IoT agriculture system based on LoRaWAN

Danco Davcev, Kosta Mitreski, Stefan Trajkovic, Viktor Nikolovski, Nikola Koteli
Laboratory of Eco-informatics
UKIM, Faculty of Computer Science and Engineering
Skopje, Macedonia
{danco.davcev, kosta.mitreski}@finki.ukim.mk, {trj.stefan, viktor.nikolovski2, nikola.koteli}@gmail.com

***Abstract*— In the last years, besides the implementation in the smart city applications, IoT has also found significant place in the agricultural and food production process. In the paper we present an innovative, power efficient and highly scalable IoT agricultural system. This system is based on LoRaWAN network for long range and low power consumption data transmission from the sensor nodes to the cloud services. Our system of cloud services is highly scalable and utilizes data stream for analytics purposes. In our case study we show some preliminary results for grape farm.**

Keywords—Internet of Things (IoT); agriculture; LoRaWAN; data streams

I. INTRODUCTION

The recent advancement of the Internet of Things (IoT) in precision agriculture allows us to improve the overall agriculture management. The IoT is perfect match for precision agriculture due to its highly interoperable, scalable, pervasive and open nature. There are a lot of IoT derived technologies and all of them bring various benefits including reducing the risk of vendor lock-in, adopting machinery and better sensing/automation systems. Being motivated by the above benefits and potentials of IoT applied in precision agriculture, considering the non-existence of complete reliable well-established and standard solution yet, we designed our model. In this paper we will propose a solution that provides easy and inexpensive network scalability, while maintaining the possibility of placing sensor nodes at a great distance from the base station which reduces the complexity and the cost of the overall network. Our model architecture is highly customizable and provides data analytics solution, enables large-scale data processing on real time observation streams of data coming from variety of sources, such as sensory network, weather forecasting services, etc. In our solution we use LoRaWAN LPWAN (Low-Power Wide-Area Network) as a transmission protocol that is designed by the LoRa Alliance and meets the need of the IoT services. It has easy implementation, out of the box security layer and ensures maximum coverage of hundreds of square meters. It requires minimal maintenance with low power consumption which makes it ideal for large number of sensors. All of above makes LoRaWAN perfect for the Internet of Things (IoT) in various fields and especially in agriculture, where the extension of the fields and their distribution across vast areas require an ad hoc protocol.

This paper is organized as follows. In section II we give an overview of the LoRaWAN network and its benefits in agricultural application. In section III, we present our system's cloud services architecture. Section IV describes the need of security of IoT services and examines LoRaWAN's security and protection mechanisms. Section V presents a case study for demonstration purposes. Finally section VI concludes our paper and presents the future work.

II. LORAWAN PROTOCOL AND ITS IMPLEMENTATION IN OUR SYSTEM

In this section we present the overall system construction, its components and their interconnection. This system was designed for agricultural purposes where there is a need for lots of sensors that generate streams of data which needed to be analyzed. Besides the main purpose for this system to be used in agriculture, it can easily be applied to other social and production processes that have similar needs.

This system consists of LoRaWAN network for data transmission between the sensor nodes and backend cloud services. Data from the sensor nodes is transmitted to the LoRaWAN base stations and from there to The Things Network (TTN) platform [1]. The TTN is an open platform for registration of LoRaWAN devices (sensor nodes) and base stations (gateways). It has an implementation of all needed backend services for LoRaWAN base station operation i.e. all functions needed for the data and the transport layer, along with all required security layers. The TTN platform is responsible for collection, formatting and rerouting the data from the sensor nodes to our cloud services, while maintaining data integrity and security. After the TTN platform receives message from the base stations, it formats with our specified custom formatter and routes the formatted message to our cloud services, which are responsible for data storage, visualization and analytics. In Fig. 1 we can see the diagram of the IoT system components, its relations and description.

