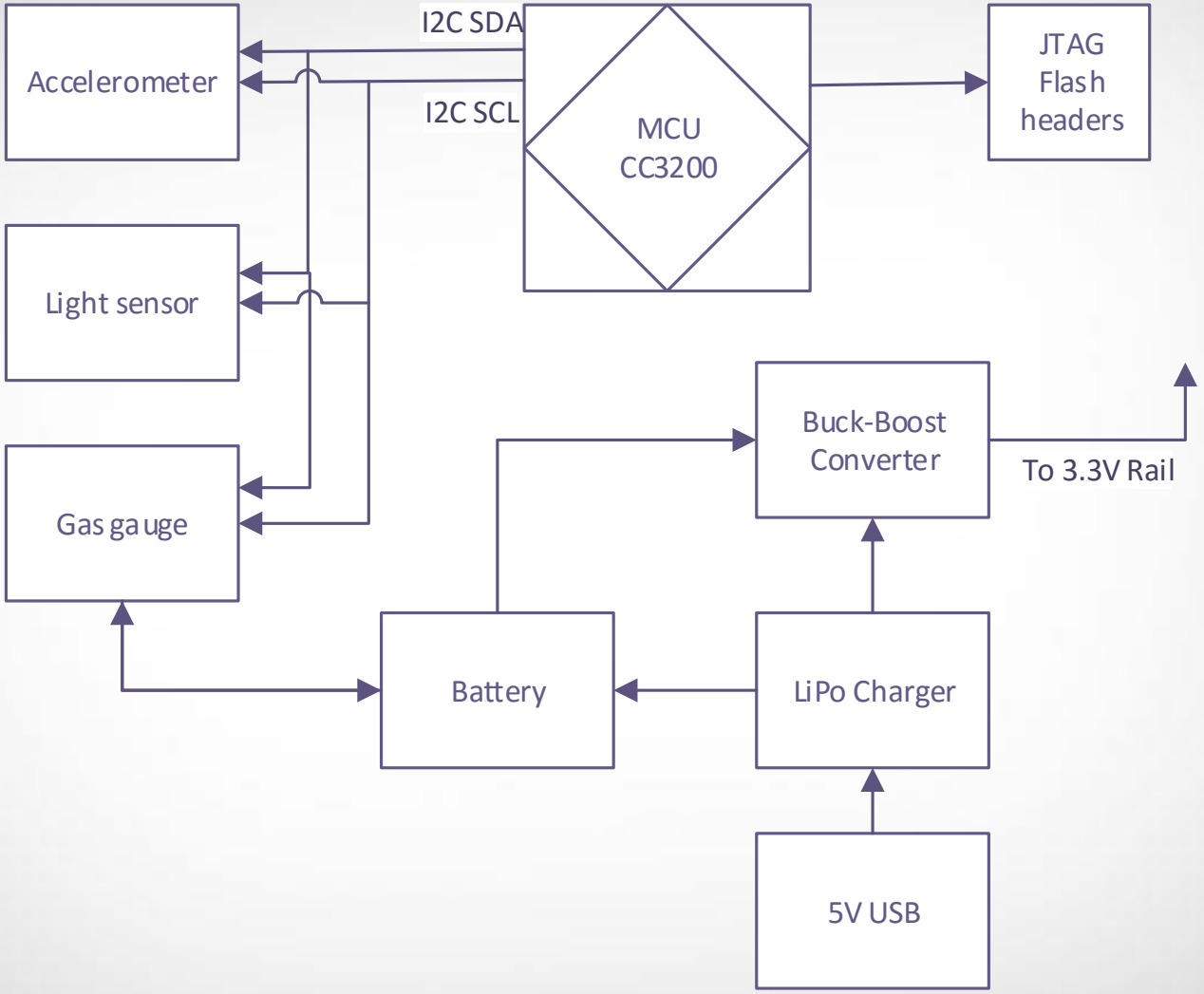
3 major components:

Mobile application, web service, and detector

Work Distribution

- Aiman Salih:
  - Administrative tasks
  - Overall system
  - PCB design
- Daniel Gibney:
  - Overall system
  - Software system
- Leaphar Castro:
  - Power system
  - Hardware system

Detector Hardware System

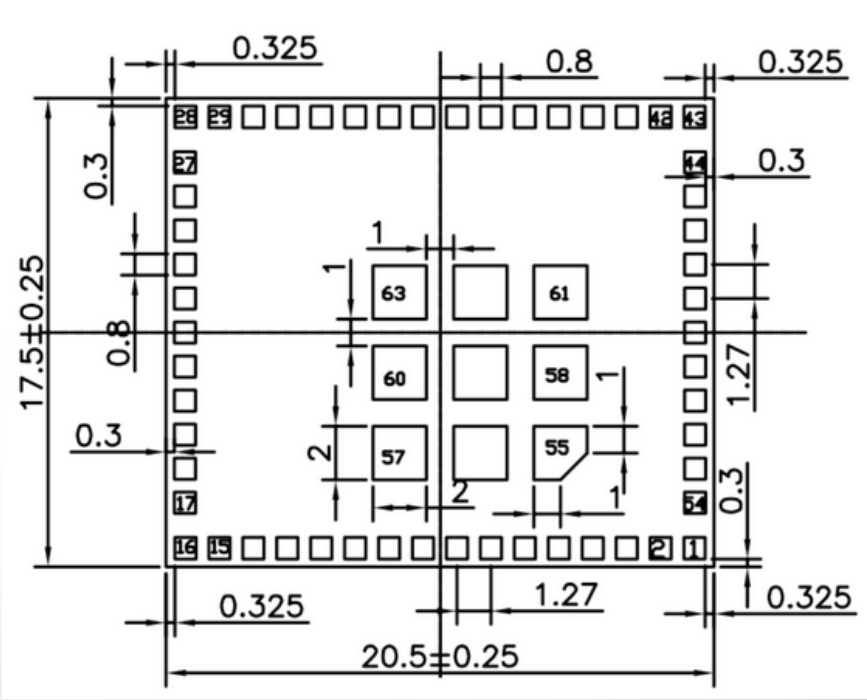


Microcontroller

T.I. SimpleLink Wi-Fi CC3200 Internet-on-a-chip Wireless MCU module:

- Most compact solution
- Crypto engine

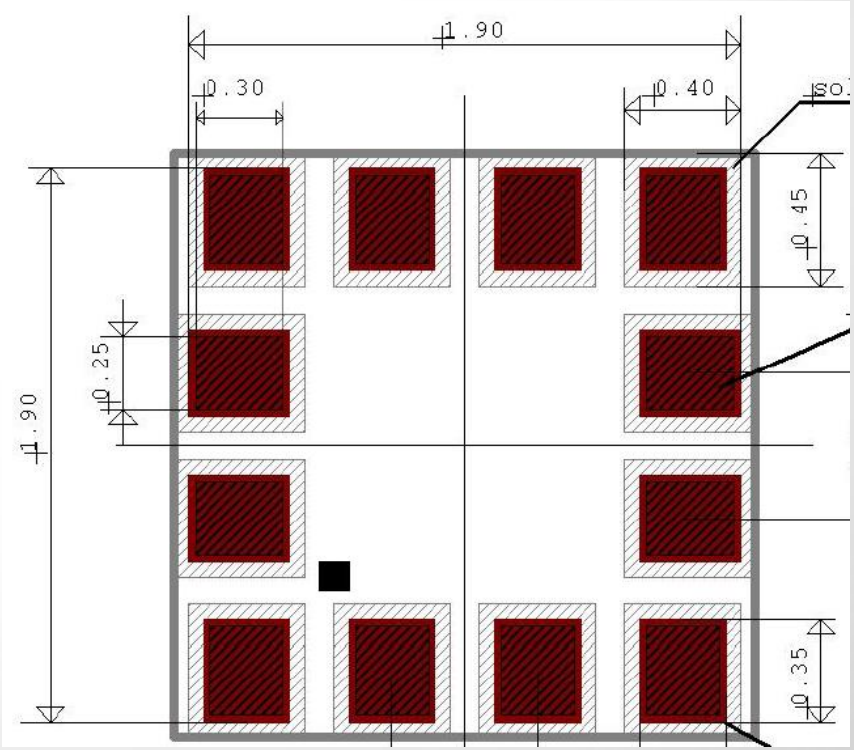
Manufacturer	Texas Instruments
Part model	CC3200mod
Price	$24.99
Purchased from	Mouser
Pins	65 pins
Vin	3.3V
Dimensions	17.5 mm X 20.5 mm



Accelerometer

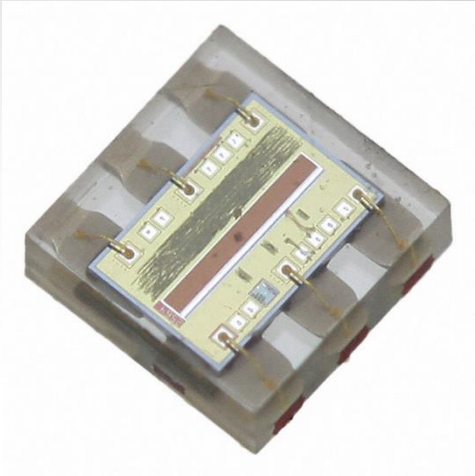
- Has a dedicated interrupt pin
- Uses the 3.3V rail
- Very compact dimensions

Manufacturer	Bosch
Part model	BMA222
Price	$1.99
Purchased from	Mouser
Pins	12-pin LGA
Vin	3V Nom.
Dimensions	1.9 mm X 1.9 mm

