Low-power Wide-Area Networks: A Comparative Analysis Between LoRaWAN and NB-IoT

Chiara Buratti*, **Konstantin Mikhaylov**†, **Riccardo Marini***, **Roberto Verdone***

*Università di Bologna, †University of Oulu

Abstract: *Low Power Wide Area Networks are becoming the most important enabler for the Internet of Things (IoT) connectivity. Application domains like smart cities, smart agriculture, intelligent logistics and transportation, require communication technologies that combine long transmission ranges, energy efficiency and low infrastructure costs. Recent and future trends make LoRaWAN and 4G/NB-IoT the main drivers of IoT business. In this contribution we briefly discuss the main features of the two technologies, analyzing some important Key Performance Indicators. The presented results have been obtained analytically, via simulations and experiments developed at the University of Bologna via testbeds, that are currently under use to verify different IoT applications and demonstrate their feasibility.*

1 Introduction

The proliferation of embedded systems, wireless technologies, and Internet protocols have enabled the Internet of Things (IoT), to bridge the gap between the virtual and physical world by enabling the monitoring and control of the physical world by data processing systems. A large variety of communication technologies has gradually emerged, reflecting a large diversity of application domains and requirements. Some of these technologies are prevalent in a specific application domain, such as Bluetooth Low Energy in Personal Area Networks [1], and Zigbee in Home Automation systems [2]. Others, like Wi-Fi Low Power, Low Power Wide Area Networks (LPWAN) [3], and cellular communications, such as the 3GPP Long Term Evolution for Machines (LTE-M) and Narrowband IoT (NB-IoT), have a much broader scope. In addition, this landscape is constantly and rapidly evolving, with new technologies being regularly proposed, and with existing ones proliferating into new application domains. In this Chapter, we focus on LoRa and NB-IoT, presenting their main features and characteristics, and some examples of achievable results via analyzing a set of selected generic Key Performance Indicators (KPIs). The Chapter is organized as follows: Section 2 deals with the LoRa technology, while Section 3 reports NB-IoT technology. Finally, Section 4 compares the two solutions and reports drawn conclusions.

LoRaWAN: current status and research directions

Lorenzo Vangelista, Andrea Zanella, Michele Zorzi

Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione

Abstract: *Among the different Low-Power Wide Area Network (LPWAN) technologies, Long-Range Wide Area Network (LoRaWAN) stands out for flexibility, performance, and open specifications, characteristics that have been attracting interest from both the industrial and scientific communities. LoRaWAN, indeed, features a number of tuneable network parameters that, in principle, make it possible to better configure the system according to the specific context, thus improving energy efficiency, fairness, and capacity. In this chapter, we discuss the main characteristics of the LoRaWAN technology and present some results that shed light on the effect of different parameter settings in some illustrative scenarios. Furthermore, we illustrate the most recent features introduced by the LoRaWAN specifications and possible future developments of the technology.*

1 Introduction

As stated in [1], the Internet of Things (IoT) paradigm underpins the place-and-play concept, according to which the end devices, i.e., the "things," just need to be placed where they are needed, and are automatically and seamlessly connected to the rest of the (cyber-physical) world. Cellular networks, with their world-wide established footprint, are the ideal candidates to provide such a service, which is indeed the target of the NB-IoT standard. On the other hand, the signaling and control traffic of NB-IoT, although optimized for sporadic machine-type communications, may become the bottleneck of the system [2].

In the meantime, a number of Low Power Wide Area Network (LPWAN) technologies have appeared in the market, in an attempt to fill this gap. Such technologies are characterized by long-range links (in the orders of kilometers), and typically have a simple star-shaped network topology, where the end nodes are directly connected to a gateway that, in turn, provides legacy IP connectivity with other networks or with the public Internet. Moreover, LPWAN implements robust modulations that guarantee excellent energy-efficiency and coverage range, at the cost of very low bitrates. Finally, most LPWANs operate on unlicensed radio bands, thus avoiding the huge royalties to access reserved frequencies, and adopt uncoordinated access schemes, which make it possible to simplify the hardware and reduce the manufacturing costs and the energy consumption.

