Center for Open Access in Science ▪ https://www.centerprode.com/ojit.html
Open Journal for Information Technology, 2022, *5*(2), 55-64.
ISSN (Online) 2620-0627 ▪ https://doi.org/10.32591/coas.ojit.0502.02055m

Enhancing Asset Security by Integrating Internet of Things on Non-Powered Assets

Joshua Mueke Mwema, John M. Kandiri & Stephen Titus Waithaka

Kenyatta University, Nairobi, KENYA
Department of Computing and Information Technology

Received: 2 May 2022 ▪ Revised: 15 September 2022 ▪ Accepted: 7 October 2022

Abstract

Rapid proliferation of the Internet of things (IoT) has helped solve a myriad of problems across different sectors. Whilst powered assets rely on their own power source to enhance asset monitoring, a need exists to develop an asset security system for non-powered assets. Since an IoT device has network layers, it can be used with the physical layer to solve this problem. As a result, a method of enhancing asset security with IoT was implemented. A GSM chip for SMS and server connection was used to communicate the battery status and location information obtained from a GPS chip. A method of detecting tamper on the device was implemented through infrared sensors. A microcontroller was the heart of the system as it interfaced with all other devices to form the IoT system. The result of the study was an efficient prototype of an IoT asset tracking device which communicates through SMS and it logs location data to a remote server through GPRS connection. There is a room for improvement in terms of optimizing power consumption to lengthen the duration before a recharge is required.

Keywords: internet, asset security, Internet of things, non-powered asset.

1. Introduction

The internet of things (IoT) technology comprises networked devices which utilize mainly the physical layer to collect data and transmit it to a destination through the network layer (Minhaj & Khaled, 2018). As such, there is a lot of potential of automating systems through IoT as it provides actionable information. One of the vibrant applications of IoT is in asset security and monitoring where many studies have been done on development of smart security systems targeting an asset's location and condition (Valente & Neto, 2017). Utilization of IoT in data analytics has yielded predictive maintenance. For instance, OracleIoT (2020) described a system of preventing unforeseen machine breakdowns by processing data received from IoT systems with advanced analytical algorithms. In the area of asset security, IoT systems require communication mechanisms to alert the user about the asset. According to Indira et al. (2019) and Andreas et al. (2018), global system for mobile communication (GSM), Wi-Fi, and remote servers are some of the main methods used alongside IoT to achieve seamless data transmission.

Asset security in vehicles and laptops may be achieved through powering an IoT system with onboard batteries (Nirit et al., 2019). On the other hand, not all assets have an onboard power supply. At the same time, IoT systems must be powered electrically to perform embedded tasks (Andrey & Raffaele, 2019). Thus, non-powered assets such a sofa sets and TV sets

Correspondence: Joshua Mueke Mwema, Kenyatta University, Department of Computing and Information Technology. E-mail: joshuamke@gmail.com.

may be lost without noticing as Smartrak (2020) notes that there is still a challenge of securing these kinds of assets. The present study aimed at developing an asset security device that would not only report location change and upload location data to a remote server but also notify the user when it required battery recharging. Further, the system would report if it was tampered by opening its casing.

2. Methods and materials

The functional features of the IoT asset security system were achieved through design and implementation of different subsystems which were brought together reaching the proposed system. The main subsystems as shown in the figure below are; GMS module, GPS module, antitamper circuit, voltage regulation module, a logic level converter and the microcontroller. The code that controls the system was developed to function as per the flow chart. The program was written in C++ language using the arduino integrated development environment (IDE). Moreover, the circuit diagram was drawn using Proteus design suite. On the other hand, ThingsSpeak open-source server was used to create a sever account where data about the location was logged remotely using API keys method. Prototyping tools such as soldering gun, solder wire, prototyping circuit board and jumper wires were utilized in assembling the circuit.