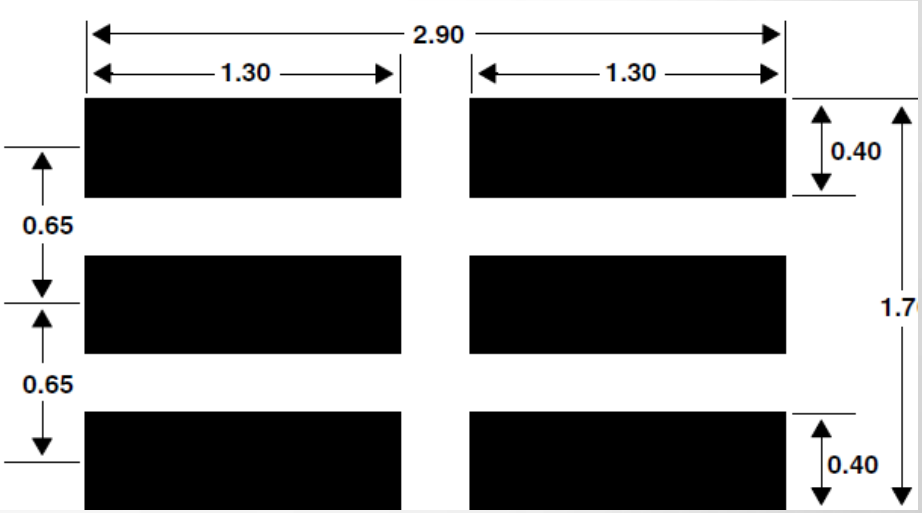


Light Sensor

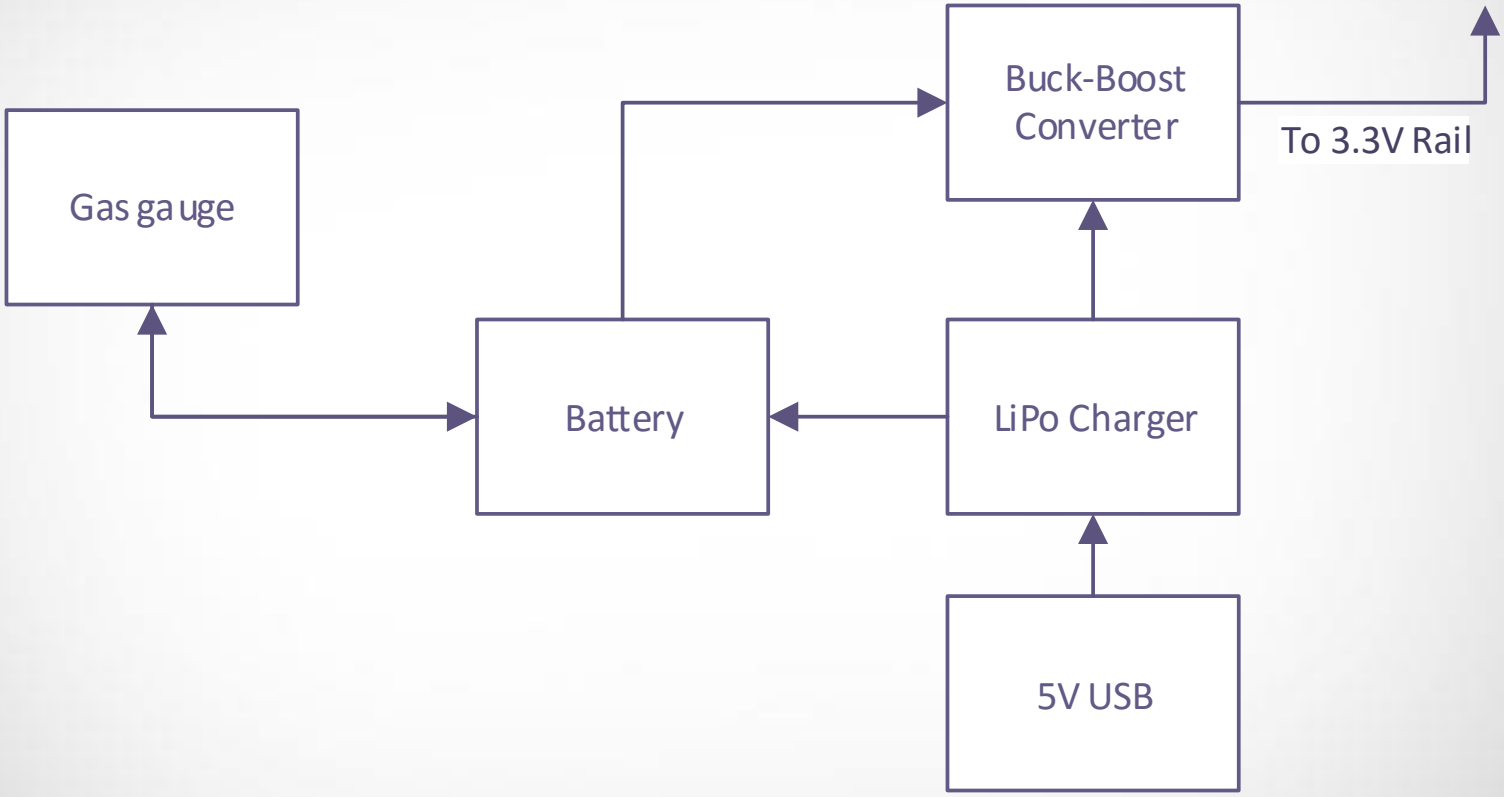
- Light responsivity down to 0.25 lux
- Offers I2C technology
- Operates on 3.3V rail



Manufacturer	TAOS
Part model	TSL561
Price	$1.84
Purchased from	Mouser
Pins	6 pins
Vin	3 V Nom.
Dimensions	2.9 mm X 1.7 mm

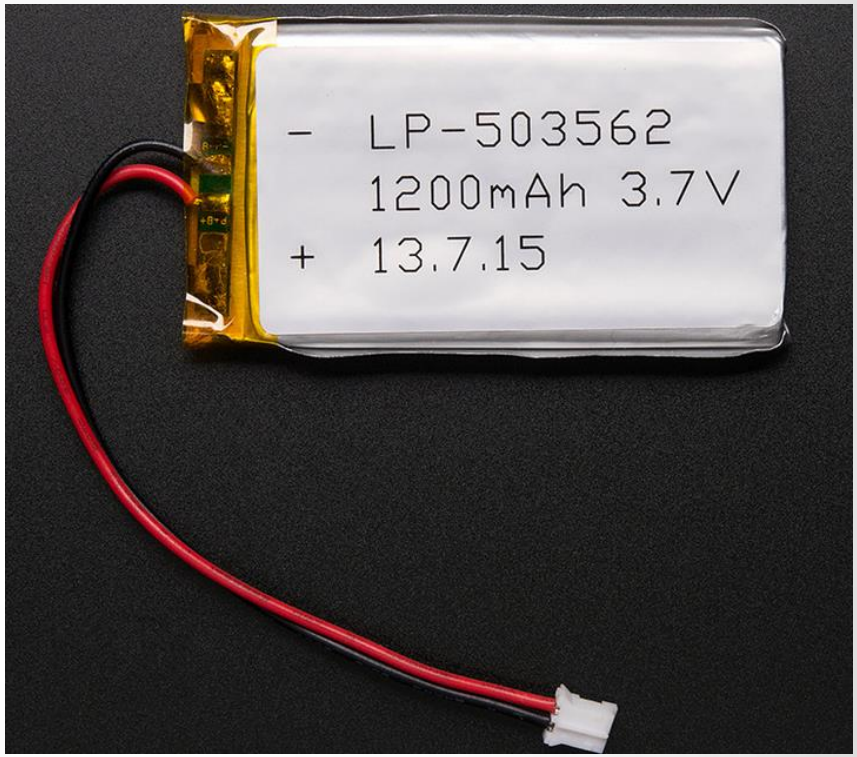


Power Flow


Buck-Boost Converter
To 3.3V Rail
Gas gauge
Battery
LiPo Charger
5V USB

Battery

Manufacturer	Hunan Sounddon New Energy Co.
Part Model:	503562
Price:	$9.95
Purchased From:	Adafruit
Type:	Polymer Lithium-Ion
Connector:	2-pin JST- PH connector
Nominal Voltage:	3.75 V
Nominal Capacity:	1200 mAh / 4.5 Wh
Weight:	23 g
Dimensions:	34mm x 62mm x 5mm



Polymer Lithium-ion Battery

- Low maintenance battery
- Self-discharge rate compared to other available technologies fairly low in most cases less than half
- Little to no harm to the environment when disposed
- No special requirements for prolong battery life
- Energy Density when compared to other technologies is typical twice as good
- Protection circuit built in
- Specialty Cells
- Dimensions
- Lightweight
- Safe to use
- Easy to implement into design and system
- Load characteristics
- Rechargeable
- Potential for even higher densities

Battery Testing

- To assure maximize battery functionality, multiple test will be ran on the battery to figure the overall performance. In order to verify the battery will not fail during normal operations.

- General Performance
- Environmental Testing
- Mechanical Testing
- Safety testing

Testing Method	Performance	Check(√)
Standard Charging and Discharging time	charge≈ 60 min	√
Standard Discharging time with different loads	1Amp load ≈ 54 min	√
Cycle Life	≈ 400 times	√
High temperature functionality	≈ 210min	√
Low temperature functionality	≈ 270min	√
Collision	No influence to battery performance	√
Drop test	No explosion of fire	√
Vibration	No influence to battery performance	√
Over charge test	No explosion of fire	√
Over discharge test	No explosion of fire	√
Short- circuit	No explosion of fire	√

LiPo Charger-MCP73871

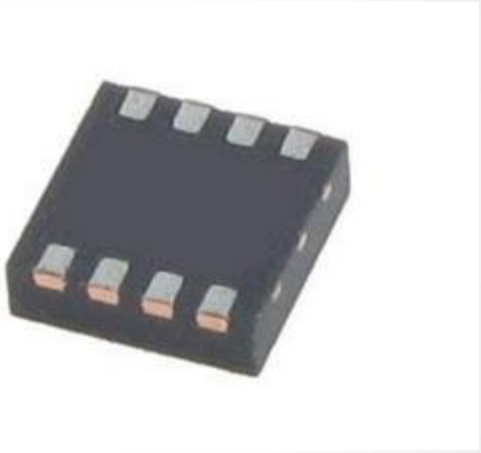
Manufacturer	Microchip Technology
Part Model:	Battery Management
Price:	$1.94
Purchased From:	Mouser
Product Type:	Charge Management
Connector:	20-pin
Output Voltage:	4.2 V
Output Current:	50mA to 1000mA
Dimensions:	4mm x 4mm