LoRaWAN is an LPWAN technology that has been gaining a considerable share of the market in the last years, thanks to some interesting features, such as the chirp modulation used at the PHY layer that allows for long-range, robust communications, with

LoRaWAN: a Deep Dive in a Large Scale Deployment and in Radio Access Optimization Strategies

Giuseppe Bianchi[1,2], Francesca Cuomo[1,3], Domenico Garlisi[1,4], Patrizio Pisani[5] and Ilenia Tinnirello[1,4]

[1]Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT)

[2]University of Roma "Tor Vergata", Italy

[3]University of Rome "La Sapienza", Italy

[4]University of Palermo, Italy

[5]UNIDATA S.P.A., Italy

Abstract: *Low-Power Wide Area Networks (LPWANs) represent one key enabling technology for the Internet of Things (IoT). LPWAN capabilities are long range, deep penetration, and ultra-low power consumption. Among the LPWAN emerging technologies, LoRaWAN (Long Range Wide Area Network) is a successful network infrastructure for ultra-low power device communication based on Long Range (LoRa) modulation, patented by Semtech. LoRa exploits free ISM bands and has been conceived for low power consumption (life device up to 10 years) and low data rate applications. LoRaWAN guaranteed easy deployment, indeed a single gateway can cover up to several kilometers. In this chapter, we present and discuss the lessons learned from a real-world LoRaWAN deployment carried out by the UNIDATA regional operator in a large terrestrial area. After presenting the basic LoRa modulation features, we discuss the LoRaWAN architecture and how the network performance are affected by radio access settings and the gateways deployment. We then present the platform designed for data collection and analytics and some statistics gathered in the first year of operation. We then discuss different strategies able to optimize the global network performance. To this aim: i) we define an algorithm to optimize LoRa Data Rate allocation along the nodes, in single and multi gateway scenarios; ii) we propose a methodology to process LoRaWAN packets and perform devices profiling; iii) we propose a methodology to predict the radio space utilization.*

1 Introduction

IoT devices and applications are playing a crucial role in the human everyday life, they are used to deploy smart environments where people live. Thanks to the IoT paradigm homes, buildings, and industries are connected together to apply the smart cities concept. Providing intelligence to these environments means enabling a broad set of operations, such as collecting data, triggering alarms, and reconfiguring smart objects. According to

Wide Area Transmission Technologies for IoT

Andrea Abrardo, Giacomo Peruzzi, Alessandro Pozzebon

Department of Information Engineering and Mathematics

University of Siena, Siena, Italy

Abstract: *In this paper, the state of the art of Wide Area transmission technologies for IoT along with their application scenarios and requirements is discussed. In particular, the paper considers the main existing technologies, both license-based (i.e., cellular) and license-free (e.g., LoRaWAN and other Sub-GHz technologies). Then, future trends are analyzed, discussing in particular the advantages expected to be brought by the introduction of the upcoming 5G cellular technology in the Internet of Things (IoT) context, with the possibility of exploiting the edge computing paradigm and the slicing concept. In the second part of the paper, the advantages and drawbacks of the two main technological frameworks (e.g., licensed and license-free) are examined according to the different system requirements. Finally, two specific use cases are presented which are currently enabled by LoRa modulation.*

1 Introduction

The Internet of Things (IoT) has become a promising, valuable and robust paradigm throughout the recent years [1]. Indeed, the IoT is a hot topic nowadays either from a research point of view and from an application perspective as well: from smart cities to environmental monitoring, from home automation to the migration towards the Industry 4.0 domain, from healthcare to smart agriculture, from intelligent transportation systems to autonomous vehicles. All these scenarios are characterized by the presence of dumb objects of broad purpose (e.g., sensor nodes, vehicles, domestic appliances, industrial machineries and so on) with Internet connectivity and computational capabilities so as it is possible to control them and, at the same time, to receive notices from them.