A. Overview of LoRaWAN

LoRaWAN network was specifically designed for IoT applications with the purpose of connecting thousands of sensors, modules and appliances over a large network. It is a network protocol that is mainly used in Smart City applications where there is a need for wide network coverage, but is starting to be implemented in almost all other social aspects where its properties suits their needs. Many countries have started national wide or major cities implementation of LoRaWAN. At

978-1-5386-1066-4/18/$31.00

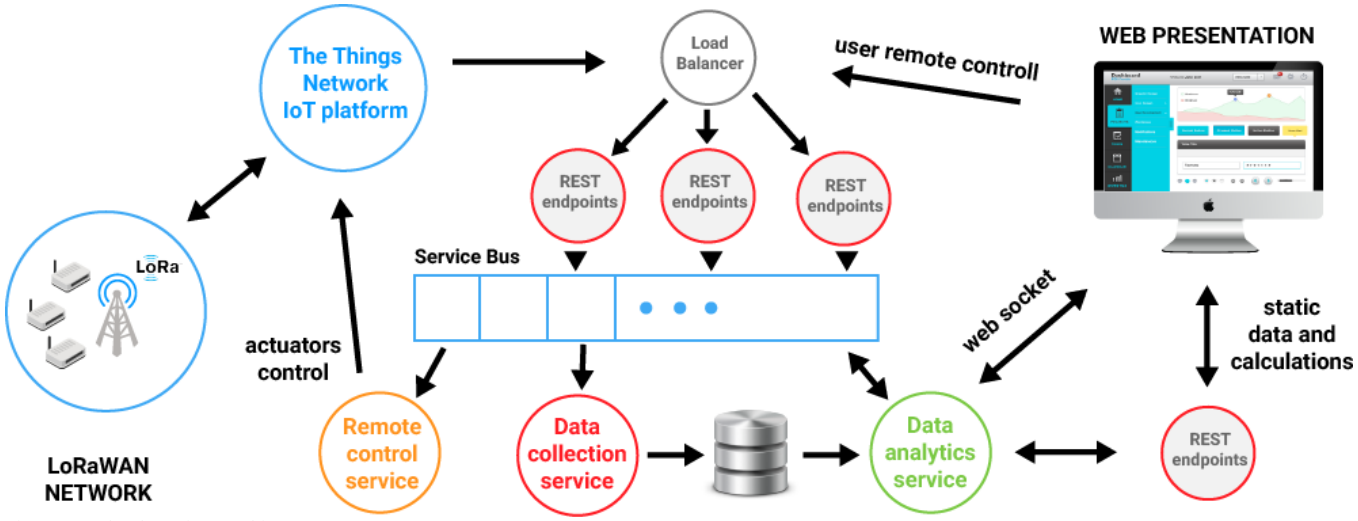

Figure 1. Cloud services architecture

the end of 2016, Netherlands and Belgium have implemented the LoRaWAN nationwide coverage, while other countries like France, Germany, Italy, and Switzerland are expected to implement full nationwide coverage of LoRaWAN by the end of 2017 and 2018 [2].

LoRaWAN differs from other protocols suited for IoT applications such as ZigBee or NRF in many categories such as network topology, data transmission range and throughput. LoRa that is the physical layer of the LoRaWAN is based on CSS (Chirp Spread Spectrum) modulation, which maintains the same low power characteristics as FSK modulation but significantly increases the communication range. Transmission range highly depends on the environment and its obstructions, but LoRa and LoRaWAN have a link budget (measured in dB) greater than any other standardized communication technology [3]. LoRaWAN can achieve data transmission range from 2-5 km in urban areas and to 15 km in suburban areas [4]. The CSS modulation, besides the great transmission ranges, it also has low power characteristics that imply that LoRaWAN can be used in applications where there is no external power supply. LoRaWAN applications can run on battery power supply for years. One disadvantage of LoRaWAN network is its low data rates i.e. throughput, which prevents this protocol to be used in real time and high throughput applications such as VoIP and video transmission.

B. Usage of LoRaWAN network in agricultural IoT systems

Usage of LoRaWAN protocol is rapidly growing as well as its implementation in many social and production processes. Besides the main target of LoRa Alliance to implement the LoRaWAN in Smart City applications, this protocol has great potential to be implemented in the food production and agricultural IoT applications. Its long range data transmission capability gives the opportunity to cover huge areas (fields) and to setup sensor nodes on great distance up to 15km in the line of site with the base station. LoRaWAN's star of stars topology in comparison with ZigBee's mesh network topology does not need additional modules to act as routers, which decreases the overall cost and complexity of the network. Besides the long range transmission and the better suited topology for agricultural purposes, LoRaWAN has also low power consumption, which makes it perfect for battery powered applications. For agricultural application, this is perfect because it removes the need of the external power supply in the fields, instead the sensors can run on battery power supply for years.