LiPo Charger

- Simultaneously Power the system and charge the battery
- Integrated reverse discharge protection
- Versatile
- Automatic recharge
- Automatic end-of-charge control
- Safety features
- Low battery Status indicator
- Power on status indictor
- Autonomous power source selection
- Low external component
- Good communication with Micro-controller
- Small size Good communication with Micro-controller

Gas Gauge - MAX17048

Manufacturer	Maxim Integrated
Product Model:	Battery Management
Price:	$2.39
Purchased From:	Mouser
Product Type:	Fuel Gauges
Connector:	9-pin
Output Voltage:	0.4 V
Operating Voltage:	2.5 V to 4.5 V
Operating Current:	23 µA
Dimensions:	2 mm x 2 mm



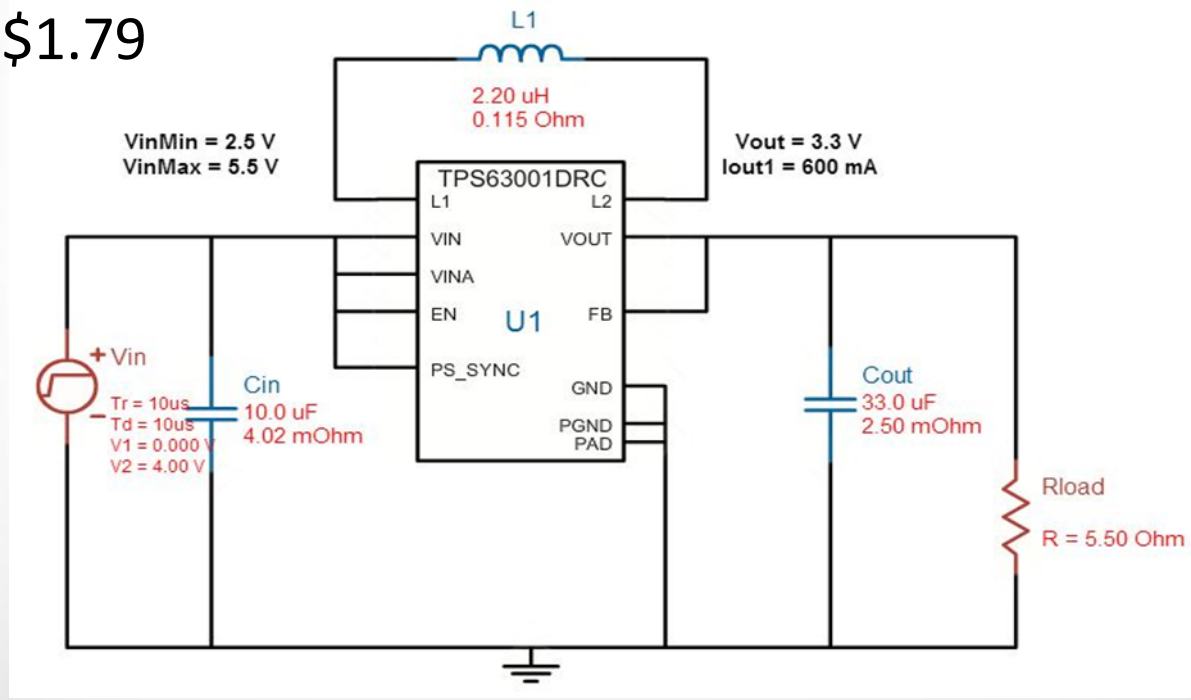
Gas Gauge

- Algorithm based sensing
- No current sense resistors
- No learned battery cycles necessary
- Temperature compensation
- Autonomous detecting
- Accurate
- Voltage measurement improvement on battery insertion
- I2C communication
- Small size
- Programmable
- Reports on battery information

- Algorithm based sensing
- No current sense resistors
- No learned battery cycles necessary
- Temperature compensation

Voltage Regulation

- Buck-boost topology (Webench).
- Vout = 3.3V
- Efficiency = 85%
- Cost = $1.79



Development

T.I. CC320MOD LaunchPad

- Contains JTAG & Flash circuitry
- Useful hardware and software files

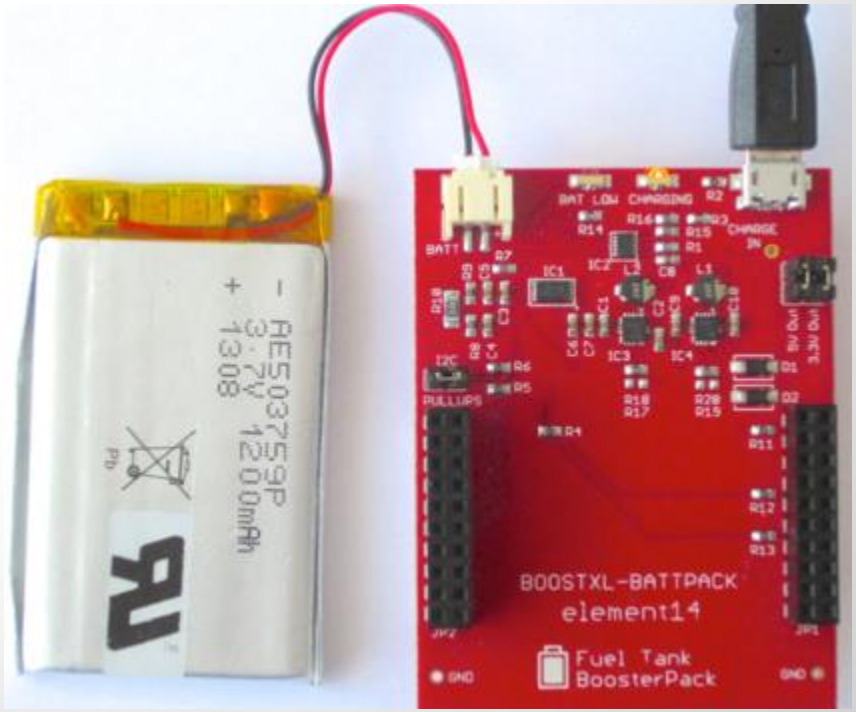
Manufacturer	Texas Instruments
Model	CC3200MODLAUNCHXL
Price	$34.99
Purchased at	Mouser

Development

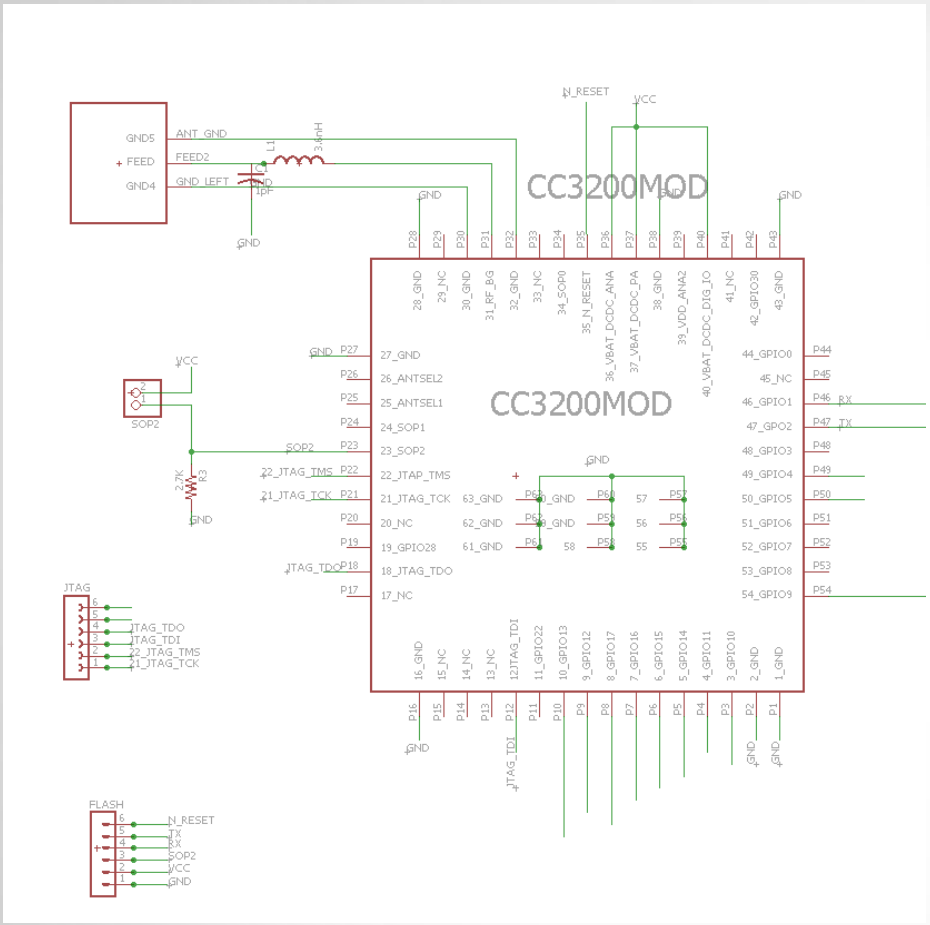
Battery Booster Pack

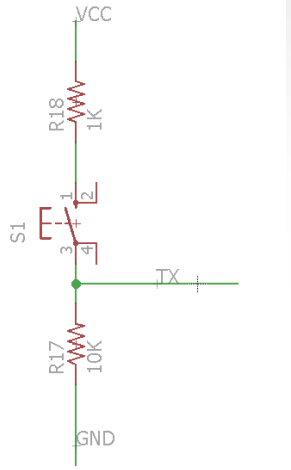
- Comes with LiPo battery
- Gave platform for hardware and software development