Ideally, IoT devices should be designed to satisfy the following characteristics: high coverage, low cost and low power. Sadly, though, a simultaneous achievement of these features is tough or nearly impossible, hence a trade-off has to be reached in most of the cases. The application scenario determines which of the aforesaid features should be fulfilled the most: a pervasive monitoring infrastructure requires cheap sensor nodes, real time monitoring needs high coverage besides a relevant amount of data to be streamed while for devices relying only on batteries as source of energy to be as low power as possible is mandatory.

The Mobility Report issued by Ericsson in June 2019 [2] foresees that wide-area IoT devices, numbering at about one billion and representing a little more than one-tenth of all IoT deployments today, will grow consistently to reach 4.5 billion devices by 2024.

Enabling technologies for the Internet of Vehicles: standards, research and open challenges

Claudia Campolo, Antonella Molinaro

University Mediterranea of Reggio Calabria

Abstract: *The recent technological advancements in the field of sensing, automation, computing and communication technologies for vehicles are revolutionizing transportation systems on a global scale, while fostering large investments in the automotive market. Vehicles, as multi-faceted objects equipped with on board sensors like cameras, radars, positioning receivers, and with storage and processing capabilities, are becoming quite rightly elements of the Internet of Things (IoT). The Internet of Vehicles (IoV) ecosystem represents a prominent instantiation of the IoT, aimed at enabling smart, efficient and green traffic management, intelligent vehicle control, safe, comfortable and pleasant driving and traveling experience. The first step for the IoV is to make vehicles connected and able to interact with nearby/remote people and objects, and among each other, thanks to vehicle-to-everything (V2X) communication technologies. By leveraging efficient air interfaces, a wide range of allocated frequencies, advanced transceivers, multiple radio access technologies, as well as cutting-edge network softwarization principles, fifth generation (5G) systems intend to guarantee ultra-low latency, ultra-high reliability, and high-data rate V2X connectivity. Further promising paradigms and technologies in the IoT and future Internet research arena can contribute to address the needs of vehicular applications. This chapter will describe the IoV status quo, by analyzing the V2X application requirements and the main enabling communications technologies; research challenges and opportunities related to edge computing, virtualization, artificial intelligence, and other IoV enablers will also be part of this chapter.*

1 Introduction

Nowadays, modern vehicles carry on board high-speed processors, high-capacity memory storage, and a multitude of sensors, ranging from side collision radars to global positioning system (GPS) and cameras, which monitor the internal state of the vehicle and its close surroundings. Thanks to on board radio transceivers, vehicles can autonomously exchange their kinematics parameters, sensed data, and driving intentions with neighboring vehicles and coordinate their maneuvers in (semi-)autonomous driving settings, or they can send diagnostics and maintenance information to the cloud servers of manufacturers. Vehicles can as well provide navigation services and other traffic telematics applications, along with on-demand video streaming and online Internet access to passengers. In short, a vehicle, being equipped with vehicle-to-everything (V2X) connectivity, can exchange data with other communicating entities in its surrounding and becomes an essential element of the Internet of Vehicles (IoV) vision, one of the most prominent instantiation of the Internet of Things (IoT).

A Machine Learning Based Non-Orthogonal Multiple Access Scheme for IoT Communications

authors Romano Fantacci, and Benedetta Picano

Università degli Studi di Firenze

Abstract: *The ever increasing diffusion of the IoT devices, able to interact and exchange data with the surrounding environment, is exponentially growing, giving rise to ubiquitous and intelligent ecosystems capable of data gathering and usually requiring low latency processing of time. As a consequence, efficient multiple access schemes have to be identified to handle a usual massive access of IoT devices to a local computation node according to the emerging edge computing paradigm to lower latency and network congestion. This chapter deals with the application of a machine learning technique, specifically an echo state (ESN) machine learning framework is considered. A key challenge in our problem formulation is that we assume that our ESN has not any a priori information on the number and behavior of IoT devices, i.e., on when to transmit and when not to. The goal of the considered ESN is to perform an effective channel access strategy for a sigle carrier two power levels non-orthogonal multiple access (NOMA) scheme with the aim at maximizing the sum throughput and minimizing the mean packet access delay among all the IoT devices. Performance comparisons with a basic, i.e., without resorting to the use of a machine learning approach, NOMA scheme are presented in order to highlight the advantages of the proposed solution. In addition to this, simulation results are also provided to validate the obtained analytical predictions.*