The security system works with help of sensors, modules and a code embedded in a microcontroller. The microcontroller first checks the battery voltage followed by the status of the device casing then location change. If the battery voltage is lower than a threshold, it sends a battery low SMS through a GSM module. The GSM module communicates with the microcontroller through AT commands and hence the serial protocol is used. At the same time, the MCU checks whether the device casing is open by reading the output of the infrared proximity sensor where it sends an SMS to the owner if the case is open. Lastly, the MCU reads the GPS module to retrieve location coordinates where it sends them to a remote server through a GPRS connection. If there is a significant change in the pre-set location, an SMS is sent to the owner about the current location. If none of the conditions mentioned here are met, there no SMS triggering. Communication between GSM, GPS and the MCU is through universal asynchronous and receiver and transmitter (UART) protocol. During serial communication, high logic signals emanate from the transmitting pin of the device, a reason why a logic level converter is used to protect non-5V ports from damage by the high voltage signals. As GSM chips draw more current during transmission, i.e., transmission bursts, they can create short circuits hence in the circuit, it is connected via a dc-dc converter that can withstand current sourcing of up to 3A without need of a heat sink. Moreover, the voltage circuit is built around a voltage divider circuit to achieve a voltage less than 5v that can be fed into the analog pin of the MCU for measurement.

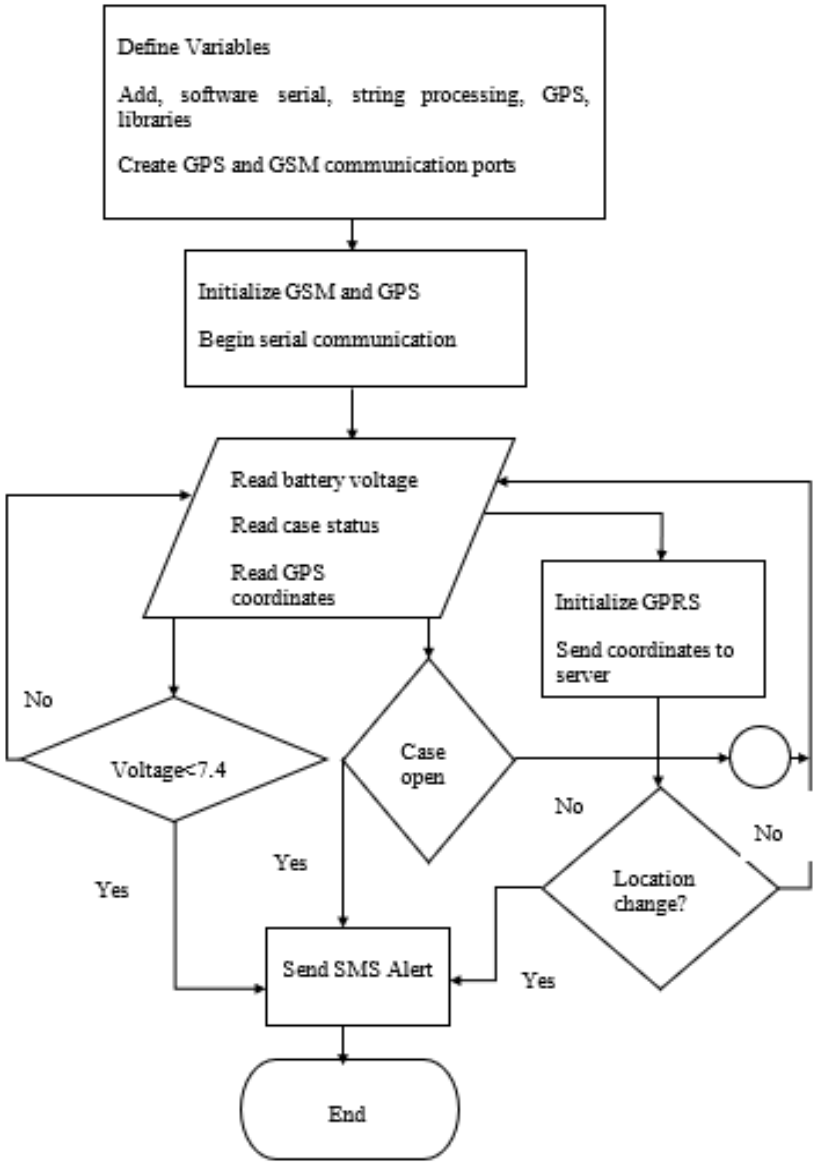


Figure 2. Flow chart diagram

3. Results

3.1 *Voltage measurement*

Using two resistors R1 and R2 of 3.3k and 1k respectively, a maximum output voltage of the sensor was achieved as 1.95V. This was a safe voltage as it cannot damage the ADC channel of the arduino. A conversion factor of 4.3 which is the total resistance was used to compute the actual voltage from the reduced voltage. As the device was in use, the battery voltages were recorded during test instances as; 7.07V, 6.97V and 6.89V.