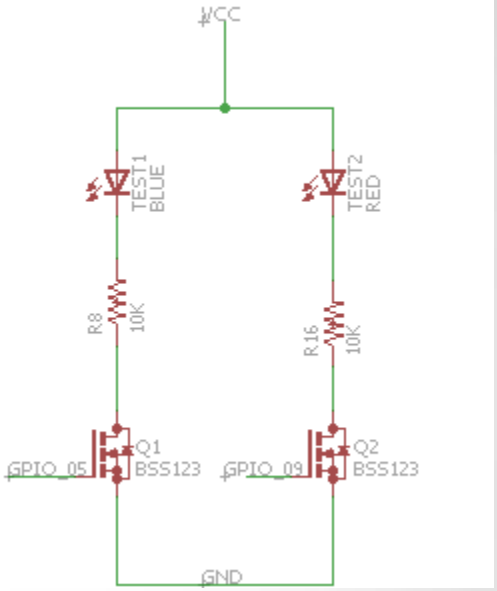
Manufacturer	Texas Instruments
Model	BOOSTXL-BATTPACK
Price	$19.99
Purchased at	Element 14

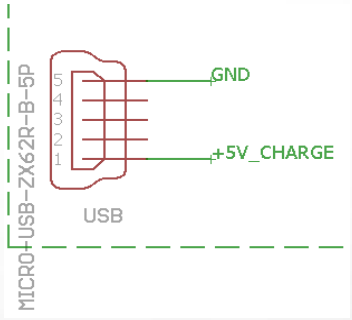


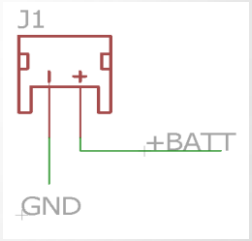
PCB Schematic



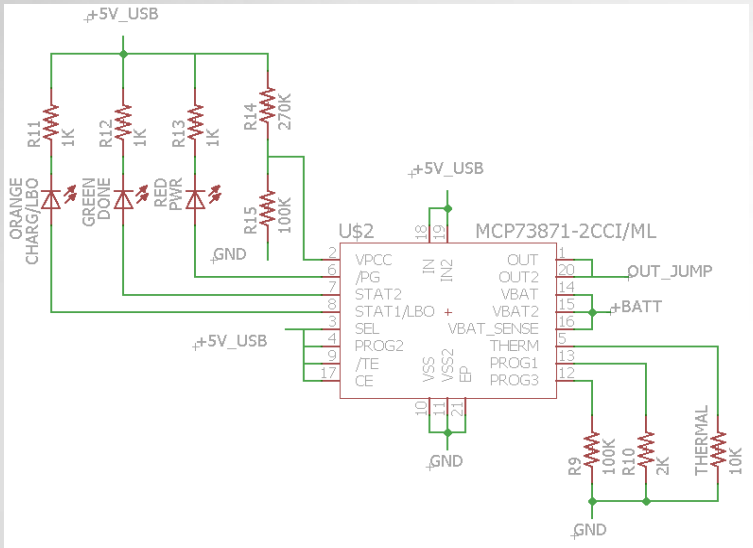


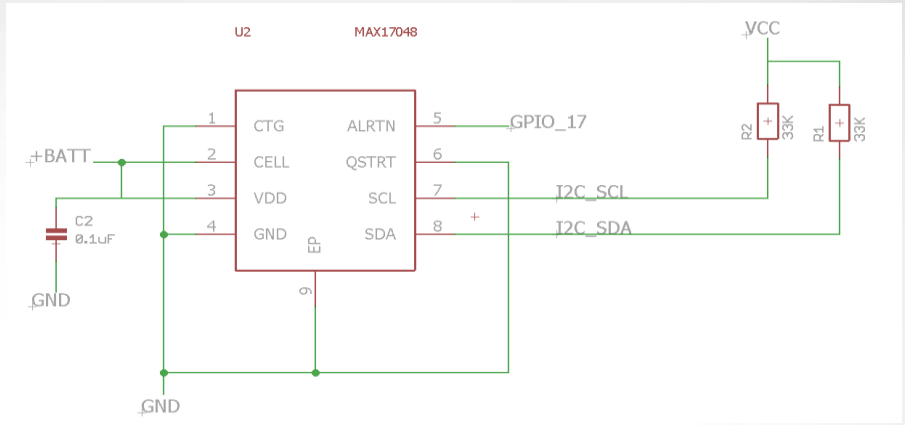


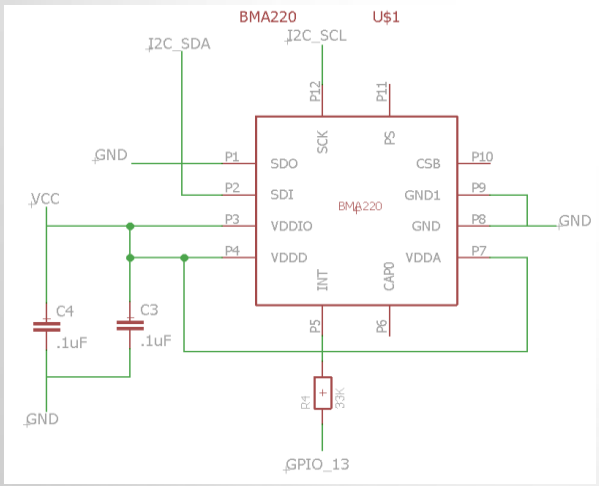


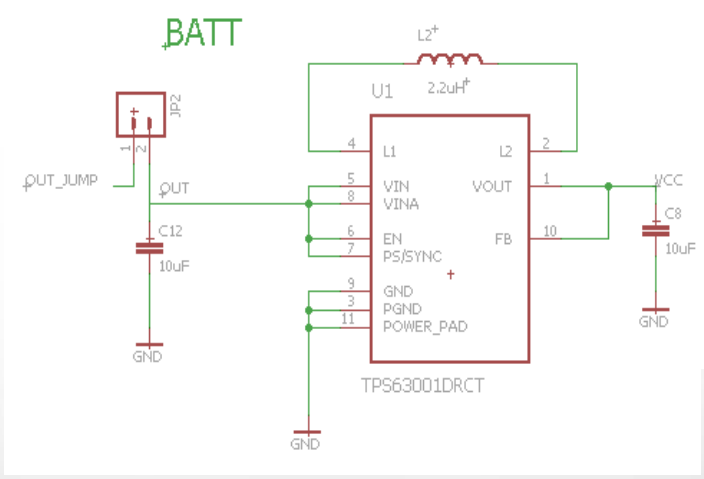


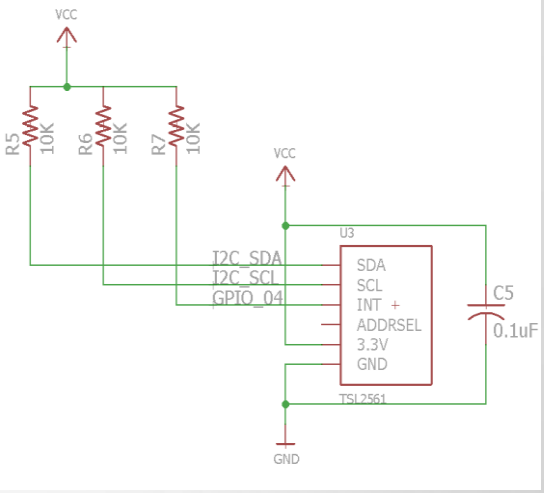
PCB Schematic



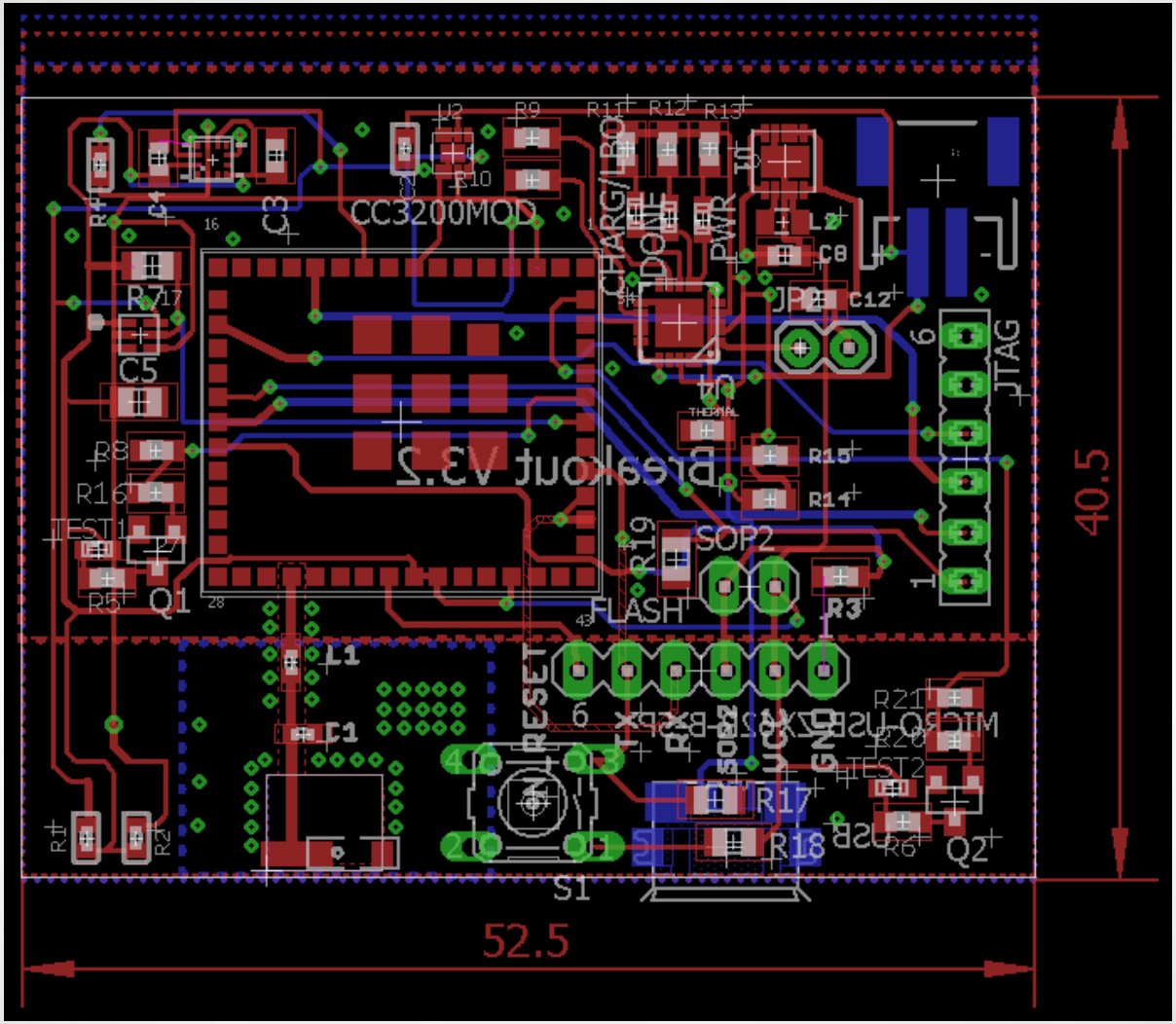




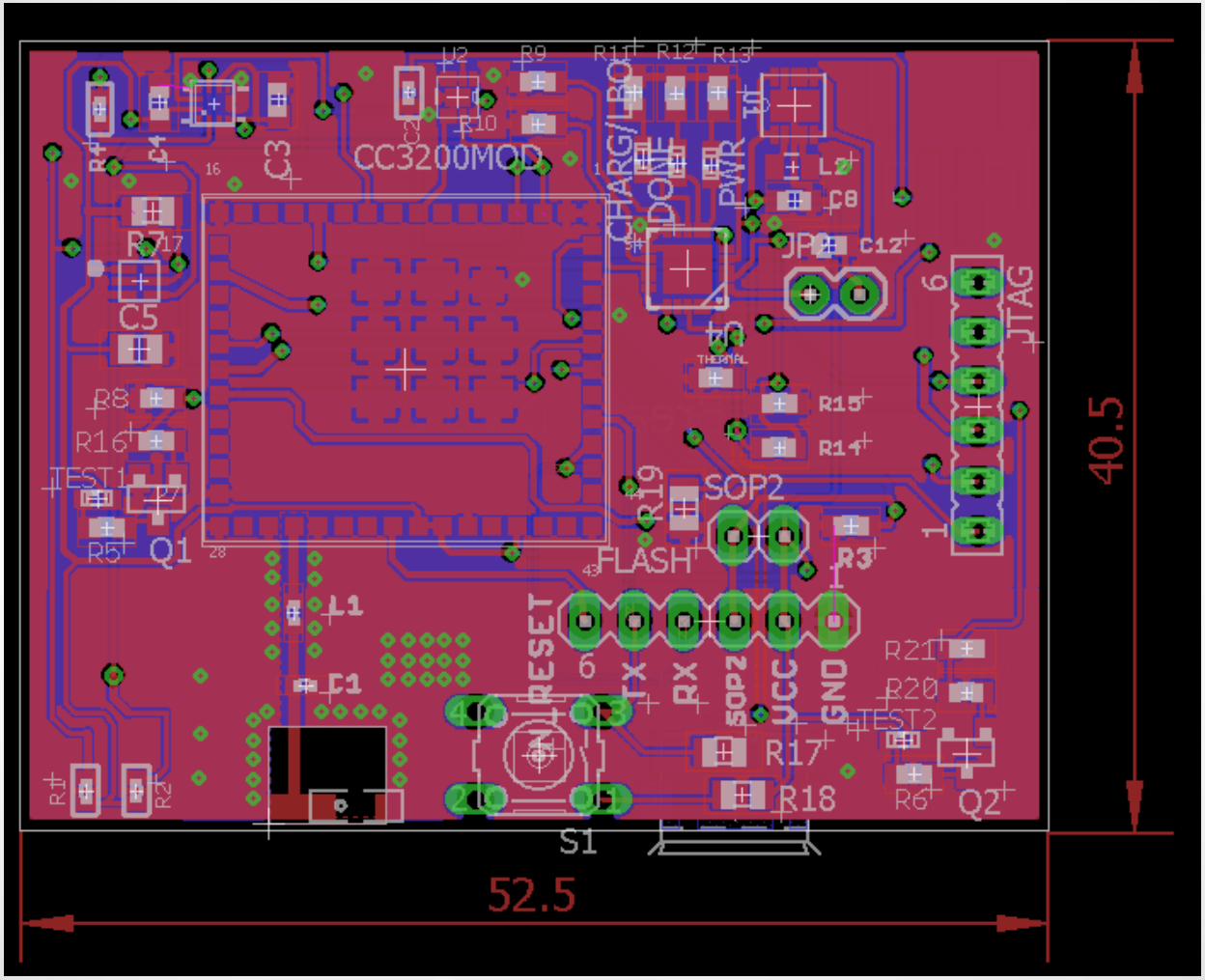




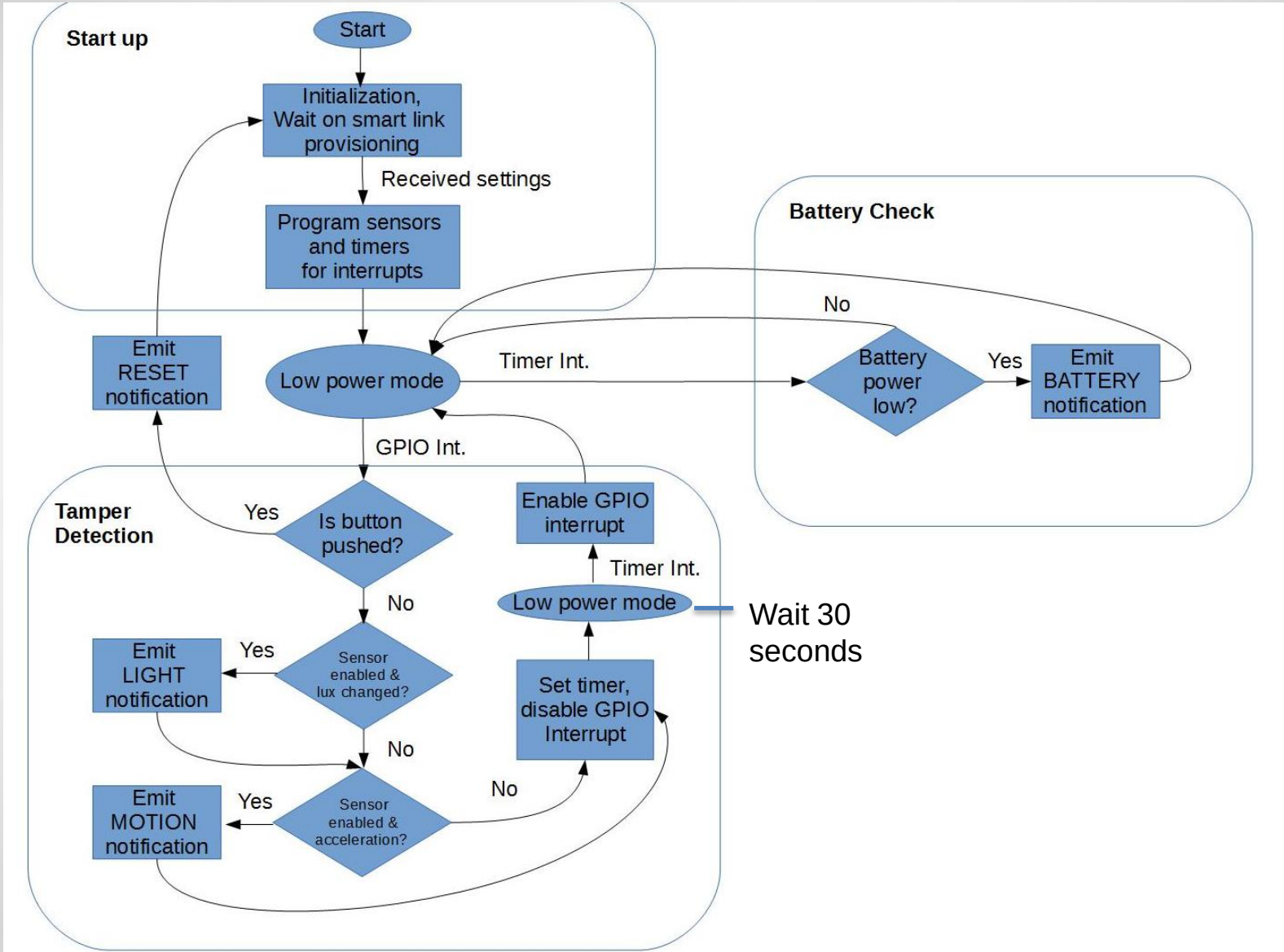
PCB Layout


CC3200MOD
CHARG/LBO
DONE
PWR
JTAG
SOP2
FLASH
RESET
GND
Breakout V3.2
40.5
52.5

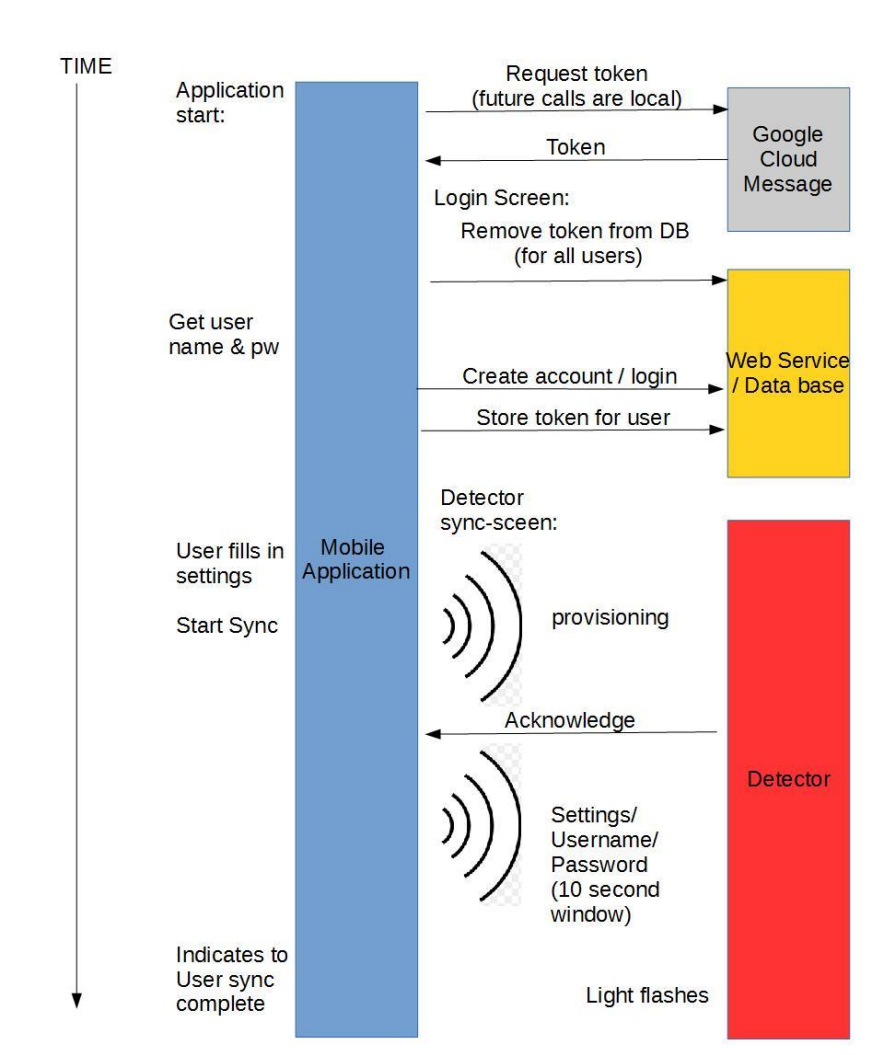
PCB Layout


CC3200MOD
CHARG/LBO
DONE
PWR
JTAG
SOP2
FLASH
RESET
TX
RX
VCC
GND
TEST1
TEST2
Q1
Q2
S1
40.5
52.5

Detector Program Flow



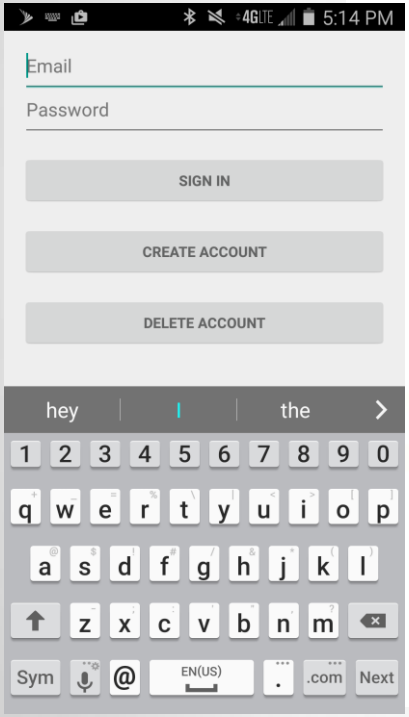
Start-up Overview



Google Cloud Messaging

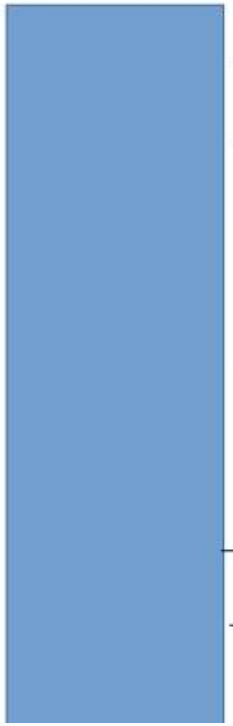
- Application ID:
- App is registered with google by developer to obtain.
- Shared amongst all instances of the application .
- Hard coded into both mobile application and detector.
- Token: Tied to particular physical device.
- Gotten at initial application start-up, stored for reuse. Communicated to detector during sync process.
- Stored in database for sending notifications.

Start-up -1



Application start:

Get user name & pw



Request token (future calls are local)