1 Introduction

The unexpected growth of the internet of things (IoT) applications and the forthcoming fifth generation (5G) has opened the door to an unprecedented connectivity demand from smart devices [1, 2]. Recently, with the advent of the promising edge computing paradigm, computation and data storage is moved close to the end-devices, limiting latency and network congestion. In such a landscape, IoTs channel access schemes represent a crucial issue in the network resource management. In this regards, the improvement of the random access techniques have appeared as an attractive solution to make possible IoT devices communications with a reduced signaling overhead and high spectral efficiency. Towards this end, in 5G and beyond 5G cellular communication systems, the use of non-orthogonal multiple access (NOMA) schemes has emerged as a promising technique to enhance throughput performance and improve the spectral efficiency. The basic principle of NOMA is to allow a simultaneous network access to multiple IoT devices over same radio resources with a low inter-IoT device interference.

In particular, NOMA superposes the different IoT devices signals in the power domain and, on the basis of the use of the successive interference cancellation (SIC) method at

Resources virtualization and task offloading towards the Edge in the IoT

Giovanni Merlino[1] **and Virginia Pilloni**[2]

[1] Department of Engineering, University of Messina, Italy
CINI, Smart Cities and Communities Lab, Research Unit of Messina, Italy
gmerlino@unime.it

[2] Department of Electrical and Electronic Engineering, University of Cagliari, Italy
CNIT, Research Unit of Cagliari, Italy
virginia.pilloni@unica.it

Abstract: *A significant role in the Internet of Things (IoT) will be played by mobile and low-cost devices, able to autonomously orchestrate workloads and share resources to meet their assigned application requirements. To increase efficiency, a recent trend promotes pushing computation from the remote Cloud as close to data sources as possible: this is the concept behind the Fog and Edge computing paradigms. Accordingly, distributed orchestration of node-hosted resources, so as to implement intelligent and fair allocation mechanisms, ensure the achievement of better performance at a lower network latency. Focusing on the aforementioned scenario, this Chapter presents a middleware architecture that relies on equipping co-located smart Edge and Fog devices with agents that virtualize real objects' features, resources and services. Thanks to an appropriate and fine-grained assessment of different combinations of offloading patterns, the middleware allows for a flexible and dynamic binding of the requested application workload to the physical IoT resources, in other terms an environment suitable for workload engineering.*

1 Introduction

The age of post-Clouds is already here, where unprecedented volume and variety of data are generated by things at the edge of networks, and many applications are being deployed on the edge networks to consume these Internet of Things (IoT) data. Some of the applications may require very short response times, some may convey personal data, and others may generate vast amounts of data. Cloud-based service models alone are not suitable for these applications.

Novel challenges are surfacing for advanced IoT services, also stemming from recent data production/consumption - and mobility - patterns, such as strict latency, constrained network bandwidth, constrained devices, uninterrupted services with intermittent connectivity, privacy and security due to the IoT environmental changes.

To address such challenges, the integration of Edge computing and IoT has emerged as a promising solution, often describing Fog computing as a paradigm to advance and support analytics [1].