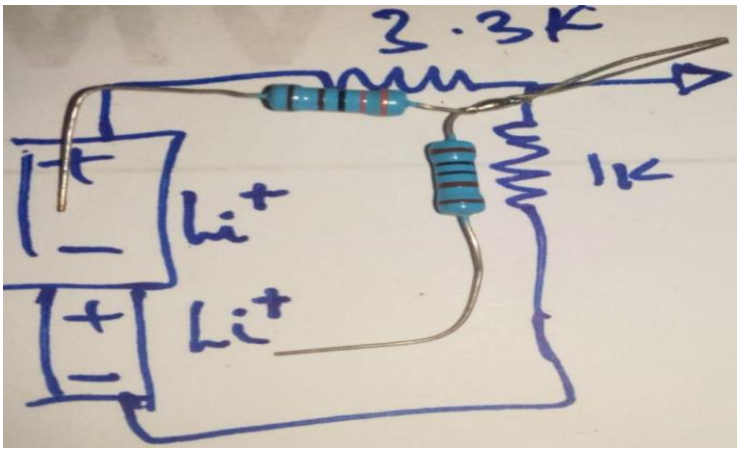
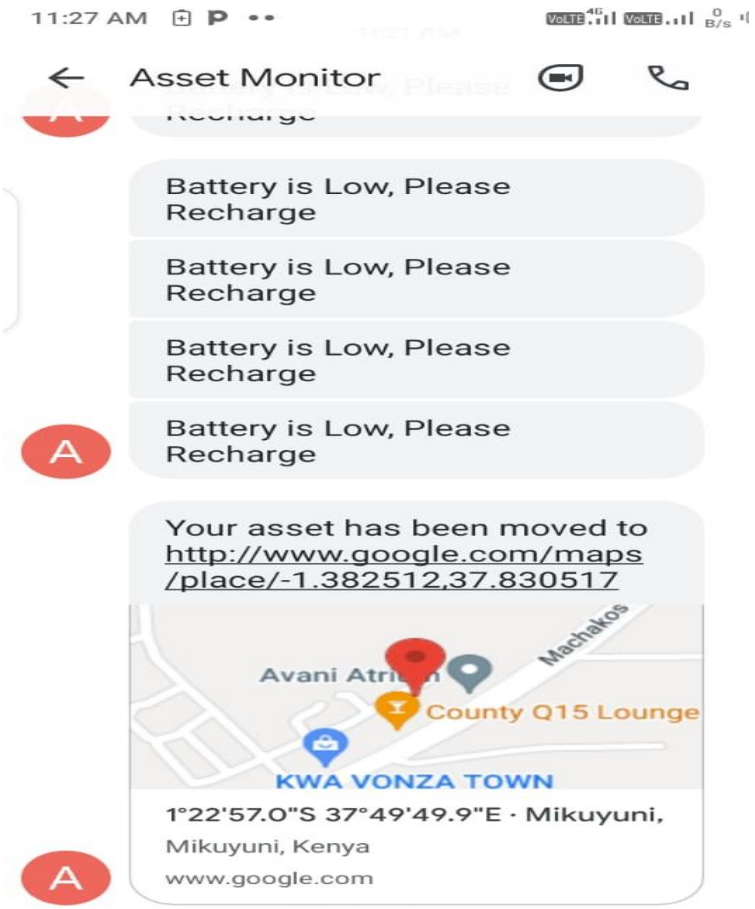


Figure 3. Voltage measurement circuit

3.2 *Location and low battery alerts*

As shown below, a battery low alert message was received when the battery was lower than the set threshold. Moreover, an SMS showing the location link was sent where the user could just click the link and view the asset location.



3.3 *Server data*

The location coordinates retrieved from the server are shown in the plot below.