Token

Google Cloud Message

Login Screen:

Remove token from DB (for all users)

Create account / login

Store token for user

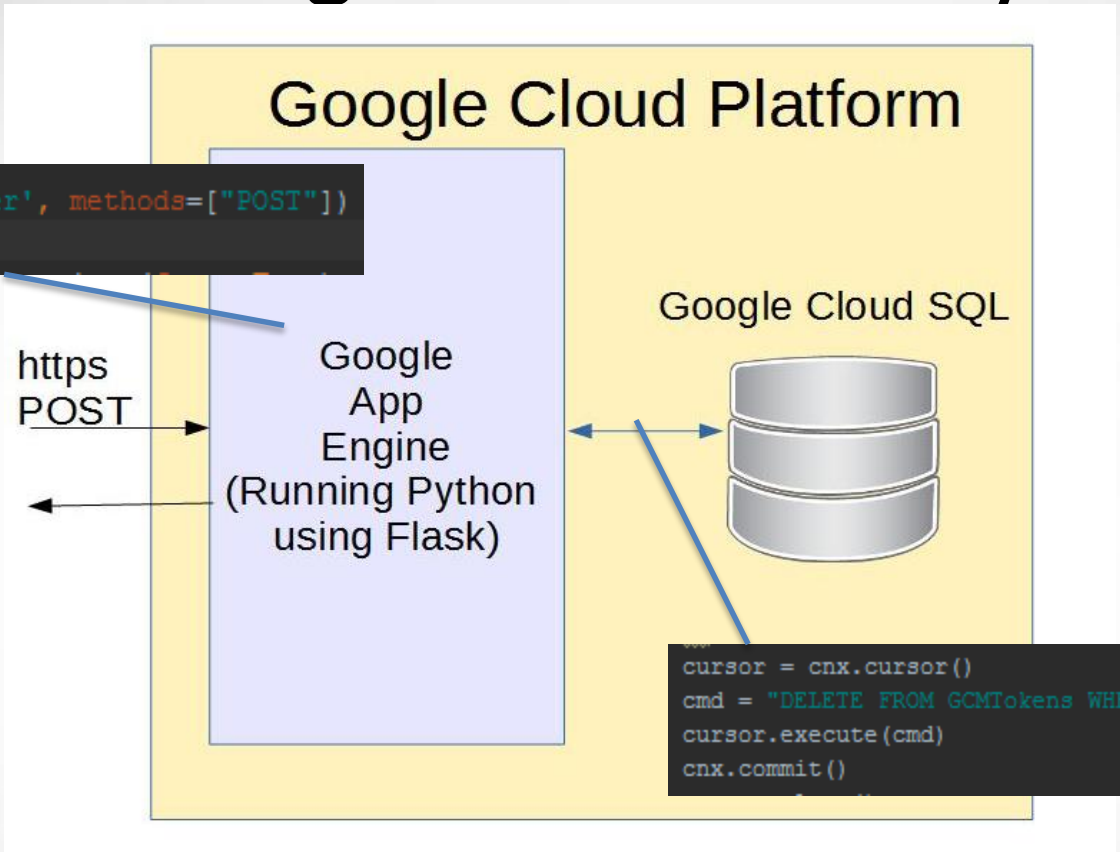
Web Service / Data base

Communication between System Components (except provisioning and mDNS)

- POST requests over https
- Data is exclusively formatted in JSON
- Example:

```
{
  "name" : "a@b.com",
  "password" : "12345",
  "detector" : "cereal",
  "message" : "cereal tasted"
}
```

The Web Service - Google makes it easy



- A total of 6 URI are used. (/logIn, /createAccount, /deleteAccount, /logTamper, /displayLog, /storeGCMToken, /deleteGCMToken)
- Google Cloud Messaging is a separate service.

Web Service Program Design – Python using Flask

- Program design is a set of functions which get called when a particular URI is requested.
- Contents of JSON are parsed and helper functions are used to access and update the database.
- Very little, to no, iteration used

Database - User

```
mysql> describe User;
+----------+------------------+------+-----+-------------------+----------------+
| Field    | Type             | Null | Key | Default           | Extra          |
+----------+------------------+------+-----+-------------------+----------------+
| id       | int(10) unsigned | NO   | PRI | NULL              | auto_increment |
| name     | varchar(100)     | YES  |     | NULL              |                |
| password | varchar(500)     | YES  |     | NULL              |                |