Albeit, hidden behind that, lies the assumption that moving data closer to the site of its processing provides a definitive answer to most aforementioned issues. Whereas a

Security and privacy in the IoT: how to enforce standard communication technologies with efficient and flexible mechanisms

Antonio Suriano, Domenico Striccoli, Giuseppe Piro, Antonio Antenore, Gennaro Boggia

DEI, Politecnico di Bari. Via Orabona 4, Bari, Italy

CNIT, Consorzio Nazionale Interuniversitario per le Telecomunicazioni

Abstract: *The revolutionary Internet of Things paradigm successfully enabled the interaction among smart objects pervasively diffused across the Internet. From the beginning, communication technologies and open standards already provided baseline techniques able to offer security and privacy, also in constrained environments. But, while data confidentiality and data integrity were immediately tackled with robust cryptosystems, authentication and key management have been frequently covered with superficiality. Not only: fine-grained authorization and anomaly and intrusion detection services have been generally ignored in most cases. As a consequence, the worldwide scientific community dedicated a high attention to the design, the implementation, and the evaluation of new approaches addressing these open issues, while taking care about the new requirements characterizing the emerging Internet of Things scenarios and the related security risks and threats. This contribution starts by providing a new set of Internet of Things-oriented definitions of security services and highlights the impact that their implementation may have on the behavior of standardized communication protocols (i.e., computational complexity in constrained environments, energy consumption, and so on). Then, it presents some interesting approaches emerged in the recent scientific literature, addressing the uncovered security services. In summary, they include: key management protocols based on Implicit Certificates and Blockchain, Attribute-Based Access Control in multi-domain and multi-authority ecosystems, anomaly and intrusion detection mechanisms based on machine learning.*

1 Introduction

The Internet of Things (IoT) is an emerging and promising technology which tends to revolutionize the global world through connected physical objects, that can be fruitfully employed to enhance the quality of everyday life. For this reason, IoT is massively present in several application scenarios, including health and environmental monitoring, home automation, smart mobility, industry applications, etc. [1]. The wide variety of public and private environments where IoT devices are employed, together with the evergrowing number of connected devices, unavoidably poses critical security concerns, in terms of privacy, authentication (AuthN) and recovery from attacks, that need to be effectively

The Social Internet of Things: a Survey

Luigi Atzori*, Antonio Iera, Giacomo Morabito*****

*UdR CNIT of Cagliari, University of Cagliari
piazza d'Armi, 09123 Cagliari, Italy
email: l.atzori@diee.unica.it

**UdR CNIT of Cosenza, University of Calabria
DIMES- Via Pietro Bucci, 87036, Arcavacata di Rende (CS), Italy
email: antonio.iera@dimes.unical.it

***UdR CNIT of Catania, University of Catania
DIEEI - V.le A. Doria 6, 95125 Catania, Italy
email: giacomo.morabito@unict.it

Abstract: *The Social Internet of Things represents a distinctive paradigm for the realization of IoT solutions which relies on the integration of social networking technologies with machine-to-machine communications. Accordingly, objects are capable of interacting in a social way with external services to improve the efficiency and the trust in the communications. As a result, a social network involving objects, services and humans is created, which supports the social network nodes communications and the deployment of IoT applications. Whereas these are the major features, not all the research groups that work in this area converge on the same vision. In this article, we discuss the different views to highlight the common features and understand the rationales behind each view. We then present the major technologies involved in the implementation of this paradigm and the applications that are enabled. The paper concludes discussing the current challenges and the future directions.*

1. Introduction

The number of objects that are reachable over the Internet is now close to 10 billion and this number is increasing very fast [1]. These devices produce a huge amount of data and provide a remarkable number of services which need to be mashed up and interconnected to extract the real value for the benefit of the society. This can be achieved through centralized approaches, where

Software Defined Fog/Edge Networking for Internet of Vehicles: a Services-Oriented Reference Architecture