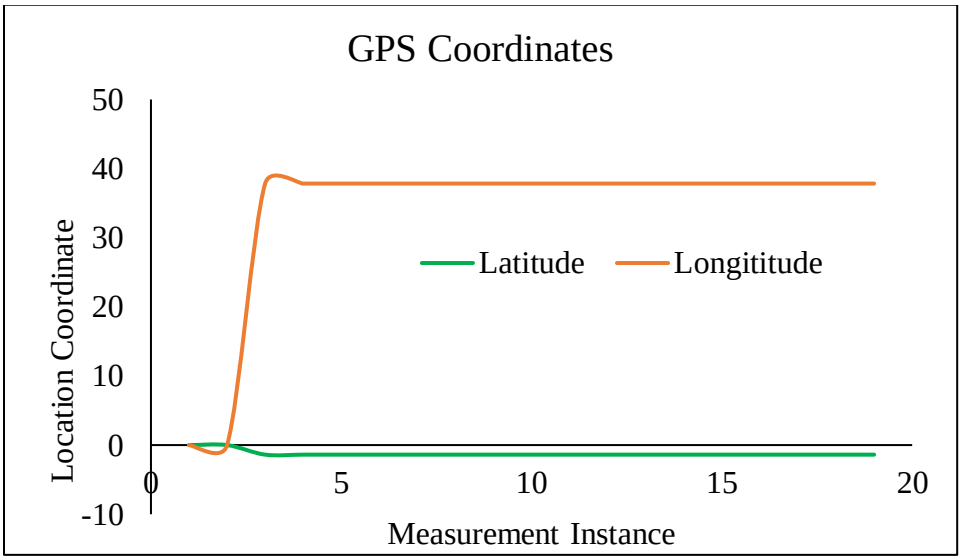


Figure 4. Location data retrieved from server

Figure 4 above was plotted using raw data imported from the server. However, the server has visualization features which were utilized to plot latitude and longitude data on separate graphs in real-time. The two visuals are shown below.

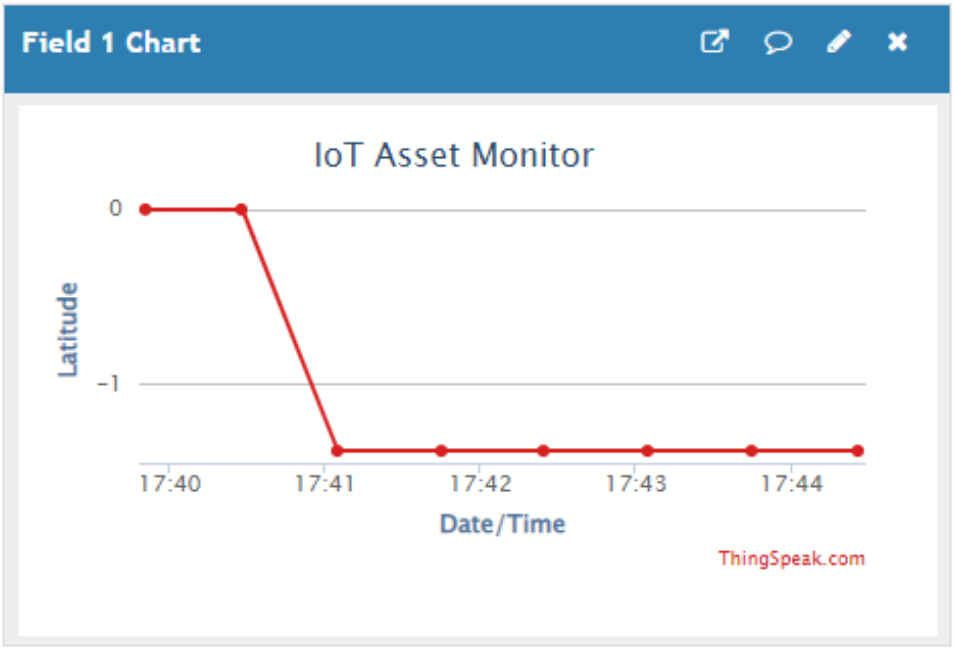


Figure 1. Latitude data

Initially, the latitude data was zero but it progressed to -1.3xxxxxx after a short time as shown in figure 4 above.