In comparison to the new emerging technologies such as NB-IoT, which targets the same scope of devices and applications as LoRaWAN, the latter has the upper hand when it comes to the price and privacy of the system. NB-IoT uses licensed frequency bands and is governed by the big telecom companies, while LoRaWAN uses unlicensed frequency bands and the backend server that the LoRaWAN base station is dependent on, can be private (not governed by other companies). According to [3] the 95%-tile uplink failure rate for outdoor users is below 5% for both technologies. LoRa struggles to provide sufficient indoor coverage and capacity. However, in this study we consider only outdoor users. In our future work we also plan to investigate the energy consumption of both technologies.

There are many use cases in agricultural and food production that LoRaWAN can be applied to. In our innovative approach the closed-loop control for sensing and actuation can be seen in Fig. 1. LoRaWAN can be used to manage sensor nodes that measure environmental parameters such as air temperature, humidity, soil moisture, etc. Additionally it can be used to operate all kinds of actuators (e.g. automatic sprinkler valve for irrigation purposes or automatic poultry feeder). It can also be used in applications such as measuring cattle's temperature in farms or following their position with GPS sensors [5].

III. Overview of our system's architecture

Our system is constructed from three services. The data collection service has the responsibility of storing the incoming data from the TTN platform, while data analytics

service operates on the stored and streams of data with predefined prediction models and data mining algorithms. The data analytics service is also responsible for filtering and formatting the data that is requested by the user. The remote control service has the purpose of sending commands to the actuators via the TTN platform back to the LoRaWAN network (see Fig. 1).

LoRaWAN nodes in our system are separated into two groups (collectors and executors). Collectors are nodes equipped with variety of sensors that collect and transmit data to our cloud services, while executors are nodes equipped with actuators for controlling the automatic sprinklers.

The whole architecture is flexible, scalable and extensible. It is not dependent on any platform and can easily be extended with other services and IoT network types. Its performance can be increased with just spawning new instances of the cloud services (e.g. if the analytics service is overloaded, we can instantiate new instance from the service to share the load).

A. *Data collection service architecture*

This service collects and stores data using event sourcing pattern. The TTN platform routes the data to our REST endpoints which only publish the message to the queue (service bus). Data collection service as consumer reads the messages from the message queue, formats and stores the data in database.

B. *Analytics service architecture*

The data analytics service purpose is to extract knowledge from the raw data that was collected from the sensors, or to send a command via remote control service to the actuators connected on the network. This service has three access points. First access point is used for requesting some static data or calculation via the dedicated REST API to this service. The second access point is to subscribe to a data stream, coming from the sensor nodes, via web socket. The data stream analytics is generated on the fly. The third access point is through the service bus which is dedicated to the incoming data streams from the TTN platform.

C. *Remote control service architecture*

This service responsibility is to manage and control the executor nodes that are connected to the network. It is also designed like a consumer on the service bus (message queue) similar to the data collection service. Remote control service receives the control messages from the queue which may be sent by the data analytics service or the user from the web presentation. After the message was received, remote control service sends the desired command to the TTN platform to be sent to the desired executor node.

IV. Security of our System

It is extremely important for IoT services to incorporate a security layer. Without this they can face a variety of attacks that can cause severe damage to the production process. Lack of availability (DoS), unauthenticated data or loss of data integrity can cause false data analysis reports, loss of product quality, as well as disturb the working process of actuators and possibly damage the plants.

The security protection of our system is consisted of two parts. The first part represent the collection of data from sensors via the LoRaWAN network and the TTN platform to the cloud. LoRaWAN utilizes two layers of security: one for the network and one for the application. These layers prevent message origin authentication, data integrity, message replay protection and encryption. Additionally LoRaWAN implements end-to-end encryption for application payloads exchanged between the end-devices and cloud services using AES encryption. For the list of most popular attacks, like node replication, base station cloning and selective forwarding, eeavesdropping and bit-flipping, and how LoRaWAN ensures safety and security from these attacks see for example [6], [7].

The second part of security protection of our system is connected with cloud services subject to our future work.