| ts       | timestamp        | NO   |     | CURRENT_TIMESTAMP |                |
+----------+------------------+------+-----+-------------------+----------------+
```

- Actual password is not stored in database, rather irreversible hash of password is stored.
- Row added to table from login screen on mobile application (create account).
- Row can be deleted from login on mobile application (delete account).
- Table checked for username and password hash match on login.

Database - Tampering

```
mysql> describe Tampering;
+----------+------------------+------+-----+-------------------+----------------+
| Field    | Type             | Null | Key | Default           | Extra          |
+----------+------------------+------+-----+-------------------+----------------+
| id       | int(10) unsigned | NO   | PRI | NULL              | auto_increment |
| name     | varchar(100)     | YES  |     | NULL              |                |
| detector | varchar(100)     | YES  |     | NULL              |                |
| message  | varchar(500)     | YES  |     | NULL              |                |
| ts       | timestamp        | NO   |     | CURRENT_TIMESTAMP |                |
+----------+------------------+------+-----+-------------------+----------------+
```

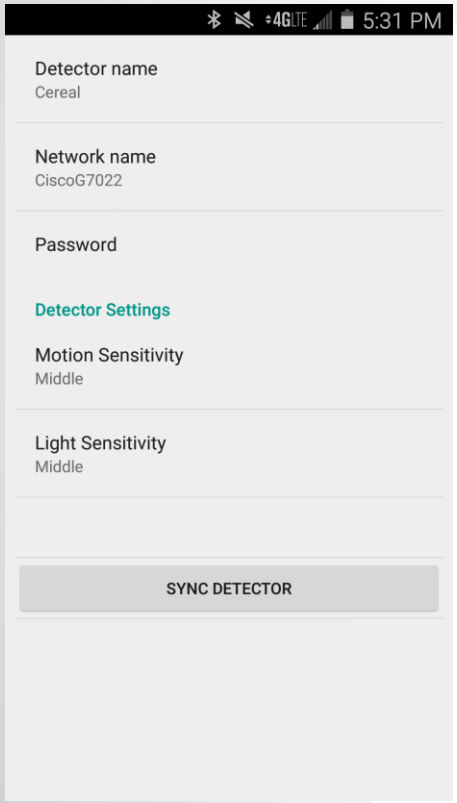
- User name must exist in the database, and password hash must agree, before tamper gets stored in the database.