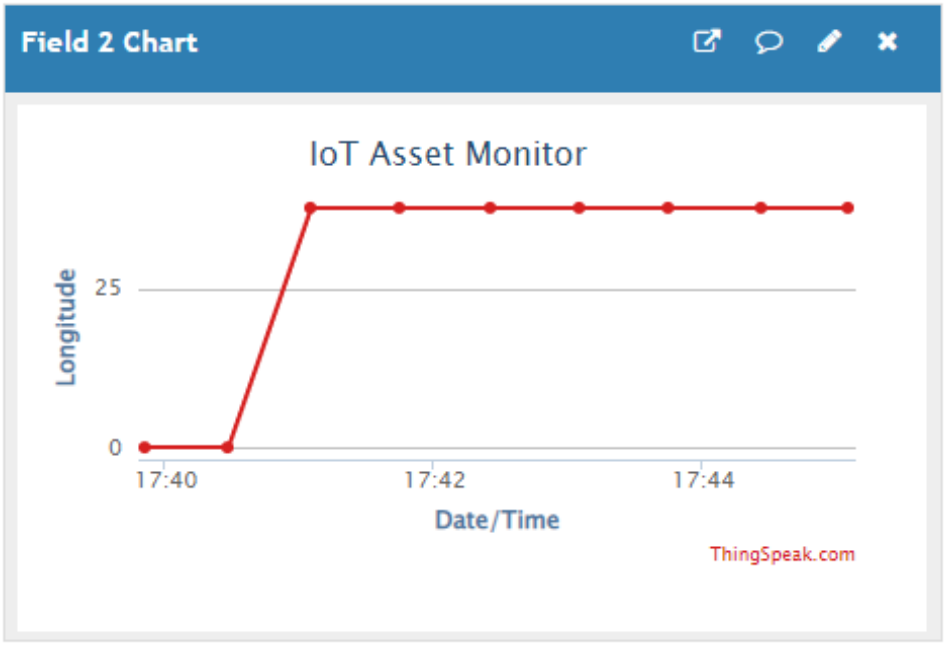
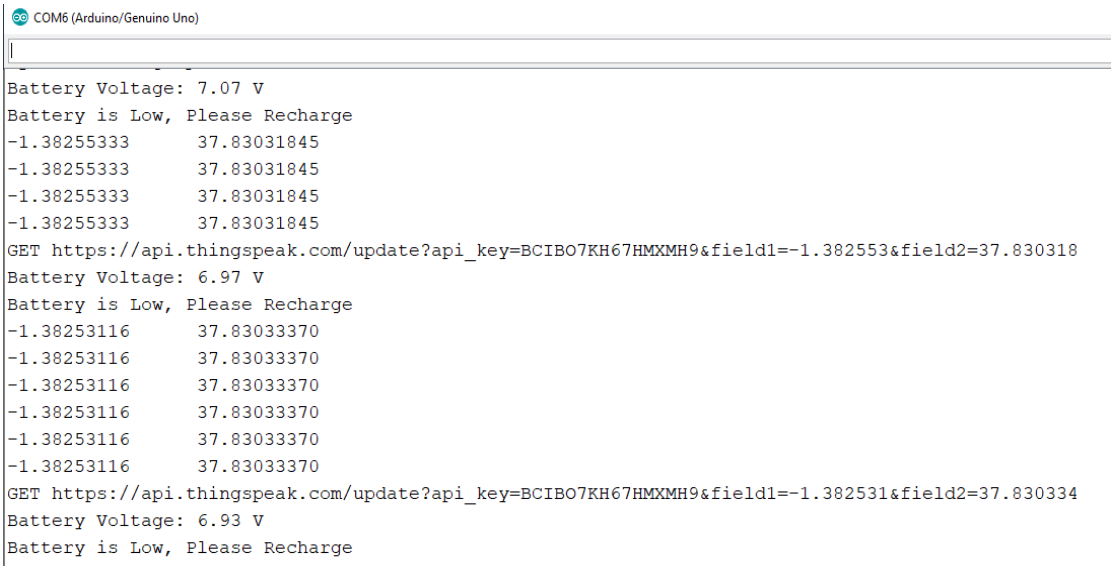


Figure 6. Longitude data

As noted in figures 4 and 5 above, there are instances where the location coordinates were both zero. After sometime, it was noticed that the value changed to several digits of different decimal values. A snip shot of serial output is shown below. The voltage is seen to decrease as GPRS transmission occurs. Data for each coordinate was logged to a separate channel using API keys shown in the serial monitor output.



The figure below shows the complete prototype with all parts labelled.