V. Case Study

As a proof of concept we have installed a prototype of our system on vineyard field to collect air temperature and

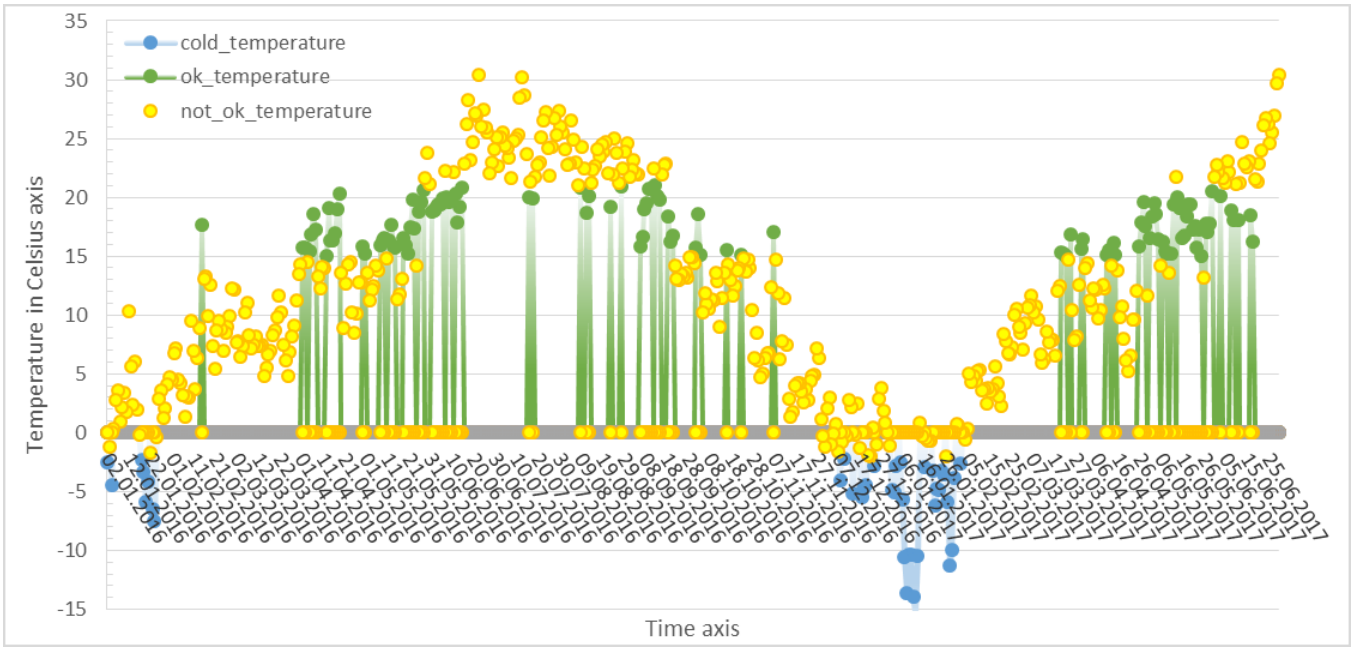

Figure 2. Sensor temperature data chart

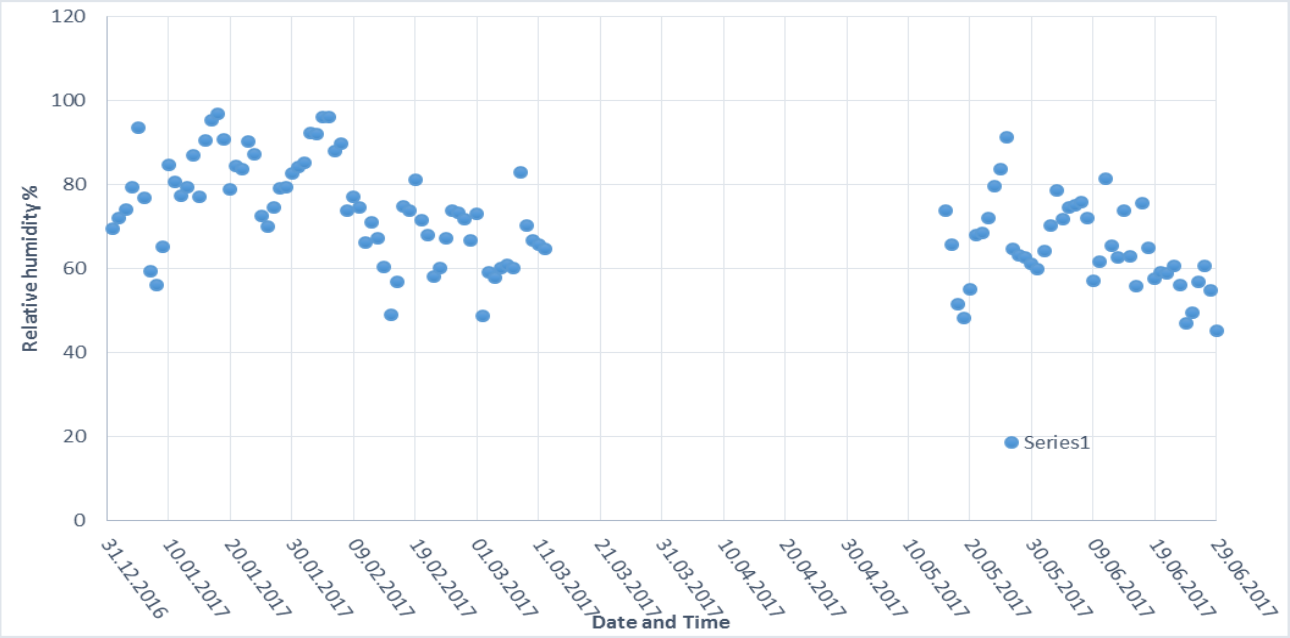

Figure 3. Relative humidity data chart

humidity, as well as leaf wetness and soil moisture readings. The prototype consists of three collector nodes and one executor nodes which are positioned in 1km radius from the base station. Based on our soil moisture and leaf wetness measurements, the analytics service makes a decision if the irrigation system needs to be turned on or off. After the decision is made, the remote control service (which controls the executor node installed in our system), turns on/off the watering pump in the field.

In Fig. 2 you can see the measurements of air temperature (ºC) taken in time period from 01.01.2016 till 01.07.2017. The measurements can be in range that is preferred for optimal quality assurance in producing grape for wine, but frequently they can fall in range that is not optimal or even in range that is harmful for the production. The green colored temperatures in this graph are the ones that are preferred for optimal quality assurance in producing grape for wine and the yellow ones are the temperature values that are not optimal ones. The blue ones are the temperatures that are harmful and should be avoided. From the data collected during this case study only 21.16% is in the optimal range of values and only 7.21% is in the harmful range.

In addition to the temperature readings, in Fig. 3 we present a chart of relative humidity measurements. These data could be useful for various analyses connected to the quality of grape, subject to our future work.