Michele Bonanni, Francesco Chiti and Romano Fantacci

Department of Information Engineering

University of Florence, via di Santa Marta 3, I-50139 ITALY

Abstract: *This chapter addresses an innovative architectural concept by integrating Software Defined Networking (SDN) and Network Function Virtualization (NFV) paradigms, together with Mobile Fog/Edge Computing (MFEC). In addition, we applied this reference architectural model to the Internet of Vehicles (IoV) domain by addressing complex mobile Intelligent Transportation Services (ITSs) with stringent temporal and spatial requirements. To this purpose, we design the vehicular communications ecosystem according to a 5G vision, as it supports both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) links by means of the cellular-enabled Vehicle-to-Everything (V2X) interface. In particular, we focus on a generalized SDN-controlled handover which is capable to handle complex traffic patterns, i.e., supporting groups of mobile nodes, geocast information delivering, and even the involvement of multiple eNodeBs. The idea behind our proposal is to provide a complete ITS migration that seamlessly allows to move the virtualized service (i.e., a VNF), requested by some vehicles, towards the most suited Fog/Edge Server (FESs). Finally, a strategy, called Swapping Migration, that can optimize both the resource utilization and availability, together with the Quality of Service and Experience (QoSE), has been introduced. This could enable innovative services like complex and composite route planner, autonomous driving, Tactile Internet (TI) inspired vehicles controlling in a green mobility perspective.*

1 Introduction and State of Art

The ever-increasing number of vehicles and their densification within typical mega-cities pose a remarkable challenge to the automotive industry and to public administrations in order to provide transportations safety and efficiency in a Smart City by relying on *smart* cars [2]. To this purpose, the emphasis should be put on *group* intelligence, rather than on individual capabilities of a device, which is, in fact, constrained and not able to face time-varying and unpredictable operative conditions. Recently, information and communication technologies (ICTs) have been regarded as the way to lead vehicular networks toward a revolutionary road. Connecting vehicles via Vehicular Ad-hoc Networks (VANET) represented an early attempt to support this vision, where closer vehicles are allowed to communicate with each other via Vehicle-to-Vehicle (V2V) or Vehicle-to-Infrastructure (V2I) interfaces to notify or collect traffic-related information, respectively [6][7]. Thanks to their high data rates and low latency communications, 5G

IoT-enabled Smart Monitoring and Optimization for Industry 4.0

Luca Davoli, Laura Belli, Gianluigi Ferrari

Internet of Things (IoT) Lab, University of Parma & things2i s.r.l.

CNIT, Research Unit of Parma

Abstract: *In the last decades, forward-looking companies have introduced Internet of Things (IoT) concepts in several industrial application scenarios, leading to the so-called Industrial IoT (IIoT) and, restricting to the manufacturing scenario, to Industry 4.0. Their ambition is to enhance, through proper field data collection and analysis, the productivity of their facilities and the creation of real-time digital twins of different industrial scenarios, aiming to significantly improve industrial management and business processes. Moreover, since modern companies should be as "smart" as possible and should adapt themselves to the varying nature of the digital supply chains, they need different mechanisms in order to (i) enhance the control of the production plant and (ii) comply with high-layer data analysis and fusion tools that can foster the most appropriate evolution of the company itself (thus lowering the risk of machine failures) by adopting a predictive approach. Focusing on the overall company management, in this chapter we present an example of a "renovation" process, based on: (i) digitization of the control quality process on multiple production lines, aiming at digitally collecting and processing information already available in the company environment; (ii) monitoring and optimization of the production planning activity through innovative approaches, aiming at extending the quantity of collected data and providing a new perspective of the overall current status of a factory; and (iii) a predictive maintenance approach, based on a set of heterogeneous analytical mechanisms to be applied to on-field data collected in different production lines, together with the integration of sensor-based data, toward a paradigm that can be denoted as Maintenance-as-a-Service (MaaS). In particular, these data are related to the operational status of production machines and the currently available warehouse supplies. Our overall goal is to show that IoT-based Industry 4.0 strategies allow to continuously collect heterogeneous Human-to-Things (H2T) and Machine-to-Machine (M2M) data, which can be used to optimize and improve a factory as a whole entity.*

1 Introduction

The wide adoption of Internet of Things (IoT) technologies has lead to a greater connectivity in industrial systems, i.e., to the paradigm of Industrial IoT (IIoT). The recent literature provides several relevant definitions for IIoT, which can be summarized as a collection of Smart Objects (SOs), cyber-physical assets, together with generic information technologies and Cloud or Edge Computing platforms allowing real-time and intelligent

transportation systems according to increasingly stringent environmental quality targets. In this context, this paper introduces an innovative mobility system based on small and low-emission vehicles aimed to spread Mobility as a Service (MaaS) paradigm. The proposed system is based on a connected heterogeneous intelligent and personalized architecture integrated within an Intelligent Transportation System (ITS) framework. We assume the mobility as no longer a product, but the interconnection of different transport modes to find the best alternative based on comfort and convenience. As a result, this mobility system will provide a service with intermediate features between the private car and transit systems without fixed-scheduling and fixed-routes.

