Remote Monitoring of Health Parameters Using Smart Walker

Harshit Mahapatra
Dept. of Computer Science
Aarhus University
Aarhus, Denmark
au608727@post.au.dk

Patrick Lewandowski
Dept. of Computer Science
Aarhus University
Aarhus, Denmark
au614714@post.au.dk

Tomas Manuel Rebelo Mota
Dept. of Computer Science
Aarhus University
Aarhus, Denmark
au614711@post.au.dk

I. Introduction

Recent advances in sensor technology have made it possible to embed sensors in everyday objects to collect data related to various parameters. With the advent of low power network technologies like LoRaWAN, it is possible to create a sensor network which requires little power and low maintenance.

Furthermore, current development in the field of machine learning and big data have made it possible to acquire valuable insight from the collected data and have thus made the acquisition of data even more lucrative.

Healthcare is a field of growing interest for this data collection, as the remote monitoring of patients not only allows us to reduce our response time for emergencies but also gives us valuable insights about the patient's health, which in turn leads to better diagnosis and insight about a disability or disease.

Our project is about building a smart walker which leverages the low power sensor technology of LoRaWAN, the decentralized computing of cloud and the power of data analysis to monitor and analyze the health parameters of it's user.

More concretely, we aim to build a walker consisting of an accelerometer, a GPS module, pulse, and pressure sensors. The accelerometer will allow us to track the usage statistics of the walker. GPS sensors will allow us to track the position and common usage area of walkers. The pulse and pressure sensors will be used to monitor the health of the walker's user.

These sensors are connected to an Arduino board that transmits the collected data through a low-cost, low-power and secure communication provided by LoRaWAN to a Raspberry PI that acts as a gateway, which is connected to an MQTT server. The MQTT server, in turn, is subscribed to by a web server which has web applications for analyzing and storing the data.

The walker will be streaming the data collected by the sensors to a central server belonging to the Municipality. This data is then used to analyze both the overall use of the walkers, information that is highly interesting for the manufacturing companies, and the over-time change of the health indicators in order to track the long-term progress of the user's well-being.

Since the infrastructure for LoRaWAN is considerably developed in Aarhus, we are confident it would be a good protocol to use for streaming data from walkers to a central server.

It should, however, be noted that the LoRaWAN protocol has low bandwidth and is thus not suitable for real-time monitoring in cases where the sensor data is large is size. To circumvent, this problem we aim to make our sensor node capable of transmitting data over GSM while keeping power usage in check. The minimum viable product of our project, however, is a LoRaWAN smart walker.

We aim to explore whether it is possible to determine the usage of walker remotely using accelerometer and GPS data. We also intend our walker to be a proof of concept of remote health monitoring system using LoRaWAN. Lastly, we would like to explore whether we can measure the overall health of a walker user using the collected data.

It should be noted that we will probably not get to the analysis point because our project intends to be the foundation for a larger scheme with the next steps including the analysis of collected data.

II. Related Work

A comprehensive survey on the application of the Internet of Things for healthcare was done by Islam et al. [?]. The paper presented the current IoT healthcare networks. It discussed the topology, architecture, and platform of the said networks. It also presented the current security models used in healthcare networks and proposed a novel security model for the same. Finally, the paper briefly presented some of the IoT healthcare technologies such as grid computing, big data, ambient intelligence, etc.

Alahmadi et al. [?] in their paper discussed in detail about the architecture of mobile e-health monitoring systems. They proposed a decentralized architecture, where the sensors are connected to a mobile device via Bluetooth, which in turn is connected to a server over the internet. They also presented a Wide Area Network architecture in which the mobile device is connected to a base station, which in turn is connected to a server over the internet. This server can then be accessed by the healthcare professionals to provide proper advice in case of unusual biosignals.

A survey on the LoRaWAN technology was presented by Silva et al. [?]. The paper presents the advantages of LoRaWAN over GSM architecture. This includes low power

consumption, low maintenance, cheap hardware, and well-defined security measures. It then also presents some of the disadvantages of LoRaWAN such as low bandwidth, slow transmission rate and lack of established infrastructure. It then presents the architecture of a typical LoRaWAN network consisting of sensor nodes, gateway, network server and web application. This is followed by a brief presentation of the two-layer security of LoRaWAN networks in the network and application layer respectively.

Aras et al. [?] in their paper present a summary of the security and vulnerabilities of the LoRa network. The paper analyzes the security risks present in the physical layer, network layer, join procedure and end gateways of LoRaWAN. The physical layer of LoRaWAN uses chip spread spectrum in which longer than usual transmission can either be corrupted or intercepted. In the network layer the payloads before and after encryption have the same length and thus can be used together with overflowing counters to restore the keystream. LoRaWAN uses two joining procedures Over The Air Activation (OTAA) and Activation By Personalization (ABP). The paper claims that while OTAA is secure, ABP's key can be compromised.

The paper also presents various possible attacks such as compromising the device and network keys via physical access, jamming using dedicated hardware, replay and wormhole attacks.

Another interesting paper about the security of LoRaWAN was presented by Tomasin et al. [?]. It presents a detailed analysis of attacks on the join procedure of LoRaWAN.

Ferdoush et al. [?] have done interesting work on the application of Wireless Personal Area Network (WPAN) for environment monitoring. They use Arduino Uno as their sensor node and the Raspberry Pi as their gateway. The Raspberry Pi itself acts as a hub containing the gateway application, database server, PHP web application, web server, and HTML web interface. This architecture fails to leverage the cloud infrastructure model.

Mdhaffar et al. [?] have used a hardware setup similar to Ferdoush but with LoRaWAN to monitor healthcare. They collected sensor data using Arduino and sent it to a Raspberry Pi acting as the gateway using LoRaWAN. The Pi then forwards the data to a network server which is connected to an application server. This is quite similar to our project's architecture. They collected data on blood pressure, glucose level and temperature and were able to successfully monitor the said data. They were also able to get a large coverage area with low power consumption.

Although several attempts have been made to create a smart walker, the most similar one to our project was done by Postolache et al. [?]. In their project they connected a MEMS accelerometer, Doppler radar and flexible force sensor to an Arduino fixed to a walker. The Arduino then sent the sensor data to an Android device via Bluetooth. The mobile device contained an application to monitor and analyze the data. This approach is significantly different from ours, as our project relies on the cloud for monitoring and analysis of collected data. Furthermore, in our project, the walker is connected to a LoRaWAN gateway directly as we do not expect the walker users to always carry a smartphone, and we aim to achieve remote monitoring with a range far greater than that of Bluetooth.

Banaee et al. [?] in their paper present the various use cases for data collected through health monitoring systems. They propose that the data can be used for anomaly detection, decision making and sending an alarm to authorities in case of emergencies. They further discuss the architecture for mining the said and the use of various popular machine learning and statistical algorithms for the same. They also present a brief summary of the various types of acquired data and their properties.

Gondalia et al. [?] recently presented an interesting paper on the remote health tracking of soldiers in battlefield using IoT. They propose an architecture in which each soldier has a sensor node which is connected to a base node belonging to squadron leader. The connection between the base node and sensor node is via Wireless Body Area Sensor Networks (WBASN). The squadron leader's node, in turn, is connected to a control room via LoRaWAN. The control room contains access to the cloud which is then used for storage and analysis. They further propose that the collected data can be fed to a K-Means clustering algorithm to classify sensor status at different events such as sitting, walking, sleeping, etc.

REFERENCES