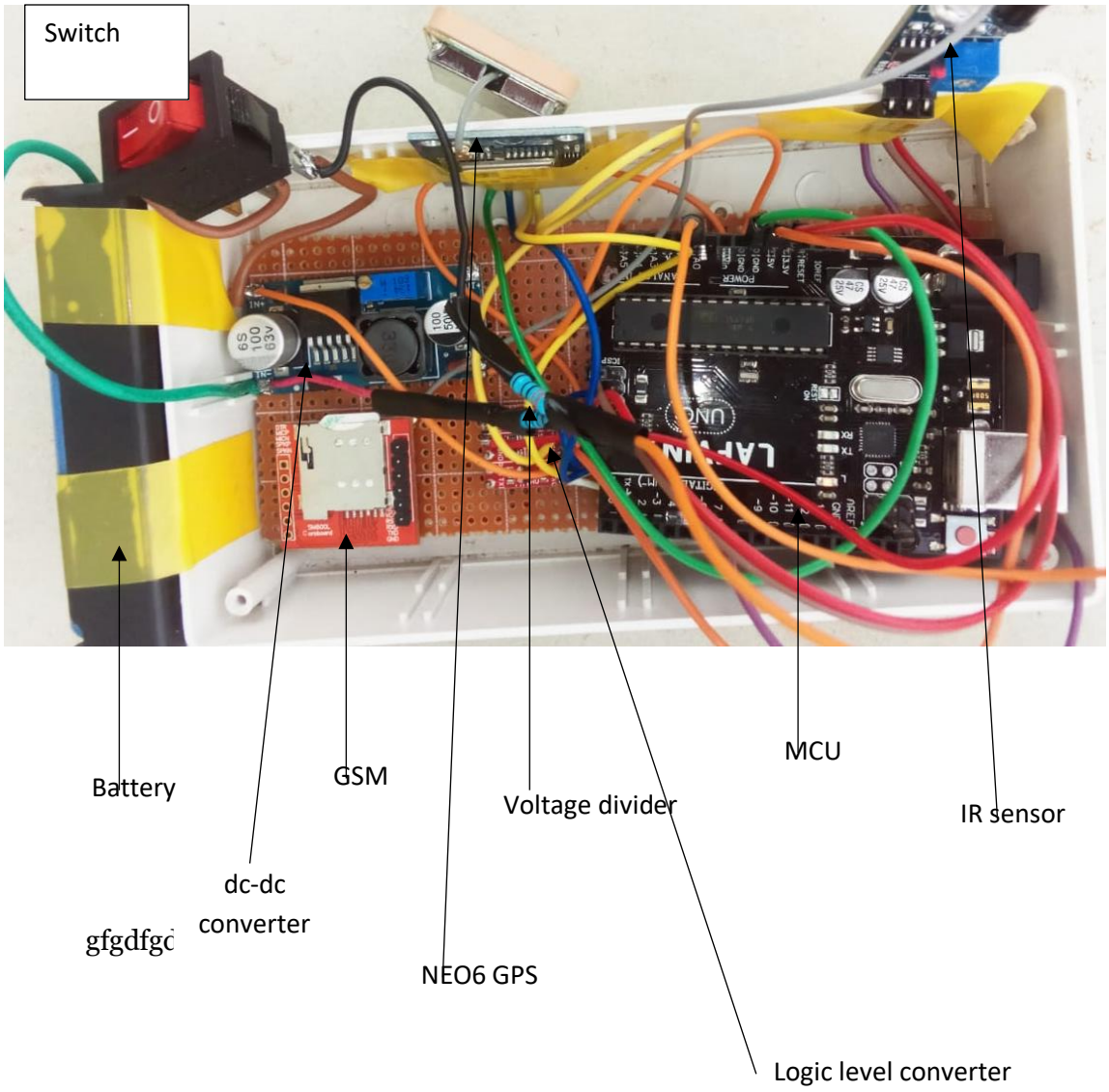


Figure 7. Completed prototype

The plastic casing was used to hold the assembled prototype together. Furthermore, some components were soldered on a PCB to reduce the number of wires required to run in the circuit. To ensure the GPS and GSM received the signals, the antennas were kept outside the plastic container.