1. Introduction

Urban and extra-urban mobility management is becoming highly complex when considering the main external impacts linked to traffic congestion, air pollution, noise and accidents.

If these impacts are neglected, it results in a loss of efficiency, increasing costs of public and private resources, and an unacceptable level of costs for sustainability.

According to the White Paper [1], the European Commission is setting up increasingly stringent environmental quality targets, such as a 60% reduction for transport emissions within 2050. Consequently, all governments should set up a broader range of leverages, policies, adoption of state-of-the-art technologies, revised economic models, tax incentives and contributions to driving investment towards new sustainable, intermodal and innovative mobility systems. In particular, the White Paper specifies the main strategies to be adopted like the improvement of vehicles' energy efficiency and more efficient use of transport modes, considering Intelligent Transportation Systems for information to users and traffic management. Moreover, strategies for urban transport and commuting involve the gradual elimination of conventional fuel vehicles, encouraging the use of smaller, lighter and specialized passenger cars, and the increase of collective transport demand.

In 2014, the Italian Ministry of Infrastructure and Transport adopted the National Plan for Intelligent Transport Systems (ITS) [2]. It pushes towards

An IoT Solution and Real-Time Detection System for Crop Protection against Ungulates

Mike O. Ojo[1], Davide Adami[2] and Stefano Giordano[1]

[1]Department of Information Engineering, Università di Pisa, Italy

[2]CNIT Research Unit, Department of Information Engineering, Università di Pisa, Italy

Abstract: *Advances in standards and protocols driven by the increasing interest in the Internet of Things (IoT) are allowing for more choice in design, thus making smart agriculture, among other sectors, to be more cost effective. The plethora of IoT compatible sensors, wireless transmission systems, and other system elements is already allowing designers a much higher degree of flexibility in realizing new designs for heretofore special purpose systems. This paper presents the development of IoT applications for crop protection to prevent animal intrusions in the crop field. A repelling and a real-time monitoring system are provided to prevent potential damages in agriculture from wild animal attacks. Moreover, this paper provides an in-depth description of a complete solution we designed and deployed, that consists of the low-power wireless network, the neural network solution for animal detection and the back-end system. Specifically, we develop a methodology for deploying the network and present the open-source tools to assist with the deployment, and to monitor the network. The system also allows the integration of neural networks that allows a real-time animal detection. Lastly, this paper also discusses how the technology used is the right one for smart agriculture in relation to crop protection.*

1 Introduction

Statistical data shows that there has been a massive surge in the loss of wine production due to the crop damages caused by animal attacks for the past 3 decades. In general, especially in Europe, the number of wine production losses due to animals' amount to 75% of the total wine production loss. Similarly, frightening statistics come from the United states wine production, that apart from the California fires, wildlife attacks to crop production has been on the increase. Taking Italy as an example, the annual production loss in the wine industry is estimated to be 13 million euros, with an annual cost to the government estimated around 3 million euro [1, 2].

Considering the above, there have been several ways to keep animals from destroying crop, which can be lethal means and sometimes non-lethal means. Lethal ways such as shooting, trapping, string and stone, are very cruel and not environment friendly, while non-lethal means such as scarecrow, chemical repellents, organic substances, fencing are sometimes inadequate, non-substantial, time consuming and also expensive [3]. Some of these methods even have environmental pollution effect on both humans and animals [4]. Technology assistance at various stages of agricultural processes can significantly enhance