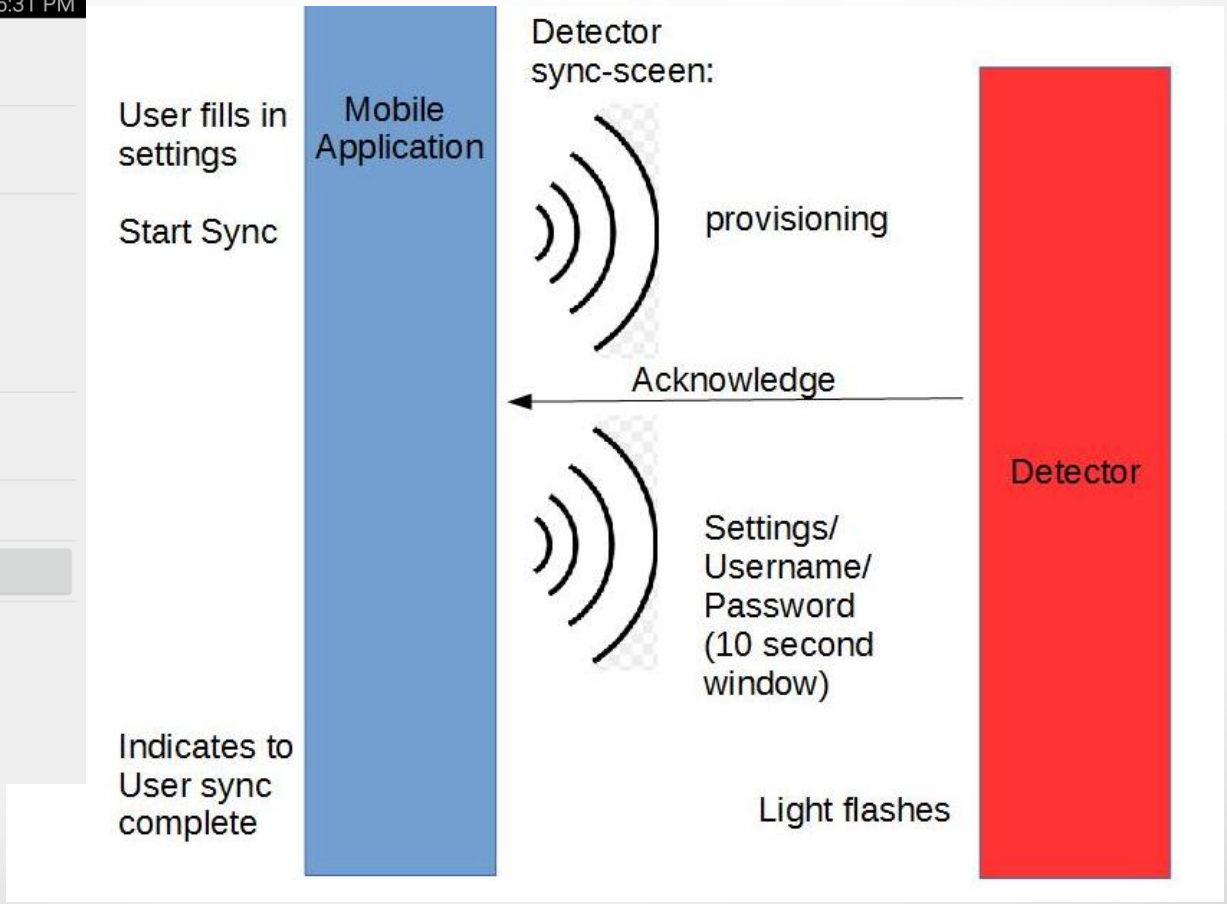
Database - Tokens

```
mysql> DESCRIBE GCMTokens;
+-------+--------------+------+-----+---------+-------+
| Field | Type         | Null | Key | Default | Extra |
+-------+--------------+------+-----+---------+-------+
| name  | varchar(255) | YES  |     | NULL    |       |
| token | varchar(500) | YES  |     | NULL    |       |
+-------+--------------+------+-----+---------+-------+
```

- User name must exists in database, and password hash agree, before the token can be stored.
- Unlimited number of tokens per user allows user to get notifications on unlimited number of devices.
- What if users are sharing a device, and one user force stops application? Will device receive notifications for both users? – This is why tokens are removed on start up.

Start-up 2


5:31 PM
Detector name
Cereal
Network name
CiscoG7022
Password
Detector Settings
Motion Sensitivity
Middle
Light Sensitivity
Middle
SYNC DETECTOR


User fills in settings
Start Sync
Mobile Application
Detector sync-sceen:
provisioning
Acknowledge
Settings/ Username/ Password (10 second window)
Light flashes
Detector
Indicates to User sync complete

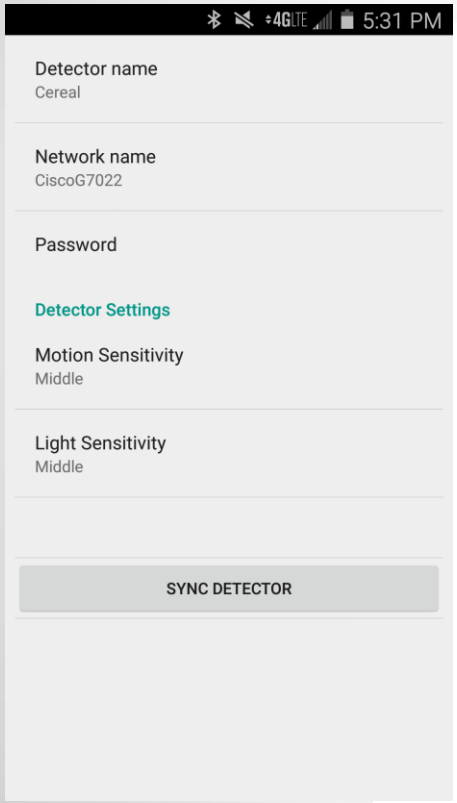
Provisioning – TI Smart-Config

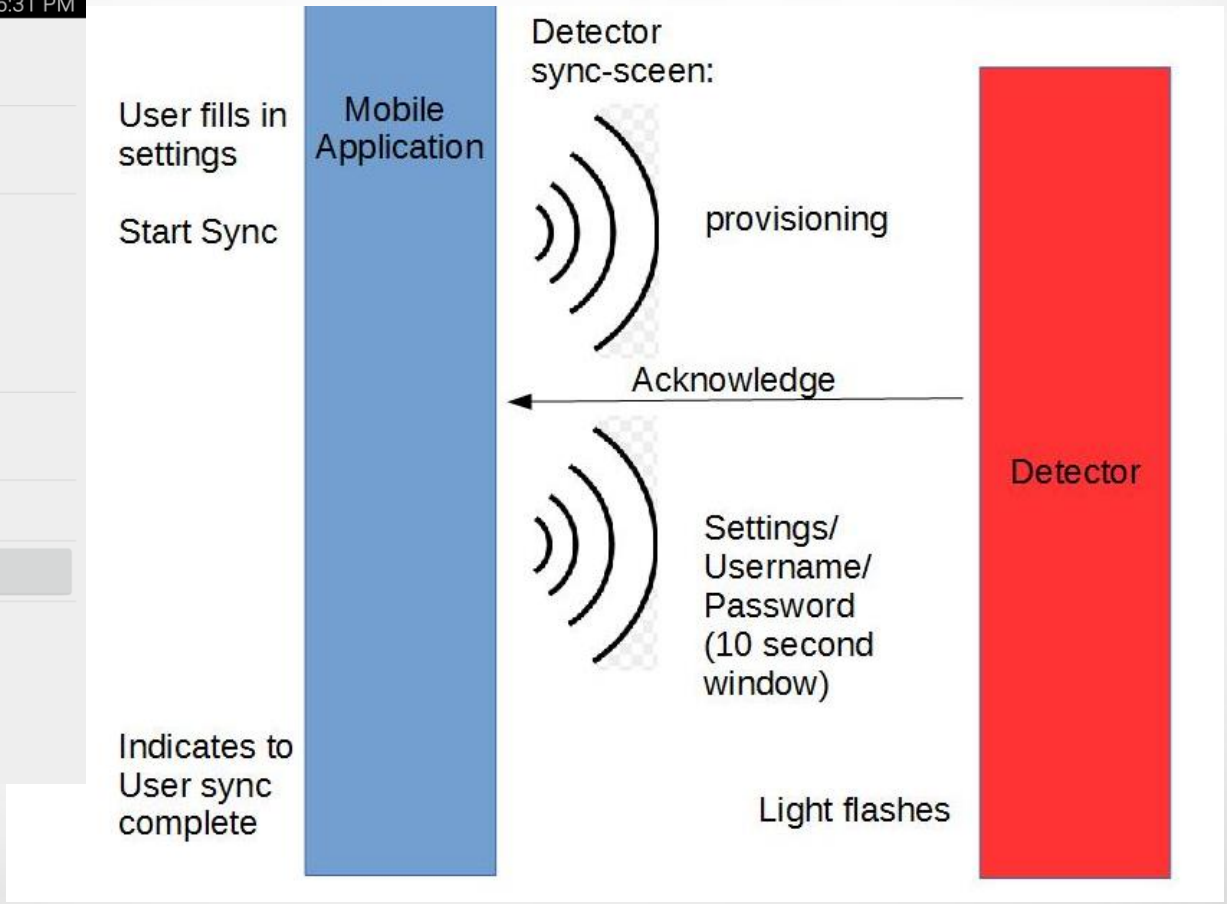
- Best seen here as a black box that gets the CC3200 on the Wi-Fi network.
- It communicates Wi-Fi ssid and passkey to CC3200 using packet lengths.
- Smart-Config libraries continue the process connecting the CC3200 to Wi-Fi network.
- ISSUE – DOES NOT SUPPORT ADDITIONAL FIELDS TO TRANSMITT SETTINGS DATA!