VI. Conclusion

In this paper we presented a model of IoT agricultural system that utilizes LoRaWAN protocol for data transmission from the sensor nodes to our cloud services and The Things Network platform that implements LoRaWAN's backend services. We designed a system that is flexible and extensible in terms of addition of new services as well as integration with other IoT platforms. It is also horizontally scalable which means that we can increase its performance with just spawning new server instances.

For the future work we plan to extend our data analytics service with more prediction models and data mining algorithms.

References

[1] The Things Network – IoT platform, https://www.thethingsnetwork.org

[2] LoRaWAN across the globe: LoRa Internet of Things networks overview, https://www.i-scoop.eu/internet-of-things-guide/iot-network-lora-lorawan, (last access July 10, 2017)

[3] LoRA aliance, https://docs.wixstatic.com/ugd/eccc1a_acef1a0dbad649bc894a372cf8ff6beb.pdf, (last access July 12, 2017)

[4] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J.Melià-Seguí, T. Watteyne, Understanding the Limits of LoRaWAN, IEEE Communication Magazine Vol. 55, Iss. 9, pp. 34-40, 2017

[5] B.Belini, A.Arnaud, A 5mA Wireless Platform for Cattle Heat Detection, 2017 IEEE 8th Latin American Symposium on Circuits & Systems (LASCAS), pp. 1-4, 2017.

[6] Md Husamuddin, M. Qayyum, Internet of Things: A Study on Security and Privacy Threats, IEEE 2nd International Conference on Anti-Cyber Crimes (ICACC), pp. 93-97, 2017.

[7] J.W. Lee1, D.Y. Hwang1, J.H. Park1, and K.H. Kim, Risk Analysis and Countermeasure for Bit-Flipping Attack in LoRaWAN, IEEE International Conference on Information Networking (ICOIN), pp. 549-551, 2017.