4. Discussion

The battery voltage sensor recorded values that were less than 7.4 V as noted earlier. Since two 4.2V lithium batteries were connected in series, the maximum actual voltage would be 8.4V while the input to the ADC pin was 1.95 at full charge given the values of the resistances were in the ratio of 1:3.3. Thus, during testing the batteries had discharged hence they had lower voltages. To prevent deep discharge, an alert was sent when the battery voltage fell below 7.4 volts. This implies that each cell may have reached 3.7V which is the nominal voltage of Lithium-ion cells. Such voltage drop can be attributed by power consumption by the IoT system. More

specifically, the GSM draws a lot of current during data transmission which reduced the voltage significantly. This is in agreement with arguments of Yassin et al. (2020) that IoT systems require optimization both in hardware and software to reduce power consumption for asset tracking systems. Regarding the graphs of location coordinates, the value of zero meant that the GPS module had not connected to any satellites. This mostly occurred when the system was placed indoors where the GPS signal was obstructed by the walls of the building. Slight variations in the location coordinates even when the device was stationary implied that location determination using GPS has a certain degree of uncertainty. Findings of Meynecke and Liebsch (2021) agree with this by the fact that localization using GPS requires clear space between the GPS module and satellite signals. Although indoor localization using GPS and GSM may not be effective due to poor network coverage, the devices work well in outdoor conditions. As an asset is exposed to outdoor conditions during relocation, the GPS module will connect with satellites where the MCU will trigger an alert about location change. Therefore, the current device has advantage because of long range data transmission and remote access through server as GPS has a comparable location accuracy. The accuracy of 3m obtained in outdoor location is comparable to the 2.5 m accuracy achieved by Devlin and Kevin (2009). Overall, the device exhibited timely data transmission both to server and through SMS and is more ideal for monitoring non-powered assets that are located in outdoor spaces where signal reception is strong.

5. Conclusions

An IoT security system relying on GPS for asset location and GSM for SMS and server communication has been designed, implemented and tested. The system boasts an onboard method of measuring battery voltage, detecting when the casing has been opened and reporting the status of the system through GSM. The GSM module consumes more energy compared to the rest of the devices hence its usage can be leveraged by optimizing the embedded code. The device is found more ideal for monitoring non-powered assets that are kept in outdoor spaces given the conventional reliance of GPS on clear space for signal reception. This study concludes that IoT has the potential to change the asset security landscape by developing stand-alone devices that can monitor and report non-powered assets' location and status.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public commercial, or not-for-profit sectors.

The authors declare no competing interests.

References

Andreas, P., Kostas, P., Christos, S., Haoxiang, W., & Gupta (2018). Efficient IoT-based sensor BIG data collection–processing and analysis in smart buildings. *Future Generation Computer Systems*, *82*, 349-357.

Andrey, S., & Raffaele, G. (2019, November 9). *Powering IoT devices: Technologies and opportunities*. IoT IEEE.

Devlin, G. J., & McDonnell, K. (2009). Performance accuracy of real-time GPS asset tracking systems for timber haulage trucks travelling on both internal forest road and public road networks.

International Journal of Forest Engineering, *20*(1), 45-49. https://doi.org/10.1080/14942119.2009.10702575

Indira, R., Bhavya, G., Dheva, D. S., & Devaraj, R. (2019). IOT asset tracking system. *International Journal of Computer Science and Engineering*, ICFTESH, 45-50.

Meynecke, J.-O., Liebsch, N. (2021). Asset tracking whales — First deployment of a custom-made GPS/GSM suction cup tag on migrating humpback whales. *J. Mar. Sci. Eng.*, *9*, 597. https://doi.org/10.3390/jmse9060597

Minhaj, A. K., & Khaled, S. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.

Nirit, D., Ashutosh, M., Mukund, A., & Anirudh, J. (2019). Real time tracking and alert system for laptop through implementation of GPS, GSM, motion sensor and cloud services for antitheft purposes. *IEEE Xplore*, *4*(19), 978-1-7281-1253.

Smartrak (2020). Smartrak. (Smartrak) Retrieved March 21, 2021, from https://smartrak.com/non-powered-asset-tracking/.

Valente, F., & Neto, A. C. (2017). Intelligent steel inventory tracking with IoT / RFID. *2017 IEEE International Conference on RFID Technology & Application* (RFID-TA). Warsaw, Poland.

Yassin-Kassab, H., Rosu, M-C. (2020). An overview of own tracking wireless sensors with GSM-GPS features. *Advances in Technology Innovation*, *6*(1), 47-66.


C O A S