mDNS and DNS-SD

- Multicast DNS resolves host names to IP addresses
- Used with DNS Service Discovery it allows one device to look for a service advertised with a particular name.
- Service advertises port, service type, and a text field.
- This text field is used here to transmit additional information from the mobile app to the detector.
- <light-settings>_<motion-settings>_<detector-name>_<user-name>_<password>
- Then service is deregistered

Start-up 2

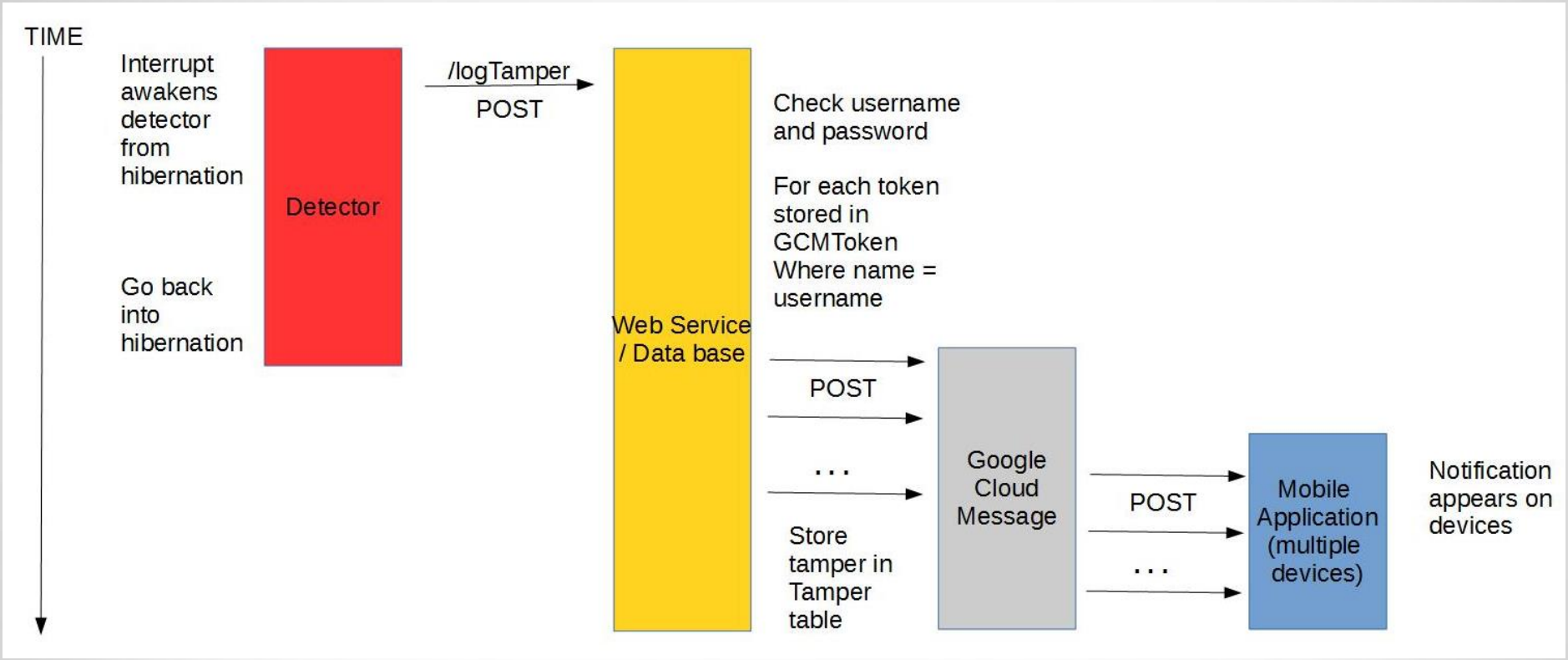

5:31 PM
Detector name
Cereal
Network name
CiscoG7022
Password
Detector Settings
Motion Sensitivity
Middle
Light Sensitivity
Middle
SYNC DETECTOR


User fills in settings
Start Sync
Mobile Application
Detector sync-sceen:
provisioning
Acknowledge
Settings/ Username/ Password (10 second window)
Light flashes
Detector
Indicates to User sync complete

Start-up Conclusion

- The detector, after receiving the string in the text field of the mDNS advertisement, blinks and proceeds with its program flow.
- After the 10 seconds of advertising the mobile app deregisters the advertised service and stops its spinner.
- When the detector is able, it sends a notification to the mobile application. Not receiving this indicates the user should re-sync.

A Tampering

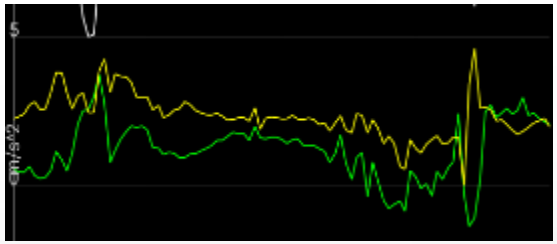

TIME
Interrupt awakens detector from hibernation
Go back into hibernation
Detector
/logTamper
POST
Web Service / Data base
Check username and password
For each token stored in GCMToken Where name = username
POST
. . .
Store tamper in Tamper table
Google Cloud Message
POST
. . .
Mobile Application (multiple devices)
Notification appears on devices

Current Design Weakness

- The mDNS advertising gives away the user name and password locally. This could be solved by encrypting it, but a hard coded key on the detector could be compromised, making it useless. Alternatively, the mobile application could generate a random user id to be used by the detector, but this too would have to be advertised. –ideas?

Current Design Issues

- The current threshold settings were determined purely heuristically, and based too few experiments.
- How can we justify these? Statistics, experiments, theory, etc…?

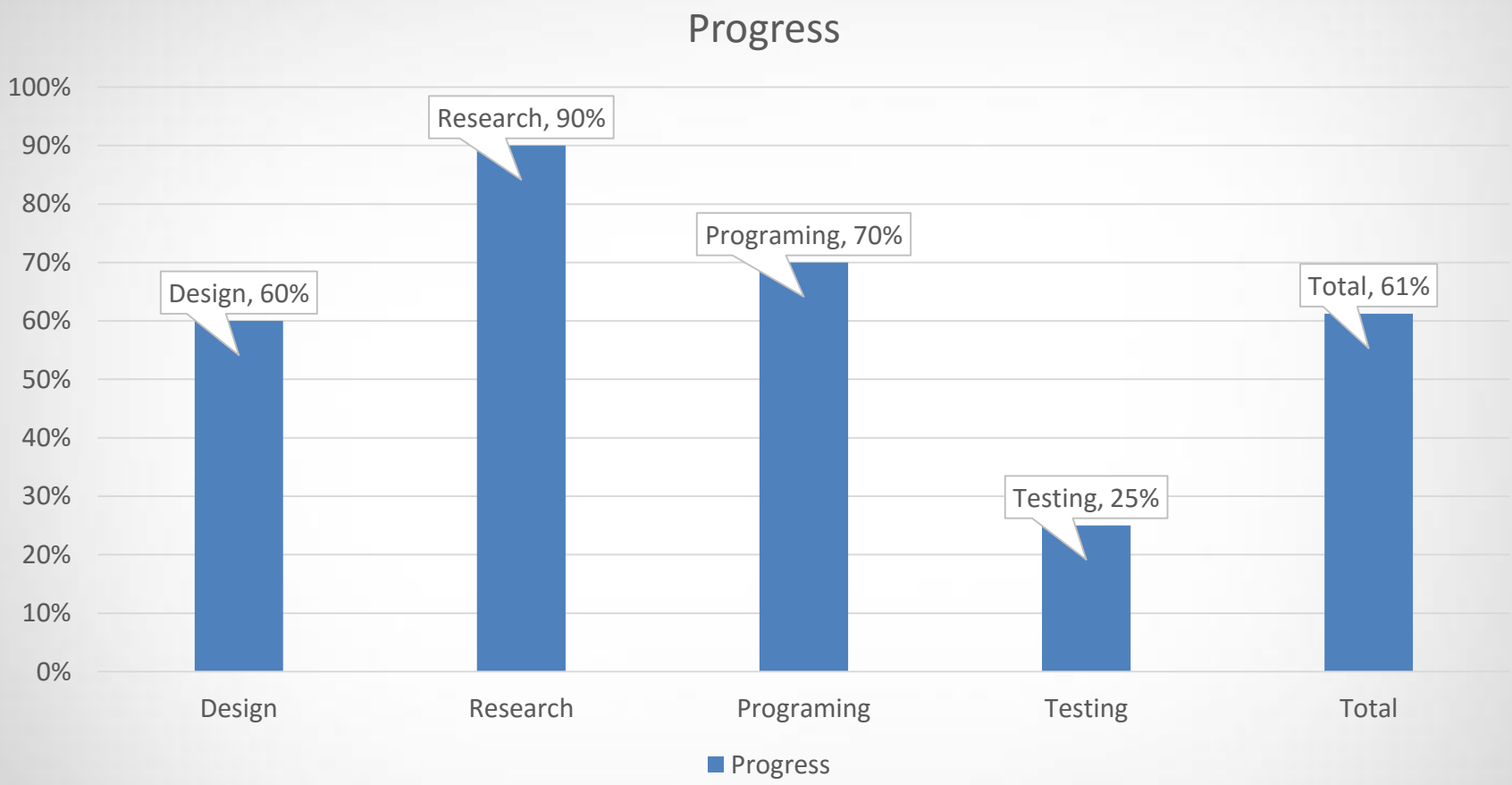


Budget

- Amount spent by purchase:

Supplier	Date	Price
Adafruit	9/23/2015	$24.73
Mouser	9/23/2015	$50.62
Banggood	9/28/2015	$10.12
Newark	11/2/2015	$36.61
Texas Instruments	11/8/2015	$31.03
Texas Instruments	11/11/2015	$41.99
UCF Print	12/8/2015	$44.46
Newark	1/20/2015	$44.08
Mouser	1/20/2015	$104.64
OSH Park	1/21/2015	$37.80
Total		$426.08
Budget		$700
Remaining		$273.92

Progress


Progress
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Design, 60%
Research, 90%
Programing, 70%
Testing, 25%
Total, 61%
Design
Research
Programing
Testing
Total
Progress

Questions?